TREND MICRO™

6.0 TREND MICRO™ Virtual Mobile Infrastructure

Installation and Deployment Guide

Centrally-managed workspace for mobile users

Endpoint Security

Document Part No.: APEM68495/180927

Release Date: April 2019

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Virtual Mobile Infrastructure collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

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

Appendix B: Public SSL Certificate Deployment

Preface

Preface

Welcome to the Trend Micro™Virtual Mobile Infrastructure™ version 6.0 Installation and Deployment Guide. This guide helps you to get "up and running" by introducing Virtual Mobile Infrastructure, assisting with deployment, installation, initial configuration, and post-installation configuration tasks.

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 Linux system administration and mobile device policies, including:

- Installing and configuring Linux servers
- Installing software on Linux servers
- Configuring and managing mobile devices (such as smartphones and tablet computers)
- 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 or iOS 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 eight-core Intel processor with SSSE3 support
Memory	8-GB
Hard disk	50-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 10.0 or later • Android 5.0 or later

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 high availability for Management Server and Secure Access.

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 1-8* for more information.

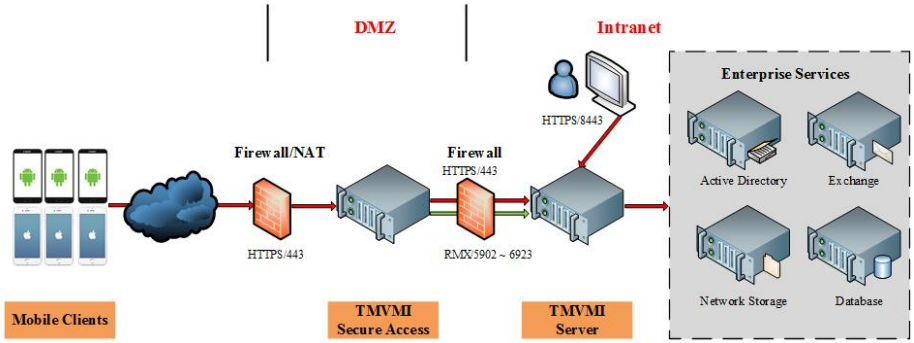


FIGURE 1-1. Trend Micro Virtual Mobile Infrastructure Single Server Installation Model

Multiple Server Installation Model

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

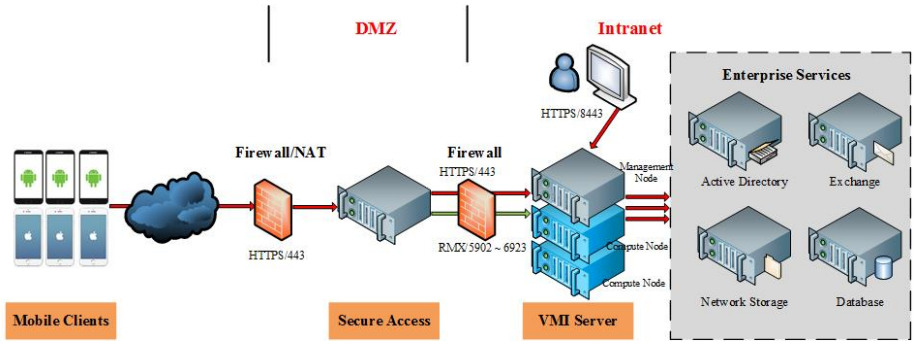


FIGURE 1-2. Trend Micro Virtual Mobile Infrastructure Multiple Server Installation Model

Virtual Mobile Infrastructure High Availability

Virtual Mobile Infrastructure enables you to configure High Availability (HA) to ensure the uninterrupted service to the users. For high availability deployment, install at least four servers: two Management Nodes, and two Compute Nodes, with all of these servers run in active-active mode. In this setup, both Management Servers provide management features, and host user workspaces, and access the same database. If one server goes down or disconnects from the network for any reason, the other server(s) can still be accessible and work as normal.

Note

Trend Micro recommends configuring an external database for data safety.

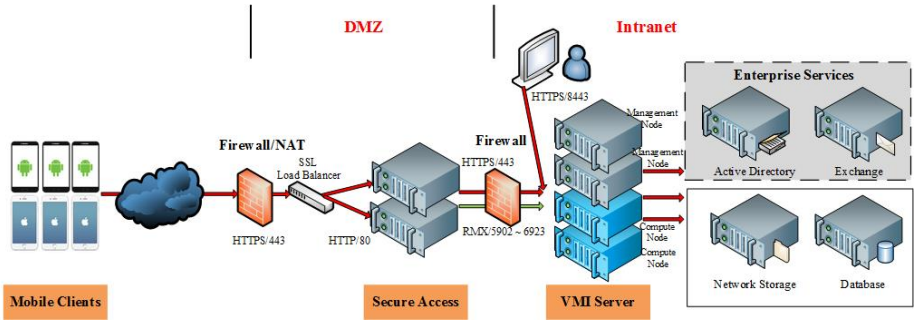


FIGURE 1-3. Trend Micro Virtual Mobile Infrastructure High Availability architecture

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 management node and compute node. • Management node provides management console for administrator and web service for user logon, logoff and connection to users's workspace. • Compute node 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

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
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 1-8* for more information.	Strongly 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
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.

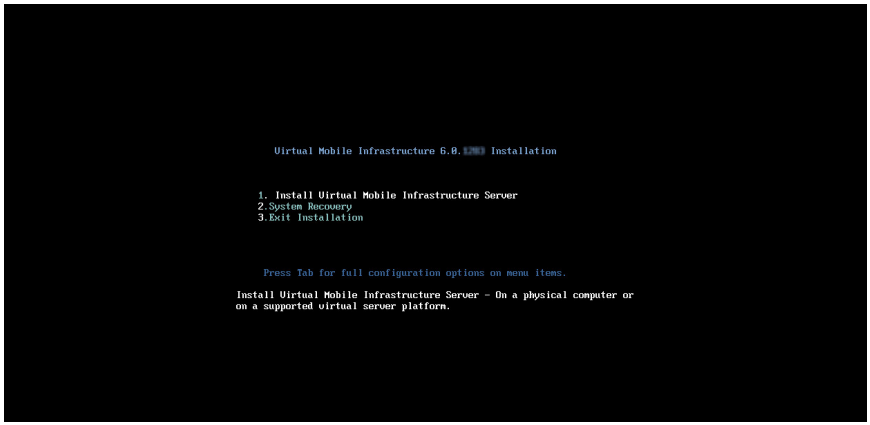
Important

If you are installing the first server, make sure to configure it as **Management Node** or **Management and Compute Node** during installation.

Procedure

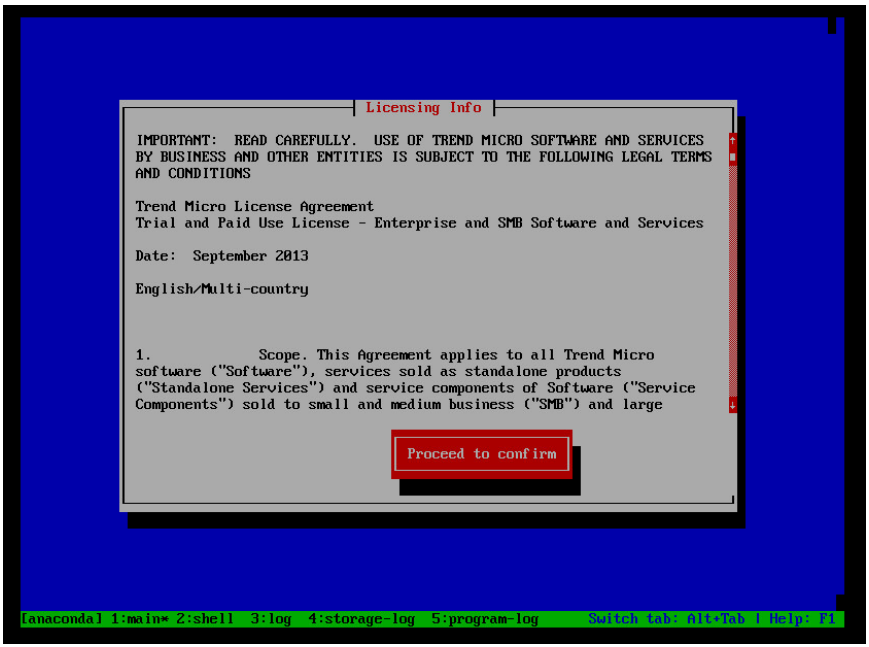
1. Power on the Bare Metal server where you want to install Virtual Mobile Infrastructure.
2. Insert the installation DVD into the DVD drive, and reboot the server.

   The Virtual Mobile Infrastructure installation menu appears.



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

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



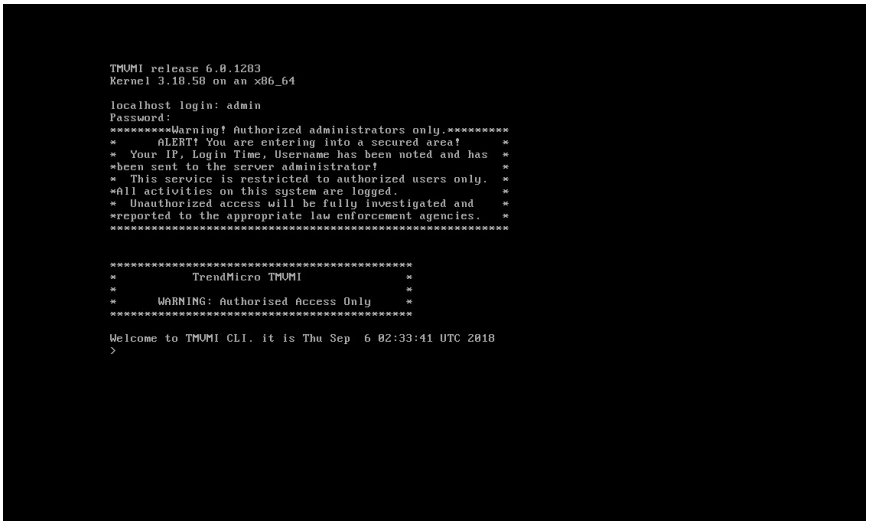
4. Press **Tab** to select **Proceed to Confirm**, and press **Enter**.

A page appears where you can accept the license agreement.

5. Press **Tab** to select **Accept**, and press **Enter** to continue.

The installation begins. The installation process may take about 10 minutes or more to complete. Once the installation process completes, the system reboots to allow configuration and displays the following screen.

6. Use username (localhost login) `admin`, and default password `admin` to log in.



7. Type `enable`, and the default password `admin` to enter the privilege mode and start the configuration steps.

8. If you need help during configuration, type `configure init help` and press **Enter** to check the configuration help.

```
After installation, please execute following command to configure your system:
1. To set root and admin account password, type command:
     configure init password
2. To setup network, type command:
     configure init network static IP_address/subnet_mask_bits gateway_address
 DNS1 [DNS2]
   For example:
     configure init network static 10.206.139.2/24 10.206.139.254 10.64.1.54
   Or type:
     configure init network dhcp
   to get a dynamic IP address.
3. VMI support 3 deploy mode, "Management and Compute node", "Compute node", "Ma
nagement node".
   To setup "Management and Compute node", type command:
     configure init server 1 new
   To setup "Compute node", type command:
     configure init server 2 vmi 10.21.22.1
4. To setup timezone, type command:
     configure init timezone
   Timezone example, "Asia/Shanghai".
5. To setup hostname, type command:
     configure init hostname
6. To setup keyboard type, type command:
     configure init keymap
# _
```

9. Type `configure init password`, to configure password for root account and admin account.

```
# configure init password
Passwords must be at least six (6) characters in length, and contain:
    a minimum of 1 lower case letter and
    a minimum of 1 upper case letter and
    a minimum of 1 numeric character and
    a minimum of 1 special character

Type the root password:
Confirm the root password:
Changing password for user root.
New password: Retype new password: passwd: all authentication tokens updated suc
cessfully.

Passwords must be at least six (6) characters in length, and contain:
    a minimum of 1 lower case letter and
    a minimum of 1 upper case letter and
    a minimum of 1 numeric character and
    a minimum of 1 special character

Type the admin and tmvmi password:
Confirm the admin and tmvmi password: _
```

10. Type one of the following to configure IP address for Virtual Mobile Infrastructure server:

    - For static IP address: `configure init network <static> <IP address/subnet_mask_bits> <gateway address> <DNS1> [DNS2]`
    - For dynamic IP address: `configure init network dhcp`

    For example, `configure init network static 10.206.139.48/22 10.206.139.254 10.64.1.54`.

Note

In multiple server setup, Trend Micro does not recommend using dhcp for the first Virtual Mobile Infrastructure server. This is because the other servers need to connect to the first Virtual Mobile Infrastructure server through an IP address. Therefore, the dynamic IP address may change later, and will cause multiple servers to work abnormally.

11. Do one of the following:

    - Set up single server
        - Setup single server with a new database. See *Table 2-1: Setting Up Single Server with New Database on page 2-8* for the procedure.
        - Setup single server and use an already installed database. See *Table 2-2: Setting Up Single Server and Configuring Existing Database on page 2-8* for the procedure.
    - Setup multiple servers
        - Setup multiple servers with a new database. See *Table 2-3: Setting Up Multiple Servers with New Database on page 2-9* for the procedure.
        - Setup multiple servers and use an already installed database. See *Table 2-4: Setting Up Multiple Servers and Configuring Existing Database on page 2-10* for the procedure.

TABLE 2-1. Setting Up Single Server with New Database

To set up a single server with a new database, install a **Management and Compute Node**.	• To install a **Management and Compute Node**: • Type `configure init server 1 new`.

TABLE 2-2. Setting Up Single Server and Configuring Existing Database

To set up a single server only, and configure an existing external database, install a **Management and Compute Node**, and then configure the existing database information.
 	
Note
Before you install a virtual machine, you must create an account for Virtual Mobile Infrastructure on your external database, and make sure that the database user account can access the database. For example, the database name may look like: **vmidb**.
 	
When you create the database, such as, **vmidb**, set the character as "UTF-8", and grant all privileges to the user. For example, mysql can use the command `GRANT ALL ON vmi_db.* TO 'vmi_user'@'%' IDENTIFIED BY 'passowrd';`.
	• To install a **Management and Compute Node**, and add an external database information:
	  a. Type `configure init server 1 db <db ip address> <db name> <db username> [db port] <db type>`, and then press **Enter**.
	
	  Note
	  `db type` can be "`mysql`" or "`oracle`".
	
	  For example, `configure init server 1 db 10.206.139.20 vmidb tmvmi 3306 mysql`.
	
	  b. Type the password for the database you want to use for Virtual Mobile Infrastructure when prompted.

TABLE 2-3. Setting Up Multiple Servers with New Database

To setup multiple servers and a new database, install at least two Virtual Mobile Infrastructure servers. **Note** When installing multiple servers, the first server must be a **Management and Compute Node** or a **Management Node**. **Note** If you install multiple servers, make sure that the first server is already configured, and then configure the other servers. Otherwise, the data in the dabatabase may gets corrupted. If you meet problems while configuring multiple servers, contact Trend Micro technical support.	a. Do one of the following to install the first server: • To install the first server as **Management and Compute Node:** • Type `configure init server 1 new`. • To install first server as **Management Node**: • Type `configure init server 3 new`. b. Follow *step 12 on page 2-11* to *step 15 on page 2-13* of this topic (configuring timezone, hostname, keyboard), and finish first server installation. c. Configure external storage. See *Configuring External Storage on page 7-11* for the procedure. d. Do one of the following to install subsequent servers: • To install subsequent server as **Management and Compute Node**: • Type `configure init server 1 vmi <first server's IP address>`. • To install subsequent server as **Compute Node**: • Type `configure init server 2 vmi <first server's IP address>`. • To install subsequent server as **Management Node:** • Type `configure init server 3 vmi <first server's IP address>`. e. Repeat *step 9 on page 2-6* (configuring password), *step 10 on page 2-7* (configuring network) and then steps *a on page 2-9* to *c on page 2-9* of this procedure to install more servers, if required.

TABLE 2-4. Setting Up Multiple Servers and Configuring Existing Database

To setup a multiple server, and configure an existing external database, you need to install at least two Virtual Mobile Infrastructure servers. **Important** See the **Notes** following this table.	a. Do one of the following to install the first server. • To install as **Management and Compute Node**: Type, `configure init server 1 db <db ip address> <db name> <db username> [db port] <db type>`, press **Enter**, and then type the database password when prompted. For example, `configure init server 3 db 10.206.139.20 vmidb tmvmi 3306 mysql`. • To install as **Management Node**: Type `configure init server 3 db <db ip address> <db name> <db username> [db port] <db type>` , press **Enter**, and then type the database password when prompted. For example, `configure init server 1 db 10.206.139.20 vmidb tmvmi 3306 mysql`. b. Follow *step 12 on page 2-11* to *step 15 on page 2-13* of this topic (configuring timezone, hostname, keyboard), and finish first server installation. c. Configure external storage. See *Configuring External Storage on page 7-11* for the procedure. d. Do one of the following to install subsequent servers: • To install as **Management and Compute Node**: Type `configure init server 1 vmi <first server's IP address>`. • To install subsequent server as **Compute Node**: Type `configure init server 2 vmi <first server's IP address>`. • To install as **Management Node**: Type `configure init server 3 vmi <first server's IP address>`. **Note** To install subsequent servers, you do not need to specify the database IP address during this step. e. Repeat *step 9 on page 2-6* (configuring password), *step 10 on page 2-7* (configuring network) and then steps *a on page 2-10* to *c on page 2-10* of this procedure to install more servers, if required.

Note

Before you install a virtual machine, you must create a database for Virtual Mobile Infrastructure on your external database, and make sure that the database user account can access the database you have just created.

For example, the database name may look like: "**vmidb**".

When you create **vmidb** database, set character as "UTF-8", and grant all privileges to the user. For example, mysql can use the command "`GRANT ALL ON vmi_db.* TO 'vmi_user'@'%' IDENTIFIED BY 'passowrd';` ".

Note

If you install multiple servers, make sure that the first server is already configured, and then configure the other servers. Otherwise, the data in the dabatabase may gets corrupted.

If you meet problems while configuring multiple servers, contact Trend Micro technical support.

12. Type `configure init timezone` to configure timezone, and type your timezone; for example, `America/Los_Angeles`.

```
# configure init timezone
Current timezone is:
      Local time: Thu 2018-12-27 17:00:44 CST
  Universal time: Thu 2018-12-27 09:00:44 UTC
        RTC time: Thu 2018-12-27 09:00:44
       Time zone: Asia/Shanghai (CST, +0800)
     NTP enabled: yes
NTP synchronized: yes
 RTC in local TZ: no
      DST active: n/a
Please input new timezone name, empty for help: America/Los_Angeles
Set timezone to: America/Los_Angeles ok
#
```

13. To change the default hostname (localhost), type `configure init hostname <host name>`. For example, `configure init hostname vmi`.

```
# configure init hostname vmi
After set, new hostname is: vmi
# _
```

14. To change the default keyboard type (US), type `configure init keymap`, and enter the type you want to set. For example, `jp`.

15. Type `reboot` to restart your system for the configurations to take effect.

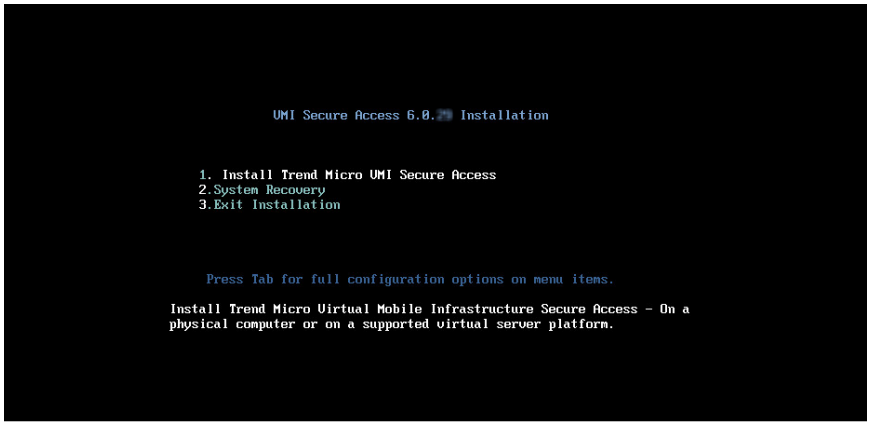
Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server

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

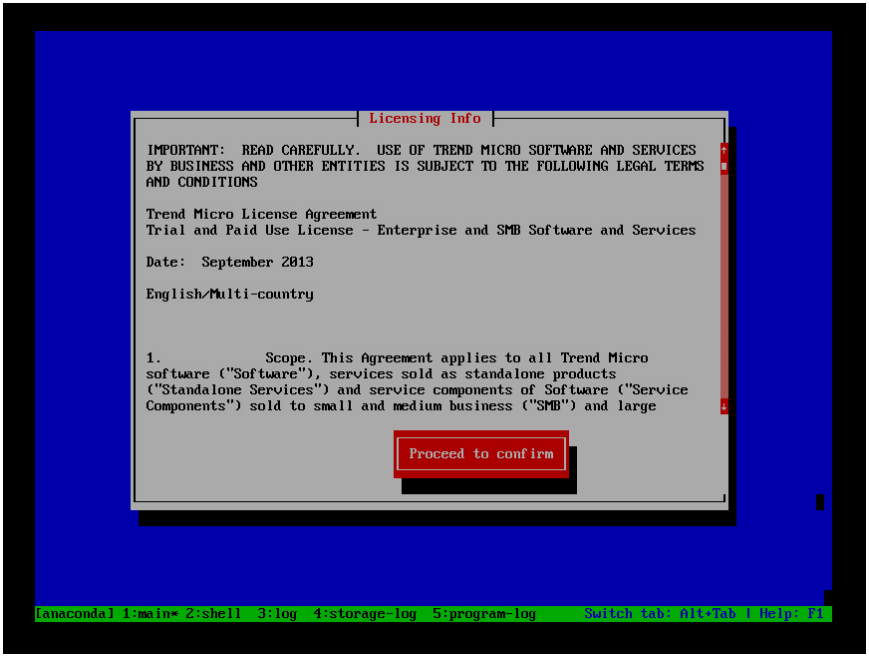
1. Power on the Bare Metal server where you want to install Virtual Mobile Infrastructure Secure Access.
2. Insert the installation DVD into the DVD drive, and reboot the server.

   The Secure Access installation menu appears.



3. Select **Install Secure Access** and press **Enter**.

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

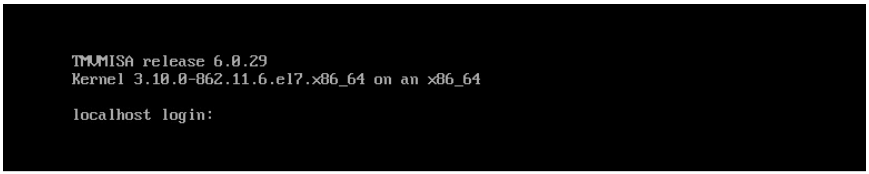


4. Press **Tab** to select **Proceed to Confirm**, and press **Enter**.

A page appears where you can accept the license agreement.

5. Press **Tab** to select **Accept**, and press **Enter** to continue.

The installation begins. The installation process may take about 10 minutes or more to complete. Once the installation process completes, the system reboots to allow configuration and displays the following screen.



6. Use username (localhost login) `admin`, and default password `admin` to log in.
7. Type `enable`, and the default password `admin` to enter the privilege mode and start the configuration steps.
8. If you need help during configuration, type `configure init help` and press **Enter** to check the configuration help.

```
# configure init help
After installation, please execute following command to configure your system:
1. To set root and admin account password, type command:
     configure init password
2. To setup network, type command:
     configure init network static IP_address/subnet_mask_bits gateway_address DNS1 [DNS2]
   For example:
     configure init network static 10.206.139.2/24 10.206.139.254 10.64.1.54
   Or type:
     configure init network dhcp
   to get a dynamic IP address.
3. To setup VMI Secure Access server, type command:
     configure init server  10.21.22.1
4. To setup timezone, type command:
     configure init timezone
   Timezone example, "Asia/Shanghai".
5. To setup hostname, type command:
     configure init hostname
6. To setup keyboard type, type command:
     configure init keymap
#
```

9. Type `configure init password`, to configure password for root account and admin account.

```
# configure init password
Passwords must be at least six (6) characters in length, and contain:
    a minimum of 1 lower case letter and
    a minimum of 1 upper case letter and
    a minimum of 1 numeric character and
    a minimum of 1 special character

Type the root password:
Confirm the root password:
Changing password for user root.
New password: Retype new password: passwd: all authentication tokens updated successfully.

Passwords must be at least six (6) characters in length, and contain:
    a minimum of 1 lower case letter and
    a minimum of 1 upper case letter and
    a minimum of 1 numeric character and
    a minimum of 1 special character

Type the admin and tmvmi password:
Confirm the admin and tmvmi password:
Changing password for user tmvmi.
New password: Retype new password: passwd: all authentication tokens updated successfully.

Finish setup password.
#
```

10. Type one of the following to configure IP address for Virtual Mobile Infrastructure server:

- For static IP address: `configure init network <static> <IP address/subnet_mask_bits> <gateway address> <DNS1> [DNS2]`
- For dynamic IP address: `configure init network dhcp`

For example, `configure init network static 10.206.139.48/22 10.206.139.254 10.64.1.54`.

Note

Trend Micro does not recommend using dynamic IP address (dhcp) for Secure Access. This is because the client mobile devices need to connect to the Virtual Mobile Infrastructure server through an IP address. Therefore, the dynamic IP address may change later, and will disconnect the communication between servers and client mobile devices.

11. Type `configure init server <VMI server IP address>` to bind a Virtual Mobile Infrastructure server to this Secure Access.

```
# configure init server 10.206.139.48
vmi_srv_addr='10.206.139.48'
protocol='https'
port='443'
Restarting vmigateway (via systemctl):                    [  OK  ]
success set master VMI manager server IP:10.206.139.48
# _
```

12. Type `configure init timezone` to configure timezone, and type your timezone; for example, `America/Los_Angeles`.

```
# configure init timezone
Current timezone is:
      Local time: Thu 2018-12-27 17:00:44 CST
  Universal time: Thu 2018-12-27 09:00:44 UTC
        RTC time: Thu 2018-12-27 09:00:44
       Time zone: Asia/Shanghai (CST, +0800)
     NTP enabled: yes
NTP synchronized: yes
 RTC in local TZ: no
      DST active: n/a
Please input new timezone name, empty for help: America/Los_Angeles
Set timezone to: America/Los_Angeles ok
#
```

13. To change the default hostname (localhost), type `configure init hostname <host name>`. For example, `configure init hostname vmi`.

```
# configure init hostname vmi
After set, new hostname is: vmi
# _
```

14. To change the default keyboard type (US), type `configure init keymap`, and enter the type you want to set. For example, `jp`.

15. Type `reboot` to restart your system for the configurations to take effect.

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**.

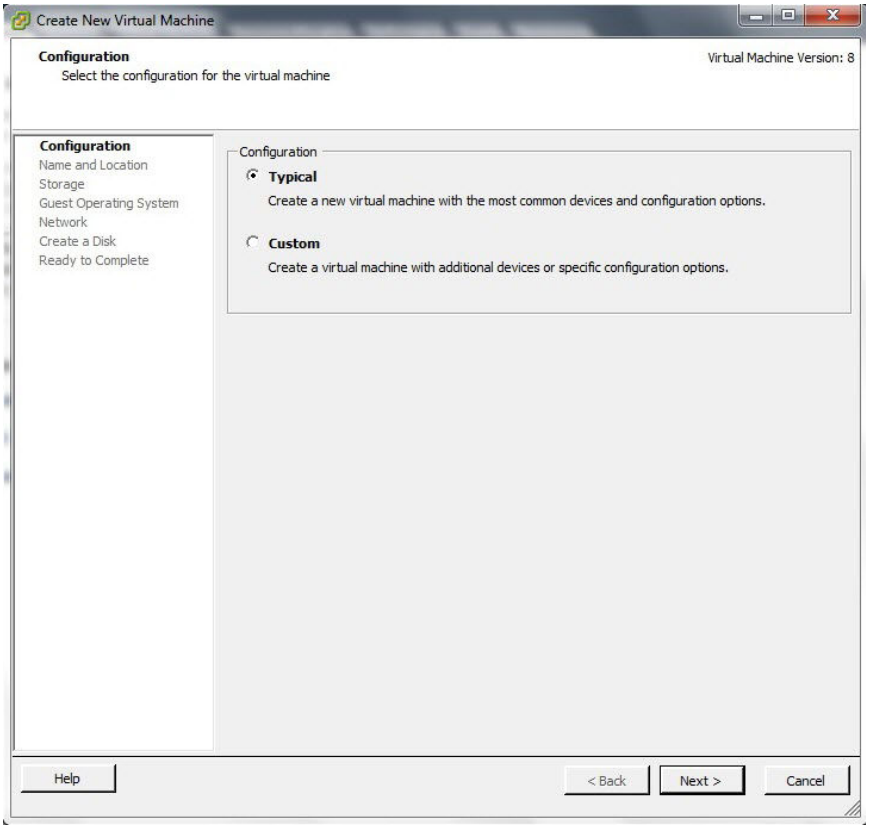


FIGURE 3-1. Select Configuration

The **Name and Location** screen appears.

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

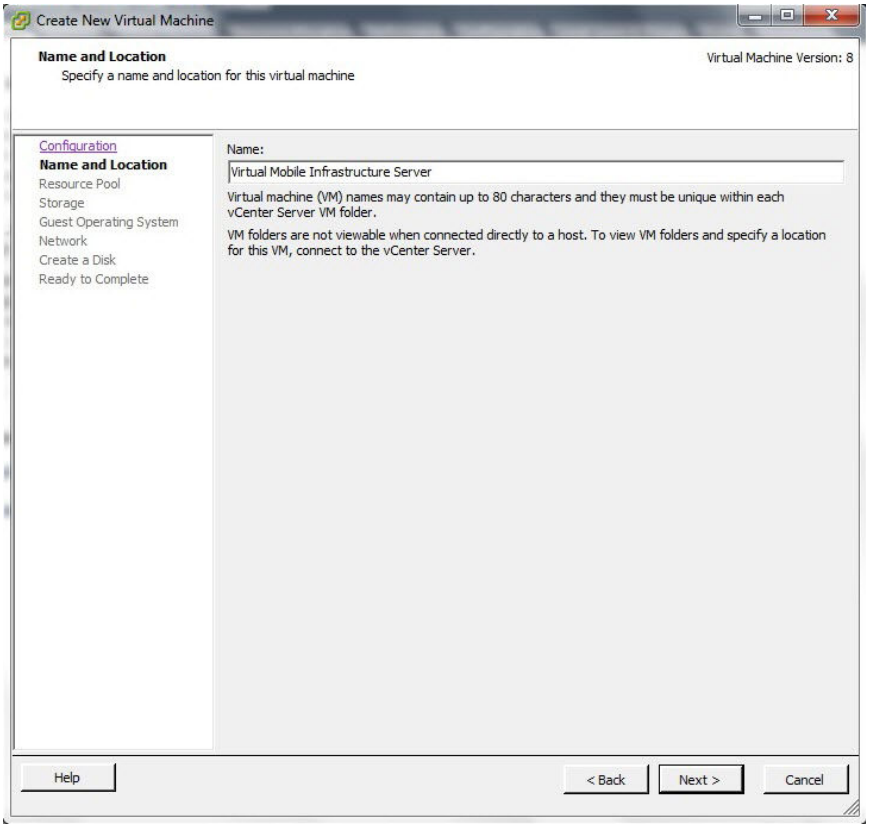


FIGURE 3-2. Type a name for the new virtual machine

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**.

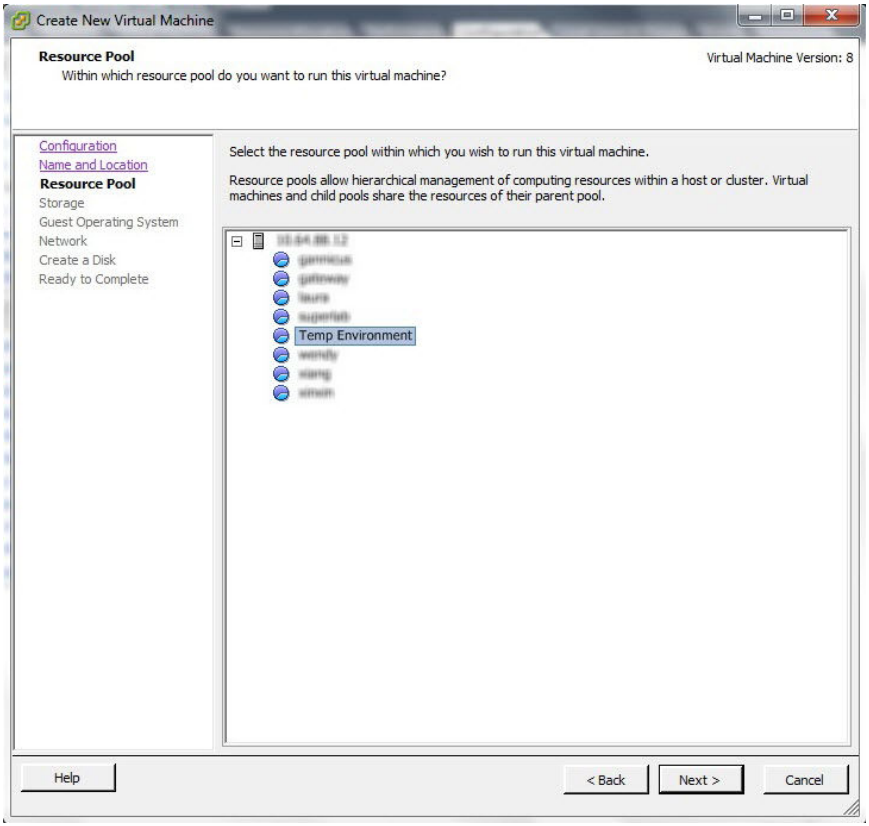


FIGURE 3-3. Select a resource pool

The **Storage** screen appears.

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

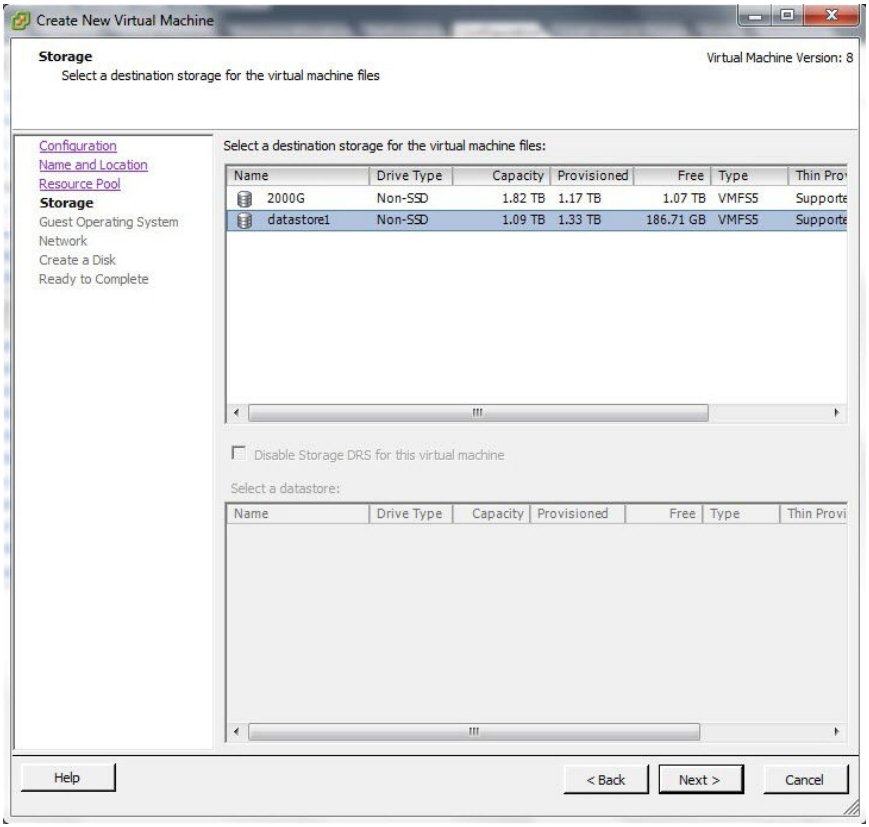


FIGURE 3-4. Select a storage to install Virtual Mobile Infrastructure Server

The **Guest Operating System** screen appears.

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

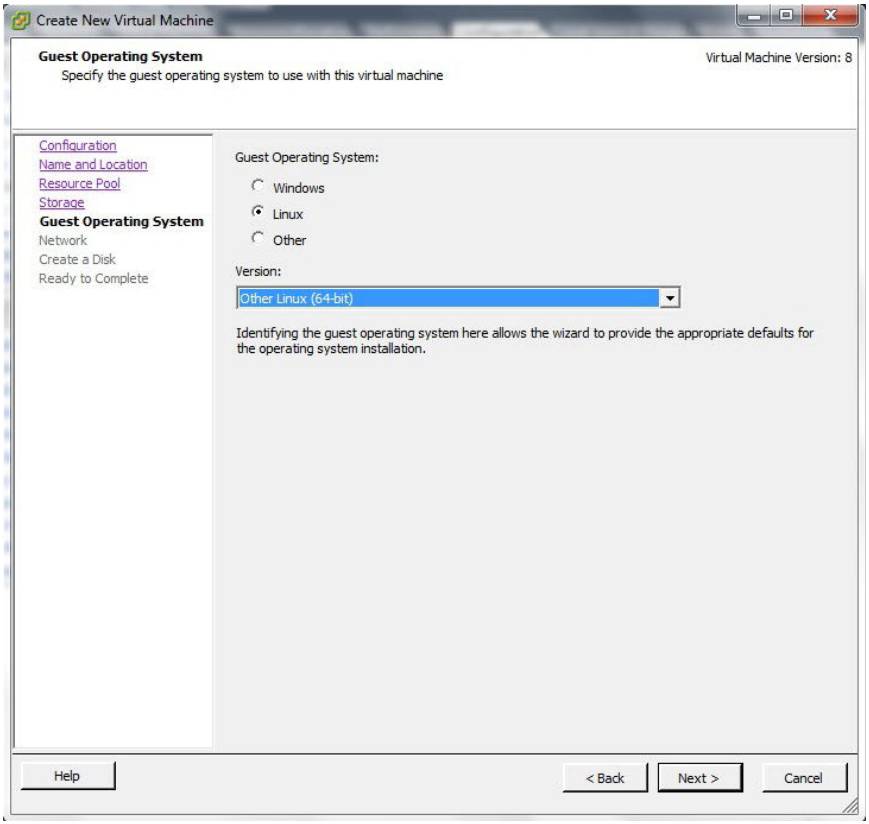


FIGURE 3-5. Select the guest operating system

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

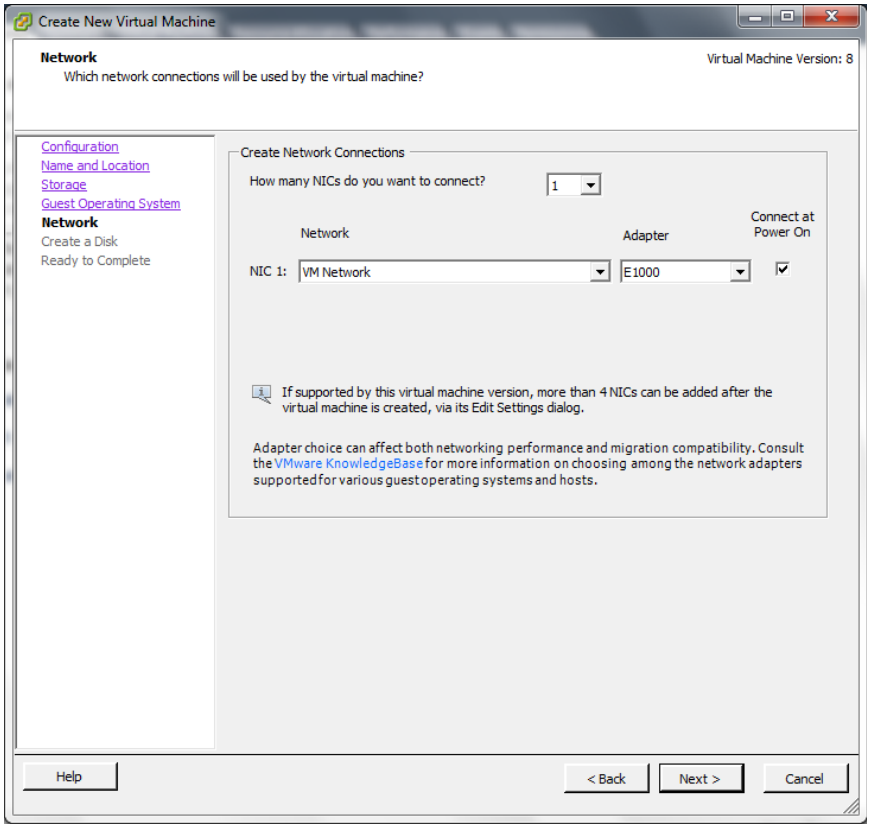


FIGURE 3-6. Create network connections

10. Click **Next**.

    The **Create a Disk** screen appears.

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

    a. Select at least 50-GB of virtual disk space for Virtual Mobile Infrastructure.

    b. Select **Thick Provision Lazy Zeroed**

    c. Click **Next**.

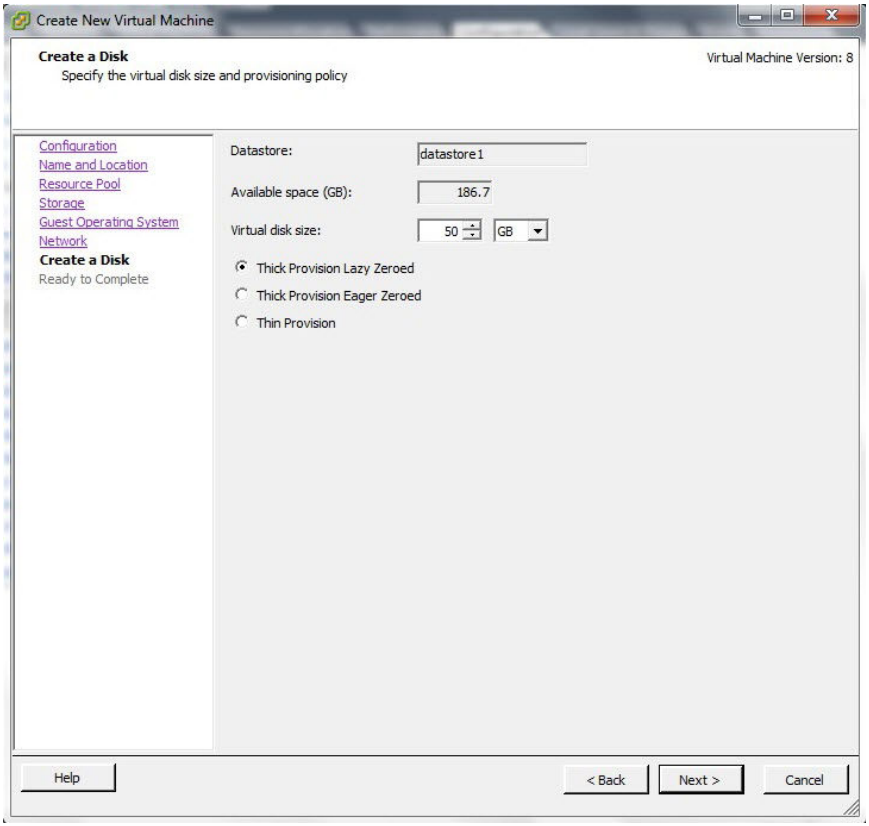


FIGURE 3-7. Specify Hard Disk Space

The **Ready to Complete** screen appears.

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

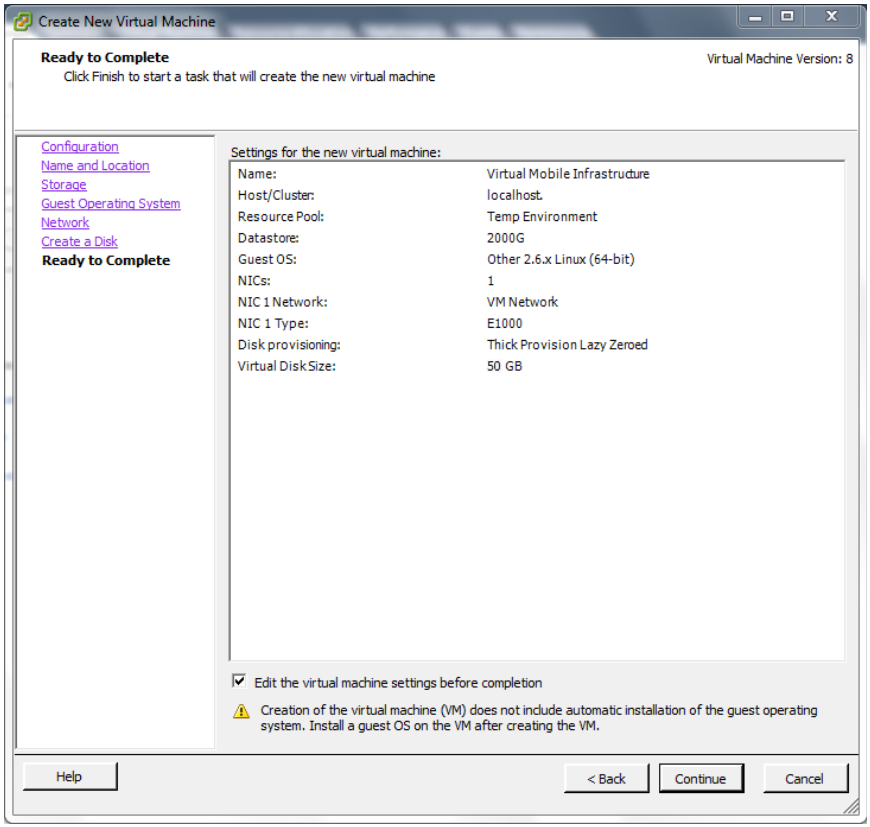


FIGURE 3-8. Ready to Complete

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 8-GB.

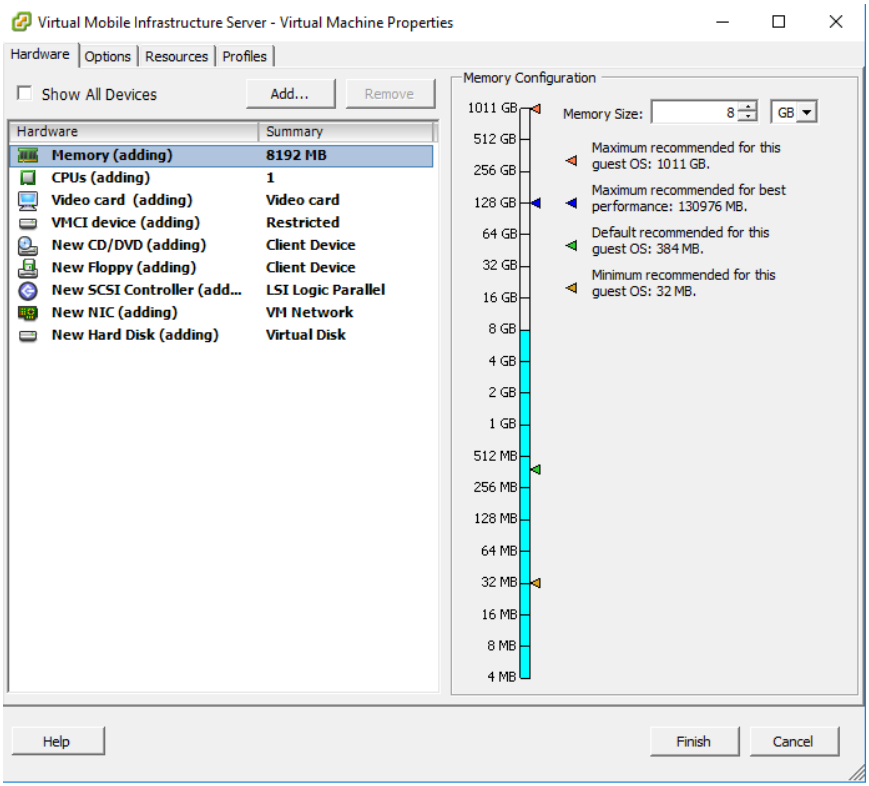


FIGURE 3-9. VM Properties - Memory Configuration

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 **4**.

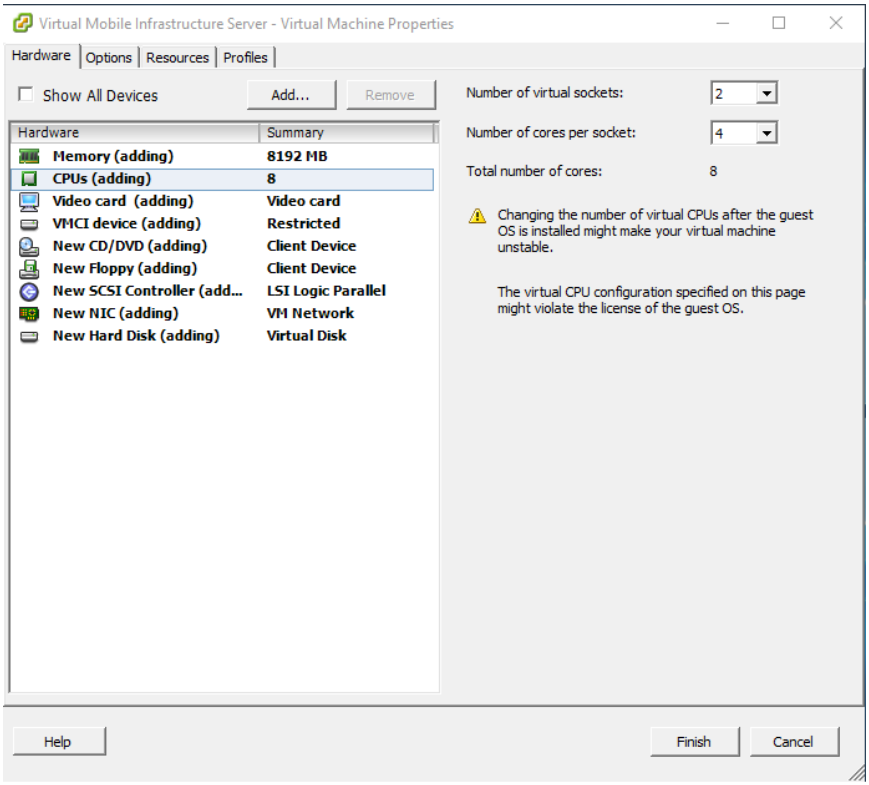


FIGURE 3-10. VM Properties - CPU Settings

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**.

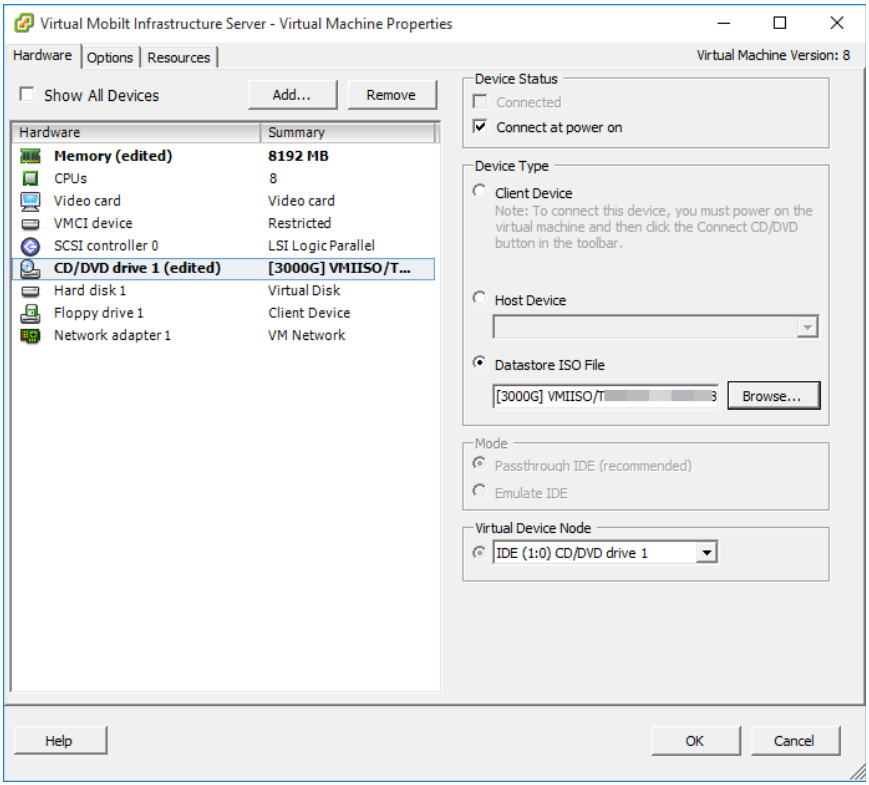


FIGURE 3-11. VM Properties - CD/DVD Settings

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 16 on page 2-13* 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 Virtual Mobile Infrastructure Secure Access on VMware ESXi on page 3-25*)

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**.

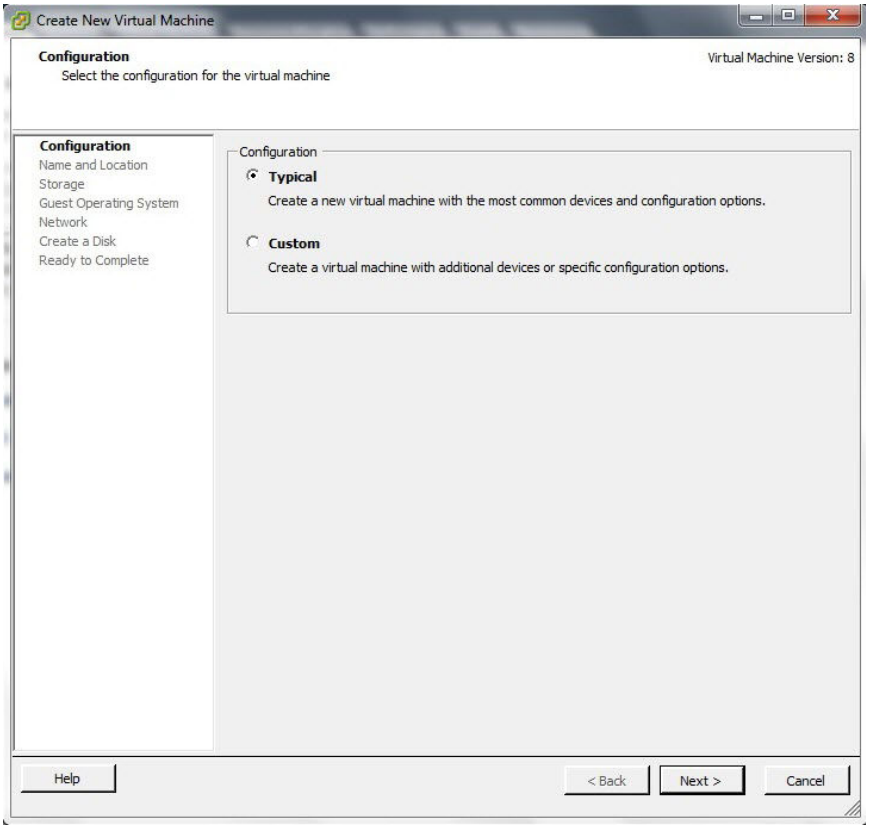


FIGURE 3-12. Select Configuration

The **Name and Location** screen appears.

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

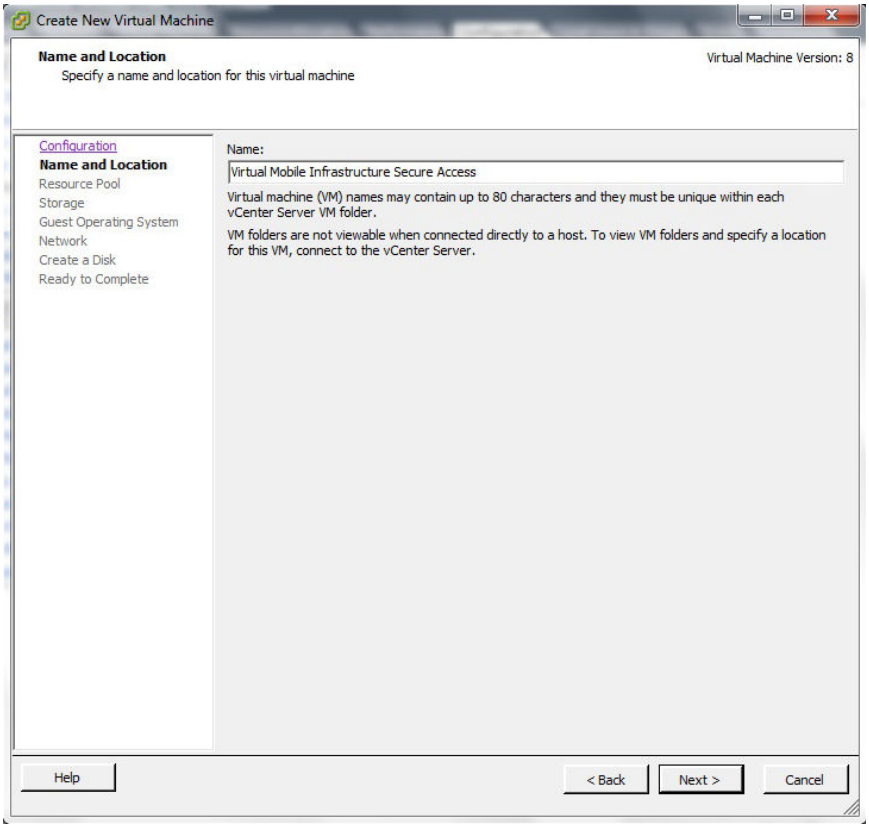


FIGURE 3-13. The Resource Pool screen appears.

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**.

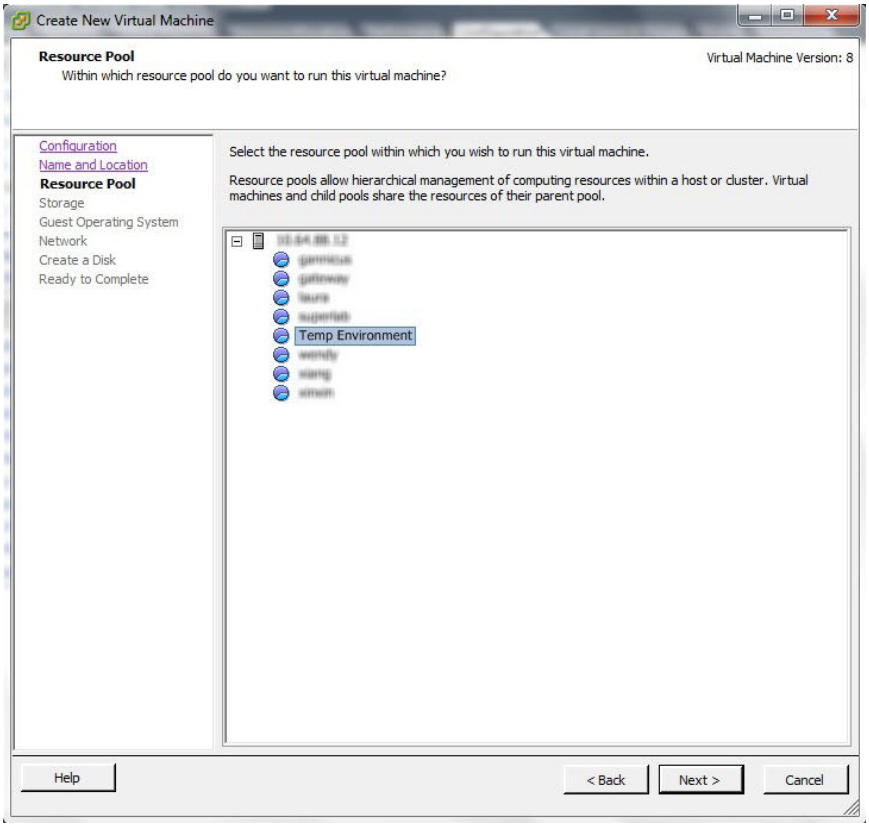


FIGURE 3-14. Select a resource pool

The **Storage** screen appears.

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

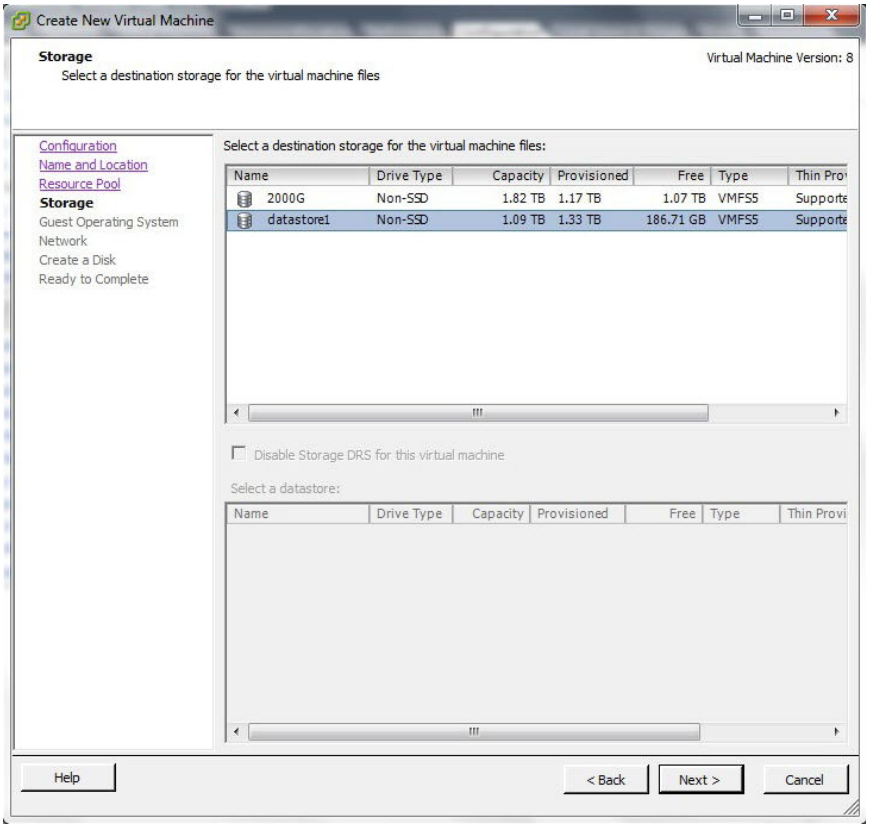


FIGURE 3-15. Select a storage to install Virtual Mobile Infrastructure Secure Access

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

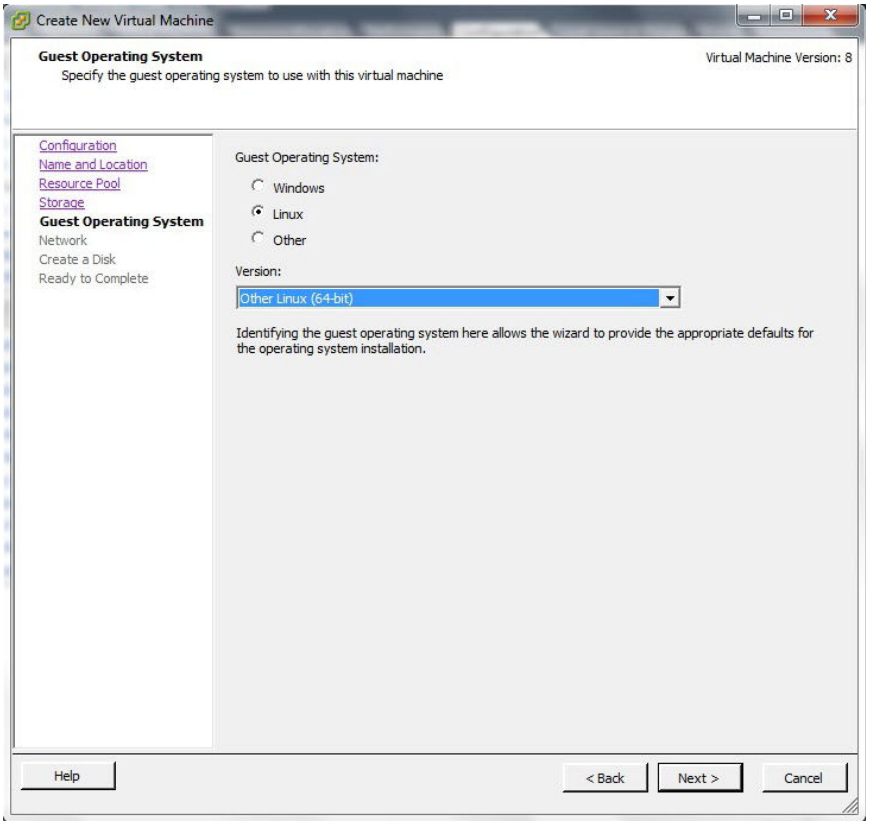


FIGURE 3-16. Guest Operating System

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

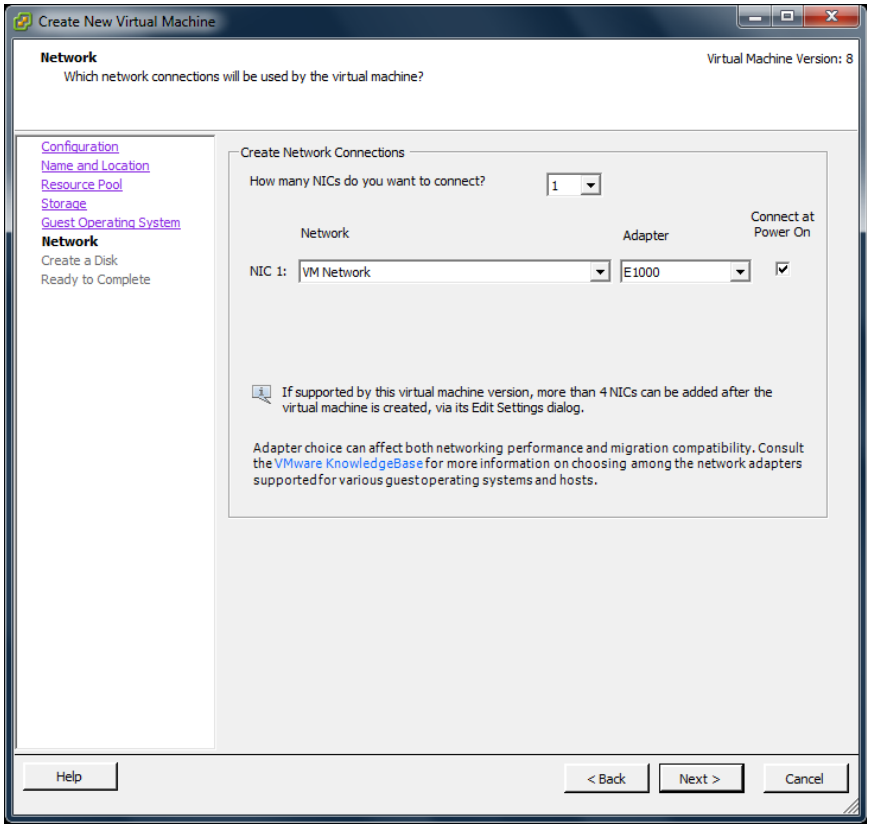


FIGURE 3-17. Create Network Connections

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**.

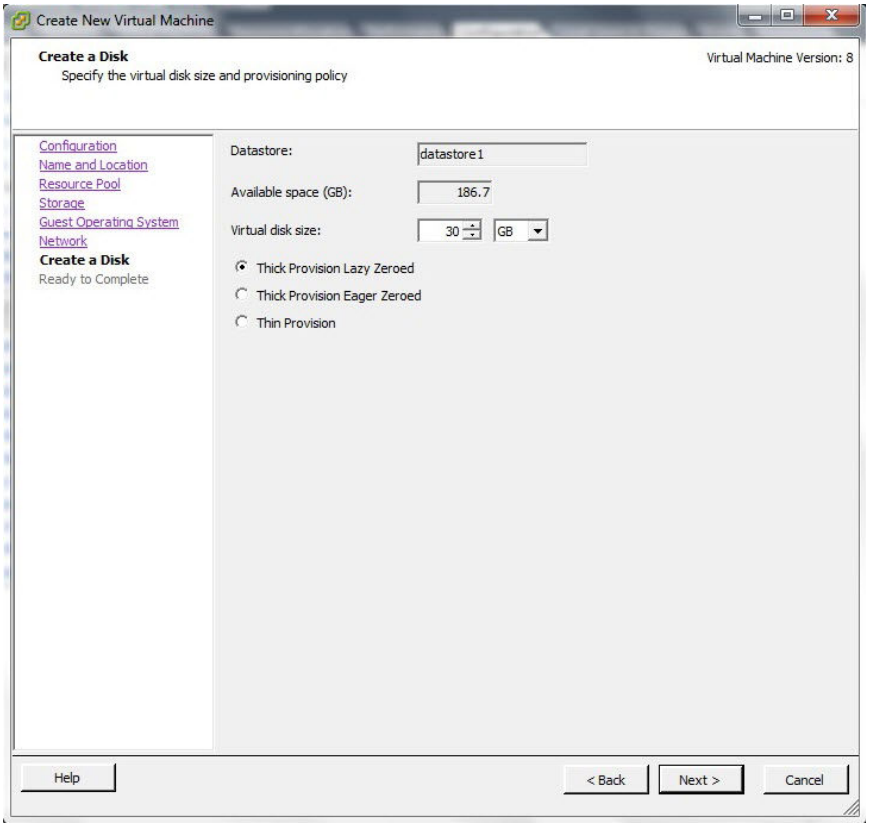


FIGURE 3-18. Specify Hard Disk Space

The **Ready to Complete** screen appears.

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

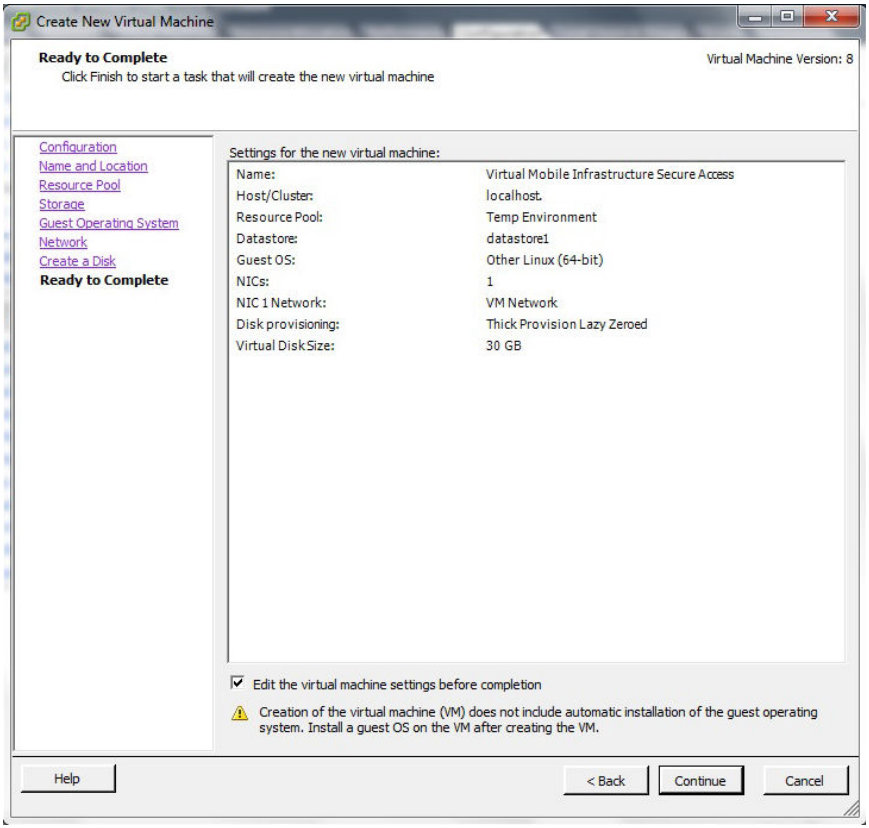


FIGURE 3-19. Ready to Complete

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.

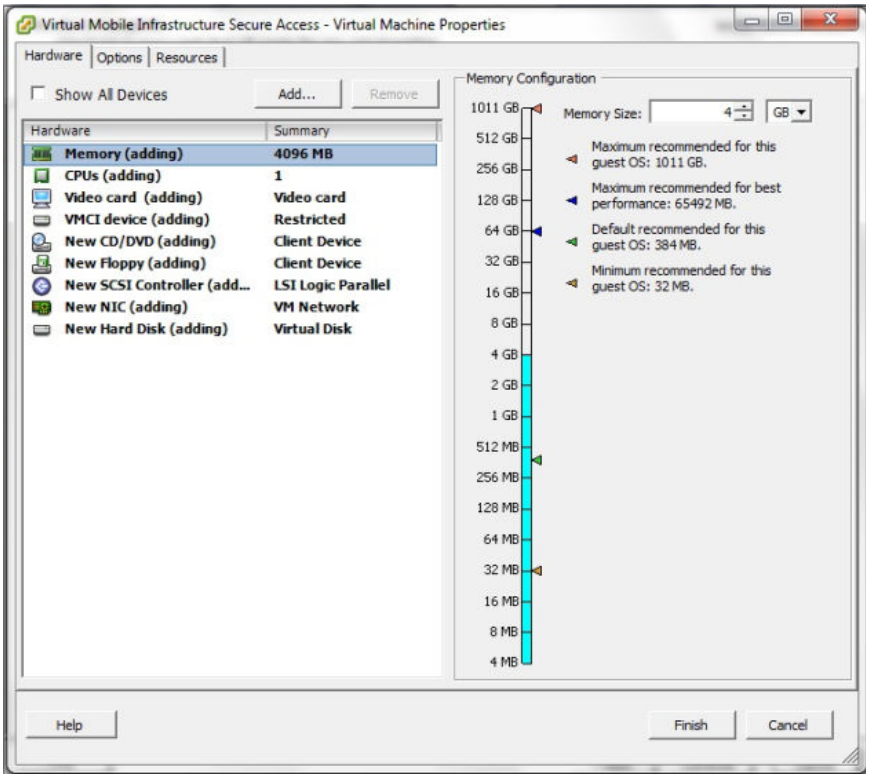


FIGURE 3-20. VM Properties - Memory Configuration

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

    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**.

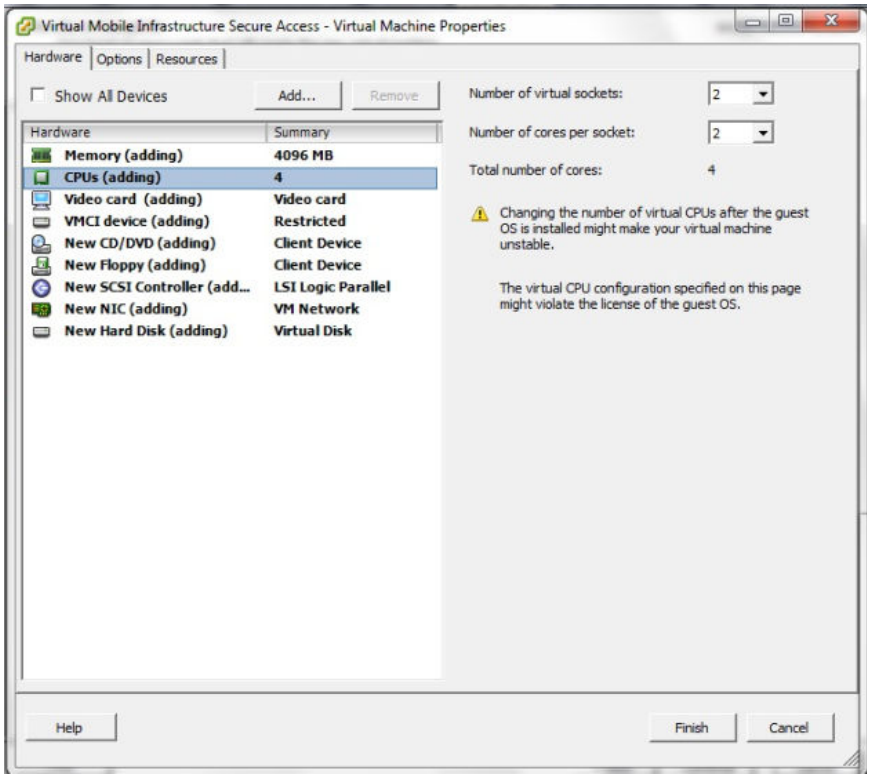


FIGURE 3-21. VM Properties - CPU Settings

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**.

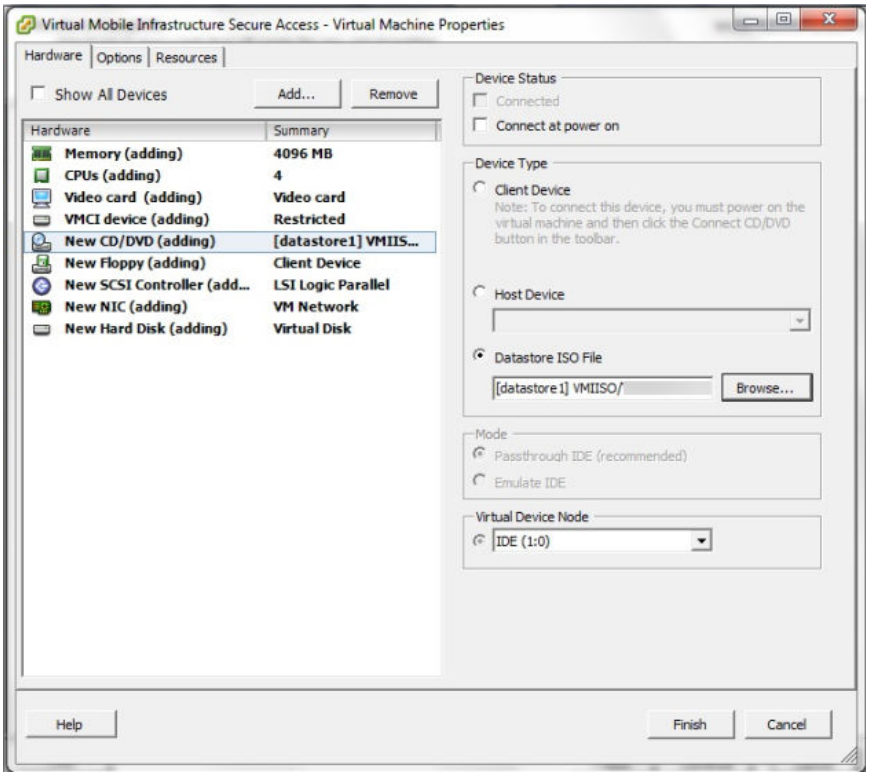


FIGURE 3-22. VM Properties - CD/DVD Settings

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

Step 2: Installing Virtual Mobile Infrastructure 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 2-14* to *step 15 on page 2-22* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-13* 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 12.5.9 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

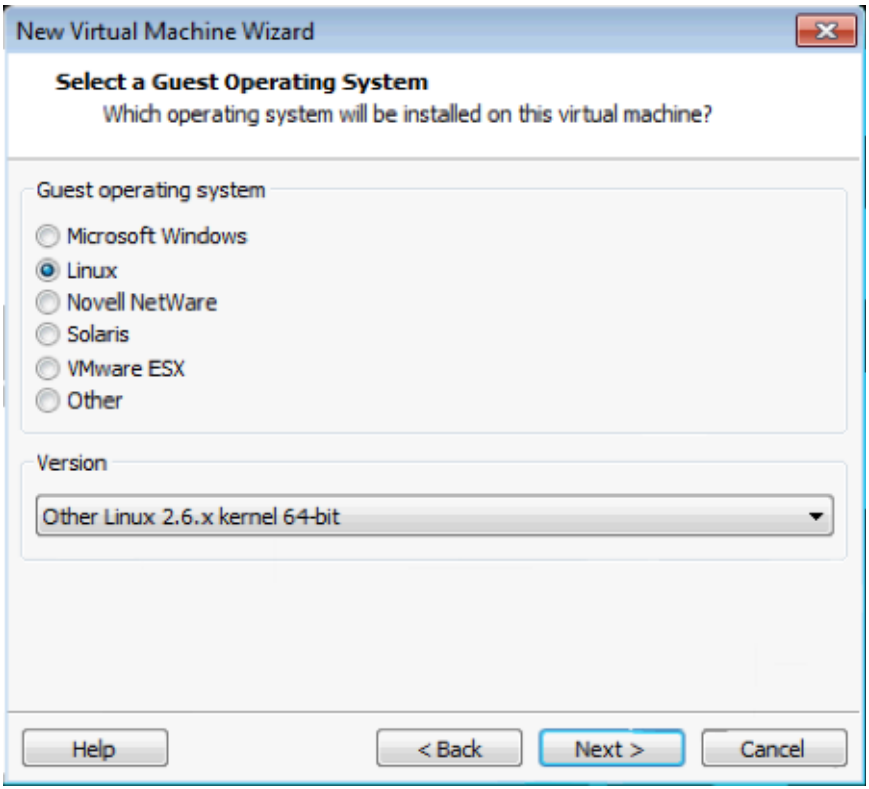


FIGURE 4-1. Select a guest operating system

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 **4**.
11. Click **Next**.

    The **Memory for the Virtual Machine** screen appears.
12. In the **Memory for the virtual machine** field, select at least **8-GB**, 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 **50-GB** for the **Maximum disk size**.
    - Select **Split virtual disk into multiple files**.

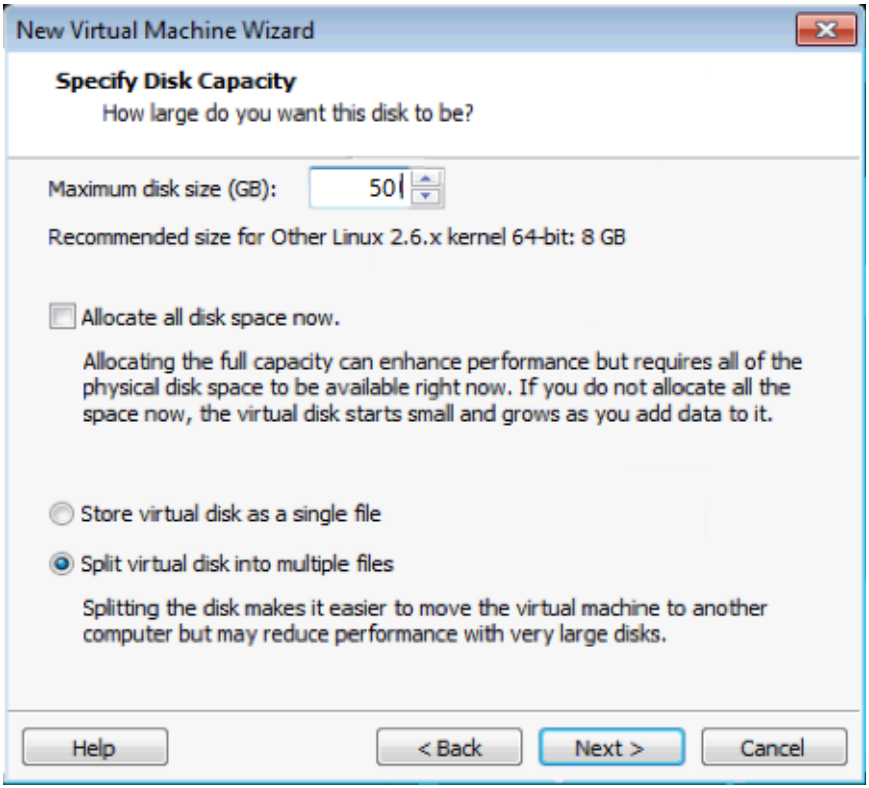


FIGURE 4-2. Specify disk capacity

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**.

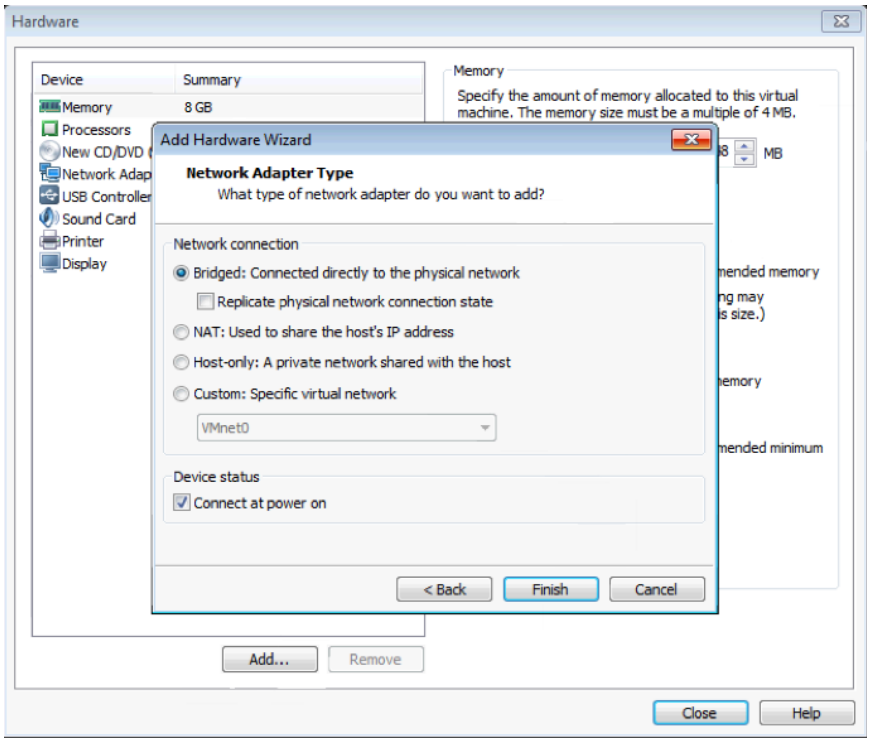


FIGURE 4-3. Configure network adapter type

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**.

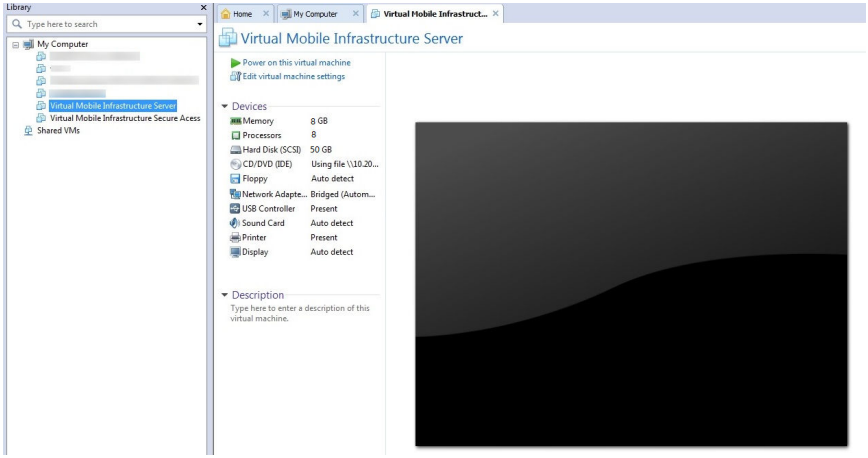


FIGURE 4-4. Virtual machines in VMware Workstation

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 12.0. 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**.

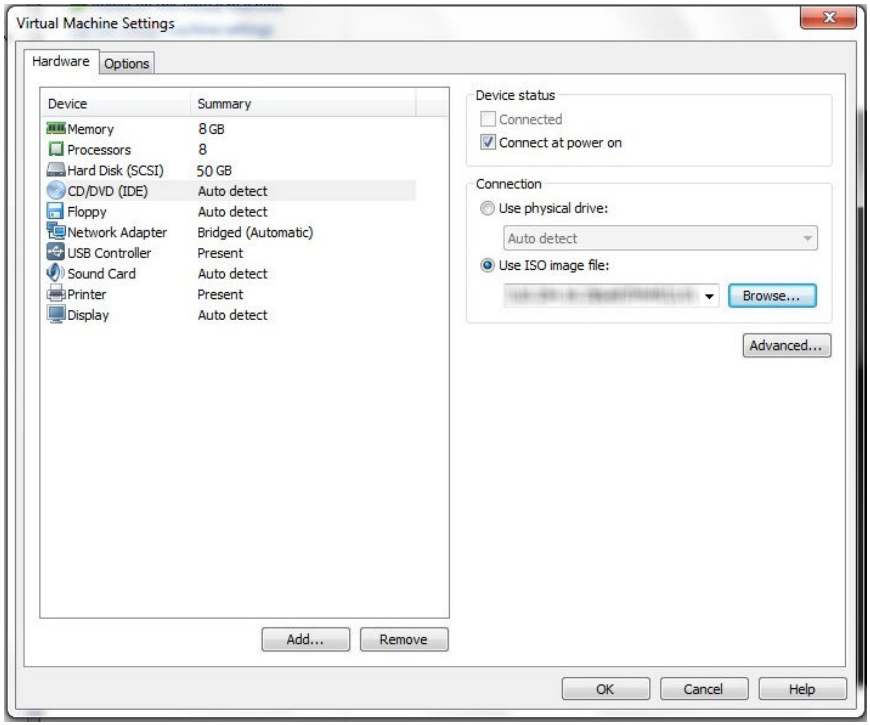


FIGURE 4-5. Browse and select Virtual Mobile Infrastructure Server ISO image file

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 16 on page 2-13* 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 12.5.9 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

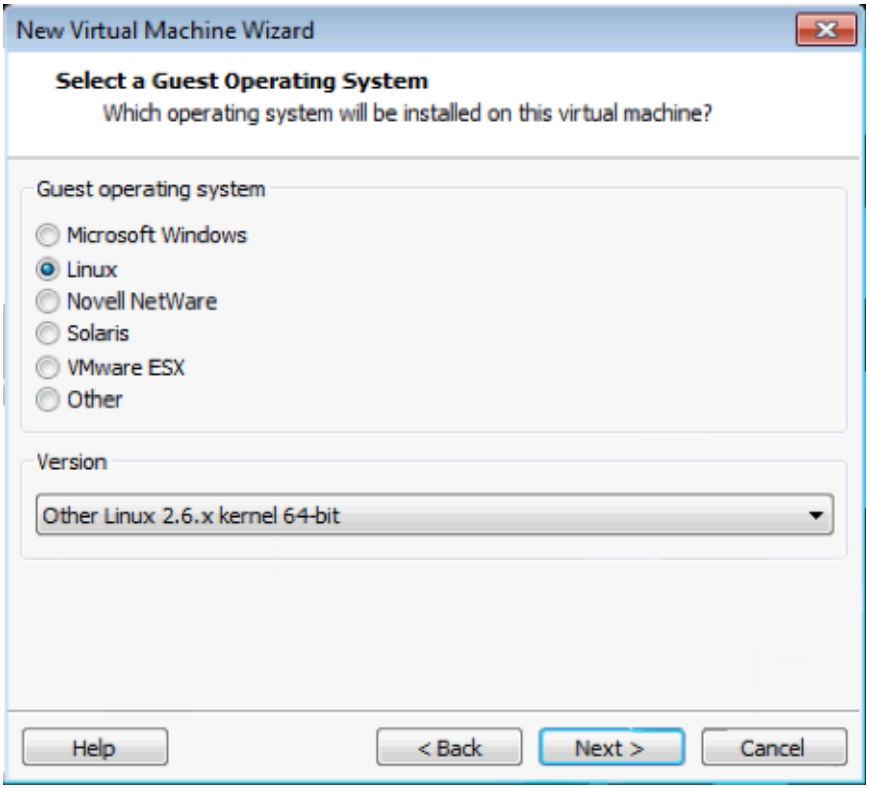


FIGURE 4-6. Select a guest operating system

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 **2**.

11. Click **Next**.

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

12. In the **Memory for the virtual machine** field, select at least **4-GB**, 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**.

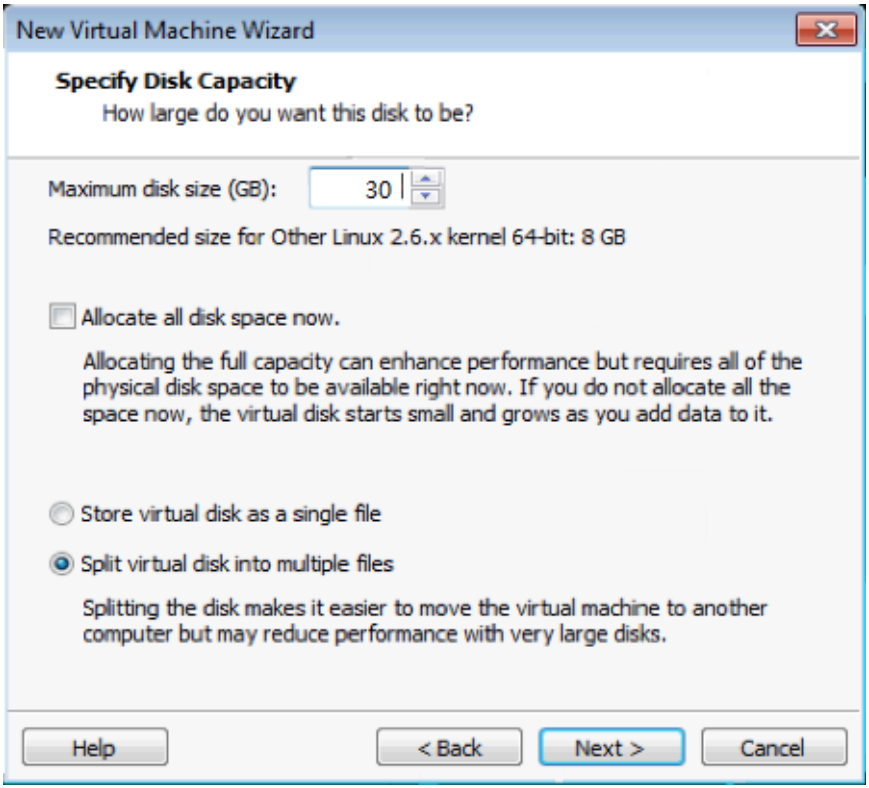


FIGURE 4-7. Specify disk capacity

18. Click **Next**.

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

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

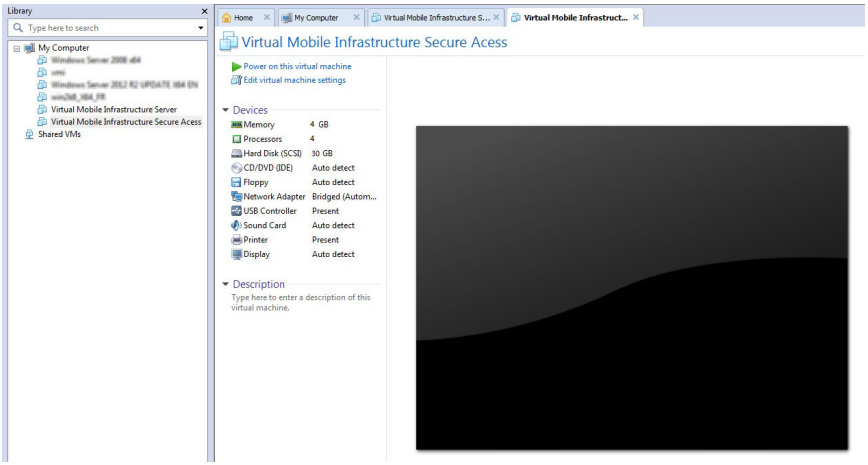


FIGURE 4-8. Virtual machines in VMware Workstation

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**.

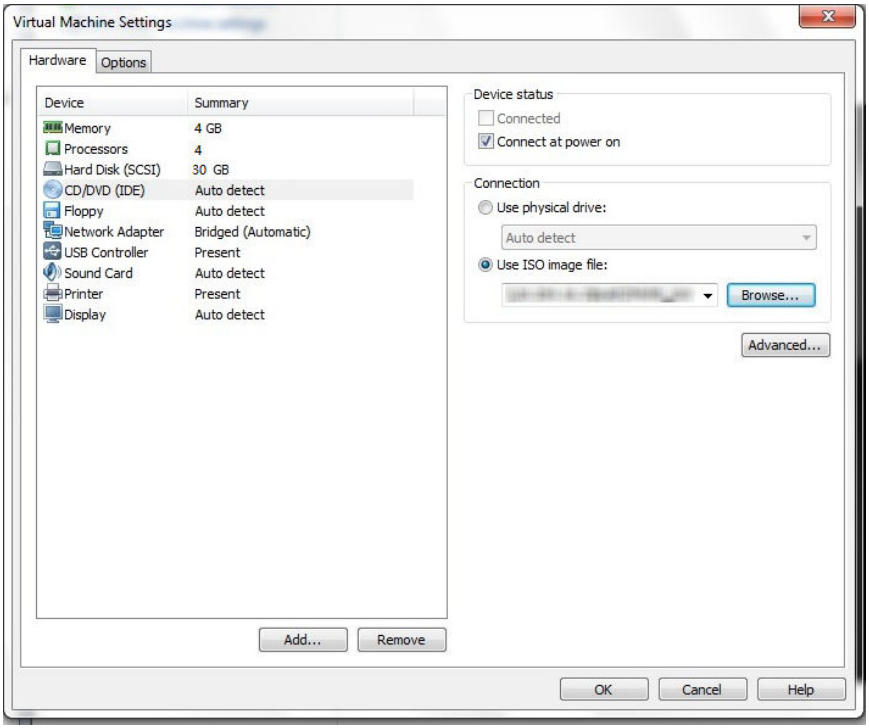


FIGURE 4-9. Browse and select Virtual Mobile Infrastructure Secure Access ISO image file

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 2-14* to *step 15 on page 2-22* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-13* 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 `8192` 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**.

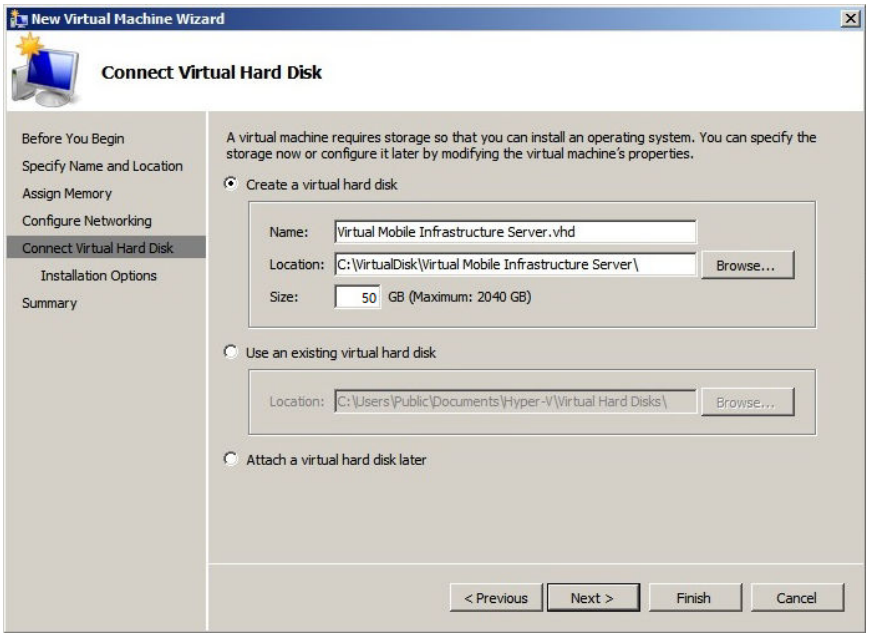


FIGURE 5-1. Create Virtual Hard Disk screen

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 8.

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.

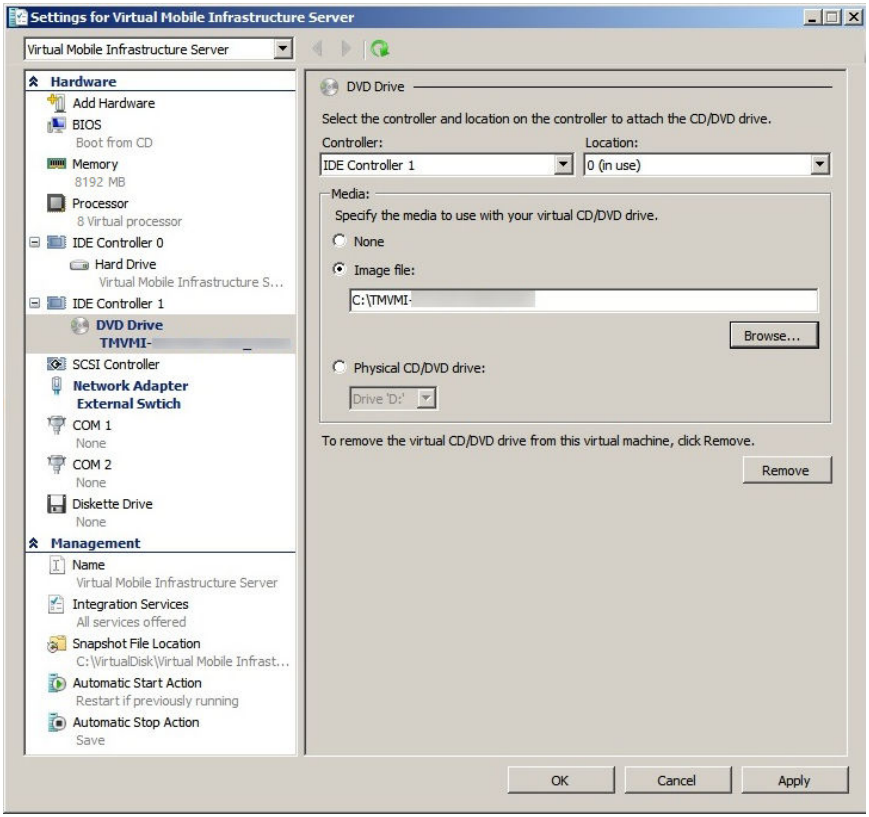


FIGURE 5-2. Select the Virtual Mobile Infrastructure server installation file

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 16 on page 2-13* 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**.

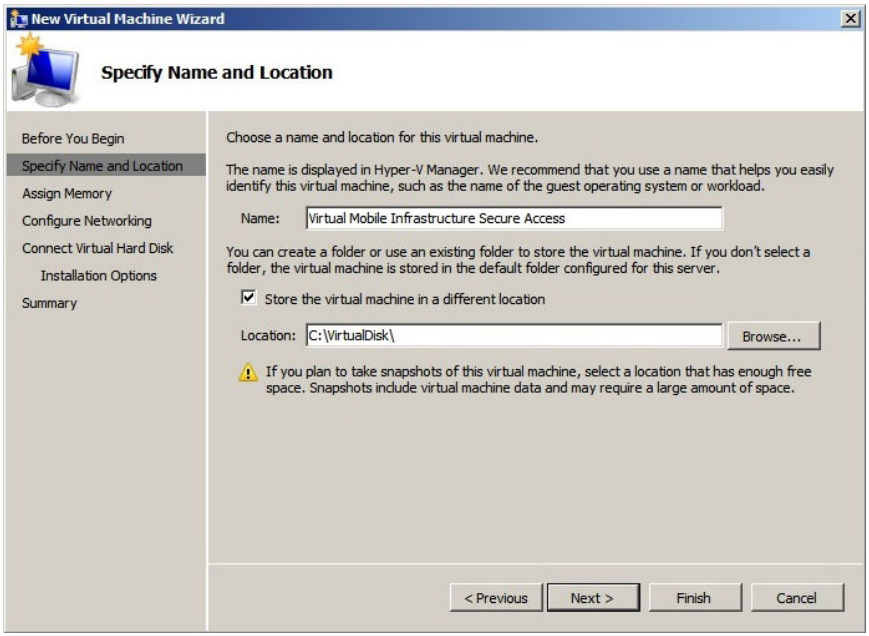


FIGURE 5-3. Create Virtual Hard Disk screen

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.

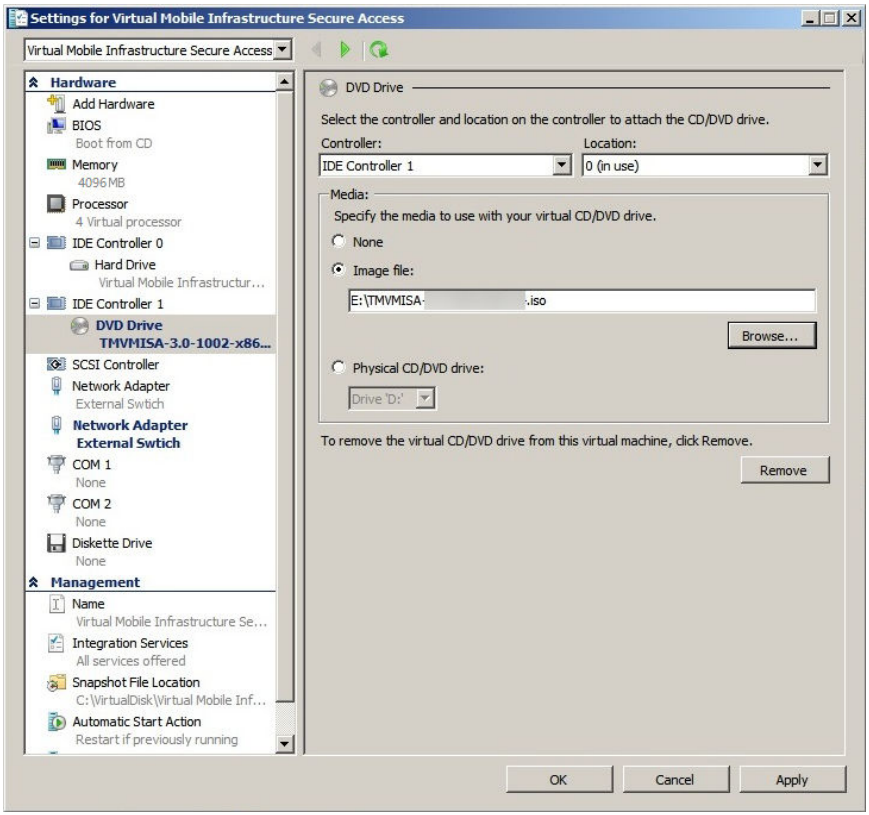


FIGURE 5-4. Select the Virtual Mobile Infrastructure Secure Access installation file

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 2-14* to *step 15 on page 2-22* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-13* 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 requires creating a virtual machine and installing Virtual Mobile Infrastructure Server. (See *Creating a Virtual Machine and Installing Virtual Mobile Infrastructure Server on page 6-2*.)

Creating a Virtual Machine and Installing Virtual Mobile Infrastructure Server

Note

The procedure is based on XenServer 7.4.

Procedure

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

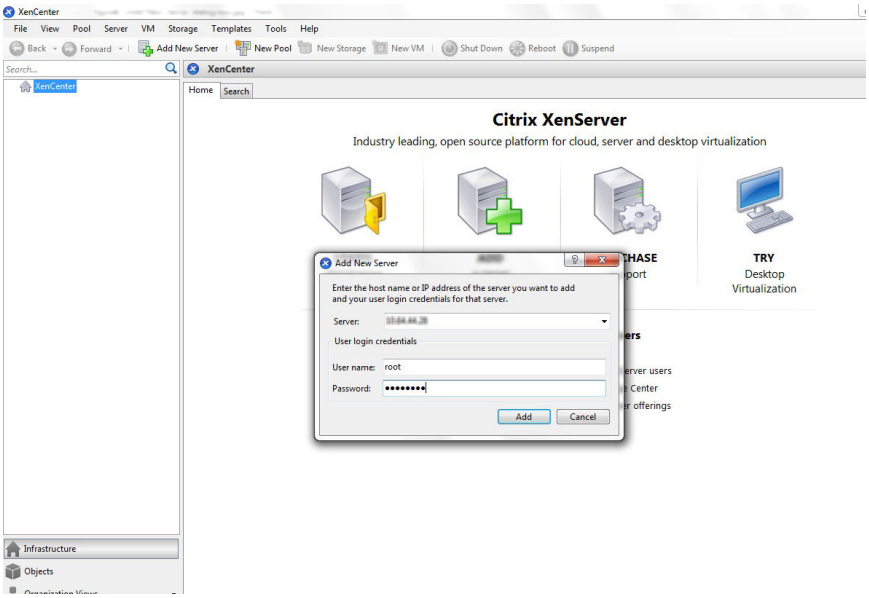


FIGURE 6-1. Add New Server dialog box

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 7**, and click **Next**.

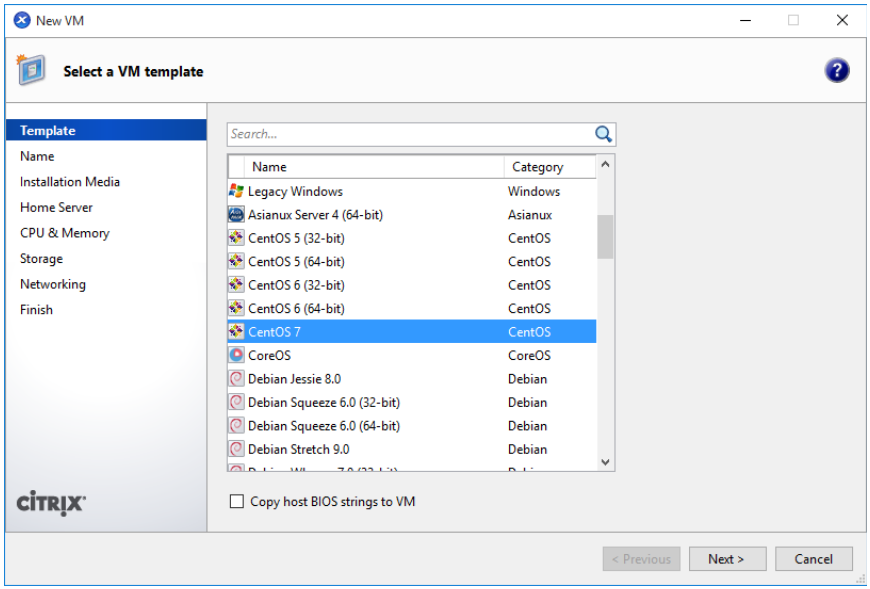


FIGURE 6-2. Select a VM template screen

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

   The **Installation Media** screen appears.

7. 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.

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**: 8

    b. **Memory**: 8 GB

11. Click **Next**.

The **Storage** screen appears.

12. Click **Properties**, and in the **Size** field, type `50` 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 the VM you just created, and click **Console**. The Virtual Mobile Infrastructure installation menu appears.
17. Follow *step 3 on page 2-2* to *step 16 on page 2-13* 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 requires creating a virtual machine and installing Virtual Mobile Infrastructure Secure Access. (See *Creating a Virtual Machine and Installing Virtual Mobile Infrastructure Secure Access on page 6-6*.)

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.

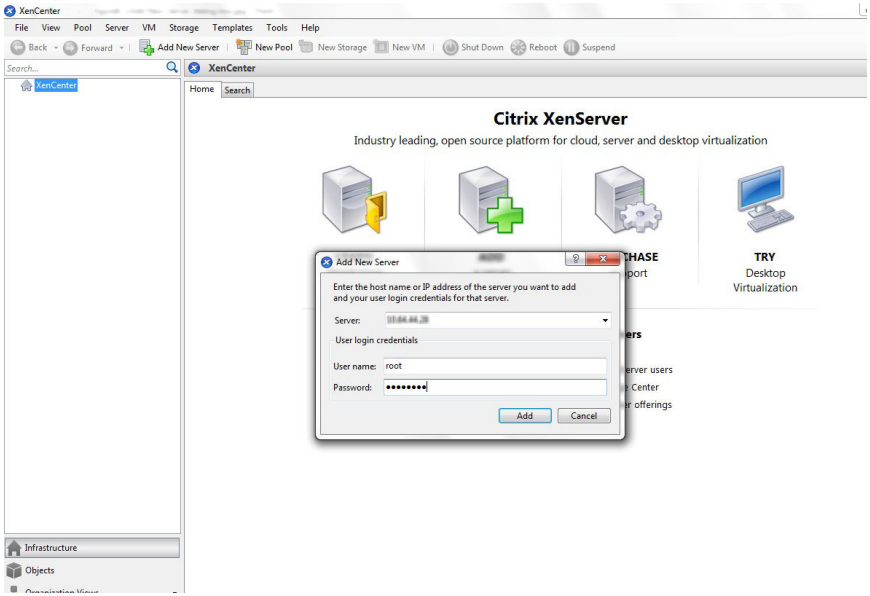


FIGURE 6-3. Add New Server dialog box

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 7 (64-bit)**, and click **Next**.

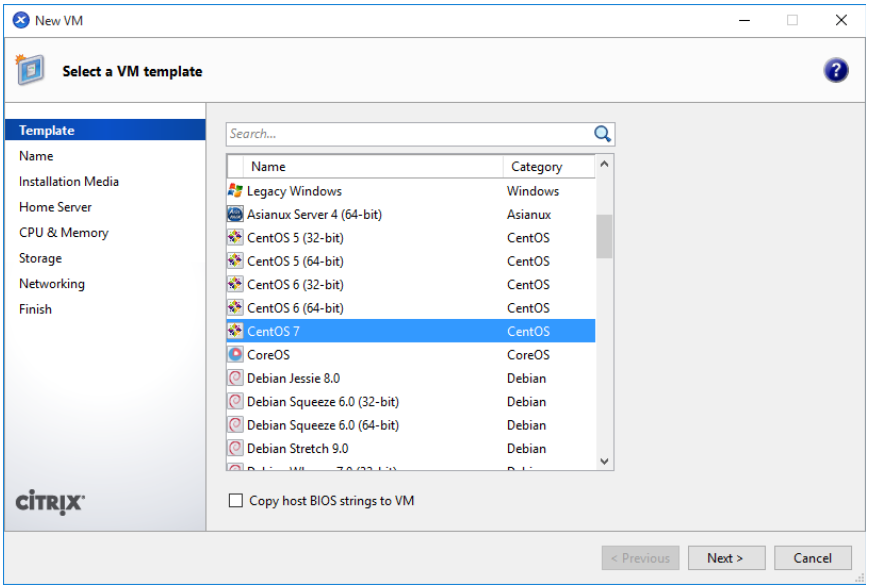


FIGURE 6-4. Select a VM template screen

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

   The **Installation Media** screen appears.

7. 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.

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**: `4` GB

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.

    The Virtual Mobile Infrastructure installation menu appears.

17. Follow *step 3 on page 2-14* to *step 15 on page 2-22* of the topic *Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-13* 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:

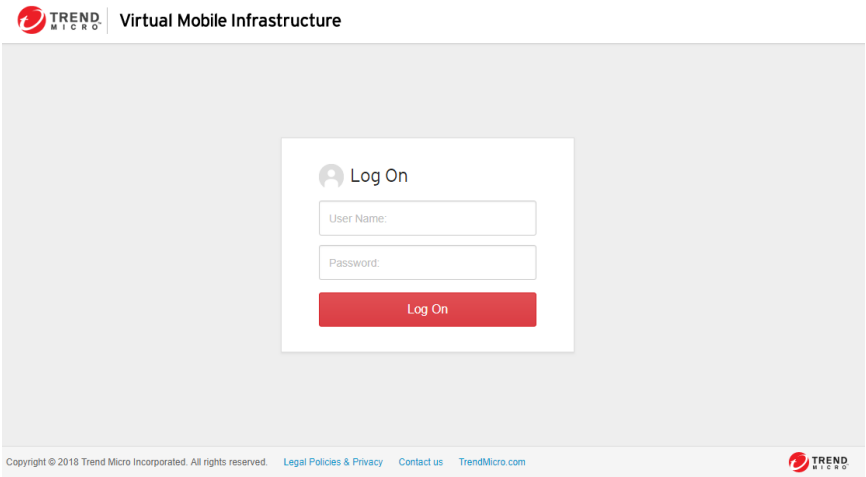
Procedure

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 7-5* for the procedure.

Activating Your Product

Virtual Mobile Infrastructure displays a **New Activation Code** screen on logging on to the administration Web console for the first time.

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

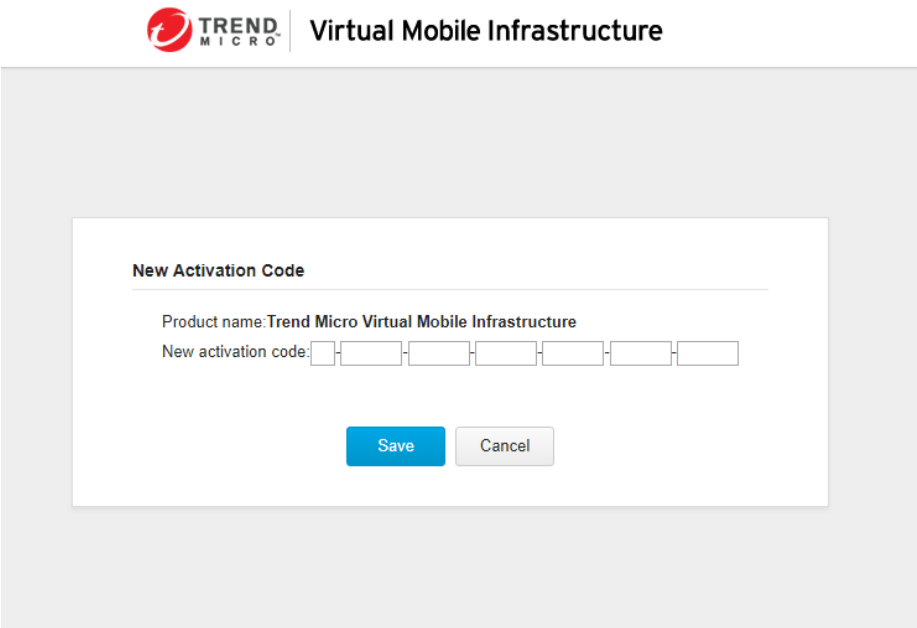


FIGURE 7-2. Product License screen

Note

If you do not have a license, contact you Trend Micro contact person to obtain your license.

Procedure

1. Type your **Activation Code** that you have received in your email in the field provided.
2. 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 7-5* 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 7-6* for the detailed procedure.
(Optional) Configure mobile client settings.	User settings for mobile client and users. See *Configuring Mobile Client Settings on page 7-7* for the detailed procedure.

ACTION	DESCRIPTION
(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 7-9* for the detailed procedure.
(Optional) Configure network settings.	Proxy and Virtual Mobile Infrastructure public IP address settings for user workspace. See *Configuring Network Settings on page 7-10* 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 on page 7-11* 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.
(Optional) Configure email notification settings.	SMTP server settings to send email notification to users. See *Configuring Email Notifications on page 7-12* for the detailed procedure.

Changing Administrator Account Password

Use the **Administrator Accounts** 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 **admin** 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.

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.
- **LDAP encryption**–select encryption method according to your LDAP server settings.

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 restriction**, 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 cloud workspace**, select the keyboard you want users to use during their Virtual Mobile Infrastructure session.
- If you want to restrict users from accessing workspace from a rooted or jailbroken mobile device, select **Do not allow users to log in from rooted or jailbroken mobile devices**.
- Select **Enable client side rendering** option to set client side rendering mode to default on TMVMI client.
- From the **Graphics Options** drop-down menu, select one of the following options:
  - **Performance**: This option provides more speed, but less quality (screen clarity), and utilizes less bandwidth.
  - **Balance** (default): This option provides balance between quality (screen clarity) and speed.

- **Quality**: This option provides more quality (screen clarity), but less speed, and utilizes more bandwidth.

3. 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 Network Settings

Use the **Network Settings** screen from the **System Settings** menu to configure VMI Public IP Address and proxy settings for Virtual Mobile Infrastructure server.

The **VMI public IP address** setting is required for mobile devices to access Virtual Mobile Infrastructure server from outside the network. If Secure Access is connected to a gateway or an external router, configure the IP address of the gateway or the router instead of the IP address of Secure Access. If Secure Access is not installed, keep the default settings.

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

Procedure

1. Under the **VMI Public IP Address** section, type the public domain name or IP address, and port number for public address.

Note

The default port number for public address is **443**.

2. Under the **Proxy** section, 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. Select one of the following options for **Apply proxy to**:
   - **Server and Workspace**
   - **Server only**
   - **Workspace only**
5. Click **Save**.

Configuring External Storage

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

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

Important

Make sure to stop all compute nodes before you add an external storage.

Procedure

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

   The server tests the connection with the external storage and saves the **Servers** 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. Select **Automatically send email notification to new users** if you want to send an invitation email to new users that are added from LDAP.

4. 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.

5. 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.

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**.

Managing Groups and Users

Virtual Mobile Infrastructure enables you to add users and groups manually or import them from the LDAP server. On importing a group from LDAP server, Virtual Mobile Infrastructure inherits all user account information from the LDAP server database.

Note

User accounts imported from the LDAP server cannot be modified from the Virtual Mobile Infrastructure server.

Importing Groups or Users from LDAP

Before importing groups or users from LDAP server, make sure that you have already configured the LDAP settings. See *Configuring LDAP Settings (Optional) on page 7-6* for the procedure.

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

Procedure

1. Click **Import Users**.

   The **Import Group or User from LDAP** 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**.

   Note

   If you configured SMTP server address in **Administration** > **Email Notifications** > **Email Settings**, and selected **Automatically send email notification to new users**, the invitation email will be sent to all new users that you import.

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 7-7* 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 7-12* 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.

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 **5902** to **6923**	Used by mobile client to access Virtual Mobile Infrastructure server.	Required	Inbound
Active Directory	TCP port **389** (Domain Controller) for Management console TCP port **636** (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

Component	Network Ports	Details	Required or Optional	Direction
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, if iOS TMVMI client is customized	Outbound
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 5902 to 6923	Used by Secure Access to communicate with Virtual Mobile Infrastructure server.	Required	Outbound

Appendix B

Public SSL Certificate Deployment

Virtual Mobile Infrastructure server and secure access are installed and managed using HTTPS and SSL, by default. The default installation of Virtual Mobile Infrastructure server and secure access uses a self-signed SSL certificate. Trend Micro recommends deploying public SSL certificate on Virtual Mobile Infrastructure server and secure access. A public SSL certificate on the server can avoid the browser security warning, and on the secure access, it can help user to make sure **tmvmi** client connects to a secure server and avoids security warning.

This chapter describes how to generate and install a public SSL certificate on Virtual Mobile Infrastructure server and secure access.

This appendix contains the following sections:

Managing Public SSL Certificate

Managing Public SSL Certificate on Virtual Mobile Infrastructure server and secure access involves the following steps:

1. Generating Certificate Signing Request (CSR) (See *Generating Certificate Signing Request (CSR) on page B-2*).

> **Note**
>
> If you already have a **Wildcard SSL Certificates**, skip this step, and proceed to the next step; *Deploying SSL Certificate on page B-4*.

2. Deploying SSL Certificate:

   - Deploying SSL certificate on Virtual Mobile Infrastructure server. (See *Deploying SSL Certificate on Virtual Mobile Infrastructure Server on page B-4*)
   - Deploying SSL certificate on Virtual Mobile Infrastructure secure access (See *Deploying SSL Certificate on Virtual Mobile Infrastructure Secure Access on page B-6*).

Generating Certificate Signing Request (CSR)

> **Note**
>
> If you already have a **Wildcard SSL Certificates**, skip this step, and proceed to the next step; *Deploying SSL Certificate on page B-4*.

> **Note**
>
> The steps to generate Certificate Signing Request (CSR) for Virtual Mobile Infrastructure server and secure access are same. However, you will need to deploy public SSL certificate on the server and secure access separately.

Procedure

1. Log on to Virtual Mobile Infrastructure server or secure access terminal (SSH) using account **tmvmi**, and then switch to root account after logging in using command "`su root`".

2. At the terminal, type the following command:

   ```
   openssl req -new -newkey rsa:2048 -nodes -keyout
   yourdomainname.key -out yourdomain.csr
   ```

   Replace `yourdomainname` with the domain name you are using. For example, if your domain name is `example.com`, you would type `example.key` and `example.csr`.

3. Provide the following information:

   - **Common Name**: The fully-qualified domain name, or URL, you are using.

     If you are requesting a Wildcard certificate, add an asterisk (*) to the left of the common name where you want the wildcard, for example *.example.com.

   - **Organization**: The legally-registered name for your business. If you are enrolling as an individual, enter the certificate requester's name.

   - **Organization Unit**: If applicable, enter the DBA (doing business as) name.

   - **City or Locality**: Name of the city where your organization is registered/located. Do not abbreviate.

   - **State or Province**: Name of the state or province where your organization is located. Do not abbreviate.

   - **Country**: The two-letter International Organization for Standardization (ISO) format country code for where your organization is legally registered.

   - **Passphrase**: If you do not want to enter a password for this SSL, you can leave this field blank. However, there might be additional risks.

4. After the process is completed, you can get the CSR and a key file in the current folder.

   Save the CSR file and the key file. The key file is required when deploying the certificate.

5. Send the CSR file to a public Certificate Authority (CA) for signing. After you send the CSR to a CA, they issue a server certificate.

Deploying SSL Certificate

After you have received the server certificate from the Certificate Authority (CA) or have a **Wildcard SSL Certificates**, you should install the certificate on the Virtual Mobile Infrastructure server and/or secure access.

Deploying SSL Certificate on Virtual Mobile Infrastructure Server

Virtual Mobile Infrastructure server uses Apache SSL HTTP server to manager SSL certificate.

Procedure

1. Log on to Virtual Mobile Infrastructure server terminal (SSH) using account **tmvmi**, and then switch to root account after logging in using command "`su root`".

2. Copy your SSL certificate files and the certificate bundle file to VMI server. For example, `/home/tmvmi/`, and unzip the certificate file. You can get certificate chain, public certificate.

Note

The CA may not provide certificate chain, and only provide root certificate and public certificate. You need to generate certificate chain using the following command:

```
cat public_certificate.crt root_certificate.crt
>servercert2to1.pem
```

3. Copy the certificate file at the correct location:
   - Copy the private key here: `/etc/pki/tls/private/`

     Note

     The private key is generated when you generate CSR file.

   - Copy the certificate file and certificate key chain here: `/etc/pki/tls/certs/`
4. Change configuration file `/etc/httpd/conf.d/wsgi-vmi.conf` by replacing corresponding file name with your real file name.
   - Use the following for certificate file:

     ```
     SSLCertificateFile /etc/pki/tls/certs/xxxx.crt
     ```

     ```
     SSLCertificateChainFile /etc/pki/tls/certs/xxxx.crt
     ```

     Note

     If your keychain is `pem` file, then it should be `SSLCertificateChainFile /etc/pki/tls/certs/servercert2to1.pem`

   - Use the following for the private key file:

     ```
     SSLCertificateKeyFile /etc/pki/tls/private/xxxx.key
     ```
5. Restart Apache service using the following command:

   ```
   service httpd restart
   ```

Deploying SSL Certificate on Virtual Mobile Infrastructure Secure Access

Procedure

1. Copy your SSL certificate file and the certificate bundle file to Virtual Mobile Infrastructure secure access, for example at `/home/tmvmi/`. You should already have a key file on the server from when you generated your certificate request. Copy the key file in the same folder as the SSL certificate file and bundle file.

   Note

   The certificate that deployed in secure access should be **p12** format. If your certificate is not **p12** file, follow step 3 and 4 to generate the certificate. If your certificate is **p12** file, skip to step 5 directly.

2. Log on to the secure access terminal by **tmvmi** account and then switch to root account by using command `su root`.

   You need to merger the server certificates from the CA into certificate keychain file in secure access, to generate the **p12** format certificate.

3. Use the following command to merge the three certificate files to certificate key chain:

   ```
   cat yourdomainname.crt public_certificate.crt
   root_certificate.crt > DefaultTempCert3to1.crt
   ```

   Note

   Replace `yourdomainname` with the domain name you are using. For example, if your domain name is `example.com`, you would type `example.crt`.

4. Generate the certificate p12 file using the following command:

   ```
   openssl pkcs12 -export -out TmmsDefaultTempCert.p12 -inkey
   xxxx.key -in DefaultTempCert3to1.crt -password pass:your_password
   ```

Note

You generated the key file when you generated the CSR file.

5. Copy the certificate file to folder `/vmi/gateway/` using the following command:

```
cp TmmsDefaultTempCert.p12 /vmi/gateway/
TmmsDefaultTempCert.p12
```

6. Skip this step if your certificate does not have a password. If you have password for your certificate, use the following command to generate key:

```
/vmi/gateway/cs -e *****
```

Note

Replace ***** with your password for the certificate.

7. Change configuration file `/vmi/gateway/configuration.json`, replace corresponding file name with your real file name, and replace the key with your key using the following commands:

```
"ssl_cert_file": "****.p12"
```

```
"ssl_key_password": "****"
```

Note

If you do not have a password for the certificate file, replace **** with blank.

8. Restart secure access for your new certificate to take effect, using the following command:

```
service vmigateway restart
```

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: APEM68495/180927