TREND MICRO™

5.3 TREND MICRO™ Virtual Mobile Infrastructure

Administrator's Guide

Centrally-managed workspace for mobile users

Endpoint Security

Document Part No.: APEM57759/170323

elease Date: March 2017

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

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Introducing Virtual Mobile Infrastructure

Chapter 2: Getting Started

Chapter 3: Managing Users and Devices

Chapter 4: Managing Profiles

Chapter 5: Mobile Device Management

Chapter 6: Managing Applications

Chapter 7: Managing Servers

Chapter 8: Managing Reports and Logs

Chapter 9: Administration Settings

Preface

Preface

Welcome to the Trend Micro™Virtual Mobile Infrastructure™ version 5.3 Administrator's Guide. This guide provides detailed information about all Virtual Mobile Infrastructure configuration options. Topics include how to update your software to keep protection current against the latest security risks, how to configure and use policies to support your security objectives, configuring scanning, synchronizing policies on mobile devices, and using logs and reports.

This preface discusses the following topics:

Audience

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

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

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

Virtual Mobile Infrastructure Documentation

The Virtual Mobile Infrastructure documentation consists of the following:

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

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

Tip

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

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

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

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

Chapter 1

Introducing Virtual Mobile Infrastructure

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

This chapter contains the following sections:

About Virtual Mobile Infrastructure

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

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

Why Use Virtual Mobile Infrastructure

Virtual Mobile Infrastructure provides the following benefits:

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

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

What's New in this Release (5.3)?

This release of Virtual Mobile Infrastructure includes the following new features:

Feature	Description
Improved Device Location Accuracy	Improves the response time and accuracy for popular services.
App Reputation Integration	Enables you to upload apps to Trend Micro Mobile App Reputation Service to query app reliability, and improves query results.

Feature	Description
Restrictions for Jailbroken and Rooted Mobile Devices	Provides options to restrict TMVMI client app to run on jailbroken and rooted mobile devices.
Performance Improvement	• Reduces start up time for faster launch of the TMVMI client app. • Enhances rendering quality and reduces bandwidth request for each user workspace. • Increases connection speed between user workspace and mobile device.
Improves Security	Fixes the potential vulnerabilities in VMI server.
Local Workspace Support (Beta)	Introduces support for app deployment and running in local mobile workspace on Android mobile devices.
Mobile Device Management (MDM) Support (Beta)	Provides lightweight MDM features for large enterprises.
Bluetooth Support (Beta)	Supports Bluetooth for selected apps.

What's New in Release 5.2?

This release of Virtual Mobile Infrastructure includes the following new features:

Feature	Description
Mobile Device Verification	Displays the accessing mobile device's information on the administration web console, and allows administrator to approve or reject access of workspace from this mobile device.
Support for Apps with OpenGL on Android	Adds support for the apps that use openGL rendering on Android.
Automatic Audio Quality Adjustment	Automatically adjusts the quality of audio recording and playback according to the network condition.

Feature	Description
Automatic Video Recording Resolution Adjustment	Automatically adjusts the quality of video recording and playback according to the network condition.
Multiple Site Deployment	Supports multiple site deployment for large-scale organizations.
Role Based Administrator	Supports multiple administrator accounts with different roles to manage and view administration web console.
Bluetooth Support	Adds Bluetooth support for Android mobile devices.
IBM Lotus Notes Support	Adds IBM Lotus Notes support for Android and iOS mobile devices.
Performance Improvement	Appropriate function clipping to reduce the unnecessary battery consumption and improve rendering speed.

What's New in Release 5.1?

This release of Virtual Mobile Infrastructure includes the following new features:

Feature	Description
Security Enhancement	Added permission control for SSH login, improved password strength, and other security enhancements for Virtual Mobile Infrastructure server and Secure Access server.
Single Sign On for Web Clips	Added single sign on support for Web clips that use http authentication.
New Default Apps	Added the following new default apps on user workspaces: • Audio Recorder • Video Recorder • Music
Touch ID in iOS Client	Added support for Touch ID on iOS clients to access user workspace.

Feature	Description
Movable Icons	Enabled dragging and moving application icon in user workspaces.
Notifications in Multiple Applications	Added support for showing the notification number in multiple applications in user workspace.
Quick Scan QR Code	Added support for QR code scanning in workspace. User can also enable quick scan QR code icon on mobile client to accelerate scanning process.
Build-in Video Player in iOS Client	Added new default iOS video player to support more video formats.
YouTube Support	Added support to play YouTube videos through Web browser in user workspace.
Office 365 Integration	Added single sign on support for Microsoft Office 365 email server.
Local Applications	Enabled administrators to deploy applications on user mobile devices, outside of user workspace.
Increased Timeout for Inactive Workspaces	Increased timeout period for inactive workspaces, where user does not sign out.
App Usage Data Collection	Enabled Virtual Mobile Infrastructure server to collect app usage information for administrator’s analysis.
Added Watermark	Added watermark on workspaces to help protecting data.
Enhanced User Experience and Server Performance	Made several enhancements to decrease bandwidth usage, reduce login time, improve service performance and user experience and expandability.
Updated UI screens on Administration Web Console	Added or modified some configurations on System Settings and Email Notifications screens on administration Web console.
Updated UI Screens on Mobile Client App	Updated Settings screen on mobile client app.

What's New in Release 5.0?

This release of Virtual Mobile Infrastructure includes the following new features:

Feature	Description
Operating System Upgrade	Upgraded the supported Android operating system to 5.1 for the virtual mobile workspace. As a result, graphics, Web rendering libraries and built-in apps are also upgraded.
Windows 10 Mobile Support	Added support for Microsoft's Windows 10 Mobile operating system on Virtual Mobile Infrastructure clients.
SELinux support	Added support for Security-Enhanced Linux (SELinux) on the Virtual Mobile Infrastructure server.
Audit Logs	Added audit logs to record all administrator operations on the Virtual Mobile Infrastructure Web console.
Client Certificate Authentication	Verifies certificates used by the mobile client installed on an Android or iOS device to sign in.
Usage alerts for Users and Administrators	Sends alerts to administrators when there is insufficient CPU, memory or storage space on the Virtual Mobile Infrastructure server. Sends alerts to administrators when users have insufficient space in their virtual mobile workspace and enables administrators to send email notifications to users.
Single Network Card Support	Requires only one network card for installing the Virtual Mobile Infrastructure server.
Quick Enrollment	Provides quick response (QR) code in invitation letters. When a user scans the QR code, the client automatically obtains the user's server IP address and user name for registration.
Audio and Video Support	Added support for recording video files and playing both audio and video files on Virtual Mobile Infrastructure clients.
Virtual Home Key for Android Clients	Provides a virtual home key on android clients for users to immediately go back to the launcher.

Feature	Description
License Seat Control	Limits the number of seats available for each license.
Hide Application Icons in User Workspace	Enables administrators to hide application icons on user workspaces. However, users can still be able to use the hidden application.
Network Connection Indicator	Adds a status icon on user mobile devices to show the network connectivity with the server.
Status Feedback During Login Process	Adds animation during the login process to show the working status to the user.

What's New in Release 3.0?

This release of Virtual Mobile Infrastructure includes the following new features:

Feature	Description
Changed Product Name	Adapts a new product name; Virtual Mobile Infrastructure.
Enforced Signin Security Level	Enables administrators to enforce signin security levels restrictions for user workspace on mobile device.
Updated Invitation Email Template	Includes a URL in email template to allow users to add server IP address and user name in the app.
Instant Logout	Allows users to immediately signout from the app, without waiting for server's response.

What's New in Release 2.1?

This release of Safe Mobile Workforce includes the following new features:

FEATURE	DESCRIPTION
Diagnosis Information	Collects diagnosis information about the mobile device and the network that is used to connect to the user workspace.
Enhanced User Experience	Reduces response time, further optimizes bandwidth and reduces the time required to prepare a workspace.
VIP Setting for Users	Introduces VIP settings for users who need uninterrupted access to make sure that the server does not disable workspace if the user disconnects.
Improved Notifications for iOS	Enables iOS client app to instantly display notification messages from the workspaces apps on the user workspace.
User Event Logs	Adds user event logs on the administration Web console.
Storage Size for User Workspaces	Enables administrators to define the storage size for users.
Kiosk Mode	Enables administrators to configure workspace to start the specified app automatically after user logs on.
Lock Screen Setting on User Workspace	Enables users to disable screen lock on user workspaces.
OpenLDAP Support	Supports configuring OpenLDAP with Safe Mobile Workforce.
Enforced Signin Security Level	Enable administrators to enforce signin security levels for user workspace.

Note

The product name Safe Mobile Workforce was changed to Virtual Mobile Infrastructure in version 3.0.

What's New in Release 2.0?

This release of Safe Mobile Workforce includes the following new features:

Feature	Description
Enhanced Server Performance	Provides improved server performance when managing a large number of users.
Enhanced User Experience	Provides improved support for reading documents. Some minor bugs are also fixed in Safe Mobile Workforce client application.
Native Launcher	Includes a bypass application launcher in Safe Mobile Workforce client application to render the workspace application list as part of the client interface. The native launcher improves the response time and log on process.
Built-in Camera and Gallery Applications	Includes the Camera and Gallery applications in the user workspace.
Easy Application Upload	Provides a separate application (**TMSMW App Push**) for the administrators to upload applications to the Safe Mobile Workforce server. **Note** The application named **TMSMW App Push** was renamed to **TMVMI App Push** in version 3.0.
Re-branding Tool	Includes a tool to customize the product branding items, such as product name, logo, banner, images, server address and other branding items on the Safe Mobile Workforce server and in the client app.

Note

The product name Safe Mobile Workforce was changed to Virtual Mobile Infrastructure in version 3.0.

What's New in Release 1.5?

The following are the new features in Safe Mobile Workforce v1.5:

FEATURE	DESCRIPTION
Camera Support	Added support for camera on iOS mobile devices for the applications that are installed on the user workspaces.
Windows Client App Enhancement	Enhanced features and improved Windows mobile client application performance.
Increased Concurrent Sessions Support	Increased the concurrent sessions supported by the server.
Supports High Availability	Added support for High Availability (HA) to ensure uninterrupted service.
Reduced Bandwidth Consumption	Reduced Internet bandwidth requirements for the client app to reduce data usage and improve user experience.
Added Options to Choose Optimize Quality or Speed	Provides option to choose between optimize quality or speed on mobile devices, to optimize the Internet bandwidth and improve user experience.
Bypass Proxy Settings	Added support for bypass proxy settings for workspaces.
OAuth 2.0 Authentication Support	Added OAuth 2.0 Authentication support for user enrollment.
User Logon Process Enhancement	Enhanced the user log on process to provide better user experience.
User Status Reset Setting	Added option to configure time after which the server resets the user status from idle to offline.
Email Notification	Added an email notification on real mobile device to notify users for the email received on the user workspace.
Client Version Verification	Added a verification for the Safe Mobile Workforce client software version before enroll. If the client software version does not match the required version, the client will not be enrolled.

Note

The product name Safe Mobile Workforce was changed to Virtual Mobile Infrastructure in version 3.0.

What's New in Release 1.1?

The following are the new features in Safe Mobile Workforce v1.1:

Feature	Description
Integration with Trend Micro Control Manager	The integration with Trend Micro Control Manager enables you to log on to the Control Manager Web console to monitor Safe Mobile Workforce usage and system status. You can also deploy Safe Mobile Workforce license from the Control Manager Web console.
Single Sign On	Includes the app-wrapper technology to prepare applications for single sign on, without involving the app developer for processing.
Client app for Windows 8	Introduces Safe Mobile Workforce client app for Windows 8 mobile devices.
Show/Hide Built-in Apps	Enables you to show or hide the following built-in apps on the user workspaces: • Email • Browser • Downloads • Calender • Contacts • Calculator
Camera Support (Android Only)	Enables the camera support for applications installed on the user workspaces.
Improved Client Performance	Significantly improves the mobile client performance by optimizing mobile device's memory and Internet bandwidth to provide the better user experience.
Improved Application Support	Improves application support for more Android apps on a user workspace.
Improved Authentication Security	Introduces restriction settings for unsuccessful sign on attempts.

FEATURE	DESCRIPTION
Disable Screenshots (Android Only)	Restricts users from taking screenshots of their workspaces on their mobile devices.

Note

The product name Safe Mobile Workforce was changed to Virtual Mobile Infrastructure in version 3.0.

Architecture of Virtual Mobile Infrastructure

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

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

Single Server Installation Model

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

Note

Trend Micro strongly recommends deploying Secure Access in your environment to enable mobile clients to access Virtual Mobile Infrastructure Server via Internet. See *Why Use Secure Access on page 1-18* for more information.

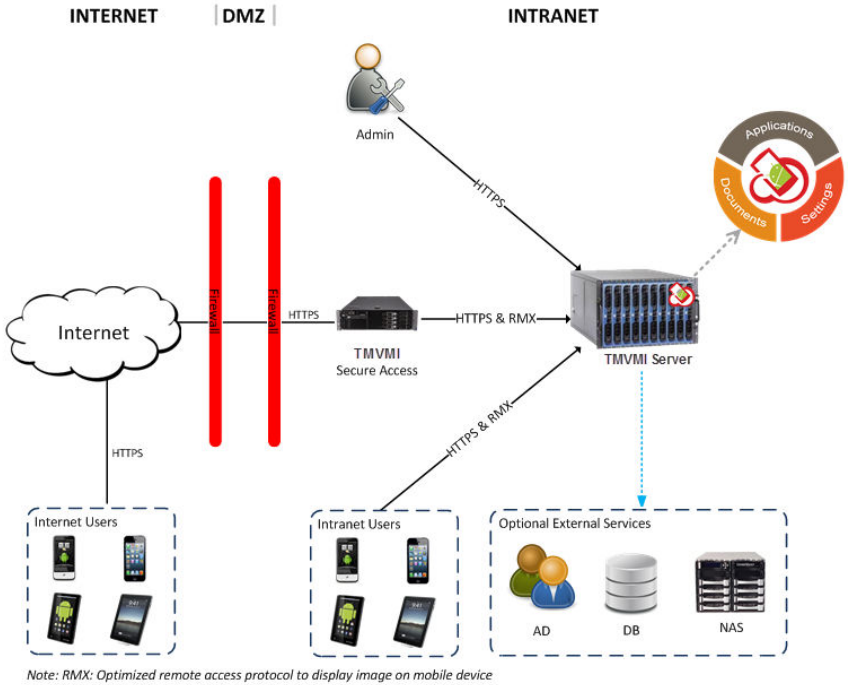


FIGURE 1-1. Trend Micro Virtual Mobile Infrastructure Single Server Installation Model

Multiple Server Installation Model

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

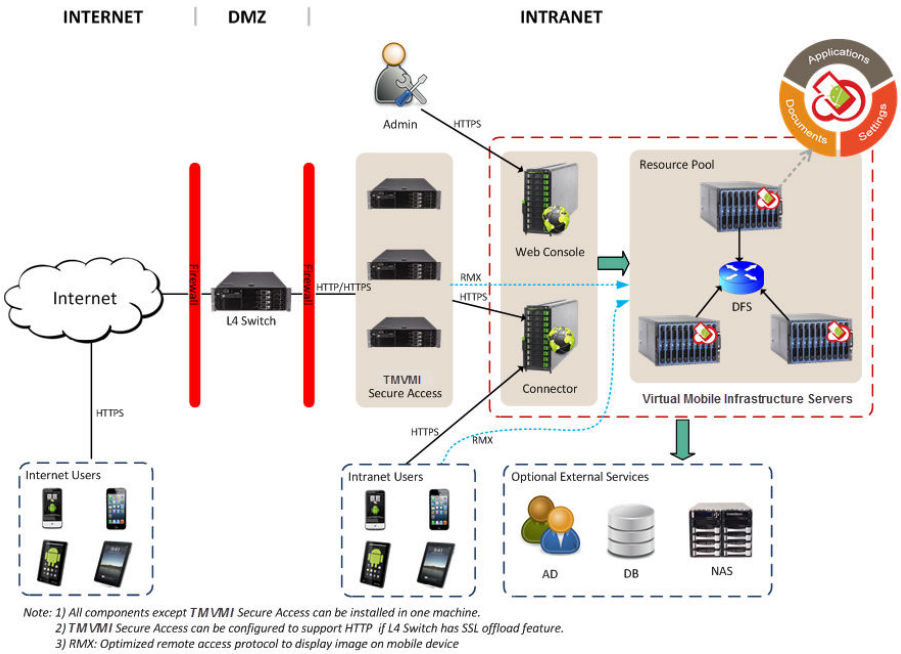


FIGURE 1-2. Trend Micro Virtual Mobile Infrastructure Multiple Server Installation Model

Multiple Sites Deployment Model

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

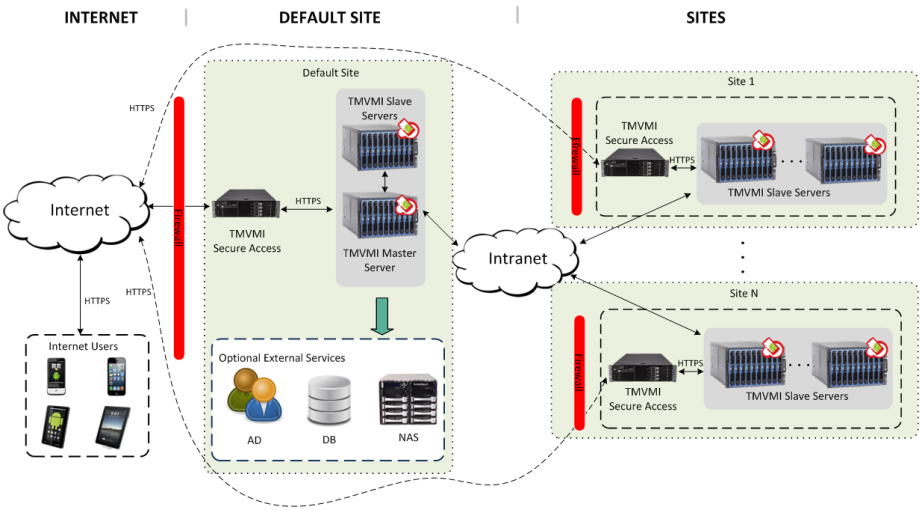


FIGURE 1-3. Trend Micro Virtual Mobile Infrastructure Multiple Site Deployment Model

Components of Virtual Mobile Infrastructure

The Virtual Mobile Infrastructure system includes the following components:

TABLE 1-1. Virtual Mobile Infrastructure Components

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Virtual Mobile Infrastructure Server	The Virtual Mobile Infrastructure Server contains Web Console, Web Service, Controller and Resource Pool. • Web console provides central management console for administrator. • Web service manages user logon, logoff and the connection to user's workspace. • Controller allows Web console to manage a resource pool. • Resource pool hosts workspaces. Each workspace runs as a Virtual Mobile Infrastructure instance.	Required
Virtual Mobile Infrastructure Mobile Client Application	The mobile client application is installed on the mobile devices. The client application connects with the Virtual Mobile Infrastructure server to allow users to use their workspaces hosted on the server.	Required
Secure Access	The Virtual Mobile Infrastructure Secure Access enables mobile clients to access Virtual Mobile Infrastructure server via Internet, and provide Mobile Device Management (MDM) services. See *Why Use Secure Access on page 1-18* for more information.	Stongly recommended
Active Directory	The Virtual Mobile Infrastructure server imports groups and users from Active Directory.	Optional

Component	Description	Required or 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.
- You can use mobile device management (MDM) features in Virtual Mobile Infrastructure, which can only be used through Secure Access.

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

- You need only one network card, if you configure the Internet mobile devices and Secure Access in different networks.

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

Chapter 2

Getting Started

This chapter contains the following sections:

Accessing Virtual Mobile Infrastructure Administration Web Console

To access the Virtual Mobile Infrastructure Web console:

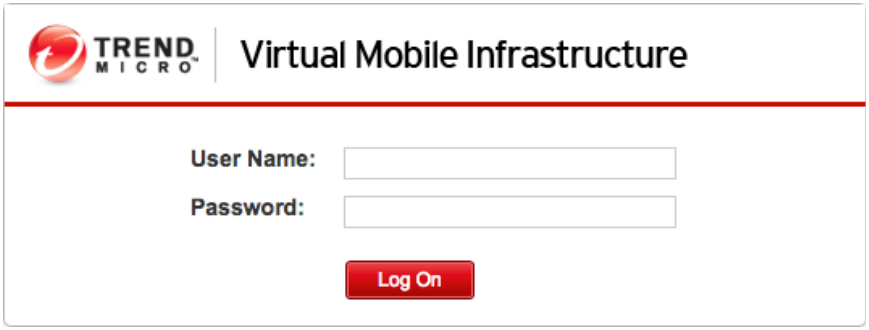
Procedure

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

   https://<Virtual Mobile Infrastructure_domain_name_or_IP_address>:8443

   The following screen appears.

FIGURE 2-1. Virtual Mobile Infrastructure Web console logon screen



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

Note

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

Make sure that you change the administrator password after your first sign in. Refer to the topic *Changing Administrator Account Password on page 9-5* for the procedure.

The Dashboard Screen

The **Dashboard** screen displays first when you access the Virtual Mobile Infrastructure Web console. This screen provides the usage overview and the server's system status.

The **Dashboard** screen is divided into two tabs:

- **Usage Overview**–shows the highlights of the workspace usage and the application usage. This tab displays the following information:
  - **Top 5 Users By Online Time**–displays the top (5) most active users who have accessed their workspace for the longest period of time.
  - **Users Status**–displays the current users' statuses. The four user statuses are:
    - **Active**–shows that the user is currently connected to the server, and is accessing the workspace.
    - **Idle**–shows that the user is connected to the server, but is not currently accessing the workspace.
    - **Offline**–shows that the user is disconnected from the server.
    - **Disabled**–shows that the user account has been disabled and the user cannot access the server.
  - **Top 5 Applications Used**–shows the top five (5) most frequently used applications in terms of:
    - **Times Launched**–shows the top five (5) application that are launched by all the users combined.
    - **Duration**–shows the top five (5) application that are used by all the users combined for the longest period (in minutes).
  - **Top 5 Web Clips Used**–shows the top five (5) most used Web clips.
- **System Status**–shows the system resource usage status. In this category, you can view:
  - **Storage Usage of All Servers**–shows the disk storage status of all Virtual Mobile Infrastructure servers.

- **Memory Usage of All Servers**–shows the current memory usage status of all Virtual Mobile Infrastructure servers.
- **CPU Usage of All Servers**–shows the CPU usage status of all Virtual Mobile Infrastructure servers. This information is updated every five minutes since the servers started running.

Chapter 3

Managing Users and Devices

This chapter contains the following sections:

User Management in Virtual Mobile Infrastructure

The **User Management** screen enables you to import users and groups from the Active Directory (AD), and enable or disable user accounts. This screen also enables you to create, modify, and delete user accounts locally.

Managing Groups and Users

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

Note

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

Importing Groups or Users from Active Directory

Before importing groups or users from Active Directory, make sure that you have already configured the Active Directory settings. See *Configuring LDAP Settings (Optional) on page 9-6* for the procedure.

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

Procedure

1. Click **Import**.

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

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

3. Select the site in which you want to import users.

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

Note

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

Creating a User Account Locally

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

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

Disabling or Enabling a User

Use the **User Management** screen to disable or enable users in Virtual Mobile Infrastructure.

Procedure

1. In the user list on the left side of the screen, click the user name that you want to enable or disable.
2. Do one of the following:
   - To disable user, click **Disable User**, and then click **OK** on the pop-up dialog box to confirm.
   - To enable user, click **Enable User**.

Enabling or Disabling VIP Setting for a User

To save resources, Virtual Mobile Infrastructure disables the inactive workspaces after the user is disconnected from the network. This means, to be able to use the workspace next time, user may need to wait a few seconds to connect to the workspace. To avoid this delay, you can enable the VIP setting for a user that needs uninterrupted access to the workspace.

CAUTION!

Use this setting with caution, because it will reserve resources on the server until the user disconnects manually, which, in turn, limits the server capacity.

Note

See *Configuring Mobile Client Settings on page 9-8* to configure the number of users you can set as VIP.

Use the **User Management** screen to enable or disable VIP setting for users in Virtual Mobile Infrastructure.

Procedure

1. In the user list on the left side of the screen, click the user name for which you want to enable or disable VIP setting.
2. Click **Enable** or **Disable** before **VIP**, and then click **OK** on the pop-up dialog box to confirm.

Wiping User Workspace

If a user does not need to use the workspace anymore, you can wipe the user workspace to delete all of the data saved on the workspace.

Use the **User Management** screen to wipe user workspace in Virtual Mobile Infrastructure.

CAUTION!

This procedure will delete all the user data from the workspace. Once the data is removed, it cannot be recovered.

Procedure

1. In the user list on the left side of the screen, click the user name for which the workspace you want to wipe.
2. To wipe the user workspace, click **Wipe** before **Wipe workspace**, and then click **OK** on the pop-up dialog box to confirm.

Resending Invitation to a User

Use the **User Management** screen to resend invitation to users in Virtual Mobile Infrastructure.

Procedure

1. In the user list on the left side of the screen, click the user name whom you want to resend the invitation.
2. Click **Resend Invitation**, and then click **OK** on the confirmation pop-up dialog box.

Sending Usage Alerts to Users

When the storage in a user workspace occupies more than 80% of its capacity, Virtual Mobile Infrastructure shows a warning message on the **Dashboard** screen.

You can modify the warning message that Virtual Mobile Infrastructure sends to the user. See *Configuring Email Notifications on page 9-12* for details.

Procedure

1. Navigate to the **User Management** screen and click **Alert User**.
2. On the **Alert Users List** screen, select the user to whom you want to send a usage alert in an email message.
3. Click **Send Mail**.

   Virtual Mobile Infrastructure sends an email to alert the user about current and remaining workspace storage.

Changing User or Group Profile

Use the **User Management** screen to change user or group profile in Virtual Mobile Infrastructure.

Procedure

1. Click the user name whose profile you want to change.
2. Click **Change**.

   The **Edit Group** dialog box pops up.
3. Select one of the following:
   - **Profile**
     - **Inherit from parent group**
     - **Specified**
   - **Site**
4. Click **Save** on the **Edit Group** dialog box.

Delete a User or a Group

Note

You cannot delete any Active Directory group or a user if it belongs to any group under **Root**.

Use the **User Management** screen to delete a user or a group in Virtual Mobile Infrastructure.

Procedure

1. Click the user or the group name that you want to delete.
2. Click **Delete**.

Viewing Application Usage for a User

Use the **User Management** screen to see the application usage for a user in Virtual Mobile Infrastructure.

Procedure

1. In the user list on the left side of the screen, click the user name for which you want to see the application usage.

   The **Applications Used** table at the bottom of the screen lists all the applications used by the user.

   Click on an application name to see the usage details for the application.

   Note

   To see the app usage duration, enable this setting on **System Settings** > **Advanced**.

Exporting User Device ID

Procedure

1. Navigate to the **User Management** screen, and do one of the following:

   - To export device ID for all users, click **Export Device ID** without selecting any user.
   - To export device ID for specific users, select user names from the list whose device ID you want to export, and then click **Export Device ID**.

2. Save file on your computer.

   Virtual Mobile Infrastructure exports the user device ID in a file on the local computer.

Searching Users

On the **User Management** screen, you can search using a name, email addresses or a keyword.

Procedure

1. In the search field **Search in selected group**, type the user name or the email address to search.
2. Press **Enter**.

Device Management in Virtual Mobile Infrastructure

The **Device Binding Management** screen enables you to bind mobile devices with certain user accounts. Whenever a users attempts to sign in from a mobile device, the **Device Binding Management** screen displays the mobile device information and provides you an option to approve or disapprove the workspace access from the mobile device.

Enabling or Disabling Device Binding

Binding mobile devices with user accounts will allow users to access mobile devices from these certain mobile devices. You can bind more than one mobile devices with one user account.

Use the **Device Binding Management** screen to bind mobile devices with user accounts.

Procedure

1. Select **Enable Device Binding** to enable this option. Clear to disable.

Importing Mobile Devices

Whenever a users attempts to sign in from a mobile device, the **Device Binding Management** screen displays the mobile device information and provides you an option to approve or disapprove the workspace access from the mobile device. However, you can also import users to the list.

You can import the device information TMVMI server before user login, the device in the list will be bind to the user. The device can login directly. Note: Import devices only support android platform. The file format is user name, IMEI1 User name, IMEI2 … You need to refresh the screen to display the information that you just imported.

Use the **Device Binding Management** screen to import mobile devices and bind with user accounts.

Procedure

1. Select **Enable Device Binding** to enable this option.
2. Click **Import Devices**.

   Virtual Mobile Infrastructure only supports importing Android mobile devices and `csv` or `txt` file format.

   The **Import Devices** screen appears.
3. Click **Browse** and select a `csv` or `txt` file that you want import.

   Note

   The imported file must contains the information in the following format:

   ```
   Username1,IMEI1
   Username2,IMEI2
   Username3,IMEI3
   ...
   ```

   ---
4. Click **Import** .

Binding or Unbinding Mobile Devices

Use the **Device Binding Management** screen to bind or unbind mobile devices in Virtual Mobile Infrastructure.

Procedure

1. On the mobile device list on the left side of the screen, click the mobile device that you want to bind or unbind.
2. Do one of the following
   - To bind a mobile device, click **Bind Device**, and then click **OK** on the pop-up dialog box to confirm.
   - To unbind a mobile device, click **Unbind Device**, and then click **OK** on the pop-up dialog box to confirm.

Deleting Mobile Device

Note

User the **Device Binging Management** screen to delete mobile devices in Virtual Mobile Infrastructure.

Procedure

1. Click the device record that you want to delete.
2. Click **Delete**.

Chapter 4

Managing Profiles

This chapter contains the following sections:

Profiles in Virtual Mobile Infrastructure

Virtual Mobile Infrastructure supports two types of profiles: VMI profiles for virtual mobile workspace, and sandbox profiles for apps that are installed on mobile devices.

Virtual Mobile Infrastructure uses profiles to let you set the default system settings and the applications for the newly added users. You can create multiple profiles and apply them to different users and groups, depending on the requirements.

Creating a VMI Profile

Use the **Profile Management** screen to create VMI profiles in Virtual Mobile Infrastructure.

Procedure

1. Click **Add**.
2. Under **Step 1: Basic Information** section, provide the following information:
   - **Profile name**
   - **Description**
   - **Profile type**–select **Workspace** to create a profile for virtual mobile workspace.
   - **Copy from**–select a previously created profile whose settings you want to copy. By default, Virtual Mobile Infrastructure copies settings from the **Default Profile**.
   - **Site**–select a site that this profile will able to.
   - **Storage limit**–set a storage limit for the profile.
3. Click **Next**.
4. Under **Step 2: Workspace System Settings** section, do the following:
   - Select a wallpaper from the list. To upload a new wallpaper to the list, click the + icon, and then select a jpg, png or a gif file.

- Select **Enable watermark in workspace**, and then type the text into the field provided, to display the text as watermark on user workspaces.

> **Note**
>
> If you do not type any text into the field provided, the client app shows the user name and the login time stamp as watermark on user workspaces.

5. Click **Next**.
6. Under **Step 3: Applications** section, do the following:
   a. Click **Add**.

      The **Add Allowed Applications** screen pops up.

   b. Select the applications you want to add to this profile, and then click **Add**.

> **Note**
>
> You can also delete an application from the list by selecting the application and clicking **Remove**.

7. Click **Next**
8. Under **Mobile Device Management (MDM) Settings** section, select **Enforce Mobile Device Management** to enable management for mobile devices.

> **Note**
>
> To use MDM features, you must configure MDM settings for Android and iOS mobile devices. Navigate to **MDM** > **Device Management** > **MDM Settings** to configure MDM settings for mobile devices.

9. Click **Save**.

Creating a Sandbox Profile

Use the **Profile Management** screen to create sandbox profiles in Virtual Mobile Infrastructure.

Procedure

1. Click **Add**.
2. Under **Step 1: Basic Information** section, provide the following information:
   - **Profile name**
   - **Description**
   - **Profile type**–select **Sandbox** to create a profile for virtual mobile workspace.
   - **Settings**–select the options that you want to configure for the sandbox profile.
3. Click **Next**.
4. Under **Step 2: Workspace System Settings** section, do the following:
   - Select a wallpaper from the list. To upload a new wallpaper to the list, click the **+** icon, and then select a jpg, png or a gif file.
   - Select **Enable watermark in workspace**, and then type the text into the field provided, to display the text as watermark on user workspaces.

     Note

     If you do not type any text into the field provided, the client app shows the user name and the login time stamp as watermark on user workspaces.

     ---
5. Click **Next**.
6. Under **Step 3: Applications** section, do the following:
   a. Click **Add**.

      The **Add Allowed Applications** screen pops up.

   b. Select the applications you want to add to this profile, and then click **Add**.

> **Note**
>
> You can also delete an application from the list by selecting the application and clicking **Remove**.

7. Click **Next**

8. Under **Mobile Device Management (MDM) Settings** section, select **Enforce Mobile Device Management** to enable management for mobile devices.

> **Note**
>
> To use MDM features, you must configure MDM settings for Android and iOS mobile devices. Navigate to **MDM** > **Device Management** > **MDM Settings** to configure MDM settings for mobile devices.

9. Click **Save**.

Changing Profile Order

Use the **Profile Management** screen to change profile order in Virtual Mobile Infrastructure.

Procedure

1. Click **Change Order**.

   The **Change Profile Order** screen pops up.

2. Click and drag the profiles to rearrange the profiles in the desired order.

3. Click **Save** on the **Change Profile Order** screen, and then click **OK** on the confirmation dialog box.

Deleting Profiles

Virtual Mobile Infrastructure uses the **Default Profile** for all users that do not use any specific profile. The **Default Profile** cannot be deleted.

Use the **Profile Management** screen to delete profiles in Virtual Mobile Infrastructure.

Procedure

1. Check the **Applied Users/Groups** column for the profile you want to delete, to make sure that the profile is not applied to any user or a group. If the profile is applied to any user or a group, change the group profile. See *Configuring LDAP Settings (Optional) on page 9-6* for the procedure.
2. Select the profiles that you want to delete.
3. Click **Delete**.

Kiosk Mode in Virtual Mobile Infrastructure

The Kiosk Mode in Virtual Mobile Infrastructure automatically launches the specified application automatically after the user signs in.

Enabling or Disabling Kiosk Mode

Use the **Profile Management** screen to enable or disable the Kiosk Mode for a profile in Virtual Mobile Infrastructure.

Procedure

1. On the **Profile Management** screen, click the profile on which you want to enable or disable the Kiosk Mode.
2. Click **Edit**.
3. Do one of the following:

- To enable Kiosk Mode, click the
  
  icon on an application. This application will be launched automatically after the user logs on to the workspaces.
- To disable Kiosk Mode, click the
  
  icon on the application that is configured as the single app.

4. Click **Save**.

Chapter 5

Mobile Device Management

Virtual Mobile Infrastructure provide lightweight security solution for your mobile devices. Administrator can remote lock, locate or wipe the mobile devices to protect sensitive data using security policies.

This chapter contains the following sections:

Configuring MDM Settings

Trend Micro Virtual Mobile Infrastructure's mobile device management (MDM) function enables you to manage and monitor any corporate- or employee¬owned mobile device that accesses business critical data.

Important

You MUST install Secure Access to use MDM features in Virtual Mobile Infrastructure.

Important

Before configuring these settings, you must generate an Apple Push Notification service (APNs) certificate, which is required for managing iOS mobile devices.

If you need assistance regarding the procedure of generating an APNS certificate for MDM, contact Trend Micro technical support.

Use the **MDM** > **Device Management** screen to configure MDM settings in Virtual Mobile Infrastructure

Procedure

1. On the **System Settings** screen, click the **Mobile Client** tab.
2. Under the **Secure Access Settings**, make sure the following information is configured:
   - **Domain name or IP address**

     Note

     If Secure Access is connected to a gateway or an external router, type the IP address or domain name of the gateway or the router instead of the IP address of Secure Access.

   - **Port number**
3. Open **Terminal** on the Virtual Mobile Infrastructure server, log on with the user account: **root**, and do the following:

a. Type the following command to generate a new SSL certificate for Secure Access:

```
python /vmi/gateway/gen_cert.py <xxxx>
```

Note

Replace <xxxx> with the Domain name or IP address that you configured in Step 1 of this procedure.

b. Type the following command to restart Secure Access service:

```
service vmigateway restart
```

4. On the **Device Management** screen, click **MDM Setting**, type the intranet IP address and port number of Secure Access server, and then upload an APNs certificate.
5. Click **Save**.

Mobile Device Enrollment

If you have configured Virtual Mobile Infrastructure user workspace or sandbox profile to enforce MDM, then the mobile device agent (**TMVMI Client**) will require users to enroll their mobile devices during the login process.

Enrolling an Android Mobile Device

When you sign in to the user workspace using user name and password, the **TMVMI** client software requires you to activate **Device Administrator** on your mobile device. If you do not activate **Device Administrator**, you will not be able to sign in to the workspace.

Enrolling an iOS Mobile Device

To manage iOS mobile devices from the Virtual Mobile Infrastructure, you must install a provisioning profile on the mobile devices. This provisioning profile must identify you

(through your development certificate) and your device (by listing its unique device identifier).

Procedure

1. Start the **TMVMI** client app on the mobile device, type user name and password to sign in.

   Note

   A dialog box may pop up requiring you to install Root CA configured for the Virtual Mobile Infrastructure. If you do not see this dialog box, skip steps 4 to 6 and proceed to step 7.

2. Tap **OK**.

   The **Install Profile** screen for **TMVMIMDM-CA** displays.

3. On the **Install Profile** screen, tap **Install**, and then on the **Warning** screen, tap **Install**.

4. After the profile is installed, click **Done** on the **Profile Installed** screen.

5. If required, type the user name and password in the fields provided, and tap **Log In**.

   The **Install Profile** screen for **MDM Enrollment Profile** displays.

6. On the **Install Profile** screen, tap **Install**, and then tap **Install Now** on the confirmation pop-up dialog box.

7. If the mobile device requires a passcode, type your passcode on the **Enter Passcode** screen that appears, and then tap **Done**.

   The **Installing Profile** screen appears.

8. Tap **Install** on the **Warning** confirmation screen.

   The profile installation process begins. After the process is completed, the **Profile Installed** screen displays.

9. Tap **Done**.

Mobile Device Management

Virtual Mobile Infrastructure enables you to perform different tasks on the mobile devices from the **Devices Management** screen.

Exporting Server Data

You can export data for further analysis or a backup from the **Managed Devices** tab on **Device Management** screen.

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.
3. Select the mobile device group from the device tree whose data you want to export.
4. Click **Export**.
5. If required, click **Save** on the pop-up that appears to save the `.zip` file on your computer.
6. Extract the downloaded `.zip` file content and open the `.csv` file to view the mobile device information.

Editing Mobile Device Information

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.

2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.

3. Click the mobile device from the device tree whose information you want to edit.

4. On the Device Details, screen, click **Edit Device**.

5. Update the information in the following fields:

   - **Device Name**—the name of the mobile device to identify the device in the device tree.
   - **Device Ownership**—the name of the group to which the mobile device belongs from the drop-down list.
   - **Asset Number**—type the asset number assigned to the mobile device.
   - **Description**—any additional information or notes related to the mobile device or the user.

6. Click **Save**.

Deleting a Mobile Device

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.

2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.

3. On the **Managed Devices** tab, click the mobile device from the device tree that you want to delete.

4. Click **Delete** and then click **OK** on the confirmation dialog box.

The mobile device is deleted from the mobile device tree, and is no longer enrolled with the Virtual Mobile Infrastructure server.

Resetting Password Remotely

If a user has forgotten the power-on password, you can remotely reset the password and unlock the mobile device from the Virtual Mobile Infrastructure. After the mobile device is successfully unlocked, the user is able to change the power-on password.

Removing the Password for an iOS Mobile Device

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.
3. Select the mobile device from the tree, and then click **Password Reset**.
4. Click **OK** on the confirmation dialog box that appears. The power on password for the selected iOS mobile device will be removed.

Updating Mobile Device Information

The Virtual Mobile Infrastructure server automatically obtains the device information from managed mobile devices at scheduled intervals and displays the device information on the **Devices** screen.

You can update the device information of a managed device on the **Managed Devices** tab before the next scheduled automatic update.

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.

3. Select the mobile device from the device tree whose information you want to update.

4. Click **Update**.

Lost Device Protection

If a user loses or misplaces the mobile device, you can remotely locate, lock or delete all of the data on that mobile device.

Locating a Remote Mobile Device

You can locate the mobile device through the wireless network or by using mobile device's GPS. The Virtual Mobile Infrastructure server displays the mobile device location on Google Maps.

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.

2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.

3. Click the mobile device from the device tree that you want to locate.

4. Click **Device Locate** and then click **OK** on the confirmation dialog-box.

   The Virtual Mobile Infrastructure tries to locate the mobile device and displays the Google Maps link on the **Remote Locate Device** screen.

5. Click the Google Maps link on the **Remote Locate Device** screen to see the mobile device's most recent GPS location on the map.

Locking a Remote Mobile Device

You can send lock instruction from the administration web console to remotely lock a mobile device.

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.
3. Click the mobile device from the device tree that you want to lock.
4. Do one of the following:

   For an Android mobile device, click **Remote Lock** and then click **OK** on the confirmation dialog-box.

   For an iOS mobile device, click **Remote Lock** then type the user's phone number and a message that you want to send to the user, and then click **Lock**.

   The **Success** message displays on the screen if the lock command is generated successfully.

Wiping a Remote Mobile Device

WARNING!

Be careful when you use this feature as the action CANNOT be undone. All data will be lost and irrecoverable.

You can remotely reset the mobile device to factory settings and clear the mobile device internal memory/SD card. This feature helps ensure the security of the data for lost, stolen or misplaced mobile devices.

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Device Management** from the menu bar.

   The **Device Management** screen displays.
3. Click the mobile device from the device tree that you want to wipe.
4. Click **Remote Wipe**.

   The **Remote Wipe Device** screen displays.
5. Click **Remote Wipe Device**.

   All data is deleted from the mobile device and the Mobile Device Agent is unregistered from the server.

Policies in Virtual Mobile Infrastructure

You can configure security policies for a user or a group on the Virtual Mobile Infrastructure server. These policies apply to all mobile devices that belong to the user account in the group.

Virtual Mobile Infrastructure provides the following policies:

- Wi-Fi Policy
- Password Policy

Password Policy

The password policy prevents unauthorized access to data on mobile devices.

To configure password policy settings, click **MDM** > **Policies**, then click the policy name, and then click **Password Policy** from the left-menu.

Wi-Fi Policy

Wi-Fi Policy enables you to deliver your organization's Wi-Fi network information to Android and iOS mobile devices; including the network name, security type and password.

To configure Wi-Fi policy settings, click **MDM** > **Policies**, then click the policy name, and then click **Wi-Fi Policy**.

Managing Policies

Virtual Mobile Infrastructure enables you to quickly create a policy using the default security policy templates.

Use the **Policy** screen to create, edit, copy or delete security policies for mobile devices.

Creating a Policy

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Policies** on the menu bar.

   The **Policy Management** screen displays.
3. Click **Add**.

   The **Create Policy** screen displays.
4. Configure the following fields:
   - **Policy Name**
   - **Description**
   - **Platform**: Select the Android or iOS from the drop-down list.
   - **Copy From**: Select a previously created profile whose settings you want to copy. By default, Virtual Mobile Infrastructure copies settings from the Default Policy.

5. Click **Next**.
6. Select the user or the ownership to whom you want to assign this policy.

Important

If you assign the policy to a user as well as to the ownership, the user MUST belong to both the groups to receive this policy. If the user belongs to only one of these groups, the policy will not be applied to such user.

7. Click **Next**.
8. Configure the policies that you want to apply to the related mobile devices.
9. Click **Save**.

Editing a Policy

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Policies** on the menu bar.

   The **Policy Management** screen displays.
3. In the policy list, click the policy name whose details you want to edit.

   The **Edit Policy** screen displays.
4. Modify the policy details and then click **Save**.

Deleting Policies

You cannot delete the **Default** policy and any policy that is applied to a group. Make sure to remove the policy from all the groups before deleting a policy. See *Editing a Policy on page 5-12* for the procedure to modify the policy.

Procedure

1. Log on to the Virtual Mobile Infrastructure administration web console.
2. Click **MDM** > **Policies** on the menu bar.

   The **Policy Management** screen displays.
3. Select the policy that you want to delete, and then click **Delete**.

Policy Deployment Statuses

The **Policy Management** screen displays the current status of each policy.

The following are the two statuses that the **Policy Management** screen displays:

- **Pending**: This column displays the number of mobile devices to which this policy is required to be deployed but has not yet been deployed.

  Click on the number displayed under **Pending** column to see the details.
- **Deployed**: This column displays the number of mobile devices to which this policy has already been deployed.

  Click on the number displayed under **Deployed** column to see the details.

Chapter 6

Managing Applications

This chapter contains the following sections:

Workspace Applications

Virtual Mobile Infrastructure enables you to upload Android applications and Web clips to the server. Using these applications, you can later create profiles for the users, which would install these applications on to the users' workspaces.

Uploading Applications to Server

Use the **Application Management** screen to upload applications on Virtual Mobile Infrastructure server.

Procedure

1. Click **Add Application**.

   The **Add Application** screen pops up.

2. Click **Browse** and select an apk file.

   The server starts uploading the selected application (apk) file. The server also scans the application file for the security risk and displays its risk level.

3. Click **OK**.

4. If **Edit Application** screen appears, edit the application details as required, and click **Done**.

Adding a Web Clip to the Server

Use the **Application Management** screen to add Web clips on Virtual Mobile Infrastructure server.

Procedure

1. Click **Add Web Clip**.

   The **Add Web Clip** screen pops up.

2. Type the URL and click **Verify URL**.

   The server starts verifying the URL. After it completes, the **Display name** and **Description** fields appear.

3. Type a name for the URL in the **Display name** field and a description in the **Description** field.

4. Click **OK**.

The Web clip appears in the applications list.

Deleting an Application or a Web Clip from the Server

Use the **Application Management** screen to delete applications or Web clips on Virtual Mobile Infrastructure server.

Procedure

1. Select the applications or Web clips you want to delete, and then click **Delete**.

2. Click **OK** on the confirmation dialog box.

Enabling or Disabling Default Applications in User Workspace

Use the **Application Management** screen to enable or disable applications on the user workspaces.

Procedure

1. On the default application that you want to enable or disable, click  or  icon to toggle the setting.

The applications with  icon will be enabled on the user workspaces, while the applications with icon will be disabled.

Hiding or Unhiding Applications in User Workspace

Use the **Application Management** screen to hide or unhide applications on the user workspaces. Hiding an application only hides the application icon, while the application reamains installed and available for use.

Procedure

1. On the **Application Management** screen, click **Hide Application**.
2. Do one of the following:
   - To hide applications, select the applications that you want to hide, and then click **Hide**.
   - To unhide applications, select the applications that you want to unhide, and then click **Unhide**.

Application Security Risk Levels

Trend Micro scans every application that is uploaded for security risk and identifies a risk level for every application.

TABLE 6-1. Virtual Mobile Infrastructure Components

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Malicious		Malicious applications can collect users' personal and private data such as pictures, contacts, videos and audio recordings.

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Notable		Notable applications can access user's email address, location information, media files and Web browser bookmarks. Applications that can change the Web browser's home page, add icons on home screen or show irremovable advertisements are also Notable applications.
PUA		Potentially unwanted applications (PUA) may pose high risk or have untoward impact on your security and/or privacy.
Safe		These are the applications that are safe to use.
Unknown		Trend Micro has not yet scanned these applications. Virtual Mobile Infrastructure checks Trend Micro's database, once a day, for the risk level of every uploaded application, and displays the latest risk level.

Sandbox Applications

Virtual Mobile Infrastructure enables you to deploy Android and iOS apps on user mobile devices, outside of user workspace, so that the users may use these apps even when the network is not available.

Virtual Mobile Infrastructure lets you modify the functionality of sandbox applications that you deploy to help align them with the organization's security policies. You can also configure the sandbox profile to protect the sandbox application data on the mobile device. For example, you can restrict copy and paste operations within a managed sandbox application, or forbid to share file in sandbox applications.

You can also remove or disable a sandbox application from administration web console. The removed or disabled application cannot be run on mobile devices.

Handling Android Sandbox Applications

Procedure

1. Make sure that the Android applications that you want to install locally on mobile devices, fullfil the following requirements:
   - The application is not encrypted.
   - The application is never modified (or "wrapped") before.
   - The application is written for Android 4.0 or later operating system.
2. Upload the modified application to Virtual Mobile Infrastructure administration web console. See *Uploading Android Application to Administration Web Console on page 6-7* for the procedure.

Uploading Android Application to Administration Web Console

Use the **Sandbox Application Management** screen to upload applications on Virtual Mobile Infrastructure server.

Procedure

1. Click **Add Android App**.

   The **Add Application** screen pops up.
2. Click **Browse** and select an apk file.
3. Click **OK**.

   The server starts uploading and modifying the selected application (apk) file. The process may take a few minutes, depending on the file size.
4. If **Edit Application** screen appears, edit the application details as required, and click **Done**.

The successfully uploaded app will be available in user workspace after the users sign in to the workspace next time. Tapping on the application icon downloads and installs the application on the mobile device.

Handling iOS Sandbox Applications

Procedure

1. Make sure that the environment for running the iOS App Wrapping Tool and the iOS applications that you want to install locally on mobile devices, fullfil the following requirements:

Option	Description
Supported operating system and toolset	You must run the app wrapping tool on a Mac computer that runs OS X 10.10 (Yosemite; minimum version) or later, which has the XCode toolset version 6 or later installed.
Signing certificate and provisioning profile	You must have an Apple signing certificate and provisioning profile. See your Apple developer documentation. https://developer.apple.com/
Processing an app with the App Wrapping Tool	Applications must be developed and signed by your company, or an independent software vendor (ISV). You cannot use this tool to process apps from the Apple Store. Applications must be written for iOS 7.1 or later. Applications must also be in the Position Independent Executable (PIE) format. For more information about the PIE format, see your Apple developer documentation. Applications must have the extension .app, or .ipa format.

Note

The wrapping tool cannot process the apps that are encrypted, unsigned, or with extended file attributes.

2. Download the iOS App Wrapping Tool from Virtual Mobile Infrastructure administration Web console.

See *Downloading iOS App Preparation Tool on page 6-9* for the procedure.

3. Prepare applications for installation on mobile devices.

   See *Preparing iOS Application for Upload on page 6-9* for the procedure.

4. Upload the iOS applications to Virtual Mobile Infrastructure administration Web console.

   See *Uploading iOS Application to Administration Web Console on page 6-11* for the procedure.

Downloading iOS App Preparation Tool

Procedure

1. On Virtual Mobile Infrastructure administration Web console, navigate to **Applications** > **Sandbox Applications**.
2. Click **Add iOS App**.

   The **Add Application** screen pops up.
3. Click the appropriate link to download the iOS app preparation tool to the local computer.

What to do next

Copy the iOS app preparation tool you have dowloaded to the Mac computer where you want to run this tool.

See *Preparing iOS Application for Upload on page 6-9*.

Preparing iOS Application for Upload

Important

Perform this procedure on a Mac computer that runs OS X 10.10 (Yosemite; minimum version) or later, which has the XCode toolset version 6 or later installed.

Procedure

1. Make sure the following items are available on your computer:
   - Original iOS application (.ipa) file
   - Distribution certificate for the app
   - Provisioning profile for the app
   - The iOS app preparaton tool downloaded from Virtual Mobile Infrastructure server. (If you have not yet downloaded the tool, see *Downloading iOS App Preparation Tool on page 6-9* for the procedure.)
2. Double-click the certificate file, and follow the on-screen instructions to install.
3. Start the iOS app preparation tool that you have downloaded from the Virtual Mobile Infrastructure server.
4. Select the following:
   - **Application IPA**: the iOS application (.ipa) file.
   - **Distribution Provisioning Profile**: the provisioning profile for the app.
   - **Distribution Certificate**: Select the certificate that you have just installed, from the drop-down list.
5. Click **Process**. If required, allow the tool to modify Keychain Access.

   The wrapping process starts.

The application is processed and is the modified .ipa file is stored at the location displayed before **output** on the screen that displays. The file name is modified to added "**wrapped_yyyy-mm-dd**" to the file name.

What to do next

Upload the processed .ipa file to Virtual Mobile Infrastructure server. See *Uploading iOS Application to Administration Web Console on page 6-11* for the procedure.

Uploading iOS Application to Administration Web Console

Use the **Sandbox Application Management** screen to upload applications on Virtual Mobile Infrastructure server.

Procedure

1. Click **Add iOS App**.

   The **Add Application** screen pops up.

2. Click **Browse** and select the wrapped ipa file.

3. Click **OK**.

   The server starts uploading and modifying the selected application (ipa) file.

4. If **Edit Application** screen appears, edit the application details as required, and click **Done**.

The successfully modified app will be made available in user workspace after the users sign in to the workspace next time. Tapping on the application icon downloads and installs the application on the mobile device.

Important

- Be sure to track when the provisioning profiles for your account are due to expire and renew the profiles before they expire. If a profile used to wrap apps expires, you must renew the profile, re-wrap the apps, and then reinstall the apps on user devices. To renew a provisioning profile, log on to your Apple Developer account, go to Certificates, Identifiers & Profiles, and then select Provisioning Profiles.

Deleting Sandbox Applications

Use the **Sandbox Application Management** screen to delete applications on Virtual Mobile Infrastructure server.

Procedure

1. Select the applications you want to delete, and then click **Delete**.
2. Click **OK** on the confirmation dialog box.

The applications are deleted from the server, and the users will not be able run these application on their mobile devices.

Enabling or Disabling Local Applications

Use the **Local Application Management** screen to enable or disable applications on the user workspaces.

Procedure

1. On the application that you want to enable or disable, click  or  icon to toggle the setting.

   The applications with  icon will be displayed on the user workspaces, while the applications with  icon will be removed from the user worspace and cannot be run on mobile device (if already installed).

Configuring Security Settings

Virtual Mobile Infrastructure lets you modify the functionality of sandbox applications that you deploy to help align them with the organization's security policies. You can also configure the sandbox profile to protect the sandbox application data on the mobile device. For example, you can restrict copy and paste operations within a managed sandbox application, or forbid to share file in sandbox applications.

Procedure

1. On the **Sandbox Application Management** screen, click **Security Settings** on the confirmation dialog box.

2. Select the settings according to your requirements.

3. Click **Done**.

Note

These settings will be applied to all uploaded applications, and may take up to one (1) hour to take effect.

Managing Wallpapers

Use the **Wallpaper Management** tab in **System Settings** to upload the wallpapers to the Virtual Mobile Infrastructure server. You can use these wallpapers to attach to a profile for the workspaces.

Procedure

1. On the **Wallpaper Management** screen, do one of the following:

   - To add a wallpaper, click **Add**, and then select an image to upload (in jpg, png or gif file format).
   - To delete wallpapers, select the wallpapers you want to delete, and then click **Delete**.

Single Sign On Processor

Trend Micro Virtual Mobile Infrastructure uses the app-wrapper technology to prepare apps for single sign on. The apps that are prepared for single sign on will not require users to provide their authentication information. Instead, these apps will use the same authentication information that the users used to sign in to Virtual Mobile Infrastructure.

Use the following URL to access the **Single Sign On Processor** screen:

https://<Virtual Mobile Infrastructure_domain_name_or_IP_address>:8443/apps/appwrap.htm

Preparing an Application for Single Sign On

Note

You must be logged on to the Virtual Mobile Infrastructure administration Web console before performing this procedure.

Procedure

1. Navigate to the following URL:

   https://<Virtual Mobile Infrastructure_domain_name_or_IP_address>:8443/apps/appwrap.htm

   This **Single Sign On Processor** screen appears.

2. Click **Upload**.

3. Click **Browse**, and then select an Android app (.apk file) that you want to prepare for single sign on.

   The application starts uploading. Wait until the upload completes.

4. After the app upload completes, click **Refresh**. Check if the status of the app in the **Status** column has changed to **Success**. If not, then wait for a while, and then click **Refresh** again.

5. In the **Action** column, click the  icon to download the app to the hard disk.

The Single Sign On Processor completes processing the app and the app is now enabled for the single sign on. Upload this app on the **Application Management** screen to install this app on the user workspaces.

Deleting Application from Single Sign On Processor

Note

You must be logged on to the Virtual Mobile Infrastructure administration Web console before performing this procedure.

Procedure

1. Navigate to the following URL:

   https://<Virtual Mobile Infrastructure_domain_name_or_IP_address>:8443/apps/appwrap.htm

   This **Single Sign On Processor** screen appears.

2. Select an application that you want to delete from the **Single Sign On Processor**, and then click **Delete**.

Chapter 7

Managing Servers

This chapter contains the following sections:

Servers in Virtual Mobile Infrastructure

Virtual Mobile Infrastructure enables you to add multiple servers and sites to increase the capacity to accommodate more users and support large-scale deployment. In the case of multiple servers or sites, Virtual Mobile Infrastructure balances the load between servers to achieve maximum efficiency.

Multiple Virtual Mobile Infrastructure servers can be installed on different physical computers or virtual machines. Refer to the *Trend Micro Virtual Mobile Infrastructure Best Practice Guide* to determine the best configuration for achieving maximum efficiency.

If your organization is located in different geographical locations, you can deploy separate servers at each location and add these servers as different **Sites** in Virtual Mobile Infrastructure. Multiple site deployment efficiently distributes load between servers and provide better experience to users. The Global Super Administrator can manage all the servers from one location and can create a Site Administrator for managing users, profiles and servers at different sites. See *Administrator Accounts Management on page 9-2* for the detailed permissions for Global Super Administrator and Site Administrator.

Note

In case of Multiple Server Installation Model, you can add all the servers under **Default Site**. However, if you have deployed Virtual Mobile Infrastructure in Multiple Sites Deployment Model, then Trend Micro strongly recommends adding the different servers under respected sites.

Starting or Stopping a Server

Use the **Server Management** screen to start or stop a Virtual Mobile Infrastructure server.

Procedure

1. Do one of the following:
   - Select a server, and then click **Start** or **Stop**.

- Click a server name, and then click **Start** or **Stop**.

Adding a Server

Before you can add and configure a Virtual Mobile Infrastructure server, make sure to do the following:

- Configure an external storage on current Virtual Mobile Infrastructure server. See *Configuring External Storage (Optional) on page 7-9* for the procedure.
- Install a new server on a separate physical computer or on a virtual machine. Refer to the *Installation and Deployment Guide* for the installation procedures.

Use the **Server Management** screen to add a Virtual Mobile Infrastructure server.

Procedure

1. Click **Add**.

   The **Add Server** screen appears.

2. Under **Step 1: Search server**, type the server IP address that you want to add.

   Note

   Make sure to type the correct IP address of the server. If the server IP address is not correct, the applications in the user workspace will not work.

3. Click **Next**.
4. Under **Step 2: Server Information**, type the server name and its description.
5. Click **Save**.

Editing a Server

Use the **Server Management** screen to edit a Virtual Mobile Infrastructure server.

Procedure

1. Click the server name whose details you want to edit.
2. Click **Edit**.
3. Update the following fields as required:
    - **Basic Information**
        - **Server name**
        - **Description**
4. Click **Save**.

Removing a Server

Note

The server localhost cannot be removed.

Use the **Server Management** screen to remove a Virtual Mobile Infrastructure server.

Procedure

1. Select a server, and then click **Remove**.

Adding a Site

Use the **Server Management** screen to add a site.

Procedure

1. Click **Add Site**.
2. Add the following information on the screen:

- **Name**: Type a name for the site.
- **Secure Access**: Type the server domain name or IP address that the mobile devices can access through the internet.
- **Description**: Type a description for the site.

3. Click **Save**.

Editing a Site

Use the **Server Management** screen to edit a site.

Procedure

1. Click the site name whose details you want to edit.
2. Click **Edit Site**.
3. Update the following fields on the screen as required:
   - **Name**
   - **Secure Access**
   - **Description**
4. Click **Save**.

Removing a Site

Procedure

1. Click the site name that you want to delete.
2. Click **Remove Site**.
3. Click **OK** on the confirmation dialog box.

Configuring Security-Enhanced Linux (SELinux)

Virtual Mobile Infrastructure server and secure access support Security-Enhanced Linux (SELinux) to support access control security policies. The SELinux setting is enabled by default in Secure Access.

Enabling, Disabling or Checking Status for SELinux

Procedure

1. Open **Terminal** on the Virtual Mobile Infrastructure server, and log on with the user account: **root**.
2. Do one of the following:
   - To enable SElinux, type the following command:
     - /vmi/manager/manage.py enable_selinux
   - To disable SELinux, type the following command:
     - /vmi/manager/manage.py disable_selinux
   - To check SELinux status:
     - /usr/sbin/sestatus -v
3. Reboot Virtual Mobile Infrastructure server for the settings to take effect.

Configuring Server High Availability (HA)

Virtual Mobile Infrastructure enables you to configure High Availability (HA) to ensure the uninterrupted service to the users. Along with the main server (primary server), you can configure another server (secondary server) to act as a backup to the primary server.

Whenever the information in the database of the primary server changes, the primary server synchronize the database with the secondary server immediately.

Important

Before performing this procedure, make sure that you have added and configured at least two Virtual Mobile Infrastructure servers. If you have configured only one server, set up and configure at least one more server to act as a backup to the primary server.

Enabling or Disabling High Availability (HA)

Procedure

1. Add a server in Virtual Mobile Infrastructure web console. Refer to the topic *Adding a Server on page 7-3* for the procedure.
2. Open **Terminal** on the Virtual Mobile Infrastructure server, and log on with the user account: **admin**.

Note

To log on, use the root account password that you created during Virtual Mobile Infrastructure server installation.

3. Type `enable` to enable privileged mode.
4. Do one of the following:
   - To enable high availability, type the following command:

     ```
     ha enable <secondary server (eth0) IP address> <common IP>
     ```

Note

Replace **<secondary server (eth0) IP address>** with the IP address of the server that you want to configure as a secondary server, and replace <common IP> with a new unoccupied IP address of the same subnet.

Important

Both the primary server and secondary server must exist in the same subnet.

- To disable high availability, type the following command:

  ```
  ha disable
  ```

5. Press **Enter**.

   The HA on Virtual Mobile Infrastructure is enabled or disabled.

6. Run the following command to verify the status of High Availability settings:

   ```
   ha status
   ```

Note

After enabling high availability, access the administrator Web console using the following format:

```
https://<Common_IP_address>:8443
```

What to do next

If you have Secure Access installed and configured, reconfigure Secure Access to use the common IP address to access Virtual Mobile Infrastructure server. Refer to *Configuring Secure Access on page 7-8* for the procedure.

Configuring Secure Access

Procedure

1. Open **Terminal** on the Virtual Mobile Infrastructure Secure Access, and log on with the root user account.
2. Open file `/vmi/gateway/configuration.json` in a text editor.
3. Search for the server IP address in the file, such as **"server": 10.18.12.1**, and change the IP address to the common IP address that you have configured in *step 2 on page 7-7* of procedure *Enabling or Disabling High Availability (HA) on page 7-7*.

4. Save changes and close the file.
5. On the **Terminal** window on Virtual Mobile Infrastructure Secure Access, type the following command to restart the Secure Access service:

   ```
   service vmigateway restart
   ```

6. Press **Enter**.

Configuring External Storage (Optional)

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

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

Procedure

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

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

Configuring Network Settings

Virtual Mobile Infrastructure enables you to configure network setting using command line interface.

Procedure

1. Open **Terminal** on the Virtual Mobile Infrastructure server, and log on with the user account: **root**.

   Note

   To log on, use the root account password that you created during Virtual Mobile Infrastructure server installation.

2. Type `enable` to enable privileged mode.
3. Do one of the following:
   - To configure eht0, type the following command:
     - `configure network interface ipv4 eth0 <ipaddress> <submask>`
   - To configure the gateway, type the following command:
     - `configure network route default ipv4 <ipaddress>`
   - To configure the DNS, type the following command:
     - `configure network dns ipv4 <ipaddress for DNS1>`
   - To configure the secondary DNS, type the following command:
     - `configure network dns ipv4 <ipaddress for DNS1> ipv4 <ipaddress for DNS2>`

Chapter 8

Managing Reports and Logs

This chapter contains the following sections:

Reports in Virtual Mobile Infrastructure

You can configure Virtual Mobile Infrastructure to generate reports to know the workspace usage and system status. The status report includes:

- **Workspace Usage Reports**:
  - **User Status**–provides count and percentage of users in the following statuses:
    - Active
    - Idle
    - Offline
    - Disabled
  - **Users Active/Idle Time**–shows time in hours for which the users were in active or idle statuses.
  - **Mobile App Launch Frequency**–shows number of times each application was launched.
  - **Mobile App Usage Duration**–shows the usage duration of each application.
  - **Web App Launch Frequency**–shows number of times each Web clip was launched.
- **System Resource Usage Reports**–shows the following information in percentage in the graphical format:
  - **Memory Usage (Percentage)**
  - **Storage Usage (Percentage)**
  - **CPU Usage (Percentage)**
- **Mobile Device Operating System Information**–shows mobile device operating system version summary for the logged in mobile devices.
  - **Mobile Device Operating System Version Summary**
  - **Android Operating System Version Summary**

    - iOS Operating System Version Summary
    - Windows Phone Operating System Version Summary
- **User Storage Information**–shows the information about the user storage.
    - User Storage Usage Summary

Virtual Mobile Infrastructure enables you to generate the following types of reports:

- Quick report
- Scheduled report

Generating a Quick Report

Use quick report to collect the details about the current workspace usage and system status.

Use the **Report Management** screen to generate a quick report.

Procedure

1. On the **Quick Report** tab, configure the following:
    - **Report name**: type a name for the report.
    - **Time range**: select a time period of the report (either **Today**, **Last 7 Days**, **Last 30 Days**, or select the date and time from the **From** and **To** fields).
    - **Action when report is generated**:
        - **Keep report online for later check only**
        - **Keep report online and send it out by email**: if you select this option, type the email address of the receivers in the **Email addresses** field. Use semicolons (;) to separate email addresses.
2. Click **Generate New Report**.

Configuring Scheduled Report

Configure Virtual Mobile Infrastructure server to automatically send workspace usage and system status report at the specified time.

Use the **Report Management** screen to configure scheduled reports.

Procedure

1. On the **Scheduled Report** tab, configure the following:
   - **Frequency**: select the frequency for the report:
     - **Daily, at 12:00 AM**
     - **Weekly, Monday at 12:00 AM**
     - **Monthly, first day of every month at 12:00 AM**
   - **Delivery**: type the email addresses of the receivers in the field provided. Use semicolons (;) to separate email addresses.
2. Click **Save**.

Logs in Virtual Mobile Infrastructure

Virtual Mobile Infrastructure keeps the user logs on server so that you can check logs whenever required. Virtual Mobile Infrastructure server records the following logs:

- Event logs
  - Successful logon or unsuccessful logon attempt
  - Successful user logoff
  - Screen capture on iOS mobile devices
- Audit logs
  - Administrator operations such as logon, adding or modifying users, uploading or modifying applications, and so on

- Application usage log
    - Name of the applications used and the usage duration for each application

You can search specific event logs or audit logs by specifying query criteria.

Viewing Logs

Use the **Log** screen to view user logs.

Procedure

1. On the **Log** tab, specify the query criteria for the logs you want to view. The parameters are:
    - **User name**: type the user name whose generated logs you want to search.
    - **Time range**: select a time period of the log (either **Today**, **Last 7 days**, and **Last 30 days**, or select the date and time from the **From** and **To** fields).
        - **From**: type the date and hour for the earliest log you want to view. Click the calendar icon to select a date from the calendar, and hour drop down list to select the hour.
        - **To**: type the date and hour for the latest log you want to view. Click the calendar icon to select a date from the calendar, and hour drop down list to select the hour.
2. Click **Query** to begin the query.

Log Maintenance

When users generate event logs, the logs are sent and stored on the Virtual Mobile Infrastructure server. To keep the size of logs from occupying too much space on your hard disk, delete the logs manually or configure Virtual Mobile Infrastructure administration Web console to delete the logs automatically based on a schedule on the **Log Maintenance** tab on the **Log** screen.

Deleting Logs Manually

Procedure

1. On the **Log** screen, click **Log Maintenance** tab.
2. Select whether to delete all the logs from the beginning or those older than the specified number of days.
3. Click **Delete Now**.

Auditing Logs

The **Audit Log** tab on the **Log** screen records all the operations performed by an administrator, such as: login, import/add/modify users, change groups, upload/modify applications, create/modify profiles and so on.

Procedure

1. On the **Log** screen, click **Audit Log** tab.
2.

Scheduling Log Deleting

Procedure

1. On the **Log** screen, click **Log Maintenance** tab.
2. Select **Enable scheduled deletion of logs**.
3. Select whether to delete all the logs from the beginning or those older than the specified number of days.
4. Specify the log deletion frequency and time.

5. Click **Save**.

Chapter 9

Administration Settings

This chapter contains the following sections:

Administrator Accounts Management

The **Administrator Account Management** screen enables you to create administrator accounts with different role for Virtual Mobile Infrastructure server.

The default **Administrator** account for accessing Virtual Mobile Infrastructure server is "admin" (password: "admin"). The **"admin"** account cannot be deleted and can only be modified.

The roles for administrator accounts in Virtual Mobile Infrastructure are as follows:

- **Super** (default): This role has the maximum access to all settings on the server.
- **Monitor**: The administrator with the monitor role can only view the web console but cannot modify any settings.

The following table provides the details regarding privileges for **Global Super Administrator** and **Site Administrator** roles in Virtual Mobile Infrastructure.

TABLE 9-1. GLOBAL AND SITE ADMINISTRATORS PRIVILEGES IN VIRTUAL MOBILE INFRASTRUCTURE

SERVER COMPONENTS	PERMISSIONS	GLOBAL SUPER ADMINISTRATOR	SITE ADMINISTRATOR
Dashboard	View Dashboard data	Can view data for all sites	Can only view data of the site the Site Administrator belongs to Can only view **Top 5 Users** and **User Status** widgets on **Usage Overview** tab on Dashboard

Server Components	Permissions	Global Super Administrator	Site Administrator
User management	Add, import or delete users	Supported	Not supported
	Enable or disable users	Supported	Supported
	Wipe workspace	Supported	Supported
	Clear workspace	Supported	Supported
	Edit user	Supported	Supported
Profile management	Manage profiles	Can manage profiles of all sites	Can only manage profiles of the site the Site Administrator belongs to
Application management	Manage workspace applications	Supported	Can view all the applications but cannot manage
	Manage local applications	Supported	Can view all the applications but can not manage
Reports	Generate and send report	Can generate and send report for all the sites	Can generate and send report for the site the Site Administrator belongs to
Logs	View and maintain logs	View and maintain logs for all the sites	Not supported
Email settings	Configure SMTP server	Supported	Not supported
Email template setting	Configure email template settings	Configure email template settings for all the sites	Not supported

Server Components	Permissions	Global Super Administrator	Site Administrator
Administrator management	Manage administrator account	Supported	Can only manage the administrator for the site the Site Administrator belongs to
System settings	Manage system settings	Supported	Not supported
Certificate settings	Manage certificate	Supported	Not supported
License management	Manage product license	Supported	Not supported

Adding Administrator Account

Procedure

1. On the Virtual Mobile Infrastructure administration web console, go to **Administration** > **Administration Account Management**.
2. Click **Add Administrator** to add a new account.
3. Update the following fields as required:
   - **Name**
   - **Description**
   - **Password**
   - **Site**: If you have configured multiple sites, select a site to add a site admin, or select the default site to add a Global Super Administrator account. If you do not have multiple sites, select the default site. See *Table 9-1: Global and Site Administrators Privileges in Virtual Mobile Infrastructure on page 9-2* for details.

- **Role**: Select a role for the administrator. A Super Administrator can manage all the settings, a monitor admin can only view the settings on administration web console.

4. Click **Save** on **Administrator Account Management** screen.

Modifying Administrator Account Information

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

Procedure

1. Update the following fields as required:
   - **First name**
   - **Last name**
   - **Email address**: add an email address to receive email notification messages from Virtual Mobile Infrastructure.
   - **Password**: click **Change password**, type the old and new passwords in the fields provided, and then click **Save**.
2. Click **Save** on **My Account** screen.

Changing Administrator Account Password

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

Attention

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

Procedure

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

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

2. Use the following fields:

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

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

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

Deleting Administrator Account

Procedure

1. On the Virtual Mobile Infrastructure administration web console, go to **Administration** > **Administration Account Management**.

2. Select the account that you want to delete, and then click **Delete**. Click **OK** on the confirmation message that appears.

Configuring LDAP Settings (Optional)

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

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

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

Procedure

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

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

Disabling LDAP Server

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

Procedure

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

Configuring Mobile Client Settings

The Virtual Mobile Infrastructure mobile client provides access to the user workspace from a mobile device.

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

Procedure

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

     Note

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

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

     Note

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

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

> **Note**
>
> The built-in keyboard for workspace supports English only.

- 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**.

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

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

See *Configuring Email Notifications on page 9-12* for details on configuring user alert notification.

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

5. Under the **Secure Access Settings**, configure the following:

   - **Domain name or IP address**

   > **Note**
   >
   > If Secure Access is connected to a gateway or an external router, type the IP address or domain name of the gateway or the router instead of the IP address of Secure Access.

   - **Port number**

6. Click **Save**.

Configuring Microsoft Exchange Server and Office 365 Settings (Optional)

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

Note

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

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

Procedure

1. On the **System Settings** screen, click the **LDAP** tab.
2. Make sure that the **Use LDAP** checkbox is selected, and the LDAP settings are configured.
3. Click the **Exchange Server** tab.
4. Select **Use automatic configuration for Exchange Server on workspace**, and then type the server name in the **Exchange server** field.
5. Select **Office 365 customization**, if you are using Exchange Online, and type the Office 365 login ID in the **User name** field.

Note

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

6. Click **Save**.

Configuring Proxy Settings

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

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

Procedure

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

     
     Note
     The bypass setting only takes effect for the user workspaces, and from the next time users sign in.
3. Type a URL in the **Test address** field, and then click **Test Connection** to verify proxy settings.
4. Click **Save**.

Configuring External Storage (Optional)

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

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

Procedure

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

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

Configuring Email Notifications

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

Use **Email Notifications** screen to configure email notifications in Virtual Mobile Infrastructure.

Procedure

1. On the **Email Settings** tab, configure the following:
   - **From**–type the address from which you want to send the email notification. SMTP
   - **SMTP Server**–type the SMTP server name or IP address.
   - **Port**–type the SMTP server port number.
   - **Authentication**–if the SMTP address requires authentication, select this option and type the following information:
     - **User name**
     - **Password**
   - **Use TLS protocol for authentication**–if the SMTP server requires TLS protocol for authentication, select this option.
2. Click **Test Connection** to verify SMTP server address and port number.

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

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

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

4. On the **Reset Password Template Settings** tab, type the following:
   - **Subject**–the subject of the email message.

- **Message**–the body of the email message.

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

5. On the **User Alert Template Settings** tab, configure the following:
   - **Subject**–the subject of the email message.
   - **Message**–the body of the email message.

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

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

Configuring Syslog (System Logs)

Configure syslog server settings to save server debug logs.

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

Procedure

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

- **Port number**

4. Click **Save**.

Configuring Advanced Settings

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

Before you can configure OAuth 2.0 authentication settings, you must configure **Secure Access Settings** in **Mobile Client** tab. Refer to *Configuring Mobile Client Settings on page 9-8*.

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

Procedure

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

Note

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

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

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

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

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

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

  Note

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

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

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

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

  Use the following command to generate the client certificate file:

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

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

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

  Note

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

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

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

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

  Note

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

Note

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

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

What to do next

Generate individual certificates for mobile users for enrollment. See *Generating Client Enrollment Certificate on page 9-18*.

Generating Client Enrollment Certificate

Before following this procedure, make sure that you have already configured OAuth 2.0 Authentication. See *Configuring Advanced Settings on page 9-15* for details.

Procedure

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

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

   Note

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

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

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

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

What to do next

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

Managing Certificates

If you want to deploy certificates to the user workspaces to enable them to access organization's resources, you can upload these certificates to the Virtual Mobile Infrastructure server. Virtual Mobile Infrastructure server will deploy these certificates to the user workspaces immediately.

Use the **Certificate Management** screen to upload single `.pfx` or `.p12` certificates to the Virtual Mobile Infrastructure server. You can also upload multiple certificates by archiving them in a `.tar`, `.gz`, `.bz2` or `.zip` file. All the certificates in the archive must use the same password.

Uploading a Certificate

Procedure

1. Click **Administration** > **Certificate Management**.
2. Click **Upload**.

   The **Upload certificate** screen appears.
3. Click **Choose File** and then do one of the following:
   - To upload a single certificate, select a `.pfx` or `.p12` certificate file.
   - To upload multiple certificates, create a `.tar`, `.gz`, `.bz2` or `.zip` archive file, and then select the file.

     Important

     The certificate files in an archive must use the same password.
4. Type the certificate password in the **Password** field.

5. Click **Save**.

Deleting Certificate

Procedure

1. Click **Administration** > **Certificate Management**.
2. Select certificates or archives that you want to delete, and then click **Delete**.

Product License

After the Trial version license expires, all program features will be disabled. A Full license version enables you to continue using all features, even after the license expires. It is important to note that the mobile client application will be unable to access the Virtual Mobile Infrastructure server, and therefore, users will not be able to access their workspaces.

If your license expires, you will need to register the Virtual Mobile Infrastructure server with a new Activation Code. Consult your local Trend Micro sales representative for more information.

Virtual Mobile Infrastructure supports seat control for the number of seats (workspaces) included in a license. This means, you can import any number of users to the Virtual Mobile Infrastructure server, but all the additional users will be disabled. Also, if the number of users reach the maximum number of seats available under your license, or is already more than the available seats, you will not be able to add users locally.

To see the number of seats available under your license, navigate to **Administration** > **Product License**.

Upgrading Virtual Mobile Infrastructure

Refer to the following URL for the detailed information and the upgrade procedure:

http://esupport.trendmicro.com/solution/en-US/1115141.aspx

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APEM57759/170323