

# TREND MICRO<sup>®</sup> Safe Mobile Workforce 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 products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Trend Micro, the Trend Micro logo and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2014 Trend Micro Incorporated. All rights reserved.

Release Date: March 2014

Document Part No.: MWEM16258/131227

The user documentation for Trend Micro<sup>TM</sup> Safe Mobile Workforce is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

# Contents

#### Preface

Audience	iv
Safe Mobile Workforce Documentation	iv
Document Conventions	iv

## Chapter 1: Introducing Safe Mobile Workforce

About Safe Mobile Workforce	1-2
Why Use Safe Mobile Workforce	1-2
System Requirements	1-4
Architecture of Safe Mobile Workforce Single Server Installation Model Multiple Server Installation Model	1-5 1-5 1-6
Components of Safe Mobile Workforce	1-7

## **Chapter 2: Installing on Bare Metal Servers**

Installing Safe Mobile Workforce Server	
Installing Safe Mobile Workforce Secure	Access 2-3

#### Chapter 3: Installing on VMware vSphere ESXi Hypervisor

Installing Safe Mobile Workforce Server	
Installing Safe Mobile Workforce Secure	Access

#### Chapter 4: Installing Safe Mobile Workforce on VMware Workstation

Installing Safe Mobile Workforce Server	
Installing Safe Mobile Workforce Secure	Access 4-8

#### Chapter 5: Installing Safe Mobile Workforce on Microsoft Hyper-V

Installing Safe Mobile Workforce Server	5-2	2
Installing Safe Mobile Workforce Secure Access	5-7	7

#### Chapter 6: Installing Safe Mobile Workforce on Citrix XenServer

Installing Safe Mobile Workforce Server	2
Installing Safe Mobile Workforce Secure Access	7

#### **Chapter 7: Post-Installation Configuration**

Accessing Safe Mobile Workforce Web Console	7-2
Activating Your Product	7-3
Changing the Logon Password	7-4
Configuring Server Network Interface (Optional)	7-4
Configuring Active Directory Settings (Optional)	7-6
Configuring Mobile Client Settings	7-7
Configuring SafeSync Integration Settings (Optional)	7-8
Configuring Microsoft Exchange Server Settings (Optional)	7-8
Configuring External Storage (Optional)	7-9
Configuring Email Notifications7-	-10
Managing Groups and Users	-11
Creating a User Account Locally	-11 -12
Deploying Safe Mobile Workforce to Mobile Devices7-	-13
Installing Android Client for Safe Mobile Workforce7-	-13
Installing iOS Client for Safe Mobile Workforce7-	-14

## **Appendix A: Network Port Configurations**

Network Port Configuration for Safe Mobile Workforce Server	A-2
Network Port Configuration for Secure Access	A-4
Network Ports in Safe Mobile Workforce Architecture	A-5



## Preface

Welcome to the Trend Micro<sup>TM</sup> Safe Mobile Workforce Administrator's Guide. This guide describes various Safe Mobile Workforce components and guides administrators in deploying and managing Safe Mobile Workforce.

This preface discusses the following topics:

- Audience on page iv
- Safe Mobile Workforce Documentation on page iv
- Document Conventions on page iv

## Audience

The Safe Mobile Workforce documentation is intended for administrators who are responsible for administering and managing mobile devices in enterprise environments.

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

- Installing and configuring Linux servers
- Configuring and managing mobile devices (such as smartphones and tablets)
- Network concepts (such as IP address, netmask, topology, and LAN settings)
- Various network topologies
- Network devices and their administration
- Network configurations (such as the use of VLAN, HTTP, and HTTPS)

## Safe Mobile Workforce Documentation

The Safe Mobile Workforce documentation consists of the following:

- Installation and Deployment Guide—this guide helps you get "up and running" by introducing Safe Mobile Workforce, and assisting with network planning and installation.
- Administrator's Guide—this guide provides detailed Safe Mobile Workforce technologies and configuration.
- **Online help**—the purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values.
- **Readme**—the Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.

## **Document Conventions**

To help you locate and interpret information easily, the documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation
Monospace	Example, sample command line, program code, Web URL, file name, and program output
<u>Link</u>	Cross-references or hyperlinks.
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

# Chapter 1

## Introducing Safe Mobile Workforce

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

This chapter contains the following sections:

- About Safe Mobile Workforce on page 1-2
- Why Use Safe Mobile Workforce on page 1-2
- System Requirements on page 1-4
- Architecture of Safe Mobile Workforce on page 1-5
- Components of Safe Mobile Workforce on page 1-7

## About Safe Mobile Workforce

Trend Micro Safe Mobile Workforce is a service that hosts mobile operating system (Android) on centralized servers, which are accessible over a network using a remote display protocol. This provides a clear separation between corporate and user data, and helps protect the sensitive information.

- For users, this means that they can access the same workspace from any location, without being tied to a single mobile device.
- For administrators, this means a more centralized, efficient workspace that is easier to manage and maintain.

## Why Use Safe Mobile Workforce

Safe Mobile Workforce provides the following:

BENEFIT	DESCRIPTION
Data Protection	All enterprise applications and data are saved in secure corporate servers under administrator's control.
Good User Experi- ence	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 workspace.
	Natural screen touch experience for smartphones and tablets.
Simplified Manage- ment	Administrator can centrally manage all users from sin- gle Web console.
Single Sign-On	Reducing time spent in re-entering passwords in work- space.
	Reducing administration cost due to lower number of IT help desk calls about passwords.

TABLE 1-1. Why use Safe Mobile Workforce

BENEFIT	DESCRIPTION
Workspace Customi- zation	Administrator can create a personal mobile workspace for employees.
	Administrator can centrally customize applications for employees in their workspace from the server.
User-based Profile	Provides user based profile management
	Users can use their own workspace from any of their mobile devices.
Manageable Life Cycle	Administrator can remotely manage a workspace's entire life cycle-from provisioning to the end of life.
Easy Deployment	Provides on-premise deployment.
	Provides self-contained Linux-based operating system for easy deployment.
Integration with Trend Micro Safe- Sync	Provides integration with Trend Micro SafeSync to provide cloud based file storage to all users.
Integration with Enterprise Infra- structure	Provides integration with LDAP and external storage.

TABLE 1-1.	Why use	Safe Mobile	Workforce
------------	---------	-------------	-----------

## **System Requirements**

Review the following requirements before installing Safe Mobile Workforce.

TABLE 1-2.	System	Requirements	for Server
------------	--------	--------------	------------

COMPONENT	REQUIREMENTS
Processor	64-bit x86 four-core Intel processor with SSSE3 support
Memory	4-GB
Hard disk	30-GB available for installation
Network Cards (NIC)	Two 1-GB NICs

#### TABLE 1-3. 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 1-4. System Requirements for Sale Mobile Workforce mobile clip
--

COMPONENT	REQUIREMENTS
Operating system	• iOS 4.3 or later
	Android 2.3 or later

## Architecture of Safe Mobile Workforce

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

## **Single Server Installation Model**

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



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

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

## **Multiple Server Installation Model**

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



Note: All components except Tried Micro Safe Mobile Workforce (TMSMW) can be installed on one computer. Remote Mobile Experience (RMX) is an intelligent remote access protocol.

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

## **Components of Safe Mobile Workforce**

The following table provides the descriptions of the Safe Mobile Workforce components.

Component	DESCRIPTION	REQUIRED OR OPTIONAL
Safe Mobile Workforce Server	The Safe Mobile Workforce Server con- tains Web Console, Web Service, Control- ler and Resource Pool.	Required
	<ul> <li>Web console provides central management console for administrator</li> </ul>	
	<ul> <li>Web service manages user logon, logoff and the connection to user's workspace.</li> </ul>	
	<ul> <li>Controller allows Web console to manage a resource pool.</li> </ul>	
	<ul> <li>Resource pool hosts workspaces. Each workspace runs as a Safe Mobile Workforce instance.</li> </ul>	
Safe Mobile Workforce Mobile Client Application	The mobile client application is installed on the mobile devices. The client applica- tion connects with the Safe Mobile Work- force server to allow users to use their workspaces hosted on the server.	Required
Secure Access	The Secure Access provides Internet access on mobile clients.	Optional
Active Directory	The Safe Mobile Workforce server imports groups and users from Active Directory.	Optional

Component	DESCRIPTION	REQUIRED OR OPTIONAL
External Data- base	External Database provides scalable data storage for user data. By default, Safe Mobile Workforce server maintains a data- base 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
SafeSync Server	SafeSync Server provides file storage for all users.	Optional



## **Installing on Bare Metal Servers**

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

This chapter contains the following sections:

- Installing Safe Mobile Workforce Server on page 2-2
- Installing Safe Mobile Workforce Secure Access on page 2-3

## Installing Safe Mobile Workforce Server

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

#### To install Safe Mobile Workforce Server on a Bare Metal server:

- 1. Power on the Bare Metal server where you want to install Safe Mobile Workforce.
- 2. Insert the installation DVD into the DVD drive, and reboot the server. The Safe Mobile Workforce installation menu appears.
- Select Install Safe Mobile Workforce Server and press Enter.
   The setup starts loading the installation image file. After it completes, Trend Micro License Agreement screen appears.
- 4. Click Accept to agree to the license agreement.

A screen appears displaying the hardware components.

5. Click Next.

A screen appears where you can configure network and general settings.

- 6. Configure the following:
  - Interface Settings for eth0:
    - **IP address**: the internal IP address for Safe Mobile Workforce server Web console.
    - **Subnet mask**: the subnet mask for the Safe Mobile Workforce server internal IP address.
  - Interface Settings for eth1:
    - **IP address**: the external IP address for mobile client application to access Safe Mobile Workforce server.
    - Subnet mask: the subnet mask for the external IP address.
  - General Settings:
    - Host name: type a Host name for Safe Mobile Workforce server.
    - Gateway
    - Primary DNS
    - Secondary DNS

- Note: Make sure that the network interfaces eth0 and eth1 are connected to the network. If the network interface eth0 is not connected to the network, you will not be able to use the Web Console to access the server. If the network interface eth1 is not connected to the network, the mobile client application will not be able to connect to the server.
- 7. Click Next.
- 8. Select your time zone and click Next.
- **9.** Set your operating system password for the administrator account, and click **Next**. The **Summary** screen appears.
- **10.** Check the summary of your configuration and if you are satisfied with the configuration, click **Next** and then click **Continue** on the confirmation dialog box that appears.

The setup will start installing Safe Mobile Workforce on the server. After the installation completes, the **Installation Completed** screen appears.

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

After the reboot completes, log on to the server using the password you set up in *step 9* of this procedure.

## Installing Safe Mobile Workforce Secure Access

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.

#### To install Safe Mobile Workforce Secure Access on a Bare Metal server:

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

The Secure Access installation menu appears.

3. Select Install Secure Access and press Enter.

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

4. Click Accept to agree to the license agreement.

A screen appears displaying the hardware components.

5. Click Next.

A screen appears where you can configure network and general settings.

- **6.** Configure the following:
  - **Network Devices**: select the network interface that you want to use to connect to the network. (Usually it is the network interface **eth0**).
  - Interface Setting:
    - IP address: the IP address for Safe Mobile Workforce server.
    - **Subnet mask**: the subnet mask for the Safe Mobile Workforce server IP address.
  - General Settings:
    - Host name: type a Host name for Safe Mobile Workforce server.
    - Gateway
    - Primary DNS
    - Secondary DNS

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

#### 7. Click Next.

A screen appears where you can configure Secure Access settings.

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

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

- Safe Mobile Workforce server IP address: type the IP address you configured for eth1 of the Safe Mobile Workforce server.
- 9. Click Next.
- 10. Select your time zone and click Next.
- **11.** Set your operating system password for the administrator account, and click **Next**. The **Summary** screen appears.
- **12.** Check the summary of your configuration and if you are satisfied with the configuration, click **Next** and then click **Continue** on the confirmation dialog box that appears.

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

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

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

# Chapter 3

# Installing on VMware vSphere ESXi Hypervisor

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

This chapter contains the following sections:

- Installing Safe Mobile Workforce Server on page 3-2
- Installing Safe Mobile Workforce Secure Access on page 3-15

## Installing Safe Mobile Workforce Server

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

- 1. Creating a virtual machine (See *Creating a Virtual Machine* on page 3-2)
- Configuring VM Network Card (See *Configuring VM Network Card (Optional*) on page 3-13)
- **3.** Installing Safe Mobile Workforce (See *Installing Safe Mobile Workforce on VMware ESXi* on page 3-15)

Step 1. Creating a Virtual Machine

#### To install Safe Mobile Workforce on VMware ESXi:

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

The Create New Virtual Machine screen appears.

4. Select Typical and click Next.



FIGURE 3-1. Select Configuration

The Name and Location screen appears.

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



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

The Resource Pool screen appears.

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

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

🚱 Create New Virtual Machin	
Resource Pool Within which resource pool	ol do you want to run this virtual machine?
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 within a host or cluster. Virtual machines and child pools share the resources of their parent pool.
Help	<pre></pre>

FIGURE 3-3. Select a resource pool

The **Storage** screen appears.

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



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

The Guest Operating System screen appears.

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

🚱 Create New Virtual Machine	
Guest Operating System Specify the guest operatin	g system to use with this virtual machine
Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Disk Ready to Complete	Guest Operating System:  C Windows C Linux C Other Version:  Other Linux (64-bit)  Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.
Help	<back next=""> Cancel</back>

FIGURE 3-5. Select the guest operating system

The **Network** screen appears.

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

#### TABLE 3-5. Network Settings for Safe Mobile Workforce

Nаме	Network	ADAPTER	CONNECT AT POWER ON
NIC 1	VM Network	E1000	Enabled
NIC 2	VM Network	E1000	Enabled

💋 Create New Virtual Machine	
Network Which network connections	will be used by the virtual machine?
Configuration Name and Location Resource Pool Storane Guest Operating System Network Create a Disk Ready to Complete	Create Network Connections How many NICs do you want to connect? Network Network Adapter On NIC 1: VM Network E1000 V V NIC 2: VM Network VIC 1: VM Network VIC 2: VIC 2: VM Network VIC 2: VIC
Help	< Back Next > Cancel

FIGURE 3-6. Create network connections

10. Click Next.

The Create a Disk screen appears.

- 11. On the Create a Disk screen, do the following:
  - a. Select at least 30-GB of virtual disk space for Safe Mobile Workforce.
  - b. Select Thick Provision Lazy Zeroed
  - c. Click Next.

😰 Create New Virtual Machine	3				- 🗆 X
Create a Disk Specify the virtual disk size	e and provisioning policy			Virtual №	lachine Version: 8
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 Z © Thick Provision Eager © Thin Provision	Jatastore 1       57.3       Jatastore 1       GB •       GB •       Zeroed			
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.



FIGURE 3-8. Ready to Complete

The Virtual Machine Properties screen appears.

- 13. On the Hardware tab, do the following:
  - a. Select Memory (adding)Memory Configuration appears in the right pane.
  - **b.** In the **Memory Size** field, select at least 4-GB.

Hardware       Options       Resources         Show All Devices       Add       Remove         Hardware       Summary       1011 GB         Hardware       Summary       1011 GB         Wemory (adding)       4096 MB       512 GB         Video card (adding)       1       Maximum recommended for this         Wetwork       VMCI (adding)       Client Device         New FO/DVD (adding)       Client Device       32 GB         New SCI Controller (add       LSI Logic Parallel         New NIC (adding)       VM Network       8 GB         New Hard Disk (adding)       Virtual Disk       4 GB         128 MB       4 GB       2 GB         128 MB       4 MB       3 MB         64 MB       4 MB       4 MB <th>Create New Virtual Machine</th> <th></th>	Create New Virtual Machine	
4 MB	Hardware       Options       Resources         Show All Devices       Add       Remove         Hardware       Summary         Memory (adding)       4096 MB         CPUs (adding)       1         Video card (adding)       Video card         New COD/DVD (adding)       Client Device         New Floppy (adding)       Client Device         New SCSI Controller (add       LSI Logic Parallel         New NIC (adding)       VM Network         New HIC (adding)       VM Network         New HIC (adding)       Vin Network         New Hard Disk (adding)       Virtual Disk	Memory Configuration          1011 GB       Memory Size:       Image: CB         512 GB       Maximum recommended for this         256 GB       Maximum recommended for this         128 GB       Default recommended for this         32 GB       Default recommended for this         32 GB       Maximum recommended for this         32 GB       Default recommended for this         32 GB       GB         16 GB       GB         2 GB       GB         128 MB       GB         64 MB       GB         32 MB       GB         64 MB       GB         32 MB       GB         16 MB       MB
		4 MB

FIGURE 3-9. VM Properties - Memory Configuration

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

CPU settings appear in the right pane.

- **15.** In the CPU settings, do the following:
  - In the Number of virtual sockets drop-down list, select 2.
  - In the Number of cores per socket drop-down list, select 2.



FIGURE 3-10. VM Properties - CPU Settings
16. On the Hardware tab, click New CD/DVD (adding).

The CD/DVD settings appear in the right pane.

- 17. In the CD/DVD settings, do the following:
  - **a.** Under **Device Type** section, select **Datastore ISO File**, and click **Browse**, and then select the iso setup image file from the ESXi server hard drive.
  - b. Under Device Status section, select Connect at power on.

Create New Virtual Machine     Safe Mobile Workforce Server - Virtual Machine P     Hardware   Options   Resources       Community Options   Resources	roperties
Hardware     Summary       Memory (adding)     4096 MB       CPUs (adding)     4       Video card (adding)     Ketricted       New CD/DVD (adding)     [datastore1]       New Floppy (adding)     Client Device       New SCSI Controller (add     LSI Logic Par       New NIC (adding)     VM Network       New NIC (adding)     VM Network       New Hard Disk (adding)     Virtual Disk	Remove       Connected         Connect at power on         Device Type         Cleant Device         Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar.         alkel         C Host Device         C Datastore ISO File         [datastore i] VMIISO/TMSMW-1.0-12         Browse         Mode         C Passthrough IDE (recommended)         C Emulate IDE         Vtrual Device Node         C IDE (1:0)
Help	FinishCancel

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

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

#### Step 2. Configuring VM Network Card (Optional)

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

- NAT: Workspaces share the server's IP address-this option enables you to share the server's IP address with the workspaces. This option is selected by default.
- **IP Range: Assign IP address to workspaces**-this option enables you to assign individual IP address to each workspace.

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

#### To configure the VM Network Card:

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



FIGURE 3-12. Networking screen

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

The switch **Properties** screen appears.

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

The VM Network Properties screen appears.

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

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

vivi network Properties	
General Security Traffic Shap	ping   NIC Teaming
Policy Exceptions	
Promiscuous Mode:	Accept
MAC Address Changes:	Accept 🗸
Forged Transmits:	Accept

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

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

#### Step 3. Installing Safe Mobile Workforce on VMware ESXi

- 1. Start VMware ESXi and power on the virtual machine that you created in *Step 1*. *Creating a Virtual Machine* on page 3-2.
- Click the Console tab on the virtual machine. The Safe Mobile Workforce installation menu appears.
- **3.** Follow *step 3* to *step 11* of the topic *Installing Safe Mobile Workforce Server* on page 2-2 to complete Safe Mobile Workforce installation.

### Installing Safe Mobile Workforce Secure Access

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

- 1. Creating a virtual machine (See Creating a Virtual Machine on page 3-15)
- 2. Installing Secure Access (See Installing Secure Access on VMware ESXi on page 3-27)

#### Step 1. Creating a Virtual Machine

#### To install Secure Access on VMware ESXi:

- 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**.

🖉 Create New Virtual Machine	
Configuration Select the configuration for t	ne virtual machine Virtual Machine Version: 8
Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Diak Ready to Complete	Configuration     Typical     Create a new virtual machine with the most common devices and configuration options.     Custom     Create a virtual machine with additional devices or specific configuration options.
Help	< Back Next > Cancel

FIGURE 3-14. Select Configuration

The Name and Location screen appears.

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



FIGURE 3-15. Name New Virtual Machine

The Resource Pool screen appears.

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

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

🚱 Create New Virtual Machin	
Resource Pool Within which resource pool	ol do you want to run this virtual machine?
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 within a host or cluster. Virtual machines and child pools share the resources of their parent pool.
Help	<pre></pre>

FIGURE 3-16. Select a resource pool

The **Storage** screen appears.

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



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

The Guest Operating System screen appears.

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

🚱 Create New Virtual Machine	
Guest Operating System Specify the guest operatin	g system to use with this virtual machine
Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Disk Ready to Complete	Guest Operating System:  C Windows C Linux C Other Version:  Other Linux (64-bit)  C deter Linux (64-bit)  C deter Linux (64-bit)  C deter Linux (64-bit) C dete
Help	_ <back next=""> Cancel</back>

FIGURE 3-18. Guest Operating System

The **Network** screen appears.

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

TABLE 3-6. Network Settings for Secure Access

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

🕖 Create New Virtual Machine		
Network Which network connection	s will be used by the virtual machine?	Virtual Machine Version: 8
Configuration Name and Location Resource Pool Storace Guest Operating System Network Create a Disk Ready to Complete	Create Network Connections How many NICs do you want to connect? Network NEC 1: VM Network If supported by this virtual machine version, more than 4 NICs can be adde virtual machine is created, via its Edit Settings dialog. Adapter choice can affect both networking performance and migration compa the VMware KnowledgeBase for more information on choosing among the ne supported for various guest operating systems and hosts.	Connect at Power On d after the atibility. Consult twork adapters
Help	< Back Next	> Cancel



10. Click Next.

The Create a Disk screen appears.

- 11. On the Create a Disk screen, do the following:
  - a. Select at least 30-GB of virtual disk space for Safe Mobile Workforce.
  - b. Select Thick Provision Lazy Zeroed
  - c. Click Next.

🖉 Create New Virtual Machine	,		
Create a Disk Specify the virtual disk size	and provisioning policy		Virtual Machine Version: 8
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 Zu Thick Provision Eager Z Thin Provision	datastore1 57.3 00 - G8 - eroed Zeroed	
Help			< Back Next > Cancel

FIGURE 3-20. Specify Hard Disk Space

The **Ready to Complete** screen appears.

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



FIGURE 3-21. Ready to Complete

The Virtual Machine Properties screen appears.

- 13. On the Hardware tab, do the following:
  - a. Select Memory (adding).

Memory Configuration appears in the right pane.

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

Create New Virtual Machine     Oreate New Virtual Machine     Properties	
Hardware       Summary         Hardware       Summary         Hardware       Summary         Memory (adding)       4096 MB         CPUs (adding)       1         Video card (adding)       Video card         WHCI device (adding)       Restricted         New CD/DVD (adding)       Client Device         New KOD/DVD (adding)       Client Device         New NSCSI Controller (add       LSI Logic Parallel         New NIC (adding)       VM Network         New NIC (adding)       Virtual Disk	Memory Configuration          1011 GB       Memory Size:       H ::       GB •         1011 GB       Memory Size:       H ::       GB •         121 GB       Maximum recommended for this       guest OS: 1011 GB         128 GB       Performance: 65492 MB.       Default recommended for this         32 GB       Default recommended for this       guest OS: 384 HB.         32 GB       Minimum recommended for this       guest OS: 384 HB.         36 GB       GB •       GB •       GB •         16 GB       guest OS: 32 MB.       GB •       GB •         16 GB       GB •       GB •       GB •         16 MB       GB •       GB •       GB •         128 MB       G       GB •       GB •         16 MB       GB •       GB •       GB •
Help	Finish Cancel

FIGURE 3-22. VM Properties - Memory Configuration

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

CPU settings appear in the right pane.



FIGURE 3-23. VM Properties - CPU Settings

- **15.** In the CPU settings, do the following:
  - In the Number of virtual sockets field, select 2.
  - In the **Number of cores per socket field**, select **2**.

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

The CD/DVD settings appear in the right pane.

- 17. In the CD/DVD settings, do the following:
  - **a.** Under **Device Type** section, select **Datastore ISO File**, and click **Browse**, and then select the iso setup image file from the ESXi server hard drive.
  - b. Under Device Status section, select Connect at power on.

<ul> <li>Create New Virtual Machine</li> <li>Safe Mobile Workforce Secure Acc Hardware Options Resources</li> <li>Show All Devices</li> <li>Hardware</li> <li>Memory (adding)</li> <li>CPUs (adding)</li> <li>Video card (adding)</li> <li>Video card (adding)</li> <li>New Floppy (adding)</li> <li>New Floppy (adding)</li> <li>New NIC (adding)</li> <li>New NIC (adding)</li> <li>New Hard Disk (adding)</li> </ul>	Add Remove Add Remove Summary 4096 MB 4 Video card Restricted [datastore1] VMIIS Client Device LSI Logic Parallel VM Network Virtual Disk	
Help		

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

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

#### Step 2. Installing Secure Access on VMware ESXi

- 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 Secure Access installation menu appears.
- **3.** Follow *step 3* to *step 13* of the topic *Installing Safe Mobile Workforce Secure Access* on page 2-3 to complete Secure Access installation.

# Chapter 4

## Installing Safe Mobile Workforce on VMware Workstation

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

This chapter contains the following sections:

- Installing Safe Mobile Workforce Server on page 4-2
- Installing Safe Mobile Workforce Secure Access on page 4-8

## Installing Safe Mobile Workforce Server

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

- 1. Creating a virtual machine (See *Creating a Virtual Machine* on page 4-2)
- 2. Installing Safe Mobile Workforce (See *Installing Safe Mobile Workforce Server on VMware Workstation* on page 4-7)

#### Step 1. Creating a Virtual Machine

#### To install Safe Mobile Workforce on VMware Workstation:

- 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.
- Click File > New > Virtual Machine from the menu. The New Virtual Machine Wizard screen appears.
- 4. Select Custom (Advanced) and click Next.
  - The Choose the Virtual Machine Hardware Compatibility screen appears.
- 5. Select an appropriate option from the Hardware compatibility drop-down list.

Note: This document uses Workstation 10.0 hardware compatibility.

The Guest Operating System Installation screen appears.

 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:
  - Guest operating system: Linux
  - Version: Other Linux 2.6.x kernel 64-bit

New Virtual Machine Wizard		<b>_</b>
Select a Guest Operating Sys Which operating system will b	<b>tem</b> e installed on this virtual mach	ine?
Guest operating system		
Microsoft Windows		
Linux		
Novell NetWare		
Solaris		
VMware ESX		
Other		
Version		
Other Linux 2.6.x kernel 64-bit		-
	< Pack Next >	Cancel
нер	< Dack Next >	Cancer

FIGURE 4-1. Select a guest operating system

8. Click Next.

The Name the Virtual Machine screen appears.

- **9.** Type a name for the virtual machine, and click **Next**. The **Processor Configuration** screen appears.
- 10. Under the **Processor** section, do the following:
  - In the Number of processors drop-down list, select 2.
  - In the **Number of cores per processor** drop-down list, select **2**.
- 11. Click Next.

The Memory for the Virtual Machine screen appears.

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

The Network Type screen appears.

- **13.** Select **Use bridged networking**, and click **Next**. The **Select I/O Controller Types** screen appears.
- 14. From the SCSI Controller list, select the recommended type: LSI Logic, and click Next.

The Select a Disk Type screen appears.

- **15.** Select the recommended disk type: **SCSI**, and click **Next**. The **Select a Disk** screen appears.
- **16.** Select **Create a new virtual disk** and click **Next**. The **Specify Disk Capacity** screen appears.
- **17.** Do the following:
  - Select **30-GB** for the **Maximum disk size**.
  - Select Split virtual disk into multiple files.



FIGURE 4-2. Specify disk capacity

18. Click Next.

The Ready to Create Virtual Machine screen appears.

19. Click Customize Hardware.

The **Hardware** screen appears.

20. Click Add.

The Add Hardware Wizard appears displaying Hardware Type screen.

21. Select Network Adapter and click Next.

The Network Adapter Type screen appears.

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

Device	Summary	Specify the amount of memory allocat	ted to this virtual
Memory	2 GB	machine. The memory size must be a	multiple of 4 MB.
Processors	Add Hardware Wizard	-	🗐 🔊 мв
Network Adap	Network Adapter Type What type of network adapter do	you want to add?	
Printer	Network connection		
Display	Bridged: Connected directly to the physical network		nended memory
	Replicate physical network connection state		ng may
	NAT: Used to share the host's IP address		
	Host-only: A private network shared with the host		
	Custom: Specific virtual network		hemory
	VMnet0	*	
			mended minimun
	Device status		
	Connect at power on		
			_
		< Back Finish Cancel	
			_
	Add Remove		

FIGURE 4-3. Configure network adapter type

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

The Ready to Create Virtual Machine screen appears.

24. Click Finish.

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



FIGURE 4-4. Virtual machines in VMware Workstation

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

The Virtual Machine Settings screen appears.

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

The CD/DVD settings appear on the right pane.

- 27. In the CD/DVD settings, do the following:
  - a. Under Connection section, select Use ISO image file, and click Browse, and then select the Safe Mobile Workforce Server iso setup image file.
  - b. Under Device status section, select Connect at power on.

Safe Mobile Work	Virtual Machine Settings		<b>•</b>	
Library Q. Type here to s W My Compu & Ubuntu & VMu & With & SA VMu & Stare S SA VMu & Shared VM	Device Pevice Pevice Protocological Protoc	Summary 2 GB 4 3 Auto delact 3 digget (Automatic) 3 digget (Automatic) 3 digget (Automatic) 3 digget (Automatic) 9 feature 4 Auto delact 3 Auto delact 3 Auto delact	Device status Connected Connect at power on Use physical drive: Auto detect Use 150 maps file: (10.204.16.2[buld]\/4[1.0]cer   Downe Advanced)	
		Add Rer	nove	Mobile Workforce\S rce.vmx 0 virtual machine
			OK Cancel Help	

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

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

#### Step 2. Installing Safe Mobile Workforce Server on VMware Workstation

- 1. Start VMware Workstation and power on the virtual machine that you created in *Step 1 on page 4-2*.
- Click the Console tab on the virtual machine. The Safe Mobile Workforce installation menu appears.
- **3.** Follow *step 3* to *step 11* of the topic *Installing Safe Mobile Workforce Server* on page 2-2 to complete Safe Mobile Workforce server installation.

## Installing Safe Mobile Workforce Secure Access

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

- 1. Creating a virtual machine (See *Creating a Virtual Machine* on page 4-8)
- 2. Installing Safe Mobile Workforce (See *Installing Safe Mobile Workforce Secure Access on VMware Workstation* on page 4-13)

Step 1. Creating a Virtual Machine

#### To install Safe Mobile Workforce Secure Access on VMware Workstation:

- 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.
- Click File > New > Virtual Machine from the menu. The New Virtual Machine Wizard screen appears.
- Select Custom (Advanced) and click Next.
   The Choose the Virtual Machine Hardware Compatibility screen appears.
- 5. Select an appropriate option from the Hardware compatibility drop-down list.

Note: This document uses Workstation 10.0 hardware compatibility.

The Guest Operating System Installation screen appears.

 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:
  - Guest operating system: Linux
  - 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	
VMware ESX	
O Other	
Version	
Other Linux 2.6.x kernel 64-bit	-
Help < Back Next > C	ancei

FIGURE 4-6. Select a guest operating system

8. Click Next.

The Name the Virtual Machine screen appears.

- **9.** Type a name for the virtual machine, and click **Next**. The **Processor Configuration** screen appears.
- 10. Under the **Processor** section, do the following:
  - In the Number of processors drop-down list, select 2.
  - In the **Number of cores per processor** drop-down list, select **1**.
- 11. Click Next.

The Memory for the Virtual Machine screen appears.

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

The Network Type screen appears.

- **13.** Select **Use bridged networking**, and click **Next**. The **Select I/O Controller Types** screen appears.
- 14. From the SCSI Controller list, select the recommended type: LSI Logic, and click Next.

The Select a Disk Type screen appears.

- **15.** Select the recommended disk type: **SCSI**, and click **Next**. The **Select a Disk** screen appears.
- **16.** Select **Create a new virtual disk** and click **Next**. The **Specify Disk Capacity** screen appears.
- **17.** Do the following:
  - Select **30-GB** for the **Maximum disk size**.
  - Select Split virtual disk into multiple files.



FIGURE 4-7. Specify disk capacity

18. Click Next.

The Ready to Create Virtual Machine screen appears.

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

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





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

The Virtual Machine Settings screen appears.

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

The CD/DVD settings appear on the right pane.

- 22. In the CD/DVD settings, do the following:
  - a. Under Connection section, select Use ISO image file, and click Browse, and then select the Safe Mobile Workforce Secure Access iso setup image file.
  - b. Under Device status section, select Connect at power on.

uware Options		
Device	Summary	Device status
Memory Processors	1 GB 2	Connected Connect at power on
Hard Disk (SCSI)	20 GB Auto detect	Connection
Network Adapter	Bridged (Automatic) Present	Use physical drive:     Auto detect
)) Sound Card Printer	Auto detect Present	Use ISO image file:
Display	Auto detect	MSMWSA-1.0-1012-x86_64.iso

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

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

- Step 2. Installing Safe Mobile Workforce Secure Access on VMware Workstation
- 1. Start VMware Workstation and power on the virtual machine that you created in *Step 1 on page 4-8.*
- 2. Click the **Console** tab on the virtual machine.

The Safe Mobile Workforce installation menu appears.

**3.** Follow *step 3* to *step 13* of the topic *Installing Safe Mobile Workforce Secure Access* on page 2-3 to complete Safe Mobile Workforce Secure Access installation.

# Chapter 5

## Installing Safe Mobile Workforce on Microsoft Hyper-V

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

This chapter contains the following sections:

- Installing Safe Mobile Workforce Server on page 5-2
- Installing Safe Mobile Workforce Secure Access on page 5-7

## Installing Safe Mobile Workforce Server

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

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

#### Step 1. Creating a Virtual Machine

#### To install Safe Mobile Workforce on Microsoft Hyper-V:

- 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.
- 1. Copy the iso image setup file on the Microsoft Hyper-V computer hard drive.
- 2. 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 Safe Mobile Workforce server, and click Next. The Specify Generation screen appears.
- Select Generation 1, and click Next. The Assign Memory screen appears.
- In the Startup memory field, type 4096 MB, and click Next. The Configure Networking screen appears.
- Select a virtual switch from the drop-down list that you want to use for the Safe Mobile Workforce Server, and click Next.

The Connect Virtual Hard Disk screen appears.

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

<b>a</b> .	New Virtual Machine Wizard
Connect Virte	ual Hard Disk
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.  Create a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk.  Name: Safe Mobile Workfroce Server.vhdx Location: D:(VitualDisk\ Browse Size: 31 GB (Maximum: 64 TB)  Use an existing virtual hard disk Use this option to attach an existing virtual hard disk, either VHD or VHDX format. Location: D:(VitualDisk\ Derowse Attach a virtual hard disk later Use this option to skip this step now and attach an existing 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.
- 12. The virtual machine setup completes, and the Settings screen appears.
- **13.** On the left side of the **Settings** screen, click **Add Hardware** under **Hardware** section.
- 14. On the right side of the screen, select Network Adapter and then click Add.



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

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

🔁 Settings for Safe Mobile Workfroce Server on STORAGE 📃 🗖 🗙		
Safe Mobile Workfroce Server	✓ ◀ ▶ 🔍	
★ Hardware         ▲ Add Hardware         ● BLOS         Boot from CD         ● Memory         4096 MB         ● Processor         1 Virbual processor         ■ IDE Controller 0         ● Flard Drive         Safe Mobile Workfroce Ser	Network Adapter      Specify the configuration of the network adapter or remove the network adapter.      Wirtual switch:      Broadcom NetXtreme Gigabit Ethernet #3 - Virtual Switch      VLAN ID      Lanble virtual LAN identification      The VLAN identifier specifies the virtual LAN that this virtual machine will use for all     network communications through this network adapter.      Z	
DVD Controller 1     DVD Drive     None     DVD Drive     None     SCSI Controller     Broadcom NetXtreme Gigabit Et     Product Adapter     Broadcom NetXtreme Giga     COM 1     None     COM 2     None     Diskette Drive     None	Bandwidth Management  Bandwidth Management  Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.  Minimum bandwidth:  Musimum bandwidth:  No Mbps  To remove the minimum or maximum unrestricted, specify 0 as the value.  To remove the network adapter from this virtual machine, click Remove.	
None  A dagement  Anne Safe Mobile Workfroce Server  Safe Nobile Workfroce Server  Some services offered  Checkopic File Location D:\\WuaDisk  Smart Paging File Location D:\\VuaDisk	Remove           Image: Second	
	OK Cancel Apply	

FIGURE 5-3. Select a network switch

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


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

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

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

- 1. Start **Microsoft Hyper-V** and power on the virtual machine that you created in *Step 1 on page 5-2*.
- Click the Console tab on the virtual machine. The Safe Mobile Workforce installation menu appears.
- **3.** Follow *step 3* to *step 11* of the topic *Installing Safe Mobile Workforce Server* on page 2-2 to complete Safe Mobile Workforce server installation.

# Installing Safe Mobile Workforce Secure Access

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

- 1. Creating a virtual machine (See *Creating a Virtual Machine* on page 5-7)
- 2. Installing Safe Mobile Workforce (See Installing Safe Mobile Workforce Secure Access on Microsoft Hyper-V on page 5-9)

#### Step 1. Creating a Virtual Machine

#### To install Safe Mobile Workforce Secure Access on Microsoft Hyper-V:

- 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. 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 Safe Mobile Workforce Secure Access, and click Next. The Specify Generation screen appears.
- 6. Select Generation 1, and click Next. The Assign Memory screen appears.
- In the Startup memory field, type 4096 MB, and click Next. The Configure Networking screen appears.
- Select a virtual switch from the drop-down list that you want to use for the Safe Mobile Workforce Server, and click Next.

The Connect Virtual Hard Disk screen appears.

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

8.	New Virtual Machine Wizard
Connect Virt	tual Hard Disk
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	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.  Careate a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk.  Name: Safe Mobile Workforce Secure Access.vhdx Location: D:{VirtualDisk} Erowse Size: 3d( GB (Maximum: 64 TB) Cuse an existing virtual hard disk Use this option to attach an existing virtual hard disk, either VHD or VHDX format. Location: D:{VirtualDisk} Cuse this option to attach an existing virtual hard disk, either VHD or VHDX format. Location: D:{VirtualDisk} Use this option to skip this step now and attach an existing virtual hard disk later.
	< Previous Next > Finish Cancel

FIGURE 5-5. Create Virtual Hard Disk screen

The Installation Options screen appears.

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

The **Summary** screen appears.

- 11. Verify the virtual hard disk settings on the **Summary** screen, and click **Finish**. Click **Previous** to go back to any previous screen and change settings, if required.
- 12. The virtual machine setup completes, and the Settings screen appears.
- **13.** On the left side of the screen, Click **DVD Drive**, and then click **Image file**, and select the Safe Mobile Workforce Secure Access installation setup file.



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

- 14. Click OK to finish setting up the virtual machine.
- Step 2. Installing Safe Mobile Workforce Secure Access on Microsoft Hyper-V
- 1. Start VMware Workstation and power on the virtual machine that you created in *Step 1 on page 5-7*.
- Click the Console tab on the virtual machine.
   The Safe Mobile Workforce Secure Access installation menu appears.
- **3.** Follow *step 3* to *step 13* of the topic *Installing Safe Mobile Workforce Secure Access* on page 2-3 to complete Safe Mobile Workforce Secure Access installation.

# Chapter 6

# Installing Safe Mobile Workforce on Citrix XenServer

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

This chapter contains the following sections:

- Installing Safe Mobile Workforce Server on page 6-2
- Installing Safe Mobile Workforce Secure Access on page 6-7

# Installing Safe Mobile Workforce Server

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

- **1.** Installing a VNC viewer application. (See *Installing a VNC Viewer Application* on page 6-2.
- 2. Creating a virtual machine and installing Safe Mobile Workforce server. (See *Creating a Virtual Machine and Installing Safe Mobile Workforce Server* on page 6-3)

#### Step 1. Installing a VNC Viewer Application

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

This document uses TightVNC viewer application for this procedure.

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

#### To install Safe Mobile Workforce on Citrix XenServer:

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

The Add New Server dialog box appears.

8			Xen	Center			- 🗆 🗙
File	View Pool Server VM ack • 💿 Forward •   📑 A	Storage Templa dd New Server   📍	es Tools Wind	<b>low Help</b> New Storage	New VM   🍈	Shut Down 🖌 No	System Alerts 💂
Views:	Server View	🔹 😣 XenCen	ter				
Search.		🔎 Home Sean	h Tags Logs				
	XenCenter By xenserver-kcjwnfvg			Ci	itrix Xen	Server	
		8	Add Ne	w Server	?	<ul> <li>I, server and deskto</li> </ul>	p virtualizatio
		Enter the host and your user Server: User login cre User name: Password:	name or IP address of ogin credentials for dentials oot	of the server you way that server.	ant to add	UPGRADE XenServer	T De: Virtua
				Com	• Network with • Visit the Citri • Learn more •	port Partners o other XenServer users x Knowledge Center about partner offerings	



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

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

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

The New VM screen appears.

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

8	XenCenter		-	
E 8	New VM		_ □	×
View Select a VM template			•	i punt
Template	Search		Q	
Name Installation Media Home Server CPU & Memory Storage Networking Finish	Name	Category CentOS CentOS CentOS CentOS CentOS Debian Debian Debian Oracle		)
сіткіх.	Copy host BIOS strings to VM		< Previous Net > Cancel	



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

The Installation Media screen appears.

- 7. Do the following:
  - Select an installation media.

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

- Under Advanced OS boot parameters section, type graphical utf8 vnc.
- 8. Click Next.
- **9.** Select a server computer from the list, where you want to install Safe Mobile Workforce, and click **Next**.

- 10. On the CPU & Memory screen, type the following:
  - Number of vCPUs: **4**
  - Memory: **4096** MB
- 11. Click Next.

The Storage screen appears.

- 12. Click Properties, and in the Size field, type 30 GB, and then click OK.
- 13. Click Next on the Storage screen.

The **Networking** screen appears.

14. Click Add to add a new network interface.

The Add Virtual Interface screen appears.

15. Without changing any configuration, click Add.

•	XenCenter		×
	New VM	- 🗆 ×	
ews 📁 Configure netw	orking on the new VM	0	In
E Template Name Installation Media	Add Virtual Interface     Add Virtual Interface     Select your network and MAC address for this virtual interface.     You can also optionally define a QoS limit.	l below. You -	
Home Server CPU & Memory Storage Networking Finish	Network: Network 0 v MAC address:	Add Delete Properties	
CITRIX.	QoS settings:  Enable a QoS limit of:  Kbytes/s radd extra virtual  Add Cancel		
•	< Previous Next >	Cancel	

FIGURE 6-3. Add Virtual Interface screen

16. Click Next on the Networking screen.

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

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

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

**18.** Select the virtual machine you have just created, and click the **Console** tab. The screen displays the options to select a network device.

General Memory Storage Networking Console Performance Snapshots Logs		
DVD Drive 1: TMSMW-1.0-1248-x86_64.iso	<ul> <li>Eject</li> </ul>	Looking for guest console
DVD Drvs1:       TMSMW-10-1248-x66_64         Welcome to TMSNW for x86_64         You have nultiple network devices on this system         Which would you like to install through?         cth0 - Ethernet device eth0 - 9e:ab:47:d9:87:c6         eth1 - Ethernet device eth1 - 16:d6:e5:75:1c:b3         OK       Identify         Back	- Eject	Looking for guett console
<tab>/<alt-tab> between elements   <space> selects   <f12> n</f12></space></alt-tab></tab>	ext scre	en
Send Ctri+Alt+Del (Ctri+Alt+Insert)	dock (Alt+Shif	t+U)   Fullsgreen (Ctrl+Enter)

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

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

The **Disc Found** screen appears.

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

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



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

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

The Safe Mobile Workforce installation menu appears.

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

## Installing Safe Mobile Workforce Secure Access

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

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

#### Step 1. Installing a VNC Viewer Application

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

This document uses TightVNC viewer application for this procedure.

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

#### To install Safe Mobile Workforce Secure Access on Citrix XenServer:

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

The Add New Server dialog box appears.



FIGURE 6-6. Add New Server dialog box

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

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

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

The New VM screen appears.

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

🗾 Select a VM tem	plate			3
Template	Search		Q	
Name	Name	Category	^	
Installation Media	CentOS 4 7 (32-hit)	Category	-	
Home Server	CentOS 4.8 (32-bit)	CentOS		
CPU & Memory	CentOS 5 (32-bit)	CentOS		
Storage	😵 CentOS 5 (64-bit)	CentOS		
Networking	😵 CentOS 6 (32-bit)	CentOS		
Finish	😵 CentOS 6 (64-bit)	CentOS		
	O Debian Squeeze 6.0 (32-bit)	Debian		
	Debian Squeeze 6.0 (64-bit)	Debian		
	Debian Wheezy 7.0 (32-bit)	Debian		
	Debian Wheezy 7.0 (64-bit)	Debian		
	🔄 Oracle Enterprise Linux 5 (32-bit)	Oracle	~	
citrix.	Copy host BIOS strings to VM			



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

The Installation Media screen appears.

- 7. Do the following:
  - Select an installation media.

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

- Under Advanced OS boot parameters section, type graphical utf8 vnc.
- 8. Click Next.
- **9.** Select a server computer from the list, where you want to install Safe Mobile Workforce Secure Access, and click **Next**.
- 10. On the CPU & Memory screen, type the following:
  - Number of vCPUs: **4**
  - Memory: **4096** MB
- 11. Click Next.

The Storage screen appears.

- 12. Click Properties, and in the Size field, type 30 GB, and then click OK.
- **13.** Click **Next** on the **Storage** screen. The **Networking** screen appears.
- 14. Click Next.

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

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

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

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

The screen displays the options to select a network device.

General Memory Storage	etworking Console Performance Snapshots Logs
DVD Drive 1: TMSMWSA	D-1012-x86_64.iso V Eject Looking for guest console
Welcome to TMSM	A for x86_64 Disc Found   To begin testing the media before installation press OK. Choose Skip to skip the media test and start the installation. Skip Skip
<tab>/<alt-ta< td=""><td>&gt; between elements   <space> selects   <f12> next screen</f12></space></td></alt-ta<></tab>	> between elements   <space> selects   <f12> next screen</f12></space>
Send Ctrl+Alt+Del (Ctrl+Alt	sert) 🗌 Scale 🔎 Undock (Alt+Shift+U)   Fullscreen (Ctrl+Enter)

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

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

The **Disc Found** screen appears.

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

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



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

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

The Safe Mobile Workforce Secure Access installation menu appears.

**20.** Follow *step 3* to *step 13* of the topic *Installing Safe Mobile Workforce Secure Access* on page 2-3 to complete Safe Mobile Workforce Secure Access installation.

# Chapter 7

# **Post-Installation Configuration**

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

This chapter contains the following sections:

- Accessing Safe Mobile Workforce Web Console on page 7-2
- Activating Your Product on page 7-3
- Changing the Logon Password on page 7-4
- Configuring Server Network Interface (Optional) on page 7-4
- Configuring Active Directory Settings (Optional) on page 7-6
- Configuring Mobile Client Settings on page 7-7
- Configuring SafeSync Integration Settings (Optional) on page 7-8
- Configuring Microsoft Exchange Server Settings (Optional) on page 7-8
- Configuring External Storage (Optional) on page 7-9
- Configuring Email Notifications on page 7-10
- Managing Groups and Users on page 7-11
- Deploying Safe Mobile Workforce to Mobile Devices on page 7-13

# Accessing Safe Mobile Workforce Web Console

#### To access the Safe Mobile Workforce Web console:

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

<u>https://<Safe Mobile Workforce\_domain\_name\_or\_IP\_address></u> The screen as shown in *Figure 7-1* appears.

Safe Mobile Workforce						
User Name: Password:						
Copyright © 2013	Trend Micro Incorporated. All rights reserved.					

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

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

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

Make sure that you change the administrator password after your first sign in. See *Changing the Logon Password on page 7-4* for the procedure.

# **Activating Your Product**

Safe Mobile Workforce displays a Product License screen on logging on to the Safe Mobile Workforce Web console for the first time. The Product License screen is shown in *Figure 7-2*.

#### Product License



#### FIGURE 7-2. Product License screen

#### To activate your product:

**1.** Log on to the server Web console.

The **Product License** screen appears.

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

# **Changing the Logon Password**

After logging on to the Safe Mobile Workforce Web console for the first time, change the logon password immediately.

Tip: Trend Micro recommends changing the logon password every 30 to 90 days.

#### To change the logon password:

- 1. Log on to the server Web console.
- Go to Administration > My Account. The My Account screen appears.
- Click Change password. The Change Password screen appears.
- 4. Type the old password in the **Old password** field.
- 5. Type a new password in the New password and Confirm password fields.
- 6. Click Save.

# Configuring Server Network Interface (Optional)

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

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

#### To configure server network interface:

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

Dashboard Us	ers Profiles	Application	ns Server	Administratio	n 🔻
u are here: <u>Server</u> > localho	ost				
calhost					
Basic Information					
Server name:	localhost				
Description:	local server				
Paddress:	127.0.0.1				
Status:	Running	► Star	t Stop		
Performance					
Jser sessions:			Active: 1 / Se	rver Capacity: 200	
Memory (MB):			Used: 2117	/ Server Capacity: 395	3
Storage (GB):			Used: 1.4 / S	Server Capacity: 21.4	
CPU:					
	C	CPU Usage Tren	d of All Servers		
100		(Time Red	corded)		
100					
X 50					
50					
0					
0:17:32	0:27:32	0:37:33	0:47:34	0:57:34	1:7:35
Network Interfaces					
/irtual Mobile IP range:	10.64.90.201-10	0.64.90.210			
Subnet mask:	255.255.252.0				
Gateway IP address:	10.64.88.1				

FIGURE 7-3. Server details screen

- 4. If the server is running, click Stop to stop the server, and then click OK to confirm.
- 5. Click Edit.
- **6.** Update the following fields as required:
  - Basic Information
    - Server name
    - Description

- Workspace Network Connection
  - NAT: Workspaces share the server's IP address-select this option if you want to share the server's IP address with the workspaces.
  - **IP Range**: Assign IP address to workspaces–select this option if you want to assign individual IP address to each workspace.
    - Workspace IP range-type a range of IP addresses that will used by the workspaces.

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

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

## **Configuring Active Directory Settings** (Optional)

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

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

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

#### To configure Active Directory:

- 1. Log on to the server Web console.
- Click Administration > System Settings. The System Settings screen appears.
- 3. Click the Active Directory tab.
- 4. Select Use Active Directory to enable the feature

- 5. Configure the following:
  - Server IP address
  - Server port
  - **Base DN**-select a Base DN from the drop down list.
  - User name and Password-a user name and password to access the Active Directory server.
  - **Update frequency**-select a time from the list to determine how often to synchronize content with the Active Directory server.
- 6. Click Save.

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

# **Configuring Mobile Client Settings**

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

#### To configure mobile client settings:

- 1. Log on to the server Web console.
- 2. Click Administration > System Settings.

The System Settings screen appears.

- 3. Click the Mobile Client tab.
- 4. Under the **Remember Password** section, if you want to allow users to save their passwords on their mobile devices, select **Allow users to save password on mobile device**.
- 5. Under the Secure Access Settings, configure the following:
  - Domain name or IP address

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

- Port number
- 6. Click Save.

# Configuring SafeSync Integration Settings (Optional)

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

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

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

#### To configure SafeSync integration settings:

- 1. Log on to the server Web console.
- 2. Click Administration > System Settings.

The System Settings screen appears.

- 3. Click the Active Directory tab.
- 4. Make sure that the Use Active Directory checkbox is selected and the Active Directory settings are configured.
- 5. Click the SafeSync Integration tab.
- 6. Select **Enable users to access SafeSync account from workspace**, and then type the SafeSync server URL in the SafeSync server field.
- 7. Click Save.

# **Configuring Microsoft Exchange Server Settings (Optional)**

If you have already set up an Exchange server in your enterprise environment, you can configure Safe Mobile Workforce to automatically configure Exchange server settings for all the users on their workspace. **Note:** You can only configure Safe Mobile Workforce to use an Exchange server if you are using Active Directory server to manage user and group permissions in Safe Mobile Workforce.

#### To configure Microsoft Exchange server integration settings:

- **1.** Log on to the server Web console.
- Click Administration > System Settings. The System Settings screen appears.
- 3. Click the Active Directory tab.
- 4. Make sure that the Use Active Directory checkbox is selected, and the Active Directory settings are configured.
- 5. Click the Exchange Server tab.
- 6. Select Use automatic configuration for Exchange Server on workspace, and then type the server name in the Exchange server field.
- 7. Click Save.

## **Configuring External Storage (Optional)**

You can configure Safe Mobile Workforce to use external storage for the database.

**Note:** You must configure external storage if you want to configure more than one Safe Mobile Workforce server

#### To configure external storage:

- **1.** Log on to the server Web console.
- 2. Click Administration > System Settings.

The **System Settings** screen appears.

- 3. Click the External Storage tab.
- 4. 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.
- 5. Click **Test Connection** and then click **OK** on the pop-up dialog box.
- 6. Click Save.

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

# **Configuring Email Notifications**

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

#### To configure email notification settings:

- **1.** Log on to the server Web console.
- 2. Click Administration > Email Notifications.

The Email Notifications screen appears.

- 3. Under the **Email Settings** section, configure the following:
  - From-type the address from which you want to send the email notification.
  - **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.
- 4. Under Invitation Email Template, type the following:
  - **Subject**-the subject of the email message.
  - Message-the body of the email message.

- **Note:** While editing the **Message** field, make sure to include the token variables %(name)s, %(username)s, %(password)s and %(url)s, which will be replaced by the actual values in the email message.
- 5. Under Reset Password Template, type the following:
  - **Subject**-the subject of the email message.
  - **Message**-the body of the email message.

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

6. Click Save to save settings.

## Managing Groups and Users

Safe Mobile Workforce enables you to import groups from Active Directory (AD) or add users and groups locally on the server.

**Note:** You can only use either Active Directory to manage users and groups, or manually add users and groups on the server.

#### Importing Groups or Users from Active Directory

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

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

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

#### To importing groups or users from Active Directory:

- **1.** Log on to the server Web console.
- 2. Click Users.

The User Management screen appears.

3. Click Import.

The Import Group or User from Active Directory screen appears.

- 4. Type the group or user information in the search field provided, and click Search.
- 5. Select the groups or users that you want to import from the search result, and then click **Import**.

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

### **Creating a User Account Locally**

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

Before you can create a local user account, make sure that you have disabled the Active Directory integration. See *Configuring Active Directory Settings (Optional)* on page 7-6 for the procedure.

#### To add a user locally:

- 1. Log on to the server Web console.
- 2. Click Users.

The User Management screen appears.

3. Click Add User.

Add A New User screen appears.

- 4. 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.

#### 5. Click Add.

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

# Deploying Safe Mobile Workforce to Mobile Devices

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

See *Configuring Email Notifications* on page 7-10 for the procedure of creating and configuring system notifications.

### Installing Android Client for Safe Mobile Workforce

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

- Open the Google Play store on an Android mobile device and search for Trend Micro.
- 2. In the search results, look for Trend Micro Safe Mobile Workforce and tap Install.
- **3.** Tap **Install** on the access permissions screen that appears and wait while the app downloads and installs, then tap **Open**.
- 4. Type User name, Password and Server address as mentioned in the email, and tap Sign In.

- 5. If a dialog box appears requiring you to enable GPS on the mobile device, tap **OK** and then enable GPS satellites.
  - **Note:** Safe Mobile Workforce requires to use the mobile device location information for any application installed in the user workspace. If you tap **Cancel**, Safe Mobile Workforce will display this pop-up dialog box again the next time you start the application.

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

### Installing iOS Client for Safe Mobile Workforce

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

#### To download the iOS client app for Safe Mobile Workforce:

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

The Safe Mobile Workforce client app Sign In screen appears.

4. Type User name, Password and Server Address as mentioned in the email, and tap Sign In.

A notification appears requiring you to allow the application to use the location.

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

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

# Appendix A

# **Network Port Configurations**

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

This appendix contains the following sections:

- Network Port Configuration for Safe Mobile Workforce Server on page A-2
- Network Port Configuration for Secure Access on page A-4
- Network Ports in Safe Mobile Workforce Architecture on page A-5

# Network Port Configuration for Safe Mobile Workforce Server

Configure the following network ports for Safe Mobile Workforce server:

COMPONENT	Network Ports	DETAILS	REQUIRED OR OPTIONAL	DIRECTION
Manage- ment Web console	HTTPS port 443	Used to access Safe Mobile Workforce management Web console.	Required	Inbound
Mobile cli- ent enroll- ment	HTTPS port 443	Used to enroll mobile client to the server.	Required	Inbound
Mobile cli- ent access	TCP port 5900 to 6156	Used by mobile cli- ent to access Safe Mobile Workforce server.	Required if using NAT. Optional if using IP range.	Inbound
Workspace Manage- ment	TCP port 16509 TCP port 16514	If you are using mul- tiple servers, config- ure this port for accessing work- spaces on second- ary servers. If you are using only one server, this port is not required.	Optional	Inbound

COMPONENT	Network Ports	DETAILS	Required or Optional	DIRECTION
Active Directory	TCP port <b>389</b> (Domain Controller) for Manage- ment console TCP port <b>3268</b> (Global Category) for Management console	Used for user authentication using Active Directory. If you are not using Active Directory to authenticate or import users, these ports are not required.	Optional	Outbound
SMTP server	TCP port <b>25</b>	Used to access email server. If you are not using SMTP server to send emails, this port is not required.	Optional	Outbound
SafeSync port	HTTPS port 443	Used to connect to the SafeSync server. If you are not using SafeSync as file storage, this port is not required.	Optional	Outbound

# **Network Port Configuration for Secure Access**

Configure the following network ports for Secure Access:

COMPONENT	Network Ports	DETAILS	Required Or Optional	DIRECTION
Mobile cli- ent enroll- ment	HTTPS Port 443	Used to enroll mobile client to the server.	Required	Inbound
Connection to Safe Mobile Workforce Server	HTTPS Port 443 TCP Port 5900 to 6156	Used by Secure Access to communi- cate with Safe Mobile Workforce server.	Required	Outbound

# Network Ports in Safe Mobile Workforce Architecture

Figure A-1 shows the network ports used in Safe Mobile Workforce architecture.



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

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