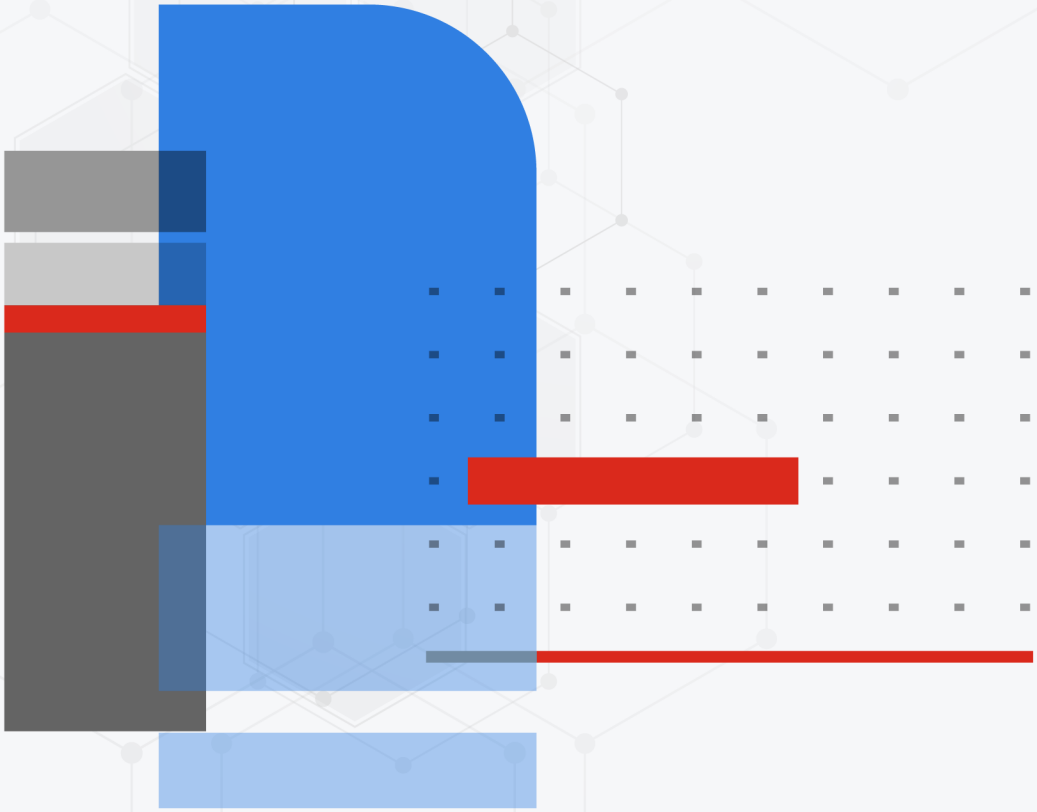
Getting Started

FortiDeceptor 5.3.0



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

March 14, 2024
FortiDeceptor 5.3.0 Getting Started
50-530-1010601-20240314

TABLE OF CONTENTS

Set up FortiDeceptor

Use the following checklist to verify you have completed all of the general configuration tasks.

Task	Description
☐ Connect to the GUI	Connect the administration interface to a management computer with an Ethernet cable, then configure the management computer to be on the same subnet as the internal interface of the FortiDeceptor unit.
☐ Change the administrator password	You are required to create a create strong password the first time you log into FortiDeceptor.
☐ Change the system hostname	Change the full host name in the *System Information* widget.
☐ Connect to the CLI	If necessary, connect to the CLI console.
☐ Configure the system time	Configure the FortiDeceptor system time manually or synchronize with an NTP server from the *System Information* widget.
☐ Upload the license file to FortiDeceptor	Go to *Dashboard* > *System Information* widget, click *Upload License* beside *Firmware License*.
☐ Review the default port information	FortiDeceptor reserves Port1 for device management. The other ports are used to deploy deception decoys.
☐ Configure Central Management on the manager	Configure the Central Management console to manage remote FortiDeceptor appliances including Decoy VMs deployment, system configuration, and incident alert monitoring.

Connect to the GUI

Use the GUI to configure and manage FortiDeceptor.

To connect to the FortiDeceptor GUI:

1. Using an Ethernet cable, connect the management computer to FortiDeceptor's port1.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiDeceptor unit:
   - Change the IP address of the management computer to `192.168.0.2`.
   - Change the IP address of the network mask to `255.255.255.0`.
3. Go to `https://192.168.0.99`.
4. Type `admin` in the *Name* field, leave the *Password* field blank, and click *Login*.
   You can now proceed with configuring your FortiDeceptor unit.

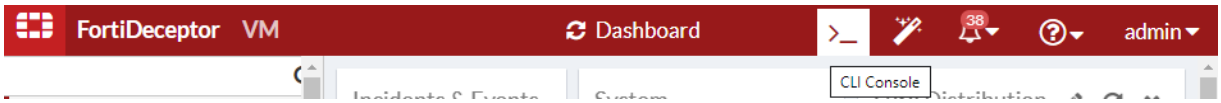
If the network interfaces have been configured differently during installation, the URL and administrative access protocols might not be in their default state.

Connect to the CLI

You can use CLI commands to configure and manage FortiDeceptor.

To connect to the FortiDeceptor CLI:

1. In the FortiDeceptor banner at the top, click the *CLI Console* icon.



   The *CLI Console* pane opens.
2. If necessary, click *Connect* and enter your username and password.
   The *CLI Console* pane has icons to disconnect from the CLI console, clear console text, download console text, copy console text, open the CLI console in its own window, and close the console.
3. To close the CLI console, click the *Close* icon.

Change the system hostname

The *System Information* widget displays the full host name. You can change the FortiDeceptor host name.

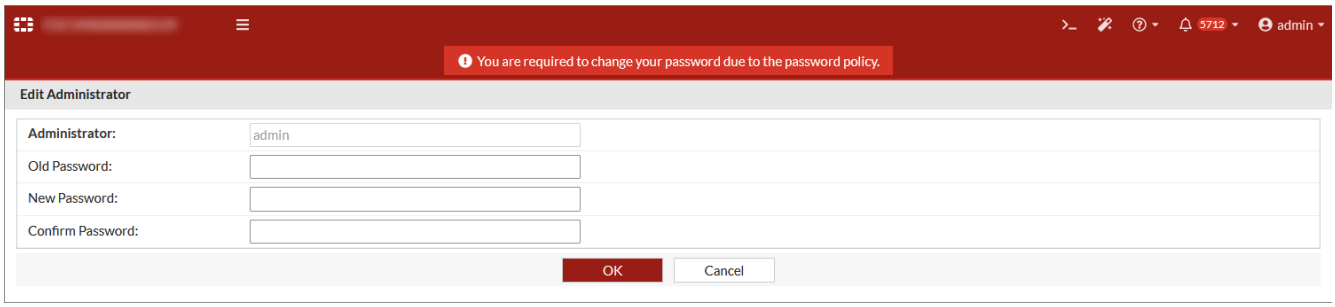
To change the host name:

1. Go to *Dashboard*, *System Information* widget.
2. Click *Change* beside *Host Name*.
3. In the *New Name* field, type a new host name.
   The hostname can start with a character or digit, and cannot end with a hyphen. A-Z, a-z, 0-9, or hyphen are allowed (case-sensitive). Other symbols, punctuation, or white space are not allowed.
4. Click *Apply*.

Change the administrator password

The first time you log into FortiDeceptor you will be prompted to change the administrator password. Passwords must be 8-60 characters long, and contain only upper/lower-case letters, numbers and special characters *!#$%()*.

Due to a higher level of password encryption introduced in version 5.2.0, users upgrading from v5.1.0 to v5.2.0 will be prompted to change their password.



To change the password of the logged in administrator:

1. In the FortiDeceptor banner at the top, click the username and select *Change Password*.
2. Change the password and click *OK*.

To change the administrator password in the Administrators page:

1. Go to *System* > *Administrators*.
2. Select an administrator and click *Edit*.
3. Change the password and click *OK*.

To change the administrator password with the CLI:

Run the following command:

```
passwd
```

Example:

```
> passwd

Old password: *************

New password: *************

Confirm password: *************

Successfully changed password, please re-login with the new password.
```

Configure the system time

You can change the FortiDeceptor system time in the *Dashboard*. You can configure the FortiDeceptor system time manually or synchronize with an NTP server.

To configure the system time:

1. Go to *Dashboard* > *System Information* widget and click *Change* beside *System Time*.
2. Select the *Time Zone* and wait for the widget to refresh.
3. Check that the *System Time* is correct. If necessary, click *Set Time* and manually set the time and date.

4. Click *Apply*.
   You might need to log in again.

If the time is not correct, we recommend configuring the NTP server for time synchronization.

Upload license file to FortiDeceptor

To upload the license to FortiDeceptor:

1. Go to *Dashboard* > *System Information* widget, click *Upload License* beside *Firmware License*.
2. Locate the license and click *Submit*.

Default port information

FortiDeceptor treats Port1 as reserved for device management. The other ports are used to deploy deception decoys.

The following table list the default open ports for each FortiDeceptor interface.

FortiDeceptor default ports:

Configure the FortiDeceptor management IP address on port1.

Configure the FortiDeceptor management IP address on port1.

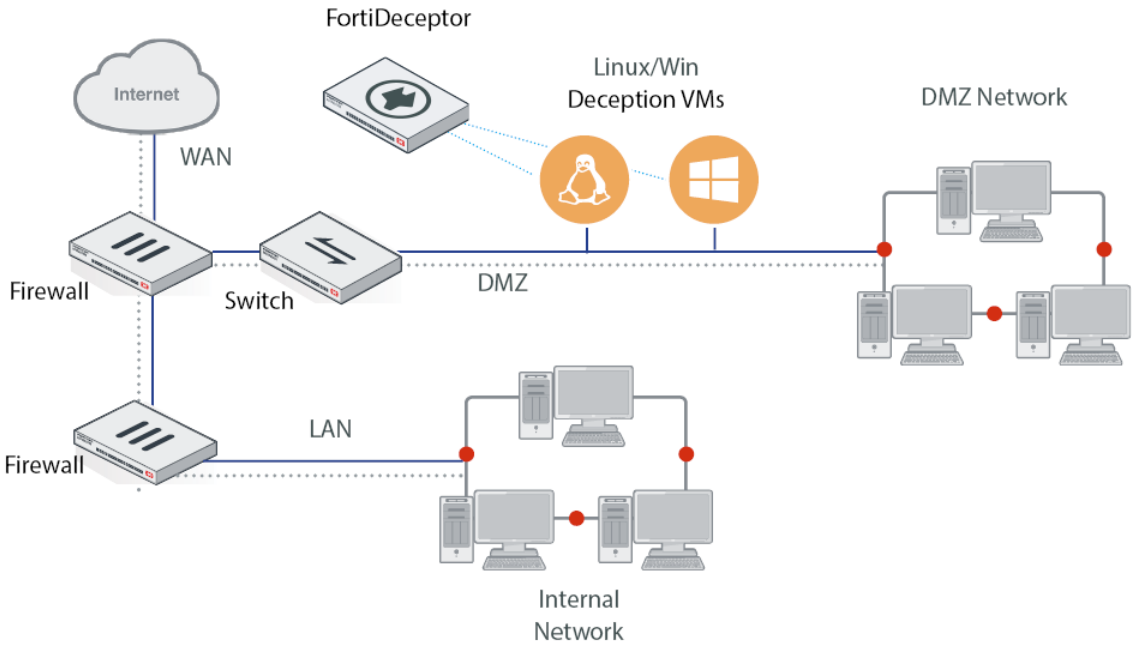
Port (Interface)	Default Open Ports
Port1	TCP ports 22 (SSH), 23 (Telnet), 80 and 443 (GUI). FortiGuard Distribution Servers (FDS) use TCP port 443 or 8890 for download. FortiDeceptor uses a random port picked by the kernel. FortiGuard Web Filtering servers use TCP port 443 or UDP port 53 or 8888. FortiDeceptor uses a random port picked up by the kernel. FortiDeceptor deception VM download uses TCP port 443 for download. FortiDeceptor uses a random port picked by the kernel. FortiDeceptor Manager is required to open port 8443 **from** the client (remote appliance) to the FortiDeceptor Manager. FortiDeceptor Manager is required to have access to *virustotal.com* over port 443 for malware analysis based on MD5 request.
Port2 to port8	Each FortiDeceptor port can be directly connected to a specific VLAN or use the network trunk to communicate with multiple VLANs from a single interface. In DMZ mode, no service listens. In regular mode, token communication service listens on deployment interface monitor IP with port 1443. The token communication uses HTTPS protocol.

The default port for FortiDeceptor VM is 443. To add HTTP, SSH, Telnet or another port, go to *Network >Interfaces > port1> Edit*.

DMZ Mode

Deploy a FortiDeceptor hardware unit or VM in the Demilitarized Zone (DMZ). You can monitor attacks on the DMZ network when FortiDeceptor is installed in the DMZ network.

DMZ mode is useful when you want to deploy decoys to a segment of the network that hosts critical services. When a threat actor attacks a server and attempts to move laterally inside the DMZ segment they are detected by the decoys without exposing the decoys on the Internet.



Limitations of the DMZ Mode

The DMZ Mode in FortiDeceptor functions like regular mode with the following exceptions:

- When DMZ mode is enabled, the banner displays *DMZ-MODE*.
- In *Deception* > *Deployment Network*, *Deception Monitor IP/Mask* is hidden. See Set up the Deployment Network.
- In *Deception* > *Decoy & Lure Status* in the Deception Status view, the Attack Test selection is disabled.
- Decoy VMs are limited to one deployment Interface. For information about IP address range, see Deploy Decoy VMs with the Deployment Wizard.

To enable DMZ mode in the CLI:

```
dmz-mode -e
```

To disable DMZ mode in the CLI:

```
dmz-mode -d
```

Enabling or disabling the DMZ mode removes all previous configurations including Decoy VMs, lures, and tokens. Deception OS is not removed.

JSON API

FortiDeceptor provides a Representational State Transfer (REST) API for interaction with system components. Programs communicate with the REST API over HTTP, the same protocol your web browser uses to interact with web pages.

The REST-API authentication is based on a token generated by the FortiDeceptor.

The FortiDeceptor API has the following capabilities:

- Get the decoy deployment template list.
- Deploy decoys based on the decoy template configuration and the deployment network configuration (both STATIC and DHCP IP).
- Get a decoy deployment status.
- Stop/start the deployed decoys.
- Get incident alerts based on filter requests like time range (last minutes/hours/days) / service name/decoy name.

The *FortiDeceptor JSON API Reference* guide is available in the Fortinet Developer Network (FNDN). To access the guide, log in to FNDN and enter `FortiDeceptor` in the *Search* field.

Fortinet Developer Network is a subscription-based community. For more information about FNDN, visit Fortinet Worldwide Developer Community.

www.fortinet.com