

TREND MICRO[™] **Virtual Mobile Infrastructure** Installation and Deployment Guide

Centrally-managed workspace for mobile users



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

http://docs.trendmicro.com/en-us/home.aspx

Trend Micro, the Trend Micro t-ball logo, InterScan, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

© 2019. Trend Micro Incorporated. All Rights Reserved.

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 <u>docs@trendmicro.com</u>.

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

Preface	v
Audience	. vi
Virtual Mobile Infrastructure Documentation	. vi
Document Conventions	vii

Chapter 1: Introducing Virtual Mobile Infrastructure

About Virtual Mobile Infrastructure	1-2
Why Use Virtual Mobile Infrastructure	1-2
System Requirements	1-3
Architecture of Virtual Mobile Infrastructure	
Single Server Installation Model Multiple Server Installation Model	
Virtual Mobile Infrastructure High Availability	
Components of Virtual Mobile Infrastructure	1-7
Why Use Secure Access	1-8

Chapter 2: Installing on Bare Metal Servers

Installing Virtual Mobile Infrastructure Server on a Bare Metal Server	
	2-2
Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal	
Server	-13

Chapter 3: Installing on VMware vSphere ESXi Hypervisor

Installing Virtual Mobile Infrastructure Server	. 3-2
Step 1: Creating a Virtual Machine	3-2
Step 2: Installing Virtual Mobile Infrastructure on VMware ESXi	
	3-13

Installing Virtual Mobile Infrastructure Secure Access	3-14
Step 1: Creating a Virtual Machine	3-14
Step 2: Installing Virtual Mobile Infrastructure Secure Access on	
VMware ESXi	3-25

Chapter 4: Installing on VMware Workstation

Installing Virtual Mobile Infrastructure Server	4-2
Step 1: Creating a Virtual Machine	4-2
Step 2: Installing Virtual Mobile Infrastructure on VMware	
Workstation	4-9
Installing Virtual Mobile Infrastructure Secure Access	4-9
Step 1: Creating a Virtual Machine	4-9
Step 2: Installing Virtual Mobile Infrastructure Secure Access on	
VMware Workstation	4-15

Chapter 5: Installing on Microsoft Hyper-V

Installing Virtual Mobile Infrastructure Server	. 5-2
Step 1: Creating a Virtual Machine	. 5-2
Step 2: Installing Virtual Mobile Infrastructure Server on Microso	
Hyper-V	5-5
Installing Virtual Mobile Infrastructure Secure Access	. 5-5
Step 1: Creating a Virtual Machine	. 5-5
Step 2: Installing Virtual Mobile Infrastructure Secure Access on	
Microsoft Hyper-V	. 5-9

Chapter 6: Installing on Citrix XenServer

Installing Virtual Mobile Infrastructure Server	6-2
Creating a Virtual Machine and Installing Virtual Mobile	
Infrastructure Server	6-2
Installing Virtual Mobile Infrastructure Secure Access	6-5
Creating a Virtual Machine and Installing Virtual Mobile	
Infrastructure Secure Access	6-6

Chapter 7: Post-Installation Configuration

Accessing Virtual Mobile Infrastructure Administration Web Console
Activating Your Product
Configuration Tasks 7-4
Changing Administrator Account Password 7-5
Configuring LDAP Settings (Optional) 7-6
Configuring Mobile Client Settings
Configuring Microsoft Exchange Server and Office 365 Settings
(Optional)
Configuring Network Settings
Configuring External Storage
Configuring Email Notifications 7-12
Configuring Syslog (System Logs) 7-14
Managing Groups and Users 7-14
Importing Groups or Users from LDAP 7-15
Creating a User Account Locally 7-15
Deploying Virtual Mobile Infrastructure to Mobile Devices
Installing Android Client for Virtual Mobile Infrastructure 7-17
Installing iOS Client for Virtual Mobile Infrastructure

Appendix A: Network Port Configurations

Network Port Configuration for Virtual Mobile Infrastructure Server	A-2
Network Port Configuration for Virtual Mobile Infrastructure Secure	
Access	A-4

Appendix B: Public SSL Certificate Deployment

Managing Public SSL Certificate	B-2
Generating Certificate Signing Request (CSR)	B-2
Deploying SSL Certificate	B-4





Preface

Preface

Welcome to the Trend MicroTMVirtual Mobile InfrastructureTM 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 on page vi
- Virtual Mobile Infrastructure Documentation on page vi
- Document Conventions on page vii

Audience

vi

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 (<u>http://www.docs.trendmicro.com/</u>) 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
Г р Тір	Recommendations or suggestions

CONVENTION	DESCRIPTION
	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options





1 - 1

Chapter 1

Introducing Virtual Mobile Infrastructure

This chapter assists administrators in planning the server components for Trend MicroTMVirtual Mobile InfrastructureTM.

This chapter contains the following sections:

- About Virtual Mobile Infrastructure on page 1-2
- Why Use Virtual Mobile Infrastructure on page 1-2
- System Requirements on page 1-3
- Architecture of Virtual Mobile Infrastructure on page 1-4
- Components of Virtual Mobile Infrastructure on page 1-7

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 pro	ovides 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

1-4

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

1-5

🔏 Note

Trend Micro strongly recommends deploying Secure Access in your environment to enable mobile clients to access Virtual Mobile Infrastructure Server via Internet. See *W hy Use Secure Access on page 1-8* for more information.

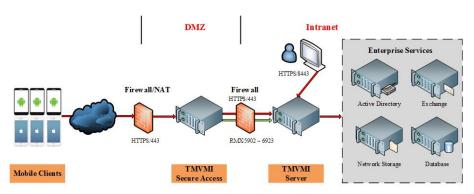


FIGURE 1-1. Trend Micro Virtual Mobile Infrastructure Single Server Installation Model

Multiple Server Installation Model

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

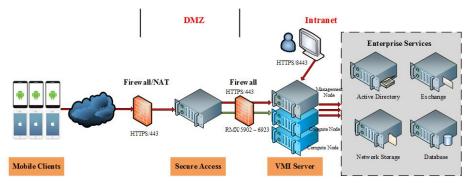


FIGURE 1-2. Trend Micro Virtual Mobile Infrastructure Multiple Server Installation Model

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.

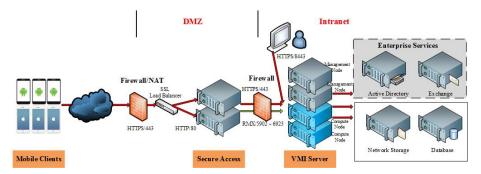


FIGURE 1-3. Trend Micro Virtual Mobile Infrastructure High Availability architecture

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.	Required
	 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. 	
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 <i>Why Use Secure Access on</i> <i>page 1-8</i> 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.

1 - 9

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.



2-1

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 on page 2-2
- Installing Virtual Mobile Infrastructure Secure Access on a Bare Metal Server on page 2-13

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

2-2

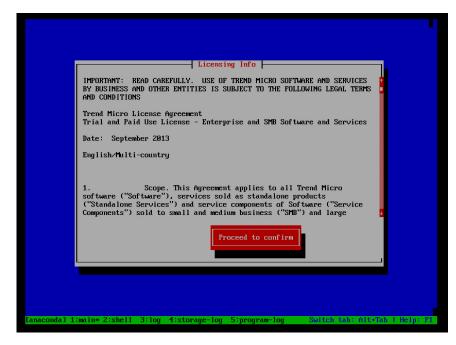
- 1. Power on the Bare Metal server where you want to install Virtual Mobile Infrastructure.
- 2. Insert the installation DVD into the DVD drive, and reboot the server.

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.

2-5

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) \tilde{a} ~~\, and default password admin to log in.

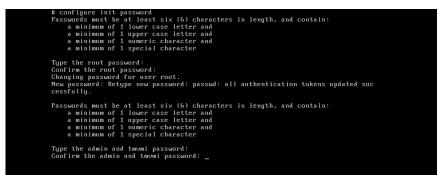
- 7. Type \rightarrow bå, and then type <u>enable</u>, to enter the privilege mode and start the configuration steps.
- 8. If you need help during configuration, type configure init help and press **Enter** to check the configuration help.

```
After installation, please execute following command to configure your system:
1. To set root and admin account password, type command:
        configure init password

    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. UMI 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.



- **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.	 To install a Management and Compute Node, and add an external database information: Type configure init server 1 db <db address="" ip=""> <db name=""> <db username> [db port] <db type="">, and then press Enter.</db></db </db></db>
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 .	 Note db type can be "mysql" or "oracle". For example, configure init server 1 db 10.206.139.20 vmidb tmvmi 3306 mysql. Type the password for the database you want to use for Virtual Mobile Infrastructure when prompted.
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 setup multiple servers	a. Do one of the following to install the first server:
and a new database, install at least two Virtual Mobile Infrastructure	 To install the first server as Management and Compute Node:
servers.	• Type configure init server 1 new.
Note When installing multiple servers, the first server must be a Management and Compute Node or a Management Node.	• To install first server as Management Node:
	• Type configure init server 3 new.
	 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 <i>Configuring</i> <i>External Storage on page 7-11</i> for the procedure.
	d. Do one of the following to install subsequent
Note	servers:
If you install multiple servers,	 To install subsequent server as Management and Compute Node:
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.	• Type configure init server 1 vmi <first address="" ip="" server's="">.</first>
	 To install subsequent server as Compute Node:
	• Type configure init server 2 vmi
	<pre><first address="" ip="" server's="">. • To install subsequent server as Management Node:</first></pre>
	• Type configure init server 3 vmi <first address="" ip="" server's="">.</first>
	e. Repeat <i>step 9 on page 2-6</i> (configuring password), <i>step 10 on page 2-7</i> (configuring network) and then steps <i>a on page 2-9</i> to <i>c on page 2-9</i> of this procedure to install more servers, if required.

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

To setup a multiple server, and configure an existing external database, you need to install at least two Virtual Mobile Infrastructure	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<br="">address> <db name=""> <db username=""> [db port] <db type="">, press Enter, and then type the database password when prompted.</db></db></db></db>
servers.		For example, configure init server 3 db 10.206.139.20 vmidb tmvmi 3306 mysql.
Important		To install as Management Node:
See the Notes following this table.		Type configure init server 3 db <db ip<br="">address> <db name=""> <db username=""> [db port] <db type=""> , press Enter, and then type the database password when prompted.</db></db></db></db>
		For example, configure init server 1 db 10.206.139.20 vmidb tmvmi 3306 mysql.
	b.	Follow <i>step 12 on page 2-11</i> to <i>step 15 on page 2-13</i> of this topic (configuring timezone, hostname, keyboard), and finish first server installation.
	C.	Configure external storage. See <i>Configuring External Storage on page 7-11</i> 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>.</first
		To install subsequent server as Compute Node:
		Type configure init server 2 vmi <first address="" ip="" server's="">.</first>
		To install as Management Node:
		Type configure init server 3 vmi <first server's IP address>.</first
		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

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

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.

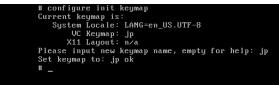


13. To change the default hostname (localhost), type configure init hostname <host name>. For example, configure init hostname vmi.



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.

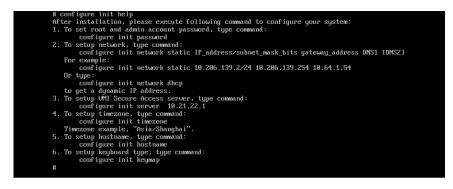
Confirm to install UMI Secur	Licensing Info	
Accept		e ject

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

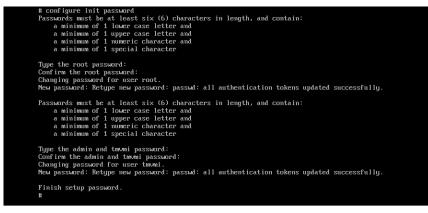
The installation begins. The installation process may take about 10 minutes or more to complete. Once the installation process completes, the system reboots to allow configuration and displays the following screen.



- 6. Use username (localhost login) \tilde{a} ~~\, and default password admin to log in.
- 7. Type →bå, and then type enable, 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.



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



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

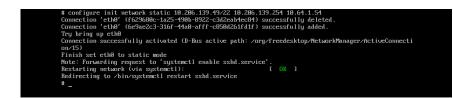
2-18

- 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

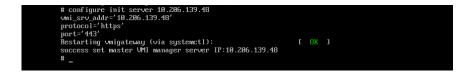
For example, configure init network static 10.206.139.48/22 10.206.139.254 10.64.1.54.

🔏 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.



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



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

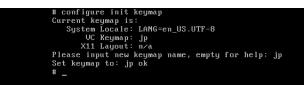
configure init timezone
Current timezone is:
Local time: Thu 2018-12-27 17:00:44 CST
Universal time: Thu 2018-12-27 09:00:44 UTC
RTC time: Thu 2018-12-27 09:00:44
Time zone: Asia/Shanghai (CST, +0800)
NTP enabled: yes
NTP synchronized: yes
RTC in local TZ: no
DST active: n/a
Please input new timezone 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 on page 3-2
- Installing Virtual Mobile Infrastructure Secure Access on page 3-14

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

3-2

- 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**.

Configuration Select the configuration fi		ual Machine Version: a
Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Configuration Typical Create a new virtual machine with the most common devices and configuration of C Custom Create a virtual machine with additional devices or specific configuration options.	
Help	< Back Next >	Cancel

FIGURE 3-1. Select Configuration

The Name and Location screen appears.

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

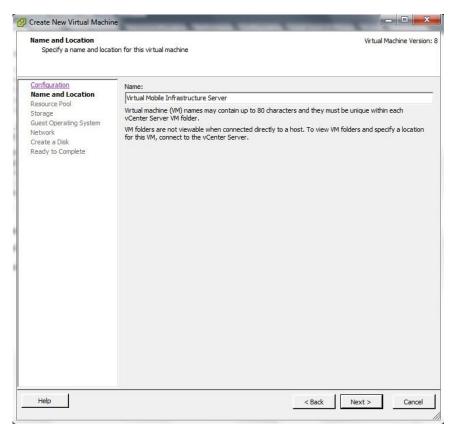


FIGURE 3-2. Type a name for the new virtual machine

The Resource Pool screen appears.



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**.

Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Disk Ready to Complete	Resource Pool Within which resource p	ool do you want to run this virtual machine?	Virtual Machine Version
	Name and Location Resource Pool Storage Guest Operating System Network Create a Disk	Resource pools allow hierarchical management of computing resources we machines and child pools share the resources of their parent pool.	

FIGURE 3-3. Select a resource pool

The **Storage** screen appears.

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

Storage Select a destination stora	age for the virtual machine	e files				Virtual Mach	ine Version:
Configuration	Select a destination st	torage for the virtua	I machine files:				
<u>Name and Location</u> Resource Pool	Name	Drive Type	Capacity	Provisioned	Free	Туре	Thin Pro
Storage	2000G	Non-SSD	1.82 TB	1.17 TB	1.07 TB	VMFS5	Suppor
Guest Operating System Network Create a Disk Ready to Complete	datastore1	Non-SSD	1.09 TB	1.33 TB	186.71 GB	VMFS5	Suppor
	Disable Storage	DRS for this virtual n	III nachine				
	1	DRS for this virtual n	nachine	ovisioned	Free	Туре	Thin Pro

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.

Suest Operating System Specify the guest operating	system to use with this virtual machine	Virtual Machine Versior
Configuration lame and Location lesource Pool Suest Operating System letwork Create a Disk teady to Complete	Guest Operating System: C Windows C Linux Other Version: Other Linux (64-bit) Identifying the guest operating system here allows the wize the operating system installation.	ard to provide the appropriate defaults for

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

3-7

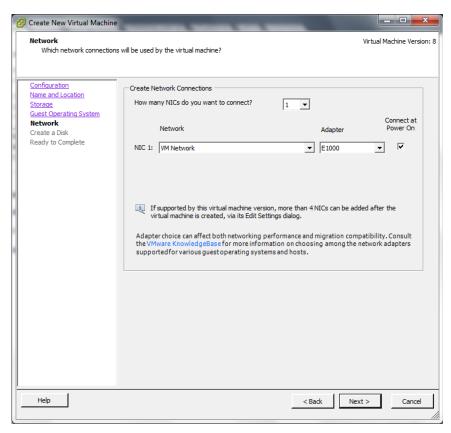


FIGURE 3-6. Create network connections

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.

Create New Virtual Machir Create a Disk Specify the virtual disk si	ze and provisioning policy		Virtual M	achine Version:
Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Disk Ready to Complete	Datastore: Available space (GB): Virtual disk size: Thick Provision Lazy i Thick Provision Eager Thin Provision			
Help		< Back	Next >	Cancel

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**.

Click Finish to start a ta	isk that will create the new virtual mac	Virtual Mach	ine Ver
Configuration Name and Location	Settings for the new virtual mac	hine: Virtual Mobile Infrastructure	
<u>Storage</u> Guest Operating System	Host/Cluster:	localhost.	
Network	Resource Pool:	Temp Environment	
Create a Disk	Datastore:	2000G	
Ready to Complete	Guest OS:	Other 2.6.x Linux (64-bit)	
	NICs:	1	
	NIC 1 Network:	VM Network	
	NIC 1 Type:	E1000	
	Disk provisioning:	Thick Provision Lazy Zeroed	
	Virtual Disk Size:	50 GB	
	The state of the s	tings before completion	
	Edit the virtual machine set		

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.

Virtual Mobile Infrastructure Ser	ver - Virtual Machine Propertie	is	- 🗆 X
Hardware Options Resources Pro	files		
Show All Devices	Add Remove	Memory Config 1011 GB	Memory Size: 8 - GB -
Hardware	Summary	512 GB	· , _ , _
🌃 Memory (adding)	8192 MB		Maximum recommended for this guest OS: 1011 GB.
🔲 CPUs (adding)	1	256 GB	Maximum recommended for best
📃 Video card (adding)	Video card	128 GB	 performance: 130976 MB.
VMCI device (adding)	Restricted	64 GB	Default recommended for this
New CD/DVD (adding) New Floppy (adding)	Client Device Client Device	32 GB-	guest OS: 384 MB.
New Floppy (adding) New SCSI Controller (add			Minimum recommended for this quest OS: 32 MB.
New NIC (adding)	VM Network	16 GB-	guest 03. 52 Mb.
New Hard Disk (adding)	Virtual Disk	8 GB -	
		4 GB -	
		2 GB	
		1 GB	
		512 MB	
		256 MB	
		128 MB	
		64 MB	
		32 MB 🚽	
		16 MB	
		8 МВ –	
		4 MB	
Help			Finish Cancel

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.

🕝 Virtual Mobile Infrastructure Ser	ver - Virtual Machine Properties	;	_		\times
Hardware Options Resources Prof	les				
Show All Devices	Add Remove	Number of virtual sockets:	2	•	
Hardware	Summary	Number of cores per socket:	4	•	
Memory (adding)	8192 MB	Total number of cores:	8		
CPUs (adding)	8	rotar hander of corest	°.		
 Video card (adding) VHCI device (adding) New CD/DVD (adding) New Floppy (adding) New SCSI Controller (add New NIC (adding) New Hard Disk (adding) 	Video card Restricted Client Device LSI Logic Parallel VM Network Virtual Disk	Changing the number of virtu OS is installed might make you unstable. The virtual CPU configuration might violate the license of th	ur virtual mac	hine	
Help			Finish	Cancel	

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.

Virtual Mobilt Infrastructure S	erver - virtuar machine Properties	
ardware Options Resources		Virtual Machine Version:
Show All Devices	Add Remove	Device Status
Hardware	Summary	Connect at power on
 Memory (edited) CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 (edited) Hard disk 1 Floppy drive 1 Network adapter 1 	8192 MB 8 Video card Restricted LST Logic Parallel [3000G] VHIISO/T Virtual Disk Client Device VM Network	Device Type Client Device Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar. Host Device Jatastore ISO File [3000G] VMIISO/T Browse Mode G Passtbrough IDE (recommended) C Emulate IDE Virtual Device Node G IDE (1:0) CD/DVD drive 1

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 VMnare 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**.

Configuration Select the configuration f	the virtual machine Virtual Machine	• Version:
Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Configuration Typical Create a new virtual machine with the most common devices and configuration options. C Custom Create a virtual machine with additional devices or specific configuration options.	
Help	< Back Next > 0	Cancel

FIGURE 3-12. Select Configuration

The Name and Location screen appears.

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

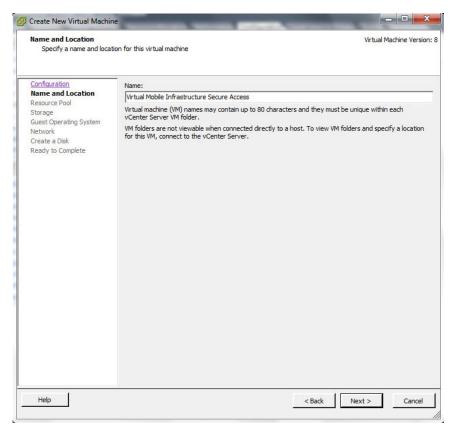


FIGURE 3-13. The Resource Pool screen appears.

The **Resource Pool** screen appears.



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**.

Resource Pool Within which resource p	ool do you want to run this virtual machine?	Virtual Machine Version
Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Disk Ready to Complete	Select the resource pool within which you wish to run this virtual machine Resource pools allow hierarchical management of computing resources of machines and child pools share the resources of their parent pool.	
Help	< Back	Next > Cancel

FIGURE 3-14. Select a resource pool

The **Storage** screen appears.

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

Storage Select a destination stora	age for the virtual machine	e files				Virtual Mach	ine Version:
Configuration	Select a destination st	torage for the virtual	machine files:				
<u>Name and Location</u> Resource Pool	Name	Drive Type	Capacity	Provisioned	Free	Туре	Thin Pro
Storage	2000G	Non-SSD	1.82 TB	1.17 TB	1.07 TB	VMFS5	Support
Guest Operating System Network Create a Disk Ready to Complete	datastore1	Non-55D	1.09 TB	1.33 TB	186.71 GB	VMF55	Support
	Disable Storage	DRS for this virtual m	III. Iachine				,
	1	DRS for this virtual m		visioned	Free	Туре	Thin Pro
	Disable Storage I Select a datastore:		achine	visioned	Free	Туре	

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.

anfiguration ame and Location asource Pool orade uest Operating System twork reate a Disk eady to Complete	Guest Operating System: C Windows Linux Other Version: Other Linux (64-bit) Identifying the guest operating system here allows the wize the operating system installation.	rd to provide the appropriate defaults for

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

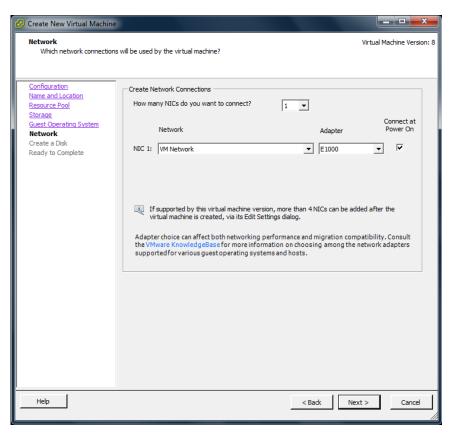


FIGURE 3-17. Create Network Connections

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.

Configuration Datastore: datastore 1 Resource Pool Available space (GB): 186.7 Storace Virtual disk size: 30 3 GB * Network Image: Complete Thick Provision Lazy Zeroed C Thick Provision Eager Zeroed C C Thin Provision Heroid Store Service Heroid Service Units of the Service Servi	Create a Disk Specify the virtual disk size	ze and provisioning policy		Virtual Machine Version:
	Name and Location Resource Pool Storage Guest Operating System Network Create a Disk	Available space (GB): Virtual disk size: Thick Provision Lazy Z Thick Provision Eager 	186.7 30 - ↓ GB -	

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**.

Ready to Complete Click Finish to start a tas	k that will create the new virtual mac	Virtual Machine Versio
Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Disk Ready to Complete	Settings for the new virtual mac Name: Host/Cluster: Resource Pool: Datastore: Guest OS: NICS: NIC1 Network: Disk provisioning: Virtual Disk Size:	hine: Virtual Mobile Infrastructure Secure Access localhost. Temp Environment datastoreI Other Linux (64-bit) 1 VM Network Thick Provision Lazy Zeroed 30 GB
	 Edit the virtual machine sett Creation of the virtual mac system. Install a guest OS 	ings before completion hine (VM) does not include automatic installation of the guest operating on the VM after creating the VM.

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.

ardware Options Resources			
Show All Devices	Add Remove	Memory Config	guration
Show Air Devices	Remove	1011 GB	Memory Size: 4 - GB -
Hardware	Summary	512 GB	
Memory (adding)	4096 MB	256 GB	Maximum recommended for this quest OS: 1011 GB.
CPUs (adding)	1	256 GB	Maximum recommended for best
Video card (adding)	Video card	128 GB	 performance: 65492 MB.
VMCI device (adding)	Restricted	64 GB	Default recommended for this
New CD/DVD (adding)	Client Device	32 GB-	 guest OS: 384 MB.
New Floppy (adding) New SCSI Controller (add	Client Device		Minimum recommended for this
New SCSI Controller (add New NIC (adding)	LSI Logic Parallel VM Network	16 GB	 guest OS: 32 MB.
New Hard Disk (adding)	Virtual Disk	8 GB	
- HEW Hard Disk (adding)	THEORY DISK	4 GB	
		2 GB -	
		1 GB -	
		512 MB	
		256 MB	
		128 MB	
		64 MB	
		22.140	
		32 MB 🔫	
		16 MB	
		8 MB	
		4 MB	
		- GH F	
Help			Finish Cancel



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**.

rdware Options Resources Show All Devices	Add Remove	Number of virtual sockets:	2 •
ardware -	Summary	Number of cores per socket:	2 -
Memory (adding) Video card (adding) Video card (adding) VHCI device (adding) New C/DVD (adding) New Floppy (adding) New SCSI Controller (add New NIC (adding) New Hard Disk (adding)	4096 MB 4 Video card Restricted Client Device Client Device LSI Logic Parallel VM Network Virtual Disk	Total number of cores: Changing the number of virtu. OS is installed might make you unstable. The virtual CPU configuration might violate the license of th	ur virtual machine

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**.

ardware Options Resources			
Show All Devices	Add Remove	Device Status	
Hardware	Summary	Connect at power on	
Memory (adding) CPUs (adding) Video card (adding) VMCI device (adding) New CD/DVD (adding)	4096 MB 4 Video card Restricted [datastore1] VMIIS	Device Type Clent Device Note: To connect this device, you must power on the writial machine and then click the Connect CD/DVD button in the toobar.	
New Floppy (adding) New SCSI Controller (add New NIC (adding) New Hard Disk (adding)	Client Device LSI Logic Parallel VM Network Virtual Disk	Host Device Vice Vice	
		[datastore 1] VMIISO/ Browse Mode (* (* Passthrough IDE (recommended) (* Emulate IDE Virtual Device Node (* (* IDE (1:0)	
Help		FinishCancel	

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 on page 4-2
- Installing Virtual Mobile Infrastructure Secure Access on page 4-9

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 VMnare 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.

4-2

- 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

lew Virtual Machine Wizard		-
Select a Guest Operating Which operating system	System will be installed on this virtual machine?	
Guest operating system		
Microsoft Windows		
Linux		
Novell NetWare		
Solaris		
VMware ESX		
Other		
Version		
Other Linux 2.6.x kernel 64-bit	1	•
·		
Usla		Connel
Help	< Back Next >	Cancel

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.

New Virtual Machine Wizard
Specify Disk Capacity How large do you want this disk to be?
Maximum disk size (GB): 50
Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
 Store virtual disk as a single file Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help < Back Next > Cancel

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**.

Device Memory	Summary 8 GB	Memory Specify the amount of memory allocate machine. The memory size must be a n	
Dracasara	Add Hardware Wizard Network Adapter Type What type of network adapter do	—	
Printer Display	Network connection Bridged: Connected directly to the ph Replicate physical network conne NAT: Used to share the host's IP add Host-only: A private network shared Custom: Specific virtual network VMnet0	ction state	nended memory ng may s size.) nemory
-	Device status Connect at power on Add Remove	< Back Finish Cancel	

FIGURE 4-3. Configure network adapter type

4-6

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.

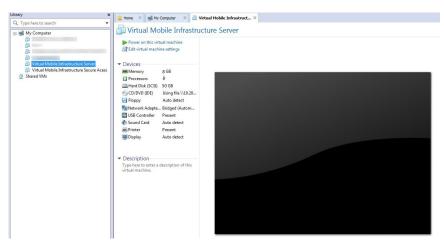


FIGURE 4-4. Virtual machines in VMware Workstation

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**.

ardware Options		
Device Memory Processors ardrd Disk (SCSI) D/DVD (IDE) Floppy USB Controller Sound Card Printer Display	Summary 8 GB 8 50 GB Auto detect Auto detect Present Auto detect Present Auto detect Present Auto detect Auto detect Auto detect Resent Auto detect Resent Auto detect	Device status Connected Connection Use physical drive: Auto detect Consection Consection Connection Connection

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.



4-10

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

New Virtual Machine Wizard	×
Select a Guest Operating System Which operating system will be installed on this virtual machine?	
Guest operating system	
Microsoft Windows	
 Linux 	
Novell NetWare	
Solaris	
O VMware ESX	
Other	
Version	
Other Linux 2.6.x kernel 64-bit	-
Help < Back Next > Ca	ncel

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.

New Virtual Machine Wizard
Specify Disk Capacity How large do you want this disk to be?
Maximum disk size (GB): 30
Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
 Store virtual disk as a single file Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help Cancel

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.

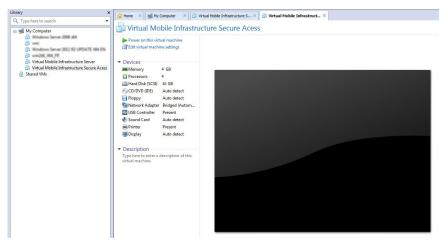


FIGURE 4-8. Virtual machines in VMware Workstation

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.

Device Memory Processors Hard Disk (SCSI)	Summary 4 GB 4 30 GB	Device status Connected Connect at power on Connection
Clovb (DE) Floppy Flop	Auto detect Auto detect Bridged (Automatic) Present Auto detect Present Auto detect	Use physical drive: Auto detect v Use ISO image file: Browse Advanced
	Add Remove	

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 on page 5-2
- Installing Virtual Mobile Infrastructure Secure Access on page 5-5

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**.

New Virtual Machine Wiz	ard tual Hard Disk	>
Before You Begin Specify Name and Location Assign Memory	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.	
Configure Networking Connect Virtual Hard Disk Installation Options Summary	Name: Virtual Mobile Infrastructure Server.vhd Location: C:\VirtualDisk\Virtual Mobile Infrastructure Server\ Browse Size: 50 GB (Maximum: 2040 GB)	
	C Use an existing virtual hard disk Location: C: \Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse	
	C Attach a virtual hard disk later	
	< Previous Next > Finish Cancel	

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.

/irtua	I Mobile Infrastructure Server	4 » Q			_
+	ardware Add Hardware BIOS Boot from CD	Select the controller and local Controller:	tion on the cont	roller to attach the C Location:	D/DVD drive.
	Memory 8192 MB	IDE Controller 1	•	0 (in use)	•
	8 Virtual processor	Specify the media to use w	ith your virtual (CD/DVD drive.	
	IDE Controller 0 Hard Drive Virtual Mobile Infrastructure S	Image file:			
9 🔳	IDE Controller 1	C:\TMVMI-			Browse
0	TMVMI- SCSI Controller Network Adapter External Swtich	C Physical CD/DVD drive:			
1	COM 1 None COM 2	To remove the virtual CD/DVI	D drive from this	s virtual machine, dick	
E	None Diskette Drive				Remove
1 5	None lanagement				
I	Name Virtual Mobile Infrastructure Server				
20	Integration Services All services offered				
	Snapshot File Location C:\VirtualDisk\Virtual Mobile Infrast				
Ĩ	Automatic Start Action Restart if previously running				
ē	Automatic Stop Action Save				

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.

 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.
- Start Microsoft Hyper-V. Click File > New > Virtual Machine from the menu. The New Virtual Machine Wizard screen appears.
- On the Before You Begin screen, click Next.
 The Specify Name and Location screen appears.
- 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**.

捷 New Virtual Machine Wiza	ard	×
Specify Nam	ne and Location	
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easilentify this virtual machine, such as the name of the guest operating system or workload. Name: Virtual Mobile Infrastructure Secure Access You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server. I✓ Store the virtual machine in a different location Location: C:\VirtualDisk\ Browse If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.	ily
	< Previous Next > Finish Cancel	

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.

Settings for Virtual Mobile Inf		a			
Hardware Add Hardware BIOS Boot from CD	Select the	e controller and locatio	n on the cont	roller to attach the CD/L Location:	DVD drive,
Memory 4096 MB Processor 4 Virtual processor DE Controller 0 Hard Drive Virtual Mobile Infrastru IDE Controller 1	C Nor © Ima	/ the media to use with ne	vour virtual	0 (in use) CD/DVD drive.	•
DVD Drive THVMISA-3.0-1002 SCIS Controller Network Adapter External Switch None COM 1 None COM 2 None Diskette Drive None Adapter External Switch COM 1 None COM 2 None None Adapter External Switch Com 2 None None Scienter Drive None	C Phy Driv	rsical CD/DVD drive:	drive from this	s virtual machine, dick Re	Browse
Name Virtual Mobile Infrastructur Integration Services All services offered Snapshot File Location C: (VirtualDisk/Virtual Mobile Automatic Start Action Restart if previously runnin	: Inf				

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 on page 6-2
- Installing Virtual Mobile Infrastructure Secure Access on page 6-5

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



The procedure is based on XenServer 7.4.

Procedure

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

Home Search Home repladers of the serve you want to add end your use login credentials for that serve. User login credentials User name: root Password: Laceter Password	:h	🔍 🔇 XenCenter			
Industry leading, open source platform for cloud, server and desktop virtualization	A XenCenter	Home Search			
Industry leading, open source platform for cloud, server and desktop virtualization			Citrix YonSo	rvor	
Add New Server Inter the host name or B address of the server you want to add Server: User login credentials for that server. User login credentials User name: root Password: erver: users center referings					irtualization
Password:			Add New Server Infort the host name or IP address of the server, you want to add Server:	A HASE port	TRY Desktop
Password: Center			User name: root	enver users	
Add Cancel r offerings			Password: ••••••		
Add Cancel				er offerings	
			Add Cance		

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.

🕉 New VM				- • >
Select a VM tem	plate			0
Template	Search		Q	
Name	Name	Category	^	
nstallation Media	🎝 Legacy Windows	Windows	-	
Home Server	Asianux Server 4 (64-bit)	Asianux		
CPU & Memory	TentOS 5 (32-bit)	CentOS		
Storage	TentOS 5 (64-bit)	CentOS		
Networking	CentOS 6 (32-bit)	CentOS		
Finish	😵 CentOS 6 (64-bit)	CentOS		
	🐼 CentOS 7	CentOS		
	CoreOS	CoreOS		
	Debian Jessie 8.0	Debian		
	Debian Squeeze 6.0 (32-bit)	Debian		
	Debian Squeeze 6.0 (64-bit)	Debian		
	Debian Stretch 9.0	Debian		
		D 11	¥	
CITRIX"	Copy host BIOS strings to VM			
			< Previous	Next > Cancel

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

6-6

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

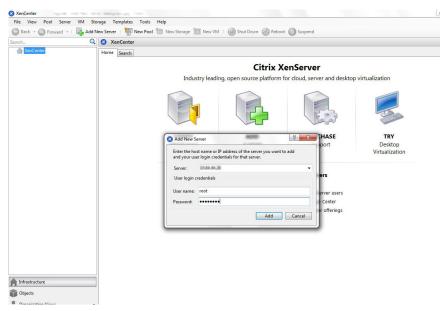


FIGURE 6-3. Add New Server dialog box

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.

😣 New VM				- 0	×
Select a VM template					8
Template	Search		Q		
Name Installation Media Home Server CPU & Memory Storage Networking Finish	Name Legacy Windows Asianux Server 4 (64-bit) CentOS 5 (32-bit) CentOS 5 (64-bit) CentOS 6 (64-bit) CentOS 6 (64-bit) CentOS 7 CoreOS Debian Jessie 8.0 Debian Squeeze 6.0 (32-bit) Debian Squeeze 6.0 (64-bit) Debian Stretch 9.0	Category Windows Asianux CentOS CentOS CentOS CentOS CentOS Debian Debian Debian Debian			
CITRIX	Copy host BIOS strings to VM	<u> </u>			
			< Previous Ne	xt > Canc	el

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.

6-8

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 on page 7-2
- Activating Your Product on page 7-3
- Changing Administrator Account Password on page 7-5
- Configuring LDAP Settings (Optional) on page 7-6
- Configuring Mobile Client Settings on page 7-7
- Configuring Microsoft Exchange Server and Office 365 Settings (Optional) on page 7-9
- Configuring Network Settings on page 7-10
- Configuring External Storage on page 7-11
- Configuring Email Notifications on page 7-12
- Configuring Syslog (System Logs) on page 7-14
- Managing Groups and Users on page 7-14
- Deploying Virtual Mobile Infrastructure to Mobile Devices on page 7-16

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

DITEND Virtual Mobile Infras	tructure	
	🔁 Log On	
	User Name:	
	Password:	
	Log On	
Copyright © 2018 Trend Micro Incorporated. All rights reserved.	Legal Policies & Privacy Contact us TrendMicro.com	

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



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.

Virtual Mobile Infrastructure
New Activation Code
Product name:Trend Micro Virtual Mobile Infrastructure
New activation code:
Save

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 <i>Changing Administrator Account Password on page</i> 7-5 for the detailed procedure.
(Optional) Configure LDAP settings.	Supports integration with Microsoft Active Directory and OpenLDAP to manager users and groups.
	See <i>Configuring LDAP Settings (Optional) on page</i> 7-6 for the detailed procedure.
(Optional) Configure mobile	User settings for mobile client and users.
client settings.	See <i>Configuring Mobile Client Settings on page</i> 7-7 for the detailed procedure.

7-5

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 <i>Configuring Network Settings on page 7-10</i> for the detailed procedure.	
(Optional) Configure external storage.	External storage to save user data.	
	(Required, if multiple Virtual Mobile Infrastructure servers are deployed.)	
	See <i>Configuring External Storage on page 7-11</i> for the detailed procedure.	
(Optional) Configure syslog	System log server settings to save server debug logs.	
settings.	See Configuring Syslog (System Logs) on page 7-14 for the detailed procedure.	
(Optional) Configure email	SMTP server settings to send email notification to users.	
notification settings.	See <i>Configuring Email Notifications on page 7-12</i> for the detailed procedure.	

Changing Administrator Account Password

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



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.
- 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

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



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



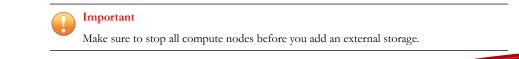
The bypass setting only takes effect for the user workspaces, and from the next time users sign in.

- **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.



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.



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.



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.



A-1

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 on page A-2
- Network Port Configuration for Virtual Mobile Infrastructure Secure Access on page A-4

A-2

Network Port Configuration for Virtual Mobile Infrastructure Server

Configure the following network ports for Virtual Mobile Infrastructure server:

Component	Network Ports	DETAILS	Require d or Optional	Directio N
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	Require d or Optional	Directio N
SMTP server	TCP port 25	Used to access email server.	Optional	Outbound
		If you are not using SMTP server to send emails, this port is not required.		
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.	Required, if iOS TMVMI client is customize d	Outbound
		The hostname of Apple Push Notification Service is gateway.push.apple.co m.		
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.	Optional	Outbound
		However, if the mobile devices are on a 3G network, you do not need to configure this port.		

A-4

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 on page B-2
- Generating Certificate Signing Request (CSR) on page B-2
- Deploying SSL Certificate on Virtual Mobile Infrastructure Server on page B-4
- Deploying SSL Certificate on Virtual Mobile Infrastructure Secure Access on page B-6

B-1

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*).



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.

B-2

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.

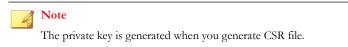
B-4



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/



- 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



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.



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
```



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:

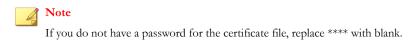
/vmi/gateway/cs -e *****

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": "****"



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



Item Code: APEM68495/180927