System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

# Fortinet Firewall Manager

NOVEMBER 2016

MN003273A01-A

# Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

## Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

## Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

## European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

# Contact Us

## Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

| For... | Phone |
|---|---|
| United States Calls | **800-221-7144** |
| International Calls | **302-444-9800** |

## North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola SSC.

| For... | Phone |
|---|---|
| Phone Orders | **800-422-4210** (US and Canada Orders)<br>For help identifying an item or part number, select choice 3 from the menu. |
|  | **302-444-9842** (International Orders)<br>Includes help for identifying an item or part number and for translation as needed. |
| Fax Orders | **800-622-6210** (US and Canada Orders) |

## Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

# Document History

| Version | Description | Date |
|---|---|---|
| MN003273A01-A | Original release of the *Fortinet Firewall Manager* manual | November 2016 |

This page intentionally left blank.

# Contents

**Copyrights................................................................................................ 3**
**Contact Us................................................................................................ 5**
**Document History................................................................................... 7**
**List of Figures........................................................................................ 11**
**List of Tables.......................................................................................... 13**
**List of Processes.................................................................................... 15**
**List of Procedures....................................................................................17**
**About Fortinet Firewall Manager........................................................... 19**
What Is Covered In This Manual?........................................................................... 19
Helpful Background Information............................................................................. 19
Related Information................................................................................................ 19
**Chapter 1: Fortinet Firewall Manager Description................................ 23**
1.1 Fortinet Firewall Manager Introduction.............................................................. 23
1.2 Fortinet Firewall Management in the ASTRO 25 System...................................23
1.3 Fortinet Firewall Management and Dynamic System Resilience........................24
1.4 Fortinet Firewall Management and ISSI 8000/CSSI 8000..................................25
**Chapter 2: Fortinet Firewall Manager Theory of Operations............... 27**
2.1 Fortinet Firewall Manager Main Window............................................................ 27
2.1.1 Fortinet Firewall Manager Tabs Area.....................................................28
2.2 Firewall Status in Device Monitor....................................................................... 28
**Chapter 3: Fortinet Firewall Manager Installation and Configuration..................31**
3.1 Installing and Configuring the Fortinet Firewall Manager Server and User Interface........... 31
3.1.1 Fortinet Firewall Manager Required Media.............................................32
3.1.2 Logging on to the Fortinet Firewall Manager.......................................... 32
3.1.3 Importing the Fortinet Firewall Manager Server Virtual Machine............................33
3.1.4 Configuring the vCenter for the Newly Deployed VM............................................. 36
3.1.5 Setting the Virtual Machine Startup and Shutdown Order...................................... 38
3.1.5.1 Zone Core Virtual Machine Boot Order.....................................................39
3.1.6 Connecting and Powering On a New Virtual Machine...........................................40
3.1.7 Obtaining the Fortinet Firewall Manager License.................................................. 40
3.1.8 Enabling/Disabling Centralized Event Logging on the Fortinet Firewall Manager... 41
3.1.9 Configuring DNS on the Fortinet Firewall Manager................................................ 42
3.1.10 Configuring NTP on the Fortinet Firewall Manager...............................................42
3.1.11 Configuring RADIUS Shared Secret on the Fortinet Firewall Manager................. 43
3.1.12 Adding FortiGate Firewalls to the Fortinet Firewall Manager................................43

3.2 Fortinet Firewall Manager Supplemental Configuration........................................................44
3.2.1 Changing Fortinet Firewall Manager Admin Account Password.............................44
3.2.2 Changing Fortinet Firewall Manager Welcome Banner.......................................... 45
**Chapter 4: Fortinet Firewall Manager Operation..................................................47**
4.1 Enabling the Fortinet Firewall Manager User Accounts in Active Directory...........................47
4.2 Changing the Backup Schedule on the Fortinet Firewall Manager.......................................48
4.3 Changing the Backup Password on the Fortinet Firewall Manager......................................49
4.4 Changing the Backup Encryption Password on the Fortinet Firewall Manager.....................50
4.5 Configuring the Fortinet Firewall Manager Schedule on a BAR Server................................51
4.6 Changing the Password for Fortinet Firewall Manager Accounts.........................................51
4.7 Deleting an Existing Fortinet Firewall Object.........................................................................52
4.8 Monitoring Events and Configuration Changes with Log Viewer..........................................52
4.9 Shutting Down Fortinet Firewall Manager.............................................................................53
**Chapter 5: Fortinet Firewall Manager Troubleshooting....................................... 55**
5.1 Checking Fortinet Firewall Manager Firmware Version........................................................55
5.2 Enabling/Disabling SSH on Fortinet Firewall Manager.........................................................55
5.3 Fixing an Incorrect Device Manager View............................................................................ 55
5.4 Rebooting the Fortinet Firewall Manager..............................................................................56
**Chapter 6: Fortinet Firewall Manager Disaster Recovery.................................... 57**
6.1 Recovering the Fortinet Firewall Manager.............................................................................57
6.1.1 Recovering Critical and Non-Critical Data in Fortinet Firewall Manager..................58

# List of Figures

Figure 1: FMS Virtual Machine on VMS Host in ASTRO 25 System M3 Master Site with ZCP.............24
Figure 2: FortiManager Main Window Example....................................................................... 27
Figure 3: Deploy OVF Template Window – Source...................................................................34
Figure 4: Deploy OVF Template Window – Name and Location...........................................................35
Figure 5: Deploy OVF Template Window – Network Mapping...............................................................36
Figure 6: Example of an Incorrect Device Manager.............................................................................. 56

This page intentionally left blank.

# List of Tables

Table 1: Motorola Solutions Documentation....19
Table 2: Non-Motorola Solutions Publications and Documentation.... 21
Table 3: Device Monitor Column Description.... 29
Table 4: Zone Core Virtual Machine Boot Order.... 39

This page intentionally left blank.

# List of Processes

Installing and Configuring the Fortinet Firewall Manager Server and User Interface ............................ 31

Recovering the Fortinet Firewall Manager ..........................................................................................57

This page intentionally left blank.

# List of Procedures

Logging on to the Fortinet Firewall Manager ........ 32
Importing the Fortinet Firewall Manager Server Virtual Machine ........ 33
Configuring the vCenter for the Newly Deployed VM ........ 36
Setting the Virtual Machine Startup and Shutdown Order ........ 38
Connecting and Powering On a New Virtual Machine ........ 40
Obtaining the Fortinet Firewall Manager License ........ 40
Enabling/Disabling Centralized Event Logging on the Fortinet Firewall Manager ........ 41
Configuring DNS on the Fortinet Firewall Manager ........ 42
Configuring NTP on the Fortinet Firewall Manager ........ 42
Configuring RADIUS Shared Secret on the Fortinet Firewall Manager ........ 43
Adding FortiGate Firewalls to the Fortinet Firewall Manager ........ 43
Changing Fortinet Firewall Manager Admin Account Password ........ 44
Changing Fortinet Firewall Manager Welcome Banner ........ 45
Enabling the Fortinet Firewall Manager User Accounts in Active Directory ........ 47
Changing the Backup Schedule on the Fortinet Firewall Manager ........ 48
Changing the Backup Password on the Fortinet Firewall Manager ........ 49
Changing the Backup Encryption Password on the Fortinet Firewall Manager ........ 50
Configuring the Fortinet Firewall Manager Schedule on a BAR Server ........ 51
Changing the Password for Fortinet Firewall Manager Accounts ........ 51
Deleting an Existing Fortinet Firewall Object ........ 52
Monitoring Events and Configuration Changes with Log Viewer ........ 52
Shutting Down Fortinet Firewall Manager ........ 53
Checking Fortinet Firewall Manager Firmware Version ........ 55
Enabling/Disabling SSH on Fortinet Firewall Manager ........ 55
Fixing an Incorrect Device Manager View ........ 55
Rebooting the Fortinet Firewall Manager ........ 56
Recovering Critical and Non-Critical Data in Fortinet Firewall Manager ........ 58

This page intentionally left blank.

# About Fortinet Firewall Manager

This manual provides information about the implementation of a firewall management system supported by the Fortinet FortiManager for Fortinet FortiGate firewalls in the ASTRO® 25 system. It covers application software on the Fortinet FortiManager Server and the web-based user interface (client software).

## What Is Covered In This Manual?

This manual contains the following chapters:

- Fortinet Firewall Manager Description on page 23 – Introduces the concept of firewall management and the components of the ASTRO® 25 system that have a role in firewall management.
- Fortinet Firewall Manager Theory of Operations on page 27 – Provides details about the components of the ASTRO® 25 system that have a role in firewall management
- Fortinet Firewall Manager Installation and Configuration on page 31 – Provides software installation/configuration procedures for the Fortinet firewall management system, including components on the Fortinet FortiManager Server and on a web-based firewall management user interface.
- Fortinet Firewall Manager Operation on page 47 – Provides basic operational procedures for the Fortinet Firewall Management Server and for the firewall management user interface.
- Fortinet Firewall Manager Troubleshooting on page 55 – Provides information that may be useful in case of a failure related to the firewall management system.
- Fortinet Firewall Manager Disaster Recovery on page 57 – Provides references and information that enable you to recover an ASTRO® 25 system Fortinet FortiGate firewall in the event of a failure.

## Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

## Related Information

Refer to the following documents for associated information about the Fortinet firewall manager.

Table 1: Motorola Solutions Documentation

| Related Information | Purpose |
|---|---|
| *Standards and Guidelines for Communication Sites* | Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as R56 manual.<br>This may be purchased on CD **9880384V83**, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842). |
| *System Overview and Documentation* | Provides an overview of the ASTRO® 25 new system features, documentation set, technical |

*Table continued…*

| Related Information | Purpose |
|---|---|
| | illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system. |
| *Virtual Management Server Hardware* | Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in an ASTRO ®25 system. |
| *Virtual Management Server Software* | Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in an ASTRO® 25 system. Includes common procedures for virtual machines/virtual appliances on the virtual server host. |
| *Unix Supplemental Configuration* | Provides additional procedures that an organization may require for Solaris-based and Linux-based devices, including procedures for configuring password aging, welcome banners and Packet Data Router (PDR) core dump. |
| *Windows Supplemental Configuration* | Provides additional procedures that must be performed on all Windows-based devices in an ASTRO® 25 system, and additional procedures that are performed only for specific Windows-based devices. |
| *Fortinet Firewall* | Provides information relating to the implementation and replacement of the firewall appliances that Motorola provides, including a firewall in the DeMilitarized Zone (DMZ) between the ASTRO® 25 radio network infrastructure and a customer's enterprise network (or the Motorola Solution Support Center); a firewall in the ISSI.1 Network Gateway between the ASTRO® 25 system and the ISSI.1 peer system, a Telephony Firewall in the Enhanced Telephone Interconnect subsystem, and a Control Room firewall. These firewalls include the following Fortinet FortiGate models: 100D and 1000C. See the Zone Core Protection manual for details about the 100D and 1000C firewalls used for that feature. |
| *ISSI 8000/CSSI 8000 – Intersystem Gateway* | Provides information associated with the ISSI 8000/CSSI 8000 feature in the ASTRO® 25 system. This manual includes information to install, configure, manage, and troubleshoot the Intersystem Gateway (ISGW) server application supporting the ISSI 8000/CSSI 8000 feature which provides an enhanced interconnectivity solution for P25 compatible systems and third-party consoles to interface with the ASTRO® 25 system. |

Table 2: Non-Motorola Solutions Publications and Documentation

| Publication | Document Number | Manufacturer | Purpose |
|---|---|---|---|
| *FortiManager 5.2.7 Administration Guide* | 02-521-232175-20141212 | Fortinet, Inc. | This document describes how to set up the FortiManager system and use it to manage supported Fortinet units. It includes information on how to configure multiple Fortinet units, configuring and managing the FortiGate VPN policies, monitoring the status of the managed devices, viewing and analyzing the FortiGate logs, updating the virus and attack signatures, providing web filtering and email filter service to the licensed FortiGate units as a local FortiGuard Distribution Server (FDS), firmware revision control and updating the firmware images of the managed units. |
| *FortiManager online help* | N/A | Fortinet, Inc. | FortiManager online help contains detailed procedures for using the FortiManager web-based manager to configure and manage FortiGate firewalls.<br>To access the online help, select **Help** on the right side of the tabs area. |
| *FortiManager 5.2.7 CLI Reference* | 02-521-232175-20150109 | Fortinet, Inc. | This document describes how to use the FortiManager Command Line Interface (CLI) and contains references for all FortiManager CLI commands. |

This page intentionally left blank.

Chapter 1

# Fortinet Firewall Manager Description

This chapter introduces the concept of firewall management and the components of the ASTRO® 25 system that have a role in firewall management supported by the Fortinet FortiManager.

## 1.1 Fortinet Firewall Manager Introduction

Firewall security management involves ensuring that only legitimate traffic from external networks accesses the radio system. It protects the ASTRO® 25 system against unauthorized connections, restricts traffic to known applications and protocols, and ensures that network resources cannot be accessed from external systems, unless authorized.

The purpose of the Fortinet FortiManager in the ASTRO® 25 system is to integrate network logging, analysis, and reporting aggregation into a single platform, whereby delivering comprehensive information concerning security events throughout the network.

## 1.2 Fortinet Firewall Management in the ASTRO 25 System

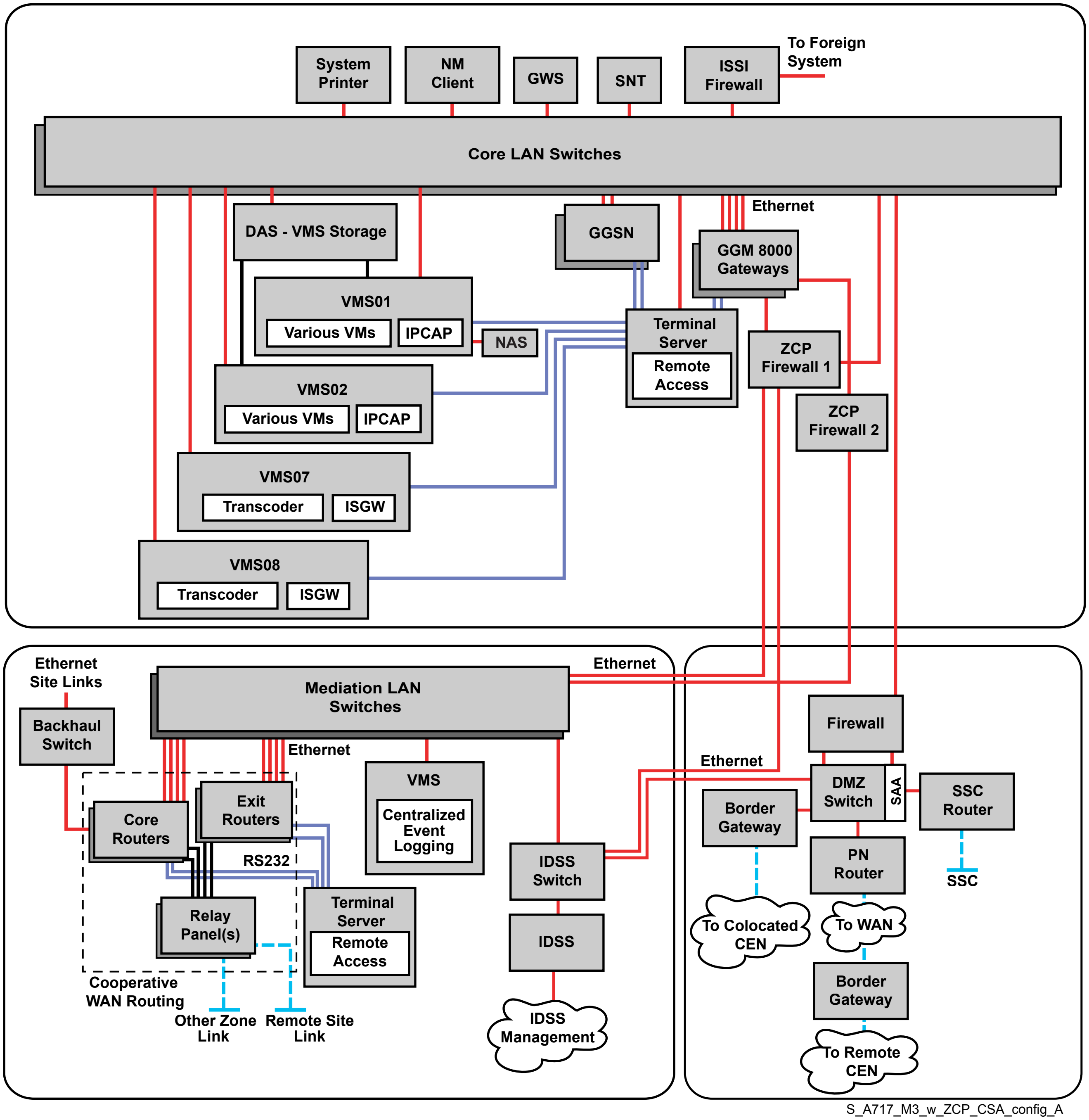
In the ASTRO® 25 system, logs may be collected and managed locally at the Fortinet firewall, or using a Fortinet FortiManager, depending on the type of firewalls implemented in the system and the system configuration.

The Fortinet FortiManager is mandatory only in an M3 ASTRO® 25 system configuration with ZCP, otherwise optional in L and M cores and not supported in a K core configuration. When present, Fortinet FortiManager is implemented as a virtual machine on an ESXi-based virtual server.

FortiManager has a web-based, graphical user interface.

The following figure shows the Fortinet virtual machine on the VMS01 ESXi-based host in an ASTRO® 25 system M3 master site. In this instance, the Zone Core Protection (ZCP) feature is implemented.

**Figure 1: FMS Virtual Machine on VMS Host in ASTRO 25 System M3 Master Site with ZCP**



## 1.3 Fortinet Firewall Management and Dynamic System Resilience

A Fortinet FortiManager server is provided in ASTRO® 25 systems with M3 master sites, if the system includes FortiGate 100D or FortiGate 1000C firewalls. There is no backup Fortinet FortiManager server. However, in the event of a failure, a secure web user interface (WebUI) on the firewalls can be used to view and retrieve logs from each firewall individually until the server is recovered.

In ASTRO® 25 systems with a Fortinet FortiManager server, logs are stored on the FortiManager server. A limited number of the same logs is also stored locally on each firewall. In ASTRO® 25 systems without a Fortinet FortiManager server, a limited number of logs is stored locally on each firewall.

## 1.4 Fortinet Firewall Management and ISSI 8000/CSSI 8000

The FortiManager is supported in systems which include the ISSI 8000/CSSI 8000 feature. ISSI 8000 firewall is accessed and managed through the Fortinet FortiManager similarly to other firewalls in the ASTRO® 25 system.

For installation and configuration procedures, see Fortinet Firewall Manager Installation and Configuration on page 31.

For more detailed information on the ISSI 8000/CSSI 8000 feature, refer to the *ISSI 8000/CSSI 8000 – Intersystem Gateway* manual.

This page intentionally left blank.

Chapter 2

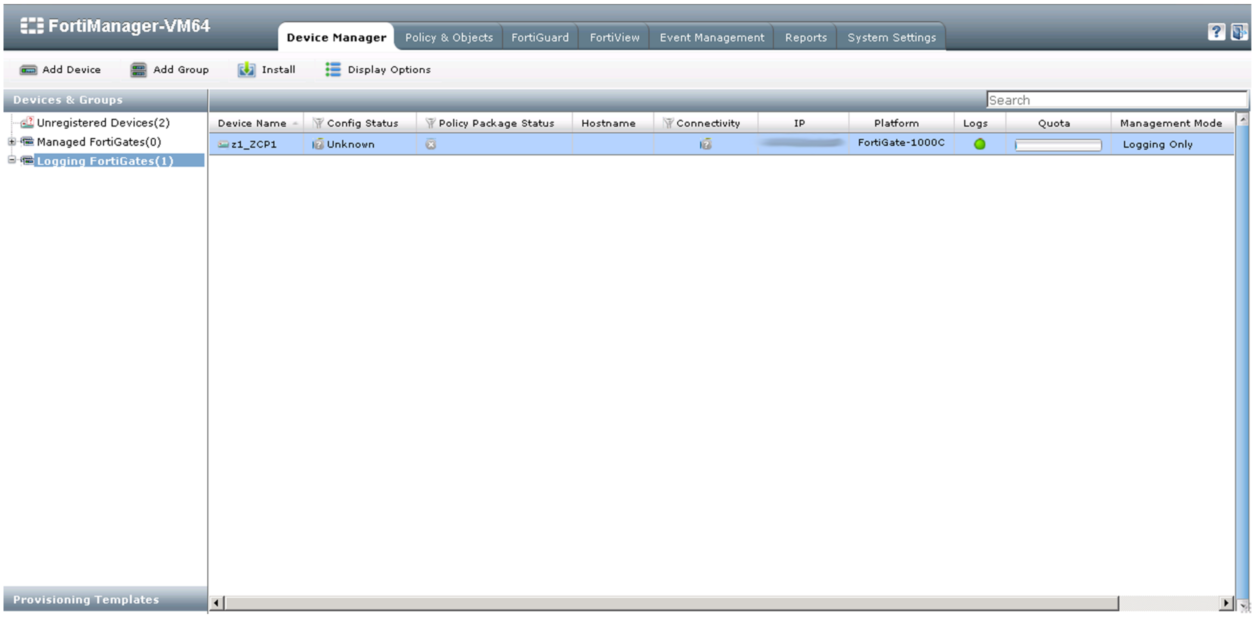
# Fortinet Firewall Manager Theory of Operations

This chapter provides details about the components of the ASTRO® 25 system that have a role in firewall management supported by the Fortinet FortiManager.

## 2.1 Fortinet Firewall Manager Main Window

The Fortinet FortiManager allows for the execution of several tasks. In the ASTRO® 25 system, the Fortinet FortiManager is used for collecting and archiving logs from all the Fortinet firewalls in the system. Before logs can be sent from the firewall to the FortiManager, a request from the firewall must be sent to the FortiManager. The request must be accepted by the FortiManager administrator. Upon logging into the FortiManger via its web interface, the administrator can use the main window to accept requests that were sent from the firewalls for sending logs to the FortiManager. Figure 2: FortiManager Main Window Example on page 27 shows an example of the main window of the FortiManager. The list of firewalls that are logging to the FortiManager appears in the main window when **Logging FortiGates** is selected from the left window pane.

**Figure 2: FortiManager Main Window Example**



| Device Name | Config Status | Policy Package Status | Hostname | Connectivity | IP | Platform | Logs | Quota | Management Mode |
|---|---|---|---|---|---|---|---|---|---|
| z1_ZCP1 | Unknown | | | | [redacted] | FortiGate-1000C | ● | | Logging Only |

**NOTICE:** There may be instances where the FortiManager main window GUI display for firewalls configured as a ZCP firewall varies from what is shown in Figure 2: FortiManager Main Window Example on page 27. If this situation is observed, see Fortinet Firewall Manager Troubleshooting on page 55 for notes regarding this known condition.

## 2.1.1 Fortinet Firewall Manager Tabs Area

The following FortiManager tabs are used for firewall configuration in the ASTRO® 25 system:

**NOTICE:** Not all functionalities available from the FortiManager GUI are supported in the ASTRO® 25 system.

### Device Manager

When you log in to the FortiManager, the **Device Manager** tab is shown by default.

The **Device Manager** tab allows the administrator of the FortiManager to accept requests from the firewall to send logs to it.

**NOTICE:** In the ASTRO® 25 system, a firewall can only be added to the FortiManager, if the FortiManager accepts a request from that firewall. The firewalls are not configured to accept requests from the FortiManager.

Click **Menu** to configure managed devices locally in the FortiManager. Click **Menu** → **Customize** to access more advanced firewall configuration options.

### Policy & Objects

Not used.

### FortiGuard

Not used.

### FortiView

The **FortiView** tab allows the administrator to view logs that were sent to the FortiManager from each firewall. From this tab, an administrator can display, download, import and delete logs. For more details, see the *FortiManager 5.2.7 Administration Guide*.

### Event Management

Not used.

### Reports

Not used.

### System Settings

The **System Settings** tab enables the management and configuration of basic system options for the FortiManager unit. This includes the basic network settings to connect the device to the UNC subnet, the configuration of administrators and their access permissions, and managing and updating firmware of the FortiManager.

## 2.2 Firewall Status in Device Monitor

Upon logging into the FortiManager, the **Device Manager** tab is shown by default. On the left of the window, the following items are listed under **Devices & Groups**:

**Unregistered Devices**

After selecting this item, a list is displayed containing requests from the firewall to send logs to the FortiManager. The number in parenthesis represents the number of firewalls in this list.

**Managed Fortigates**

After selecting this item, a list of firewalls the FortiManager is currently managing is displayed. In the ASTRO® 25 system, the FortiManager does not manage any of the Fortinet Firewalls, therefore no ASTRO® 25 system Fortinet firewalls should be listed here.

**Logging FortiGates**

After selecting this item, a list of firewalls the FortiManager is currently accepting logs from is displayed. The number in parenthesis represents the number of the firewalls in this list. All of the ASTRO® 25 system Fortinet firewalls should be in this list.

The following table provides description of Device Monitor columns and their function.

Table 3: Device Monitor Column Description

| Column Name | Description |
|---|---|
| Device Name | Provides hostname of each device. |
| Config Status | Not used in logging-only Fortinet firewalls. |
| Policy Package Status | Not used in logging-only Fortinet firewalls. |
| Hostaname | Not used in logging-only Fortinet firewalls. |
| Connectivity | Not used in logging-only Fortinet firewalls. |
| Platform | Hardware platform of the firewall |
| Logs | Logging status of the firewall. |
| Quota | Provides a bar graph of usage relative to allowed quota. |
| Management Mode | Provides the management mode. If the firewall and FortiManager are properly configured, the entry for each firewall should be: “Logging Only”. |
| Description | Not used in logging-only Fortinet firewalls. |

This page intentionally left blank.

Chapter 3

# Fortinet Firewall Manager Installation and Configuration

This chapter provides software installation/configuration procedures for the Fortinet FortiManager.

## 3.1 Installing and Configuring the Fortinet Firewall Manager Server and User Interface

Perform this process to install all the Fortinet FortiManager system software, and configure the components of the ASTRO® 25 firewall management system.

**Prerequisites:** Complete the installation/configuration process for the virtual server host. It includes installation/configuration procedures for the virtual server host from the *Virtual Management Server Hardware* and *Virtual Management Server Software* manuals.
Obtain the following from your system administrator:

- Virtual Server host (ESXi server) IP address and login credentials
- *Virtual Appliance – FMS* DVD that contains the Fortinet FortiManager Server virtual machine file
- Passwords for the following accounts:
  - ESXi-based server root account
  - Fortinet FortiManager Server root account
  - Fortinet FortiManager “suppuser” user account

**When and where to use:** To safeguard the integrity of your system, procedures requiring the Fortinet FortiManager Server root account password should be performed only by experts in the operating system and the ASTRO® 25 system.
For information about accounts on the Windows-based devices that can host the FortiManager user interface, see the *Private Network Management Client* and *Authentication Services* manuals.

**Process:**

1. Import the virtual machine.

   See Importing the Fortinet Firewall Manager Server Virtual Machine on page 33.
2. For systems where vCenter is already installed, configure the vCenter for the virtual machine.

   See Configuring the vCenter for the Newly Deployed VM on page 36.
3. Set the virtual machine startup and shutdown order.

   See Setting the Virtual Machine Startup and Shutdown Order on page 38.
4. Connect and power on the virtual machine.

   See Connecting and Powering On a New Virtual Machine on page 40.
5. Obtain the Fortinet FortiManager license.

   See Obtaining the Fortinet Firewall Manager License on page 40.
6. Optional: Enable Centralized Event Logging, if it is implemented in your system.

See Enabling/Disabling Centralized Event Logging on the Fortinet Firewall Manager on page 41.

7. Configure DNS.

   See Configuring DNS on the Fortinet Firewall Manager on page 42.

8. Configure NTP.

   See Configuring NTP on the Fortinet Firewall Manager on page 42.

9. Configure RADIUS.

   See Configuring RADIUS Shared Secret on the Fortinet Firewall Manager on page 43.

10. Configure security settings on virtual machines.

    See the “Virtual Management Server Operation” chapter in the *Virtual Management Server Software* manual.

11. Add FortiGate firewalls to the Fortinet FortiManager.

    See Adding FortiGate Firewalls to the Fortinet Firewall Manager on page 43.

12. Enable the Fortinet Firewall Manager user accounts in Active Directory.

    See Enabling the Fortinet Firewall Manager User Accounts in Active Directory on page 47.

13. Change the backup password on the Fortinet Firewall Manager.

    See Changing the Backup Password on the Fortinet Firewall Manager on page 49.

### 3.1.1 Fortinet Firewall Manager Required Media

The *Virtual Appliance – FMS* DVD is required for the installation of all software components of the firewall management system when the Fortinet FortiManager Server is implemented as a virtual machine.

### 3.1.2 Logging on to the Fortinet Firewall Manager

**Prerequisites:** Obtain the username and password for the FortiManager administrative account from your system administrator.

**Procedure:**

1. Log on to the Network Management (NM) client using the Windows administrator account.

   The account name set up by Motorola Solutions for Windows 7 and Windows 10-based devices is “secmoto”.

2. From the NM client, open the **Internet Explorer**.
3. In the **Internet Explorer** address bar, enter: `https://ffwm01`
4. At the prompt, type the username and password for the FortiManager administrative or local account. Click **Login**.

   The default account name is `suppuser`.

5. At the disclaimer prompt, click **Accept**.

**Postrequisites:** The **FortiManager** main window appears.

## 3.1.3 Importing the Fortinet Firewall Manager Server Virtual Machine

Perform this procedure to import the Fortinet FortiManager Server virtual machine from a DVD provided by Motorola Solutions.

**Prerequisites:**
Before performing this procedure, obtain from your system administrator:

- Password to the Windows-based device hosting the VMware vSphere Client for an account which belongs to the platadm group in Active Directory
- *Virtual Appliance – FMS* DVD (contains the Fortinet FortiManager Server virtual machine files)
- Virtual Server host (ESXi server) IP address and login credentials
- ESXi server administrator account name and password

**Procedure:**

1. Log on to the Windows-based device hosting the VMware vSphere Client using an account which belongs to the platadm group in Active Directory.

   The desktop appears.

2. Launch the **VMware vSphere Client**.

   A desktop shortcut was created during installation.

3. At the dialog box, perform the following actions:

   a. Type the ESXi server's IP Address.

   b. Type `root` in the **Username** field.

   c. Type ESXi server's root password in **Password** field.

   d. Click **Log in**.

   The vSphere Client Inventory screen appears.

4. In the DVD drive of the Windows server where the vSphere Client resides, insert the *Virtual Appliance – FMS* DVD.

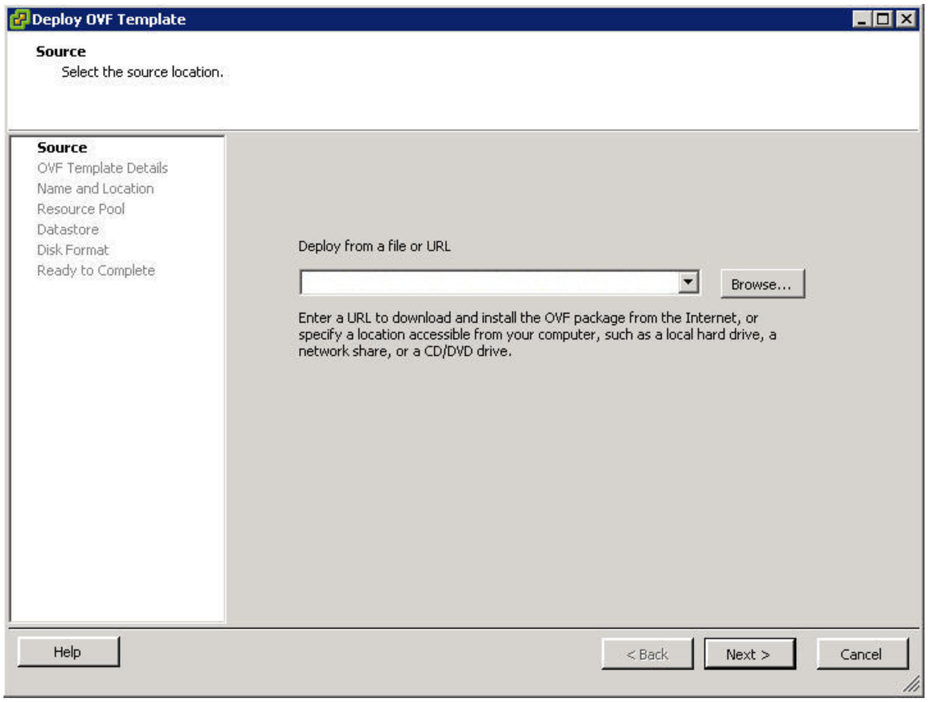
5. For optimal speed during the import process, copy the `\FMS-Astro-`***`<version number>`*** files from the DVD to any location on the hard drive of the Windows server that you are using for this import

   At this time, you can copy the files for all the virtual machines you intend to import, using this Windows server.

6. In the vSphere Client menu bar, select **File** → **Deploy OVF Template**.

   The following window appears.

**Figure 3: Deploy OVF Template Window – Source**



Source

Select the source location.

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

**7** Click **Browse**.

A window displays file directories.

**8** Select the `FMS-Astro-`***`<version number>`***`.ovf` file on the DVD, or if you copied it to the hard drive, in the directory where you pasted it. Click **Open**.

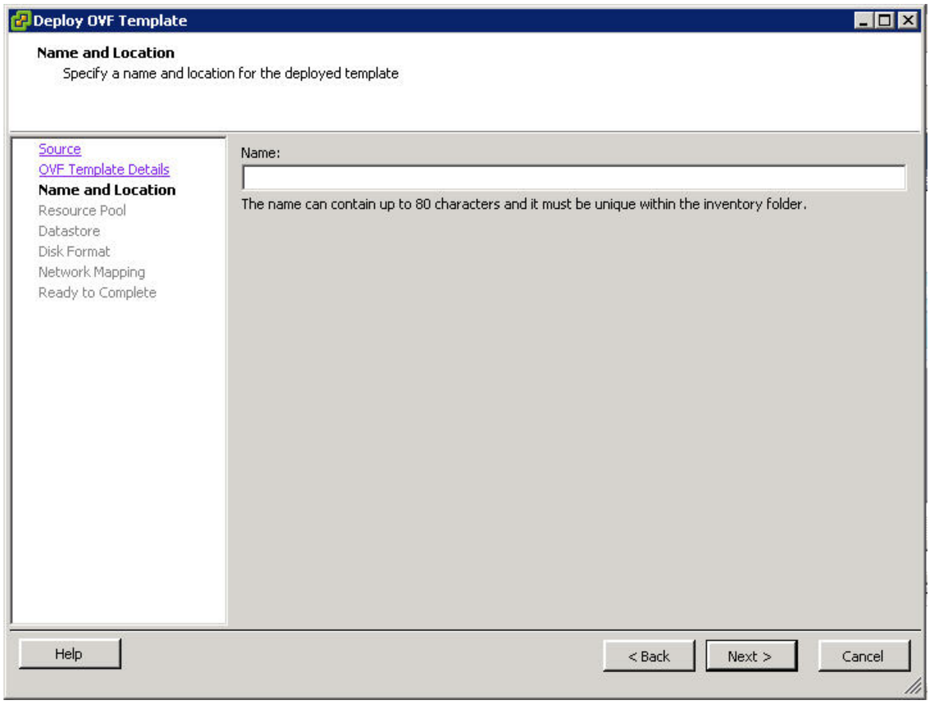
The file name and path for the virtual machine you selected appear on the **Deploy OVF Template** window.

**9** Click **Next**.

**10** In the OVF Template Details screen in the **Deploy OVF Template** window, click **Next**.

The following screen appears.

**Figure 4: Deploy OVF Template Window – Name and Location**



**11** In the **Name** field, enter the hostname for the Firewall Management Server: `ffwm01`. Click **Next**.

**12** Perform one of the following actions:

- If a DAS device is used and the Datastore screen appears in the **Deploy OVF Template** window, enter: `z`***<ZZZ>***`das`***<XX>***`datastore1` where:

  ***<ZZZ>*** is the zone number

  ***<XX>*** is the number of the DAS from the IP Plan

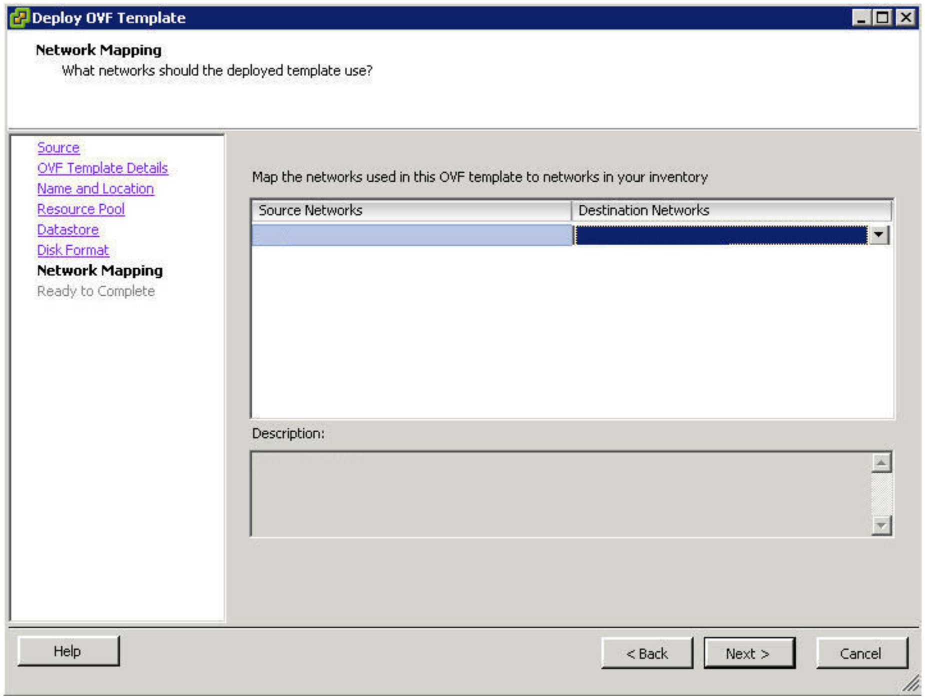
- If a DAS device is used and the Datastore screen does not appear before the Disk Format screen in the **Deploy OVF Template** window, no local hard drives are configured on the Virtual Management Server.

- If no DAS device is used and the Datastore screen does not appear before the Disk Format screen in the **Deploy OVF Template** window, only local hard drives are configured on the Virtual Management Server.

**13** On the **Disk Format** screen, select **Thick Provision Eager Zeroed** or **Thick Provision**, if **Thick Provision Eager Zeroed** is not available. Click **Next**.

The following screen appears.

**Figure 5: Deploy OVF Template Window – Network Mapping**



**14** Verify that **ucs0** displays in the **Destination Network** drop-down list. Click **Next**.

**NOTICE:** The Destination Networks in the drop-down list correspond to the Network Labels entered in the properties for the virtual switches on the Hardware: Networking screen in vSphere Client.
The Source Network column lists the networks specified in the OVF file.

If no zone network choice appears in the Destination Networks drop-down list, review the procedure for configuring Virtual Networking in the *Virtual Management Server Software* manual to determine what steps were missed.

**15** In the **Ready to Complete** screen, verify the information that is displayed. Click **Finish**.

The Firewall Management Server virtual machine is imported. This takes 10 to 20 minutes.

**IMPORTANT:** Do not leave the installation unattended for more than 8 minutes, or you may be logged out, and the installation may fail.

**16** Verify that the left pane of the **vSphere Client** main window displays the Fortinet FortiManager Server virtual machine name that you entered in step 11.

You may need to expand the list in the left pane to locate the virtual machine name.

**17** Remove the media from the drive.

## 3.1.4 Configuring the vCenter for the Newly Deployed VM

For newly deployed virtual machines to run properly in an existing vCenter environment, you must override the default HA cluster settings and modify the restart priority for the new VMs. After a host failure, the VMs are restarted in the relative order determined by their restart priority.

**When and where to use:**

- This procedure applies only to systems where vCenter is installed.

- Run this procedure only if a VM OVF was deployed after the vCenter was originally configured.

**Procedure:**

**1** Launch the Internet Explorer from a Windows-based device, such as the Network Management (NM) Client, or a service computer or laptop.

- Connect to: `https://`***`<vCenterIP>`***`/vsphere-client`
- Ignore or accept any warnings about the connection security or self-signed certificates.

**2** In the dialog box, perform the following actions:

**a** Type in the user name `administrator@z00`***`<Z>`***`vcs`***`<H>`***`.zone`***`<Z>`***

where ***<Z>*** is the zone number and ***<H>*** is the vCenter instance number

**b** Type in the administrator user password.

**c** Click **Login**.

The vSphere Web Client homepage appears.

**3** In the left pane, click **Hosts and Clusters**.

**4** Expand the tree and right-click the **Zone*<X>*** HA cluster

where ***<X>*** is the zone number.

**5** Select **Settings**.

**6** In the **Settings** window, click **VM Overrides**.

**7** Click **Add**.

**8** Click the **+** button.

**9** Select the check box for the VM you are configuring. Click **OK**.

**10** Depending on the VM you are configuring, perform the following actions:

- For the vCenter VM, change the **VM Restart Priority** to **Medium**.
- For the VMs that are monitored under Fault Tolerance, change the **VM Restart Priority** to **High**.
- For the VMs that are not monitored under Fault Tolerance/HA, change the **VM Restart Priority** to **Disabled**.

**11** Click **OK**.

**12 Perform the following actions only if you are recovering the VM after a failure and the VM is not monitored under Fault Tolerance:**

**a** In the **Settings** window, click **VM/Host Groups**.

**b** Select the group for the Virtual Management Server (VMS) on which the VM resides and click **Edit**.

**c** Click **Add**.

**d** Select the check box next to the VM and click **OK**.

For information about the locations of virtual machines on the VMS and their configurations with regard to vCenter, see "Virtual Machine Locations for vCenter Configs" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.

**e** Click **OK**.

The restart priority setting for the newly deployed virtual machine is configured.

### 3.1.5 Setting the Virtual Machine Startup and Shutdown Order

In an ASTRO® 25 system, virtual machines hosted on a Virtual Management Server (VMS) are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

**Procedure:**

1. From a Windows-based device, launch the VMware vSphere Client.

   A desktop shortcut was created during installation.
2. Log on to the server as a user with root privileges.
3. On the upper left side of the **vSphere Client Inventory** window, select the ESXi server.
4. On the right side of the window, select the **Configuration** tab.

   The window displays information about the configuration of the ESXi server.
5. In the **Software** section, select **Virtual Machine Startup/Shutdown**.
6. On the right side of the main window, select **Properties**.
7. In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.
8. In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.
9. In the **Default Shutdown Delay** area, from the **Shutdown Action** drop-down list, select **Guest Shutdown**.
10. Put the virtual machines hosted on the ESXi server in the correct boot order:

    a. In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.

    b. By using the **Move Up** and **Move Down** buttons, move the virtual machine to the correct ordered slot.

       **NOTICE:**
       Zone Core Virtual Machine Boot Order on page 39 outlines the boot order for the virtual machines that can reside on an ESXi-based Zone Core Virtual Management Server (VMS).

       To determine the correct ordered slot for each virtual machine hosted on the ESXi server that you are configuring, see the boot order table.

    c. Repeat step 10 a and step 10 b until the boot order for the virtual machines is correct.
11. Click **OK**.

    The **Properties** window closes.

### 3.1.5.1 Zone Core Virtual Machine Boot Order

**NOTICE:**
Up to two instances of the GMC can be on the server.

If UNCDS is present, three instances of the UNCDS are on the server.

Table 4: Zone Core Virtual Machine Boot Order

| Order | Virtual Machine | Startup | Startup Delay | Shutdown | Shutdown Delay |
|---|---|---|---|---|---|
| Automatic Startup | | | | | |
| 1 | ZC | Enabled | Use Default | Use Default | Use Default |
| 2 | Transcoder | Enabled | Use Default | Use Default | Use Default |
| 3 | ISGW | Enabled | Use Default | Use Default | Use Default |
| 4 | PDG-Conv | Enabled | Use Default | Use Default | Use Default |
| 5 | PDG-HPD | Enabled | Use Default | Use Default | Use Default |
| 6 | PDG-IV&D | Enabled | Use Default | Use Default | Use Default |
| 7 | License Manager | Enabled | Use Default | Use Default | Use Default |
| 8 | ATR | Enabled | Use Default | Use Default | Use Default |
| 9 | DC-System | Enabled | Use Default | Use Default | Use Default |
| 10 | DC-Zone | Enabled | Use Default | Use Default | Use Default |
| 11 | IPCAP | Enabled | Use Default | Use Default | Use Default |
| Any Order | AuC | Enabled | Use Default | Use Default | Use Default |
| | BAR | Enabled | Use Default | Use Default | Use Default |
| | CSMS | Enabled | Use Default | Use Default | Use Default |
| | InfoVista | Enabled | Use Default | Use Default | Use Default |
| | FMS – Fortinet | Enabled | Use Default | Use Default | Use Default |
| | GDG | Enabled | Use Default | Use Default | Use Default |
| | GMC | Enabled | Use Default | Use Default | Use Default |
| | NM Client | Enabled | Use Default | Use Default | Use Default |
| | UCS | Enabled | Use Default | Use Default | Use Default |
| | SSS | Enabled | Use Default | Use Default | Use Default |
| | Syslog | Enabled | Use Default | Use Default | Use Default |
| | UEM | Enabled | Use Default | Use Default | Use Default |
| | UNC | Enabled | Use Default | Use Default | Use Default |
| | UNCDS | Enabled | Use Default | Use Default | Use Default |
| | vCenter App | Enabled | Use Default | Use Default | Use Default |
| | ZDS | Enabled | Use Default | Use Default | Use Default |
| | ZSS | Enabled | Use Default | Use Default | Use Default |

*Table continued…*

| Order | Virtual Machine | Startup | Startup Delay | Shutdown | Shutdown Delay |
|---|---|---|---|---|---|
| Manual Startup | DESU Waypoint | Disabled | Use Default | Use Default | Use Default |

## 3.1.6 Connecting and Powering On a New Virtual Machine

Perform this procedure to connect and power on a virtual machine after you import it.

**Procedure:**

1. In the navigation pane, right-click the virtual machine that you imported.

   A pop-up menu appears.
2. Select **Edit Settings**.

   A dialog box appears.
3. In the left pane:
   a. Select the network adapter.
   b. Select the **Connect at power on** check box.
   c. Ensure that **ucs0** displays for Network Label.
4. Click **OK**.

   For information about Network Adapters, Network Labels and other virtual networking settings, see the Virtual Networking sections in the “Virtual Management Server Configuration” chapter of the *Virtual Management Server Software* manual.
5. In the navigation pane, right-click the virtual machine you imported.
6. In the pop-up menu, select **Power** → **Power On**.

   The selected virtual machine powers on, and the screen for the selected virtual machine opens. Ignore any failure messages displayed during the power on of the virtual machine.

## 3.1.7 Obtaining the Fortinet Firewall Manager License

Perform this procedure after powering on a new Fortinet FortiManager virtual machine for the first time.

**Prerequisites:** Obtain the following information from your system administrator:

- Username and password for the Fortinet FortiManager administrative account
- License `.lic` file

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. Perform one of the following actions:

| If… | Then… |
|---|---|
| **If you install the license for the first time and the** | At the evaluation mode prompt, click **Upload License File**. |

| If… | Then… |
|---|---|
| **evaluation mode has expired,** | |
| **If you install the license for the first time and the evaluation mode has not expired yet or if you already have a license or if you want to install another license,** | perform the following actions:<br>**a** From the **FortiManager** main window, select the **System Settings** tab.<br>**b** In the **License Information** area, select **Upload License**.<br>**c** In the **VM License Upload** window, click **Browse** and select the license `.lic` file. Click **OK**.<br>A restarting message appears.<br>**d** Wait for a couple of minutes and refresh the page.<br>**e** Log back in to the Fortinet FortiManager.<br>**f** In the **System Settings** tab, verify if a valid serial number is displayed in the **System Information** area and license information is updated in the **License Information** area. |

3.1.8

## Enabling/Disabling Centralized Event Logging on the Fortinet Firewall Manager

Perform this procedure to enable or disable Centralized Event Logging on Fortinet FortiManager, if Centralized Event Logging is implemented in your system.

**Prerequisites:** Obtain the following from your system administrator:

- ESXi server administrator account name and password
- Username and password for the FortiManager administrative account

Perform Obtaining the Fortinet Firewall Manager License on page 40.

**Procedure:**

1. After powering on the FortiManager virtual machine, perform the following actions:
   **a** From the navigation tree in the left pane, select the FortiManager virtual machine.
   **b** In the right pane, click the **Console** tab.
2. In the console area for the FortiManager virtual machine, if boot up messages are generated, wait for the device login prompt.
3. Click anywhere inside the console area. After your cursor disappears, press ENTER.
   Your cursor is active at the command prompt.
4. At the command prompt, log on using the administrative account and password.
   If prompted to accept, enter: a
5. At the prompt, enter one of the following commands:

| If… | Then… |
|---|---|
| **You want to enable Centralized Event Logging on Fortinet FortiManager,** | enter: |

| If… | Then… |
|---|---|
| | **a** `config system locallog syslogd setting`<br>**b** `set status enable`<br>**c** `end` |
| **You want to disable Centralized Event Logging on Fortinet FortiManager,** | enter:<br>**a** `config system locallog syslogd setting`<br>**b** `set status disable`<br>**c** `end` |

6. To exit from the command prompt of the FortiManager virtual machine on the ESXi server, press Ctrl + ALT.

3.1.9
## Configuring DNS on the Fortinet Firewall Manager

**Prerequisites:** Obtain the following information from your system administrator:

- IP address of the primary and secondary DNS server
- Username and password for the FortiManager administrative account

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. Click the **System Settings** tab.
3. From the tree view in the left pane, select **Network**.
4. In the DNS area, type the **Primary DNS Server** and **Secondary DNS Server** IP address.
5. To confirm changes, click **Apply**.

3.1.10
## Configuring NTP on the Fortinet Firewall Manager

Perform this procedure to configure the system time on the Fortinet FortiManager.

**Prerequisites:** Obtain the following information from your system administrator:

- IP address of the primary and secondary Network Time Protocol (NTP) server
- Username and password for the FortiManager administrative account

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. Click the **System Settings** tab.
3. From the tree view in the left pane, select **Dashboard**.
4. In the **System Information** area, **System Time** row, click **Change**.

5. In the **Change System Time Settings** window, ensure that the **Synchronize with NTP server** radio button is selected.
6. In the **Server** fields, type the primary and secondary NTP server IP address, successively. Click **OK**.

## 3.1.11 Configuring RADIUS Shared Secret on the Fortinet Firewall Manager

**Prerequisites:**
Obtain the following from your system administrator:

- Username and password for the FortiManager administrative account
- Primary and secondary shared secret.

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. Click the **System Settings** tab.
3. From the tree view in the left pane, select **Admin** → **Remote Auth Server**.
4. Click inside the **Name** field for the desired server to open the **Edit RADIUS Server** window.
5. In the **Server Name/IP** field, enter: `ucs-rad01.ucs`
6. In the **Server Secret** field, enter the shared secret of the primary RADIUS server.
7. In the **Secondary Server Name/IP** field, perform one of the following actions:
   - If this is a DSR system, enter: `ucs-rad03.ucs`
   - If this is a non-DSR system, enter: `z`***<ZZZ>***`rad01.zone`***<Z>***

   where ***<ZZZ>*** and ***<Z>*** indicate the zone to which the device belongs
8. In the **Secondary Server Secret** field, enter the shared secret of the secondary RADIUS server.
9. Click **OK**.

## 3.1.12 Adding FortiGate Firewalls to the Fortinet Firewall Manager

**Prerequisites:** Obtain the following information from your system administrator:

- Fortinet Firewall properly configured to communicate with the Fortinet FortiManager
- Username and password for the FortiManager administrative account

**NOTICE:** This procedure can only be performed on the FortiManager for firewalls that have sent a logging request to the FortiManager.

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. On the **Device Manager** tab, in the left pane, select **Unregistered Devices** to view the list of requests from firewall(s) to send logs to the FortiManager.

   **NOTICE:** If the firewall which you want to add is not listed, contact your system administrator.

3. In the right pane, right-click on the firewall you want to add, and select **Add** from the context menu.
4. In the **Add Device** window, click **OK**.

   The firewall is added. It is listed under **Logging FortiGates**.

## 3.2 Fortinet Firewall Manager Supplemental Configuration

This section provides additional procedures for Fortinet FortiManager configuration.

**NOTICE:** Perform the following procedures from the ESXi server.

### 3.2.1 Changing Fortinet Firewall Manager Admin Account Password

**Procedure:**

1. After powering on the FortiManager virtual machine, perform the following actions:
   a. From the navigation tree in the left pane, select the FortiManager virtual machine.
   b. In the right pane, click the **Console** tab.
2. In the console area for the FortiManager virtual machine, if boot up messages are generated, wait for the device login prompt.
3. Click anywhere inside the console area. After your cursor disappears, press ENTER.

   Your cursor is active at the command prompt.
4. At the command prompt, log on using the administrative account and password.

   If prompted to accept, enter: a
5. At the prompt, enter:
   a. `config system admin user`
   b. `edit admin`
   c. `set password` ***`<password>`***
   d. `end`

   where ***`<password>`*** is the new administrative password that must meet the following criteria:

   - Must be at least fourteen characters long
   - Must contain at least one character from following groups:
     - Upper-case letters
     - Numerical digits
     - Lower-case letters
     - Non-alphanumeric characters
6. To exit from the command prompt of the FortiManager virtual machine on the ESXi server, press CTRL + ALT.

## 3.2.2 Changing Fortinet Firewall Manager Welcome Banner

**Procedure:**

1. After powering on the FortiManager virtual machine, perform the following actions:
   - **a** From the navigation tree in the left pane, select the FortiManager virtual machine.
   - **b** In the right pane, click the **Console** tab.
2. In the console area for the FortiManager virtual machine, if boot up messages are generated, wait for the device login prompt.
3. Click anywhere inside the console area. After your cursor disappears, press ENTER.

   Your cursor is active at the command prompt.
4. At the command prompt, log on using the administrative account and password.

   If prompted to accept, enter: a
5. At the prompt, enter:
   - **a** `config system admin setting`
   - **b** `set banner-message` ***“<welcome message>“***
   - **c** `end`

   where ***<welcome message>*** maximum length is 255 characters
6. To exit from the command prompt of the FortiManager virtual machine on the ESXi server, press CTRL + ALT.

This page intentionally left blank.

Chapter 4

# Fortinet Firewall Manager Operation

This chapter provides operation procedures for the Fortinet FortiManager.

## 4.1 Enabling the Fortinet Firewall Manager User Accounts in Active Directory

Perform this procedure to enable the **suppuser** and **fwm_backup** users needed to access FortiManager when joined to the Active Directory (AD) domain. For more information on Active Directory user accounts, see “Creating Active Directory User Accounts” in the *Authentication Services* manual.

**Procedure:**

1. Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

   The account name set up by Motorola Solutions is `motosec`.

   The administrator’s desktop appears.

2. From **Start**, search for `administrative`. Click **Administrative Tools**.
3. In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
4. From the **Active Directory Users and Computers** window, select **Users** in the left pane.
5. In the list of users and groups in the right pane, perform the following actions:
   - a. Right-click **suppuser**.
   - b. From the context menu, select **Enable Account**.
   - c. In the message window, click **OK**.

     The message window closes and the user account is now enabled.

   - d. From the context menu, select **Reset Password**.
   - e. In the **Password Change** window, type **<*`new password`*>** twice.

     Where:

     The minimum password length is 14 characters.

     The password must have at least two of the following: lowercase character, uppercase character, and number.

     The password must have at least one of the following symbols: hyphen (-), underscore (_), dollar ($), pound/hash (#)

   - f. Clear the **User must change password at next login** check box. Click **OK**.

     The message window closes and the **suppuser** account password is configured.

6. In the list of users and groups in the right pane, perform the following actions:
   - a. Right-click **fwm_backup**.
   - b. From the context menu, select **Enable Account**.

c In the message window, click **OK**.

The message window closes and the user account is now enabled.

d From the context menu, select **Reset Password**.

e In the **Password Change** window, type ***`<new password>`*** twice.

Where:

The minimum password length is 14 characters.

The password must have at least two of the following: lowercase character, uppercase character, and number.

The password must have at least one of the following symbols: hyphen (-), underscore (_), dollar ($), pound/hash (#)

f Clear the **User must change password at next login** check box. Click **OK**.

The message window closes and the **fwm_backup** account password is configured.

g Change the **fwm_backup** user password on FortiManager.

See “Resetting User Passwords in Active Directory” in the *Authentication Services* manual.

## 4.2 Changing the Backup Schedule on the Fortinet Firewall Manager

**Prerequisites:** Obtain from your system administrator:

- Username and password for the FortiManager administrative account
- ESXi server administrator account name and password

Obtain the Fortinet FortiManager license. See Obtaining the Fortinet Firewall Manager License on page 40.

**Procedure:**

1 After powering on the FortiManager virtual machine, perform the following actions:

a From the navigation tree in the left pane, select the FortiManager virtual machine.

b In the right pane, click the **Console** tab.

2 In the console area for the FortiManager virtual machine, if boot up messages are generated, wait for the device login prompt.

3 Click anywhere inside the console area. After your cursor disappears, press ENTER.

Your cursor is active at the command prompt.

4 At the command prompt, log on using the administrative account and password.

If prompted to accept, enter: a

5 At the prompt, enter:

a `config system backup all-settings`

b `set week_days` ***`<day>`***

c `set time` ***`<time>`***

d `end`

e `config system log settings`

f `config rolling-regular`

g `set when weekly`

h `set days` ***<ddd>***

i `set hour` ***<hh>***

j `end`

k `end`

l `config system locallog disk setting`

m `set roll-day` ***<day>***

n `set roll-time` ***<hh:mm>***

o `end`

where:

***<day>*** is name of week day, for example: `Monday`
***<time>*** is the timestamp in the ***<hh:mm:ss>*** format, for example: `02:00:00`
***<ddd>*** is a three-letter, lower-case abbreviation of a day name, for example: `mon`
***<hh>*** is hour, for example: `02`
***<day>***
***<hh:mm>*** is time example: `02:00`

**Postrequisites:** After performing this procedure, configure the schedule on the BAR server. See Configuring the Fortinet Firewall Manager Schedule on a BAR Server on page 51.

## 4.3 Changing the Backup Password on the Fortinet Firewall Manager

This procedure describes how to change password for a user that the Fortinet FortiManager uses to connect and transfer the backup data.

**Prerequisites:** Obtain from your system administrator:

- Username and password for the FortiManager administrative account
- ESXi server administrator account name and password

Change the password for **fwm_backup**. See “Resetting User Passwords in Active Directory” in the *Authentication Services* manual.

**Procedure:**

1 After powering on the FortiManager virtual machine, perform the following actions:

   a From the navigation tree in the left pane, select the FortiManager virtual machine.

   b In the right pane, click the **Console** tab.

2 In the console area for the FortiManager virtual machine, if boot up messages are generated, wait for the device login prompt.

3 Click anywhere inside the console area. After your cursor disappears, press Enter.

   Your cursor is active at the command prompt.

4 At the command prompt, log on using the administrative account and password.

   If prompted to accept, enter: a

5. At the command prompt, enter:
   - **a** `config system backup all-settings`
   - **b** `set passwd` ***`<password>`***
   - **c** `end`
   - **d** `config system log settings`
   - **e** `config rolling-regular`
   - **f** `set password` ***`<password>`***
   - **g** `end`
   - **h** `end`
   - **i** `config system locallog disk setting`
   - **j** `set upload enable`
   - **k** `set uploadpass` ***`<password>`***
   - **l** `end`

   where ***`<password>`*** is the new backup password

   The minimum password length is 14 characters.

4.4

## Changing the Backup Encryption Password on the Fortinet Firewall Manager

This procedure describes how to update an additional password that is used to encrypt the Fortinet FortiManager critical settings.

**Prerequisites:** Obtain from your system administrator:

- Username and password for the FortiManager administrative account
- ESXi server administrator account name and password

**Procedure:**

1. After powering on the FortiManager virtual machine, perform the following actions:
   - **a** From the navigation tree in the left pane, select the FortiManager virtual machine.
   - **b** In the right pane, click the **Console** tab.
2. In the console area for the FortiManager virtual machine, if boot up messages are generated, wait for the device login prompt.
3. Click anywhere inside the console area. After your cursor disappears, press ENTER.

   Your cursor is active at the command prompt.
4. At the command prompt, log on using the administrative account and password.

   If prompted to accept, enter: a
5. At the prompt, enter:
   - **a** `config system backup all-settings`
   - **b** `set crptpasswd` ***`<password>`***
   - **c** `end`

where **`<password>`** is the backup encryption password

## 4.5 Configuring the Fortinet Firewall Manager Schedule on a BAR Server

**Procedure:**

1. Log on to the Backup and Recovery (BAR) server using one of the following methods:
   - Your Active Directory account that is a member of the **bkupadm** user group, if the server is joined to the domain and a domain controller is available on the network (recommended)
   - The root account on the server

   For the Active Directory user groups to use for administration menu options on ASTRO® 25 system Linux-based servers, see the *Authentication Services* manual.
2. At the command prompt, enter: `admin_menu`
3. In the server administration **Main Menu**, enter the number for **Application Administration**.
4. Enter the number for **Client administration**.
5. Enter the number for **Change FortiManager backup schedule**.
6. Enter the backup start time information:
   - **a** Enter the number for the day of the week for the backup.

     where Monday = `1`, Tuesday = `2`, and so on
   - **b** Enter the number for the hour for the backup.

     where 01:00 AM is `1`, 01:00 PM is `13`, and so on

   The backup schedule is changed. A confirmation message appears, and the **Client Administration Menu** reappears.

## 4.6 Changing the Password for Fortinet Firewall Manager Accounts

This procedure is only for changing password of local accounts on the Fortinet FortiManager.

**Prerequisites:** Obtain the following password and account information:

- If this procedure is to be executed from an NM Client, obtain login and password for the NM Client
- Network reachability/connectivity to the UCS subnet of the FortiManager.
- FortiManager username and password
- IP address of the FortiManager (contact your system administrator)

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. Click the **System Settings** tab.
3. In the **System Settings** pane on the left, expand **Admin**. Click **Administrator**.
4. In the **System Settings** tab on the right, from the list of accounts, double-click the row with the local account.

   The local account **Type** attribute is **LOCAL**.

5 Click on the **Change Password** button.

6 Type the old password in the **Old password** field and the new password in the **New Password** field.

7 Retype the new password in the **Confirm Password** field.

8 Click **OK**.

9 Optional: Repeat step 4 through step 8 for the remaining local account(s).

## 4.7 Deleting an Existing Fortinet Firewall Object

**Prerequisites:** Obtain the following password and account information:

- If this procedure is to be executed from an NM Client, obtain login and password for the NM Client
- Network reachability/connectivity to the UCS subnet of the FortiManager.
- FortiManager username and password
- IP address of the FortiManager (contact your system administrator)

**Procedure:**

1 Log on to the Fortinet FortiManager.

See Logging on to the Fortinet Firewall Manager on page 32.

2 In the **Device Manager** tab, select **Logging FortiGates** to display the list of firewalls that are configured in the FortiManager for logging.

3 From the list of firewalls on the right, right-click the object to be deleted. From the context menu, select **Delete**.

A confirmation dialog displays.

4 Click **OK**.

The firewall is removed from the list of **Logging FortiGates**.

**NOTICE:** If the deleted firewall sends another logging request to the FortiManager, it may appear in the **Unregistered Devices** list in the FortiManager.

## 4.8 Monitoring Events and Configuration Changes with Log Viewer

The **FortiView** tab of the Fortinet FortiManager provides the ability to monitor and review logs and events of each firewall registered with the FortiManager.

**Procedure:**

1 Log on to the Fortinet FortiManager.

See Logging on to the Fortinet Firewall Manager on page 32.

2 Click the **FortiView** tab.

3 From the list of firewalls in the **FortiView** pane on the left, expand each firewall to see **Traffic** and **Event** logs.

4 Click the **Refresh** icon on the **FortiView** tab toolbar to refresh the browser window with the most recent snapshot.

## 4.9 Shutting Down Fortinet Firewall Manager

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. Click the **System Settings** tab.
3. In the **Unit Operation** area, click **Shutdown**.
4. In the confirmation window, click **OK**.

   Optionally, you can type a message to be logged in the event log.

This page intentionally left blank.

Chapter 5

# Fortinet Firewall Manager Troubleshooting

This chapter provides troubleshooting procedures for the Fortinet FortiManager.

## 5.1 Checking Fortinet Firewall Manager Firmware Version

Perform this procedure to check the firmware version of the Fortinet FortiManager.

**Procedure:**

1. Log on to the Fortinet FortiManager.

   See Logging on to the Fortinet Firewall Manager on page 32.
2. Click the **System Settings** tab.
3. In the **System Information** panel, locate **Firmware Version**.

## 5.2 Enabling/Disabling SSH on Fortinet Firewall Manager

Secure Shell (SSH) should be disabled by default on the FortiManager. Enabling SSH can be performed only by advanced users for troubleshooting purposes.

**Procedure:**

1. Log on to the Fortinet Firewall Manager.

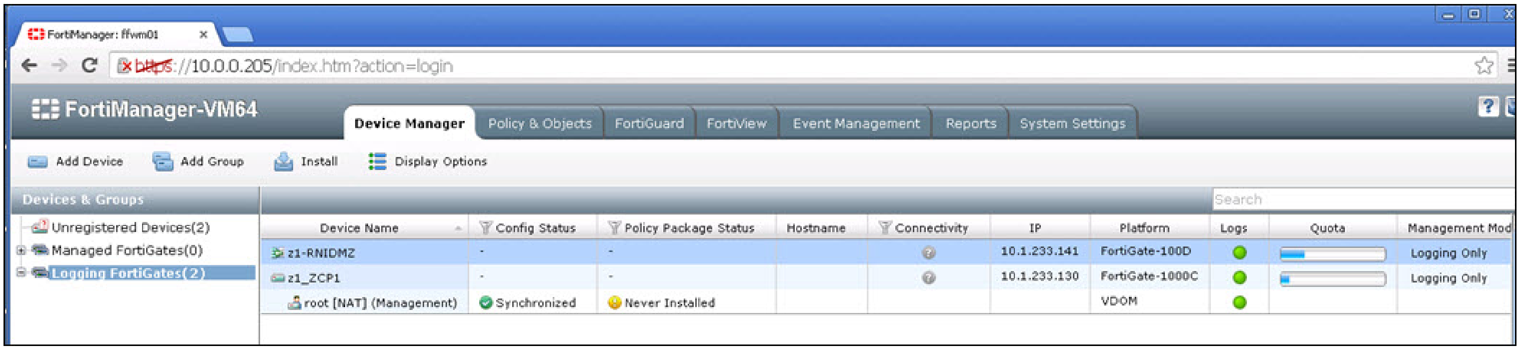
   See Logging on to the Fortinet Firewall Manager on page 32.
2. Click the **System Settings** tab.
3. From the tree view in the left pane, select **Network**.
4. In the **Administrative Access** area, perform one of the following actions:
   - To disable SSH (default setting), clear the **SSH** checkbox.
   - To enable SSH (advanced users only), select the **SSH** checkbox.
5. To confirm changes, click **Apply**.

## 5.3 Fixing an Incorrect Device Manager View

**When and where to use:** After upgrading the Fortinet FortiManager firmware to version 5.2.7, or after installing a Fortinet firewall object into the Fortinet FortiManager with firmware version 5.2.7, the **Device Manager** tab of the FortiManager may display incorrect information for firewalls configured with multiple VDOMs.
In the current ASTRO® 25 software release and prior, the only Fortinet firewall device configured with multiple VDOMs is the ZCP firewall. Therefore, this issue, as well as the accompanying recovery procedure, applies to the ZCP firewall.

The following figure shows an example of the FortiManager's **Device Manager** tab exhibiting the display issue described. The Fortinet firewall with the hostname z1_ZCP1 is configured with multiple VDOMs. However, only the root VDOM is shown; the other VDOM that is configured on the ZCP firewall is not shown in the FortiManager **Device Manager** tab. Also, the icons shown in the **Config Status** and the **Policy Package Status** columns report status information that should be disregarded.

**Figure 6: Example of an Incorrect Device Manager**



| Device Name | Config Status | Policy Package Status | Hostname | Connectivity | IP | Platform | Logs | Quota | Management Mod |
|---|---|---|---|---|---|---|---|---|---|
| z1-RNIDMZ | - | - | | ? | 10.1.233.141 | FortiGate-100D | ● | | Logging Only |
| z1_ZCP1 | - | - | | ? | 10.1.233.130 | FortiGate-1000C | ● | | Logging Only |
| root [NAT] (Management) | Synchronized | Never Installed | | | | VDOM | ● | | |

**NOTICE:** In the current software release and prior, the ZCP firewall is only supported on the Fortinet 100D hardware platform as well as on the Fortinet 1000C hardware platform models. The procedure that follows corrects the display issue for the Fortinet 100D hardware platform only. The procedure will not correct the display issue for the Fortinet 1000C hardware platform. If a Fortinet 1000C hardware platform is installed in the ASTRO® 25 system and is experiencing this issue, then the Device Manager entry for that firewall should be disregarded. Note however, that the logs from all VDOMs are still collected and stored on the FortiManager and they can be viewed, analyzed, archived, etc. For more details on viewing the logs, see the *FortiManager 5.2.7 Administration Guide*.

**Procedure:**

1 Delete the firewall entry from the FortiManager. See Deleting an Existing Fortinet Firewall Object on page 52.

  After the FortiManager receives a new request from the same firewall to send logs to the FortiManager, the requesting firewall will be listed under **Unregistered Devices**.

2 Add the firewall to the FortiManager. See Adding FortiGate Firewalls to the Fortinet Firewall Manager on page 43.

3 If the Device Manager still displays the serial number of the firewall instead of the configured hostname, repeat step 1 and step 2.

## 5.4
## Rebooting the Fortinet Firewall Manager

**Procedure:**

1 Log on to the Fortinet FortiManager.

  See Logging on to the Fortinet Firewall Manager on page 32.

2 Click the **System Settings** tab.

3 In the **Unit Operation** area, click **Reboot**.

4 In the confirmation window, click **OK**.

  Optionally, you can type a message to be logged in the event log.

## Chapter 6

# Fortinet Firewall Manager Disaster Recovery

This chapter provides disaster recovery procedure for the Fortinet FortiManager.

## 6.1 Recovering the Fortinet Firewall Manager

**Prerequisites:** For information on DAS devices, see the *Virtual Management Server Software* manual.

**Process:**

1. If applicable, perform one of the following actions. Otherwise, skip this step.

| If… | Then… |
|---|---|
| **You are recovering the VMware ESXi-based virtual server that hosted the Fortinet FortManager virtual machine and the DAS Disaster Recovery does not need to be performed...** | **a** Perform the disaster recovery process for the virtual server host.<br>See the disaster recovery information in the *Virtual Management Server Software* manual.<br>**b** Add the existing Fortinet FortManager virtual machine to the new virtual server host from the DAS storage.<br>See "Adding a Virtual Machine to the Inventory for Expansions" in the *Virtual Management Server Software* manual.<br>**c** Connect and power on the Fortinet FortiManager virtual machine.<br>See Connecting and Powering On a New Virtual Machine on page 40.<br>**NOTICE:** The recovery process is finished. Skip the rest of the steps. |
| **You are recovering the VMware ESXi-based virtual server that hosted the Fortinet FortManager virtual machine and the DAS Disaster Recovery needs to be performed...** | **a** Perform the disaster recovery process for the virtual server host.<br>See the disaster recovery information in the *Virtual Management Server Software* manual.<br>**b** Continue with the next step. |

2. If applicable, delete the existing Fortinet FortManager virtual machine.

   See "Deleting a Virtual Machine" in the *Virtual Management Server Software* manual.

3. Set up the Fortinet FortiManager:

   - If the Backup and Restore (BAR) service is implemented in the system, perform the following to restore data from the BAR server to the Fortinet FortiManager:

     1. Importing the Fortinet Firewall Manager Server Virtual Machine on page 33

2. For systems where vCenter is already installed: Configuring the vCenter for the Newly Deployed VM on page 36
3. Setting the Virtual Machine Startup and Shutdown Order on page 38
4. Connecting and Powering On a New Virtual Machine on page 40
5. Obtaining the Fortinet Firewall Manager License on page 40
6. Configuring DNS on the Fortinet Firewall Manager on page 42
7. Recovering Critical and Non-Critical Data in Fortinet Firewall Manager on page 58
8. Configure security settings on virtual machines.

   See the “Virtual Management Server Operation” chapter in the *Virtual Management Server Software* manual.

- If the Backup and Restore (BAR) service is not implemented in the system, install and configure the Fortinet FortiManager server and user interface.

  See Installing and Configuring the Fortinet Firewall Manager Server and User Interface on page 31.

6.1.1

## Recovering Critical and Non-Critical Data in Fortinet Firewall Manager

**Prerequisites:**

1. Ensure that your organization accounts in the `bkupadm` user group are enabled and their passwords have been reset in Active Directory.
2. Ensure that all Domain Controller installation/configuration has been completed.
3. Ensure that the Backup and Restore (BAR) server is joined to the ASTRO® 25 system Active Directory domain.
4. Obtain the ***<IP address>*** of the BAR server in the UCS zone. Contact your system administrator.

See the *Authentication Services* manual.

**Procedure:**

1. Log in to the BAR server as the user that is a member of the `bkupadm` user group:
   a. At the login prompt, enter the user name.
   b. At the password prompt, enter the password.
2. At the command prompt, enter: `sudo /opt/Motorola/bar/bin/media_prepare_fortimanager_restore`
3. From the list of available backups, enter the number of the backup you want to restore.

   Restore data successful message appears.

4. Log in to the Fortinet FortiManager server as the user that is a member of the `Super_User` group:
   a. At the login prompt, enter the user name.
   b. At the password prompt, enter the password.
   c. If prompted to accept, enter: a
5. At the command prompt, perform the following actions:

| If… | Then… |
|---|---|
| **If you want to restore critical data,** | perform the following actions:<br>**a** At the prompt, enter:<br>`execute restore all-settings sftp` ***`<IP address>`*** `/export/fwm_restore/critical_data/latest fwm_backup` ***`<password>`*** ***`<backup_password>`***<br>Where:<br>***`<IP address>`*** is the BAR server IP address in the UCS zone<br>***`<password>`*** is the `fwm_backup` user password<br>***`<backup_password>`*** is the password that is used to encrypt the Fortinet FortiManager critical settings<br>A warning message appears.<br>**b** Enter y to confirm the restore operation.<br>The restore operation finishes and the Firewall FortiManager reboots. |
| **If you want to restore non-critical data,** | perform the following actions:<br>**a** At the prompt, enter:<br>`execute restore logs all sftp` ***`<IP address>`*** `fwm_backup` ***`<password>`*** `/export/fwm_restore/non_critical_data/`<br>Where:<br>***`<password>`*** is the `fwm_backup` user password<br>***`<IP address>`*** is the BAR server IP address in the UCS zone<br>**b** Enter y to confirm the restore operation.<br>A warning message appears.<br>**c** Enter y to confirm the restore operation.<br>The restore operation finishes and a successful message appears. |

**6** At the BAR server prompt, enter: `sudo /opt/Motorola/bar/bin/media_prepare_fortimanager_restore -c`

This page intentionally left blank.