FortiADC Manager - Handbook

Version 6.2.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
October 22, 2021	Initial release.

Introduction

Welcome, and thank you for selecting Fortinet products for your network.

FortiADC Manager is a web-based management tool which allows you to centrally manage multiple FortiADC devices remotely. Network administrators can better control their devices by logically grouping devices, efficiently managing jobs and licenses, quickly checking various logs, and monitoring threat statistics in real time.

Setting up the system

Welcome to FortiADC Manager! Here's how to get started.

You'll see a **blank dashboard** upon logging in. It's blank because the ADC Manager is a service that manages ADC's, and currently there aren't any ADC's assigned to it. Let's do that, first.
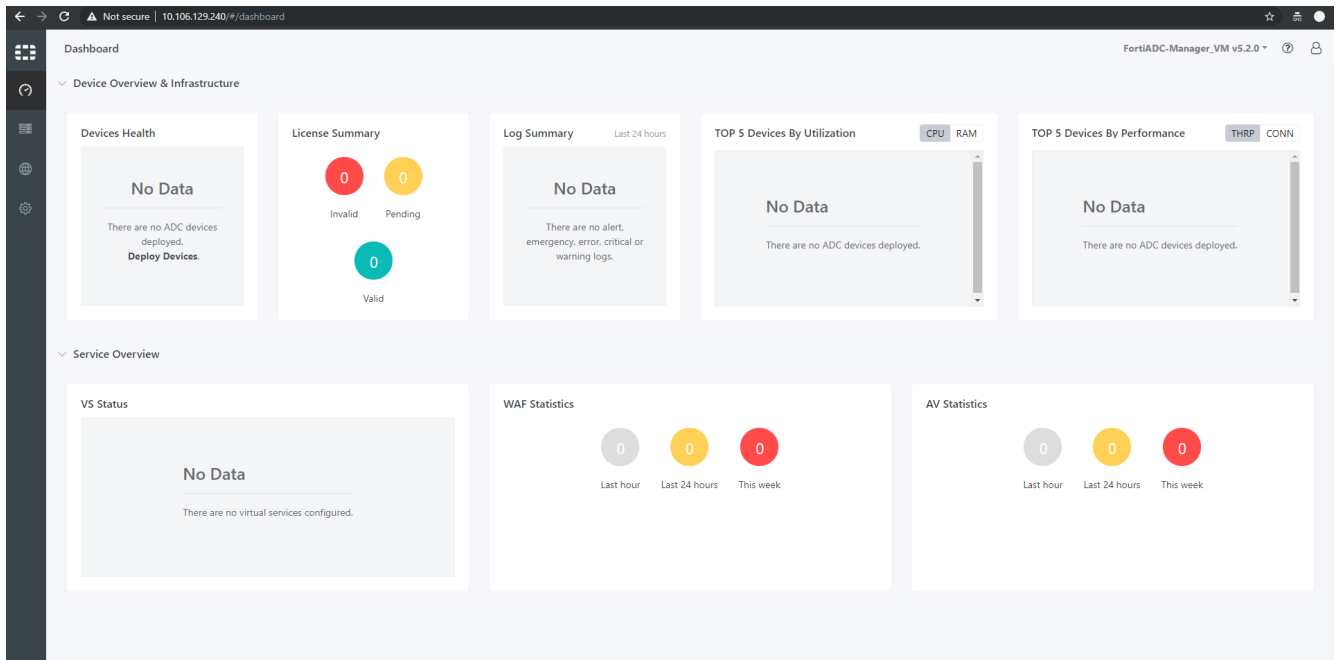

Assigning the individual ADC to the Manager

Don't bother clicking around the Manager for now. Get out of its GUI and go into the specific ADC that you want to assign to the Manager. But first note the following:

1. You are allowing your ADC to be accessed through the Manager, where it will be viewed and edited.

2. ADC-VM's prior to 5.2 are not supported.

Now, enter the vdom as Global. Local vdom's will not work. Then go to **System** > **Central Management**. By default you will see a blank page, with 'none' under **Type**.
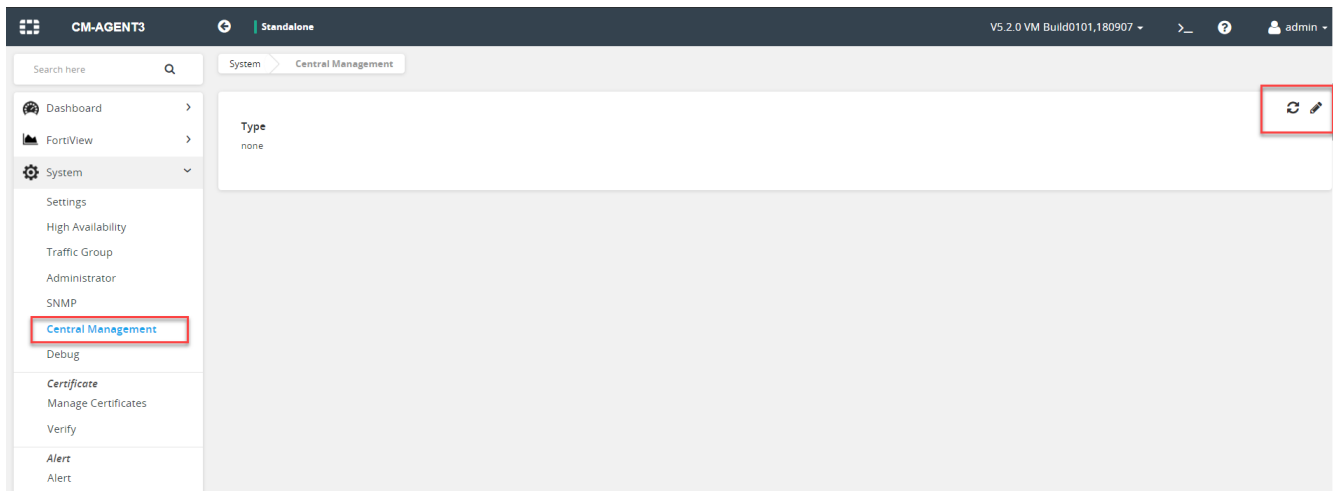
Click **edit.**

The Central Management dialogue box will open. Nothing shows up until you assign **Type** to **FortiADC Manager**.

Now, do the following: enter the **IP address or Hostname of your ADC Manager.** Enter the interval (in seconds) that separates the ADC's attempts to reconnect to the Manager. When all this is done, you can set the **status** to On. As soon as you do so, you can no longer edit the previous information, unless you turn the status off again.

Note: the Management Status will be 'None' until you deploy the device from within the Manager, at which point it will say 'Online.' Then some information should show up on your ADC Manager dashboard.

Type	The management type of the ADC. Default 'None' means no access from Manager to ADC.
Address	The IP address or hostname of FortiADC-Manager.
Interval	How often the ADC tries to connect to the Manager. Default 10 seconds. Range 10-120.
Register	Enable/disable register to Manager. Default is disable.
Management status	The connection status of the ADC. There are two statuses: online/offline/rejected.

Configure the ADC Manager settings

Select the highlighted section on the sidebar, to the far left. This will bring us into **Settings**.
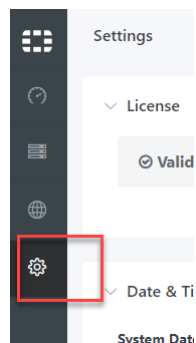
Settings
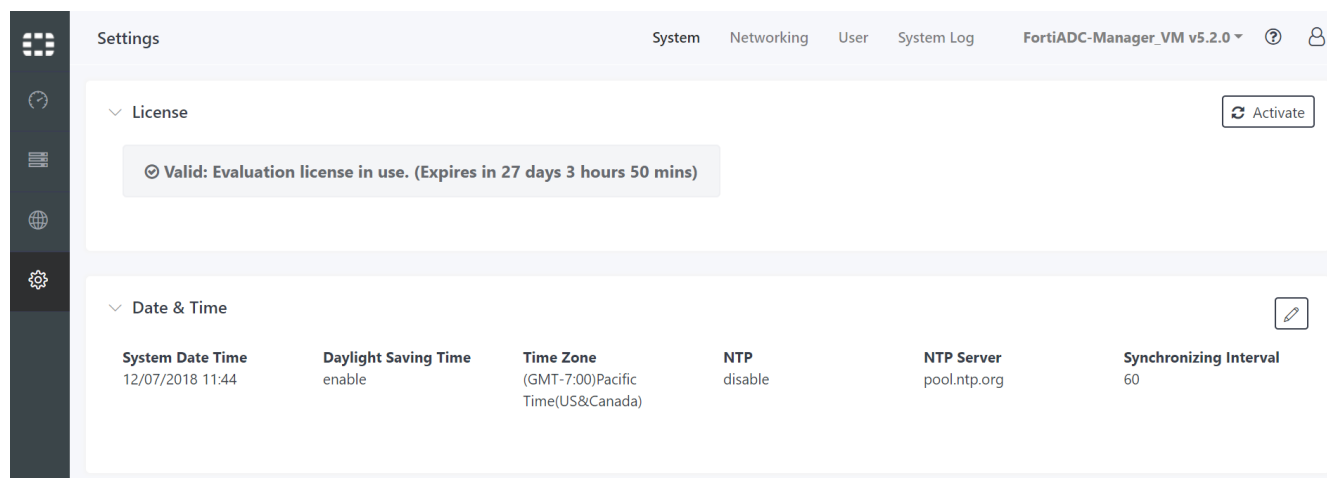
Important! Consult the ADC Manager handbook page Settings for configuration details.

To configure general settings:

1. Activate your license. The default license is an evaluation license. With it, you can only manage two ADC's. Note: A base license supports up to ten devices, while an unlimited license supports any number of ADC's. Go to

support.fortinet.com to register and get an activation code.

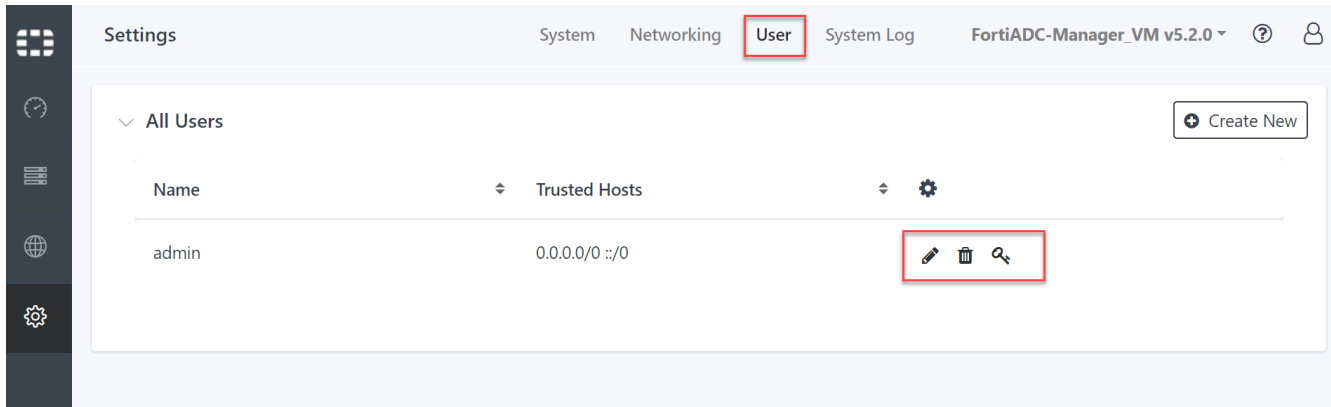2. Date and time. Change the date and time; the default might not be correct.

3. Don't worry about Firmware and Configuration right now.

4. Go to **Networking**. Edit the Interface, Static Route, and DNS to your liking. Again, reminder to see Settings for configuration details.

5. Go to User. Here, edit the user name or password, or even create a new user.

Importing certificates for GUI access

To use a customized certificate for FortiADC Manager's GUI access, use either of the following two options to import the certificate.

Option 1: Importing the certificate from external location

Generate a Certificate Signing Request (CSR) on FortiADC Manager, and have it signed by a trusted Certification Authority (CA). This is done using a private key generated on FortiADC Manager during the CSR generation process.

1. Generate the CSR with the following command:
   ```
   exec certificate local generate <cert_name>...
   ```
   The "cert_name" above is the administrative name of the certificate object in FortiADC Manager. Use tab and ? to discover all the options and parameters for the CSR. The "subject" should match the hostname (or possibly the IP address) used to access FortiADC Manager to prevent certificate warning messages to the users.

2. Export the CSR to have it signed by the CA using the following command:
   ```
   exec certificate local export tftp <cert_name> <file_name> <IP_of_TFTP_server>
   ```
   The "cert_name" is the name used in Step 1. "file_name" is the name of the file as it will be on the TFTP server directory. Typically with a .csr or .pem suffix.

3. Import the signed certificate in the FortiADC-CM using the following command:
   ```
   exec certificate local import tftp <file_name> <IP_of_TFTP_server>
   ```
   The "file_name" is the name of the file on the TFTP server. FortiADC Manager will automatically map it to the corresponding CSR generated in step 1.

4. (optional) If the certificate is signed by a CA intermediate in one or multiple steps to the Root CA trusted by the clients, the intermediate CA certificates need to be imported for FortiADC Manager to be able to provide them on

TLS connection establishment.

- Import the intermediate certificate(s) using the following command:

```
exec certificate intermediate_ca import tftp <intermediate_file_name> <IP_of_
TFTP_server>
```

The "intermediate_file_name" is the name of the intermediate CA as read from the TFTP server. This, without the filename suffix, will also be the name of the Intermediate cert object in FortiADC Manager's CLI.

- Repeat the above step until all the intermediate CA certificates are imported.
- Create an intermediate CA group. The following code adds two intermediate CAs in the group. This is just an example. You can add more or less as you desire.

```
config system certificate intermediate_ca_group
   edit <myGroupName>
      config group_member
      edit 1
         set ca <name_of_first_intermediate_CA_cert>
      next
      edit 2
         set ca <name_of_second_intermediate_CA_cert>
      next
   end
end
```

5. Activate the Intermediate CA cert group and the custom certificate to be used by the HTTPS server on FortiADC Manager:

```
config system global
   set default-certificate <cert_name>
   set default-intermediate-ca-group <myGroupName>
end
```

The "<cert_name>" is the one used in step 1, and "myGroupName" is the one set in step 4.

Option 2: Importing both certificate and private key from external location

In this option, you import both the certificate and private key externally.

1. Create the certificate and key object using the following command.
Use quotation marks to start and end multi-line input. A multi-line certificate can be pasted in one-go when quotation marks are used correctly.
Important: The private key needs to be in unencrypted PEM format, and will later be encrypted for storage on the FortiADC Manager.

```
config system certificate local
   edit <cert_name>
      set private-key "-----BEGIN RSA PRIVATE KEY-----
      >
      >
      > -----END CERTIFICATE-----"
      set certificate "-----BEGIN CERTIFICATE-----
      >
      >
      > -----END CERTIFICATE-----"
   end
end
```

The certifciate is now created/imported including its private key.

2. (optionally) Refer to step 4 in Option 1 if you need to import intermediate CAs
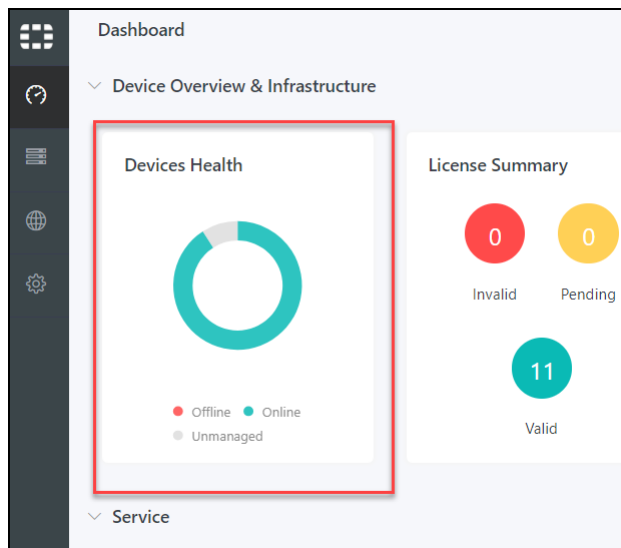3. Activate the certificate as introduced in step 5 of Option 1.

GUI Overview

Here's what your Manager dashboard should look like if you've connected a lot of ADC's to it.
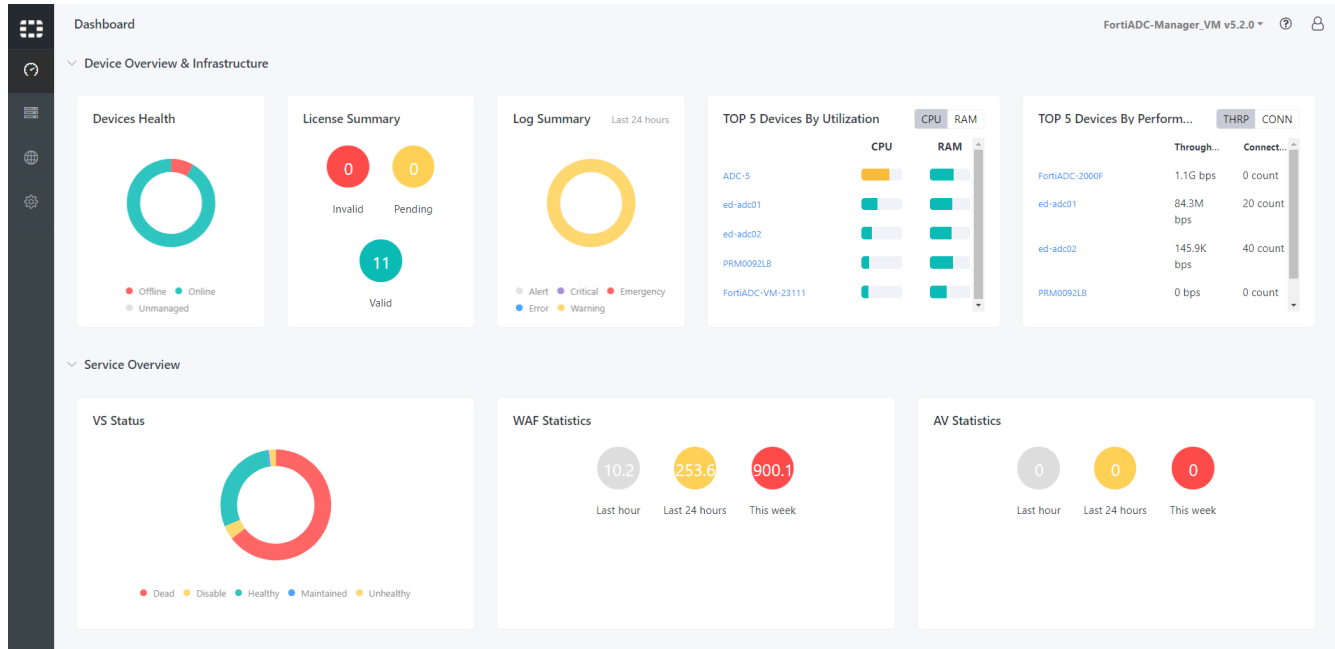
How to use the dashboard

If you want to know more about a particular subject, click on the corresponding widget. We'll look at Devices Health.

In the dashboard view, you see only three options, Offline, Online, Unmanaged. At first view, it will tell you only the rough proportion of which devices are offline/online/unmanaged.

But if you hover your cursor over it, it will give you the specific number of, say, offline devices.

If you want to know more, however, if you want to see *all* the information, click on the widget and it will bring you to Device Management

What's on the dashboard

Device Overview & Infrastructure	
Devices Health	Shows the status of your managed/unmanaged devices that connect to manage.online/offline/unmanaged.
License Summary	Shows the status of your licenses, what proportion is invalid/pending/valid.
Log Summary	Shows the status of logs, and what proportion of your logs are in danger.
TOP 5 Devices By Utilization	Shows which five devices are using the most CPU/RAM.
TOP 5 Devices By Performance	Shows which five devices are performing at the highest throughput/connection.

| Service Overview	
VS Status	Shows the status of the virtual servers.
WAF Statistics	Shows how many Web Application Firewall logs were created in the given time span.
AV Statistics	Shows how many Antivirus logs were created in the given time span.

Device Management

We'll go about this in two ways. First, we'll show you how to deploy a single device. Currently we've *assigned* an ADC to the Manager, but it hasn't been deployed; an ADC shows up on the Manager, but the Manager can't yet manage it. After that, when we've familiarized ourselves, we'll show you all the useful GUI functions of the Device Management dashboard.

1. Explore the individual managed ADC

2. Explore how to manage the ADC's in groups

Confused by the Device Management dashboard? See: Managing your ADC's.

Deploy your ADC

Here's your Device Management dashboard. Look on the sidebar to the left.
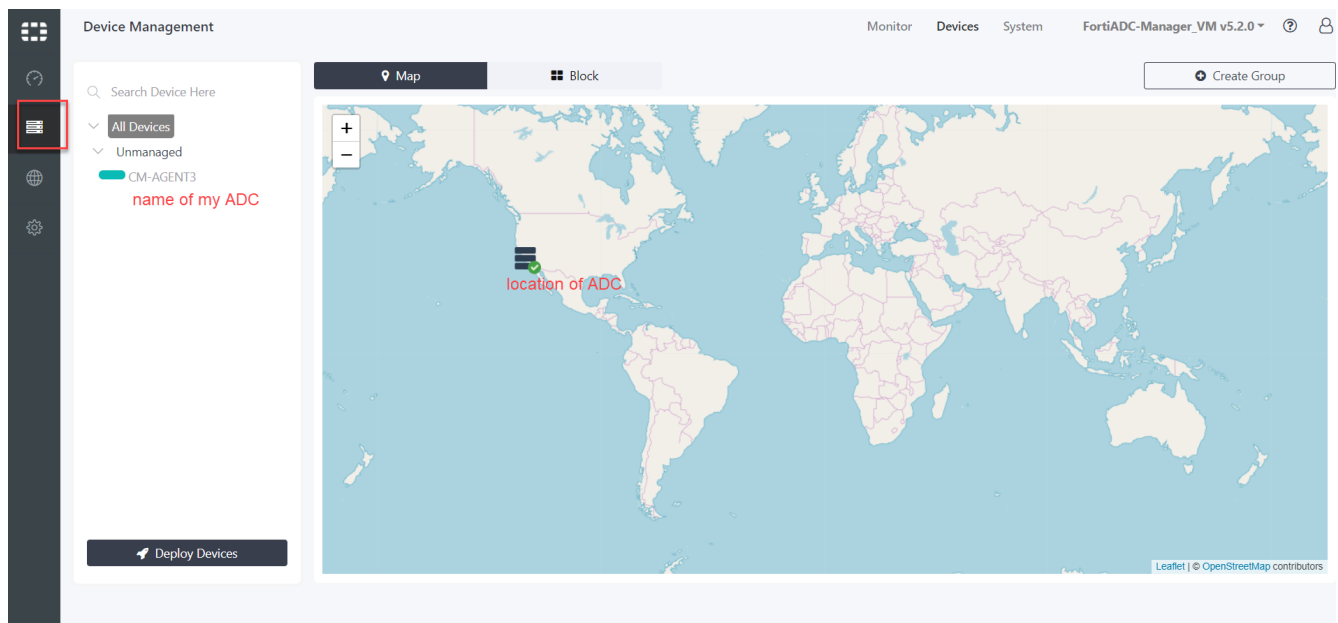
Right now we only have one ADC connected, CM-AGENT3. It's under the group "Unmanaged." It is represented on the map, near California. Ignore the other details for now.
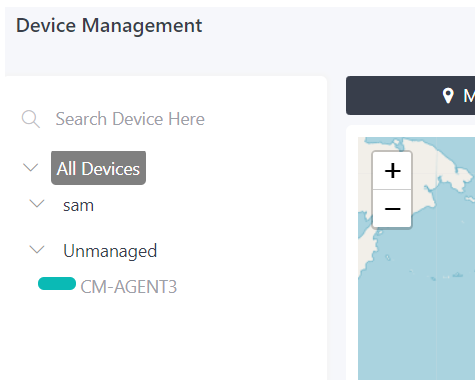
1. Create Group

The ADC Manager uses groups to organize its ADC devices. Every ADC is placed into either "Unmanaged" or a group that you create. You cannot deploy an ADC without first moving it into a managed group.

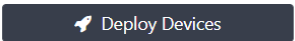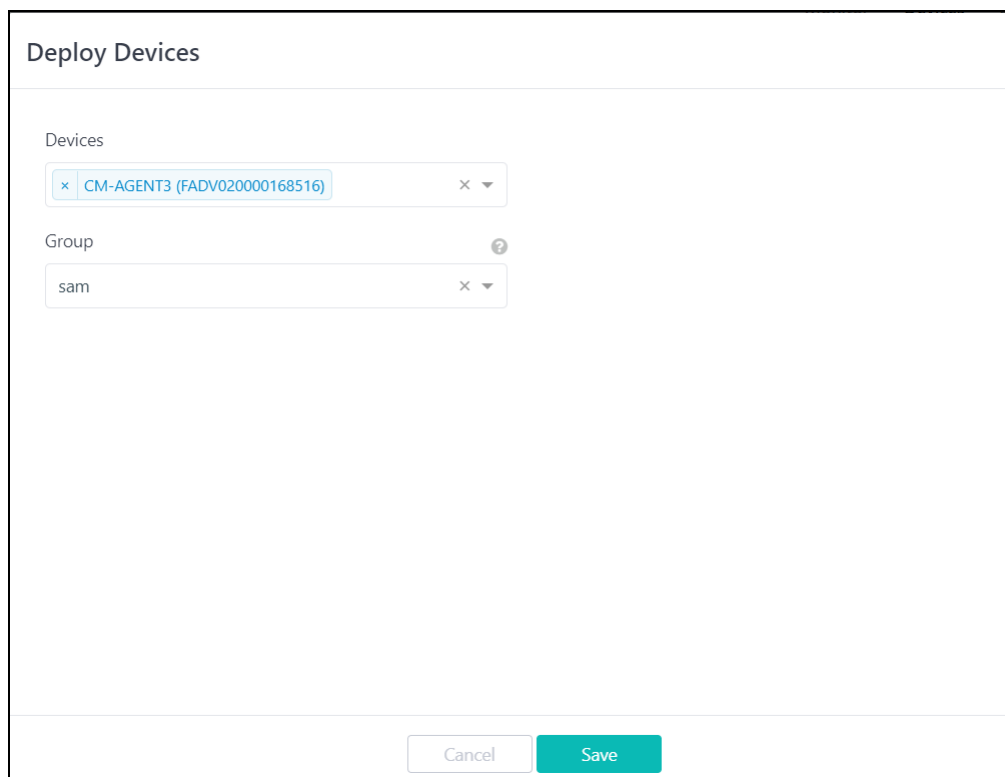Look on the top right. Use the Create Group function.

It will open a simple dialogue box. Name your group. Now it will appear on the left sidebar. I've named mine "sam."

Now I have two groups, "sam" and "unmanaged."

2. Deploy Devices

Finally, I can go to Deploy Devices, at the bottom left. A dialogue box will show. You will have the option to place your device into the group that you just created. Do that.

Deploy Devices

Devices

| × CM-AGENT3 (FADV020000168516) | × ▼ |

Group ⍰

| sam | × ▼ |

Cancel   Save

Your device will move into the created group. See how CM-AGENT3 has moved under "sam"?

Now you can click into the ADC, **in my case, CM-AGENT3.** Enter to see the individual ADC dashboard.

The Deployed ADC

Now the ADC is deployed. We can begin to manage it. The ADC Manager has this advantage: you can edit or view the individual ADC without having to open it up, saving time. All of these functions may be done within the ADC itself, it should be noted.
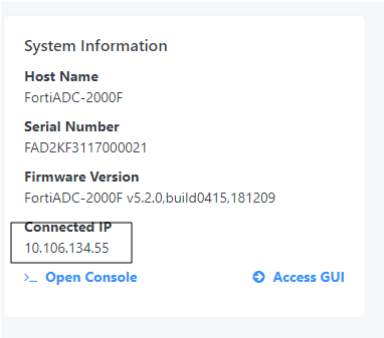
The ADC dashboard

Here is the dashboard for the *individual* ADC. It's not the Device Management dashboard. If you don't know how to get here, click one of your ADC's on the Device Management page, as shown below:
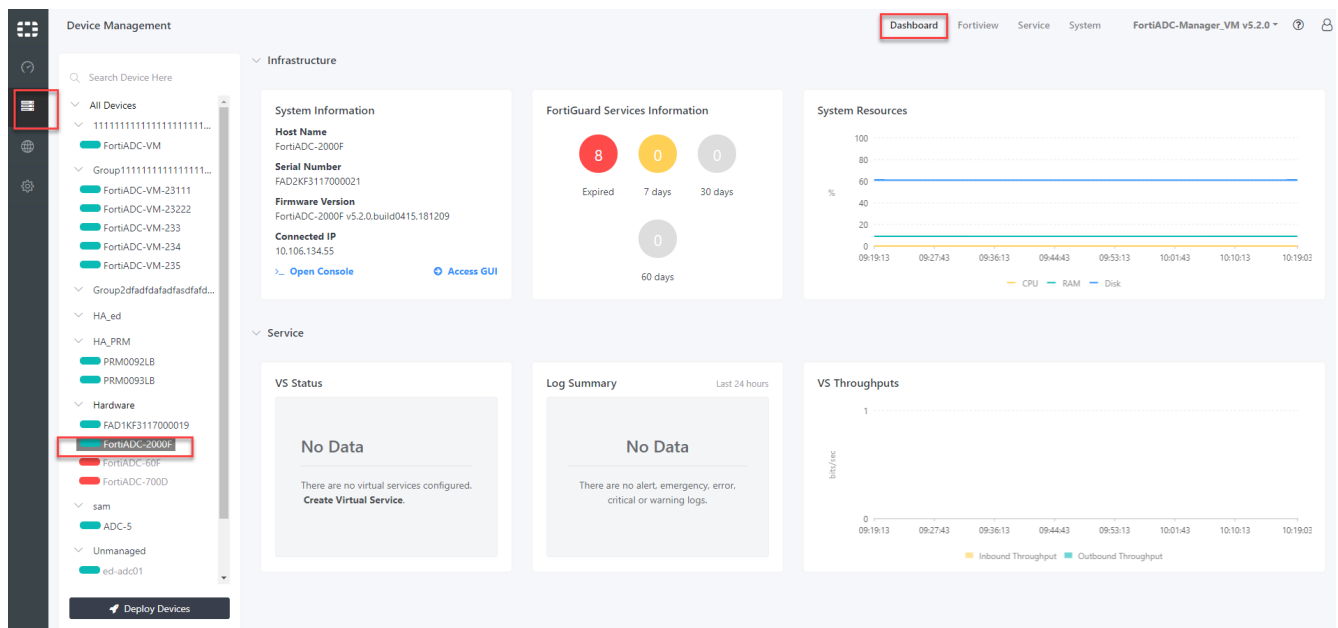
System Information

Shows information about the individual ADC device. The connected IP is the ADC's IP.

Host Name	The hostname part of the FQDN, such as www. Note: You can specify the @ symbol to denote the zone root. The value substituted for @ is the preceding $ORIGIN directive.
Serial Number	Serial Number of the ADC
Firmware version	Firmware version of the ADC
Connected IP	IP of the ADC connected to the Manager

1. Open Console. Pulls up a console black box through which you can edit the ADC, without going into the ADC itself.
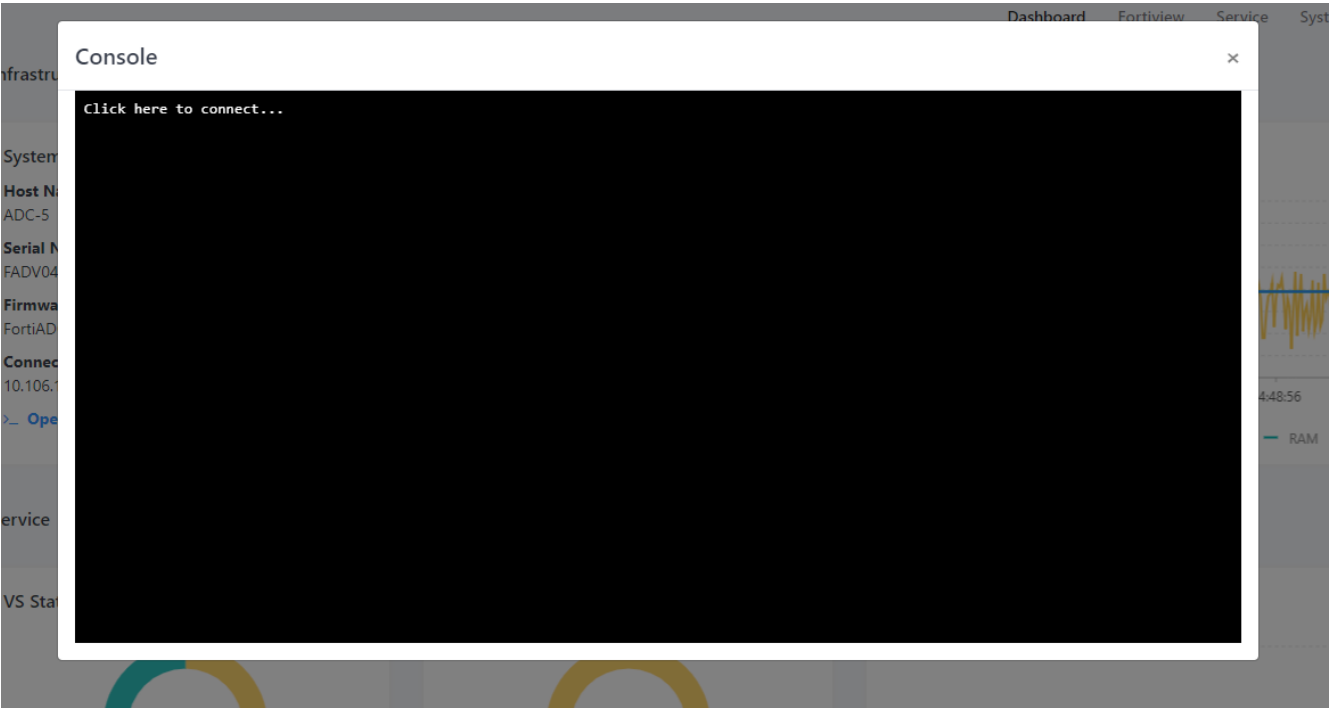
2. Access GUI. Brings you into the managed ADC - no longer in the Manager; we're in the ADC. Note: On that ADC web page the IP address will not show the normal ADC IP; it will show the Manager's IP with the port number (the port number used to connect to the ADC).

As in: xx.xxx.xxx.xxx:yyyyy

The 'x' belongs to the manager, whereas the 'y' is the port number.

Dashboard widgets

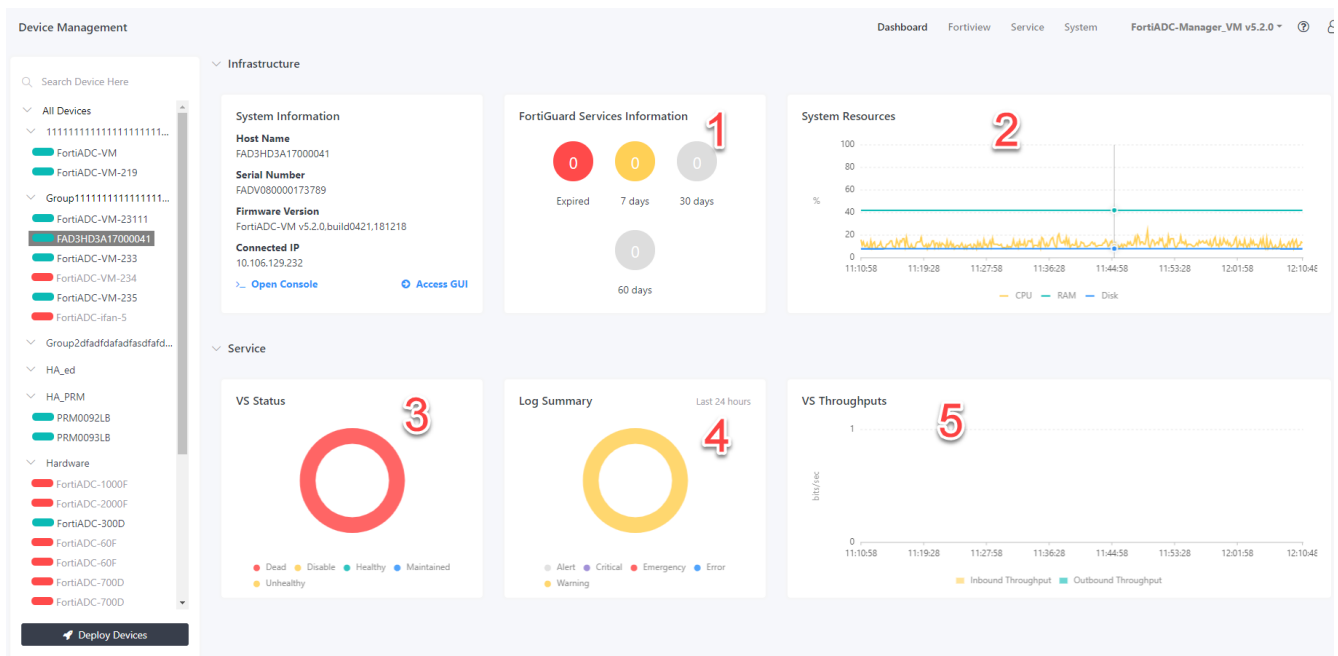| 1. FortiGuard Services Information	Displays the status of FortiGuard services, their expiration dates. When you hover over it, the **See More** will make you jump to System.
2. System Resources	Shows the percentage utilization of CPU, RAM, and Disk by the ADC. Hover over it to see the usage for a particular time stamp.
3. VS Status	Shows the status of the virtual servers for this particular ADC. Hover over it to see the number of devices that are, for example, 'healthy,' or 'unhealthy.'
4. Log Summary	Shows information received from the logs of this particular ADC. Hover over it to see the number of Logs that are in, say, 'warning.' Also hover over it to go into Global Repository > Log. This is a comprehensive page that shows all the logs for not just this ADC, but every ADC connected to the Manager. Emergency—The system has become unstable. Alert—Immediate action is required. Critical—Functionality is affected. Error—An error condition exists and functionality could be affected. Warning—Functionality might be affected.
5. VS Throughputs	Shows how much traffic is coming into the VS's of the ADC and how much is going out. Hover over it to see the time stamp.

Fortiview

The Server Load Balance>Logical Topology page uses the tree-view format to show the internal configuration of each virtual server on the FortiADC. See the handbook for more information.
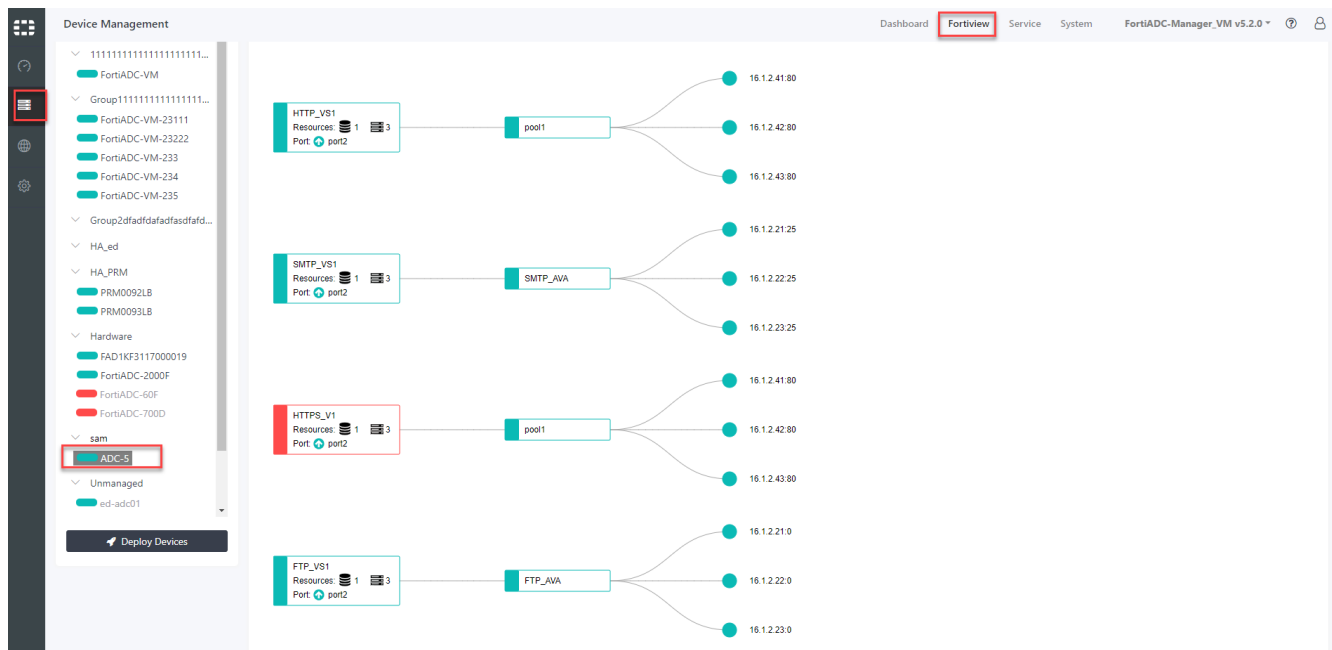
Virtual Server, Real Server, and Health Check

Under **Service**, gives 'at a glance' information about **Virtual Server**, **Real Server**, and **Health Check**.

Virtual Server

To configure a virtual server, see the **Create New** button on the top right. Follow the steps detailed here in the handbook. You can ignore the bottom half of the guide, which deals with advanced configuration. Essentially, you are configuring a virtual server from within the Manager.

You can also create a real server inside the VS. This real server will show up below, on the same page, under Real Server.

Virtual Server ×

Name *

Application

Click to select. ▾

Address *

Port *

Interface *

Click to select. ▾

Existing Real Server

Click to select. ▾　⊕ Create New Real Server

Real Server	Address	Port

Health Check

Enable　Disable

Cancel　Save

Real Server

To configure a real server, click the **Create New** button on the top right. Follow the steps detailed here in the handbook.

Health Check

Displays status of health checks. For more information, go to the handbook.

System

This pages shows the individual ADC System. Device Management > your individual ADC > System. Here you can upgrade your firmware, backup configurations, apply logs, etc.
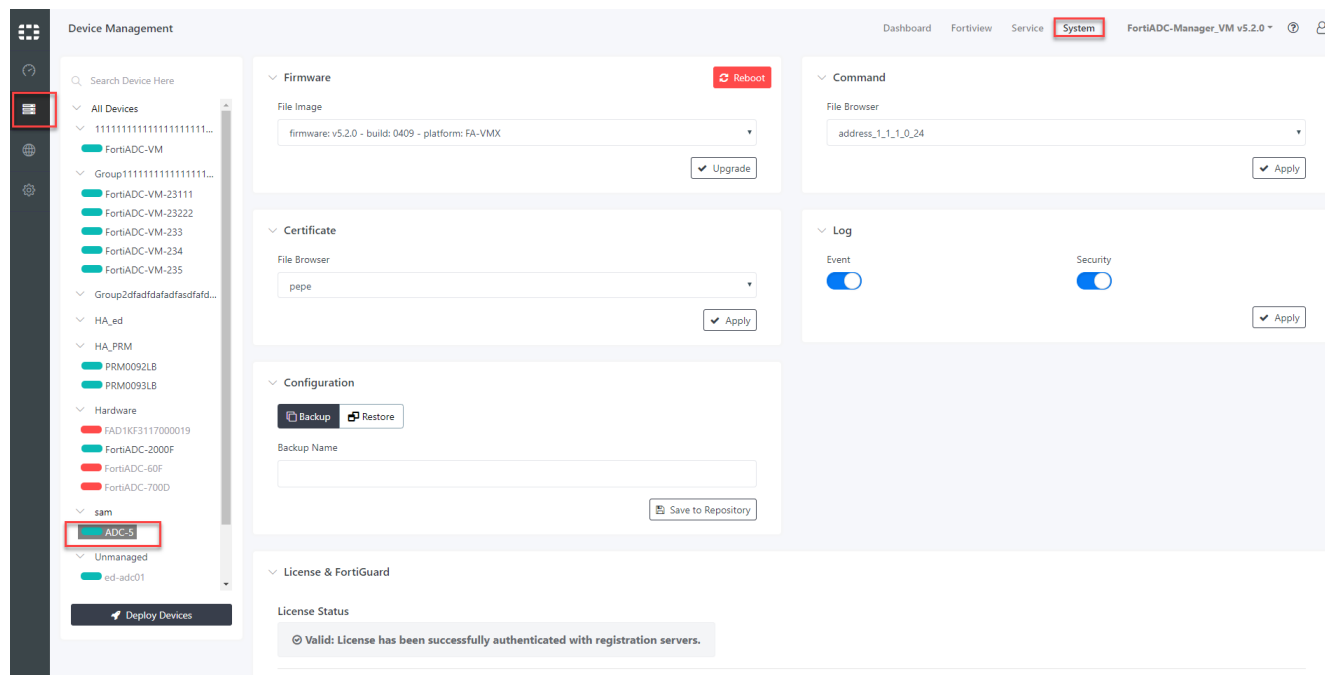
Upgrade firmware

See information on upgrading firmware in the handbook.

Here you have the opportunity to upgrade the firmware of your ADC from within the Manager. Select your firmware from the **drop down.** If nothing appears, you have yet to upload a firmware image into the Global Repo Firmware.

To do so, navigate to Global Repository > Firmware > Upload Firmware. See Global Repository

Go back to System, where the firmware should now appear. Choose what you want, upgrade, then reboot.
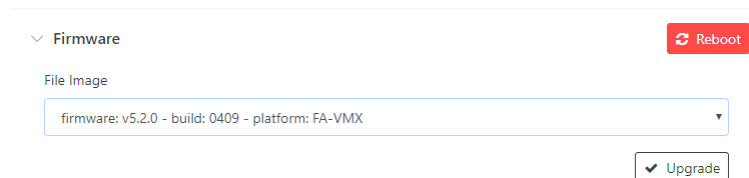
You are upgrading the individual ADC, using a firmware image from the Global Repo. You cannot add file images here in the individual ADC system, you can only select from preexisting ones. Note: it is also possible to upload images from the individual ADC GUI, not in the Manager. These images will show up here as well.

Apply command

See information about commands in the handbook.

Premade commands may be applied to the individual ADC. If you don't see anything, it means you haven't created any commands. To do so, go to Global Repository > Command. See Global Repository

If you've created a command, choose from the **drop down**, then apply.

⌄ Command
File Browser
address_1_1_1_0_24 ▾
✔ Apply
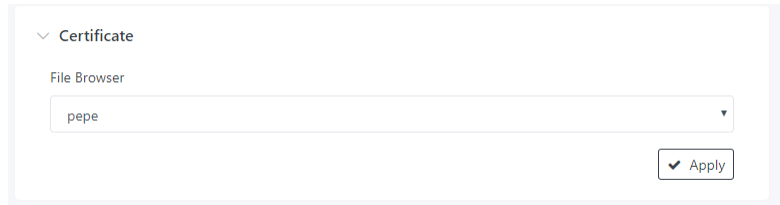
Apply local certificate

See information about certificates in the handbook.

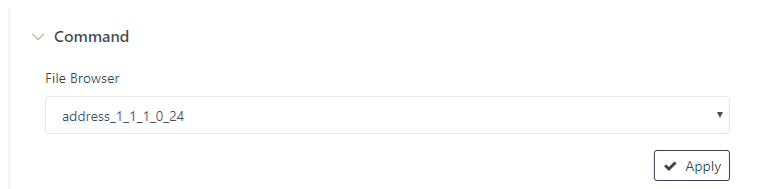Local certificates may applied to the individual ADC. If you don't see anything, it means you don't have any certificates. To get one, go to Global Repository > Certificate. Upload a certificate there. See Global Repository

If you have a certificate available, choose from **drop down**, then apply.

⌄ Certificate
File Browser
pepe ▾
✔ Apply

Apply Event and Security Log

Apply the Event and Security Log.

See information about the event log in the handbook.

See information about the security log in the handbook.

These new logs will appear alongside other ADC logs, this time in the Manager, in Global Repository Log. This is the page where all the logs are gathered. They will also appear on the Manager dashboard, as one of the widgets, under Log Summary.
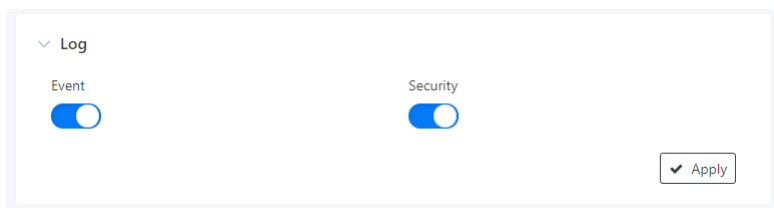
If you want to see what's changed, click into the individual ADC GUI.

Go to Log & Report > Log Setting > Syslog Server. Click one of the logs. In this image, its ID is "2".
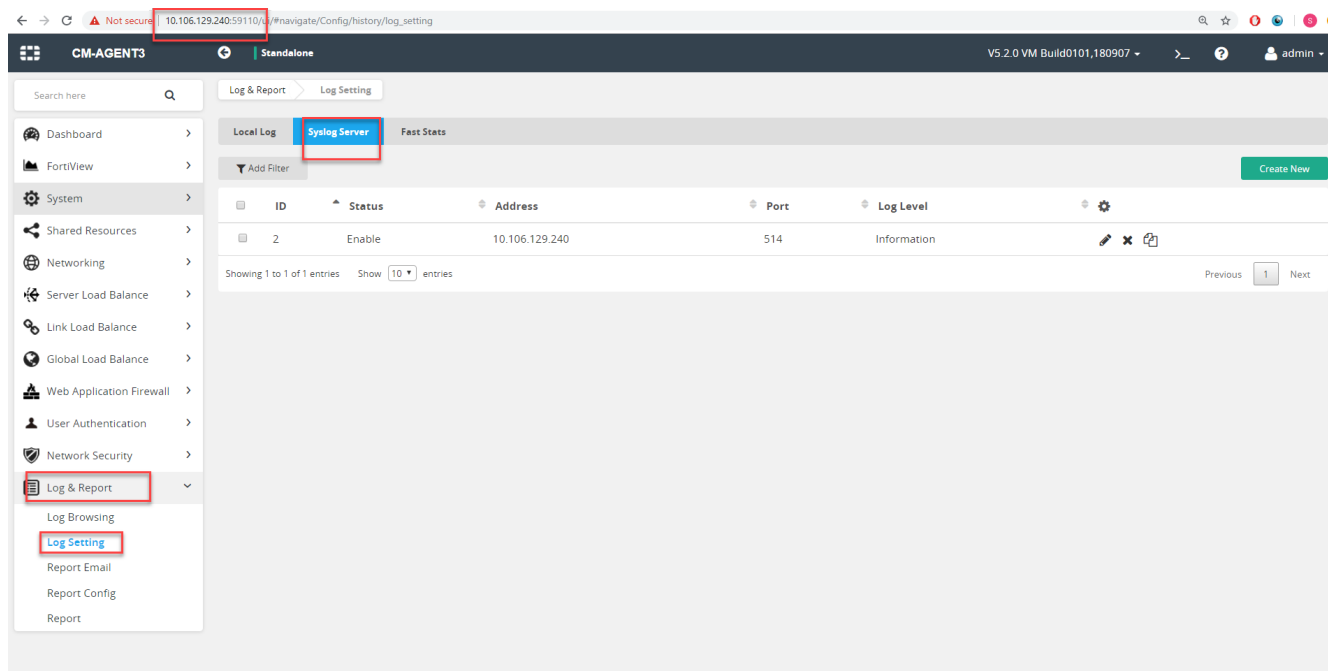
Applying the Event and Security logs in the Manager will have an affect on the individual ADC.

Now the dashboard of the individual ADC - not in the Manager - will show an Event and Security log.

Syslog Server

Status
ON

Address
10.106.129.240

Port
514

Log Level
Information

CSV
OFF

Facility
Kern

Event
ON

Event Category
☑ Configuration ☑ Admin ☑ System ☑ User ☑ Health Check
☑ SLB ☑ LLB ☑ GLB ☑ Firewall ☑ Enable All
Required. Please select at least one category.

Traffic
OFF

Security
ON

Security Category
☑ Synflood ☑ IP Reputation ☑ WAF ☑ GEO ☑ AV ☑ Enable All
Required. Please select at least one category.

Save   Cancel

Backup and Restore

See more information in the handbook.

Choose from the drop down.

Configuration

Backup   Restore

Select Configuration

Name: 11111111111111111111111111 : Build: 0407 : Version: v5.2.0

✔ Apply

There are two options:

1. **Backup** a configuration of the individual ADC. It will be stored in the manager. Go see it in Global Repository > Configuration.

System

2. **Restore** the ADC to a previous configuration. These configurations are available in the same place, Global Repository > Configuration.

Note: You can use this backup to restore another ADC. It's useful if you want to **duplicate ADC's**, or to create many of the same kind.

Restoring another ADC with a configuration

1. If you have one configuration that you like, back it up, and it will appear in Global Repository > Configuration.
2. Then, staying in the Manager, go to the Manager dashboard of the *other* ADC.
3. Go to its System and restore it with the ADC configuration you just made.

License Status

Tells you the status of your licenses. For information about Fortiguard Services, see the ADC Handbook, Network Security.

License & FortiGuard

License Status

⊘ **Valid: License has been successfully authenticated with registration servers.**

FortiGuard Services

Support Contract

Status	Category	Expiration
▬	Hardware	(Expires: Unknown)
▬	Firmware	8 X 5 support (Expires: 2019-06-18)
▬	Enhanced Support	8 X 5 support (Expires: 2019-06-18)
▬	Comprehensive Support	(Expires: Unknown)

FortiGuard Services

Status	Category	Version	Last Update Time	Last Update Method
▬	WAF Signature	00001.00020 (Expires: 2019-06-18)	2018-12-12 14:30:13	Schedule
▬	IP Reputation	00001.00094 (Expires: 2019-06-18)	2018-12-12 14:30:13	Schedule
▬	Geo IP	00002.00027 (Expires: Unknown)	2018-12-12 14:30:13	Schedule
▬	Web Filter	Licensed (Expires: 2019-06-18)		

Antivirus

| Status	Category	Version	Last Update Time	Last Update Method
▬	Regular Virus Database	00062.00346 (Expires: 2019-06-18)	2018-12-12 14:30:13	Schedule
▬	Extended Virus Database	00062.00299 (Expires: 2019-06-18)	2018-12-12 14:30:13	Schedule
▬	Extreme Virus Database	00062.00323 (Expires: 2019-06-18)	2018-12-12 14:30:13	Schedule
▬	AV Engine	00006.00006 (Expires: 2019-06-18)	2018-12-12 14:30:13	Schedule

Managing your ADC's

Now that you've deployed your individual ADC, we can step back and view multiple ADC's in groups. The advantage of the Manager is this: the ability to group your ADC's and receive a variety of 'at a glance' information.

The Device Management dashboard

Here's your Device Management dashboard, with many ADC's connected. This is *not* the dashboard of the general ADC Manager, which you saw when you opened up the Manager itself; it was the first thing you saw. Rather, this dashboard appears when you click Device Management in the sidebar.

Click around the map to see what information appears.
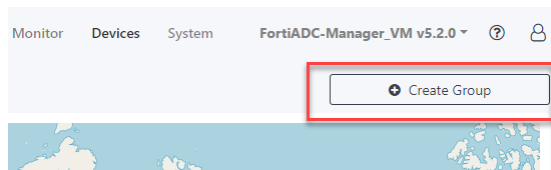
Map view
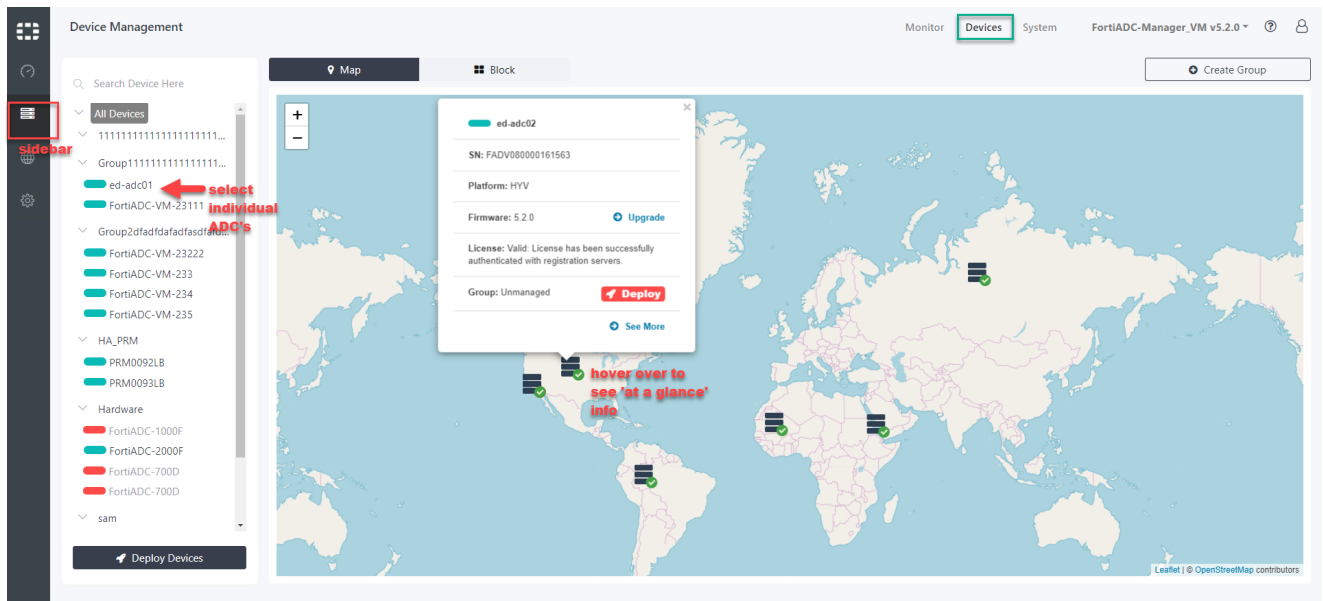
Device Management sidebar

This is your control room. It's the sidebar above with all the names of the ADC's, some in green, some in red. Here your ADC appears in the groups to which they're assigned. By default, at the very bottom will appear (unseen in this diagram) a group called "Unmanaged."

- You can search your ADC by name.
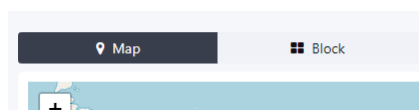- You can't search by place.

Create group

Use this to create a group. You cannot deploy an ADC without having a group. By default the ADC is in the "unmanaged" group, where it is basically useless.

Map and Block

You're currently in Map view, with the worldview and the oceans. Click Block.

Block view

The Block is separated into three parts: Groups, Deployed, and Unmanaged Devices.

Groups	
Edit	Edit name.
Deployed	
Edit	Edit name (only for active/green devices)
Undeploy	Undeploy the device. It will then appear in the group Unmanaged devices
Upgrade firmware	Upgrade the firmware (only for active/green devices)
Unmanaged Devices	
Deploy	Deploy the device. It will then appear in Deployed.

Map view

This mode presents information in map form, so you can see the location of your ADC. Hover over the device to open up the 'at a glance' information. This floating box will shift between ADC's.

Note: Overlap issue. When two or more ADC's are in the same location, you sometimes can't click into the ADC you want. In this case, switch to Block view.

Name	Name of the ADC

Serial Number	Serial number of the ADC
Platform	The platform the ADC is running on.
Firmware	Upgrade the firmware (only for healthy devices). If you can't upgrade your firmware, it means that your device isn't deployed. Deploy it by clicking the red 'rocket' button.
License	The status of the license. • The default license is an evaluation license. With it, you can only manage two ADC's. • A base license supports up to ten device. • An unlimited license supports any number of ADC's. Go to **support.fortinet.com** to register and get an activation code.
Group	The group that the ADC belongs to.
Undeploy/deploy	Deploy or undeploy your device
See More	Only shows up for deployed devices. Goes into the Individual ADC dashboard. The Deployed ADC

Note: Let us say you have a deployed ADC that is connected to the Manager. If you go into the individual ADC > Central Management and turn off the connection (i.e. disable the register), then the ADC will appear in the Manager as red. The license will be unknown, but you can still Undeploy it.

Monitor

Device Management > Monitor. Shows a view of what devices/VS are Healthy, Dead/Disabled, and Unhealthy/Maintained.

System

Device Management > System. Shows the version and status of each device.

Device Name	Name of the individual ADC device
Version	Version number of the individual ADC device
Status	Status of the individual ADC device's license • Unknown - The license is unknown. Probably the ADC is either undeployed or unmanaged. Go check the Central Management of the ADC • Valid (just one word) - Some license are valid while others are not. • Valid: License has been successfully authenticated with registration servers - All licenses are valid.
See More	Only available for valid licenses. Click in to see more information about the license. Jumps into Individual ADC > System > License & Fortiguard

Global Repository

The Global Repository collects various firmwares, configurations, templates, etc. Whatever you upload here can be applied in the individual ADC. It is useful if you wish to mass produce certain types of ADC's, say, if you want them all configured in a certain way, you might upload a configuration and then apply it to each ADC.

Firmware

Global Repository > Firmware. Firmware repository shows you the available firmwares that you can apply to the individual ADC. When you upload a firmware here, it will appear in the individual ADC system as an option which you can boot up (see: Individual ADC > System > Firmware.)

See information on upgrading firmware in the handbook.

Version	The version of the firmware
Platform	The platform the firmware is running on
Build Number	The build number of the firmware
	Opens up a dialogue box where you can upload a file.
	Download the firmware or trash it

Configuration

Global Repository > Configuration. Configuration repository shows you the available configurations that you can apply to the individual ADC. These configurations will appear as options in Individual ADC > System > Configuration > Restore. You can apply them there.

Name	Name of the configuration
Device	Name of the device from which the configuration originates
Time	Time when the configuration was created
Type	The type of the configuration. • Full -- will show all the default and hidden items • No full option -- will show only the key items, no default settings and no hidden settings Note: There is now only the 'full' option.
User	The user who created the configuration
Version	The ADC version which the configuration is based off of
Platform	The platform the configuration is running on
Build Number	The build number of the configuration

	View, download, or trash the configuration
	Opens a dialogue box where you can upload a configuration. Name it, choose a file, and save.

Command

Global Repository > Command. Command repository shows you the available commands that you can apply to the individual ADC. They will appear as options in Individual ADC > System> Command, where you can apply them. See the CLI reference.

Name	Name of the command
	Edit or trash the command
	Opens up a dialogue asking you to name and create a command.

Certificate

Global Repository > Certificate. Certificate repository shows you the available certificates that you can apply to the individual ADC. They will appear as options in Individual ADC > System> Certificate, where you can apply them.

Name	Name of the certificate
Subject	The information of this certificate
Type	The encryption type of the certificate • RSA • ECDSA
Certificate Type	The type of certificate • Local • CA
Status	Status of the certificate • OK • Expired • Pending
	See/download/trash the certificate
	Opens up a dialogue box to upload a certificate. To configure the certificate, see the handbook.

Log

Collects all logs that the ADC's give. You can sort by device (seeing all the logs for only one device) and severity, as well as choose a start/end time for the log.

Device	Name of the device from which the log originates
IP	The IP of the device from which the log originates
Message	The content of the log
Severity	Info
	Notice
	Warning
	Alert
	Error
Time	Time stamp of the log
	Opens up more information about the log.

Settings

License

To activate your license:

1. Go to support.fortinet.com and log in or register for a new account before proceeding
2. Once you are logged in, go to the home page and click **Register/Activate Contracts** under the **Asset** section.
3. Enter the license registration code as listed on your license certificate when prompted, and click **Next**.
4. On the **Specify Fortinet Registration Information** page, enter a brief product description and select your **Fortinet Partner**. Find your computer ID by going to the FortiADC-Manager CLI and entering the command: `execute computerid`, and input it into the **Computer ID** field.
5. Follow the remaining prompts to complete the activation process.

License overview:

- The default license is an evaluation license. With it, you can only manage two ADCs.
- A base license supports up to ten devices.
- An unlimited license supports any number of ADCs.

Date & Time

See the handbook.

Upgrading firmware

Before you begin:

- Download the firmware file from the Fortinet Customer Service & Support website: https://support.fortinet.com/
- Read the release notes for the version you plan to install.
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- You must have super user permission (user admin) to upgrade firmware.

To boot the firmware on the alternate partition:

- Click **Boot Alternate Firmware.**

The system reboots, the alternate becomes the active firmware, and the active becomes the alternate firmware.

To upgrade firmware:

1. Go to Settings > System.
2. Click Upgrade Firmware
3. Click Choose File to locate and select the file.
4. Click save

Configuration Backup/Restore

You use the backup procedure to save a copy of your system configuration. A full backup is a zip file.

The backup feature has a few basic uses:

- Saving the configuration as CLI commands that a co-worker or Fortinet support can use to help you resolve issues with misconfiguration.
- Restoring the system to a known functional configuration.
- Creating a template configuration you can edit and then load into another system using the restore procedure.

A complete configuration backup is a zip file that includes the complete configuration files, plus any files you have imported, including error page files, script files, and ISP address book files.

In the event that FortiADC Manager experiences hardware failure, being able to restore the entire backup configuration minimizes the time to reconfigure the system.

All backup files follow the same file-naming convention: `hostname_date_time`. For example, a backup file named "FortiADCManager-VM_20171214_0830.txt" means that the backup is made of a system whose hostname is "FortiADCManager-VM", the backup is made at 08:30 on December 14, 2017. It must be noted that the date and time in the backup file name reflects the date and time in your FortiADC Manager's system settings when the backup is performed.

Note: Configuration backups do not include data such as logs and reports.

Back up files can include sensitive information, such as HTTPS certificate private keys. We strongly recommend that you password-encrypt your backup files and store them in a secure location.

Run a manual backup

You can back up your FortiADC Manager system configuration at any time from the Settings > System > Configuration > Backup/Restore

1. Select Back Up.
2. Select a storage location for the backup file, Local PC/Server or FortiADC Manager.
3. Specify a name
4. The maximum total backup file size differs by model. For more information, see Table 131.
5. Click Save.

If you've chosen to back up to FortiADC Manager, the backup file will show up below on a table below Configuration > Backup > FortiADC Manager. You will then have the option of restoring from this backup. Moreover, it will appear in Individual ADC > System > Configuration.

Restore a backup configuration

Use the following procedures to restore a backup of a previous configuration.

1. Select Restore.
2. Select the storage location where the backup file resides.
3. To restore from the Local PC/Server, click Choose File, then upload the desired file.
4. To restore from FortiADC Manager, select the backup from the table, and click the corresponding Restore icon, on the far right.

Note: The time required to restore a backup file varies, depending on the size of the file and the speed of your network connection. Your web UI session is terminated when the system restarts. To continue using the web UI, refresh the web page and log in again.

Static Routes

Static routes specify the IP address of a next-hop router that is reachable from that network interface. Routers are aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets' ultimate destinations. The FortiADC system itself does not need to know the full route, as long as the routers can pass along the packet.

You must configure at least one static route that points to a router, often a router that is the gateway to the Internet. You might need to configure multiple static routes if you have multiple gateway routers, redundant ISP links, or other special routing cases.

For more information about static routes, see the handbook.

DNS

Primary DNS	The system must be able to contact DNS servers to resolve IP addresses and fully qualified domain names. Your Internet service provider (ISP) might supply IP addresses of DNS servers, or you might want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Localhost and broadcast addresses are not accepted.
	Incorrect DNS settings or unreliable DNS connectivity can cause issues with other features, such as FortiGuard services and NTP system time.
Secondary DNS	IPv4/IPv6 address of the secondary DNS server for your local network.

User

	Edit, delete, or change password.
Name	Name of the administrator account, such as admin1 or admin@example.com.
	Do not use spaces or special characters except the 'at' symbol (@). The maximum length is 35 characters.
	If you use LDAP or RADIUS, specify the LDAP or RADIUS username. This is the user name that the administrator must provide when logging in to the CLI or web UI. The users are authenticated against the associated LDAP or RADIUS server.
	After you initially save the configuration, you cannot edit the name.
Trusted Hosts	Source IP address and netmask from which the administrator is allowed to log in. For multiple addresses, separate each entry with a space. You can specify up to three trusted areas. They can be single hosts, subnets, or a mixture.
	Configuring trusted hosts hardens the security of the system. In addition to knowing the password, an administrator must connect only from the computer or subnets you specify.
	Trusted host definitions apply both to the web UI and to the CLI when accessed through Telnet, SSH, or the CLI console widget. Local console access is not affected by trusted hosts, as the local console is by definition not remote, and does not occur through the network.

	If ping is enabled, the address you specify here is also a source IP address to which the system will respond when it receives a ping or traceroute signal. To allow logins only from one computer, enter only its IP address and 32- or 128-bit netmask: 192.0.2.1/32 2001:0db8:85a3::8a2e:0370:7334/128 To allow login attempts from any IP address (not recommended), enter: 0.0.0.0/0 Caution: If you restrict trusted hosts, do so for all administrator accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even one administrator account unrestricted (i.e. 0.0.0.0/0), the system must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until after a login attempt has been received in order to check that user name's trusted hosts list. Tip: If you allow login from the Internet, set a longer and more complex New Password, and enable only secure administrative access protocols. We also recommend that you restrict trusted hosts to IPs in your administrator's geographical area. Tip: For improved security, restrict all trusted host addresses to single IP addresses of computer (s) from which only this administrator will log in.
Password	Set a strong password for all administrator accounts. The password should be at least eight characters long, be sufficiently complex, and be changed regularly. To check the strength of your password, you can use a utility such as Microsoft's password strength meter.

System Log

Collects all logs on the ADC Manager and its connected devices.

Date	Date of the log
Type	System - logs from the Manager Device - logs from the individual ADC
Message	The content of the log
Level	Info Notice Warning Alert Error
User	Admin System