



FortiWeb Manager - Administration Guide

Version 7.4.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



Oct 31, 2023

FortiWeb Manager 7.4.0 Administration Guide

02-602-476230-20180904

TABLE OF CONTENTS

Introduction	5
What's new	6
GUI overview	7
Setting up the system	8
Setting up the network	8
Configuring the network interfaces	8
Configuring routes	9
Configuring DNS	10
Setting up user accounts	11
Configuring profiles	11
Configuring user accounts	11
Configuring authentication server	11
Configuring HTTPS ports	13
Setting the system time & date	13
Setting up notification method for job status	14
Managing FortiWeb devices	16
Adding device groups	16
Adding devices	17
Upgrading devices	18
Managing FortiWeb-VM licenses	20
Applying license to FortiWeb-VM	21
Reclaiming license from FortiWeb-VM	21
Deleting licenses	21
Jobs	23
Managing jobs	23
Creating jobs	24
Viewing job events	25
Managing workflow jobs	27
Creating workflow jobs	27
Viewing workflow events	30
Managing config files	30
Managing command files	31
Managing backup files	33
Plugins	35
FortiWeb CLI commands	36
System	36
User	36
WAF	36
Server Policy	38
Monitoring FortiWeb devices	39
Managing dashboard	39

Viewing logs	41
Filtering logs	41
Log types	41
Attack logs	42
Traffic logs	47
Event logs	48
API Proxy	49
Using API proxy	50
Maintaining the system	51
Viewing system logs	51
Upgrading firmware for FortiWeb Manager	51
Retrieving debug logs	51
Scheduling files deletion	52
CLI Commands	53
set interface	53
Syntax	53
Example	54
set route	54
Syntax	54
Example	54
unset Route	55
Syntax	55
Example	55
show interface	55
Syntax	55
Example	55
get system status	55
Syntax	56
execute formatlogdisk	56
Syntax	56
execute ping	56
Syntax	56
Example	57
execute reboot	57
Syntax	57
Example	57
execute shutdown	58
Syntax	58
Example	58

Introduction

FortiWeb Manager is a web-based management tool, which allows you to centrally manage multiple FortiWeb 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.



FortiWeb Manager 7.4.0 supports image upgrade from 6.2.4 and higher versions. Also you can not restore configurations of this release to any previous version.



FortiWeb Manager 7.4.0 supports managing FortiWeb gateway 6.3.16 and higher versions.

What's new

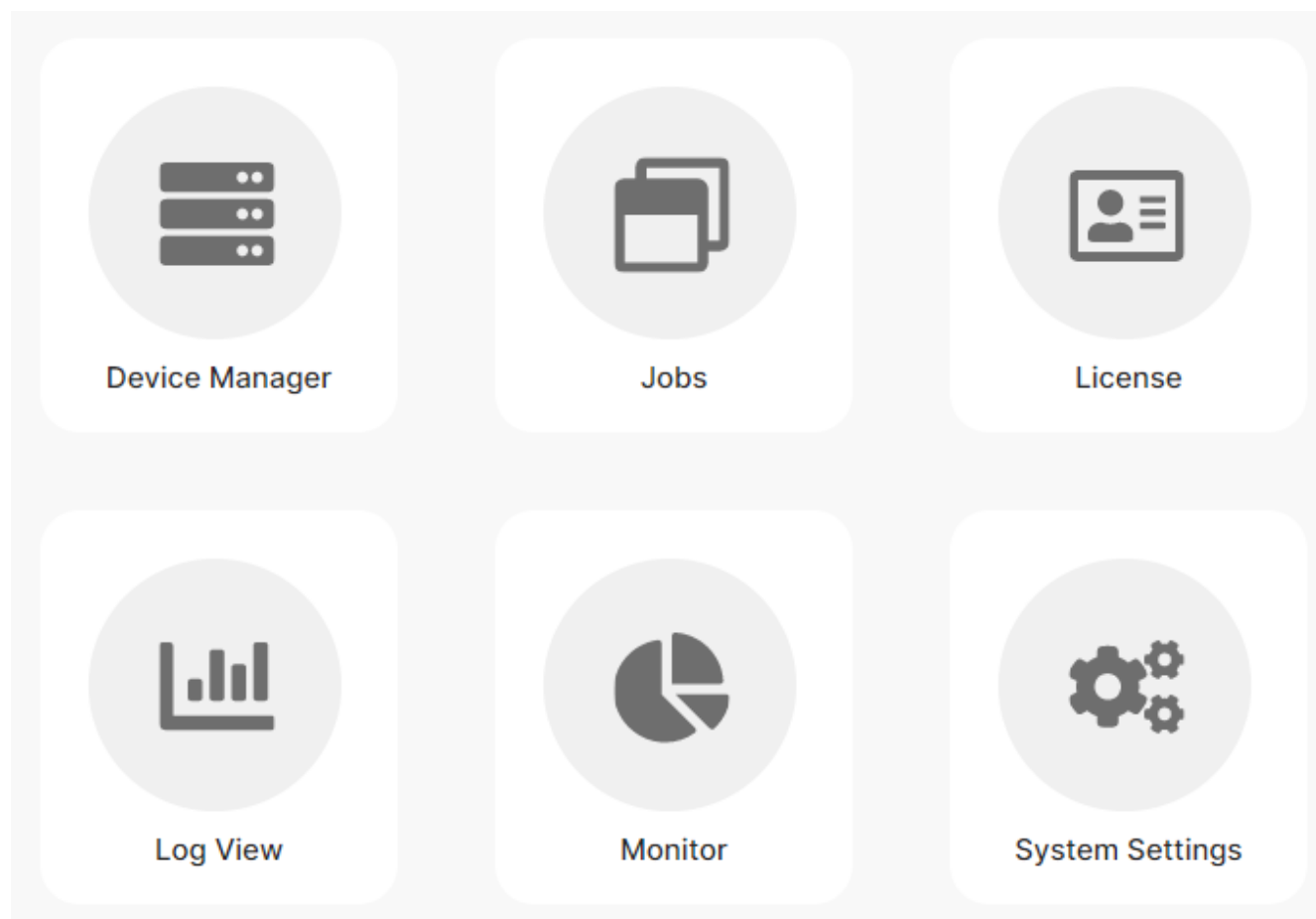
FortiWeb Manager 7.4.0 provides the following new features and enhancements:

FortiWeb 7.4.0 support

FortiWeb 7.4.0 can now be managed in FortiWeb Manager.

GUI overview

When you log into FortiWeb Manager, the following homepage is displayed.



Select one of the following menus to display the respective pane. The available menus will vary, depending on the privileges of current user.

Device Manager	Manage devices such as adding, editing, and deleting FortiWeb devices and device groups, updating device status and information, upgrading device signature and firmware. Allow administrators to export the configuration from FortiWeb.
Jobs	Manage FortiWeb device related jobs in batch with specific scripts.
License	Manage FortiWeb licenses by importing, applying, or reclaiming them.
Log View	Allow you to view all the logs of managed FortiWeb devices.
Monitor	Monitor the threat statistics for the group and each device.
System Settings	Configure and monitor FortiWeb Manager.

Setting up the system

Go to **System Settings** to set up the network, user accounts, system time and job notifications.

Setting up the network

The network settings are used to configure interfaces for the FortiWeb Manager unit. You should also specify what interface that an administrators can use to access the FortiWeb Manager unit. If required, static routes can be configured.



For the initial network settings after deploying the FortiWeb Manager-VM, you need to log in to CLI to configure the network interface and route. For more information, see the "Configuring access to FortiWeb Manager" section in *FortiWeb Manager Deployment Guide*.

The default interface for FortiWeb Manager units is port1. It can be used to configure one IP address for the FortiWeb Manager unit, or multiple ports can be configured with multiple IP addresses for improved security.

You can configure administrative access in IPv4 or IPv6, and the allowed access methods include HTTPS, HTTP, PING, SSH.



The HTTP traffic will be automatically redirected to HTTPS.

Configuring the network interfaces

FortiWeb devices can be connected to any of FortiWeb Manager unit's network interfaces (ports). The DNS servers must be on the networks to which the FortiWeb Manager unit connects, and should have two different IP addresses.

FortiWeb Manager supports the following ports by default. You can edit ports settings, but you cannot add more ports.

Network Interface*	IPv4 Address/Netmask	IPv6 Address/Netmask
port1	192.168.1.99/24	::/0
port2	0.0.0.0/0	::/0
port3	0.0.0.0/0	::/0
port4	0.0.0.0/0	::/0

To configure the interface:

1. Go to **System Settings > Network > Interface**.

2. Select the port1 row.

3. Click **Edit**.

The **Edit Interface** dialog appears. **Name** displays the name and media access control (MAC) address of this network interface. The network interface is directly associated with one physical link as indicated by its name, such as **port1** by default.

4. Configure these settings:

IPv4 Addressing mode	Specify whether FortiWeb Manager acquires an IPv4 address for this network interface manually or using DHCP to allow DHCP server to automatically assign IP address.
IPv4/Netmask	Type the IP address and subnet mask, separated by a forward slash (/), such as 192.0.2.2/24 for an IPv4 address. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet. By default, the system enables HTTPS, HTTP, PING and SSH methods.
IPv6 Addressing mode	Specify whether FortiWeb Manager acquires an IPv6 address for this network interface manually or using DHCP to allow DHCP server to automatically assign IP address.
IPv6/Netmask	Type the IP address and subnet mask, separated by a forward slash (/), 2001:0db8:85a3:::8a2e:0370:7334/64 for an IPv6 address. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet. By default, the system enables HTTPS, HTTP, PING and SSH methods.
Description	Type a comment. The maximum length is 63 characters. Optional.



You can also configure the network interface through CLI: `Set interface <PORT> (ip|ip6) <IPADDRESS/LENGTH>`

5. Click **OK**.

Configuring routes

The Route options allow you to configure a gateway for FortiWeb Manager.

Routes direct traffic exiting FortiWeb Manager based on the packet's destination — you can specify through which network interface a packet leaves and the IP address of the 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. Your FortiWeb Manager 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 route that points to a router, often a router that is the gateway to the Internet. You can configure multiple static routes if you have multiple gateway routers (for example, each router receives packets destined for a different subset of IP addresses), redundant routers (for example, redundant Internet/ISP links), or other special routing cases.

However, in most cases, you configure only one route: a default route.

To add a route, go to **System Settings > Network > Route**, and then click **Create**

Setting name	Description
Destination IP/Mask (IPv4/IPv6)	Enter the destination IP address and network mask of packets that use this static route, separated by a slash (/). Enter 0.0.0.0/0.0.0.0, 0.0.0.0/0 or ::/0 to create a default route that matches the DST field in the IP header of all packets.
Gateway (IPv4/IPv6)	Enter the IP address of the next-hop router to which FortiWeb Manager forwards packets that match Destination IP/Mask (IPv4/IPv6). Ensure that this router knows how to route packets to the destination IP addresses or forward packets to another router with this information. For a direct Internet connection, this is the router that forwards traffic towards the Internet, and could belong to your ISP.
Interface	Select the network interface through which FortiWeb Manager routes the packets that match Destination IP/Mask (IPv4/IPv6) to the next-hop router.



You can also configure the route through CLI: `set route <DST/LENGTH> gw <GATEWAY> device <DEVICE>`

Configuring DNS

Like many other types of network devices, FortiWeb appliances require connectivity to DNS servers for DNS lookups.

Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Local host and broadcast addresses will not be accepted.

To configure DNS settings:

1. Go to **System Settings > Network > DNS**.
2. In **Primary DNS Server**, type the IP address of the primary DNS server.
3. In **Secondary DNS Server**, type the IP address of the secondary DNS server.

Setting up user accounts

You can create user accounts in **System Settings > Admin**, and associate different profiles to the user accounts, so that different users have different operation permissions (for example, read-only, read-and-write) to the features in FortiWeb Manager.

You can setting up LDAP and RADIUS servers to authenticate users with accounts stored on remote servers, rather than with accounts on the FortiWeb Manager itself.

If you want to use ports other than 443 to access FortiWeb Manager's GUI, you can change the port in **Admin Settings**.

Configuring profiles

Create a user account permission profile, so that you can assign permissions to an user account.

To create a profile:

1. Go to **System Settings > Admin > Profile**.
2. Click **Create**.
3. Enter a name for the profile.
4. Enter comments if any.
5. Select operation permission for each feature.

Configuring user accounts

Create user accounts to access FortiWeb Manager's GUI, API and CLI.

To create user accounts:

1. Go to **System Settings > Admin > Administrators**.
2. Click **Create**.
3. For the **Profile** parameter, select a profile you have created in **System Settings > Admin > Profile** to grant permissions for this account. For the **Admin Type** parameter, Select the type of authentication the administrator will use when logging into the FortiWeb Manager unit. See [Configuring Authentication Server](#) for more information.

Configuring authentication server

FortiWeb Manager supports multiple query types that you can use to authenticate users with accounts stored on remote servers, rather than with accounts on the FortiWeb Manager itself.

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiWeb Manager unit sends the administrator's credentials to the LDAP server for authentication. If the LDAP server

can authenticate the administrator, they are successfully authenticated with the FortiWeb Manager unit. If the LDAP server cannot authenticate the administrator, the FortiWeb Manager unit refuses the connection.

To add an LDAP server:

1. Go to **System Settings > Admin > Authentication Server**.
2. Select **Create > LDAP Server** from the toolbar. The **New LDAP Server** pane opens.
3. Configure the following settings, and then click **OK** to add the LDAP server.

Name	Enter a name to identify the LDAP server.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use <code>cn</code> . However, some servers use other common name identifiers such as <code>uid</code> .
Distinguished Name	The distinguished name is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Clicking the <i>query distinguished name</i> icon will query the LDAP server for the name and open the <i>LDAP Distinguished Name Query</i> window to display the results.
Bind Type	Select the type of binding for LDAP authentication: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> .
User DN	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the user DN.
Password	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the password.
filter	Specify the filter in the format <code>(objectclass=*)</code>
Secure Connection	Select to use a secure LDAP server connection for authentication.

RADIUS servers

Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they type a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

You can create or edit RADIUS server entries in the server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiWeb Manager unit uses the RADIUS server to verify the administrator password at log on. The password is not stored on the FortiWeb Manager unit.

To add a RADIUS server:

1. Go to **System Settings > Admin > Authentication Server**.
2. Select **Create > RADIUS Server** from the toolbar. The **New RADIUS Server** pane opens.
3. Configure the following settings, and then click **OK** to add the RADIUS server.

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.

Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Server Secret	Enter the RADIUS server secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.
Authentication Type	Select the authentication type the RADIUS server requires. If you select the default ANY , FortiWeb Manager tries all authentication types.

Configuring HTTPS ports

The default HTTPS port for accessing FortiWeb Manager's GUI is 443. If you want to use ports other than 443, you can change the port number in **System Settings > Admin > Admin Settings**.



If you change the port number here, you need to go to **Device Manager**, edit each of the devices, replace the old port number in the **Allow Origin** field with the new one.

You can also set the **Idle Timeout**. By default, the GUI disconnects administrative sessions if no activity occurs for 30 minutes. This prevents someone from using the GUI if the management computer is left unattended.

Setting the system time & date

You can either manually set the FortiWeb Manager system time or configure the FortiWeb Manager appliance to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

For many features to work, including scheduling, logging, and SSL/TLS-dependent features, the FortiWeb Manager system time must be accurate.

To configure the system time:

1. Go to **System Settings > Maintenance > Time Settings**. Alternatively, go to **System Settings > Status > Status**. In the **System Information** widget, in the **System Time** row, click **Update**.
2. For **Time Zone**, select the time zone where FortiWeb Manager is located.
3. If you want FortiWeb Manager to automatically synchronize its clock with an NTP server (recommended), configure these settings:

Synchronize with NTP Server	Select this option to automatically synchronize the date and time of the FortiWeb Manager appliance's clock with an NTP server, then configure the Server and Sync Interval before you click Apply . Note: NTP requires that FortiWeb Manager be able to connect to the Internet on UDP port 123.
Sync Interval	Enter how often in minutes the FortiWeb Manager appliance should

synchronize its time with the NTP server. For example, entering 1440 causes the FortiWeb Manager appliance to synchronize its time once a day.

Server

Type the IP address or domain name of an NTP server or pool, such as `pool.ntp.org`. IPv4 and IPv6 addresses are both supported here. To find a NTP server that you can use, go to <http://www.ntp.org>.

Otherwise, select **Set Time**, then manually set the current date and time. If you want FortiWeb Manager to automatically adjust its own clock when its time zone changes between daylight saving time (DST) and standard time, enable **Automatically adjust clock for daylight saving changes**. The clock will be initialized with the manually specified time when you click **OK**.

4. Click **OK**.

If you manually configured the time, or if you enabled NTP and the NTP query for the current time succeeds, the new clock time should appear for the **System Time** in the **System Information** widget. (If the query reply is slow, you may need to wait a couple of seconds, then click **Refresh** to update the display in **System time**.)

If the NTP query **fails**, the system clock will continue without adjustment. If FortiWeb Manager's time was 3 hours late, for example, the time will still be 3 hours late. Verify your DNS server IPs, your NTP server IP or name, routing, and that your firewalls or routers do not block or proxy UDP port 123.

Setting up notification method for job status

To receive notifications for the job status (successful or failed), you need to create notification method in **System Settings > Notifications**. When you create a job, you can select the notification method for the job. For more information on jobs, see [Jobs on page 23](#).

1. Go to **System Settings > Notifications > Notifications**.
2. Click **Create**. The New Notifications window will open.
3. Configure the following settings.

Name	Enter a name for this method.
Type	Select the notification type.
SMTP server	Type the fully qualified domain name (FQDN, e.g. <code>mail.example.com</code>) or IP address of the SMTP relay or server, such as a FortiMail appliance, that the FortiWeb Manager appliance uses to send alerts and generated reports. Caution: If you enter a domain name, you must also configure the FortiWeb Manager appliance with at least one DNS server. Failure to configure a DNS server may cause the FortiWeb Manager appliance to be unable to resolve the domain name, and therefore unable to send the alert. For details about configuring a DNS server, see Configuring DNS on page 10 .
Security Mode	Select one of the following options: • None—FortiWeb Manager applies no security protocol to email. • SSL/TLS—Encrypts the connection to the SMTP server using SSL/TLS. • STARTTLS—Encrypts the connection to the SMTP server using STARTTLS.

Port	Enter the port on the SMTP server that listens for alerts and the generated reports from FortiWeb Manager. The default port is 25.
Authentication	Enable if the SMTP relay requires authentication.
SMTP Username	Type the user name of the account on the SMTP relay that FortiWeb Manager uses to send alerts. This option is available only if Authentication is enabled.
SMTP Password	Type the password of the account on the SMTP relay that FortiWeb Manager uses to send alerts. This option is available only if Authentication is enabled.
Email From	Type the sender email address that the FortiWeb Manager appliance will use when sending alert email messages.
Email To	Type up to five recipient email addresses. Enter one per field.

Managing FortiWeb devices

Use the **Device Manager** pane to add, edit, and delete FortiWeb devices and device groups. Also you can update FortiWeb device status and information, upgrade device signature and firmware.

You can find all the managed FortiWeb devices here. Clicking the device name to check its configuration or synchronize the configurations of a device to other devices in the same group with GUI.

Also, on the right side of the page, you can view the device description and detailed variable information added for the device.



FortiWeb Manager does not support viewing or configuring ADOM related features of FortiWeb.



When you delete a group, all the devices in the group will be deleted.



For device information, the device status is updated automatically every 15 seconds.



FortiWeb Manager 7.4.0 supports managing FortiWeb 6.3.16, 6.3.17, 6.4.0, 6.4.1, and 6.4.2.

Adding device groups

With **Device Manager**, you can add a group, and then add devices to this group. These groups allow you to organize your devices in the navigation tree.

To add a device group:

1. Click **Add Group**. The **Add Group** dialog appears.
2. Configure these settings:

Name	Type the name of the device group that can be referenced by other parts.
Description	Optionally, enter a description for the group, such as its geographic location.

The variable added here is used in the command line of **Jobs > Config File Management** below:

```

Edit Command File
1  config vdom
2    edit root
3      config server-policy vserver
4        edit "Demo Vserver"
5          set vip {{ vip }}
6          set interface port1
7        next
8      end
9
10     #####Add Server pool
11     config server-policy server-pool
12       edit "Demo_ServerPool"
13         set flag 1
14         config pserver-list
15           edit 1
16             set ip {{ pserverip }}
17           next
18         end
19       next
20     end

```



Variables for a group will apply to all devices once the configuration is pushed. If the variable name for a group is the same as that of a device, the variable for the device shall be prioritized.

3. Click **OK**, and the newly added group can be found on the left pane below:

Adding devices

After you add a device group, you can add devices to this group.

To add a device:

1. Click **Add Device**.
2. Configure the following settings:

Name	Enter the device name.
Description	Enter a description for the device optionally (for example, a description of its physical location).
Group	Select a group for the device from the drop-down list.

IP Address	Enter the IP address that FortiWeb Manager can use to communicate with the device.
Username	Enter the administrator user name of the device.
Password	Enter the administrator user password.
Allow Origin	This field is automatically filled when a device is added. The default value is the URL that you access FortiWeb Manager, for example, https://10.200.111.100. Usually, this value does not need to be changed, while if you change the IP address, replace IP address with the domain name or use NAT, you need to amend this value manually. Otherwise, you can not log into FortiWeb Manager automatically. Also, if you change the HTTPS port from System Settings > Admin Settings , for example, you change the port from 443 to 8443, then the Allow Origin value shall include the port as https://10.200.111.100:8443.
HTTPS Port	The HTTPS port used to specify the FortiWeb device. If this port is changed from System > Admin > Settings of a FortiWeb device, you need to manually update the port for all the devices in Device Manager .
FDS Proxy	You can configure FortiWeb Manager to act as an FDS proxy so that FortiWeb devices in the network are able to connect to FortiGuard for license validation. Also, the devices in the network can update services from the FortiWeb Manager FDS proxy. When FDS Proxy is enabled, the option Override default FortiGuard address at System > Config > FortiGuard will be changed to FortiWeb Manager IP:8989 automatically, for example, 10.200.111.100:8989, 10.200.111.100 is the FortiWeb Manager IP address.



You are recommended to add devices with similar configurations to a same group.
The FortiWeb Manager and SSH options of the interface on the managed device must be enabled.



For the username, you are recommended to use admin user or the user available to all permissions of the device.

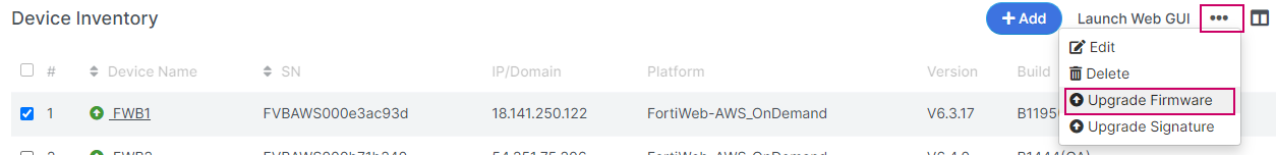
- Click **OK**, and a window pops up showing the progress of adding a device. Wait for around one minute until it is finished.
- After the device is added, you can see it in the device list of the group.
- To enter into the Web GUI of this device, click the device name, or check the box before the device name, then click **Launch Web GUI**.
- To export the CLI config file of this device, check the box before the device name, then click **Export CLI Template**.
- To add variables, click the device name, then click the Edit icon beside the "Variable List" at the right side frame.

Upgrading devices

With **Device Upgrade** button, you can upgrade firmware and signature of managed devices.

To upgrade the firmware:

1. Select at least one device.
2. Click **Device Upgrade > Upgrade Firmware**.



3. Choose FortiWeb firmware related image files, and click **Upload**.
If the image files are uploaded successfully, you can see the green icon ; otherwise, a red icon is shown.
4. Once the files are successfully uploaded, click **Upgrade**. You may see the upgrading progress page and upgrade details (the upgrade succeeds or fails).



You can also upgrade the device firmware from **System Settings > FortiWeb Upgrade > Firmware Upgrade**.

To upgrade the signature:

1. Select at least one device.
2. Click **Device Upgrade > Signature Upgrade**.
3. Choose the signature file, and click **Upload**.
If the image files are uploaded successfully, you can see the green icon ; otherwise, a red icon is shown .
4. Once the files are successfully uploaded, click **Upgrade**. You may see the upgrading progress page and upgrade details (the upgrade succeeds or fails).



You can also upgrade the device signature from **System Settings > FortiWeb Upgrade > Signature Upgrade**.

Managing FortiWeb-VM licenses

The license feature provides you with an easy way to manage your FortiWeb-VM licenses. You can import all your FortiWeb-VM licenses to FortiWeb Manager, apply them to FortiWeb-VMs, or reclaim them from FortiWeb-VMs. You can also view the information of all your licenses, such as the license status, the CPU number, and the expiration time.

The following table describes the action buttons in **License**.

Import	Import licenses to FortiWeb Manager.
Delete	Delete licenses from FortiWeb Manager.
Apply	Apply licenses to FortiWeb-VMs. The system automatically chooses any available licenses and apply them to the FortiWeb-VMs you have selected.
Reclaim	Reclaim licenses from FortiWeb-VMs.

The following information of a license is displayed in the license table. You can choose which information you want to view in this table by using the **Column Settings** filter.

#	The identifier of the license.
License	The serial number of the license. The first two digits after FVVM indicate the CPU number supported by this license. For example, if the serial number is FVVM02xxxxxx. 02 means this license supports 2 CPUs.
Status	The license can be in the following four status: • Available: The license are available to use. When you click the Apply button and select the FortiWeb-VMs, the system will choose from the available licenses and apply them to FortiWeb-VMs. • In use: The license is applied to a FortiWeb-VM. • Locked: After you reclaim license from FortiWeb-VM, the license will be in Locked status for two hours, then turn into Available status. • Expired: The license is expired. It cannot be applied to FortiWeb-VM anymore.
Device Name	The name of the FortiWeb-VM to which this license is applied.
IP Address	The IP Address of the FortiWeb-VM.
Import Time	The time when you imported this license to FortiWeb Manager.
Expiration Time	The expiration date of the license. The system can get the expiration information only after the license is applied to a FortiWeb-VM.

Applying license to FortiWeb-VM

You can apply multiple licenses to different FortiWeb-VMs at a time. The system automatically chooses any available licenses and apply them to the FortiWeb-VMs you have selected.

Before applying license to FortiWeb-VM, you must have already completed the Route and DNS configurations for the FortiWeb-VM.

To apply license to FortiWeb-VM:

1. If you have already imported your licenses, skip this step. If not, click the **Import** button to import licenses from your local directory to FortiWeb Manager. Repeat this step if you want to import multiple licenses.
2. Click the **Apply** button. The **Apply License** page will be opened.
3. Click the **Add** button  beside **Device**. The **Select Entries** window appears at the right side of the page.
4. Select the devices to which you want to apply licenses. You can select multiple devices.
Please note that the physical machines are also displayed in this window, but you cannot apply licenses to them. Licenses are only used on FortiWeb-VMs.
5. Click the **Apply** button at the bottom of the page.

The system will apply the available licenses to the selected devices.

The Apply operation may fail under the following situations:

- There isn't any available license.
- The devices you selected outnumber the available licenses. In this case, the system will apply the licenses to device list from the top to the bottom until the licenses are used out, and then report an error message listing the devices that are not applied with licenses.
- The device already has a valid license. In this case, the system will not apply new license to this device.

Reclaiming license from FortiWeb-VM

You can reclaim license from FortiWeb-VMs. Once reclaimed, the license is in locked status and will be available until two hours.

To reclaim license from FortiWeb-VMs:

1. Click the **Reclaim** button. The **Reclaim License** page will be opened.
2. Click the **Add** button  beside **Device**. The **Select Entries** window appears at the right side of the page.
3. Select the devices from which you want to reclaim licenses. You can select multiple devices.
4. Click the **Reclaim** button at the bottom of the page.

Deleting licenses

You can delete licenses from FortiWeb Manager. If the license is valid, it will still be valid even you delete it from FortiWeb Manager. You can import it again, so that the system can use it when it applies license to FortiWeb-VM.

To delete license:

1. Select the checkbox in the license row. You can select multiple checkboxes at a time.
2. Click the **Delete** button to delete the license(s) you have selected.

Jobs

The **Jobs** feature is specially designed for Internet Service Providers (ISPs) and Managed Security Service Providers (MSSPs). With this feature, administrators can manage FortiWeb device related jobs in batch with specific scripts provided to realize automated management, operation and maintenance.

#	Name	Devices	Description	Plugin	Plugin Option	Activity	Action
1	ygeng-test-backup	FWB1		backup-config-for-fortiweb		✓	
2	ygeng-test-restore	FWB1		restore-config-for-fortiweb			

The **Jobs** pane includes the following tabs in the blue banner:

Jobs	Manage job tasks. You can create, edit, clone, and delete jobs.
Workflow Jobs	Manage job workflows. The added jobs can form the workflow according to expected execution conditions, which allows the administrators to maintain FortiWeb tasks in automated way.
Job Events	Show the execution results of the jobs.
Workflow Events	Show the execution results of the job workflows.
Config File Management	Store the CLI config files of FortiWeb devices, and configure the command files.
Plugins	Display all the plugins and their descriptions.

Managing jobs

Use the **Jobs** pane to create, edit, clone, delete, and view related jobs.

The **Jobs** pane includes the following functions:

Add	Create new jobs per specific devices.
Edit	Edit the selected job.
Clone	Clone the selected job.
Delete	Delete the selected job(s).
Column Settings	Click to select the columns to display or click Reset to Default to display the default columns: Name, Devices, Description, Plugin, Plugin Option, Activity, and Action.

It displays the following job information:

Name	The name of the job.
-------------	----------------------

Devices	The devices to be managed.
Description	The description of the job, optional.
Plugin	The plugin selected for the job.
Plugin Option	The configurations of plugins such as config files and command lines.
Activity	The activities of latest five times. At most five icons are displayed here with three status, Successful  , Failed  , and Cancel  .
Action	Launch  : Manually launch the job. Create Schedule for this job  : Schedule to launch the job.



For settings specially for "install-config-using-restfulapi", "push-command-file-to-fortiweb", and "push-command-to-fortiweb", see [Plugins on page 35](#) for details.

Creating jobs

Follow steps below to create a job:

1. Click **Add**.
2. Configure the following settings:

Name	Enter a job name that can be referenced by other parts of the configuration.
Description	Enter a description for the job. Optional.
Device	Click  to select one or more devices, or a device group.
Notification	Enable this option and click Add Notifications to choose a notification method. Currently, only the method email is supported. You can enable Success or Failure to determine the condition to send the notifications. Click the selected notification method to navigate to Edit Notifications page.
Plugin	Click  to select one of the eight plugins from the right list. See Plugins on page 35 for specific settings of each plugin.
Plugin Option	The parameter descriptions of plugins.

3. Click **OK**.
4. Click  to manually launch the job.
5. Or click  to create a schedule for the job.

Schedule

Enable ☒

Start Date

2018-09-11

8

:

14

:

0

Repeat Frequency

Hour

Local Time Zone

(GMT+08:00)Beijing,ChongQing,Hongk

Frequency Details

*Every

1

Hour

*End

After

*Occurrence(s)

1

Occurrences (Limited to first 5)

Date Format

☐ Local Time
 ☒ UTC

2018-09-11 00:14:00 UTC

OK

Cancel

Viewing job events

Once you launch or schedule the job, it goes to **Job Events** pane automatically.

You can view the execution results from **Job Events**. Also, you can delete one or more job events from the event list with the **Delete** button.

The tab includes the following information:

Name	The name of the job.
Type	The type that the job is executed, Scheduled, Manual, Relaunch, and Workflow.
Devices	The name of the device to be managed.
Finished	The time when the job finishes executing.
Action	Click  to view the job event details. Click  to relaunch the job.

In the example below, the job is launched successfully.

The screenshot displays the 'Summary' tab for a job event named 'FWB1'. The job status is 'Successful', completed on 2022-01-26 at 15:35:37. The job name is 'ygeng-serverPolicy' and the type is 'Workflow'. The job was launched by 'Workflow'. The 'Plugin' is 'push-command-to-fortiweb', with options 'Force' and 'Push Type' set to 'Config'. The 'Command Input' and 'Command Output' sections show the configuration commands and their execution results.

Summary

Status	Successful	Plugin	push-command-to-fortiweb
Started	2022-01-26 15:35:37	Plugin Option	-
Finished	2022-01-26 15:35:40	Force	-
Job Name	ygeng-serverPolicy	Push Type	add
Job Type	Workflow	Config	config server-policy policy edit ygeng-serverPolicy set ssl enable set vserver ygeng-vserver set service HTTP set web-protection-profile ygeng-protectionProfile set replacemsg Predefined set server-pool ygeng-serverpool set allow-hosts ygeng-allowHosts set https-service HTTPS config http-content-routing-list end set tlog enable next end
Launched By			

Command Input

```

1 config server-policy policy
2 edit ygeng-serverPolicy
3 set ssl enable
4 set vserver ygeng-vserver
5 set service HTTP
6 set web-protection-profile ygeng-protectionProfile
7 set replacemsg Predefined
8 set server-pool ygeng-serverpool
9 set allow-hosts ygeng-allowHosts
10 set https-service HTTPS
11 config http-content-routing-list
12 end
13 set tlog enable
14 next
15 end

```

Command Output

```

1 FortiWeb (policy) #
2 FortiWeb (ygeng-serverPo-i) #
3 FortiWeb (ygeng-serverPo-i) #
4 FortiWeb (ygeng-serverPo-i) #
5 FortiWeb (ygeng-serverPo-i) #
6 FortiWeb (ygeng-serverPo-i) #
7 FortiWeb (ygeng-serverPo-i) #
8 FortiWeb (ygeng-serverPo-i) #
9 FortiWeb (ygeng-serverPo-i) #
10 FortiWeb (ygeng-serverPo-i) #
11 FortiWeb (http-content-r-u) #
12 FortiWeb (ygeng-serverPo-i) #
13 FortiWeb (ygeng-serverPo-i) #
14 FortiWeb (policy) #
15 FortiWeb #

```

You can relaunch, cancel, or delete the job event with the buttons on the top right.

The screenshot displays the 'Summary' tab for a job event named 'FWB10'. The job status is 'Running', started on 2019-01-04 at 17:28:58. The job name is 'job_install' and the type is 'Manual'. The job was launched by 'admin'. The 'Plugin' is 'install-config-using-restfulapi', with options 'URL' and 'Data' set to 'POST'. The 'Method' is 'POST'. The 'Command Input' and 'Command Output' sections show the configuration commands and their execution results.

Summary

Status	Running	Plugin	install-config-using-restfulapi
Started	2019-01-04 17:28:58	Plugin Option	api/v1.0/cli-direct-view
Finished	-	URL	{ "path": "router/static", "action": "set_table", "data": { "dst": "101.100.0.0/16", "gateway": "10.200.0.1", "device": "port1", "id": "3" } }
Job Name	job_install	Data	POST
Job Type	Manual	Method	POST
Launched By	admin		



The  icon is only available when the job status is Pending, Waiting , and Running.

The screenshot displays the 'Summary' tab for a job event named 'FWB114'. The job status is 'Successful', completed on 2019-01-04 at 17:24:40. The job name is 'job_pushcommand' and the type is 'Manual'. The job was launched by 'admin'. The 'Plugin' is 'push-command-to-fortiweb', with options 'Force' and 'Push Type' set to 'Config'. The 'Command Input' and 'Command Output' sections show the configuration commands and their execution results.

Summary

Status	Successful	Plugin	push-command-to-fortiweb
Started	2019-01-04 17:24:40	Plugin Option	-
Finished	2019-01-04 17:24:43	Force	-
Job Name	job_pushcommand	Push Type	add
Job Type	Manual	Config	config vdom edit root set replacemsg Predefined
Launched By	admin		



The  icon is only available when the job status is Successful, Failed, and Error.



FortiWeb Manager does not save the logs to local disk, but obtains them in real time from FortiWeb by the RESTful API.



You can schedule automatic deletion of job events from **System Settings > Advanced > File Management**. Check the box for job events, and set the time periods and deletion time accordingly.

Managing workflow jobs

This feature allows you to group multiple jobs according to certain logic to perform a series of logical and complex tasks.

Use the **Workflow Jobs** pane to create, edit, clone, delete, and view related workflow jobs.

The **Workflow Jobs** pane includes the following tabs:

Create Workflow Job	Create new workflow jobs per specific jobs.
Edit	Edit the selected workflow job.
Clone	Clone the selected workflow job.
Delete	Delete the selected workflow job(s).
Column Settings	Click to select the columns to display or click Reset to Default to display the default columns: Name, Related Jobs, Description, Activity, and Action.

The pane includes the following job information:

Name	The name of the workflow job.
Related Jobs	The jobs included in the workflow.
Description	The description of the workflow job.
Activity	The operation activities of latest five times. At most five icons are displayed here with three status, Successful  , Failed  , and Cancel  .
Action	Launch  : Manually launch the workflow job. Create Schedule for this job  : Schedule to launch the workflow job.

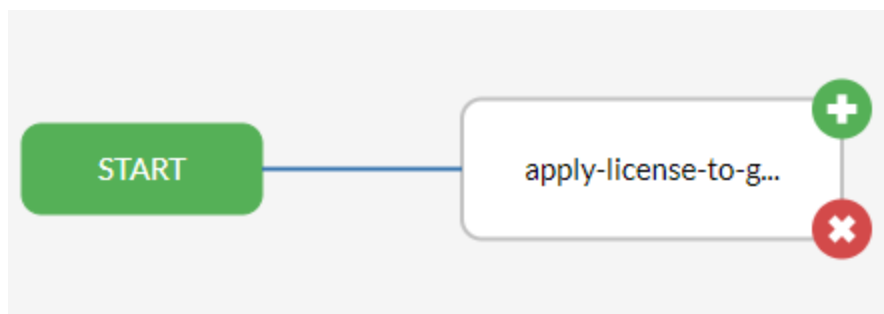
Creating workflow jobs

Follow steps below to create a workflow job:

1. Click **Add**.
2. Configure the following settings:

Name	Enter a workflow job name.
Description	Enter a description for the job, optional.
Notification	Enable this option and click the button to choose a notification method. Currently, only the method email is supported.

3. Click **START**.
4. Select a job from the right list, and click **Select**.
5. Hover over the selected job, and click the  icon.



You can also delete the selected job and re-select one.

6. Select a second job from the right list.
7. Select a condition for the job, and click **Select**.



The next job to be executed depends on the execution results (Success, Failure, Always) of last job. You can define the jobs to be selected according to actual needs.

- Click **OK** once the setting is finished.
- Click  to manually launch the workflow job as below.

2494 - workflow1

Details

Status

2018-09-11 22:52:57

2018-09-11 22:53:23

Workflow Job Name

workflow1

Job Type

Manual

Launched By

admin

workflow1

TOTAL JOBS 3 ELAPSED 00:00:26

Type: Success Failure Always

START

backup-config-for-00:00:05

push-command-to-fs-00:00:14

restore-config-for-00:00:06

You can relaunch, cancel, or delete the workflow event with the buttons on the top right.

Details		 
Status	 Running	
Started	2018-09-11 23:04:59	
Finished	-	
Workflow Job Name	workflow1	
Job Type	Relaunch	
Launched By	admin	



The  icon is only available when the job status is Pending, Waiting , and Running.

Details		 
Status	 Successful	
Started	2018-09-11 23:04:59	
Finished	2018-09-11 23:05:23	
Workflow Job Name	workflow1	
Job Type	Relaunch	
Launched By	admin	



The  icon is only available when the job status is Successful, Failed, and Error.

10. Or click  to create a schedule for the workflow job.

Schedule

Enable

☒

Start Date

2018-09-12

1

:

0

:

0

Repeat Frequency

Day

Local Time Zone

(GMT+08:00)Beijing,ChongQing,Hongk

Frequency Details

*Every

1

Day

*End

After

*Occurrence(s)

2

Occurrences (Limited to first 5)

Date Format

☒ Local Time

☐ UTC

2018-09-12 01:00:00 HKT

2018-09-13 01:00:00 HKT

OK

Cancel

Once you launch or schedule the workflow, it goes to **Workflow Events** pane automatically.

Viewing workflow events

After you launch a workflow job or create schedule for a workflow job, you can view the execution results from **Workflow Events**.

The tab includes the following information:

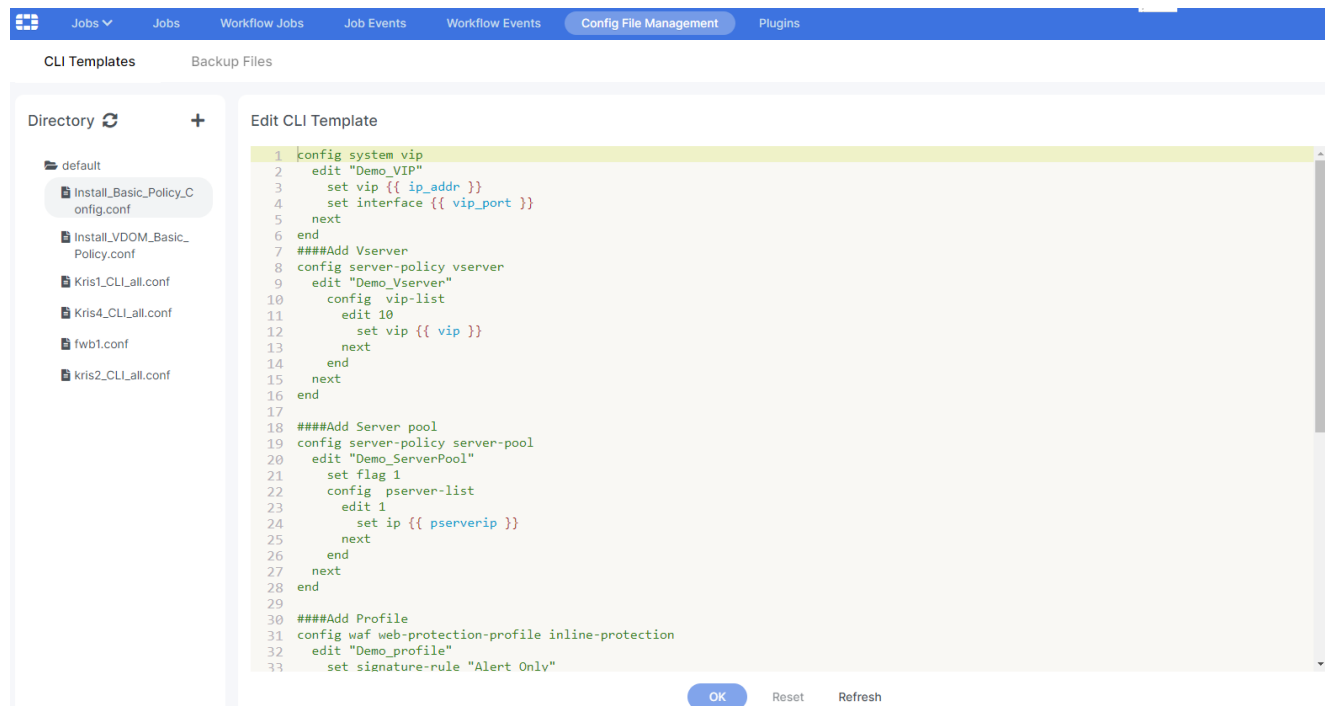
Name	The name of the workflow.
Type	The type that the workflow job is executed, Scheduled, Manual, Relaunch.
Finished	The time when the workflow finishes executing.
Action	Click  to view the workflow event details. Click  to relaunch the workflow. Click  to delete the workflow event.

Managing config files

This pane stores the command files and backup files of FortiWeb devices.

Managing command files

This tab stores the config files that can be called by the plugin push-command-file-to-fortiweb. Two command file templates are provided here, and you can create new command files with the templates and store them in the default or newly created directory. After the command file is created, you can push the config to certain device.

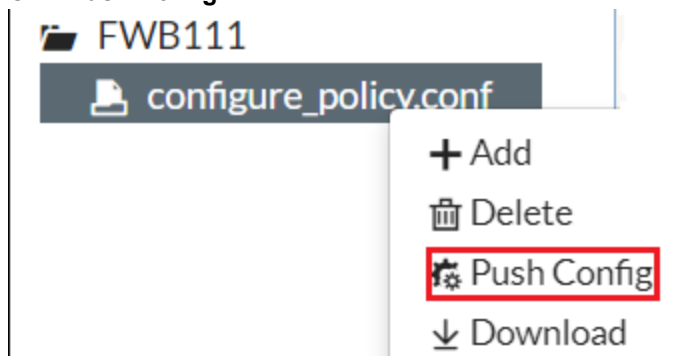


To create a new directory:

1. Click the  icon.
2. Input a directory name, for example, FWB111.
3. Click **OK**, and you can see the new directory in the left pane.

To create a new command file:

1. Right click the directory name **FWB111**.
2. Click **Add**.
You can click **Delete** to remove a directory.
3. Input a command file name, for example, configure_policy.
4. Click **OK**, and you can see the new command file.
5. Edit the command file in **Edit Command File** section. You can also refer to the template file and make updates accordingly.
6. Click **OK** to finish the command file.
7. Right click the command file name.

8. Click **Push Config**.

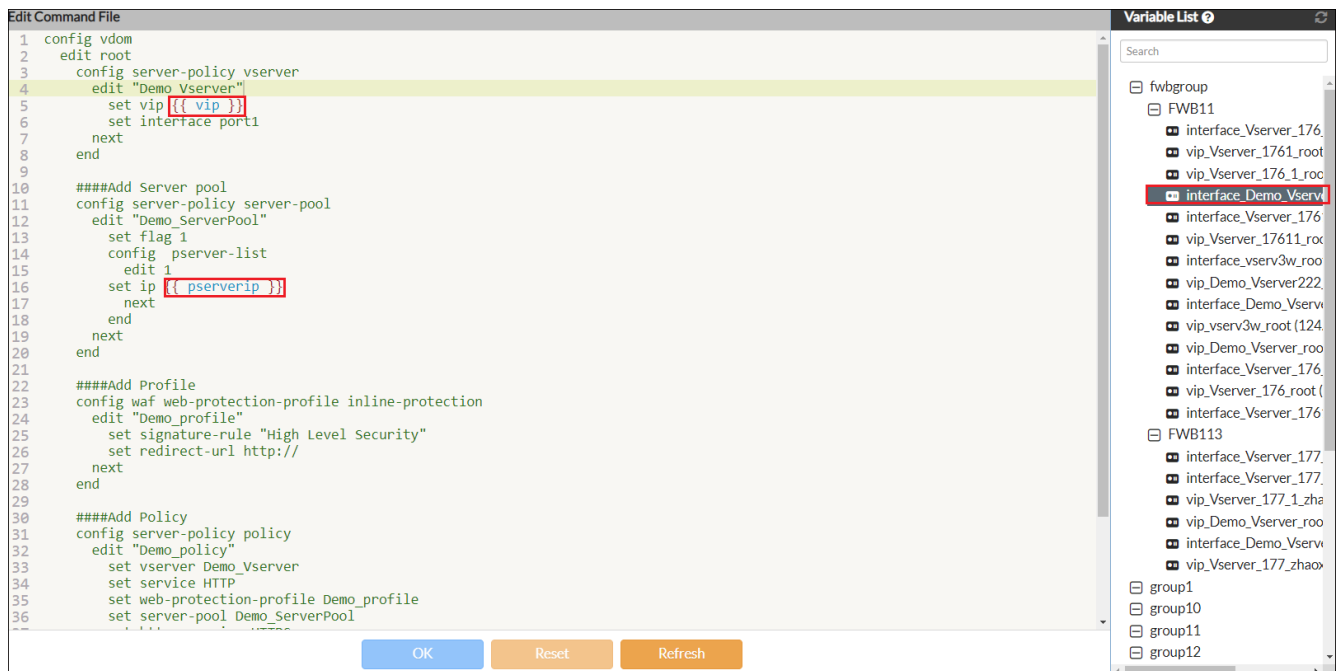
Also, you can click **Add** to add a new command file, or click **Delete** and **Download** to delete or download a command file.

9. Configure the push settings below.

Name	A default name is available here.
Description	Enter a description for the operation.
Device	Select a device for this push.
Plugin	A default plugin name.
Plugin Option	The parameter descriptions of plugins.
Force	Enable this option to execute the config file by force or not.
Push Type	Only one type is available currently.
Config File	A default config file is included here, or you can select one file from the right list.

10. Click **Launch** to push the configuration to the device, and this goes to **Job Events** pane.

In addition, a variable list for devices or device groups is displayed on the right side of the page. Choose the variable in **Edit Command File** section, double click the variable on the right, and the variables (highlighted in red) in the command file are updated.



Managing backup files

This tab stores the config files that are generated by backup-config-for-fortiweb related jobs and can be called by restore-config-for-fortiweb to restore the configurations of related FortiWeb devices.

Jobs ▾ Jobs Workflow Jobs Job Events Workflow Events **Config File Management** Plugins

CLI Templates Backup Files

Directory ↻ +

- FWB1
 - 1_20220124_151441.conf
- kris1
 - 1_20220124_202536.conf

Edit Backup File

```

1 [header]
2 magic=CC05E358
3 version=1.4
4 image_version=FVAWS1-6.317-FW-build1195-211130
5 model=FVAWS1
6 type=cli_config
7 file_number=2
8 file_split=-----FVAWS1-6.317-FW-build1195-211130-----2022-01-24 15:14:41-----FF4A517EFF7B78FFFF12-
9 [/header]
10 [file]
11 name=/data/config/sys_global.conf.gz
12 domain=global
13 type=config
14 encrypt=no
15 compress=no
16 -----FVAWS1-6.317-FW-build1195-211130-----2022-01-24 15:14:41-----FF4A517EFF7B78FFFF12-----
17 #config-version=FVAWS1-6.317-FW-build1195-211130:opmode=0:vdom=0
18 #conf_file_ver=0
19 config system encryption-method
20 end
21 config system hsm partition
22 end
23 config system admin-certificate local
24 end
25 config system global
26   set admintimeout 480
27   set https-certificate defaulthttpscert
28 end
29 config system accprofile
30 end
31 config system dashboard
32 end
33
            
```

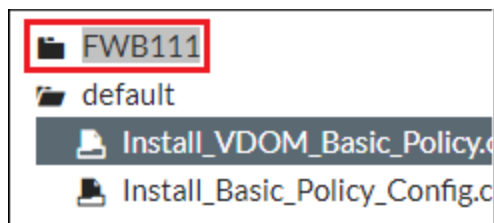
OK Reset Refresh



You can schedule automatic deletion of backup files from **System Settings > File Management**. Check the box for backup config, and set the time periods and deletion time accordingly.

To create a new directory:

1. Click the  icon.
2. Input a directory name, for example, FWB111.
3. Click **OK**, and you can see the new directory.



To create a new backup file:

1. Right click the directory name.
2. Click **Add**.
You can click **Delete** to remove a directory, or click **Download** to fetch the backup file.

3. Input a backup file name. Check the highest sequence number from the backup file list, for example, 1178_20180912_044109_UTC.conf, then use 1179, followed by the date when the file is created to name the file.
4. Click **OK**, and you can see the new backup file.
5. Edit the backup file in **Edit Command File** section.
6. Click **OK** to finish the backup file.

Plugins

For each job, one plugin shall be appointed. Currently, the following plugins are provided, and more will be supported per users' need.

- **backup-config-for-fortiweb**
Backup the config file generated from configuring FortiWeb device. You can find the config file from **Jobs > Config File Management > Backup Files**. The config file is named by sequence number and the time when the file is generated.
- **restore-config-for-fortiweb**
Restore the configurations of FortiWeb device. Find the config file with the highest sequence number and push it to FortiWeb device to restore the configuration.
- **apply-license-to-fortiweb**
Apply the license to FortiWeb device. Randomly select a license with "Available" status from the license pool uploaded to FortiWeb Manager and apply it to FortiWeb device.

URL	The URL of the FortiWeb device.
Data	The API data.
Method	Only POST is supported currently.

- **reclaim-license**
Reclaim the license used for FortiWeb device. Reclaim the license used for one FortiWeb device.
- **push-command-file-to-fortiweb**
Push the command file to FortiWeb device and apply it to the device. You need to prepare the CLI file of the device and upload it to FortiWeb Manager in advance. If the CLI file is exported by FortiWeb Manager with a template header, FortiWeb Manager will check its version before pushing it to devices. Configure the following settings specially for this plugin.

Enforce	Enable this option to always push commands to devices regardless of errors and CLI template versions.
Push Type	Only one type is available currently.
Config File	Select the config file from the right list.

- **push-command-to-fortiweb**
Push single command to FortiWeb device and apply it to the device. Configure the following settings specially for this plugin.

Enforce	Enable this option to always push commands to devices regardless of errors and CLI template versions.
----------------	---

Push Type	Only one type is available currently.
Config	Fill in the detailed command here.
Auto Update	With this option checked, FortiWeb Manager will automatically connect to AWS/Azure to obtain the latest member information in autoscaling group.

FortiWeb CLI commands

FortiWeb Manager supports exporting the following FortiWeb CLI commands.

System

```
config system global
config system dashboard
config system password-policy
config system settings
config system vip
config system feature-visibility
config system replacemsg
config system replacemsg-image
config system replacemsg-admin
config system credential-stuffing-online-check
config system csf
config system saml
config system sdn-connector
config system sso-admin
```

User

```
config user ldap-user
config user radius-user
config user tacacs+-user
config user local-user
config user ntlm-user
config user kerberos-user
config user saml-user
config user user-group
config user oauth-user request
config user oauth-user server
config user recaptcha-user
```

WAF

```
config waf allow-method-exceptions
config waf allow-method-policy
config waf allowed-origins
config waf api-policy
```

```
config waf api-rules
config waf api-user-group
config waf api-users
config waf application-layer-dos-prevention
config waf base-signature-disable
config waf biometrics-based-detection
config waf bot-deception
config waf bot-detection-policy
config waf bot-mitigate-policy
config waf cookie-security
config waf cors-protection-policy
config waf cors-protection-rule
config waf csrf-protection
config waf custom-protection-group
config waf custom-protection-rule
config waf exclude-url
config waf fds-update-flag
config waf file-compress-rule
config waf file-upload-restriction-policy
config waf file-upload-restriction-rule
config waf ftp-command-restriction-rule
config waf ftp-file-security
config waf ftp-protection-profile
config waf geo-ip-except
config waf hidden-fields-protection
config waf hidden-fields-rule
config waf http-authen
config waf http-connection-flood-check-rule
config waf http-constraints-exceptions
config waf http-header-security
config waf http-protocol-parameter-restriction
config waf http-request-flood-prevention-rule
config waf input-rule
config waf ip-intelligence
config waf ip-intelligence-exception
config waf ip-list
config waf json-schema
config waf json-validation
config waf known-bots
config waf layer4-access-limit-rule
config waf layer4-connection-flood-check-rule
config waf machine-learning
config waf machine-learning-policy
config waf mitb-policy
config waf mitb-rule
config waf mobile-api-protection
config waf openapi-file
config waf openapi-validation-policy
config waf padding-oracle
config waf parameter-validation-rule
config waf signature
config waf signature_update_policy
config waf site-publish-helper
config waf staged_signature_list
config waf syntax-based-attack-detection
config waf threshold-based-detection
config waf url-access
```

```
config waf url-encryption
config waf url-rewrite
config waf user-tracking
config waf web-cache-policy
config waf web-cache-rule
config waf web-protection-profile
config waf websocket-security
config waf ws-security
config waf x-forwarded-for
config waf xml-exempted-urls
config waf xml-schema
config waf xml-validation
config waf xml-wsdl
config waf api-learning-policy
config waf api-learning-rule
config waf bot-mitigation-exception
config waf http-header-security-exception
config waf webshell-detection-policy
```

Server Policy

```
config server-policy setting
config server-policy service custom
config server-policy service predefined
config server-policy pattern custom-data-type
config server-policy health
config server-policy vserver
config server-policy pattern predefined-global-white-list-group
config server-policy pattern threat-weight
config server-policy allow-hosts
config server-policy acceleration exception
config server-policy acceleration policy
config server-policy persistence-policy
config server-policy server-pool
config server-policy http-content-routing-policy
config server-policy traffic-mirror
config server-policy policy
```

Monitoring FortiWeb devices

When you create a device group in **Device Manager**, the system will automatically create a dashboard for this group in **Monitor**. The dashboard displays the threat statistics for the group and each device. It also displays other information for individual devices, including the up/down **State**, the **Memory/CPU** usage, **Traffic In/Out**, **TCP Connections**, and **Threats**.

As shown in the following graph, the dashboard contains five parts:

1. The Dashboard Selector. You can click the arrow icon to open a drop down list, from which you can select the dashboard you want to view. The dashboard created by the system has the same name with the device group.
2. The display area of threat statistics for the device group. In this area, you can view the statistic graphs for the group, including **Threats Classified by Type**, **Threats Classified by Country**, and **Group Threats**. You can click the arrow icon beside **Group Threats** to collapse the graphs.
3. The tool bar of the dashboard. It contains the **Zoom out** tool, the **Time Range Selector**, the **Save** button, and the **Refresh** button.
 - The **Zoom out** tool . Use it to display the statistics for a longer period in the graph. For example, if the current time range is Last 15 minutes and you click the Zoom out button once, the time range displayed in the graph will change to Last 30 minutes.
 - The **Time Range Selector**. You can select a preset quick range or customize the time range by specifying the beginning and end time, select the refreshing time interval, then click **Apply**. The dashboard will show statistics for the selected time period and refresh the statistics as specified.
 - The **Save** button . When you make changes to the current dashboard, for example, zoom out or change the time range, adjust the position of the graphs, please remember to click the **Save** button, otherwise your changes will be lost when you switch to another dashboard.
 - The **Refresh** button. Click the **Refresh** button to refresh the statistics in real time.
4. The Dashboard & Widget tool.
For the dashboards created by the system, you can edit, and reset them.

You can create your own dashboard by clicking the **Add Dashboard** button; for the self-created dashboards, you can delete the dashboards, or customize the forms of the widgets. See [Managing dashboard](#) for more information.

For the widgets (graphs), you can add, edit, or delete them or adjust the position of the widgets.

With the Global Setting button, you can configure the data collection interval and data retention days.

5. The display area of statistics for individual devices. In this area, you can view the statistic graphs for individual devices, including the up/down **State**, the **Memory/CPU** usage, **Traffic In/Out**, **TCP Connections**, and **Threats**.

Managing dashboard

By creating your own dashboard, you can customize the dashboard such as displaying statistics for devices from different groups, or reclassifying the categories of the graphs.

To create a dashboard:

1. Move the mouse to the bottom right corner of any dashboard page in **Monitor**, click  .
2. Click **Add Dashboard**. The **Add Dashboard** window is opened.
3. Enter a name for the Dashboard.
4. Click **OK**.

To create a statistic graph in a dashboard:

1. Select the dashboard in the drop down list of the Dashboard Selector to open the dashboard page.
2. Move the mouse to the bottom right corner of the page, click  .
3. Click **Add Widget**. The **Add Dashboard Widget** window is opened.
4. Select a widget type as you desire from the **System**, **Resource Usage**, and **Threats**. Do not select **Row** if you want to create a statistic graph. For more information on the usage of Row, see [To categorize the widgets](#).
5. Enter the title of the widget. If you plan to add widgets for more than one device in this dashboard, it's recommended to reflect the device name in the title, so that it will be easy to distinguish the statistic graphs for different devices.
6. Select the device for which you want to show the statistic graph.
7. Click **OK**.
8. The widget is displayed on the dashboard page. To adjust the position of the widget, click its title, then drag-and-drop to the desired position.

To categorize the widgets:

1. Select the dashboard in the drop down list of the Dashboard Selector to open the dashboard page.
2. Move the mouse to the bottom right corner of of the page, click  .
3. Click **Add Widget**. The **Add Dashboard Widget** window is opened.
4. Select the **Row**.
5. Enter the title of the row. For example, if you want to categorize multiple widgets into a group, you can name the group in this field.
6. Click **OK**.
7. On the dashboard page, find the row you have created, then drag-and-drop widgets under this row. You can click the arrow icon before the row title to collapse the widgets under it.

Viewing logs

Log View allows you to view all the logs of managed FortiWeb devices. You can filter the logs with **Add Filter** icon or view logs by log type, device or device group, or by the period.



FortiWeb Manager does not save the logs to local disk, but obtains them in real time from FortiWeb by the RESTful API.

The following buttons are available for log filtering and view resetting.

Add Filter	This button allows you to filter the logs by certain categories.
Column Settings	Click to select the columns to display or click Reset to Default to display the default columns.
Log Type	Three types of logs are supported to view here: Attack Logs, Traffic Logs, and Event Logs. See also Viewing logs on page 41 .
Devices	With All Devices button, you can view logs by Groups or Devices.
Time Period	You can select the period to view logs generated in certain time periods; For example, Last 5 Minutes, Last 1 Hour, and Last 1 Day. Also, you can define the period by adding N: value with Last N minutes, Last N Hours, and Last N Days. The maximum value of N is 999.
Reset	Reset allows you to reset all the log query conditions. Filter settings, log type, device or device group, and time periods will all be reset if you click Reset .

Filtering logs

Click the **Add Filter** icon to filter the logs. Here, you can select available categories from the drop-down menu or enter the specific category that you want to filter. Also, you can filter for a combination of these categories.

The categories available depend on the log type you select.

Log types

FortiWeb Manager provides three types of logs. You can select the log type to view related logs.

- Attack Logs
- Traffic Logs
- Event Logs

Attack logs

Attack logs record attacks or intrusion attempts against the web servers protected by the FortiWeb appliance. This pane includes the following information:

Date/Time	The date/time when the log is generated.
Device Name	The name of the managed device.
Threat Level	The level of the threat.
Action	The actions that FortiWeb has taken.
Source	The source IP address of the client where the attack comes from.
Destination	The destination IP address where the attack happens.
HTTP Host	The HTTP host name.
Method	The HTTP method used, such as GET, POST, PUT, and DELETE, etc.
Main Type	The signature detection category.
Sub Type	The specific type of signature in the category.

Click any log item, and you can see the **Log Details** page.

Log Details ✕	
Date	2019-01-11
Time	18:19:25
Log ID	20000003
MSG ID	000001503916
Type	attack
Device Name	FWB-24
Time Zone	(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi
Protocol	tcp
Service	https/tls1.2
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
HTTP Version	1.x
Action	Alert_Deny
Policy	http_server_policy1
Method	get
URL	/
HTTP Host	10.200.111.24:8888
FortiWeb Session ID	none
Severity Level	Medium
Signature Subclass Type	N/A
Signature ID	N/A
Source Country	Reserved
HTTP Content Routing	none
Server Pool	http_server_pool_rp_1
Username	Unknown
Monitor Mode	Enabled
HTTP Referer	none
Client Device ID	none
Main Type	Page Access
Sub Type	N/A
Machine Learning Domain Index	0
Machine Learning URL ID	0
Machine Learning ARG ID	0
Threat Level	Medium
Threat Weight	9
Historical Threat Weight	0
User Agent	curl/7.55.1
Message	Page Access Rule Violation
Connection	
10.200.111.102:39584 -> 10.0.0.22:443	

When the Main Type is **Signature Detection**, two additional buttons appear on the **Log Details** page.

Viewing logs

#	Date/Time	Device Name	Threat Level	Action	Source	Destination	HTTP Host	Method	Main Type	Sub Type	Log Details
1	01-13-22:26:50	2-J-085441cf0eb83761	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error	Signature View Add Exception Date2019-01-13 Time22:15:54 Log ID20000008 MSG ID00000027227 Typeattack Device Name2-J-0bb48f7465d40bf0 Time Zone(GMT-8:00) Pacific Time(US&Canada) Protocoltcp Servicehttp Cipher Suitenone HTTP Version1.x ActionErase Policypolicy Methodget URL/ HTTP Host172.31.21.76 FortiWeb Session IDnone Severity LevelHigh Signature Subclass TypeHTTP Header Leakage Signature ID080200004 Source CountryReserved HTTP Content Routingpservier UsernameUnknown Monitor ModeDisabled HTTP Referrernone Client Device IDnone Main TypeInformation Detection Sub TypeSignature Detection Machine Learning Domain Index0 Machine Learning URL ID0 Machine Learning ARG ID0 Threat LevelLow Threat Weight5 Historical Threat Weight0 User AgentELB-HealthChecker/2.0 MessageHTTP Header triggered signature ID 080200004 of Signatures policy clone _signature
2	01-13-22:16:06	2-J-0368eb179f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
3	01-13-22:16:02	2-J-0368eb179f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
4	01-13-22:15:59	2-J-0bb48f7465d40bf0	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure	
5	01-13-22:15:56	2-J-0bb48f7465d40bf0	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure	
6	01-13-22:15:55	2-J-0368eb179f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
7	01-13-22:15:52	2-J-0368eb179f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
8	01-13-22:15:48	2-J-0bb48f7465d40bf0	Low	Erase	172.31.18.40	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure	
9	01-13-22:15:47	2-J-085441cf0eb83761	Low	Erase	172.31.17.27	13.209.66.90	172.31.11.162	get	Signature Detection	Information Disclosure	
10	01-13-22:15:45	2-J-0bb48f7465d40bf0	Low	Erase	172.31.18.40	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure	
11	01-13-22:15:44	2-J-0368eb179f21a0e5e	Low	Erase	34.235.161.174	13.209.66.90	18.136.194.235	get	Signature Detection	Information Disclosure	
12	01-13-22:15:44	2-J-085441cf0eb83761	Low	Erase	172.31.17.27	13.209.66.90	172.31.11.162	get	Signature Detection	Information Disclosure	
13	01-13-22:15:42	2-J-0368eb179f21a0e5e	Low	Erase	34.235.161.174	13.209.66.90	18.136.194.235	head	Signature Detection	Information Disclosure	
14	01-13-22:15:39	2-J-0368eb179f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
15	01-13-22:15:37	2-J-0368eb179f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
16	01-13-22:15:37	2-J-085441cf0eb83761	Low	Erase	172.31.18.40	13.209.66.90	172.31.11.162	get	Signature Detection	Information Disclosure	
17	01-13-22:15:36	2-J-080120e3cf6f780be	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure	
18	01-13-22:15:34	2-J-085441cf0eb83761	Low	Erase	172.31.18.40	13.209.66.90	172.31.11.162	get	Signature Detection	Information Disclosure	
19	01-13-22:15:33	2-J-035b171443a84e1d7	Low	Erase	172.31.17.27	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure	
20	01-13-22:15:33	2-J-080120e3cf6f780be	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure	
21	01-13-22:15:33	2-J-0bb48f7465d40bf0	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure	
22	01-13-22:15:30	2-J-035b171443a84e1d7	Low	Erase	172.31.17.27	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure	
23	01-13-22:15:30	2-J-0bb48f7465d40bf0	Low	Erase	172.31.18.40	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure	
24	01-13-22:15:25	2-J-080120e3cf6f780be	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure	
25	01-13-22:15:22	2-J-035b171443a84e1d7	Low	Erase	172.31.18.40	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure	
26	01-13-22:15:22	2-J-080120e3cf6f780be	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure	
27	01-13-22:15:21	2-J-085441cf0eb83761	Low	Erase	172.31.17.27	13.209.66.90	172.31.11.162	get	Signature Detection	Information Disclosure	
28	01-13-22:15:19	2-J-035b171443a84e1d7	Low	Erase	172.31.18.40	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure	
29	01-13-22:15:19	2-J-085441cf0eb83761	Low	Erase	172.31.18.40	13.209.66.90	172.31.11.162	get	Signature Detection	Information Disclosure	
30	01-13-22:15:10	2-J-080120e3cf6f780be	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure	
31	01-13-22:15:07	2-J-035b171443a84e1d7	Low	Erase	172.31.17.27	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure	
32	01-13-22:15:07	2-J-080120e3cf6f780be	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure	
33	01-13-22:15:04	2-J-035b171443a84e1d7	Low	Erase	172.31.18.40	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure	
34	01-13-21:41:36	2-J-0368eb179f21a0e5e	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error	Connection172.31.17.27:3616 -> 13.209.66.90:80
35	01-13-20:42:17	2-J-080120e3cf6f780be	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error	
36	01-13-20:37:40	2-J-0bb48f7465d40bf0	Critical	Alert_Deny	198.108.66.192	13.209.66.90	52.221.227.126	get	Signature Detection	Bad Robot	
37	01-13-20:16:47	2-J-035b171443a84e1d7	Off	Alert_Deny	106.75.93.37	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error	
38	01-13-20:15:33	2-J-0bb48f7465d40bf0	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error	
39	01-13-19:40:33	2-J-085441cf0eb83761	Critical	Alert_Deny	13.76.158.116	13.209.66.90	30.100.107	get	Signature Detection	Bad Robot	
40	01-13-19:37:26	2-J-0368eb179f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
41	01-13-19:37:20	2-J-0bb48f7465d40bf0	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure	
42	01-13-19:37:16	2-J-0368eb179f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure	
43	01-13-19:37:13	2-J-0bb48f7465d40bf0	Critical	Alert_Deny	118.24.83.220	13.209.66.90	52.221.227.126	get	Signature Detection	Trojans	
44	01-13-19:37:13	2-J-0bb48f7465d40bf0	Critical	Alert_Deny	118.24.83.220	13.209.66.90	52.221.227.126	get	Signature Detection	Trojans	

Click **Signature View** and you can see the signature details as below:

Log View ▾					
Signature Detail					
Signature ID:	080200004				
HTTP/2 Compatible					
Description:	This rule checks if the HTTP response header contains specific header field :X-Powered-By. This leakage can be achieved in HTTP response header.				
Found In:	RESPONSE_HEADER				
Match Example:	<table><tr><th>HTTP1X</th><th>HTTP2</th></tr><tr><td colspan="2"><pre>HTTP/1.1 200 OK Date: Wed, 30 Jan 2013 09:48:44 GMT &lt;#X-Powered-By: Asp.Net#&gt; Last-Modified: Sat, 20 Nov 2004 20:16:24 GMT ETag: &quot;483e6d-2c-3e9564c23b600&quot; Accept-Ranges: bytes Content-Length: 44 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html &lt;html&gt;&lt;body&gt;&lt;h1&gt;It works!&lt;/h1&gt;&lt;/body&gt;&lt;/html&gt;</pre></td></tr></table>	HTTP1X	HTTP2	<pre>HTTP/1.1 200 OK Date: Wed, 30 Jan 2013 09:48:44 GMT &lt;#X-Powered-By: Asp.Net#&gt; Last-Modified: Sat, 20 Nov 2004 20:16:24 GMT ETag: &quot;483e6d-2c-3e9564c23b600&quot; Accept-Ranges: bytes Content-Length: 44 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html &lt;html&gt;&lt;body&gt;&lt;h1&gt;It works!&lt;/h1&gt;&lt;/body&gt;&lt;/html&gt;</pre>	
HTTP1X	HTTP2				
<pre>HTTP/1.1 200 OK Date: Wed, 30 Jan 2013 09:48:44 GMT &lt;#X-Powered-By: Asp.Net#&gt; Last-Modified: Sat, 20 Nov 2004 20:16:24 GMT ETag: &quot;483e6d-2c-3e9564c23b600&quot; Accept-Ranges: bytes Content-Length: 44 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html &lt;html&gt;&lt;body&gt;&lt;h1&gt;It works!&lt;/h1&gt;&lt;/body&gt;&lt;/html&gt;</pre>					

Return

Click **Add Exception**, configure the settings below to add the signature exception rule per specific log to different group policies at the same time.

Signature Policy Name	Click  to select the group signature policy.
Disable Signature	Enable if you do not want to detect such attacks.
Alert Only	Enable this option if you want to receive only logs or alert email about detections, but do not want to block matching requests.
Add Exception	Enable this option if you want to exempt specific host name/URL combinations. The following fields can be configured only when Add Exception option is enabled.
URI	• String Match—Value is a literal URL, and it starts with a forward slash (/). • Regular Expression Match—Value is a regular expression that matches all and only the URLs that the exception applies to, and it does not require a forward slash (/). This field is automatically configured as default value. Do not include a domain name or parameters. To match a domain name, use the Host element type. To match a URL that includes parameters, use the Full URL type.
HOST	• String Match—Value is a literal host name. • Regular Expression Match—Value is a regular expression that matches all and only the hosts that the exception applies to. This field is automatically configured as default value.
Full URL	• String Match—Value is a literal URL. • Regular Expression Match—Value is a regular expression that matches all and only the URLs that the exception applies to.
HTTP Method	Select the methods to include or exclude from the signature exemption. • Include—FortiWeb does not perform a signature scan for requests that include the specified HTTP methods. • Exclude—FortiWeb only performs signature scans for requests that include the specified HTTP methods.
Client IP	Specify the client IP address or IP range that FortiWeb uses to determine whether or not to perform a signature scan for the request. • Equal—FortiWeb does not perform a signature scan for requests with a client IP address or IP range that matches the value of Client IP. • Not Equal—FortiWeb only performs a signature scan for requests with a client IP address or IP range that matches the value of Client IP.
Parameter	• String Match—Name is the literal name of a cookie. • Regular Expression Match—Name is a regular expression that matches all and only the name of the cookie that exception applies to. Specify the name of the cookie and cookie value.
Cookie	• String Match—Name is the literal name of a parameter. • Regular Expression Match—Name is a regular expression that matches all and

only the name of the parameter that exception applies to.
Specify the name of the parameter and parameter value.

After you finish the settings, click **Push** to apply the signature exception rule to related FortiWeb device groups. See *FortiWeb Administration Guide* document in the Fortinet Document Library at <https://docs.fortinet.com/fortiweb/admin-guides> for more information about configuring signature exception rules.

Add Signature Exception Rule

Signature ID080200004

Signature Policy Name

group1>signature-1

group1>signature-3

group1>Scanner Integration

AWS>clone_signature

Disable Signature

Alert Only

Add Exception

URIString Match/

HostString Match172.31.21.76

Full URLString Match

HTTP MethodInclude

Client IPEqual

ParameterString Match

CookieString Match

GET

POST

HEAD

OPTIONS

TRACE

CONNECT

DELETE

PUT

PATCH

OTHERS

(e.g. 1.2.3.4, 2001-1, 1.2.3.4-1.2.3.40, 2001-1-2001-100)

NameValue

NameValue

Push

Cancel

Select Entries

Search

AWS

clone_signature

group1

signature-1

signature-2

signature-3

Scanner Integration

max-name111111111111111111

blank name

specialchar-name-!@%'^&*_-+[]

specialchar-name-!@%'^&*_-+[]

When the Main Type is **HTTP Protocol Constraints**, one additional button **Add Exception** appears on the **Log Details** page.

#	Date/Time	Device Name	Threat Level	Action	Source	Destination	HTTP Host	Method	Main Type	Sub Type
1	01-13-22:26:50	2-j-085441cf0eb83761	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error
2	01-13-22:16:06	2-j-0368eb19f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
3	01-13-22:16:02	2-j-0368eb19f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
4	01-13-22:15:59	2-j-0bb48f7465d40b0f	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure
5	01-13-22:15:56	2-j-0bb48f7465d40b0f	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure
6	01-13-22:15:55	2-j-0368eb19f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
7	01-13-22:15:52	2-j-0368eb19f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
8	01-13-22:15:48	2-j-0bb48f7465d40b0f	Low	Erase	172.31.18.40	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure
9	01-13-22:15:47	2-j-085441cf0eb83761	Low	Erase	172.31.17.27	13.209.66.90	172.31.1.162	get	Signature Detection	Information Disclosure
10	01-13-22:15:45	2-j-0bb48f7465d40b0f	Low	Erase	172.31.18.40	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure
11	01-13-22:15:44	2-j-0368eb19f21a0e5e	Low	Erase	34.235.161.174	13.209.66.90	18.136.194.235	get	Signature Detection	Information Disclosure
12	01-13-22:15:44	2-j-085441cf0eb83761	Low	Erase	172.31.17.27	13.209.66.90	172.31.1.162	get	Signature Detection	Information Disclosure
13	01-13-22:15:42	2-j-0368eb19f21a0e5e	Low	Erase	34.235.161.174	13.209.66.90	18.136.194.235	head	Signature Detection	Information Disclosure
14	01-13-22:15:39	2-j-0368eb19f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
15	01-13-22:15:37	2-j-0368eb19f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
16	01-13-22:15:37	2-j-085441cf0eb83761	Low	Erase	172.31.18.40	13.209.66.90	172.31.1.162	get	Signature Detection	Information Disclosure
17	01-13-22:15:36	2-j-080120c3cf6f780be	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure
18	01-13-22:15:34	2-j-085441cf0eb83761	Low	Erase	172.31.18.40	13.209.66.90	172.31.1.162	get	Signature Detection	Information Disclosure
19	01-13-22:15:33	2-j-035b171443a84e1d7	Low	Erase	172.31.17.27	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure
20	01-13-22:15:33	2-j-080120c3cf6f780be	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure
21	01-13-22:15:33	2-j-0bb48f7465d40b0f	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure
22	01-13-22:15:30	2-j-035b171443a84e1d7	Low	Erase	172.31.17.27	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure
23	01-13-22:15:30	2-j-0bb48f7465d40b0f	Low	Erase	172.31.18.40	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure
24	01-13-22:15:25	2-j-080120c3cf6f780be	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure
25	01-13-22:15:22	2-j-035b171443a84e1d7	Low	Erase	172.31.18.40	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure
26	01-13-22:15:22	2-j-080120c3cf6f780be	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure
27	01-13-22:15:21	2-j-085441cf0eb83761	Low	Erase	172.31.17.27	13.209.66.90	172.31.1.162	get	Signature Detection	Information Disclosure
28	01-13-22:15:19	2-j-035b171443a84e1d7	Low	Erase	172.31.18.40	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure
29	01-13-22:15:19	2-j-085441cf0eb83761	Low	Erase	172.31.18.40	13.209.66.90	172.31.1.162	get	Signature Detection	Information Disclosure
30	01-13-22:15:10	2-j-080120c3cf6f780be	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure
31	01-13-22:15:07	2-j-035b171443a84e1d7	Low	Erase	172.31.17.27	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure
32	01-13-22:15:07	2-j-080120c3cf6f780be	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.160	get	Signature Detection	Information Disclosure
33	01-13-22:15:04	2-j-035b171443a84e1d7	Low	Erase	172.31.18.40	13.209.66.90	172.31.22.5	get	Signature Detection	Information Disclosure
34	01-13-21:41:36	2-j-0368eb19f21a0e5e	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error
35	01-13-20:42:17	2-j-080120c3cf6f780be	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error
36	01-13-20:37:40	2-j-0bb48f7465d40b0f	Critical	Alert_Deny	198.108.66.192	13.209.66.90	52.221.227.126	get	Signature Detection	Bad Robot
37	01-13-20:16:47	2-j-035b171443a84e1d7	Off	Alert_Deny	106.75.50.37	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error
38	01-13-20:15:33	2-j-0bb48f7465d40b0f	Off	Alert_Deny	178.128.194.144	13.209.66.90	none	none	HTTP Protocol Constraints	HTTP Parsing Error
39	01-13-19:40:33	2-j-085441cf0eb83761	Critical	Alert_Deny	137.6.158.116	13.209.66.90	30.100.107	get	Signature Detection	Bad Robot
40	01-13-19:37:26	2-j-0368eb19f21a0e5e	Low	Erase	172.31.17.27	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
41	01-13-19:37:20	2-j-0bb48f7465d40b0f	Low	Erase	172.31.17.27	13.209.66.90	172.31.21.76	get	Signature Detection	Information Disclosure
42	01-13-19:37:16	2-j-0368eb19f21a0e5e	Low	Erase	172.31.18.40	13.209.66.90	172.31.10.39	get	Signature Detection	Information Disclosure
43	01-13-19:37:13	2-j-0bb48f7465d40b0f	Critical	Alert_Deny	118.248.32.20	13.209.66.90	52.221.227.126	get	Signature Detection	Trojans
44	01-13-19:37:13	2-j-0bb48f7465d40b0f	Critical	Alert_Deny	118.248.32.20	13.209.66.90	52.221.227.126	get	Signature Detection	Trojans

Log Details

Add Exception

Date

2019-01-13

Time

22:26:50

Log ID

20000026

MSG ID

00000015215

Type

attack

Device Name

2-j-085441cf0eb83761

Time Zone

(GMT-8:00)Pacific Time(US&Canada)

Protocol

tcp

Service

http

Cipher Suite

none

HTTP Version

1.x

Action

Alert_Deny

Policy

policy

Method

none

URL

none

HTTP Host

none

FortiWeb Session ID

none

Severity Level

High

Signature Subclass Type

N/A

Signature ID

N/A

Source Country

Germany

HTTP Content Routing

none

Server Pool

pserver

Username

Unknown

Monitor Mode

Disabled

HTTP Referer

none

Client Device ID

none

Main Type

HTTP Protocol Constraints

Sub Type

HTTP Parsing Error

Machine Learning Domain Index

0

Machine Learning URL ID

0

Machine Learning ARG ID

0

Threat Level

Off

Threat Weight

0

Historical Threat Weight

0

User Agent

none

Message

Malformed HTTP Protocol (Error: 10)
: Malformed Request

Connection

178.128.194.144:34918 -> 13.209.66.90:80

Packet Header

Click **Add Exception**, configure the settings below to add the HTTP constraint exception rule per specific log.

HTTP Protocol	Click  to select group HTTP protocol constraint policy.
Constraint Policy Name	
URL Pattern	• String Match—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (<code>/</code>). • Regular Expression Match—such as <code>^/*\.php</code>, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the Host drop-down list.
Host	Enter the IP address or fully qualified domain name (FQDN) of the protected host to which this exception applies.
Source IP	Enable to check requests for matching the HTTP constraint exceptions rule by their source IP addresses.
Protocol Constraint(s)	Select the protocol constraint(s) that you want to add to the exception rule according to the table below.

After you finish the settings, click **Push** to apply the HTTP constraint exception rule to related FortiWeb device groups. See *FortiWeb Administration Guide* document in the Fortinet Document Library at <https://docs.fortinet.com/fortiweb/admin-guides> for more information about configuring HTTP protocol constraint exceptions.

Add HTTP Constraint Exception Rule

HTTP Protocol
Constraint Policy
Name

group1>HTTP Protocol Constraints-1

group1>HTTP Protocol Constraints2

group1>specialchars-name-!@%*<"-'~[]\|/?

URL Pattern

String Match

Host

Source IP

(e.g. 1.2.3.4, 2001::1, 1.2.3.4-1.2.3.40, 2001::1-2001::100)

Status	Name	Description
☒	Content Length (2)	
☐	Content Length	Maximum acceptable length in bytes of the request body (16,384 by default).
☐	Illegal Content Length	Checks that the Content-Length header includes numeric characters only.
☒	HTTP Header (6)	
☐	Header Length	Maximum acceptable size in bytes of all HTTP header lines (8192 bytes by default).
☐	Header Name Length	Maximum acceptable size in bytes of a single HTTP header name (50 bytes by default).For example, Host, Content-Type, User-Agent
☐	Header Value Length	Maximum acceptable size in bytes of a single HTTP header value (4096 bytes by default).For example, Host, Content-Type, User-Agent
☐	Illegal Character in Header Name	Checks for illegal characters in the HTTP header name.For example, Host, Content-Type, User-Agent
☐	Illegal Character in Header Value	Checks for illegal characters in the HTTP header value.For example, Host, Content-Type, User-Agent
☐	Redundant HTTP Headers	Invoked if an HTTP request contains multiple redundant headers.
☒	HTTP Parameter (10)	
☐	Total URL Parameters Length	Maximum acceptable length in bytes of all parameters, including their names and values, in the URL (8192 bytes by default).
☐	Total Body Parameters Length	Maximum total acceptable size in bytes of all parameters in the URL and/or, for HTTP POST requests, the HTTP body (8192 bytes by default).
☐	Number of URL Parameters	Maximum number of parameters in a URL (128 by default).
☐	NULL Character in Parameter Name	Checks for NULL characters in parameter names.
☐	NULL Character in Parameter Value	Checks for NULL characters in parameter values.
☐	Maximum URL Parameter Name Length	Maximum acceptable length in bytes of a single URL parameter name (4096 bytes by default).
☐	Maximum URL Parameter Value Length	Maximum acceptable length in bytes of a single URL parameter value (4096 bytes by default).
☐	Illegal Character in Parameter Name	Checks for illegal characters in the parameter name. For example, non-printable ASCII characters.
☐	Illegal Character in Parameter Value	Checks for illegal characters in the parameter value. For example, non-printable ASCII characters.
☐	Duplicate Parameter Name	Checks for duplicated parameter name.
☒	HTTP Request (5)	
☐	Illegal HTTP Request Method	Checks for invalid HTTP request methods according to RFC 2616 or RFC 4918. Any method undefined in these RFCs – including misspellings like GETT as well as other HTTP extension methods (e.g. CalDAV) like MKCA LENDAR – are considered illegal.
☐	HTTP Request Filename Length	Maximum acceptable length of HTTP request filename (2048 bytes by default).
☐	HTTP Request Path Length	Maximum acceptable length of the entire HTTP request, including both headers and body (2048 KB by default).

Push

Cancel

Select Entries

Search

AWS

group1

HTTP Protocol Constraints-1

HTTP Protocol Constraints2

HTTP Protocol Constraints3

scannerimport

max-name1111111111111111111111

blank name

specialchars-name-!@%*<"-'~[]\|/?

specialchars-name-!@%*<"-'~[]\|/?

Traffic logs

Traffic logs record the traffic flowing through your FortiWeb device, such as HTTP/HTTPS requests and responses. This pane includes the following information:

Date/Time	The date/time when the log is generated.
Device Name	The name of the managed device.
Source	The source ID address of the client where the attack comes from.
Destination	The destination IP address where the attack happens.
Service	The web service used, such as HTTP, HTTPS.
Method	The HTTP method used, such as GET, POST, PUT, and DELETE, etc.
Return Code	The HTTP response codes returned from the web server.
Message	The detailed traffic log information.

Event logs

Event logs display administrative events, such as downloading a backup copy of the configuration, and hardware failures. This pane includes the following information:

Date/Time	The date/time when the log is generated.
Device Name	The name of the managed device.
Level	The level of the log, critical, information, and notice.
User Interface	The interface the user uses, daemon, GUI or sshd.
Action	The action items that FortiWeb has taken.
Message	The detailed action information of FortiWeb.

Note: **Log View** can not show logs of managed devices that fail to communicate with FortiWeb Manager, and a red down arrow indicates such devices on **Device Manager** page.

#	Device Name	SN	IP Address	Platform	Version	Build	Activity
1	↑ dev2	FV400C3M12000023	172.22.6.189	FortiWeb-400C	V6.01	B0035	🟢🟡🟡🟡🟡
2	↓ test123	FV100D3915000118	10.200.30.104	FortiWeb-100D	V6.01	B0036	



You can schedule automatic deletion of event logs from **System Settings > File Management**. Check the box for event logs, and set the time periods and deletion time accordingly.

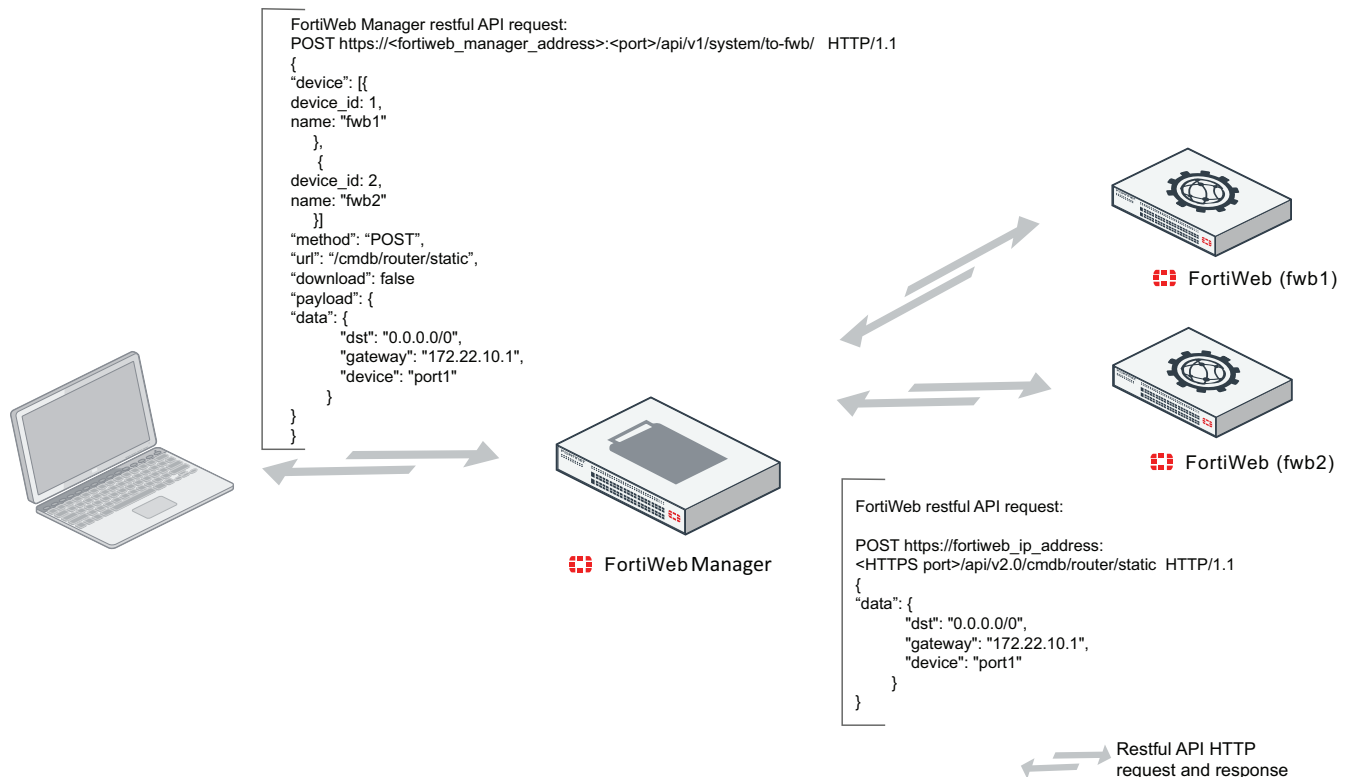
If you enter a comment when you reboot or shut down a FortiWeb Manager device from **Status > Status** page, you can view such log.

API Proxy

FortiWeb device has provided a series of native APIs for the user to manage its own internal items, e.g. <https://172.22.10.74:443/api/v2.0/cmdb/router/static>. FortiWeb Manager encapsulates all necessary information of native FortiWeb APIs and uses two easier-to-use APIs for configuration management:

- **to-fwb API:** https://<fortiweb_manager_address>:<port>/api/v1/to-fwb/, used for all remote configuration requests, including fetching, creating, updating and deleting. You can specify parameters such as device, method and URL to let FortiWeb Manager know more details of the configuration requests.
- **to-fwb/upload API:** https://<fortiweb_manager_address>:<port>/api/v1/to-fwb/upload/, used to upload files, for instance, certificate uploading. FortiWeb Manager supports three pre-set file types: Certificate, Local Certificate, PKCS12 Certificate. You can also select **File - Custom** to upload customized files.

The following diagram shows the process of FortiWeb Manager receiving these API requests, translating them to native FortiWeb APIs and forwarding the corresponding ones to the remote FortiWeb devices.



Using API proxy is an easier way to integrate multiple FortiWeb devices into your own management system.

Using API proxy

The API proxy page is a useful tool to look up the HTTP request and HTTP response of the **to-fwb API** and **to-fwb/upload API**. You can configure the following parameters and click **Send**, the page then displays the HTTP request and HTTP response for the parameters you have specified.

Device	Select the devices to which the API request sends.
Type	• JSON - Custom: customize the HTTP request parameters as JSON format payload when connecting to FortiWeb devices. • File - Custom: specify local files for uploading to FortiWeb devices. • File - Certificate: upload certificate to FortiWeb devices. • File - Local Certificate: upload local certificate to FortiWeb devices. • File - PKCS12 Certificate: upload PKCS12 certificate to FortiWeb devices.
Method	Select GET, POST, PUT or DELETE methods, depending on the operations you desire.
URL	Enter the FortiWeb API URL for the specific operations.
Parameter List	This displays when you select File types in Type . You can select the files you want to upload.



For more information on the FortiWeb Manager API and FortiWeb API usage, see:

- [FortiWeb Manager API Reference Guide](#)
- [FortiWeb API Reference Guide](#)

Maintaining the system

You can upgrade the firmware of FortiWeb Manager, view the system logs, retrieve debug logs and schedule file deletion.

Viewing system logs

The Log pane (**System Settings > Log**) provides an audit log of actions made by users on FortiWeb Manager. It allows you to view log messages that are stored in database. You can filter the logs using the **Add Filter** box in the toolbar.

To filter logs using the toolbar:

1. Specify filters in the *Add Filter* box.
 - In the selected summary view, click in the **Add Filter** box, select a filter from the dropdown list, then type a value.
 - Click NOT to negate the filter value.
 - You can add multiple filters at a time, and connect them with an "or".
 - For the Date filter, click **<=**, **>=** or **A-B** to specify a period earlier than the date, later than the date, or between date A and date B. You can also click **Last 24 hours**, **Last 5 hours** and **Last hour**.
2. Click **Go** to apply the filter.

By default, the system saves the logs generated within 365 days. If you want to change the days, go to **System Settings > Advanced > File Management**, specify the number of days in **Events logs older than** field.

Upgrading firmware for FortiWeb Manager

To upgrade the firmware for FortiWeb Manager:

1. Go to **System Settings > Maintenance > Firmware Upgrade**.
2. Click **Select File**, browse to the FortiWeb Manager image file on your local computer, then click **Open**.
3. Click **Upload** at the bottom of the page.

Retrieving debug logs

If your troubleshooting issue requires debugging, go to **System Settings > Maintenance > Debug > Download** to retrieve the logs. You can download the following logs:

- crash logs
- daemon logs

- kernel logs
- netstat logs
- core dump logs
- perf log
- top log
- tcpdump logs

Scheduling files deletion

You need to clear the files regularly to ensure enough space of the storage disk. **File Management** module allows you to schedule automatic deletion of the files.

Check the box of the item to delete, and set the time periods and deletion performing time accordingly.

CLI Commands

FortiWeb Manager provides the following CLI commands:

- `set interface`
- `set route`
- `unset route`
- `show interface`
- `show route`
- `execute formatlogdisk`
- `execute ping`
- `execute reboot`
- `execute shutdown`
- `get system status`

You can enter `help` to display a list of the commands. To exit the CLI, enter `exit`.

set interface

This command configures the network interfaces of FortiWeb Manager.

FortiWeb Manager supports the following interfaces by default. You can set the parameters for these ports.

Network Interface*	IPv4 Address/Netmask	IPv6 Address/Netmask
port1	192.168.1.99/24	::/0
port2	0.0.0.0/0	::/0
port3	0.0.0.0/0	::/0
port4	0.0.0.0/0	::/0

Syntax

```
set interface <port> {(ip | ip6) <IPADDRESS/LENGTH> | (addressing-mode | addressing6-mode) (manual | dhcp) }
```

Variable	Description
<port>	Select the physical network port of the FortiWeb Manager appliance.
addressing-mode {manual dhcp}	Specify whether FortiWeb Manager acquires an IP address for this network interface manually or using DHCP to allow DHCP server to automatically assign IP address.
<IPADDRESS/LENGTH>	Type the IP address and subnet mask, separated by a forward slash (/

Variable	Description
	), such as 192.0.2.2/24 for an IPv4 address.

Example

```
set interface port1 ip 10.200.111.98/24
set interface port1 addressing-mode dhcp
```

set route

This command sets the gateway for FortiWeb Manager.

Syntax

```
set route <DST/LENGTH> gw <GATEWAY> device <DEVICE>
```

Variable	Description
<DST/LENGTH>	Enter the destination IP address and network mask of packets that use this static route, separated by a slash (/). Enter 0.0.0.0/0.0.0.0 , 0.0.0.0/0 or ::/0 to create a default route that matches the DST field in the IP header of all packets.
gw <GATEWAY>	Enter the IP address of the next-hop router to which FortiWeb Manager forwards packets that match Destination IP/Mask (IPv4/IPv6) . Ensure that this router knows how to route packets to the destination IP addresses or forward packets to another router with this information. For a direct Internet connection, this is the router that forwards traffic towards the Internet, and could belong to your ISP.
device <DEVICE>	Enter the network interface through which FortiWeb Manager routes the packets that match Destination IP/Mask (IPv4/IPv6) to the next-hop router.

Example

```
set route 0.0.0.0/0 gw 10.200.0.1 device port1
set route ::/0 gw 10::1 device port1
```

unset Route

This command deletes the corresponding route which you specify in the command.

Syntax

```
unset route <ID>
```

you can run `show route` to get the route ID.

Example

```
unset route 1
```

show interface

This command displays the network interface information, including name, IPv4 address/length, IPv6 address /Length and description.

Syntax

```
show interface
```

Example

The following is an example of the printout of `show interface`.

Name	IP Address/Length	IPv6 Address/Length	Description
port1	10.200.111.98/16	10:200::111:98/64	
port2	0.0.0.0/0	::/0	
port3	0.0.0.0/0	::/0	
port4	0.0.0.0/0	::/0	

get system status

This command displays system status information including:

- system time
- system uptime

- host name
- firmware version, build number and date
- boot time
- computer ID
- License start date
- device limit
- license period
- serial number
- plugin version

Syntax

```
get system status
```

execute formatlogdisk

This command clears all logs on the hard disk.

Syntax

```
Execute formatlogdisk
```

When you execute this command, the FortiWeb appliance displays the following message:

This operation will clear all data on the log disk and take a few minutes according to the disk size!!

Do you want to continue? (y/n)

Enter `y` to continue. Enter `n` if you want to abort the operation.

execute ping

This command runs a ping request to a host by specifying its IPv4 address. Pings are often used to test IP-layer connectivity during troubleshooting.

Syntax

```
Execute ping <IPADDRESS>
```


Example

This example pings a host with the IP address 192.0.2.10.

```
execute ping 192.0.2.10
```

The CLI displays the following:

```
PING 192.0.2.10 (192.0.2.10): 56 data bytes
64 bytes from 192.0.2.10: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 192.0.2.10: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 192.0.2.10: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 192.0.2.10: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 192.0.2.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 192.0.2.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results indicate that a route exists between the FortiWeb Manager and 192.0.2.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds.

execute reboot

This command restarts the FortiWeb Manager.

Syntax

```
execute reboot
```

Example

This example shows the reboot command in action.

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages while the reboot is occurring.

If you are connected to the CLI through the network, the CLI will not display any notification while the reboot is occurring, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection is

terminated. Time required by the reboot varies by many factors, such as whether or not hard disk verification is required, but may be several minutes.

execute shutdown

This command prepares FortiWeb Manager to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.

Power off FortiWeb Manager only after issuing this command. Unplugging or switching off the FortiWeb appliance without issuing this command could result in data loss.

Syntax

```
execute shutdown
```

Example

This example shows the reboot command in action.

```
execute shutdown
```

The CLI displays the following:

This operation will halt the system

(power-cycle needed to restart)!Do you want to continue? (y/n)

After you enter `y`, the CLI displays the following:

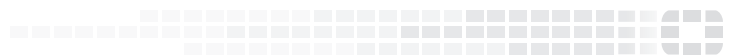
System is shutting down...(power-cycle needed to restart)

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI will not display any notification when the shutdown is complete, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection times out.



FORTINET



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.