TREND MICRO™

6.0 TREND MICRO™ Virtual Mobile Infrastructure

Administrator's Guide

Centrally-managed workspace for mobile users

Endpoint Security

Document Part No.: APEM68494/180927

Release Date: April 2019

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

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

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

Table of Contents

Preface

Preface v

Audience vi

Virtual Mobile Infrastructure Documentation vi

Document Conventions vii

Chapter 1: Introducing Virtual Mobile Infrastructure

About Virtual Mobile Infrastructure 1-2

Why Use Virtual Mobile Infrastructure 1-2

What's New in this Release (6.0)? 1-3

Architecture of Virtual Mobile Infrastructure 1-4

- Single Server Installation Model 1-4
- Multiple Server Installation Model 1-5
- Virtual Mobile Infrastructure High Availability 1-5

Components of Virtual Mobile Infrastructure 1-6

- Why Use Secure Access 1-8

Chapter 2: Getting Started

Accessing Virtual Mobile Infrastructure Administration Web Console 2-2

The Dashboard Screen 2-3

Chapter 3: Managing Users and Devices

User Management in Virtual Mobile Infrastructure 3-2

- Managing Groups and Users 3-2
- Searching Users 3-8

Device Management in Virtual Mobile Infrastructure 3-8

- Enabling or Disabling Device Binding 3-9

Importing Mobile Devices 3-9
Binding or Unbinding Mobile Devices 3-10
Deleting Mobile Device 3-11

Chapter 4: Managing Profiles

Profiles in Virtual Mobile Infrastructure 4-2
Creating a Cloud Workspace Profile 4-2
Changing Profile Order 4-3
Deleting Profiles 4-4
Kiosk Mode in Virtual Mobile Infrastructure 4-4
Enabling or Disabling Kiosk Mode 4-4

Chapter 5: Managing Applications

Cloud Workspace Applications 5-2
Adding Application Category 5-2
Editing or Deleting Application Category 5-2
Uploading Applications to Server 5-3
Adding a Web Clip to the Server 5-3
Deleting an Application or a Web Clip from the Server 5-4
Application Security Risk Levels 5-4

Chapter 6: Managing Servers

Configuring External Storage 6-2
Servers in Virtual Mobile Infrastructure 6-2
Typical Server Deployment Scenarios 6-3
Starting or Stopping a Server 6-4
Adding a Server 6-4
Editing a Server 6-5
Removing a Server 6-6
Configuring Security-Enhanced Linux (SELinux) 6-7
Enabling, Disabling or Checking Status for SELinux 6-7
Configuring Server High Availability (HA) 6-7

Upgrading Virtual Mobile Infrastructure and Secure Access 6-11
Upgrading Virtual Mobile Infrastructure Server 6-11
Upgrading Secure Access 6-11

Configuring Network Settings 6-12

Chapter 7: Managing Reports and Logs

Reports in Virtual Mobile Infrastructure 7-2
Generating a Quick Report 7-3
Configuring Scheduled Report 7-3

Logs in Virtual Mobile Infrastructure 7-4
Viewing Event Logs 7-5
Viewing Audit Logs 7-5
Viewing Application Usage Log 7-6
Log Maintenance 7-7

Chapter 8: Administration and System Settings

Administrator Accounts Management 8-2
Adding Administrator Account 8-3
Modifying Administrator Account Information 8-4
Changing Administrator Account Password 8-4
Deleting Administrator Account 8-5

Configuring LDAP Settings (Optional) 8-5
Disabling LDAP Server 8-6

Configuring Mobile Client Settings 8-7

Configuring Microsoft Exchange Server and Office 365 Settings (Optional) 8-8

Configuring Network Settings 8-9

Configuring External Storage 8-11

Configuring Email Notifications 8-11

Configuring Syslog (System Logs) 8-13

Configuring Advanced Settings 8-14

Configuring Re-branding 8-15

Product License 8-15

Preface

Preface

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

This preface discusses the following topics:

- *Audience on page vi*
- *Virtual Mobile Infrastructure Documentation on page vi*
- *Document Conventions on page vii*

Audience

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

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

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

Virtual Mobile Infrastructure Documentation

The Virtual Mobile Infrastructure documentation consists of the following:

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

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

Tip

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

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

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

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

Chapter 1

Introducing Virtual Mobile Infrastructure

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

This chapter contains the following sections:

- *About Virtual Mobile Infrastructure on page 1-2*
- *Why Use Virtual Mobile Infrastructure on page 1-2*
- *What's New in this Release (6.0)? on page 1-3*
- *Architecture of Virtual Mobile Infrastructure on page 1-4*
- *Components of Virtual Mobile Infrastructure on page 1-6*

About Virtual Mobile Infrastructure

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

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

Why Use Virtual Mobile Infrastructure

Virtual Mobile Infrastructure provides the following benefits:

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

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

What's New in this Release (6.0)?

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

Feature	Description
New Distributed Architecture	Provides three kinds of installation modes to deploy based on your enterprise network requirements: **Management and Compute Node**, **Management Node**, and **Compute Node**.

FEATURE	DESCRIPTION
Improved High Availibility	Supports active-active load balancing mode for management console, and enables you to replace any node at any time.
Upgraded User Workspace to Android 8.1	Provides the latest Android operating system to bring new user experience and better application compatibility.
New Installation Process	Adapts command line based installation, and enables you to configure the server and Secure Access after installation.
New Administration Web Console User Interface	Adapts Trend Micro new user interface standard for web console.
Better Client Rendering	Supports server side rendering as well as the client side rendering for the client mobile devices.

Architecture of Virtual Mobile Infrastructure

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

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

Single Server Installation Model

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

Note

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

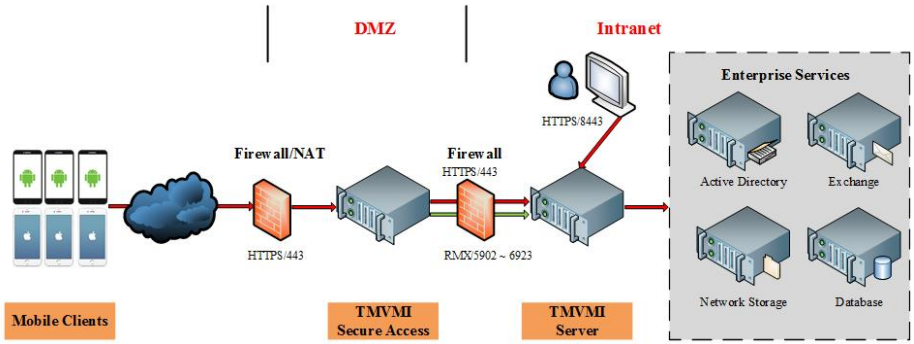


FIGURE 1-1. Trend Micro Virtual Mobile Infrastructure Single Server Installation Model

Multiple Server Installation Model

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

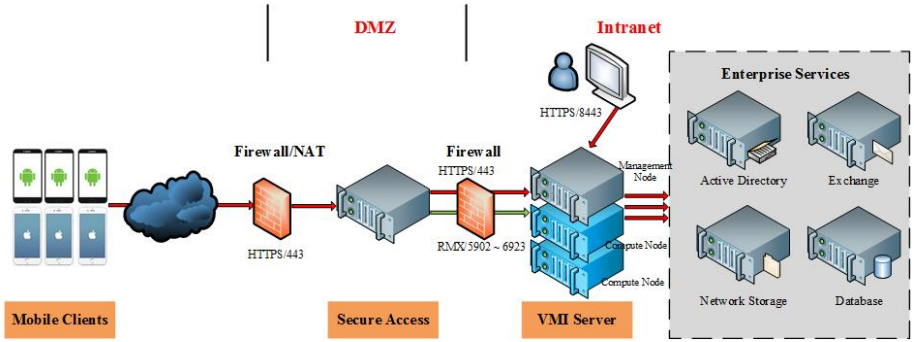


FIGURE 1-2. Trend Micro Virtual Mobile Infrastructure Multiple Server Installation Model

Virtual Mobile Infrastructure High Availability

Virtual Mobile Infrastructure enables you to configure High Availability (HA) to ensure the uninterrupted service to the users. For high availability deployment, install at least

four servers: two Management Nodes, and two Compute Nodes, with all of these servers run in active-active mode. In this setup, both Management Servers provide management features, and host user workspaces, and access the same database. If one server goes down or disconnects from the network for any reason, the other server(s) can still be accessible and work as normal.

Note

Trend Micro recommends configuring an external database for data safety.

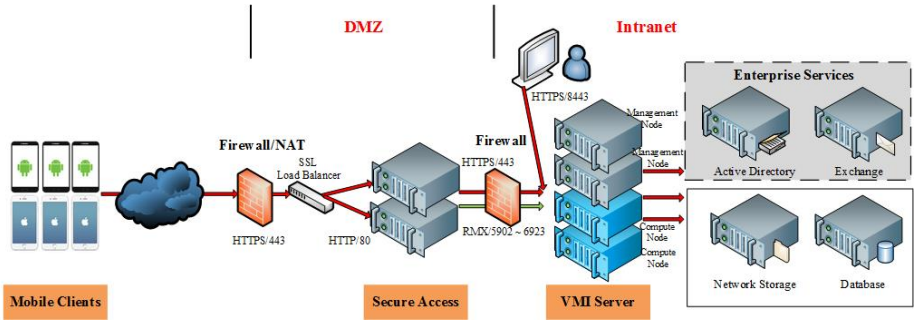


FIGURE 1-3. Trend Micro Virtual Mobile Infrastructure High Availability architecture

Components of Virtual Mobile Infrastructure

The Virtual Mobile Infrastructure system includes the following components:

TABLE 1-1. Virtual Mobile Infrastructure Components

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Virtual Mobile Infrastructure Server	The Virtual Mobile Infrastructure server contains management node and compute node. • Management node provides management console for administrator and web service for user logon, logoff and connection to users's workspace. • Compute node hosts workspaces. Each workspace runs as a Virtual Mobile Infrastructure instance.	Required
Virtual Mobile Infrastructure Mobile Client Application	The mobile client application is installed on the mobile devices. The client application connects with the Virtual Mobile Infrastructure server to allow users to use their workspaces hosted on the server.	Required
Secure Access	The Virtual Mobile Infrastructure Secure Access enables mobile clients to access Virtual Mobile Infrastructure server via Internet. See *Why Use Secure Access on page 1-8* for more information.	Strongly recommended
Active Directory	The Virtual Mobile Infrastructure server imports groups and users from Active Directory.	Optional
External Database	External Database provides scalable data storage for user data. By default, Virtual Mobile Infrastructure server maintains a database on its local hard drive. However, if you want to store the data on an external location, then you will need to configure External Database.	Optional
External Storage	Using this option will enable you to store the user data in an external storage.	Optional

Why Use Secure Access

Virtual Mobile Infrastructure Secure Access enables mobile device clients to securely access the Virtual Mobile Infrastructure server via the Internet. If you do not want to expose the Virtual Mobile Infrastructure Server on the Internet, not even in the DMZ, you will need to install Secure Access. If required, you can install multiple Secure Access through an L4 switch for load balancing.

The following are the advantages of using Secure Access:

- If using Secure Access, you only need to open one IP Address and one port number for mobile clients. The Secure Access receives a mobile device client enrollment request through HTTPS, and relays it to the Virtual Mobile Infrastructure server.
- Secure Access and Virtual Mobile Infrastructure server use a firewall for outbound network connections to ensure security.

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

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

Chapter 2

Getting Started

This chapter contains the following sections:

- *Accessing Virtual Mobile Infrastructure Administration Web Console on page 2-2*
- *The Dashboard Screen on page 2-3*

Accessing Virtual Mobile Infrastructure Administration Web Console

To access the Virtual Mobile Infrastructure Web console:

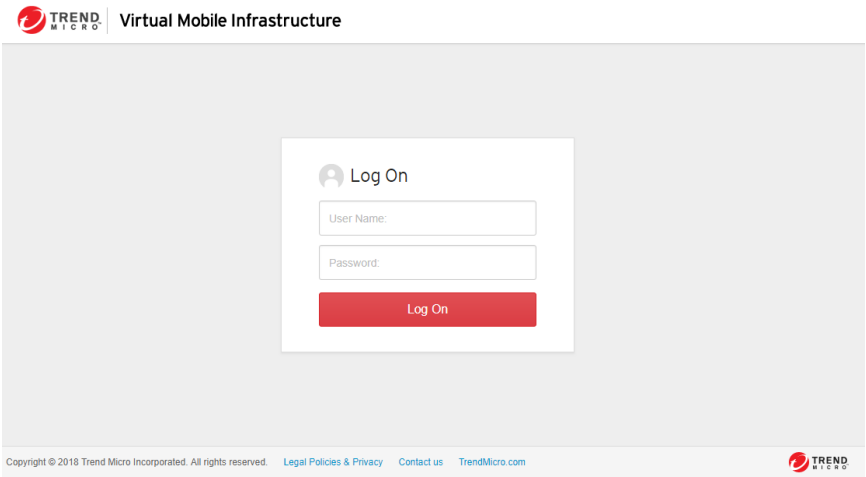
Procedure

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 8-4* 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 displays the following information:

- **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.
- **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 Trend 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 on page 3-2*
- *Managing Groups and Users on page 3-2*
- *Searching Users on page 3-8*
- *Device Management in Virtual Mobile Infrastructure on page 3-8*

User Management in Virtual Mobile Infrastructure

The **User Management** screen enables you to import users and groups from an LDAP server, 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 LDAP server. On importing a group from LDAP server, Virtual Mobile Infrastructure inherits all user account information from the LDAP server database.

Note

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

Importing Groups or Users from LDAP

Before importing groups or users from LDAP server, make sure that you have already configured the LDAP settings. See *Configuring LDAP Settings (Optional) on page 8-5* for the procedure.

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

Procedure

1. Click **Import Users**.

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

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

Note

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

Creating a User Account Locally

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

Before you can create a local user account, make sure that you have disabled the Active Directory integration. See *Disabling LDAP Server on page 8-6* 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**.

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.

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

Before you can export user device ID, make sure that you have already configured the Active Directory settings. See *Configuring LDAP Settings (Optional) on page 8-5* for the procedure.

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

Procedure

1. Navigate to the **Users** 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.
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.

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 on page 4-2*
- *Creating a Cloud Workspace Profile on page 4-2*
- *Deleting Profiles on page 4-4*
- *Changing Profile Order on page 4-3*
- *Deleting Profiles on page 4-4*
- *Kiosk Mode in Virtual Mobile Infrastructure on page 4-4*

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 **Profiles** screen to create Cloud Workspace profiles in Virtual Mobile Infrastructure.

Procedure

1. Click **Add**.
2. Under **Basic Information** section, provide the following information:
   - **Profile name**
   - **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 apply to.
3. Click **Next**.
4. Under **Basic Information** section, add the description for the profile, if required.
5. Under **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.
   - If you want the user status to change to offline after a certain time, select the time from the list.

- 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.

6. Under **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, hide or unhide an application from the list by selecting a built-in or server application and clicking **Delete**, **Hide** or **Unhide** repectively.

7. 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 *Changing User or Group Profile on page 3-6* 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

Managing Applications

This chapter contains the following sections:

- *Cloud Workspace Applications on page 5-2*
  - *Uploading Applications to Server on page 5-3*
  - *Adding a Web Clip to the Server on page 5-3*
  - *Deleting an Application or a Web Clip from the Server on page 5-4*
  - *Application Security Risk Levels on page 5-4*

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.

Adding Application Category

You can add application categories using **Cloud Workspace Applications** screen on Virtual Mobile Infrastructure server.

Procedure

1. Under **Server Applications and Web Clips** section, click **Add Category**.

   The **Add Category** screen pops up.

2. Type the **Category Name** and then click **OK**.

   The category is added to the list, and can be selected while adding an application.

Editing or Deleting Application Category

You can edit or delete application categories using **Cloud Workspace Applications** screen on Virtual Mobile Infrastructure server.

Procedure

1. Under **Server Applications and Web Clips** section, do one of the following:

   - To edit an application cateogry, click **Edit Cateogry** before the category name on the screen, modify the information on the pop-up screen, and then click **OK**.
   - To delete an application cateogry, click **Delete Cateogry** before the category name on the screen, and then click **OK**.

Uploading Applications to Server

Use the **Cloud Workspace Applications** 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.

Application Security Risk Levels

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

TABLE 5-1. 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.
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.

Component	Description	Required or Optional
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.

Chapter 6

Managing Servers

This chapter contains the following sections:

- *Configuring External Storage on page 6-2*
- *Servers in Virtual Mobile Infrastructure on page 6-2*
- *Starting or Stopping a Server on page 6-4*
- *Adding a Server on page 6-4*
- *Editing a Server on page 6-5*
- *Removing a Server on page 6-6*
- *Configuring Server High Availability (HA) on page 6-7*

Configuring External Storage

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

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

Important

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

Procedure

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

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

Servers in Virtual Mobile Infrastructure

Virtual Mobile Infrastructure enables you to add multiple servers to increase the capacity to accommodate more users and support large-scale deployment. In the case of multiple servers, 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.

Typical Server Deployment Scenarios

The following are the typical deployment scenarios for Virtual Mobile Infrastructure servers:

- **Single Server Deployment (All-in-one Server)**:

  For the all-in-one server setup, you must install and configure the server as Management and Compute Node. However, running large number of user workspaces utilizes much of the hardware resources (CPU, memory, disk and so on). Therefore it may affect the smooth running of administration tasks.

- **Multiple Server Deployment**:

  For the multiple server setup, you must first install a Management Node, and then proceed to installing one or more Compute Nodes as required.

  The Management Node only provides administration features, and provides connectivity with mobile clients to log on.

  The Compute Node runs user workspaces. You can add multiple Compute Nodes to add large number of user workspaces when required.

- **High Availability Deployment**:

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

Note

If you changed the time on a server, multiple server statuses may not synchronize. Trend Micro suggests rebooting server computer to proceed after deployment.

Starting or Stopping a Server

Use the **Servers** 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

Important

To follow this procedure, you must already have a **Management and Compute Node** or a **Management Node** installed. If you are performing a fresh installation, refer to the *Installation and Deployment Guide* for the installation procedures.

To add a server, install a new server on a separate physical computer or on a virtual machine, and then configure it as a **Management and Compute Node**, a **Management Node**, or a **Compute Node** during installation.

Before you can add and configure a Virtual Mobile Infrastructure server, make sure to configure an external storage on current Virtual Mobile Infrastructure. See *Configuring External Storage on page 6-2* for the procedure.

Procedure

1. Stop the current server. See *Starting or Stopping a Server on page 6-4* for the stoping procedure.

2. Start installing a new server (as explained in the *Installation and Deployment Guide*).
3. During installation, when the setup requires you to select the type of server you want to install, do one of the following:
   - To install **Management and Compute Node**:

     Type `configure init server 1 vmi <first server's IP address>`.
   - To install **Compute Node** only (for multiple server setup):

     Type `configure init server 2 vmi <first server's IP address>`.
   - To install **Management Node** only (for multiple server setup):

     Type `configure init server 3 vmi <first server's IP address>`.

Note

Refer to the topic *Installing Virtual Mobile Infrastructure Server on a Bare Metal Server* in *Installation and Deployment Guide* for the detailed procedure.

4. If you want to add more servers, repeat *Step 2 on page 6-5* and *Step 3 on page 6-5* of this procedure.
5. After you have finished installing all the servers, go to the **Servers** screen on the administration console of the first server, select all the servers, and then click **Start Server**.

Editing a Server

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

Procedure

1. Click the server name whose details you want to edit.

2. Click **Edit** at the bottom of the screen.
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 **Servers** screen to remove a Virtual Mobile Infrastructure server.

Important

You can only remove a server if the server's status shows **Error**.

Procedure

1. Disconnect the server from network or power off the server to change it status to show as **Error**.
2. Select a server, and click **Remove**.

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. You can configure four Virtual Mobile Infrastructure servers and Secure Access where all servers and Secure Access access the

same respective database. If one server goes down or disconnects from the network for any reason, the other server(s) can still be accessible and work as normal.

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

Important

Before performing this procedure, make sure:

- to configure an external storage on current Virtual Mobile Infrastructure server. See *Configuring External Storage on page 6-2* for the procedure.
- to configure an external database on current Virtual Mobile Infrastructure server.
- that you have added and configured at least two Virtual Mobile Infrastructure servers and two Virtual Mobile Infrastructure Secure Access. If you have configured only one server and/or Secure Access, set up and configure at least one more server and one more Secure Access to act as backup to the other server and Secure Access.

The typical Virtual Mobile Infrastructure HA configuration is as follows:

- Two Virtual Mobile Infrastructure servers, with both of the servers configured as **Management Node**
- Two Virtual Mobile Infrastructure servers, with both of the servers configured as **Compute Node**
- An external storage
- An external database

The configuration steps are explained in the table below:

STEP NUMBER	STEP DETAILS	REFERENCE
1	Install first Virtual Mobile Infrastructure server, and: • configure the server as **Management Node** during installation. • configure an external database during installation using the following command: `configure init server 3 db <db ip address> <db name> <db username> [db port]`	Refer to the *Installation and Deployment Guide* for the installation procedures.
2	Open the first server web console, and provide the activation code.	Refer to the topic *Accessing Virtual Mobile Infrastructure Administration Web Console* in *Installation and Deployment Guide* to help on accessing the web console. Refer to the topic *Activating Your Product* in *Installation and Deployment Guide* for the activation procedure.
3	Configure an external storage on first server's web console.	Refer to the topic *Configuring External Storage on page 6-2* for the procedure.
4	Install second Virtual Mobile Infrastructure server, and configure the server as **Management Node** during installation and enable it to access the first server using the following command: `configure init server 3 vmi <first server's IP address>`	Refer to the *Installation and Deployment Guide* for the installation procedures.

Step Number	Step Details	Reference
5	Install two servers and configure them as **Compute Node**. During installation, enable the second server to access the first server using the following command: `configure init server 2 vmi <first server IP address>`	Refer to the *Installation and Deployment Guide* for the installation procedures.
6	Open first server's web console, and go to the **Servers** screen. Both of the servers should now be displayed on this screen under **Management Node** section, as well as under **Compute Node** section. Select the second server, and click **Start** to start the server.	Refer to the topic *Starting or Stopping a Server on page 6-4* for the procedure.
7	Install first Virtual Mobile Infrastructure Secure Access, and configure it to access the first server using the following command: `configure init server <first server's IP address>`	Refer to the *Installation and Deployment Guide* for the installation procedures.
8	Install second Virtual Mobile Infrastructure Secure Access, and configure it to access the second server using the following command: `configure init server <second server's IP address>`	Refer to the *Installation and Deployment Guide* for the installation procedures.
9	On you L4 switch, configure a virtual IP address to link client logon requests to the first and second Secure Access.	

In this configuration, both the Secure Access and Virtual Mobile Infrastructure server work in active-active mode. You can now access the web console from either of the servers. When the client logs on, the first or the second server processes the request. Both the servers use the same database. Therefore, if the client logs on through the virtual IP address, the client is able to access the same workspace.

Upgrading Virtual Mobile Infrastructure and Secure Access

Important

Before performing the upgrade to Virtual Mobile Infrastructure and Secure Access, 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.

Upgrading Virtual Mobile Infrastructure Server

Procedure

1. Download the upgrade package for Virtual Mobile Infrastructure from the download center.
2. Open the administration web console, and navigate to **Servers** screen.
3. Click **Upload Upgrade File**, select the `bz2` upgrade file, and click **Close**.
4. Click **Upgrade** to upgrade the server to the newer version.
5. Wait until the upgrade process is finished, and then click **Reboot** to reboot the Virtual Mobile Infrastructure server.

After rebooting, navigate to the administration web console, and check the server version number on **Administration** > **About** to confirm the latest version. If you have multiple servers installed, all the servers upgrade at the same time.

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.

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 eth0, type the following command:
     - `configure network interface ipv4 eth0 <ipaddress/submask_netmask_bits>`
   - 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 7

Managing Reports and Logs

This chapter contains the following sections:

- *Reports in Virtual Mobile Infrastructure on page 7-2*
- *Generating a Quick Report on page 7-3*
- *Configuring Scheduled Report on page 7-3*
- *Logs in Virtual Mobile Infrastructure on page 7-4*
- *Viewing Event Logs on page 7-5*
- *Deleting Logs Manually on page 7-7*
- *Scheduling Log Deleting on page 7-8*

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:

- **Cloud Workspace Usage Reports**:
  - **Users Active 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.
  - **Mobile App Network Data Consumed**–shows the top 10 applications that consumed the most data traffic from all the users combined.
- **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**

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:
  - **Never**
  - **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
  - Never
  - 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

Note

Application usage log only appears if **Enable App Usage Log** option is selected on **System Settings** > **Advanced** screen.

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

Viewing Event Logs

The **Event Logs** tab on the **Logs** screen records all the events occurred on the administration web console.

Procedure

1. On the **Event 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.
3. If you want to export logs to your computer in `csv` format, click **Export**.

Viewing Audit Logs

The **Audit Log** tab on the **Logs** 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 **Audit Log** tab, specify the query criteria for the logs you want to view. The parameters are:
   - **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.
3. If you want to export logs to your computer in `csv` format, click **Export**.

Viewing Application Usage Log

The **Application Usage Log** tab on the **Logs** screen records the usage of all the apps installed on user workspace.

Note

Application usage log only appears on the **Logs** screen if **Enable App Usage Log** option is selected on **System Settings** > **Advanced** screen.

Procedure

1. On the **Application Usage 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.
   - **Application name**: type the application name whose related 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.
3. If you want to export logs to your computer in `csv` format, click **Export**.

Log Maintenance

When users or administrators generate event logs, audit logs, or application 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 **Logs** screen.

Deleting Logs Manually

Procedure

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

Scheduling Log Deleting

Procedure

1. On the **Logs** 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 8

Administration and System Settings

This chapter contains the following sections:

- *Modifying Administrator Account Information on page 8-4*
- *Configuring LDAP Settings (Optional) on page 8-5*
- *Configuring Mobile Client Settings on page 8-7*
- *Configuring Microsoft Exchange Server and Office 365 Settings (Optional) on page 8-8*
- *Configuring Network Settings on page 8-9*
- *Configuring External Storage on page 6-2*
- *Configuring Email Notifications on page 8-11*
- *Configuring Syslog (System Logs) on page 8-13*
- *Configuring Advanced Settings on page 8-14*
- *Product License on page 8-15*
- *Configuring Re-branding on page 8-15*

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 Admin** (default): This role has the maximum access to all settings on the server.
- **Application Admin**: The administrator with this role can only manage applications on user workspace.
- **User Admin**: The administrator with this role can only manage users on administration web console.

The following table provides the details regarding privileges for **Super Administrator**, **Application Administrator** and **User Administrator** roles in Virtual Mobile Infrastructure.

TABLE 8-1. Administrators Privileges in Virtual Mobile Infrastructure

SERVER COMPONENTS	SUPER ADMINISTRATOR	APPLICATION ADMINISTRATOR	USER ADMINISTRATOR
Dashboard	□	□	□
User management	□		□
Mobile device management	□		□
Profile management	□		□
Application management	□	□	
Reports	□		

SERVER COMPONENTS	SUPER ADMINISTRATOR	APPLICATION ADMINISTRATOR	USER ADMINISTRATOR
Logs	□		
System settings	□		
Administrator management	□		
Help	□	□	□

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**
   - **Role**: Select a role for the administrator. A Super Administrator can manage all the settings, an Application Administrator can only manage applications on user workspace, and a User Administrator can only manage users on administration web console.
4. Click **Save** on **Administrator Account Management** screen.

Modifying Administrator Account Information

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

Procedure

1. On the **Administrator Accounts Management** screen, click **Edit** under the account information that you want to edit.
2. Update the following fields as required:
   - **Email address**: add an email address to receive email notification messages from Virtual Mobile Infrastructure.
   - **Role**
   - **Site**

   Note

   Role and **Site** cannot be modified for the **admin** account.
3. Click **Save**.

Changing Administrator Account Password

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

Attention

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

Procedure

1. Under **admin** section, click **Change password**.

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

2. Use the following fields:

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

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

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**.
- Select **Enable client side rendering** option to set client side rendering mode to default on TMVMI client.
- From the **Graphics Options** drop-down menu, select one of the following options:
  - **Performance**: This option provides more speed, but less quality (screen clarity), and utilizes less bandwidth.
  - **Balance** (default): This option provides balance between quality (screen clarity) and speed.
  - **Quality**: This option provides more quality (screen clarity), but less speed, and utilizes more bandwidth.

3. Click **Save**.

Configuring Microsoft Exchange Server and Office 365 Settings (Optional)

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

Note

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

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

Procedure

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

Note

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

6. Click **Save**.

Configuring Network Settings

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

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

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

Procedure

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

   Note

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

2. Under the **Proxy** section, select **Use the following proxy settings**, and configure the following:

   - **Host name or IP address**
   - **Port number**
   - **Proxy server authentication**
     - **User name**
     - **Password**
     - **Bypass proxy for these addresses**

     Note

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

3. Type a URL in the **Test address** field, and then click **Test Connection** to verify proxy settings.
4. Select one of the following options for **Apply proxy to**:
   - **Server and Workspace**
   - **Server only**
   - **Workspace only**
5. Click **Save**.

Configuring External Storage

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

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

Important

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

Procedure

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

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

Configuring Email Notifications

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

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

Procedure

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

   Note

   This test does not verify the user name and password configured to access the SMTP server.
3. Select **Automatically send email notification to new users** if you want to send an invitation email to new users that are added from LDAP.
4. On the **Invitation Email Template Settings** tab, type the following:
   - **Subject**–the subject of the email message.
   - **Message**–the body of the email message.

   Note

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

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

Note

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

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

Configuring Syslog (System Logs)

Configure syslog server settings to save server debug logs.

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

Procedure

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

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.
- Screen resolution setting for user workspace.

Use the **Advanced** tab in **System Settings** to configure advance settings for Virtual Mobile Infrastructure.

Procedure

1. Click **System Settings** > **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:
        - **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 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.

4. Click **Save**.

Configuring Re-branding

Procedure

1. Go to **System Settings** > **Rebranding** screen
2. Select **default**.
3. Click **Download Sample**, and prepare your source files based on the downloaded sample.
4. Click **Upload**, select the source file you have just prepared, and then click **Close**.
5. Click **Apply**.

The new resource files will be deployed to the client mobile devices when the client mobile devices log on to the server next time.

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**.

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: APEM68494/180927