TREND MICRO™

5.2 TREND MICRO™ Virtual Mobile Infrastructure

Installation and Deployment Guide

Centrally-managed workspace for mobile users

Endpoint Security

Document Part No.: APEM57685/161227

Release Date: December 2016

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 Virtual Mobile Infrastructure

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

Index

Preface

Preface

Welcome to the Trend Micro™Virtual Mobile Infrastructure™ version 5.2 Administrator's Guide. This guide provides detailed information about all Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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)

Virtual Mobile Infrastructure Documentation

The Virtual Mobile Infrastructure documentation consists of the following:

- *Installation and Deployment Guide*—this guide helps you get "up and running" by introducing Virtual Mobile Infrastructure, and assisting with network planning and installation.
- *Administrator's Guide*—this guide provides detailed Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure

This chapter assists administrators in planning the server components for Trend Micro™Virtual Mobile Infrastructure™.

This chapter contains the following sections:

About Virtual Mobile Infrastructure

Trend Micro Virtual Mobile Infrastructure is a service that hosts independent workspaces for every user. A user workspace is based on the Android operating system, which is accessible via the Virtual Mobile Infrastructure 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, Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure

Virtual Mobile Infrastructure 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 Enterprise Infrastructure	Provides integration with LDAP and external storage.

System Requirements

Review the following requirements before installing Virtual Mobile Infrastructure.

Table 1-1. System Requirements for Server

Component	Requirements
Processor	64-bit x86 four-core Intel processor with SSSE3 support
Memory	4-GB
Hard disk	30-GB available for installation

COMPONENT	REQUIREMENTS
Network Card (NIC)	One 1-GB NIC

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 Virtual Mobile Infrastructure mobile client

COMPONENT	REQUIREMENTS
Operating system	• iOS 7.0 or later • Android 4.0 or later • Windows 8.1/Windows Phone 8.1, Windows 10 Mobile

Architecture of Virtual Mobile Infrastructure

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

Trend Micro Virtual Mobile Infrastructure also supports large-scale deployment at different sites. If your users are located at different geographical locations, you can deploy Virtual Mobile Infrastructure servers at these sites to provide efficient service to users. You can manage all the servers from one centralized location.

Single Server Installation Model

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

Note

Trend Micro strongly recommends deploying Secure Access in your environment to enable mobile clients to access Virtual Mobile Infrastructure Server via Internet. See *Why Use Secure Access on page 1-9* for more information.

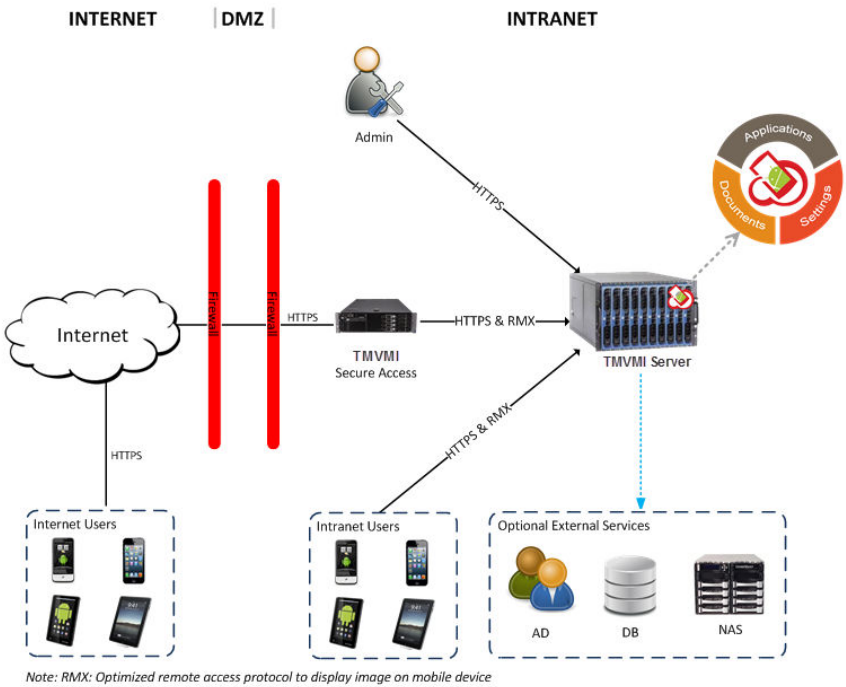


FIGURE 1-1. Trend Micro Virtual Mobile Infrastructure Single Server Installation Model

Multiple Server Installation Model

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

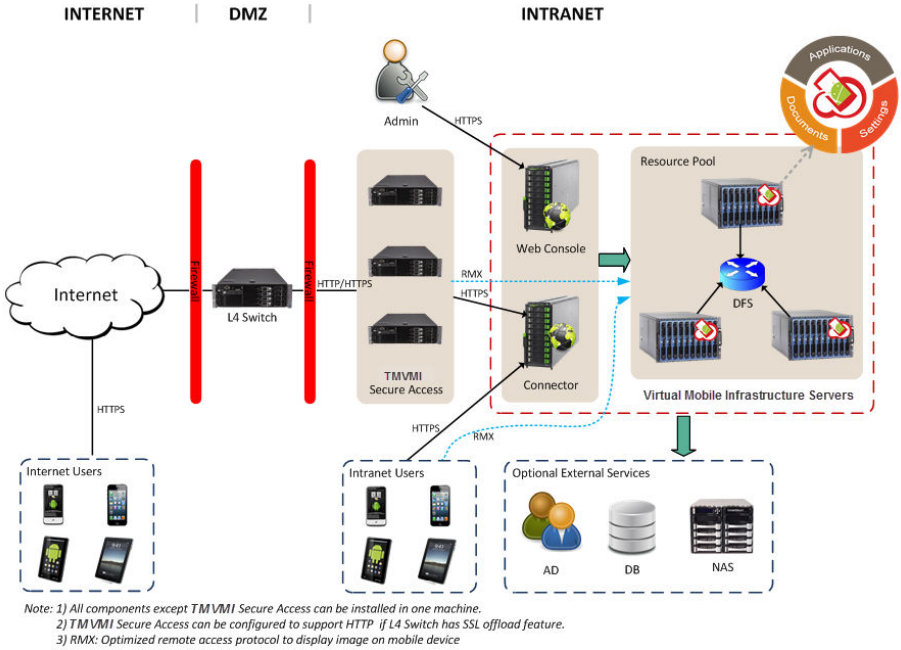


FIGURE 1-2. Trend Micro Virtual Mobile Infrastructure Multiple Server Installation Model

Multiple Sites Deployment Model

The Multiple Sites Deployment Model is the deployment of Virtual Mobile Infrastructure Server at separate geographical locations.

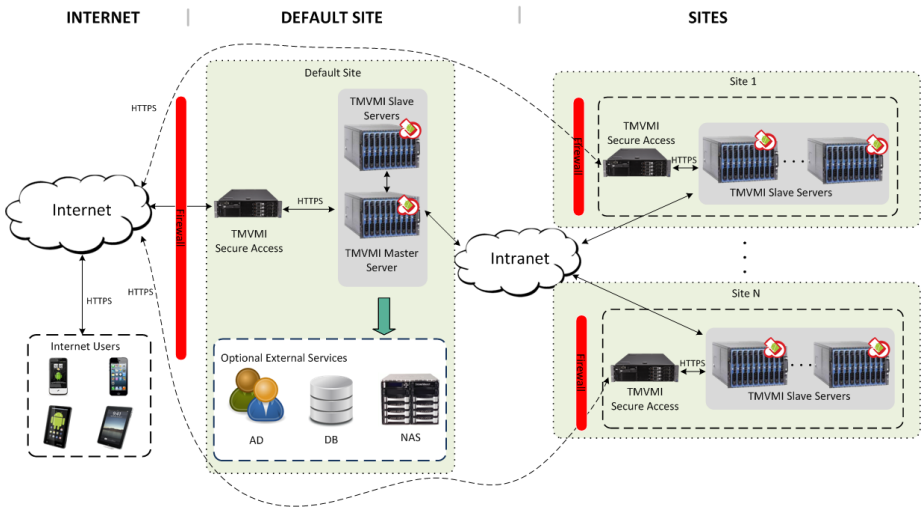


FIGURE 1-3. Trend Micro Virtual Mobile Infrastructure Multiple Site Deployment Model

Components of Virtual Mobile Infrastructure

The Virtual Mobile Infrastructure system includes the following components:

TABLE 1-4. Virtual Mobile Infrastructure Components

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Virtual Mobile Infrastructure Server	The Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure instance.	Required
Virtual Mobile Infrastructure Mobile Client Application	The mobile client application is installed on the mobile devices. The client application connects with the Virtual Mobile Infrastructure server to allow users to use their workspaces hosted on the server.	Required
Secure Access	The Virtual Mobile Infrastructure Secure Access enables mobile clients to access Virtual Mobile Infrastructure server via Internet. See *Why Use Secure Access on page 1-9* for more information.	Stongly recommended
Active Directory	The Virtual Mobile Infrastructure server imports groups and users from Active Directory.	Optional
External Database	External Database provides scalable data storage for user data. By default, Virtual Mobile Infrastructure 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

Why Use Secure Access

Virtual Mobile Infrastructure Secure Access enables mobile device clients to securely access the Virtual Mobile Infrastructure server via the Internet. If you do not want to expose the Virtual Mobile Infrastructure 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 a mobile device client enrollment request through HTTPS, and relays it to the Virtual Mobile Infrastructure server.
- Secure Access and Virtual Mobile Infrastructure server use a firewall for outbound network connections to ensure security.

Secure Access can be deployed in a DMZ or an 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 Virtual Mobile Infrastructure server.

Chapter 2

Installing on Bare Metal Servers

This chapter provides the information that you will need to install Trend Micro Virtual Mobile Infrastructure.

This chapter contains the following sections:

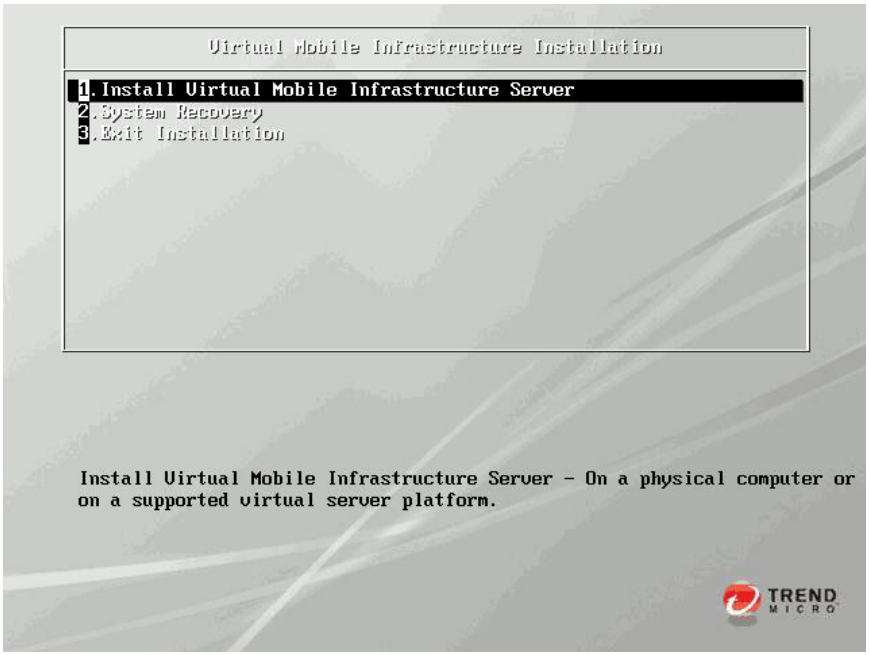
Installing Virtual Mobile Infrastructure Server on a Bare Metal Server

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

Procedure

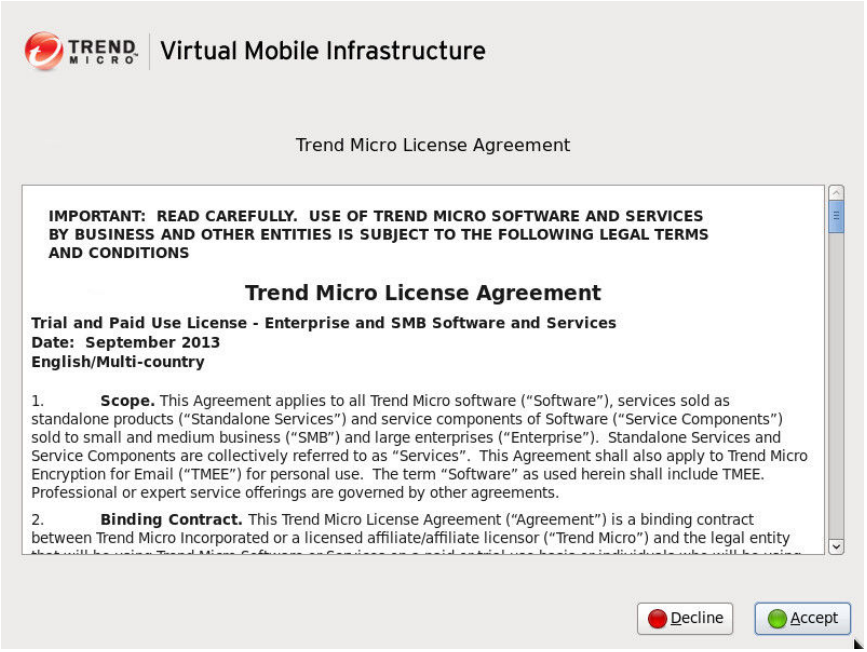
1. Power on the Bare Metal server where you want to install Virtual Mobile Infrastructure.
2. Insert the installation DVD into the DVD drive, and reboot the server.

   The Virtual Mobile Infrastructure installation menu appears.



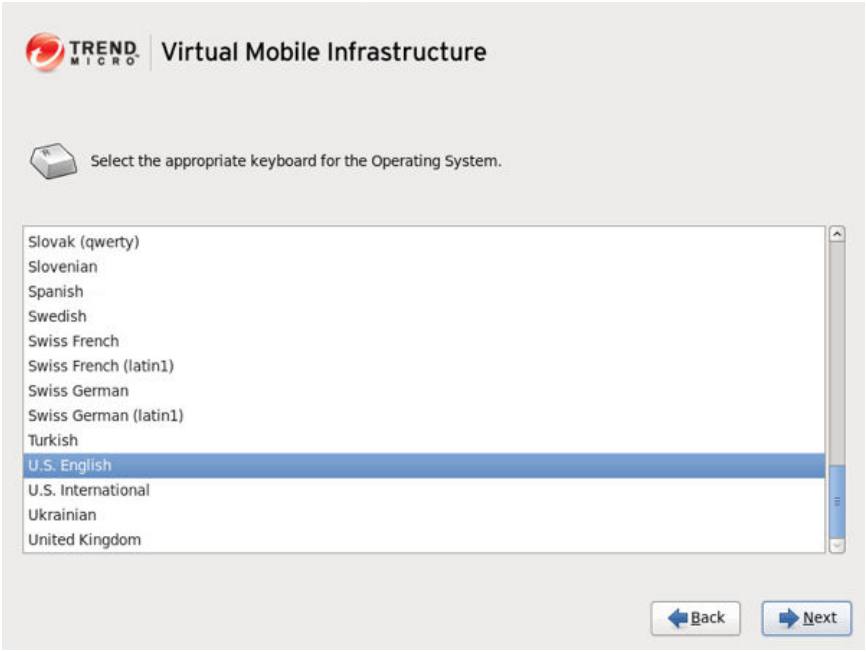
3. Select **Install Virtual Mobile Infrastructure Server** and press **Enter**.

The setup starts loading the installation image file. After it completes, **Trend Micro License Agreement** screen appears.



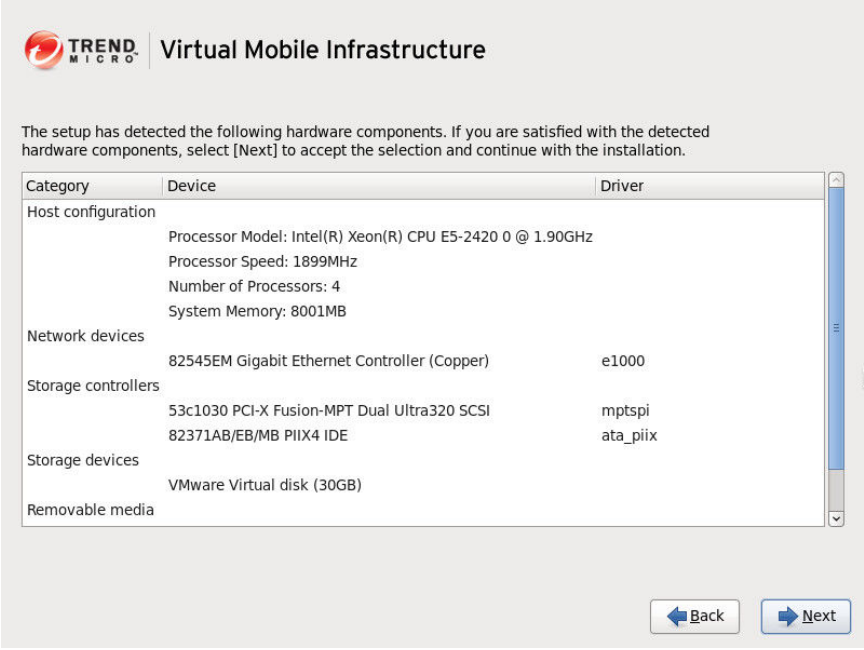
4. Click **Accept** to agree to the license agreement.

A screen appears where you can select a keyboard for the operating system.



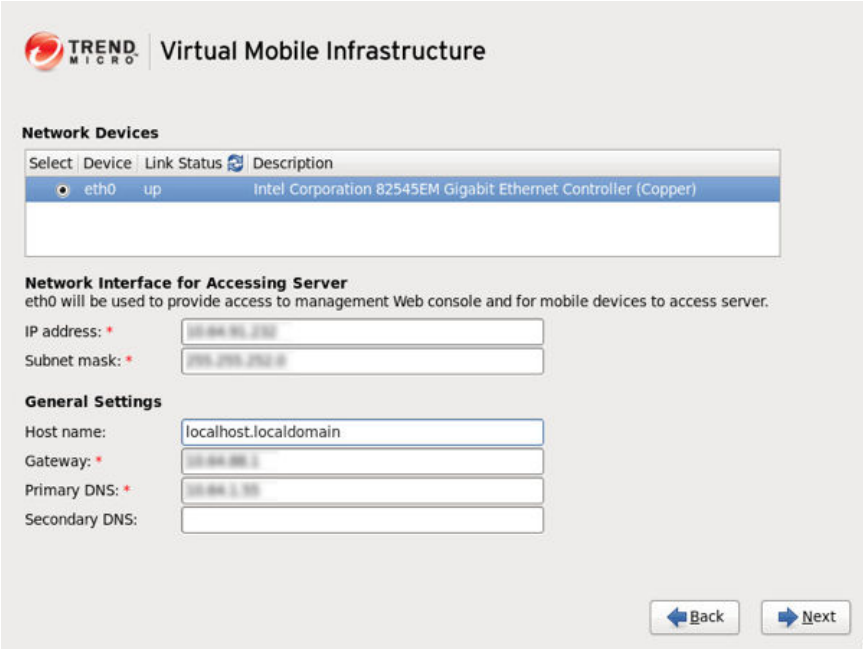
5. Select a keyboard for the operating system, and then click **Next**.

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 IP address for Virtual Mobile Infrastructure server Web console and for mobile client application to access Virtual Mobile Infrastructure server.
  - **Subnet mask**: the subnet mask for the internal and external IP address.
- **General Settings**:
  - **Host name**: type a Host name for Virtual Mobile Infrastructure server.
  - **Gateway**
  - **Primary DNS**

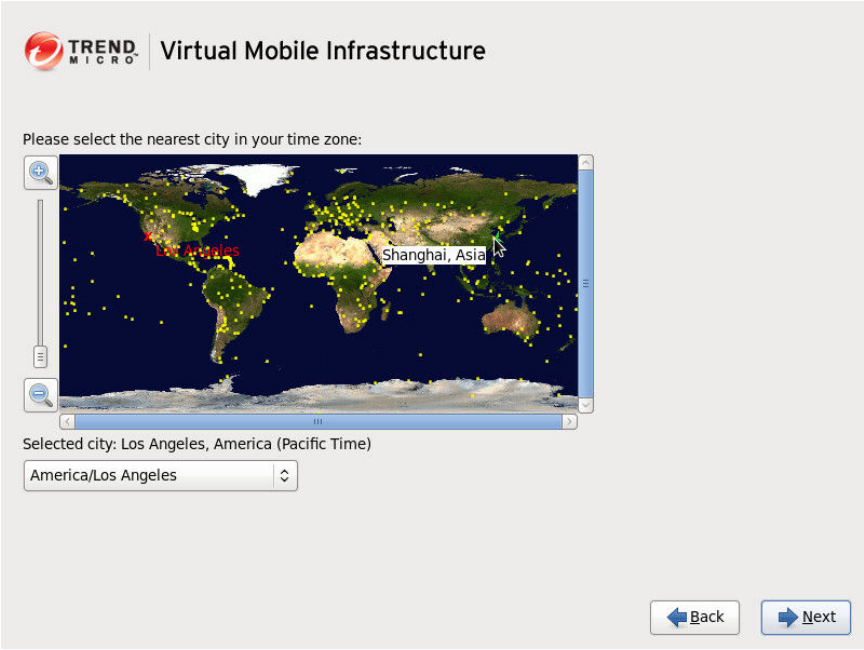
- Secondary DNS

Note

Make sure that the network interface **eth0** is 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, and the mobile client application will not be able to connect to the server.

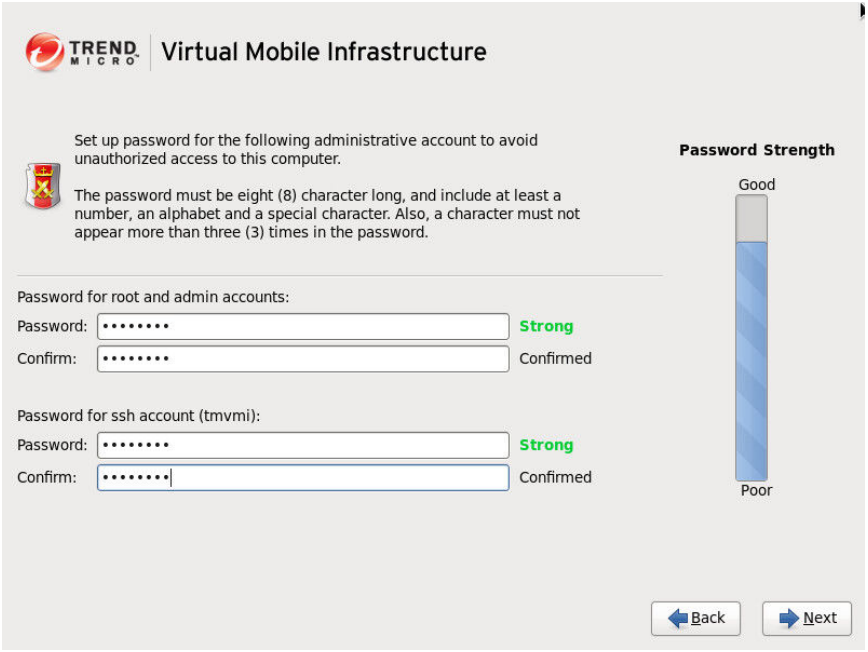
8. Click **Next**.

A screen appears where you can configre your server time zone.



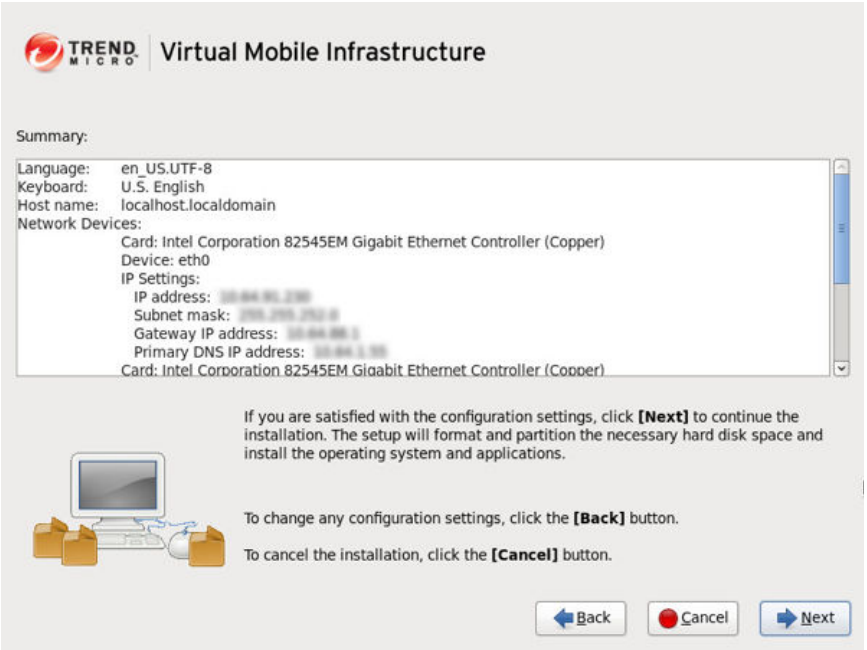
9. Select your time zone and click **Next**.

A screen appears where you can configure your operating system password.



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 Virtual Mobile Infrastructure 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 10 on page 2-8* of this procedure.

Installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure server.
     - **Subnet mask**: the subnet mask for the Virtual Mobile Infrastructure server IP address.
   - **General Settings**:
     - **Host name**: type a Host name for Virtual Mobile Infrastructure server.
     - **Gateway**
     - **Primary DNS**

- **Secondary DNS**

> **Note**
>
> If you are deploying Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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.

   - **Virtual Mobile Infrastructure server IP address**: type the IP address you configured for **eth0** of the Virtual Mobile Infrastructure server. If you have multiple sites configured, make sure to type the IP address of **eth0** of the Master Server configured in the Default Site.

     > **Note**
     >
     > If you have High Availability (HA) configured, type the common IP address on this screen.

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 2-12* 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 Virtual Mobile Infrastructure.

This chapter contains the following sections:

Installing Virtual Mobile Infrastructure Server

Installing Virtual Mobile Infrastructure 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. Installing Virtual Mobile Infrastructure (See *Step 2: Installing Virtual Mobile Infrastructure on VMware ESXi on page 3-13*).

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**.

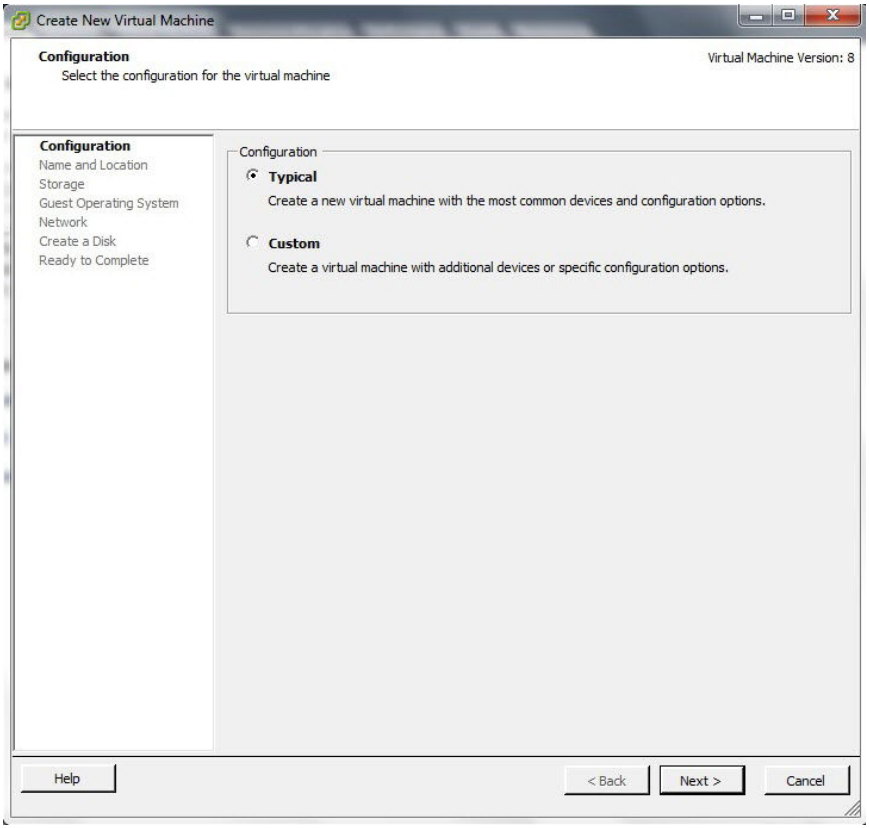


FIGURE 3-1. Select Configuration

The **Name and Location** screen appears.

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

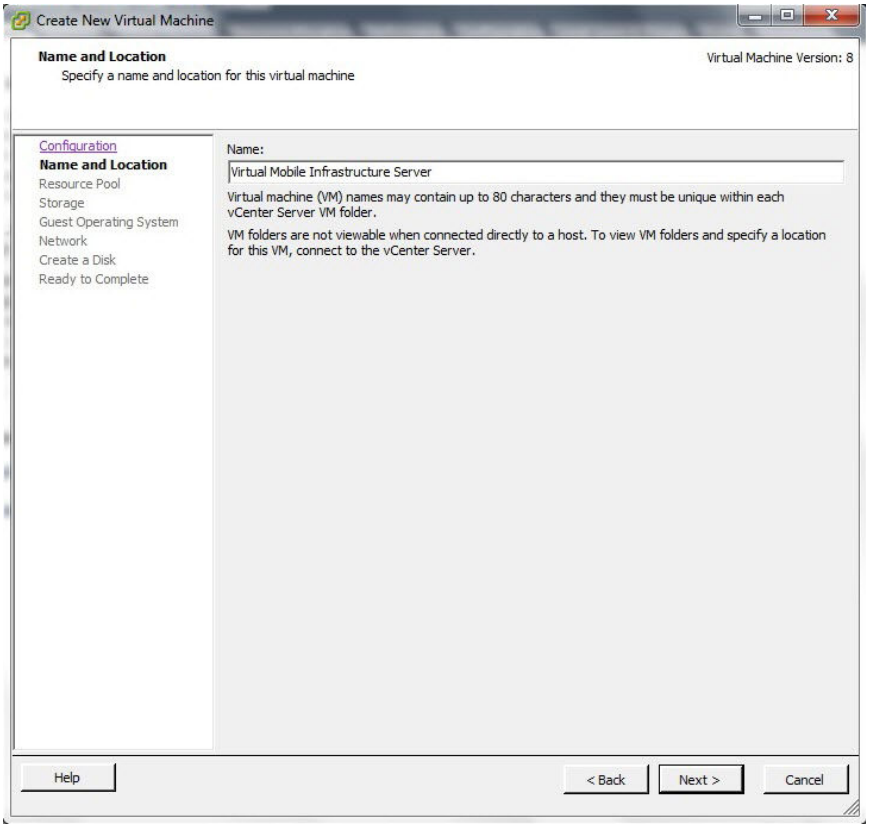


FIGURE 3-2. Type a name for the new virtual machine

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**.

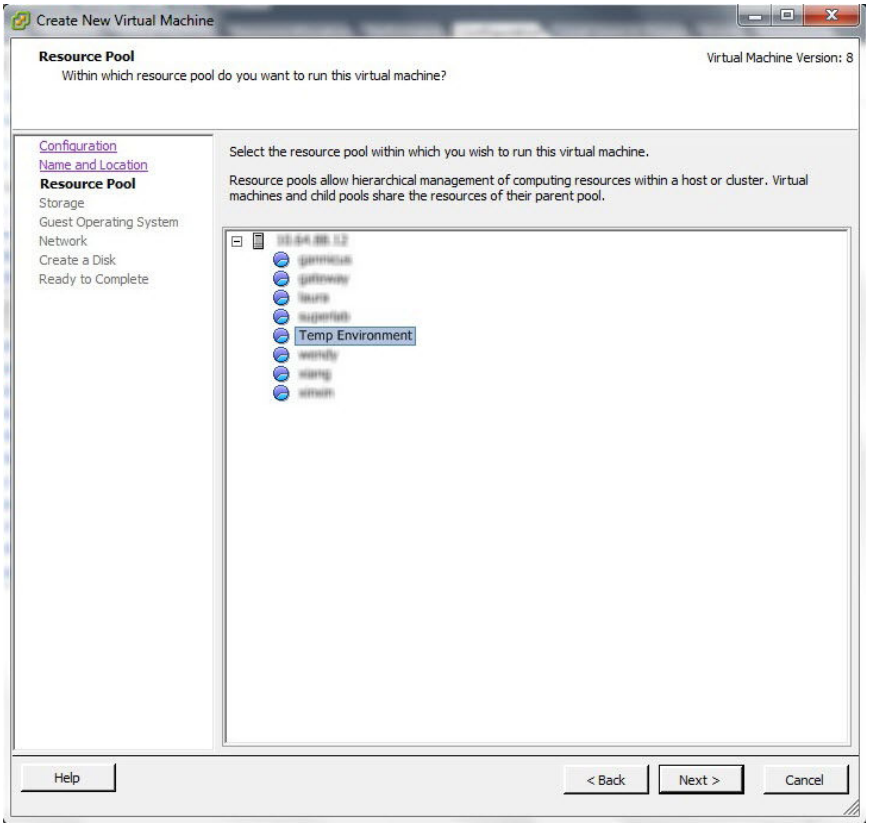


FIGURE 3-3. Select a resource pool

The **Storage** screen appears.

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

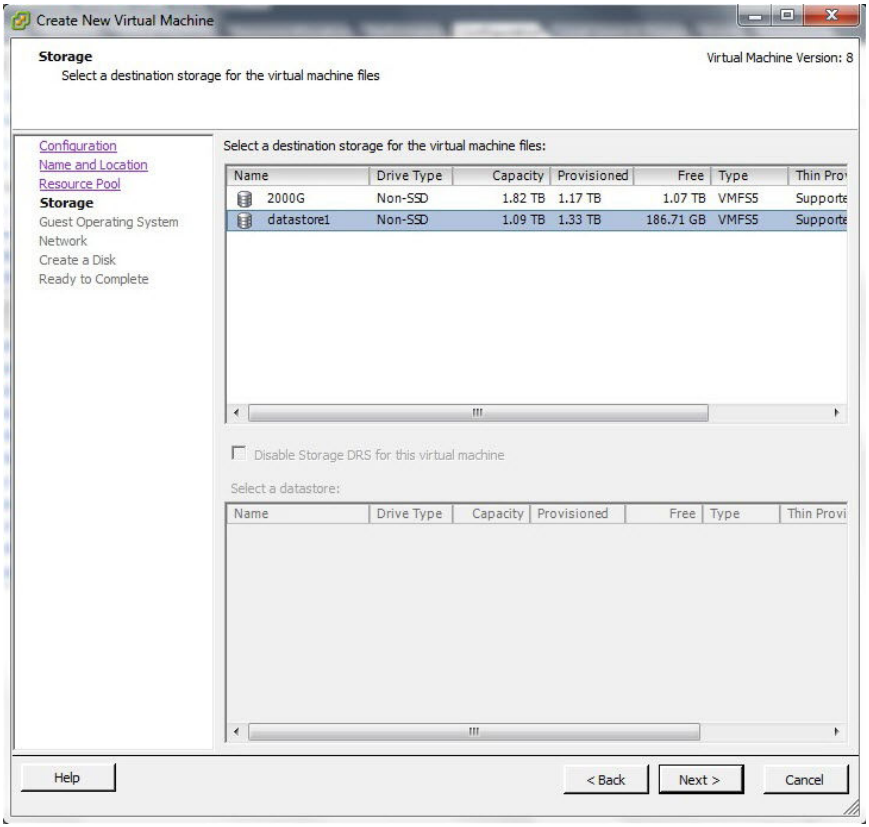


FIGURE 3-4. Select a storage to install Virtual Mobile Infrastructure Server

The **Guest Operating System** screen appears.

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

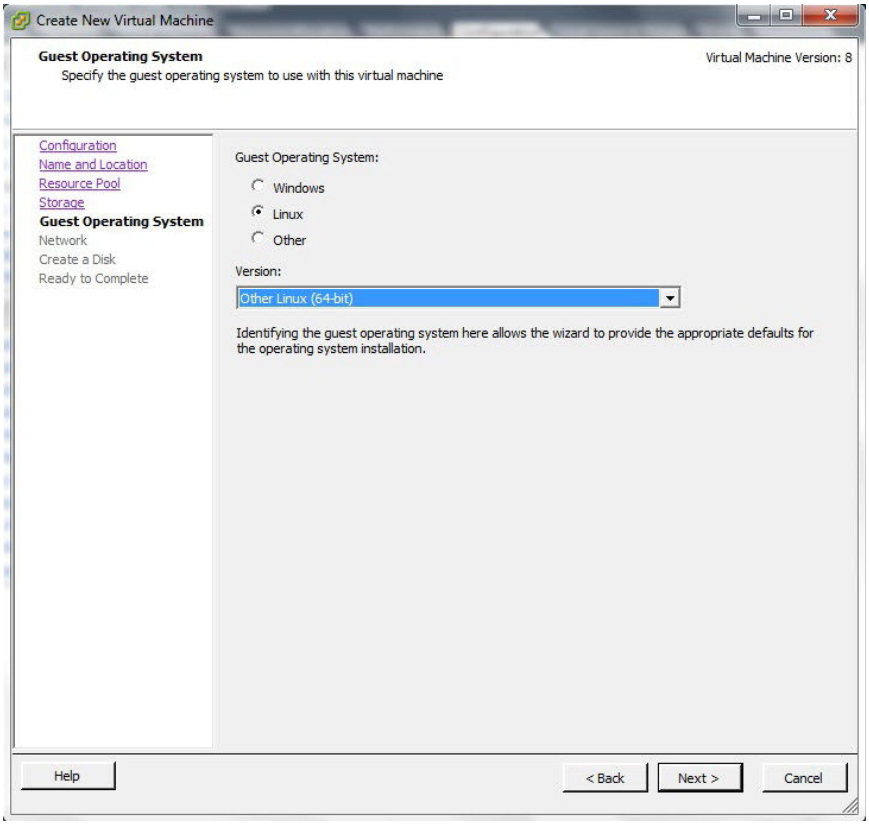


FIGURE 3-5. Select the guest operating system

The **Network** screen appears.

9. Select one NIC and specify the following settings:

TABLE 3-1. Network Settings for Virtual Mobile Infrastructure

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

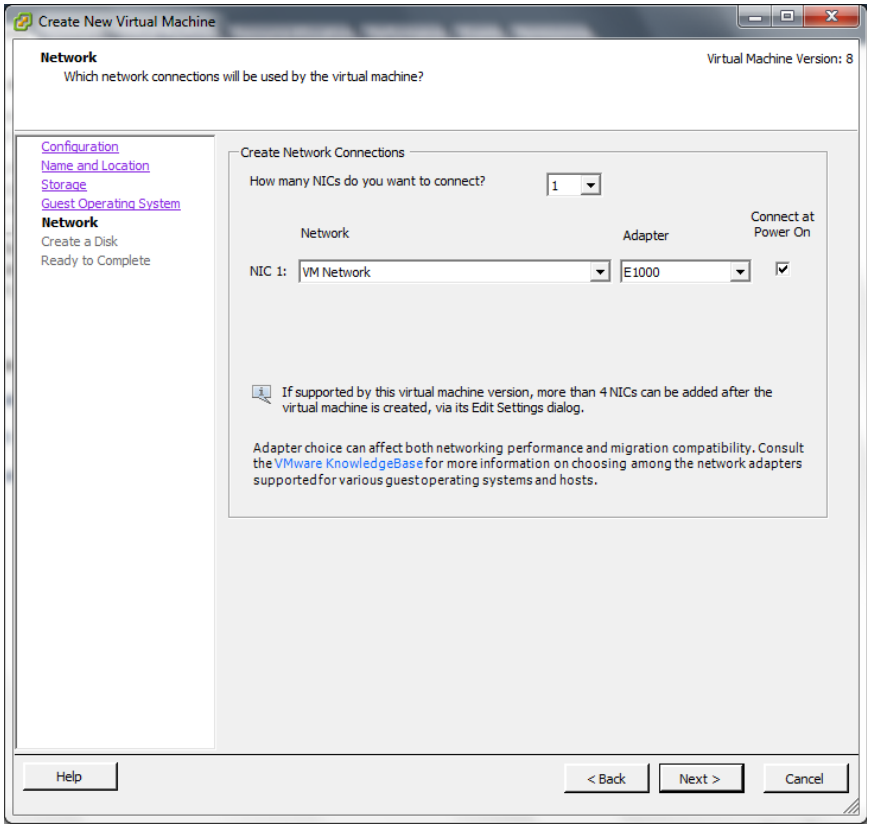


FIGURE 3-6. Create network connections

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 Virtual Mobile Infrastructure.

    b. Select **Thick Provision Lazy Zeroed**

    c. Click **Next**.

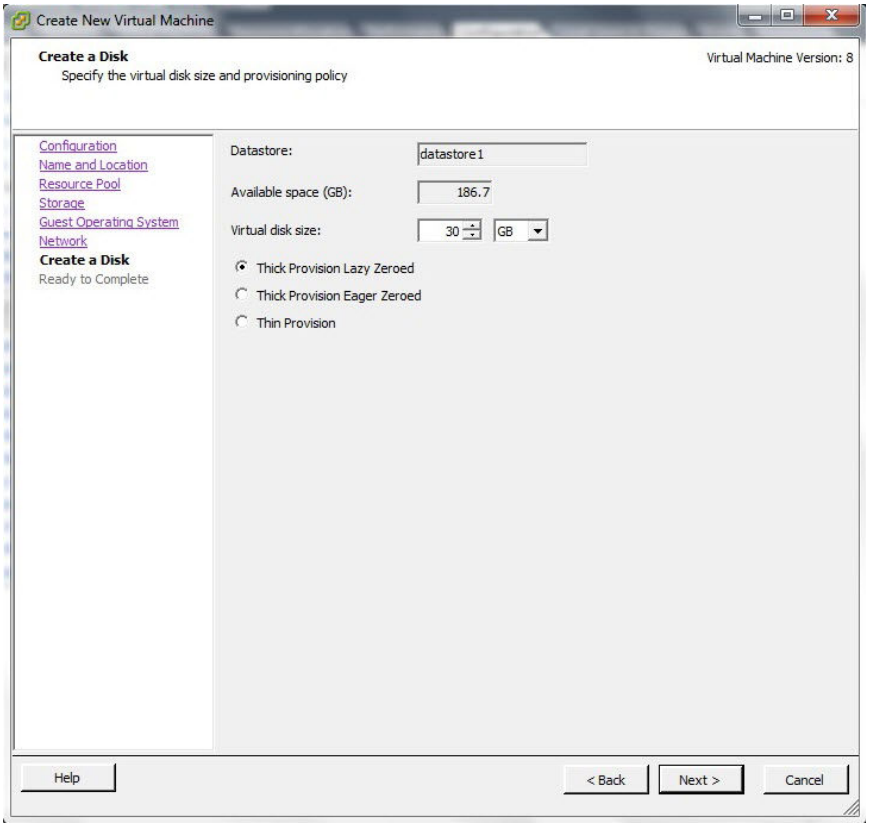


FIGURE 3-7. Specify Hard Disk Space

The **Ready to Complete** screen appears.

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

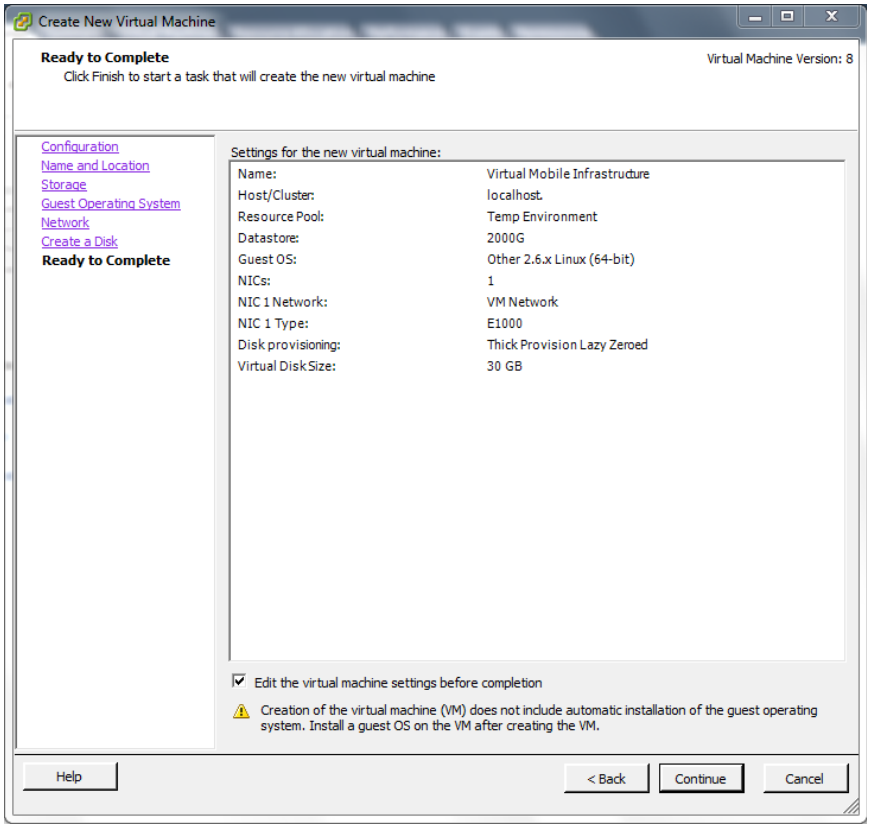


FIGURE 3-8. Ready to Complete

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.

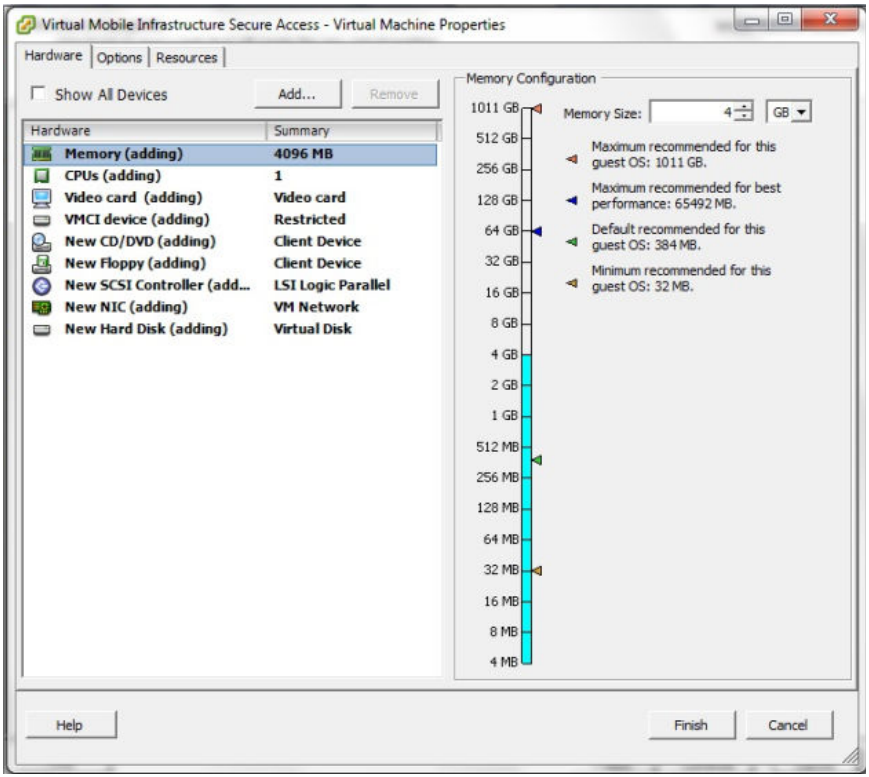


FIGURE 3-9. VM Properties - Memory Configuration

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**.

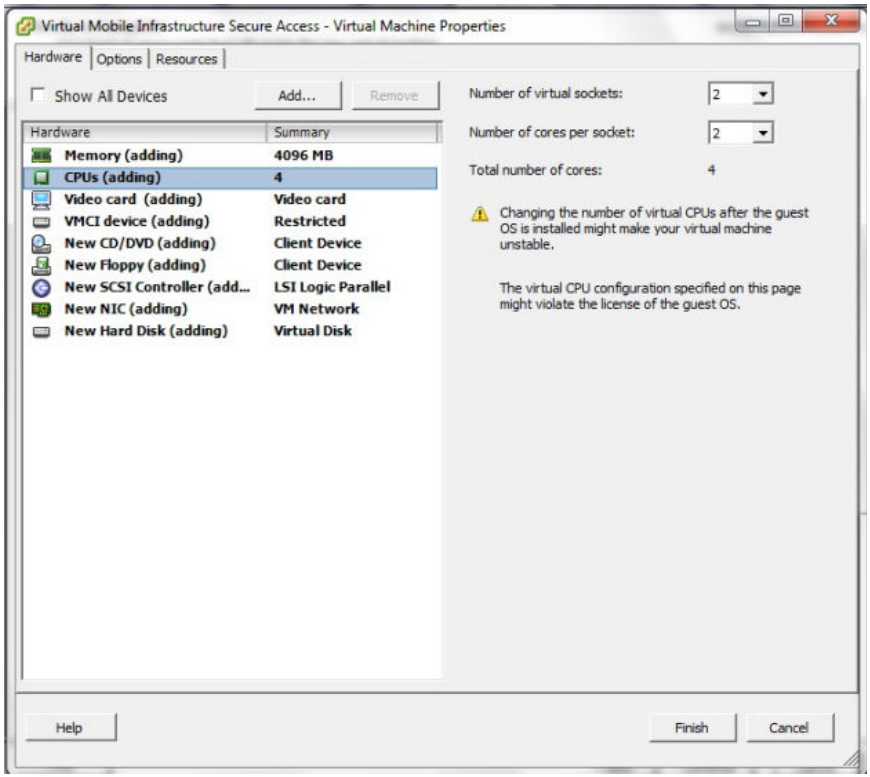


FIGURE 3-10. VM Properties - CPU Settings

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**.

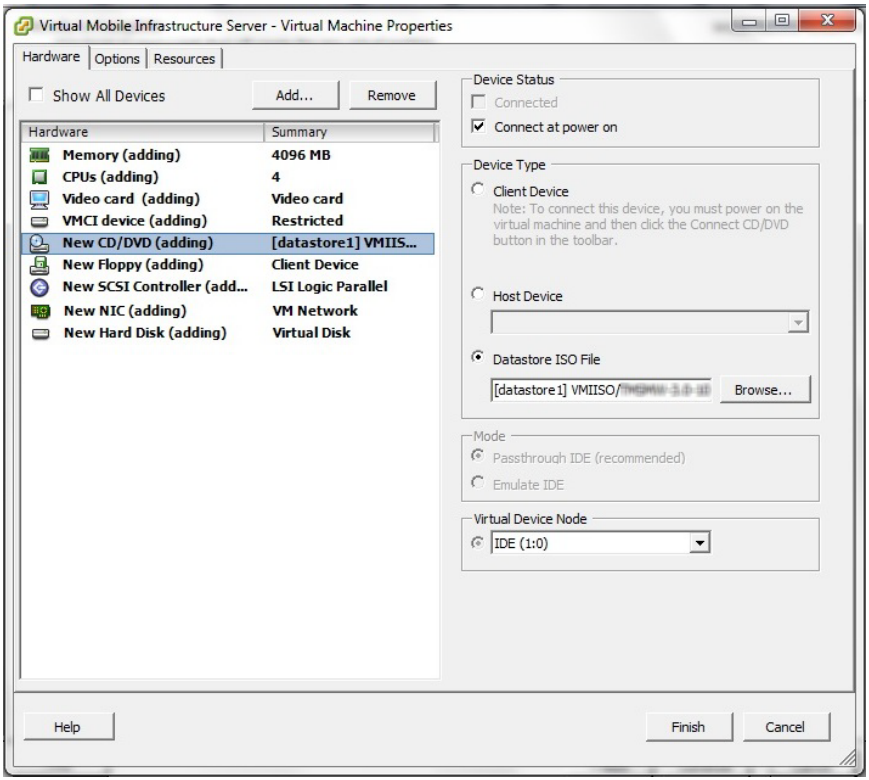


FIGURE 3-11. VM PROPERTIES - CD/DVD SETTINGS

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

Step 2: Installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure installation menu appears.

3. Follow *step 3 on page 2-2* to *step 11 on page 2-10* of the topic *Installing Virtual Mobile Infrastructure Server on a Bare Metal Server on page 2-2* to complete Virtual Mobile Infrastructure installation.

Installing Virtual Mobile Infrastructure 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 3-14*)
2. Installing Secure Access (See *Step 2: Installing Secure Access on VMware ESXi on page 3-26*)

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**.

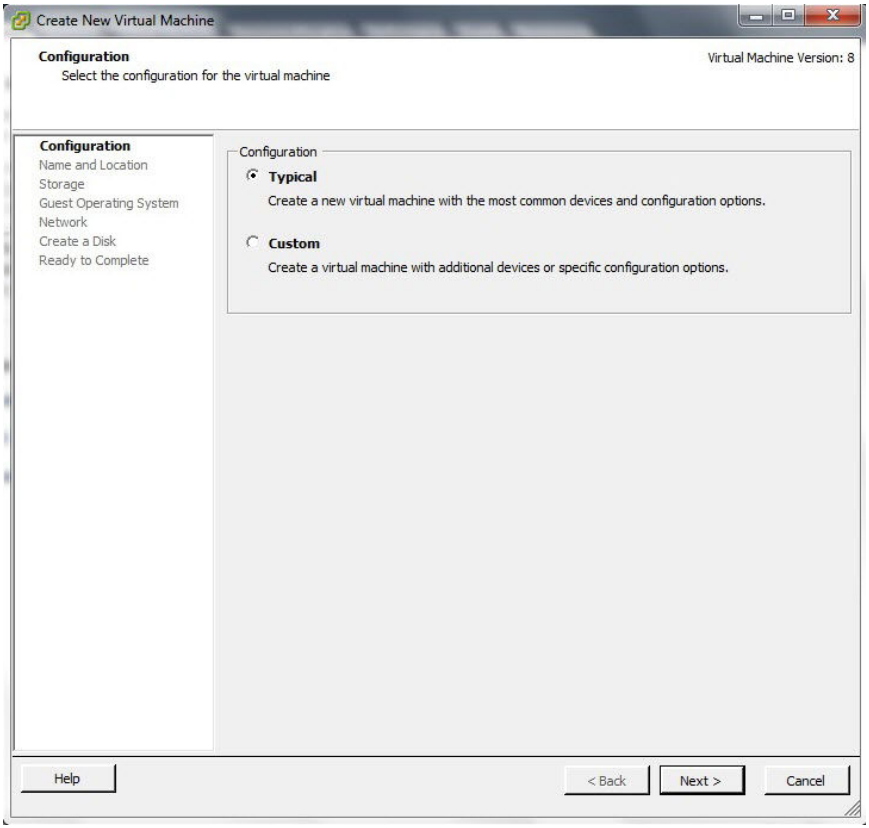


FIGURE 3-12. Select Configuration

The **Name and Location** screen appears.

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

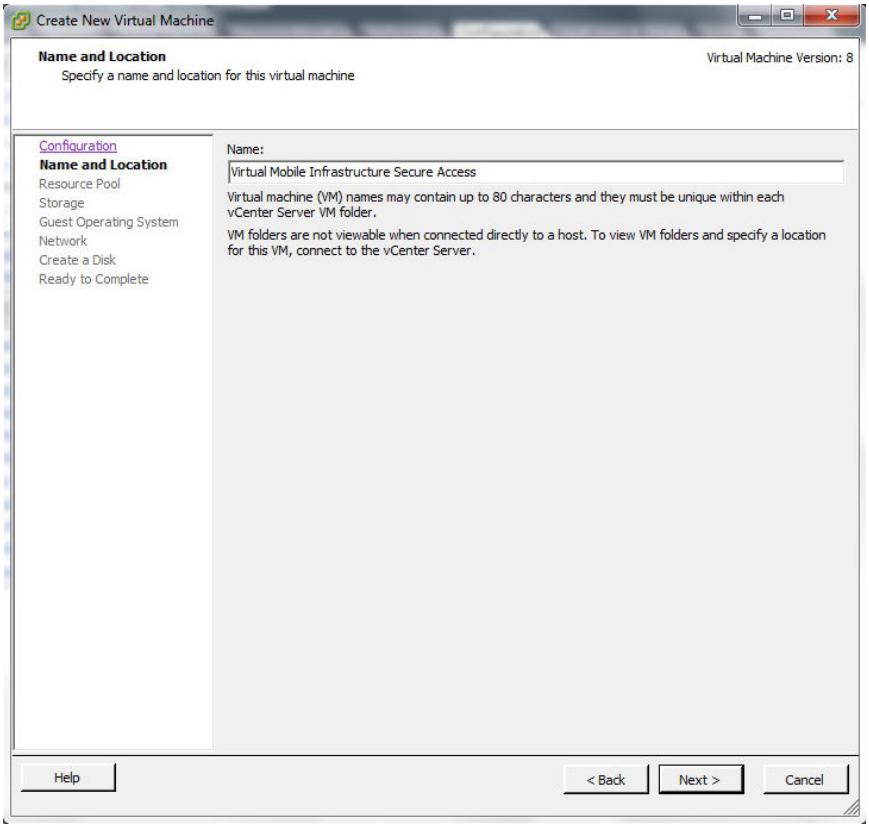


FIGURE 3-13. The Resource Pool screen appears.

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 3-16* and proceed to *step 7 on page 3-17* to configure the **Storage** screen.

---

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

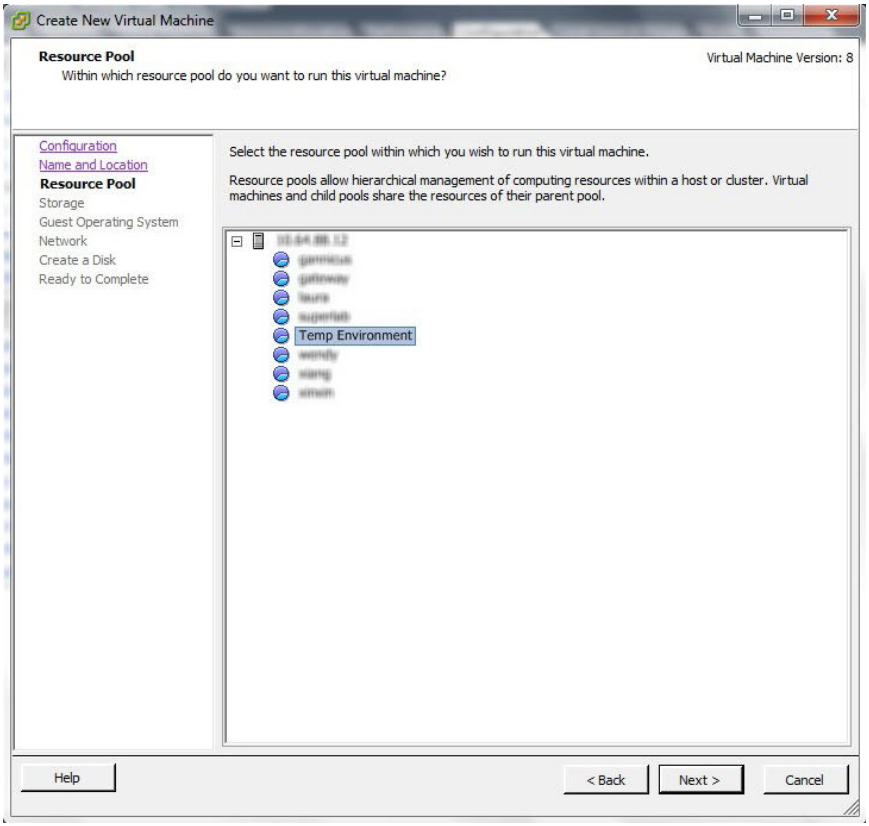


FIGURE 3-14. Select a resource pool

The **Storage** screen appears.

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

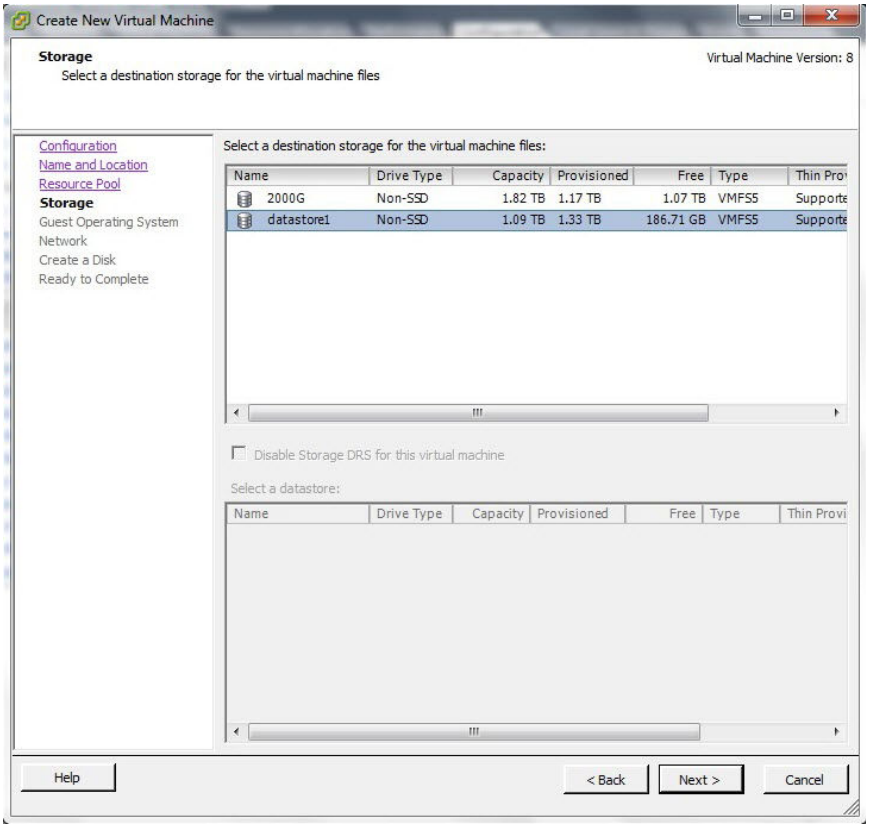


FIGURE 3-15. Select a storage to install Virtual Mobile Infrastructure Secure Access

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

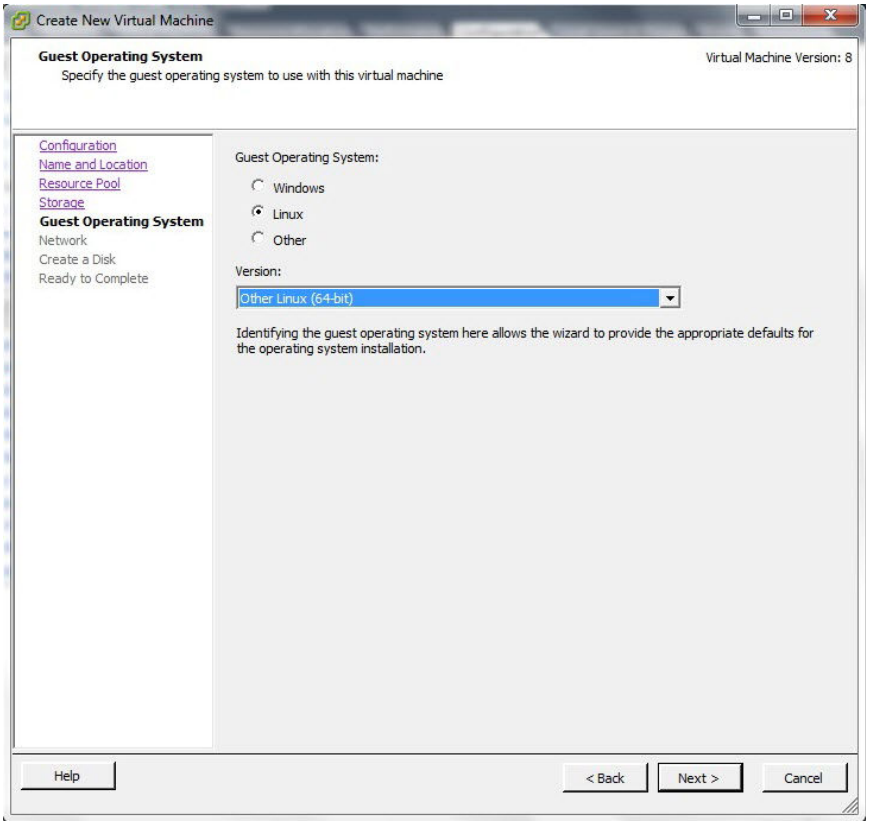


FIGURE 3-16. GUEST OPERATING SYSTEM

The **Network** screen appears.

9. Select one 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

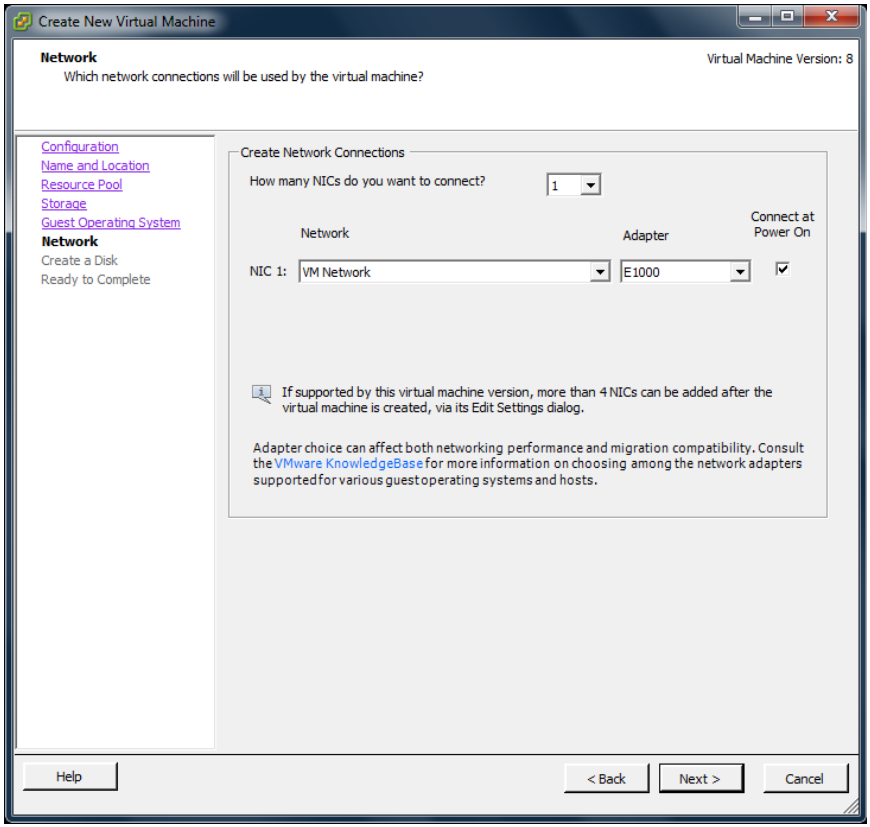


FIGURE 3-17. Create Network Connections

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 Virtual Mobile Infrastructure.

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

    c. Click **Next**.

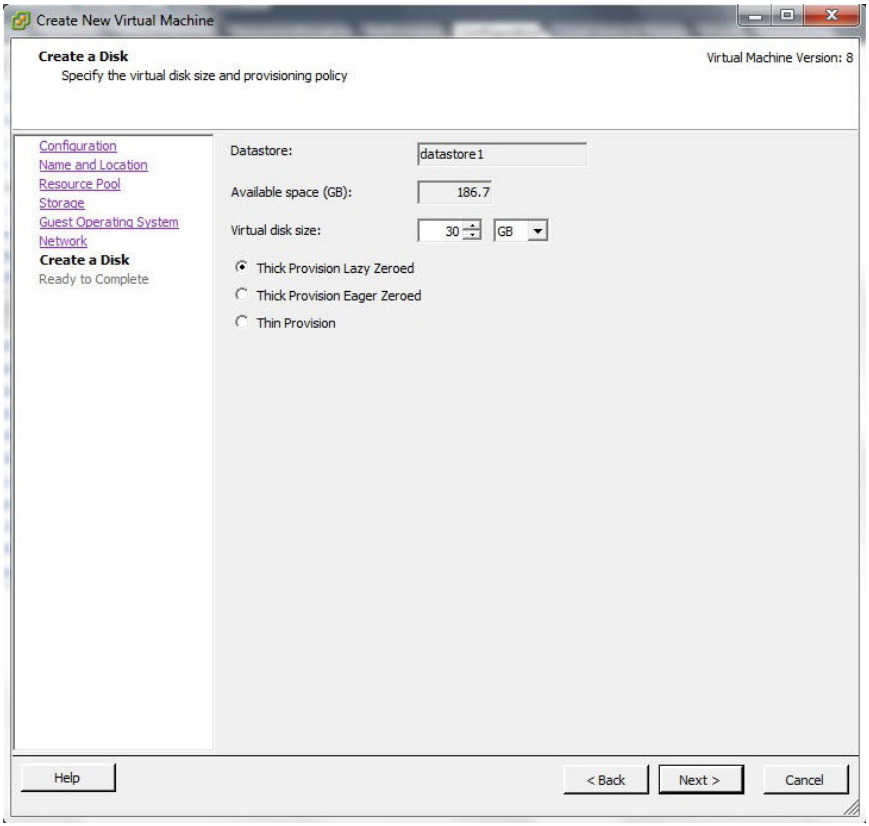


FIGURE 3-18. Specify Hard Disk Space

The **Ready to Complete** screen appears.

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

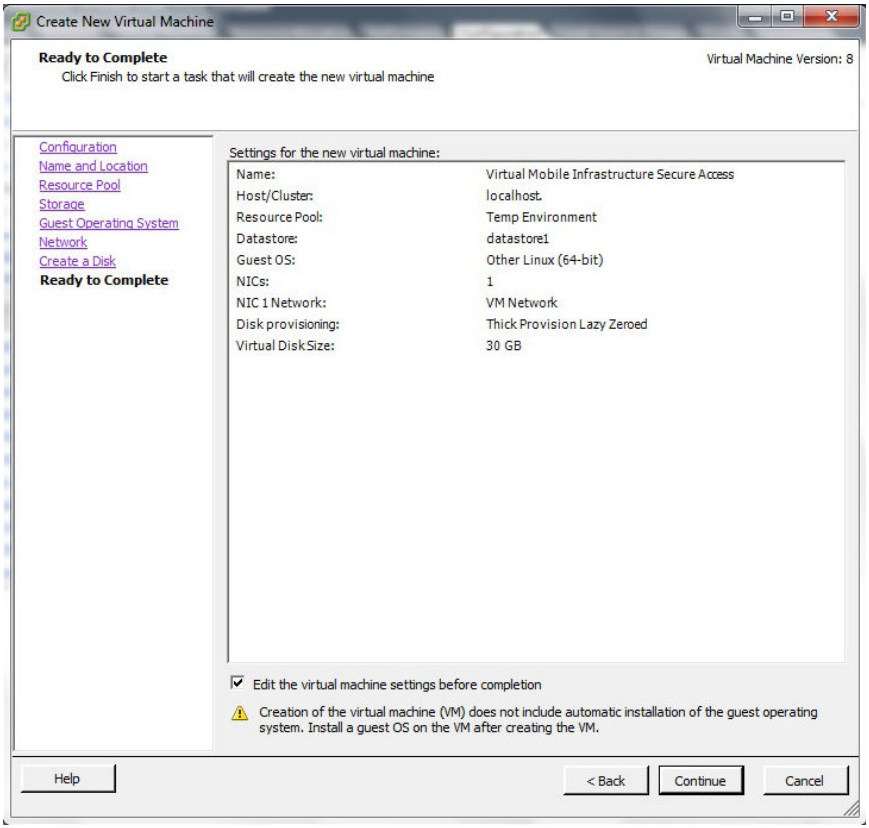


FIGURE 3-19. Ready to Complete

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.

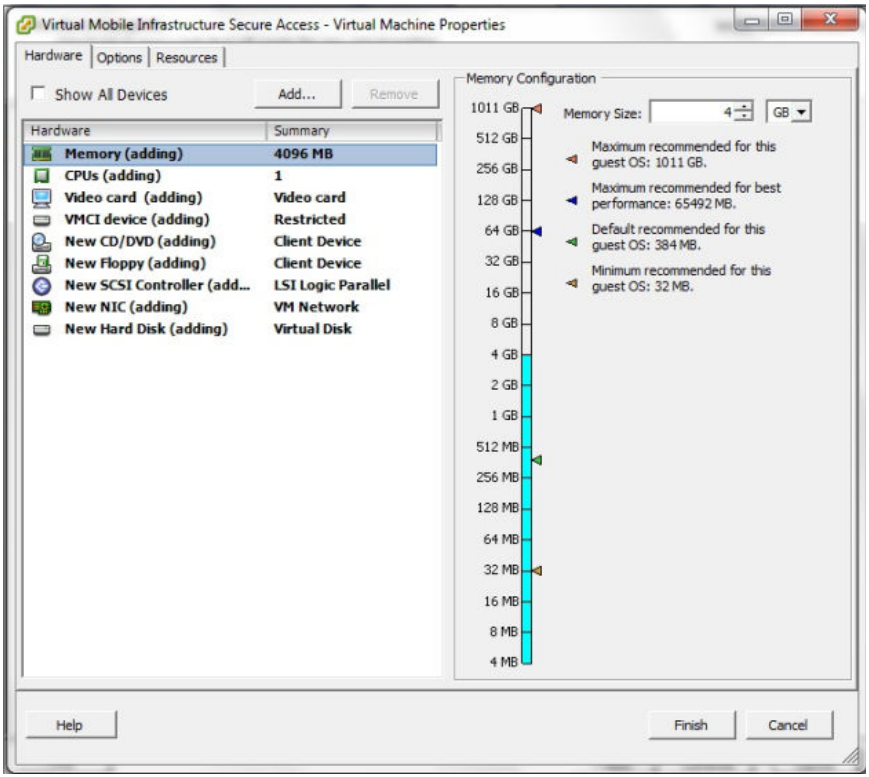


FIGURE 3-20. VM Properties - Memory Configuration

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

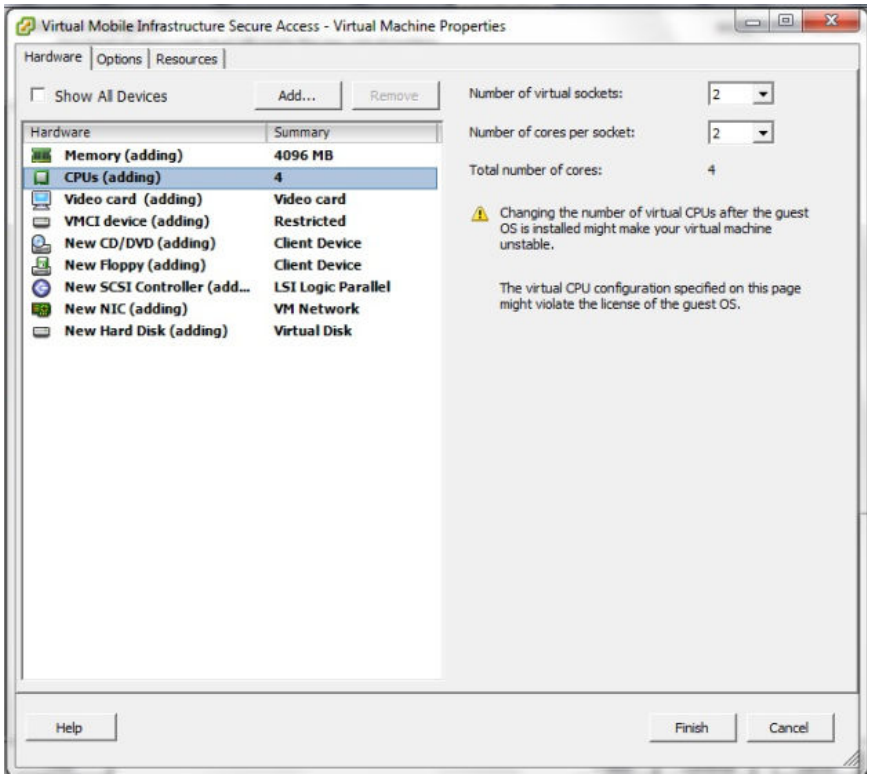


FIGURE 3-21. VM Properties - CPU Settings

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**.

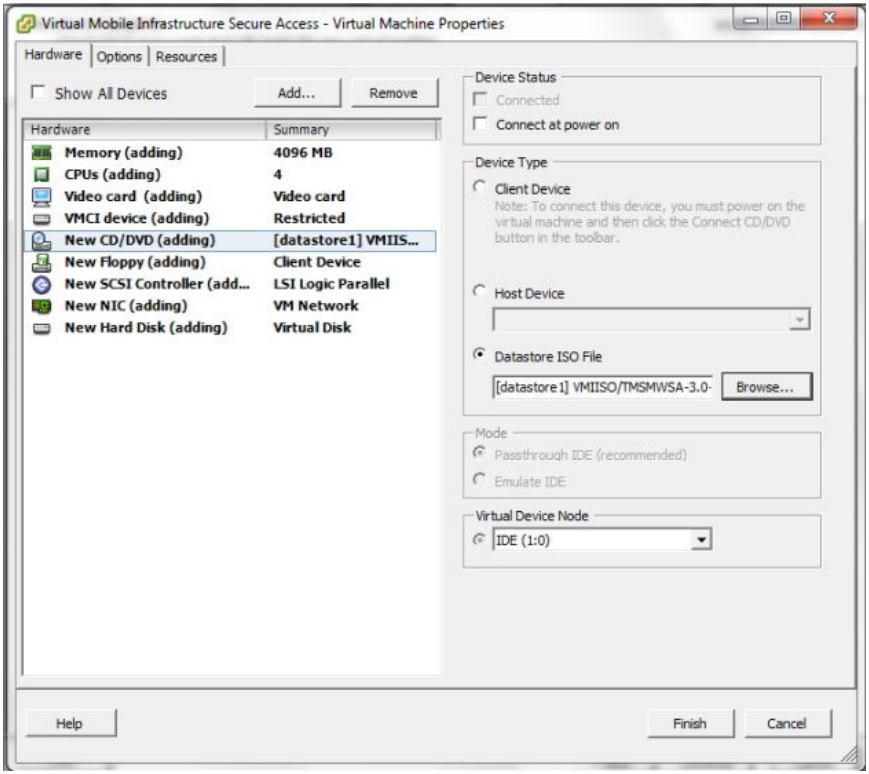


FIGURE 3-22. VM Properties - CD/DVD Settings

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 3-14*.
2. Click the **Console** tab on the virtual machine.

   The Secure Access installation menu appears.
3. Follow *step 3 on page 2-11* to *step 13 on page 2-13* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-10* 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 Virtual Mobile Infrastructure.

This chapter contains the following sections:

Installing Virtual Mobile Infrastructure Server

Installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure (See *Step 2: Installing Virtual Mobile Infrastructure 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

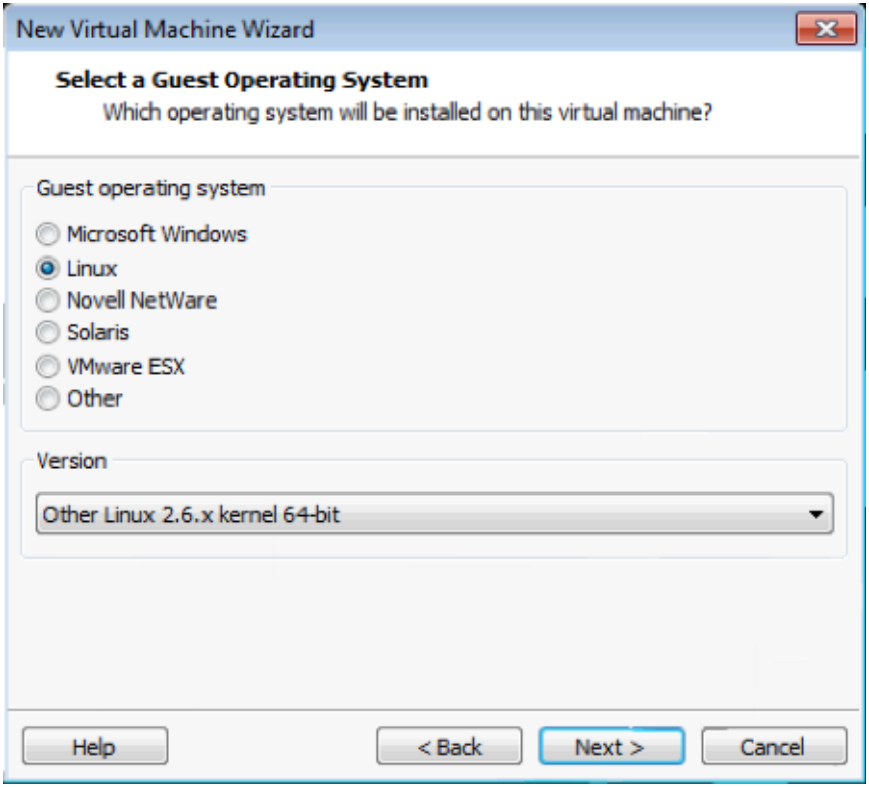


FIGURE 4-1. Select a guest operating system

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**.

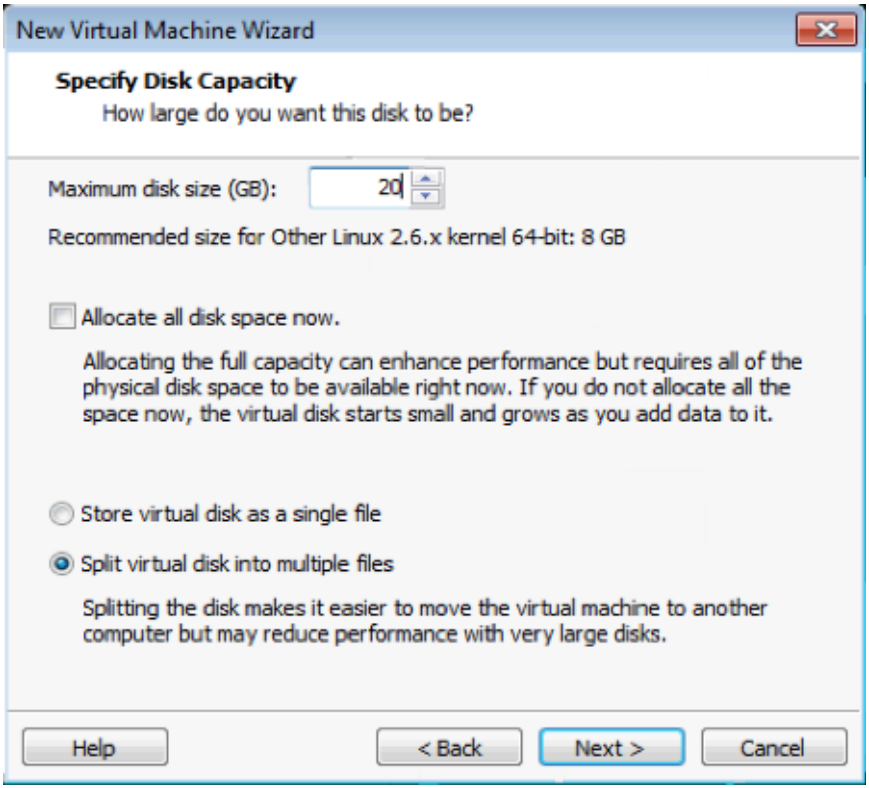


FIGURE 4-2. Specify disk capacity

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**.

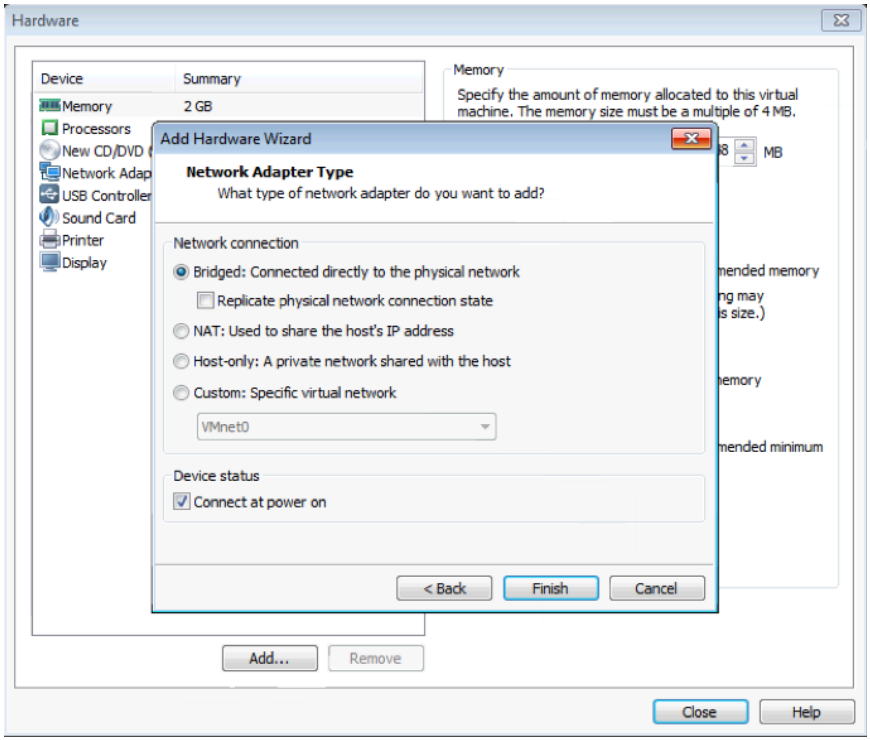


FIGURE 4-3. Configure network adapter type

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**.

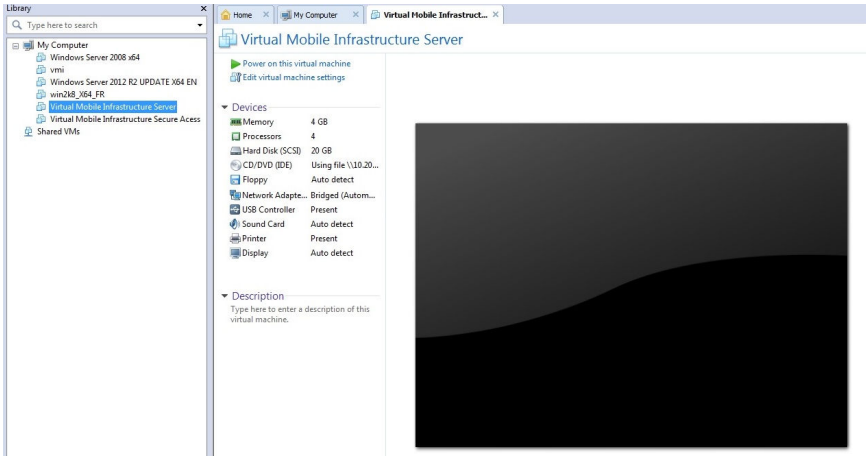


FIGURE 4-4. Virtual machines in VMware Workstation

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 key exists in the configuration file:

    - ethernet0.virtualDev = "e1000"

    If they do not exist, or have the wrong values, add the keys at the bottom 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 Virtual Mobile Infrastructure Server iso setup image file.

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

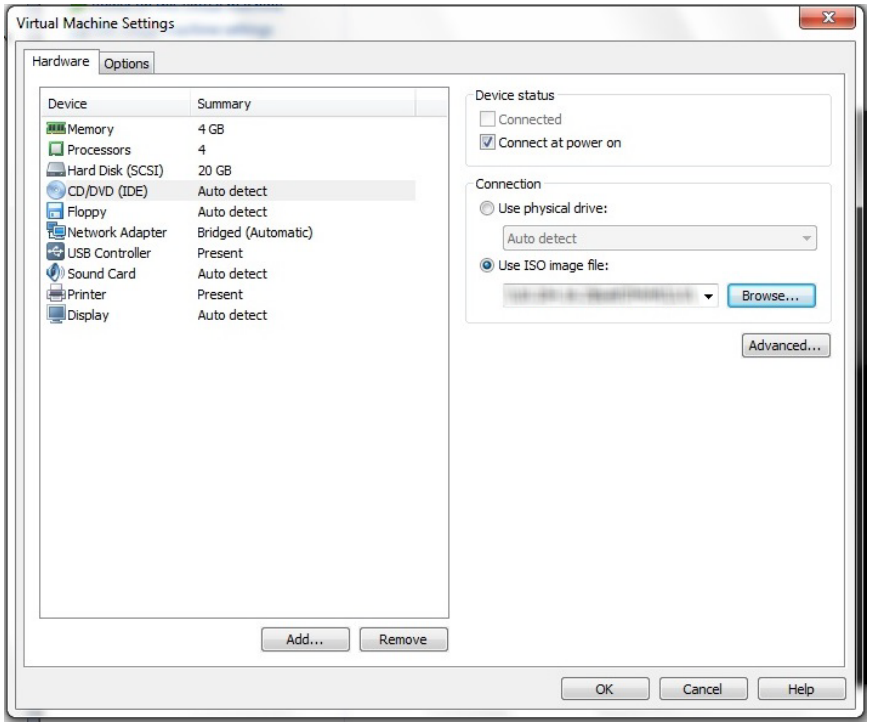


FIGURE 4-5. Browse and select Virtual Mobile Infrastructure Server ISO image file

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

Step 2: Installing Virtual Mobile Infrastructure 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 4-2*.
2. Click the **Console** tab on the virtual machine.

   The Virtual Mobile Infrastructure installation menu appears.
3. Follow *step 3 on page 2-2* to *step 11 on page 2-10* of the topic *Installing Virtual Mobile Infrastructure Server on a Bare Metal Server on page 2-2* to complete Virtual Mobile Infrastructure installation.

Installing Virtual Mobile Infrastructure Secure Access

Installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure Secure Access (See *Step 2: Installing Virtual Mobile Infrastructure 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

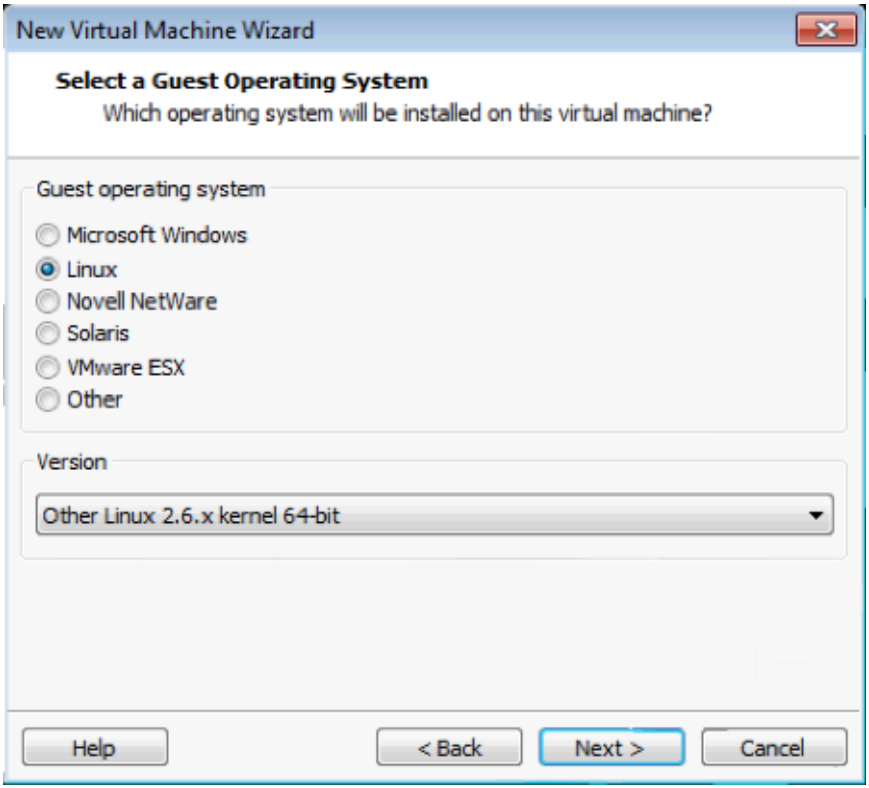


FIGURE 4-6. Select a guest operating system

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**.

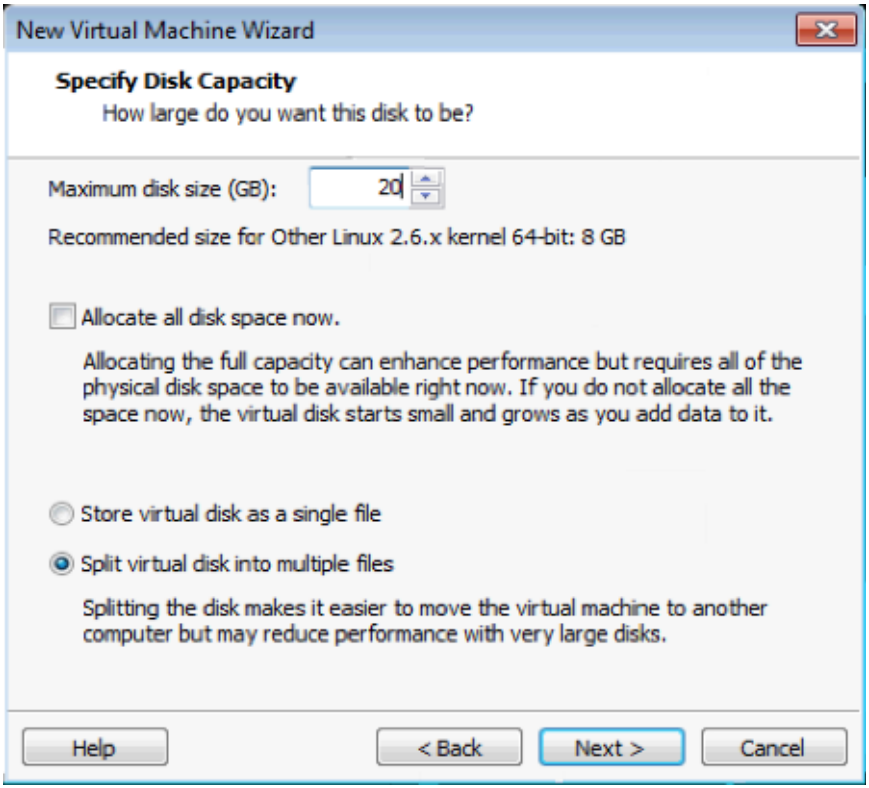


FIGURE 4-7. Specify disk capacity

18. Click **Next**.

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

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

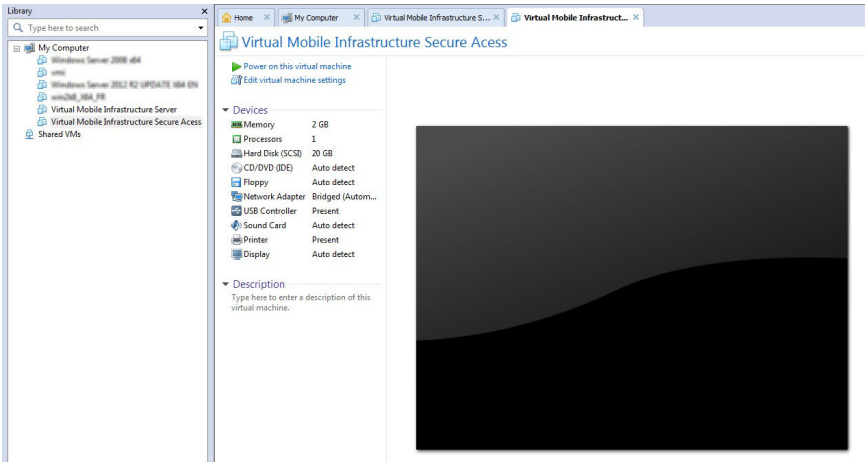


FIGURE 4-8. Virtual machines in VMware Workstation

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 Virtual Mobile Infrastructure Secure Access iso setup image file.

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

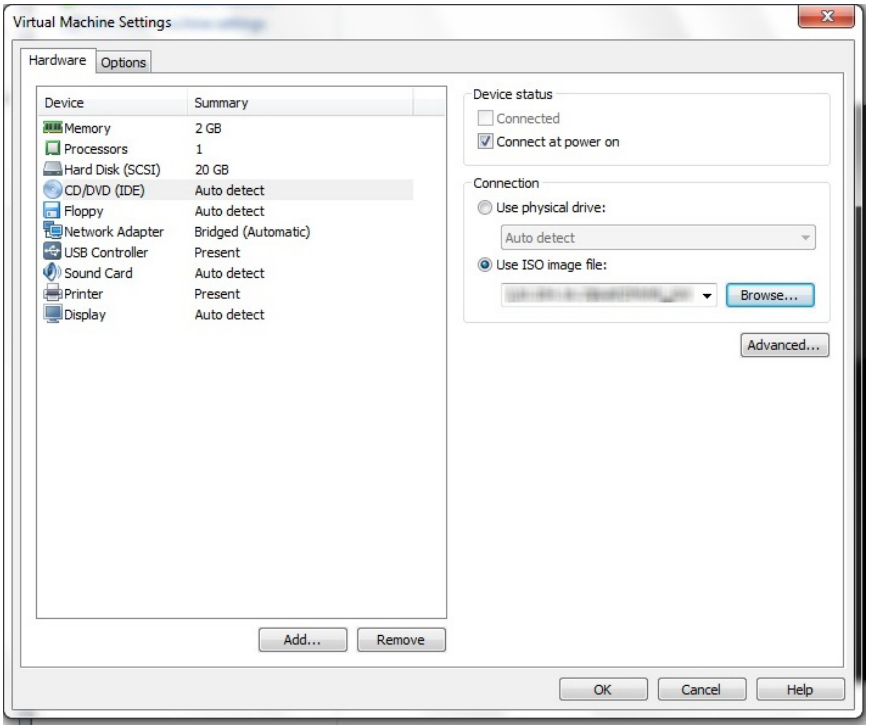


FIGURE 4-9. Browse and select Virtual Mobile Infrastructure Secure Access ISO image file

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

Step 2: Installing Virtual Mobile Infrastructure 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 4-9*.
2. Click the **Console** tab on the virtual machine.

The Virtual Mobile Infrastructure installation menu appears.

3. Follow *step 3 on page 2-11* to *step 13 on page 2-13* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-10* 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 Virtual Mobile Infrastructure.

This chapter contains the following sections:

Installing Virtual Mobile Infrastructure Server

Installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure (See *Step 2: Installing Virtual Mobile Infrastructure Server on Microsoft Hyper-V on page 5-5*).

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 Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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**.

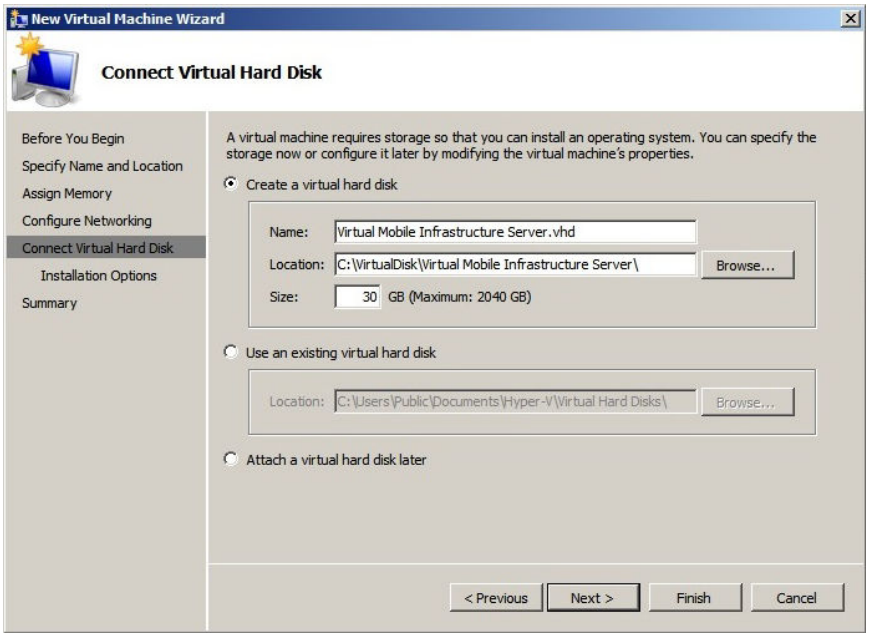


FIGURE 5-1. Create Virtual Hard Disk screen

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 screen, click **DVD Drive**, and then click **Image file**, and select the Virtual Mobile Infrastructure Server installation setup file.

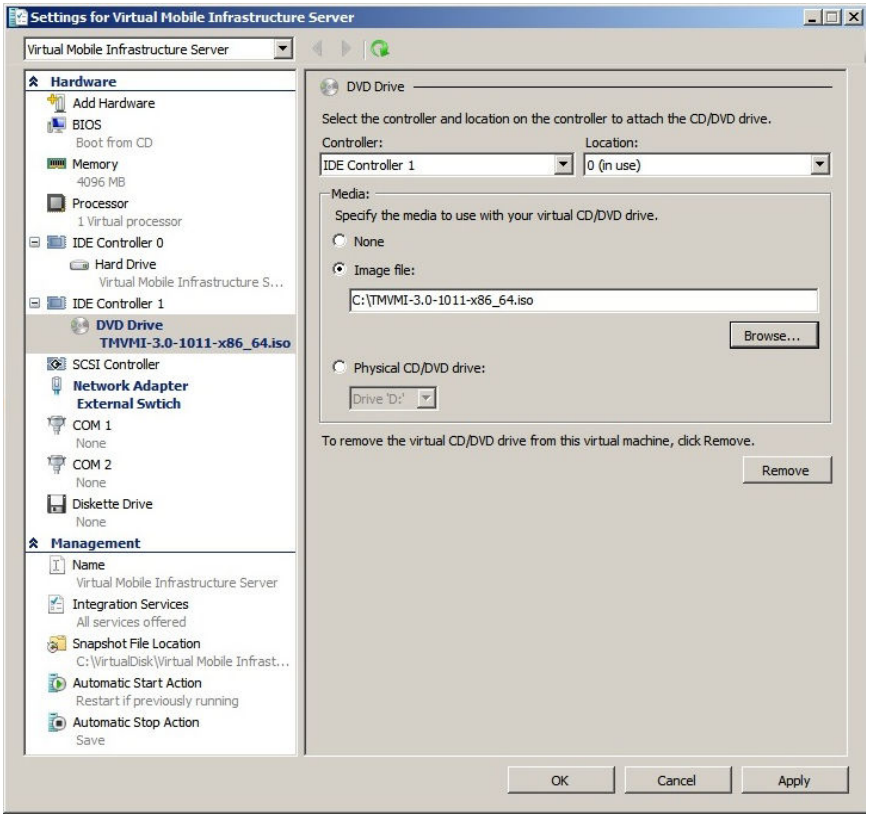


FIGURE 5-2. Select the Virtual Mobile Infrastructure server installation file

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

Step 2: Installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure installation menu appears.
3. Follow *step 3 on page 2-2* to *step 11 on page 2-10* of the topic *Installing Virtual Mobile Infrastructure Server on a Bare Metal Server on page 2-2* to complete Virtual Mobile Infrastructure installation.

Installing Virtual Mobile Infrastructure Secure Access

Installing Virtual Mobile Infrastructure Secure Access on Microsoft Hyper-V involves the following steps:

1. Creating a virtual machine (See *Step 1: Creating a Virtual Machine on page 5-5*).
2. Installing Virtual Mobile Infrastructure Secure Access (See *Step 2: Installing Virtual Mobile Infrastructure Secure Access on Microsoft Hyper-V on page 5-9*).

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 Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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**.

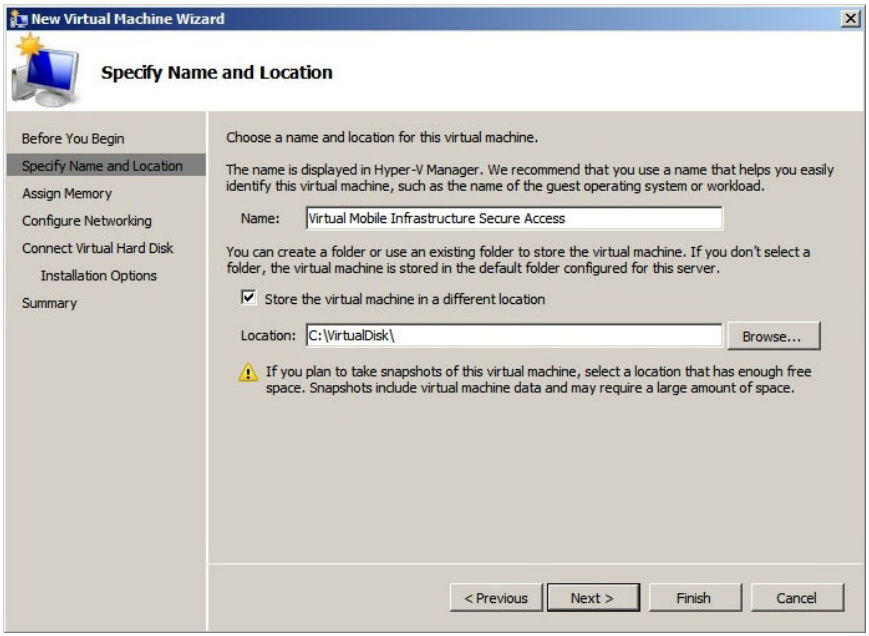


FIGURE 5-3. Create Virtual Hard Disk screen

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 Virtual Mobile Infrastructure Secure Access installation setup file.

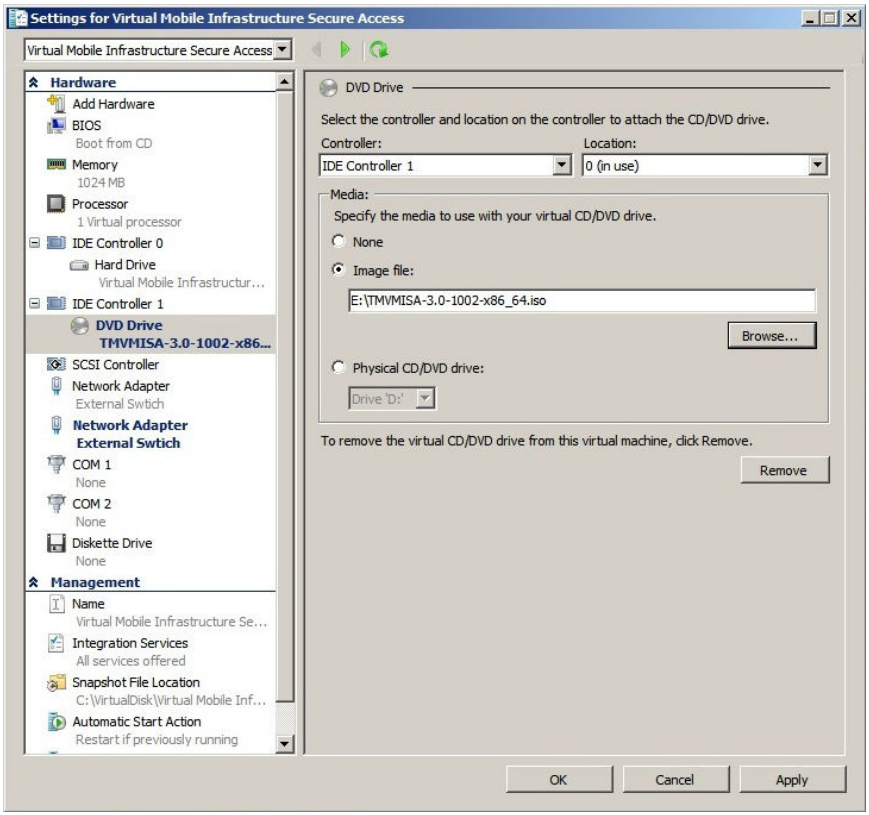


FIGURE 5-4. Select the Virtual Mobile Infrastructure Secure Access installation file

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

Step 2: Installing Virtual Mobile Infrastructure 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 5-5*.
2. Click the **Console** tab on the virtual machine.

   The Virtual Mobile Infrastructure Secure Access installation menu appears.
3. Follow *step 3 on page 2-11* to *step 13 on page 2-13* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-10* 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 Virtual Mobile Infrastructure.

This chapter contains the following sections:

Installing Virtual Mobile Infrastructure Server

Installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure Server. (See *Step 2: Creating a Virtual Machine and Installing Virtual Mobile Infrastructure Server on page 6-2*.)

Step 1: Installing a VNC Viewer Application

The Virtual Mobile Infrastructure server installation requires a VNC viewer to complete the installation. Before you begin installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure Server

Procedure

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

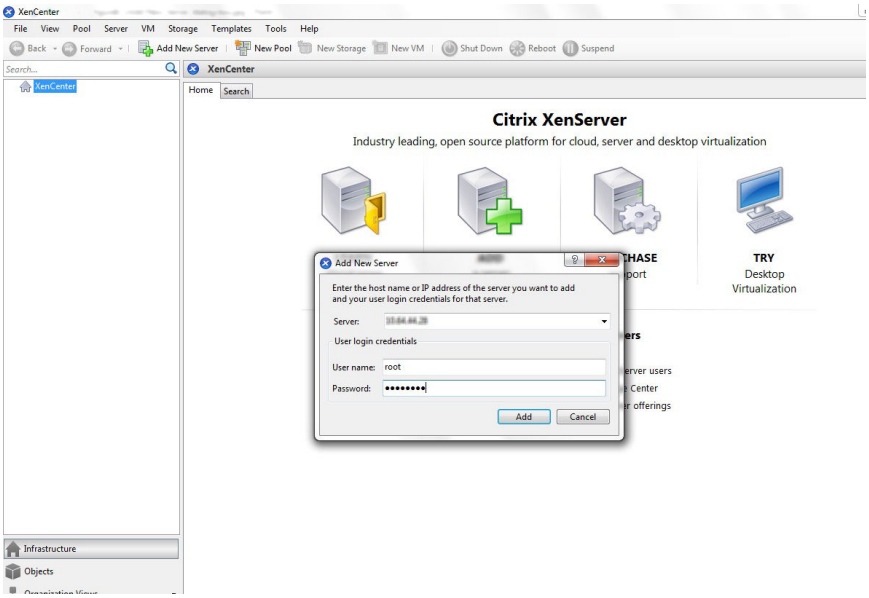


FIGURE 6-1. Add New Server dialog box

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**.

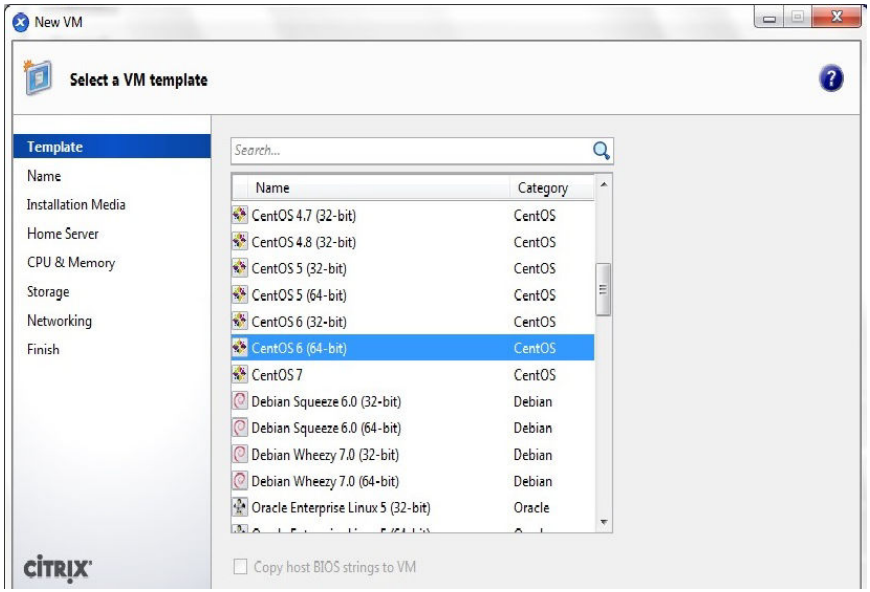


FIGURE 6-2. Select a VM template screen

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 Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure, 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** on the **Networking** screen.

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

    The **Disc Found** screen appears.

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

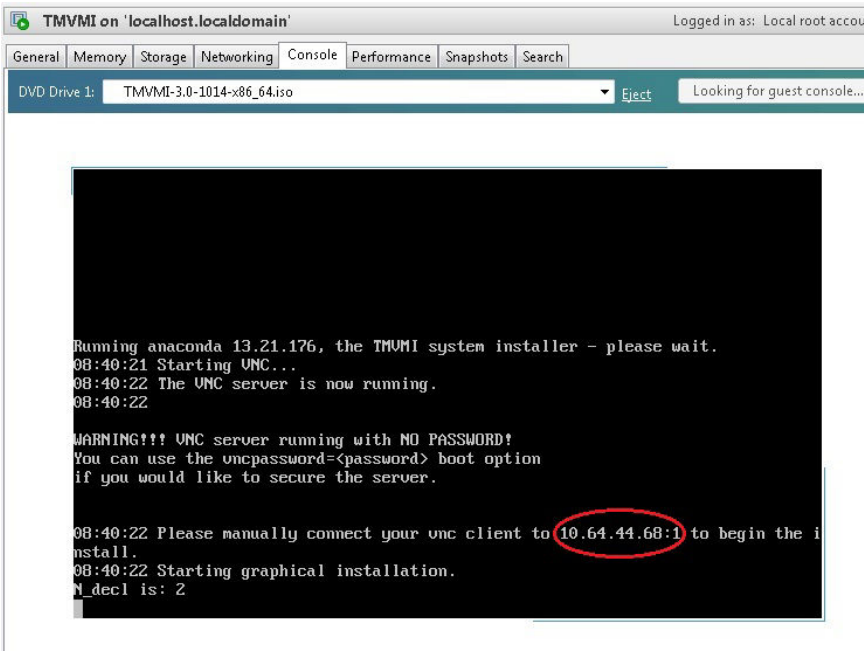


FIGURE 6-3. Screen displaying the VNC server IP address

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

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

    The Virtual Mobile Infrastructure installation menu appears.

19. Follow *step 3 on page 2-2* to *step 11 on page 2-10* of the topic *Installing Virtual Mobile Infrastructure Server on a Bare Metal Server on page 2-2* to complete Virtual Mobile Infrastructure installation.

Installing Virtual Mobile Infrastructure Secure Access

Installing Virtual Mobile Infrastructure 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 6-7*.)
2. Creating a virtual machine and installing Virtual Mobile Infrastructure Secure Access. (See *Step 2: Creating a Virtual Machine and Installing Virtual Mobile Infrastructure Secure Access on page 6-7*.)

Step 1: Installing a VNC Viewer Application

The Virtual Mobile Infrastructure server installation requires a VNC viewer to complete the installation. Before you begin installing Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure Secure Access

Procedure

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

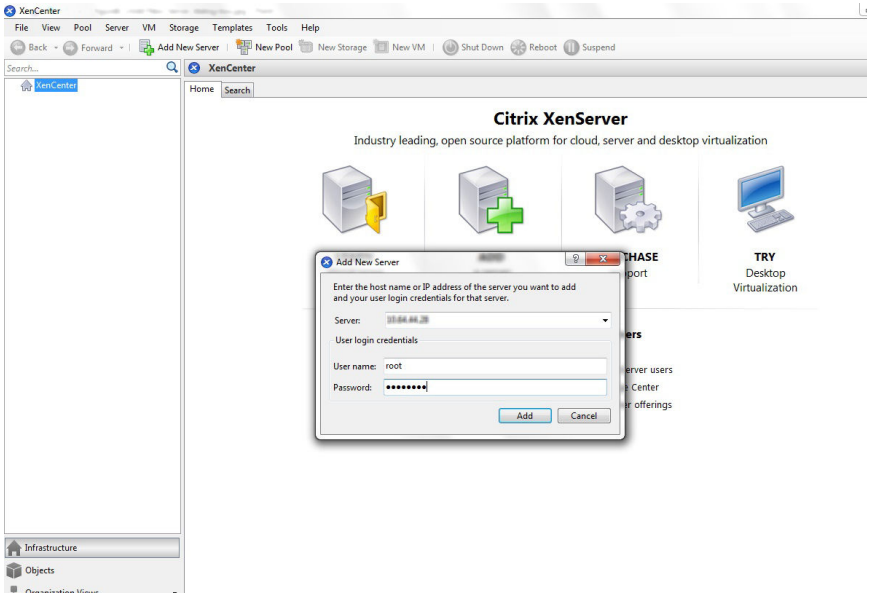


FIGURE 6-4. Add New Server dialog box

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**.

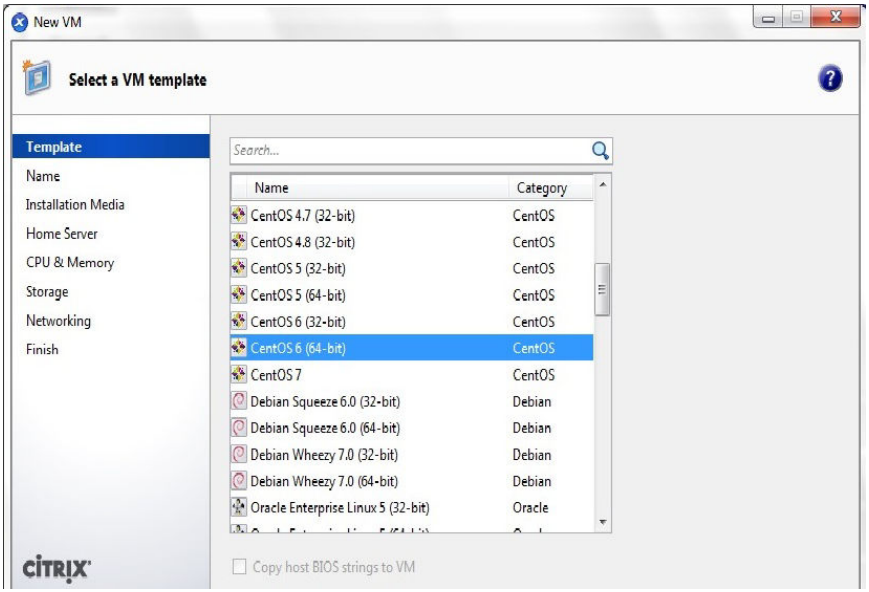


FIGURE 6-5. Select a VM template screen

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 Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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.

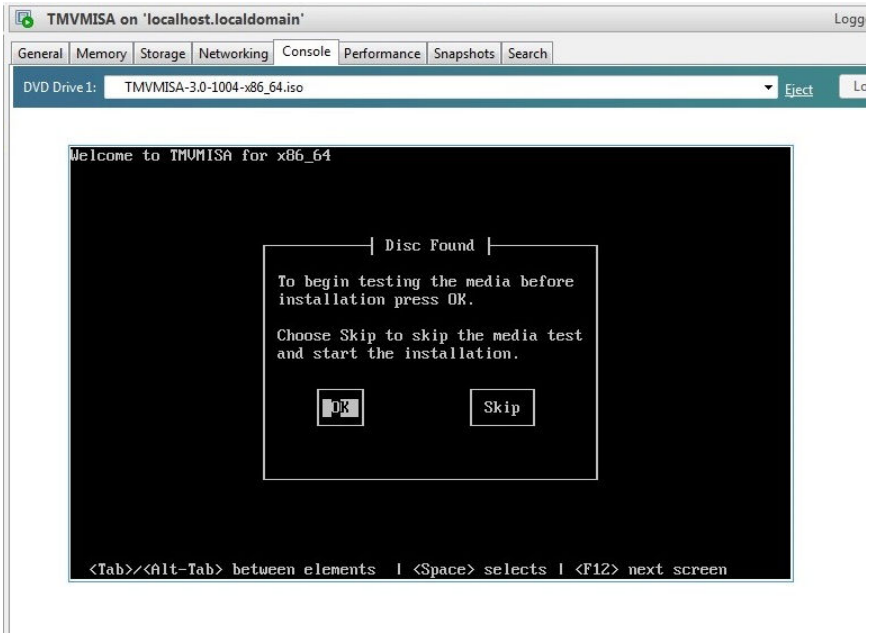


FIGURE 6-6. Select a network device for the installation

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.

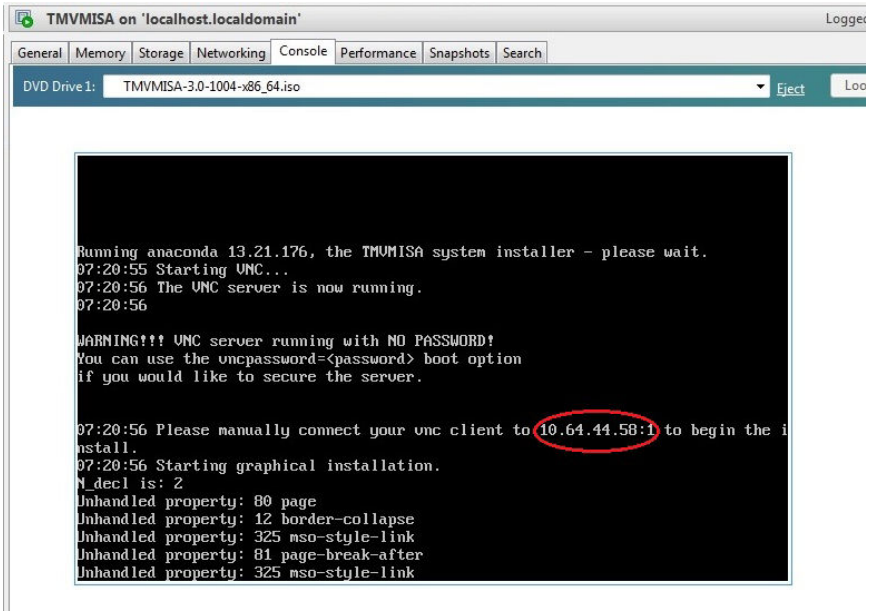


FIGURE 6-7. Screen displaying the VNC server IP address

The Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure Secure Access installation menu appears.

20. Follow *step 3 on page 2-11* to *step 13 on page 2-13* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-10* to complete Secure Access installation.

Chapter 7

Post-Installation Configuration

Trend Micro recommends performing all tasks in this chapter before using Virtual Mobile Infrastructure.

This chapter contains the following sections:

Accessing Virtual Mobile Infrastructure Administration Web Console

To access the Virtual Mobile Infrastructure Web console:

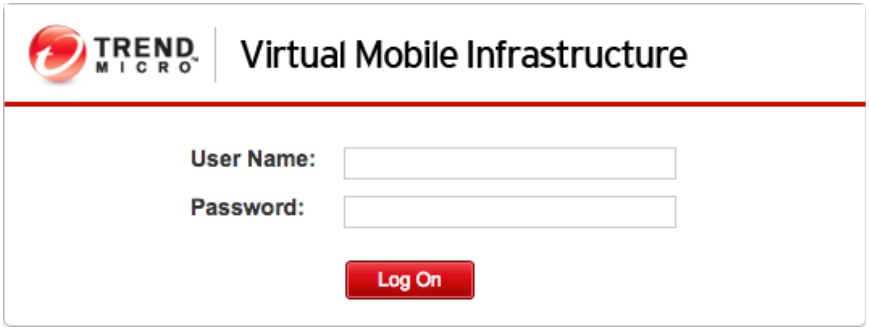
Procedure

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

   https://<Virtual Mobile Infrastructure_domain_name_or_IP_address>:8443

   The following screen appears.

FIGURE 7-1. Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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 7-6* for the procedure.

Activating Your Product

Virtual Mobile Infrastructure 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.

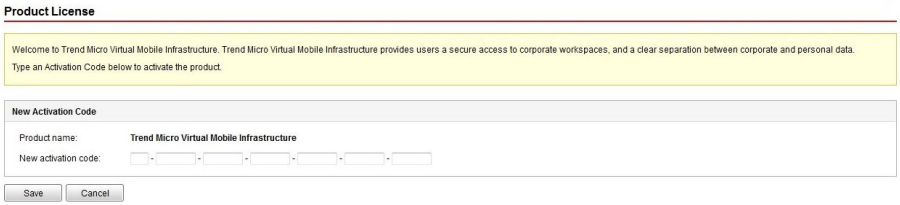


FIGURE 7-2. Product License screen

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**.

Configuration Tasks

The following table depicts the configuration tasks for Virtual Mobile Infrastructure server after installation.

TABLE 7-1. Post installation configuration tasks for Virtual Mobile Infrastructure server

ACTION	DESCRIPTION
(Optional) Configure administrator account setting.	Administrator account, email address and password settings. See *Changing Administrator Account Password on page 7-6* for the detailed procedure.
(Optional) Configure LDAP settings.	Supports integration with Microsoft Active Directory and OpenLDAP to manager users and groups. See *Configuring LDAP Settings (Optional) on page 7-7* for the detailed procedure.
(Optional) Configure mobile client settings.	Security settings, user settings, audio/video playback settings and Secure Access settings for mobile client and users. See *Configuring Mobile Client Settings on page 7-8* for the detailed procedure.
(Optional) Configure Exchange settings.	Microsoft Exchange server settings to user single sign on for workspace. See *Configuring Microsoft Exchange Server and Office 365 Settings (Optional) on page 7-10* for the detailed procedure.
(Optional) Configure proxy settings.	Proxy setting for user workspace. See *Configuring Proxy Settings on page 7-11* for the detailed procedure.
(Optional) Configure external storage.	External storage to save user data. (Required, if multiple Virtual Mobile Infrastructure servers are deployed.) See *Configuring External Storage (Optional) on page 7-12* for the detailed procedure.
(Optional) Configure syslog settings.	System log server settings to save server debug logs. See *Configuring Syslog (System Logs) on page 7-14* for the detailed procedure.

ACTION	DESCRIPTION
(Optional) Configure advanced settings.	Application usage log and OAuth 2.0 setting for user authentication. See *Configuring Advanced Settings on page 7-15* for the detailed procedure.
(Optional) Configure email notification settings.	SMTP server settings to send email notification to users. See *Configuring Email Notifications on page 7-13* for the detailed procedure.
(Optional) Enable high availability (HA)	Enable HA, if required, using command line. Refer to *Configuring Server High Availability (HA)* in chapter 6 of *Administrator's Guide* for the detailed procedure.
(Optional) Enable Security-Enhanced Linux (SELinux)	Enable Security-Enhanced Linux (SELinux), if required, using command line. Refer to *Configuring Security-Enhanced Linux (SELinux)* in chapter 6 of *Administrator's Guide* for the detailed procedure.

Changing Administrator Account Password

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

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 LDAP Settings (Optional)

Virtual Mobile Infrastructure provides optional integration with Microsoft Active Directory and OpenLDAP to manage users and groups more efficiently.

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

If you do not want to import users and groups from LDAP, or want to manage users locally on the Virtual Mobile Infrastructure server, then you will need to disable the LDAP integration.

Procedure

1. On the **System Settings** screen, click the **LDAP** tab.
2. Select **Use LDAP** to enable the feature
3. Configure the following:
   - **LDAP Server Type**–select the LDAP server.
   - **Server name or 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 LDAP server.
   - **Update frequency**–select a time from the list to determine how often to synchronize content with the LDAP server.
4. Click **Save**.

The server tests the connection with the LDAP server and saves System Settings.

Disabling LDAP Server

Use the **LDAP** tab in **System Settings** to disable the LDAP settings.

Procedure

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

Configuring Mobile Client Settings

The Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure.

Procedure

1. On the **System Settings** screen, click the **Mobile Client** tab.
2. Under **User Settings** section, configure the following:
   - If you want to allow users to save their passwords on their mobile devices, select **Allow users to save password on mobile device**.
   - If you want users to wait for a certain time before retrying after typing in a wrong password, select **Enable unsuccessful signin restrictions for LDAP users**, and then select the number of attempts and the waiting time from the drop-down lists.

- If you want to configure the password security level for user workspaces on their mobile devices, select a security option from the **Workspace screen lock security level** drop-down list.

  Note

  This setting will take effect when the users sign in the next time.

- If you want to stop users from taking screenshots on Android, select **Do not allow user to take screenshot**.

  Note

  On iOS mobile devices, if the screenshot is taken, the Virtual Mobile Infrastructure mobile client logs the event and transfers it to the server.

- From **User keyboard for workspace**, select the keyboard you want users to use during their Virtual Mobile Infrastructure session.

  Note

  The built-in keyboard for workspace supports English only.

3. Under **User Alert Email Setting** section, select **Send an alert email automatically to user when the user storage is 80% full**, if you want to send email to the users automatically.

   Note

   If enabled, sends the alert email at 00:00 AM to the concerned user.

   See *Configuring Email Notifications on page 7-13* for details on configuring user alert notification.

4. Under **QR Code Scanning and Audio/Video Playback** section, if you want to allow users to scan QR code and play audio or video files residing on the workspace or streaming online, select **Allow users to scan QR code and play audio/video files on mobile device**.

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 Microsoft Exchange Server and Office 365 Settings (Optional)

If you have already set up an Exchange server in your enterprise environment, you can configure Virtual Mobile Infrastructure to automatically configure Exchange server and Office 365 settings for all the users on their workspace.

Note

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

Use the **Exchange Server** tab on **System Settings** screen to configure Microsoft Exchange Server and Microsoft Office 365 settings.

Procedure

1. On the **System Settings** screen, click the **LDAP** tab.
2. Make sure that the **Use LDAP** checkbox is selected, and the LDAP 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. Select **Office 365 customization**, if you are using Exchange Online, and type the Office 365 login ID in the **User name** field.

Note

For Office 365 Exchange Online, usually the user name in email account setting is the value of the user's User Principal Name (UPN) in Active Directory. However, in some environments administrators use the alternate login ID functionality. If you have used an alternate login ID, type the correct attribute of the a user object other than UPN in the **User name** field.

6. Click **Save**.

Configuring Proxy Settings

If your network settings require a proxy to connect to the Internet, configure the proxy settings on Virtual Mobile Infrastructure server.

Use the **Proxy** tab in **System Settings** to configure proxy settings for Virtual Mobile Infrastructure server.

Procedure

1. Click the **Proxy** tab.
2. Select **Use the following proxy settings**, and configure the following:
    - **Host name or IP address**
    - **Port number**
    - **Proxy server authentication**
        - **User name**
        - **Password**
        - **Bypass proxy for these addresses**

> **Note**
>
> The bypass setting only takes effect for the user workspaces, and from the next time users sign in.

3. Type a URL in the **Test address** field, and then click **Test Connection** to verify proxy settings.
4. Click **Save**.

Configuring External Storage (Optional)

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

Use the **Server Management** screen to configure external storage for Virtual Mobile Infrastructure server.

Procedure

1. On the **Server Management** screen, click **Default Site**.
2. Click **External Storage**.
3. 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.
4. Click **Test Connection** and then click **OK** on the pop-up dialog box.
5. Click **Save**.

   The server tests the connection with the external storage and saves the **Server Management** screen.

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 Virtual Mobile Infrastructure.

Procedure

1. On the **Email Settings** tab, 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. On the **Invitation Email Template Settings** tab, 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. On the **Reset Password Template Settings** tab, 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. On the **User Alert Template Settings** tab, configure 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.

6. Click **Save** to save settings.

Configuring Syslog (System Logs)

Configure syslog server settings to save server debug logs.

Use the **Syslog** tab in **System Settings** to configure system logs settings for Virtual Mobile Infrastructure.

Procedure

1. On the **System Settings** screen, click the **Syslog** tab.
2. Select **Enable syslog**.
3. Configure the following settings for the syslog server:
   - **Protocol**
   - **Host name or IP address**
   - **Port number**
4. Click **Save**.

Configuring Advanced Settings

The advanced settings in Virtual Mobile Infrastructure include application usage log setting to collect application usage log from user workspaces to learn more about user behavior. The advanced settings also enable you to use OAuth 2.0 protocol for user authorization. OAuth 2.0 provides specific authorization flows for Web applications, desktop applications, mobile phones, and living room devices. Virtual Mobile Infrastructure Secure Access includes the Authorization Server, which is required for OAuth 2.0 authentication.

Before you can configure OAuth 2.0 authentication settings, you must configure **Secure Access Settings** in **Mobile Client** tab. Refer to *Configuring Mobile Client Settings on page 7-8*.

Use the **Advanced** tab in **System Settings** to configure application log settings and OAuth 2.0 authentication settings for Virtual Mobile Infrastructure.

Procedure

1. On the **System Settings** screen, click the **Advanced** tab.
2. Under **Application Usage Log** section, select **Enable application usage log**.

Note

If enabled, you can view the application usage log on the following screens:

- **Dashboard**, in **Top 5 Applications Used** widget (also available even when the feature is disabled).
- **User Management**, on the user details screen for each user. Click on a user name to see user details. The applications usage information on this screen includes the complete list of applications used, sequence and duration of usage and the locations where the applications were used.
- **Logs**, using **Apps Used Log** query, you can look at the name of the applications used by users and the usage duration for each application.

3. Under **OAuth 2.0 Authentication** section, select **Enable OAuth 2.0 authentication**.
4. Configure the following options:

- **Client ID** and **Client Secret**: The Virtual Mobile Infrastructure server ID and secret code generated by the Authorization Server. The Client ID represents Virtual Mobile Infrastructure in Authorization Server and the secret code is required by the Authorization Server for access authorization.

  Use the following command on the command console on Secure Access to get the Client ID and Client Secret:

  ```
  /vmi/authorizationService/manage.py create_app "Trend
  Micro Virtual Mobile Infrastructure" https://{your
  secure access address:port}/api/v1/portal/oauth
  ```

  Note

  Replace {your secure access address:port} with Secure Access IP address and port number.

- **Authorization URL**: The Authorization URL for the users to provide certificate authorization.
- **Token URL**: The Token URL for the Virtual Mobile Infrastructure to get access token and refresh token from the Authorization Server. An access token has a limited lifetime. If Virtual Mobile Infrastructure needs access to Authorization Server beyond the lifetime of a single access token, it obtains a

refresh token. The refresh token allows Virtual Mobile Infrastructure to obtain new access tokens.

- **Account Information URL**: The Account Information URL is generated by the Authorization Server and includes the user account information for authentication.
- **Client Certificate**: Client certificate is used to create a mutual authentication SSL connection to Authorization Server or Identity Provider (IdP). Generate, and then upload the client certificate file here.

  Use the following command to generate the client certificate file:

  ```
  /vmi/authorizationService/manage.py init_cert
  ```

  The Authorization Server generates the client certificate file at the following location:

  ```
  /etc/pki/vmi/client.pass.p12
  ```

  Note

  Virtual Mobile Infrastructure only supports `.p12` and `.pfx` client certificate file types.

- **Certificate Password**: Type the following client certificate password: `vmi`
- **Verify authorization server certificate**: Select this option if you want to verify the CA certificate, and then upload the CA certificate in the **Certificate Authority** field. The CA Certificate is available at the following location:

  ```
  /vmi/testcert/root.crt
  ```

- **Certificate Authority**: Certificate Authority is used to avoid man-in-the-middle (MitM) attack and verify Authorization Server certificate.

  Note

  Virtual Mobile Infrastructure only supports `.pem` CA certificate file types.

Note

The **Authorize URL**, **Token URL** and **Account Information URL** fields are automatically filled with the relevant information.

5. (Optional) Click **Test Connection** to verify your settings.
6. Click **Save**.

What to do next

Generate individual certificates for mobile users for enrollment. See *Generating Client Enrollment Certificate on page 7-18*.

Generating Client Enrollment Certificate

Before following this procedure, make sure that you have already configured OAuth 2.0 Authentication. See *Configuring Advanced Settings on page 7-15* for details.

Procedure

1. Log on to the Secure Access server.
2. On the Secure Access server command console, type the following command and press **Enter**:

```
/vmi/authorizationService/manage.py create_cert "Full Name"
full_name@example.com
```

Note

Replace **Full Name** with the actual user name, and **full_name@example.com** with the actual user email address that is configured on the administration Web console.

Secure Access generates the client enrollment certificate at the following location:

```
/vmi/testcert/full_name
```

Where, **full_name** is the name of the folder created for the user.

What to do next

Provide the certificate to the user to enroll to the Virtual Mobile Infrastructure server.

Managing Groups and Users

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

Note

User accounts imported from the Active Directory cannot be modified from the Virtual Mobile Infrastructure 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 LDAP Settings (Optional) on page 7-7* 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 site in which you want to import users.

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

Note

If you click **Import & Send Invitation**, the Virtual Mobile Infrastructure server imports the selected users or groups, and sends an invitation email to all users and users in the imported groups. The invitation email includes the user account information to log on to server.

Creating a User Account Locally

Virtual Mobile Infrastructure 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 LDAP Server on page 7-8* 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**.

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

Deploying Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure 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 7-13* for the procedure of creating and configuring system notifications.

Installing Android Client for Virtual Mobile Infrastructure

Download the Android client application for Virtual Mobile Infrastructure from Google Play store.

Procedure

1. Open Google Play store on an Android mobile device and search for `TMVMI Client`.
2. In the search results, look for **Trend Micro Virtual Mobile Infrastructure** 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

Virtual Mobile Infrastructure requires to use the mobile device location information for any application installed in the user workspace. If you tap **Cancel**, Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure

Download the iOS client app for Virtual Mobile Infrastructure from Apple App Store.

Procedure

1. Open App Store on an iOS mobile device and search for `TMVMI Client`.
2. In the search results, look for **Trend Micro Virtual Mobile Infrastructure** 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 Virtual Mobile Infrastructure 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

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

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

Installing Windows Client for Virtual Mobile Infrastructure

Download the Windows client from the Windows Store.

Procedure

1. Open the Store on a Windows mobile device and search for `TMVMI Client`.
2. In the search results, look for **Trend Micro Virtual Mobile Infrastructure** 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 Virtual Mobile Infrastructure 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**
>
> Virtual Mobile Infrastructure requires to use the mobile device location information for any application installed in the user workspace. If you tap **Cancel**, Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure.

This appendix contains the following sections:

Network Port Configuration for Virtual Mobile Infrastructure Server

Configure the following network ports for Virtual Mobile Infrastructure server:

Component	Network Ports	Details	Required or Optional	Direction
Management Web console	HTTPS port **8443**	Used to access Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure server.	Required	Inbound
	TCP port **5902** to **6923**	Used by mobile client to access Virtual Mobile Infrastructure server.	Required if using NAT.	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
Notification Channel port	HTTPS port **443**	Used to connect to the Trend Micro Cloud Communication server to receive APNs notifications.	Required	Outbound
APNs Center	TCP port **2195**	Allows outbound connection to Apple Push Notification Server. The hostname of Apple Push Notification Service is gateway.push.apple.com.	Required	Outbound

Component	Network Ports	Details	Required or Optional	Direction
Wi-Fi-network port	TCP port **5223**	Allows iOS mobile devices to receive push notifications from Apple's server, especially when conecting through Wi-Fi network where port 5223 is blocked. However, if the mobile devices are on a 3G network, you do not need to configure this port.	Optional	Outbound

Network Port Configuration for Virtual Mobile Infrastructure Secure Access

Configure the following network ports for Virtual Mobile Infrastructure 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 Virtual Mobile Infrastructure	HTTPS Port 443 TCP Port 5900 to 6923	Used by Secure Access to communicate with Virtual Mobile Infrastructure server.	Required	Outbound
OAuth 2.0 authentication	8443	Used for user authentication using OAuth 2.0.	Optional	Inbound

Component	Network Ports	Details	Required or Optional	Direction
Play Video	HTTP Port 80 or any other HTTP port	Used for playing video through Secure Access, without requiring you to deploy a public certificate on Secure Access.	Optional	Outbound

Network Ports in Virtual Mobile Infrastructure Architecture

The following figure shows the network ports used in Virtual Mobile Infrastructure architecture.

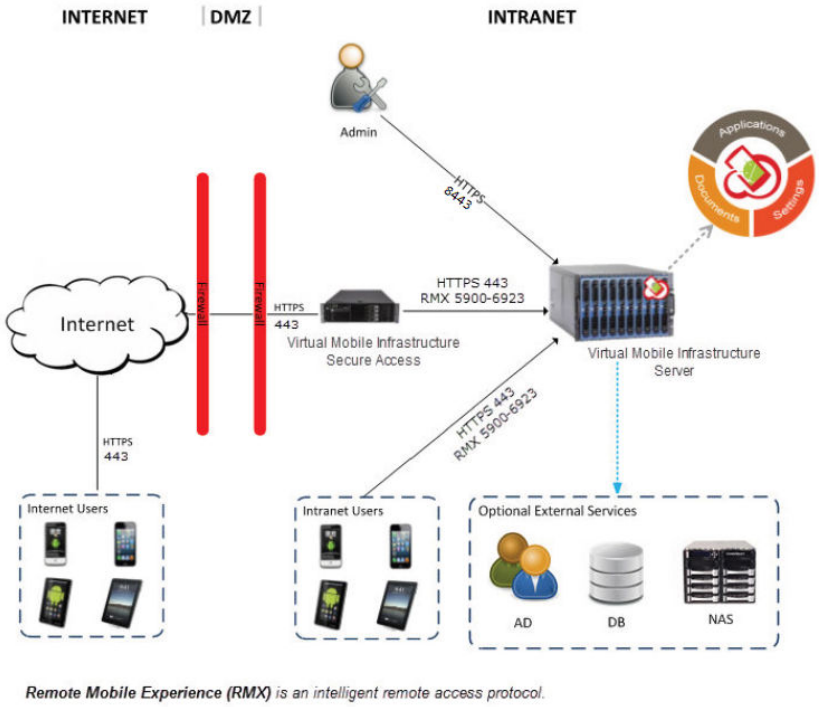


FIGURE A-1. Network Ports in Virtual Mobile Infrastructure Architecture

Index

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: APEM57685/161227