TREND MICRO™

5.5 TREND MICRO™ Virtual Mobile Infrastructure

Administrator's Guide

Centrally-managed workspace for mobile users

Endpoint Security

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

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

Document Part No.: APEM57876/170627

Release Date: June 2018

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

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

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

Table of Contents

Preface

Chapter 1: Introducing Virtual Mobile Infrastructure

Chapter 2: 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 5.5 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 (5.5)?

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

FEATURE	DESCRIPTION
Improved support for bare metal servers	Supports more bare metal servers by upgrading kernel to version 3.18.58.
Date and time Verification During Installation	Added a verification step for system time during Virtual Mobile Infrastructure server and Secure Access installation.

FEATURE	DESCRIPTION
Bluetooth Support in Cloud Workspace	Supports Bluetooth 3.0 and 4.0 in Android and iOS client applications, and enables you to configure Bluetooth settings in profiles.
License Seat Control	• Improves seat control for locally imported and LDAP users. • Restricts uploading applications after license expires. • Displays a warning message on client application after the license expires.
Audio/video support in workspaces	Adds audio/video playback and recording quality options on Web console.
High-Resolution App Support	Supports configuring workspace resulution higher than 1080p for the applications that do not display in user workspaces with resolution less than 1080p.
Application Data Traffic Monitoring	Monitors real-time data traffic consumption for the applications deployed in Virtual Mobile Infrastructure, and displays these statistics for the top 5 applications on administration web console.
Enhanced Email User Experience	A quick action bar is added at the bottom to enable users to reply, replay all, and forward email messages. A floating menu is also added for easily selecting and copying text.
SMS Support	Supports sending SMS messages on real mobile devices from user cloud workspace.
Client App Availability on Official Stores	Enables users to download client app directly from Google Play store, Apple App Store and Windows Store.
APNs via Secure Access	Supports APNs connection via Secure Access for VMI servers with no Internet connection to receive Apple push notifications.
Integration with Google Cloud Message	Provides support for Google Cloud Message to display Android Client notifications.
Bandwidth Test on Virtual Mobile Infrastructure Client	Enables you to test bandwidth between Virtual Mobile Infrastructure server and mobile device on Android and iOS client applications.

FEATURE	DESCRIPTION
Session Resumption (iOS Only)	Supports session resumption after network connection changes or the mobile device disconnects from the network for a short interval.
Updated Rendering Options (iOS Only)	Provides three rendering options: **Quality**, **Balance**, and **Performance**.
Security Enhancement	Uses SSL certificate to verify server integrity. Uses advanced checks to avoid data changes on client mobile devices.
Fingerprint Unlock (Android 6.0 or later only)	Supports unlocking using fingerprint in TMVMI client on the mobile devices that provide fingerprint support.
Full Camera Support	Supports front and rare camera on the mobile device when using TMVMI client.
iPhone X support	Adds support for iPhone X.
Secure LDAP Integration	Supports integration with secure LDAP server to enable you to import users from secure LDAP server.
Enhanced Device Binding Feature	Enables you to configure Virtual Mobile Infrastructure to automatically bind the first mobile device used by a new user, with their account.
Enhanced User Management Feature	• Enables you to configure Virtual Mobile Infrastructure to automatically send an email notification to new users. • In multiple-server environment, displays the IP address of the server on which the user is running in active or idle mode.
Updated Lock Screen	Adds a **Sign Out** button on the lock screen.
Enhanced Dashboard	Displays information about the top five (5) applications used, based on launch times, network data consumed, and the duration of the usage for each application. The **Dashboard** also displays the top five (5) applications used based on launch times.

FEATURE	DESCRIPTION
Updated Settings in Workspace	Enables you to configure display notifications and clear the default launch preferences for each application in user workspace.
Picture Attachment in Email App	Enables you to capture a picture using camera to attach in the Email app in user workspace.
Kernel Upgrade	Upgrades kernel to enhance system stability.
Enhanced Administrator Account Management	Enables adding administrator accounts from the active directory.
Enhanced User Management	Enables wiping user workspace and resend invitation email messages to multiple users at the same time.
Graphics Quality Settings on Server	Provides an option on the management console to set default graphics quality on mobile devices.
Enhanced Application Usage Settings	Provides option on management console to collect user location for applications.
Enhanced Reports	Collects and display the application launch time for each user separately.

Architecture of Virtual Mobile Infrastructure

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

Trend Micro Virtual Mobile Infrastructure also supports high availability for Management Server and Secure Access.

Single Server Installation Model

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

Note

Trend Micro strongly recommends deploying Secure Access in your environment to enable mobile clients to access Virtual Mobile Infrastructure Server via Internet. See *Why Use Secure Access on page 1-10* for more information.

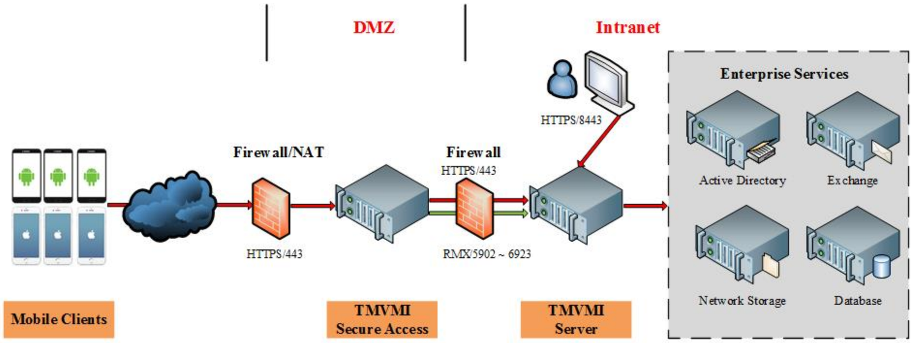


FIGURE 1-1. Trend Micro Virtual Mobile Infrastructure Single Server Installation Model

Multiple Server Installation Model

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

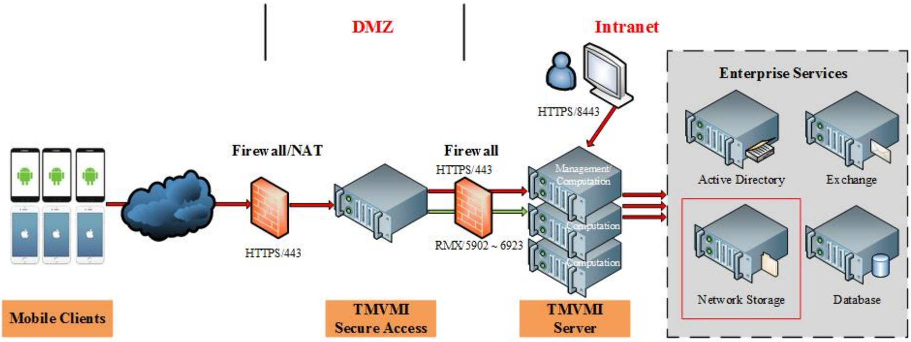


FIGURE 1-2. Trend Micro Virtual Mobile Infrastructure Multiple Server Installation Model

Virtual Mobile Infrastructure High Availability

Virtual Mobile Infrastructure enables you to configure High Availability (HA) to ensure the uninterrupted service to users. To support HA, you need at least two Virtual Mobile Infrastructure servers. One server acts as a primary server, and the other server acts as a backup server. Similarly, to support HA for Virtual Mobile Infrastructure Secure Access, you must configure at least two active Secure Access servers.

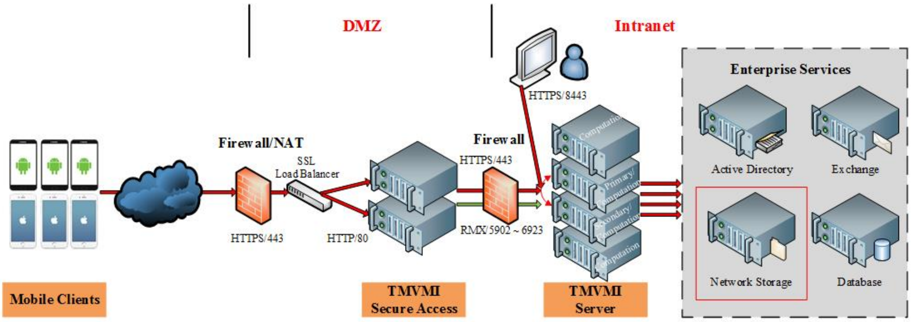


FIGURE 1-3. Trend Micro Virtual Mobile Infrastructure High Availability architecture

Components of Virtual Mobile Infrastructure

The Virtual Mobile Infrastructure system includes the following components:

TABLE 1-1. 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 1-10* for more information.	Strongly 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:

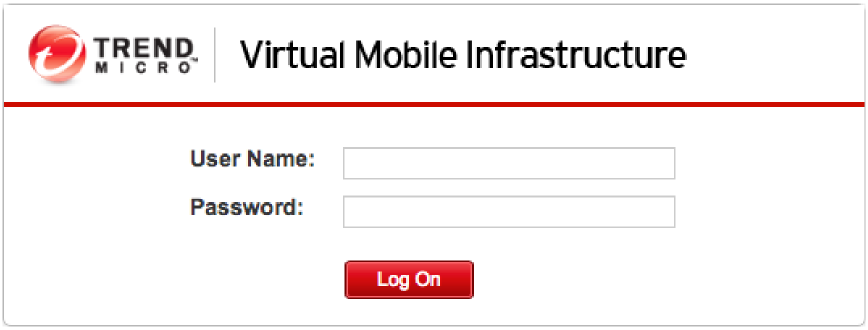
Procedure

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).
    - **Network Data Consumed**–shows the top five (5) application that consumed the most data traffic from all the users combined.
  - **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.

Import Users from File

Virtual Mobile Infrastructure allows you to import multiple local users via `csv` or `txt` file format.

Procedure

1. Click **Import User**.

   The **Import Users** screen appears.

2. Click **Download the sample file** to download a file with sample data. Use this file to ensure that your data is in the correct format.

   Note

   The data should be the following format:

   ```
   display_name1,login_name1,email1,group1,password1
   ```

   ```
   display_name2,login_name2,email2,group2,password2.
   ```

   The password is optional. If you keep password cell blank, the default password is `123456`.

3. Modify the file that you just downloaded in the previous step, to add the information of all the users that you want to add.

Note

If the data in the imported file is not correct, the user will fail to import. You need to follow the format in the data file.

User login name: The User name must be between 3 and 20 characters long and contain the following characters: A to Z, a to z, 0 to 9, - or _.

User Email: The length of the email address should not exceed 75 characters, and should be in the format: myname@example.com.

Group: The Group name must be between 3 and 20 characters long and contain the following characters: A to Z, a to z, 0 to 9, - or _.

Important

Virtual Mobile Infrastructure has the seat contrl for users. If the account of user is more than the seat, the exceed user can not import.

4. Click **Browse** on the **Import Users** screen to upload the file.

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 for several hours. 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 signs out manually, which, in turn, limits the server capacity.

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. Do one of the following:
   - To wipe workspace for multiple users:
     a. On the user list on the left side of the screen, select the user names for which the workspace you want to wipe.

   b. Click **Wipe** on the menu bar, and then click **OK** on the pop-up dialog box to confirm.

- To wipe workspace for single user:

   a. On the user list on the left side of the screen, click the user name for which the workspace you want to wipe.

   b. Click **Wipe** before **Wipe workspace**, and then click **OK** on the pop-up dialog box to confirm.

2.

Resending Invitation to a User

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

Procedure

1. Do one of the following:

   - To resend invitation to multiple users:

      a. On the user list on the left side of the screen, select the user names whom you want to resend the invitation.

      b. Click **Resend Invitation** on the menu bar, and then click **OK** on the confirmation pop-up dialog box.

   - To resend invitation to single user:

      a. On the user list on the left side of the screen, click the user name whom you want to resend the invitation.

      b. 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 9-13* 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 workspace 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.

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. Select **Automatically bind the first mobile device used by new user** if you want to bind the first mobile device for users that are not yet registered with the server.

3. Click **Import Devices**.

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

   The **Import Devices** screen appears.

4. 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
   ...
   ```

5. 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: Cloud Workspace profiles for virtual mobile workspace, and local workspace 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 Cloud Workspace Profile

Use the **Profile Management** screen to create Cloud Workspace 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 **Cloud 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: Cloud 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 cloud workspace**, and then type the text into the field provided, to display the text as watermark on user cloud 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 cloud workspaces.

- If the application that is installed in user cloud workspace need to translate data through Bluetooth, select **Enable Bluetooth in cloud workspace**, and then select the **Device synchronization** list to use:
  - **All**: All the bluetooth devices that are detected by the mobile device will be allowed to connect to the user cloud workspace.

    Approved list: Only the bluetooth devices that are added into the approved list will be allowed to connect to the user cloud workspace.

    Blocked list: Only the bluetooth devices that are added into the blocked list will not be allowed to connect to the user cloud workspace.

  If there are applications in the user workspace that use Bluetooth 3.0 protocol on iOS devices, select **Enable Bluetooth 3.0 conversion on iOS devices** option to support such application on iOS client, and then click **Add** to add the Bluetooth ID. If you have any difficulty in locating the Bluetooth ID, contact Trend Micro technical support for help.

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.
- open inbound TCP port 8883 for Android Push Notification service on Secure Access.

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 Secure Access, 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 local workspace 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:

Cloud 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 **Cloud Workspace 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 **Cloud Workspace 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 **Cloud Workspace 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 **Cloud Workspace 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 **Cloud Workspace 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 **Cloud Workspace 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.
Clean	✓	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.

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 Support

Virtual Mobile Infrastructure enables you to configure single sign on for the applications. 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.

Virtual Mobile Infrastructure provides two options for single sign on for the applications:

- **Intent method**: This method enables you to modify the application to receive the user name and password through the Android operating system's Intent service. You can add the following sample code to the application with the help of the developer:

```
@Override
protected void onCreate(Bundle savedInstanceState) {
    String strUsernameFromIntent = null;
    String strPasswordFromIntent = null;

    Intent intent = getIntent();
    Bundle bundleExtra = intent.getExtras();
    if (bundleExtra != null) {
        strUsernameFromIntent = bundleExtra.getString("username");
        strPasswordFromIntent = bundleExtra.getString("password");
        if (strUsernameFromIntent == null && strPasswordFromIntent == null)
            // No username/password in Bundle
        }
    } else {
        // No extras in Intent
    }
}
```

  You can enable or disable single sign on whenever required from the **Edit Application** screen. This method works well in most of the cases.

- **App wrapper method**: This method wraps the application to enable single sign on. The application will be signed again by Trend Micro during the wrap process. You will not be able to disable single sign on once the wrapped application is uploaded to the cloud workspace. This method may not work in some cases.

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 using 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. 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 by each user.
  - 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.
    - **LDAP encryption**–select encryption method according to your LDAP server settings.
4. Click **Save**.

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

Disabling LDAP Server

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

Procedure

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

Configuring Mobile Client Settings

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

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

Procedure

1. On the **System Settings** screen, click the **Mobile Client** tab.

2. Under **User Settings** section, configure the following:

   - If you want to allow users to save their passwords on their mobile devices, select **Allow users to save password on mobile device**.

   - If you want users to wait for a certain time before retrying after typing in a wrong password, select **Enable unsuccessful signin restriction**, and then select the number of attempts and the waiting time from the drop-down lists.

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

     Note

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

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

     Note

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

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

- If you want to restrict users from accessing workspace from a rooted or jailbroken mobile device, select **Do not allow users to log in from rooted or jailbroken mobile devices**.
- From the **Graphics Options** drop-down menu, select one of the following options:
  - **Performance**: This option provides more speed, but less quality (screen clarity), and utilizes less bandwidth.
  - **Balance** (default): This option provides balance between quality (screen clarity) and speed.
  - **Quality**: This option provides more quality (screen clarity), but less speed, and utilizes more bandwidth.

3. 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 9-13* for details on configuring user alert notification.

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

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. Select **Automatically send email notification to new users** if you want to send an invitation email to new users that are added from LDAP.

4. On the **Invitation Email Template Settings** tab, type the following:

   - **Subject**–the subject of the email message.

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

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

5. On the **Reset Password Template Settings** tab, type the following:

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

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

6. 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.

7. 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 includes the following:

- Application usage log setting, to collect application usage log from user workspaces, to learn more about user behavior.
- Mobile device location for each users using applications in user workspace.
- Port range manual configuration for Virtual Mobile Infrastructure.
- Screen resolution setting for user workspace.
- OAuth 2.0 protocol configuration 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 advance settings for Virtual Mobile Infrastructure.

Procedure

1. On the **System Settings** screen, click the **Advanced** tab.

2. Under **Application Usage Log** section, configure the following settings:

   - **Collect application usage log**: 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.

   - **Configure mobile device location**: If enabled, you can view the details about location of users using certain applications.

3. Under **Virtual Mobile Infrastructure Server Port Setting** section, type the port range in the field provided. Change this setting only if any of your application requires a port number ranging between 5900 and 6923, to avoid network conflict.

4. Under **Virtual Mobile Infrastructure Server Screen Resolution Setting** section, select **Enable high quality screen resolution for user workspaces**option if any of the applications installed in user workspace requires high-resolution, or does not display correctly using the default resolution.

   > Note
   >
   > Enabling this feature consumes more data traffic for the Virtual Mobile Infrastructure server.

5. Under **OAuth 2.0 Authentication** section, select **Enable OAuth 2.0 authentication**.

6. 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.

7. (Optional) Click **Test Connection** to verify your settings.
8. 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. However, you must also configure OAuth 2.0 for user authentication to delpoy certificates to user workspaces. See *Configuring Advanced Settings on page 9-15* for configuring OAuth 2.0 settings.

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.

If your license expires, you will need to renew your current Activation Code, or 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 and Secure Access

Important

Before performing the upgrade to Virtual Mobile Infrastructure and Secure Access, consider the following reminders:

- Make sure that the users are offline before upgrading. Otherwise, the TMVMI server will lose all the application and user data after the upgrade. To disconnect all the users, you may consider stopping the server.
- If you have enabled High Availability (HA) mode in TMVMI server, you need to run the "ha disable" command to disable it. Once the server upgrade is done, you can enable the HA mode again by running the "ha enable <secondary server eth0> <common IP>" command.

Upgrading Virtual Mobile Infrastructure Server

Procedure

1. Download the upgrade package for Virtual Mobile Infrastructure from the download center.

2. Use the account **tmvmi** to copy the `upgrade.tar.gz2` file to the `/home/tmvmi/` folder on the Virtual Mobile Infrastructure server.

3. Open a terminal connection to the Virtual Mobile Infrastructure server using **PuTTY** software, and log on using account **tmvmi**.

4. After logging on, change to root account using command `su root`.

5. Copy the `upgrade.tar.gz2` file to folder `/gluster/upload/`.

6. Type the command "`clish`" to enter the Virtual Mobile Infrastructure CLT.

7. In Virtual Mobile Infrastructure CLT, run command "`enable`" to enter the privileged mode.

8. Run command "`upgrade`" to upgrade the server to the new version.

9. Wait until the upgrade process is finished, and then reboot the Virtual Mobile Infrastructure server.

After rebooting, navigate to the administration web console, and click server version on **Administration** > **About** to confirm the latest version.

Upgrading Secure Access

Procedure

1. Download the upgrade package for Virtual Mobile Infrastructure Secure Access from the download center.

2. Use the account **tmvmi** to copy the `upgrade.tar.gz2` file to the `/home/tmvmi/` folder on the Virtual Mobile Infrastructure Secure Access.

3. Open a terminal connection to the Virtual Mobile Infrastructure server using **PuTTY** software, and log on using account **tmvmi**.

4. After logging on, change to root account using command `su root`.

5. Copy the `upgrade.tar.gz2` file to folder `/gluster/upload/`.

6. Type the command "`clish`" to enter the Virtual Mobile Infrastructure Secure Access CLT.

7. In Virtual Mobile Infrastructure CLT, run command "`enable`" to enter the privileged mode.

8. Run command "`upgrade`" to upgrade the server to the new version.

9. Wait until the upgrade process is finished, and then reboot the Virtual Mobile Infrastructure Secure Access.

TREND MICRO™

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: APEM57876/170627