TREND MICRO™

3.0 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.: APEM37233/151022

Release Date: November 2015

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

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 (3.0)? 1-3

What's New in Release 2.1? 1-4

What's New in Release 2.0? 1-5

What's New in Release 1.5? 1-6

What's New in Release 1.1? 1-7

Architecture of Virtual Mobile Infrastructure 1-8
- Single Server Installation Model 1-9
- Multiple Server Installation Model 1-9

Components of Virtual Mobile Infrastructure 1-10
- Why Use Secure Access 1-12

Chapter 2: Getting Started

Accessing Virtual Mobile Infrastructure Administration Web Console 2-2

The Dashboard Screen 2-3

Upgrading Virtual Mobile Infrastructure 2-4

Chapter 3: Managing Users

User Management in Virtual Mobile Infrastructure 3-2

Managing Groups and Users 3-2
Importing Groups or Users from Active Directory 3-2
Creating a User Account Locally 3-3
Disabling or Enabling a User 3-4
Enabling or Disabling VIP Setting for a User 3-4
Wiping User Workspace 3-5
Resending Invitation to a User 3-5
Changing User or Group Profile 3-6
Delete a User or a Group 3-6

Searching Users 3-7

Chapter 4: Managing Profiles

Profiles in Virtual Mobile Infrastructure 4-2

Deleting Profiles 4-2

Creating a Profile 4-2

Changing Profile Order 4-3

Kiosk Mode in Virtual Mobile Infrastructure 4-4
Enabling or Disabling Kiosk Mode 4-4

Chapter 5: Managing Applications

Application List in Virtual Mobile Infrastructure 5-2
Uploading Applications to Server 5-2
Adding a Web Clip to the Server 5-2
Deleting an Application or a Web Clip from the Server 5-3
Show or Hide Default Applications in User Workspace 5-3
Application Security Risk Levels 5-4

Single Sign On Processor 5-4
Preparing an Application for Single Sign On 5-5
Deleting Application from Single Sign On Processor 5-5

Chapter 6: Managing Servers

Servers in Virtual Mobile Infrastructure 6-2
Starting or Stopping a Server 6-2
Adding a Server 6-2

Editing a Server 6-3
Removing a Server 6-4
Configuring Server High Availability (HA) 6-5

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 Logs 7-4
Log Maintenance 7-5

Chapter 8: Administration Settings

Modifying Administrator Account Information 8-2
Changing Administrator Account Password 8-2

Configuring Email Notifications 8-3

Configuring LDAP Settings (Optional) 8-4
Disabling LDAP Server 8-5

Configuring Mobile Client Settings 8-6

Configuring Microsoft Exchange Server Settings (Optional) 8-7

Configuring Proxy Settings 8-8

Configuring External Storage (Optional) 8-9

Configuring OAuth 2.0 Authentication 8-10

Generating Client Enrollment Certificate 8-12

Managing Wallpapers 8-13

Managing Certificates 8-13
Uploading a Certificate 8-14
Deleting Certificate 8-14

Product License 8-15

Index

Preface

Preface

Welcome to the Trend Micro™Virtual Mobile Infrastructure™ version 3.0 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 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 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 on page 1-2*
- *Why Use Virtual Mobile Infrastructure on page 1-2*
- *What's New in this Release (3.0)? on page 1-3*
- *Architecture of Virtual Mobile Infrastructure on page 1-8*
- *Components of Virtual Mobile Infrastructure on page 1-10*

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 Android operating system, which is accessible via 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 (3.0)?

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

Feature	Description
Changed Product Name	Adapts a new product name; Virtual Mobile Infrastructure.
Enforced Signin Security Level	Enables administrators to enforce signin security levels restrictions for user workspace on mobile device.

Feature	Description
Updated Invitation Email Template	Includes a URL in email template to allow users to add server IP address and user name in the app.
Instant Logout	Allows users to immediately signout from the app, without waiting for server's response.

What's New in Release 2.1?

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

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

Feature	Description
Enforced Signin Security Level	Enable administrators to enforce signin security levels for user workspace.

Note

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

What's New in Release 2.0?

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

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

Feature	Description
Re-branding Tool	Includes a tool to customize the product branding items, such as product name, logo, banner, images, server address and other branding items on the Safe Mobile Workforce server and in the client app.

Note

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

What's New in Release 1.5?

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

Feature	Description
Camera Support	Added support for camera on iOS mobile devices for the applications that are installed on the user workspaces.
Windows Client App Enhancement	Enhanced features and improved Windows mobile client application performance.
Increased Concurrent Sessions Support	Increased the concurrent sessions supported by the server.
Supports High Availability	Added support for High Availability (HA) to ensure uninterrupted service.
Reduced Bandwidth Consumption	Reduced Internet bandwidth requirements for the client app to reduce data usage and improve user experience.
Added Options to Choose Optimize Quality or Speed	Provides option to choose between optimize quality or speed on mobile devices, to optimize the Internet bandwidth and improve user experience.
Bypass Proxy Settings	Added support for bypass proxy settings for workspaces.
OAuth 2.0 Authentication Support	Added OAuth 2.0 Authentication support for user enrollment.

Feature	Description
User Logon Process Enhancement	Enhanced the user log on process to provide better user experience.
User Status Reset Setting	Added option to configure time after which the server resets the user status from idle to offline.
Email Notification	Added an email notification on real mobile device to notify users for the email received on the user workspace.
Client Version Verification	Added a verification for the Safe Mobile Workforce client software version before enroll. If the client software version does not match the required version, the client will not be enrolled.

Note

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

What's New in Release 1.1?

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

Feature	Description
Integration with Trend Micro Control Manager	The integration with Trend Micro Control Manager enables you to log on to the Control Manager Web console to monitor Safe Mobile Workforce usage and system status. You can also deploy Safe Mobile Workforce license from the Control Manager Web console.
Single Sign On	Includes the app-wrapper technology to prepare applications for single sign on, without involving the app developer for processing.
Client app for Windows 8	Introduces Safe Mobile Workforce client app for Windows 8 mobile devices.

Feature	Description
Show/Hide Built-in Apps	Enables you to show or hide the following built-in apps on the user workspaces: • Email • Browser • Downloads • Calender • Contacts • Calculator
Camera Support (Android Only)	Enables the camera support for applications installed on the user workspaces.
Improved Client Performance	Significantly improves the mobile client performance by optimizing mobile device's memory and Internet bandwidth to provide the better user experience.
Improved Application Support	Improves application support for more Android apps on a user workspace.
Improved Authentication Security	Introduces restriction settings for unsuccessful sign on attempts.
Disable Screenshots (Android Only)	Restricts users from taking screenshots of their workspaces on their mobile devices.

Note

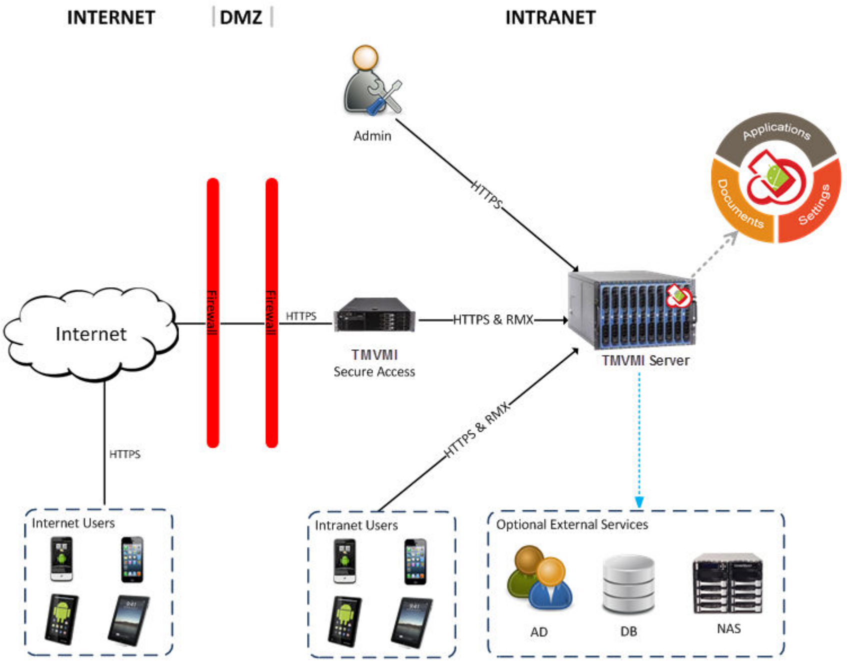
The product name Safe Mobile Workforce was changed to Virtual Mobile Infrastructure in version 3.0.

Architecture of Virtual Mobile Infrastructure

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

Single Server Installation Model

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

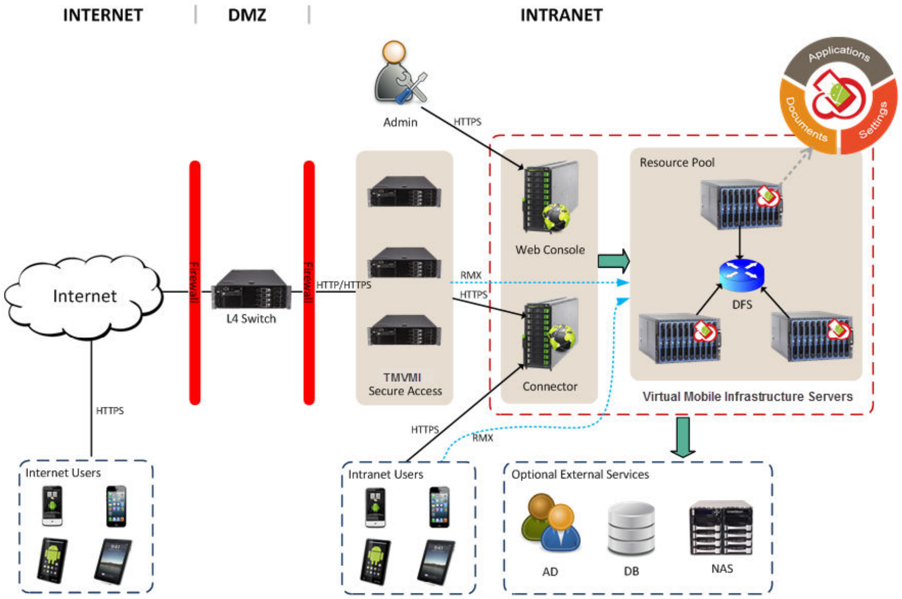


Note: RMX: Optimized remote access protocol to display image on mobile device

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.



Note: 1) All components except TMVMI Secure Access can be installed in one machine.
2) TMVMI Secure Access can be configured to support HTTP if L4 Switch has SSL offload feature.
3) RMX: Optimized remote access protocol to display image on mobile device

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

Components of Virtual Mobile Infrastructure

The Virtual Mobile Infrastructure system includes the following components:

TABLE 1-1. Virtual Mobile Infrastructure Components

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Virtual Mobile Infrastructure Server	The Virtual Mobile Infrastructure Server contains Web Console, Web Service, Controller and Resource Pool. • Web console provides central management console for administrator. • Web service manages user logon, logoff and the connection to user's workspace. • Controller allows Web console to manage a resource pool. • Resource pool hosts workspaces. Each workspace runs as a Virtual Mobile Infrastructure instance.	Required
Virtual Mobile Infrastructure Mobile Client Application	The mobile client application is installed on the mobile devices. The client application connects with the Virtual Mobile Infrastructure server to allow users to use their workspaces hosted on the server.	Required
Secure Access	The Virtual Mobile Infrastructure Secure Access enables mobile clients to access Virtual Mobile Infrastructure server via Internet. See *Why Use Secure Access on page 1-12* for more information.	Optional
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

Component	Description	Required or 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 mobile device client enrollment request through HTTPS, and relays it to the Virtual Mobile Infrastructure server.

- Secure Access and Virtual Mobile Infrastructure server use firewall for outbound network connections to ensure security.

Secure Access can be deployed in DMZ or 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*
- *Upgrading Virtual Mobile Infrastructure on page 2-4*

Accessing Virtual Mobile Infrastructure Administration Web Console

To access Virtual Mobile Infrastructure Web console:

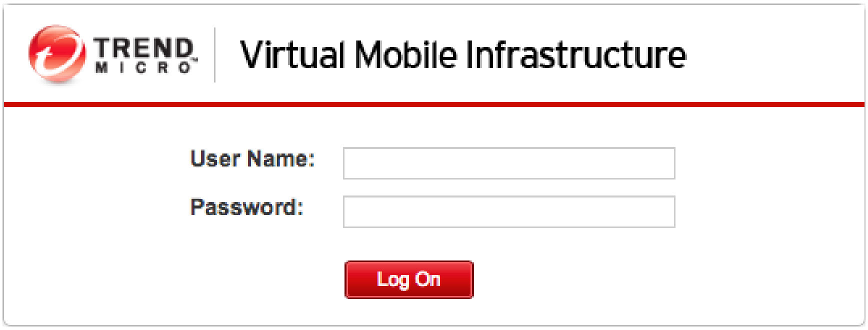
Procedure

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

   https://<Virtual Mobile Infrastructure_domain_name_or_IP_address>

   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 8-2* 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.
    - **Top 5 Web Clips Used**–shows the top five (5) most used Web clips.
    - **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.

Upgrading Virtual Mobile Infrastructure

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

http://esupport.trendmicro.com/solution/en-US/1112879.aspx

Chapter 3

Managing Users

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 3-7*

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 8-4* 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 groups or users that you want to import from the search result, and then click **Import**.

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

Creating a User Account Locally

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 8-5* for the procedure.

Use the **User Management** screen to create a user account locally.

Procedure

1. Click **Add User**.

   Add A New User screen appears.

2. Configure the following:

   - **User name**
   - **First name**
   - **Last name**
   - **Email address**
   - **Group**—select a group from the drop-down menu for the user.
   - **Profile**—select a profile from the drop-down menu for the user.

3. Click **Add**.

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

Disabling or Enabling a User

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

Procedure

1. In the user list on the left side of the screen, click the user name that you want to enable or disable.

2. Do one of the following:

    - To disable user, click **Disable User**, and then click **OK** on the pop-up dialog box to confirm.

    - To enable user, click **Enable User**.

Enabling or Disabling VIP Setting for a User

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

CAUTION!

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

Note

See *Configuring Mobile Client Settings on page 8-6* to configure the number of users you can set as VIP.

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

Procedure

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

Wiping User Workspace

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

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

⚠ CAUTION!

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

Procedure

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

Resending Invitation to a User

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

Procedure

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

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

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 **Change Profile** dialog box pops up.

3. Select one of the following:

   - **Inherit from parent group**
   - **Specified**

4. Click **Save** on the **Change Profile** 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**.

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**.

Chapter 4

Managing Profiles

This chapter contains the following sections:

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

Profiles in Virtual Mobile Infrastructure

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.

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 8-4* for the procedure.

2. Select the profiles that you want to delete.

3. Click **Delete**.

Creating a Profile

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

Procedure

1. Click **Add**.

2. Under **Step 1: Basic Information** section, provide the following information:

    - Profile name

- **Description**
- **Copy from**–select a previously created profile whose settings you want to copy. By default, Virtual Mobile Infrastructure copies settings from the **Default Profile**.
- **Storage limit**–set a storage limit for the profile.

3. Click **Next**.
4. Under **Step 2: Workspace System Settings** section, 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.
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 **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.

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 Single App 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:

- *Application List in Virtual Mobile Infrastructure on page 5-2*
- *Uploading Applications to Server on page 5-2*
- *Adding a Web Clip to the Server on page 5-2*
- *Deleting an Application or a Web Clip from the Server on page 5-3*
- *Show or Hide Default Applications in User Workspace on page 5-3*
- *Application Security Risk Levels on page 5-4*
- *Single Sign On Processor on page 5-4*
- *Preparing an Application for Single Sign On on page 5-5*
- *Deleting Application from Single Sign On Processor on page 5-5*

Application List in Virtual Mobile Infrastructure

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

Uploading Applications to Server

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

Procedure

1. Click **Add Application**.

   The **Add Application** screen pops up.

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

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

3. Click **OK**.

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

Adding a Web Clip to the Server

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

Procedure

1. Click **Add Web Clip**.

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

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

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

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

4. Click **OK**.

The Web clip appears in the applications list.

Deleting an Application or a Web Clip from the Server

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

Procedure

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

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

Show or Hide Default Applications in User Workspace

Use the **Application Management** screen to show or hide apps on the user workspaces.

Procedure

1. On the default application that you want to show or hide, click ✓ or ✖ icon to toggle the setting.

   The applications with ✓ icon will be shown on the user workspaces, while the applications with ✖ icon will be hidden.

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	ℹ	Malicious applications can collect users' personal and private data such as pictures, contacts, videos and audio recordings.
Notable	ℹ	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.
Safe	ℹ	These are the applications that are safe to use.
Unknown	ℹ	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

Single Sign On Processor

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

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

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

Preparing an Application for Single Sign On

Note

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

Procedure

1. Navigate to the following URL:

   https://<Virtual Mobile Infrastructure_domain_name_or_IP_address>/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>/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 6

Managing Servers

This chapter contains the following sections:

- *Servers in Virtual Mobile Infrastructure on page 6-2*
- *Starting or Stopping a Server on page 6-2*
- *Adding a Server on page 6-2*
- *Editing a Server on page 6-3*
- *Removing a Server on page 6-4*
- *Configuring Server High Availability (HA) on page 6-5*

Servers in Virtual Mobile Infrastructure

Virtual Mobile Infrastructure enables you to add multiple servers to increase the capacity to accommodate more users. In the case of multiple servers, Virtual Mobile Infrastructure balances the load between servers to achieve maximum efficiency.

Virtual Mobile Infrastructure enables you to add multiple servers to increase the capacity to accommodate more users. In the case of multiple servers, Virtual Mobile Infrastructure balances the load between servers to achieve maximum efficiency.

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 8-9* 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.

3. Click **Next**.

4. Under **Step 2: Server Information**, type the server name and its description.

5. Click **Next**.

6. Under **Step 3: Workspace Network Connection**, select one of the following:

   - **NAT: Workspaces share the server's IP address**–select this option if you want to share the server's IP address with the workspaces.

   - **IP Range: Assign IP address to workspaces**–select this option if you want to assign individual IP address to each workspace.

     - **Workspace IP range**–type a range of IP addresses that will used by the workspaces.

       Note

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

     - **Subnet mask**

     - **Gateway IP address**

     - **DNS server IP address**

7. Click **Save**.

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. If the server is running, click **Stop** to stop the server, and then click **OK** to confirm.
3. Click **Edit**.
4. Update the following fields as required:
   - **Basic Information**
     - **Server name**
     - **Description**
   - **Workspace Network Connection**
     - **NAT: Workspaces share the server's IP address**–select this option if you want to share the server's IP address with the workspaces.
     - **IP Range: Assign IP address to workspaces**–select this option if you want to assign individual IP address to each workspace.
       - **Workspace IP range**–type a range of IP addresses that will used by the workspaces.
       - **Subnet mask**
       - Gateway IP address
       - DNS server IP address
5. 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**.

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 6-2* 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. 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
  ```

4. Press **Enter**.

   The HA on Virtual Mobile Infrastructure is enabled or disabled.

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 6-6* 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 6-5* of procedure *Enabling or Disabling High Availability (HA) on page 6-5*.

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**.

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 Logs on page 7-4*
- *Deleting Logs Manually on page 7-5*
- *Scheduling Log Deleting on page 7-5*

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 the count and percentage of users in the following statuses:
        - Active
        - Idle
        - Offline
        - Disabled
    - Users Active/Idle Time–provides the time in hours for which the users were in active or idle statuses.
    - Mobile Apps Launched Times–provides the number of times each application was launched.
    - Web Apps Launched Times–provides the number of times each Web clip was launched.
- System Resource Usage Reports–provides the following information in percentage in the graphical format:
    - Memory Usage
    - Storage Usage
    - CPU Usage

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 log on server so that you can audit logs whenever required. Virtual Mobile Infrastructure server records the following logs:

- Successful logon or unsuccessful logon attempt
- Successful user logoff
- Screen capture on iOS mobile devices

You can search specific user events by specifying user names and time periods.

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**.

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 8

Administration Settings

This chapter contains the following sections:

- *Modifying Administrator Account Information on page 8-2*
- *Changing Administrator Account Password on page 8-2*
- *Configuring Email Notifications on page 8-3*
- *Configuring LDAP Settings (Optional) on page 8-4*
- *Configuring Mobile Client Settings on page 8-6*
- *Configuring Microsoft Exchange Server Settings (Optional) on page 8-7*
- *Configuring Proxy Settings on page 8-8*
- *Configuring External Storage (Optional) on page 8-9*
- *Configuring OAuth 2.0 Authentication on page 8-10*
- *Managing Wallpapers on page 8-13*
- *Managing Certificates on page 8-13*
- *Product License on page 8-15*

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**
   - **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.

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 Notifications** screen, under the **Email Settings** section, 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. Under **Invitation Email Template**, type the following:

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

   Note

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

4. Under **Reset Password Template**, type the following:

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

   Note

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

5. Click **Save** to save settings.

Configuring LDAP Settings (Optional)

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

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

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

Procedure

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

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

Disabling LDAP Server

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

Procedure

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

3. Click **Save**.

Configuring Mobile Client Settings

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

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

Procedure

1. On the **System Settings** screen, click the **Mobile Client** tab.
2. Under **Remember Password** section, if you want to allow users to save their passwords on their mobile devices, select **Allow users to save password on mobile device**.
3. Under **Unsuccessful Signin Restriction Settings** section, if you want users to wait for a certain time before retrying after typing in a wrong password, select **Enable unsuccessful signin restrictions for Active Directory users**, and then select the number of attempts and the waiting time from the drop-down lists.
4. Under **User Password Security Level Setting** section, if you want to configure the password security level for user workspaces on their mobile devices, select a security option from the **User password security level** drop-down list.

   Only your selected option and the ones below it will be available to the users, and other options will be disabled.

   For example, if you select **Pin**, only **Pin** and **Password** security options will be available to users, and **None** and **Pattern** will be disabled on their mobile devices.

   Note

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

5. Under **User Idle Time Setting** section, configure the time in minutes for the server, after which the server changes the user status from idle to offline.

6. Under **VIP User Setting** section, set the number of VIP users to be granted uninterrupted resources.

   By default, the number of VIP users is one-half of the total user capacity.

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

   - **Domain name or IP address**

     Note

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

   - **Port number**

8. Click **Save**.

Configuring Microsoft Exchange Server 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 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 settings.

Procedure

1. On the **System Settings** screen, click the **Active Directory** tab.

2. Make sure that the **Use Active Directory** checkbox is selected, and the Active Directory 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. 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.

Virtual Mobile Infrastructure uses network interface **eth0** for control and management information. Therefore, Trend Micro recommends connecting the external storage to network interface **eth0**.

Use the **External Storage** tab in **System Settings** to configure external storage for Virtual Mobile Infrastructure server.

Procedure

1. On the **System Settings** screen, click the External Storage tab.

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 **System Settings**.

Configuring OAuth 2.0 Authentication

Virtual Mobile Infrastructure enables you to use OAuth 2.0 protocol for user authorization. OAuth 2.0 provides specific authorization flows for Web applications, desktop applications, mobile phones, and living room devices. Virtual Mobile Infrastructure Secure Access includes the Authorization Server, which is required for OAuth 2.0 authentication.

Before you can configure OAuth 2.0 authentication settings, you must configure **Secure Access Settings** in **Mobile Client** tab. Refer to *Configuring Mobile Client Settings on page 8-6*.

Use the **Advanced** tab in **System Settings** to configure OAuth 2.0 Authentication settings for Virtual Mobile Infrastructure.

Procedure

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

2. Select **Enable OAuth 2.0 Authentication**

3. 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 URI**: The Authorization URI for the users to provide certificate authorization.

- **Token URI**: The Token URI 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 URI**: The Account Information URI 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 URI**, **Token URI** and **Account Information URI** fields are automatically filled with the relevant information.

4. (Optional) Click **Test Connection** to verify your settings.

5. Click **Save**.

What to do next

Generate individual certificates for mobile users for enrollment. See *Generating Client Enrollment Certificate on page 8-12*.

Generating Client Enrollment Certificate

Before following this procedure, make sure that you have already configured OAuth 2.0 Authentication. See *Configuring OAuth 2.0 Authentication on page 8-10* 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 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**.

Managing Certificates

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

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

Uploading a Certificate

Procedure

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

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

   Important

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

Deleting Certificate

Procedure

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

Product License

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

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

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: APEM37233/151022