

# FortiDeceptor - Administration Guide

Version 2.1.0

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



Aug 28, 2019

FortiDeceptor 2.1.0 Administration Guide

50-200-548424-20190828

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
<b>Set up FortiDeceptor</b>	<b>8</b>
Connect to the GUI	8
Change the system hostname	8
Change the administrator password	9
Configure the system time	9
<b>Deploy Decoy VM</b>	<b>11</b>
View Available Deception OS	11
Set up the Deployment Network	11
Deploy Decoy VMs with the Deployment Wizard	12
Deploy the FortiDeceptor Token Package	14
Monitor Decoy & Lure Status	15
View the Decoy Map	16
Configure a Whitelist	17
DMZ Mode	17
Limitations of the DMZ Mode	18
<b>Monitor Attacks</b>	<b>19</b>
Analysis	19
Campaign	20
Attack Map	21
Incidents and Events Distribution	22
Incidents and Events Count	22
Top 10 Attackers by Events	23
Top 10 Attackers by Incidents	23
Top 10 IPS Attacks	23
Incidents Distribution by Service	23
Global Attacker Distribution	24
<b>Fabric</b>	<b>25</b>
Blocking	25
Quarantine Status	26
IOC Export	26
<b>System</b>	<b>27</b>
Administrators	27
Admin Profiles	30
Certificates	33
LDAP Servers	34
RADIUS Servers	36
Mail Server	37
SNMP	38
FortiGuard	41

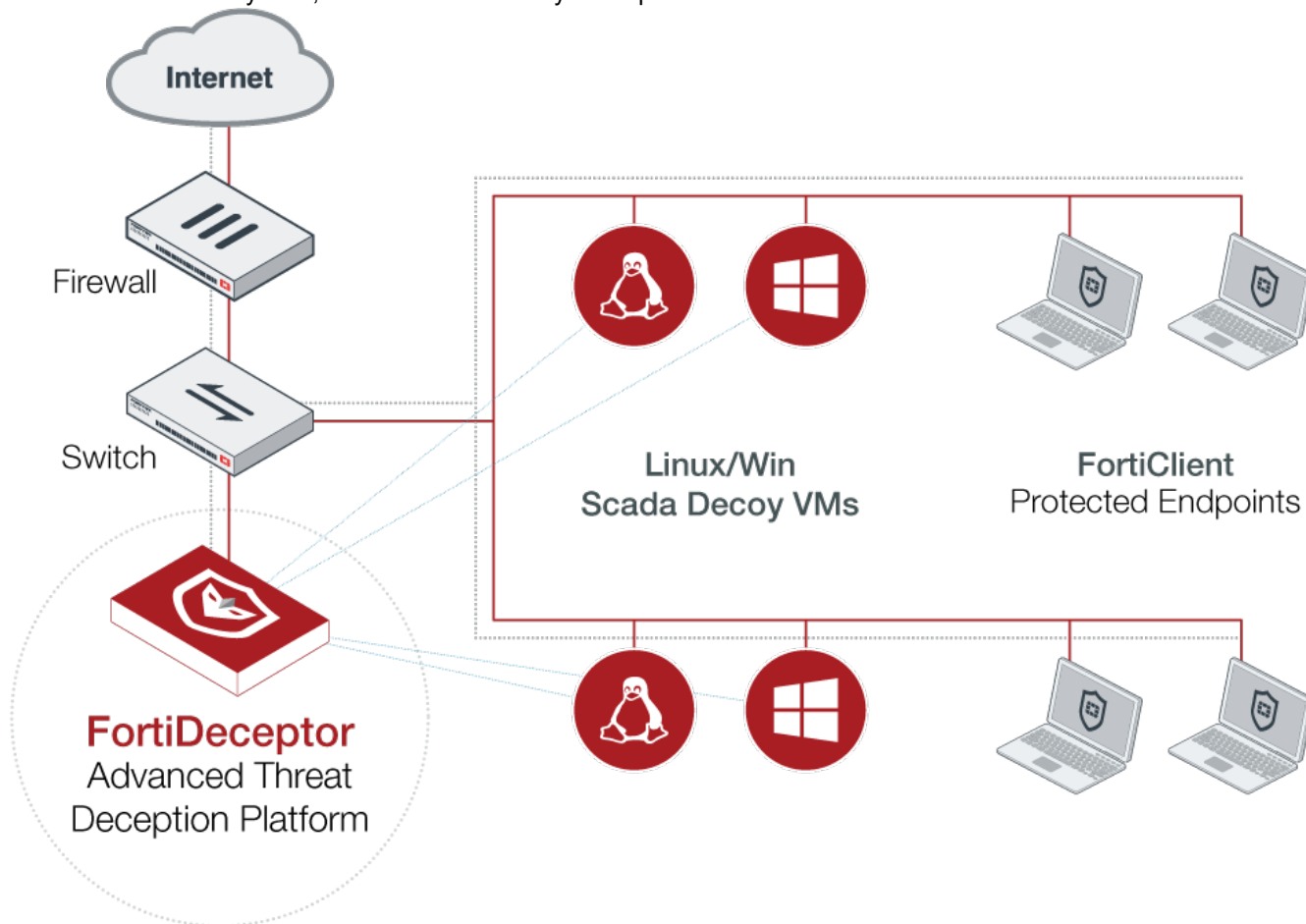
Login Disclaimer .....	42
Table Customization .....	42
Settings .....	42
<b>System Settings .....</b>	<b>43</b>
Dashboard .....	43
Customizing the dashboard .....	44
System Information .....	45
System Resources .....	46
Decoy Distribution by OS .....	46
Lure Distribution .....	47
Top Critical Logs .....	48
Disk Monitor .....	48
Basic System Settings .....	48
Change the GUI idle timeout .....	49
Microsoft Windows VM license activation .....	49
Log out of the unit .....	49
Refresh Current Web Page .....	49
Update the FortiDeceptor firmware .....	50
Reboot and shut down the unit .....	50
Back up or restore the system configuration .....	51
Network .....	51
Interfaces .....	52
DNS Configuration .....	53
System Routing .....	53
<b>System Log .....</b>	<b>55</b>
Log Details .....	55
Logging Levels .....	55
Raw logs .....	56
Log Categories .....	57
Log Servers .....	58

## Change Log

Date	Change Description
2019-08-28	Initial release of FortiDeceptor 2.1.0.

# Introduction

FortiDeceptor creates a network of Decoy VMs to lure attackers and monitor their activities on the network. Once attackers attack Decoy VMs, their actions are analyzed to protect the network.



Key features of FortiDeceptor include:

- Deception OS: Windows, Linux or Scada OS images are available to create Decoy VMs
- Decoy VMs: Decoy VMs that behave like real endpoints can be deployed through FortiDeceptor.
- Lures: Lures are services, applications, or users added to a Decoy VM to simulate a real user environment.
- FortiDeceptor Token Package: Install a FortiDeceptor Token Package to add breadcrumbs on real endpoints and lure an attacker to a Decoy VM. Tokens are normally distributed within the real endpoints and other IT assets on the network to maximize the deception surface. Tokens are used to influence attacker's lateral movements and activities. For example, cached credentials, database connections, network share, data files, or configuration files can be used in a token.
- Monitor the hacker's actions: Monitor *Incidents*, *Events*, and *Campaign*.
  - An *Event* represents a single action, for example, a login-logout on a victim host.
  - An *Incident* represents all actions on a single victim host, for example, a login-logout, file system change, a registry modification, and a website visit on a single victim host.

- A *Campaign* represents the hacker's lateral movement. All *Incidents* that are co-related are a *Campaign*. For example, an attacker logs on to a system using the credentials found on another system.
- Log Events: Log all FortiDeceptor system events.

# Set up FortiDeceptor

This chapter explains the initial set up of FortiDeceptor such as connecting to the GUI, changing the hostname, changing the administrator password, and configuring the system time.

The following topics explain the initial set up:

- [Connect to the GUI on page 8](#)
- [Change the system hostname on page 8](#)
- [Change the administrator password on page 9](#)
- [Configure the system time on page 9](#)

## Connect to the GUI

The FortiDeceptor unit is configured and managed using the GUI. This section will step you through connecting to the unit via the GUI.

### To connect to the FortiDeceptor GUI:

1. Connect the port1 (administration) interface of the device to a management computer using the provided Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiDeceptor unit:
  - a. Change the IP address of the management computer to 192.168.0.2 and the network mask to 255.255.255.0.
3. Start a supported web browser and browse to `https://192.168.0.99`.
4. Type `admin` in the *Name* field, leave the *Password* field blank, and select *Login*.  
You can now proceed with configuring your FortiDeceptor unit.



If the network interfaces have been configured differently during installation, the URL and/or permitted administrative access protocols may no longer be in their default state.

---

## Change the system hostname

The *System Information* widget will display the full host name. You can change the FortiDeceptor host name as required.

### To change the host name:

1. Go to *Dashboard > System Information > Host Name*.
2. Click *[Change]*.



3. In the *New Name* field, type a new host name.  
The hostname can start with English characters/digits, and must not end with a hyphen. It may contain only the ASCII letters *a* through *z* (in a case-insensitive manner), the digits *0* through *9*, and the hyphen ('-'). No other symbols, punctuation characters, or white space are permitted.
4. Select *Apply*.

## Change the administrator password

By default, you can log in to the GUI using the *admin* administrator account and no password. It is highly recommended that you add a password to the *admin* administrator account. For improved security, you should regularly change the *admin* administrator account password and the passwords for any other administrator accounts that you add.

You can change the password by clicking the current login username on the top-right corner of the GUI and selecting *Change Password*.

### To change the administrator password

1. Go to *System > Administrators*
2. Select the administrator's account you want to edit.
3. Click the *Edit* button in the toolbar.
4. Change the password.

## Configure the system time

The FortiDeceptor unit's system time can be changed from the *Dashboard*. You can configure the FortiDeceptor system time locally or select to synchronize with an NTP server.

### To configure the system time:

1. Go to *System Information widget > System Time*.
2. Click *[Update]*.
3. Configure the following settings:

<b>System Time</b>	The date and time according to the FortiDeceptor unit's clock at the time that this tab was loaded.
<b>Time Zone</b>	Select the time zone in which the FortiDeceptor unit is located.
<b>Set Time</b>	Select this option to manually set the date and time of the FortiDeceptor unit's clock, then select the <i>Hour</i> , <i>Minute</i> , <i>Second</i> , <i>Month</i> , <i>Day</i> , and <i>Year</i> fields before you select <i>Apply</i> .
<b>Synchronize with NTP Server</b>	Select this option to automatically synchronize the date and time of the FortiDeceptor unit's clock with an NTP server. The synchronization interval is hard-coded to be 5 minutes. You can configure only one NTP server.

**Server**

Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to <http://www.ntp.org>. Ensure that the applicable routing is configured when an NTP server is used.

4. Click *Apply* to apply the changes, then select *OK* in the confirmation dialog box. You may need to log in again after changing the time.

# Deploy Decoy VM

The *Deception* menu allows you to deploy Decoy VMs on your network. When a hacker gains unauthorized access to the Decoy VMs, their movements can be monitored to understand how they attack the network.

## To use FortiDeceptor to monitor the network:

1. Go to *Deception > Deception OS* to check the Deception OS available. See [View Available Deception OS on page 11](#)
2. Go to *Deception > Deployment Network* to Auto-Detect or specify the network where the Decoy VMs will be deployed. See [Set up the Deployment Network on page 11](#)
3. Go to *Deception > Deployment Wizard* to deploy the Decoy VM on the network. See [Deploy Decoy VMs with the Deployment Wizard on page 12](#)
4. Go to *Deception > Decoy & Lure Status* to see the Decoy VM deployed, start, stop, or download the FortiDeceptor Token Package to manually install on computers. See [Monitor Decoy & Lure Status on page 15](#)
5. Go to *Deception > Decoy Map* to see the network of Decoy VMs. See [View the Decoy Map on page 16](#)
6. Go to *Deception > Whitelist* to specify the network that is to be considered safe. This is useful if the administrator wants to log into the deployment network and not be flagged as an attacker. See [Configure a Whitelist on page 17](#)

## View Available Deception OS

The Deception OS available for creating Decoy VMs is shown on the *Deception OS* page. The following information is shown:

Column	Description
Status	Shows if the Deception OS is <i>Initialized</i> or <i>Not Initialized</i> .
Name	Name of the Deception OS.
OS Type	Shows the Operating System type (Ubuntu or Windows 7).
VM Type	Shows if the Deception OS is a Linux or a Windows endpoint.
Services	Shows the services used by the Decoy VM (SSH, SAMBA, SMB, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, Guardian-AST or IEC104).

## Set up the Deployment Network

The *Deployment Network* page allows administrators to set up a monitoring interface into a VLAN or a subnet.

**To add a VLAN or subnet to FortiDeceptor:**

1. Select *Deception > Deployment Network*.
2. Select *Auto VLAN Detection* to automatically detect the VLANs on your network. Auto VLAN detection allows FortiDeceptor to detect the available VLANs on the deployment network interface and display them in the GUI. You can select and add the VLANs for the deployment of Decoys later.
3. Select the Detection Interface. You can select multiple ports from Port 2 to Port 8. Click *OK*.
4. Click *Add New VLAN/Subnet* to manually add a VLAN or a subnet to FortiDeceptor. Configure the following settings:

<b>Interface</b>	The port that will connect to the VLAN or subnet.
<b>VLAN ID</b>	Specify an integer to assign a unique ID to the VLAN.
<b>Deception Monitor IP/Mask</b>	Specify an IP address to monitor. This is useful to mask the actual IP address.
<b>Ref</b>	Shows the number of objects referring to this object.
<b>Status</b>	Shows if the IP address is initialized.
<b>Action</b>	Click <i>Edit</i> to edit the VLAN or Subnet entry. The <i>Edit</i> button is visible only after the entry is saved.

5. Click *Save*.



The Monitor IP/Mask must be set as an IP address and not as a subnet.

You must use the following guidelines to set the Monitored IP/Mask:

- Interface name and VLAN ID is unique among all Monitored IP/Mask.
- If VLAN ID is 0, the Monitored IP/Mask is unique among all the Monitored IP/Mask without VLAN and all system interfaces.
- If VLAN is not 0, the Monitored IP/Mask is unique among all subnets in the same VLAN.

## Deploy Decoy VMs with the Deployment Wizard


The Deployment Wizard allows you to create and deploy Decoy VMs on your network. These Decoy VMs appear as real endpoints to the hacker and can collect valuable information about attacks.

**To deploy Decoys on the network:**

1. Go to *Deception > Deployment Wizard*.
2. Click + to add a Decoy VM.
3. Configure the following:

<b>Name</b>	Specify the name of the deployment profile in 1-15 characters. A-Z, a-z, 0-9, dash or underscore allowed. Cannot be duplicate of the existing profile name.
<b>Available Deception OSEs</b>	Select a Deception OS. Windows, Ubuntu VM or SCADA are available.
<b>Selected Services</b>	The selected services are shown. This field is not editable.

4. Set SSH or SAMBA to *ON* for an Ubuntu VM. Set RDP or SMB to *ON* for Windows. Set HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST or IEC104 to *ON* for SCADA.
5. Click + *Add Lure* for the respective service and configure the following:

<b>Username</b>	Specify the username for the decoy in 1-19 characters. <i>A-Z</i> , <i>a-z</i> , or <i>0-9</i> , allowed.
	 <p>The user name of the lures should not be the existing user name in the decoy, such as <i>administrator</i> for RDP/SMB services on Windows, or <i>root</i> for SSH/SAMBA services on Linux.</p>
<b>Password</b>	Specify the password for the decoy in 1-14 non-unicode characters.
<b>Sharename</b>	Specify a Sharename in 3-63 characters. <i>A-Z</i> , <i>a-z</i> , or <i>0-9</i> , allowed. This option is only available for SAMBA (Ubuntu) or SMB (Windows).
<b>Update or Cancel</b>	Click <i>Update</i> to save the username and password. Click <i>Cancel</i> to discard the username and password. Click <i>Delete</i> to delete an existing lure.

6. Repeat step 5 to add more decoys.
7. Switch *Launch Immediately* to *ON* to launch the Decoy VMs.
8. Switch *Reset Decoy* to *ON* to reset the decoy VM once incidents are detected.
9. Input the *Reset interval* value in seconds.
10. Click *Next*.
11. Specify the *Hostname* in 1-15 characters. The hostname can start with English characters/digits, and must not end with a hyphen. It may contain only the ASCII letters *a* through *z* (in a case-insensitive manner), the digits *0* through *9*, and the hyphen ('-'). No other symbols, punctuation characters, or white space are permitted. Hostname cannot conflict with existing Decoy names.
12. Click *Add Interface*.
13. In the *Add Interface for Decoy* screen, use the drop down menu to select the *Deploy Interface*. This should be set to the VLAN or Subnet added in [Set up the Deployment Network on page 11](#)
14. Configure the following settings in the Add Interface for Decoy VM screen:

<b>Addressing Mode</b>	Select <i>Static</i> or <i>DHCP</i> . Selecting Static will allow you to configure the IP address for all the decoys. Selecting DHCP will enable the decoys to receive IP address from the DHCP server.
<b>Network Mask</b>	The network mask is shown automatically.
<b>Gateway</b>	Specify the gateway.
<b>IP Count</b>	Specify the number of IP address to be assigned. The maximum per Decoy VM is 16 IPs. IP count will automatically switch to 1 if the addressing mode is DHCP.
<b>Min</b>	The minimum IP address in the IP range.
<b>Max</b>	The maximum IP address in the IP range.
<b>IP Ranges</b>	Specify the IP range between <i>Min</i> and <i>Max</i> .

15. Click *Done*.

16. Click *Template* to save as a template. The template is visible with the Profile Name in *Deception > Deploy Wizard*.
17. Click *Deploy* to deploy the decoys on the network.

## Deploy the FortiDeceptor Token Package

A FortiDeceptor Token Package is used to add breadcrumbs on real endpoints and lure an attacker to a Decoy VM. Tokens are normally distributed within the real endpoints and other IT assets on the network to maximize the deception surface.



The saved view is associated with the administrator login and will remain saved, including after logging in and out, until the view is reset.

---

### To download and deploy a FortiDeceptor Token Package on an existing endpoint:

1. Go to *Deception > Decoy & Lure Status*.
2. Select the Decoy VM(s) by clicking the appropriate check boxes. The topmost check box will select all VMs.
3. Click *Download Package* to download the FortiDeceptor Token Package. Packages can only be downloaded from Deceptions VMs with valid IPs. They must also be in one of the following statuses: *Initialized*, *Stopped*, *Running*, or *Failed*.
4. Copy the FortiDeceptor Token Package to an endpoint (Windows or Linux).
5. Unzip the FortiDeceptor Token Package:
  - For Windows, copy the file under the *Windows* directory and execute the *windows\_token.exe* by double-clicking the file.
  - For Ubuntu, open Terminal and execute *python ./ubuntu\_token.py*.

Once the FortiDeceptor Token Package is installed on a real Windows or Ubuntu endpoint, it increases the deception surface and lures the attacker to a Decoy VM.

### To uninstall a FortiDeceptor Token Package:

1. Go to *Deception > Decoy & Lure Status*.
2. Select the Decoy VM.
3. Click *Download Package* to download the FortiDeceptor Token Package.
4. Copy the FortiDeceptor Token Package to the endpoint (Windows or Linux).
5. Unzip the FortiDeceptor Token Package:
  - For Windows, copy the file under the *Windows* directory and execute the *uninstall.exe* by double-clicking the file.
  - For Ubuntu, open Terminal and execute *ubuntu/uninstall.py*.

## Monitor Decoy & Lure Status

The *Decoy & Lure Status* page shows the status of the decoys deployed on your network.

### To view the Deception Status:

1. Go to *Deception > Decoy & Lure Status*.
2. The following information is shown:

<b>Action</b>	Click <i>View</i> to view details of the decoy. Click <i>Start</i> or <i>Stop</i> to start or stop the decoy. Click <i>Delete</i> to delete the decoy.
<b>Status</b>	The current status of the decoy is shown as <i>Running</i> , <i>Stopped</i> , or <i>Cannot Start</i> . If the Decoy VM cannot start, hover over the VM to see the reason for failure to start.
<b>Name</b>	Name of the decoy.
<b>OS</b>	Operating system of the decoy whether <i>Ubuntu</i> or <i>Windows</i> .
<b>VM</b>	The name of the Decoy VM.
<b>Enabled Decoys</b>	The number of decoys enabled on this VM.
<b>IP</b>	The IP address of the Decoy VM.
<b>Services</b>	List of Services enabled. Mouse hovering displays a text list.
<b>Network Type</b>	Shows if the IP address is <i>Static</i> or <i>Dynamic</i> .
<b>DNS</b>	Shows the DNS.
<b>Gateway</b>	Shows the gateway.

### To delete one or more Decoy VMs:

1. Go to *Deception > Decoy & Lure Status*.
2. Select the Decoy VM.
3. Click *Delete*.
4. Click *OK*.

### To start one or more Decoy VM:

1. Go to *Deception > Decoy & Lure Status*.
2. Select one or more Decoy VMs that are stopped.
3. Click *Start*.

### To stop one or more Decoy VMs:

1. Go to *Deception > Decoy & Lure Status*.
2. Select one or more Decoy VMs that are running.
3. Click *Stop*.



It is recommended to operate the Decoy VMs with the same status for expected behavior.

---

## View the Decoy Map

The Decoy Map page is a visual representation of the entire network showing real endpoints and Decoy VMs.

### To view the details of the node in the Decoy Map:

1. Go to *Deception > Decoy Map*.
2. Click the node.
3. A dialog with the following information is shown:
  - IP
  - DNS
  - Gateway
  - OS
  - Status

### To search for information about a node in the Decoy Map:

1. Click the *Search* field.
2. Enter the name, IP address or VLAN ID of the node.

### To change the mode:

1. Go to *Deception > Decoy Map*.
2. Click *Modes* from the bottom taskbar.
3. Select one of the following options:
  - *Pick and Pin*
  - *Hide Labels*
  - *Dark Mode*

### To reset the Decoy Map to the default settings:

Click *Reset*.

### To pause the visual representation of ongoing activity:

Click *Pause*.



**To change display options:**

1. Click *Options*. Configure one of the following options:
  - *Zoom controls* - select the check box to show zoom controls on the Decoy Map.
  - *Node distance* - drag the slider to set the distance between nodes.
  - *Edge distance* - drag the slider to set the distance between the edges of nodes.

## Configure a Whitelist

The Whitelist page is used to add an IP address that can be used by an administrator to log into the network. Actions of the users from a whitelisted IP address will not be recorded as an *Event* or *Incident* by FortiDeceptor.

**To add a new whitelist IP:**

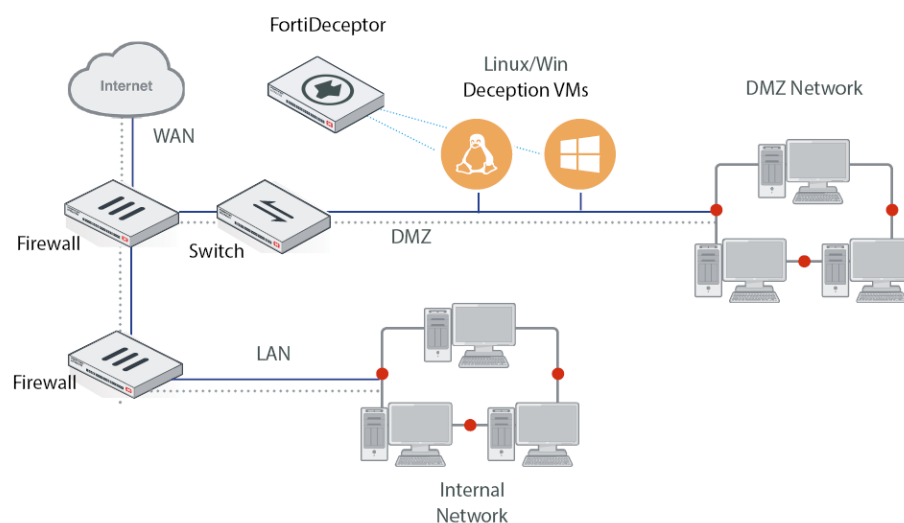
1. Go to *Deception > Whitelist*.
2. Click *Add New Whitelist IP*.
3. Configure the following settings:

<b>IP Address</b>	Specify the IP address from where the connection originates. This field is mandatory.
<b>Source Port</b>	Specify the source port from where the connection originates.
<b>Destination Port</b>	Specify the destination port on the network where the connection terminates.
<b>Description</b>	Specify a description. For example, you can name it as <i>Safe_Network</i> .
<b>Services</b>	Select the name of the services used to connect to the network.
<b>Status</b>	Select <i>Enabled</i> or <i>Disabled</i> .

4. Click *Update*.

## DMZ Mode

Deploy a FortiDeceptor hardware unit or VM in the Demilitarized Zone (DMZ) network. Attacks on the DMZ network can be monitored when FortiDeceptor is installed in the DMZ network.



### To enable DMZ mode:

Go to the command line and specify the following command:

```
dmz-mode enable
```



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

## Limitations of the DMZ Mode

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

- When DMZ mode is enabled, the label *DMZ-MODE* is shown on the top banner.
- In the Deployment Network view, Deception Monitor IP/Mask is hidden when in DMZ Mode. See [Set up the Deployment Network on page 11](#) for more information about Deception IP/Mask.
- Under Deception Status view, the Attack Test selection is disabled.
- When DMZ mode is enabled, Decoy VMs are limited to 1 Deploy Interface. See [Deploy Decoy VMs with the Deployment Wizard on page 12](#) for more information about IP address range.

# Monitor Attacks

Administrators can monitor the Attacks in two ways:

## To monitor Attacks from the Incident Menu:

- Analysis page lists the *Incidents* (related *Events*) detected by FortiDeceptor. See [Analysis on page 19](#)
- Campaign page lists the Attacks (related *Events*) detected by FortiDeceptor. See [Campaign on page 20](#)

## To monitor Attacks from the Widgets:

- Incidents and Events Distribution widget. See [Incidents and Events Distribution on page 22](#).
- Incidents and Events Count widget. See [Incidents and Events Count on page 22](#).

## Analysis

The *Analysis* page lists the *Incidents* detected by FortiDeceptor. The detailed Analysis report can be downloaded from the *Export to PDF* option.

## To see the list of Events:

1. Go to *Incident > Analysis*.
2. The following information is shown:

<b>Severity</b>	Severity of the Event is shown as Critical, High, Medium, Low, or Unknown.
<b>Last Activity</b>	Date and time of the last activity.
<b>Type</b>	Type of Event.
<b>Attacker IP Mask</b>	IP mask of the attacker.
<b>Attacker User</b>	User name of the attacker.
<b>Victim IP</b>	IP address of the victim.
<b>Start</b>	Date and time when the attack started.
<b>Attacker Port</b>	Port from where the attack originated.
<b>Attacker Type</b>	The Attacker type is shown as <i>Unknown</i> , <i>Connection</i> , <i>Interaction</i> , or <i>Reconnaissance</i> .
<b>Victim Port</b>	Port of the victim.
<b>Attacker Password</b>	Password used by the attacker.

<b>Download File</b>	Download the PCAP files or dumped files, if the Decoy VM captured network traffic or files.
<b>Timeline</b>	Click <i>Timeline</i> to see the entire timeline of all the <i>Incidents</i> from start to finish.
<b>Table</b>	Click <i>Table</i> to see all the <i>Incidents</i> in a table view.

#### To refresh the data:

Click *Refresh* to refresh the data.

#### To export to PDF:

1. Click *Export to PDF*.
2. Click *OK* to save the PDF.

#### To mark all items as read:

Newly detected incidents will be displayed in bold to indicate as unread. The rows can be marked as read by expanding the Incident details or by clicking the *Mark all as read* button.

#### Show Options:

The radio buttons beside the *Show* label are as follows: *All* to display all incidents and Events, *IPS Events Only* to display all incidents with IPS events, *Web Filter Events Only* to display all incidents with Web Filter events. When the *IPS Events Only* and *Web Filter Events Only* radio buttons are selected, no other types of incidents will be displayed until the *All* radio button is re-selected.

## Campaign

The *Campaign* page lists the *Attacks* detected by FortiDeceptor. An *Attack* consists of multiple *Incidents*. The detailed Campaign report can be downloaded from the *Export to PDF* option.

#### To see the list of Attacks:

1. Go to *Incident > Campaign*.
2. The following information is shown:

<b>Severity</b>	Severity of the <i>Attack</i> is shown as Critical, High, Medium, Low, or Unknown.
<b>Last Activity</b>	Date and time of the last activity.
<b>Start</b>	Date and time when the attack started.
<b>Attacker IP</b>	IP mask of the attacker.
<b>ID</b>	ID of the campaign record.

<b>Screenshot</b>	Screenshot of the attack in progress.
<b>Timeline</b>	Click <i>Timeline</i> to see the entire timeline of the <i>Attack</i> from start to finish.
<b>Table</b>	Click <i>Table</i> to see all the <i>Events</i> in a table view.

#### To refresh the data:

Click *Refresh* to refresh the data.

#### To export to PDF:

1. Click *Export to PDF*.
2. Click *OK* to save the PDF.

## Attack Map

The *Attack Map* page is a visual representation of the entire network showing real endpoints, Decoy VMs, and ongoing attacks.

#### To change filtering arguments:

1. Go to *Incident > Attack Map*.
2. At the bottom of the Attack Map, drag the timestamp indicator to identify a start and end time. Move the left red arrow to change the start time, move the right red arrow to change the end time.
3. Click the *Filter Input* box to choose a different filter type and type values.

You can input multiple arguments with different filter types. All the filter arguments and the time indicator arguments are considered "AND" conditions.

The filter types are as follows:

- Attacker IP
- Victim IP
- Decoy VM IP

#### To locate the node in the map:

In the *LOCATE* box on the right, type the IP address, and press Enter.

#### To save a snapshot of the map:

Click the *Save View*  button.



The saved view is associated with the administrator login and will remain saved, including after logging in and out, until the view is reset.

### To change display options:

Scroll the mouse to zoom in and out on the Attack Map.

## Incidents and Events Distribution

This widget displays the number of Incidents and Events with the following risk level information and options:

<b>Unknown</b>	Shows the <i>Incident</i> or <i>Event</i> where the risk level is unknown. The entries are shown in grey color.
<b>Low Risk</b>	Shows the <i>Incident</i> or <i>Event</i> where the risk level is low. The entries are shown in green color.
<b>Medium Risk</b>	Shows the <i>Incident</i> or <i>Event</i> where the risk level is medium. The entries are shown in yellow color.
<b>High Risk</b>	Shows the <i>Incident</i> or <i>Event</i> where the risk level is high. The entries are shown in orange color.
<b>Critical</b>	Shows the <i>Incident</i> or <i>Event</i> where the risk level is critical. The entries are shown in orange color.



Hover over the pie chart to see the number of *Incidents* or *Events* and their percentage. Click the edit icon and select a time period to be displayed from the drop-down list. The options are: *Last 24 hours*, *Last 7 days*, *Last 4 weeks*.

## Incidents and Events Count

This widget displays the number of Incidents and Events occurring each day:

<b>Event</b>	Click <i>Event</i> to see the number of events occurring each day. The events are shown in blue color.
<b>Incidents</b>	Click <i>Incident</i> to see the number of incidents occurring each day. The incidents are shown in orange color.
<b>Day/Date</b>	Shows the day or date the <i>Incident</i> or <i>Event</i> occurred.



Click the edit icon and select a time period to be displayed from the drop-down list. The options are: *Last 24 hours*, *Last 7 days*, *Last 4 weeks*.

## Top 10 Attackers by Events

This widget displays the top 10 attackers by the number of Events:

<b>IP Address</b>	Shows the IP address of the attacker.
<b>Number of Events</b>	Hover over the graph for the particular IP address to see the total number of <i>Events</i> .

## Top 10 Attackers by Incidents

This widget displays the top 10 attackers by the number of Incidents:

<b>IP Address</b>	Shows the IP address of the attacker.
<b>Number of Incidents</b>	Hover over the graph for the particular IP address to see the total number of <i>Incidents</i> .

## Top 10 IPS Attacks

This widget displays the top 10 IPS attacks by the number of attack events:

<b>IPS attack name</b>	Show the name of IPS attack name.
<b>Number of attack events</b>	Hover over the graph for the particular IPS attack name to see the total number of attack events.

## Incidents Distribution by Service

This dashboard widget displays the number of *Incidents* by service with the following information and options:

<b>SSH</b>	Shows the number of incidents occurring on SSH service with the percentage on a pie chart.
<b>SAMBA</b>	Shows the number of incidents occurring on SAMBA service with the percentage on a pie chart.
<b>SMB</b>	Shows the number of incidents occurring on SMB service with the percentage on a pie chart.
<b>RDP</b>	Shows the number of incidents occurring on RDP service with the percentage on a pie chart.

<b>HTTP</b>	Shows the number of incidents occurring on HTTP service with the percentage on a pie chart.
<b>FTP</b>	Shows the number of incidents occurring on FTP service with the percentage on a pie chart.
<b>TFTP</b>	Shows the number of incidents occurring on TFTP service with the percentage on a pie chart.
<b>SNMP</b>	Shows the number of incidents occurring on SNMP service with the percentage on a pie chart.
<b>MODBUS</b>	Shows the number of incidents occurring on MODBUS service with the percentage on a pie chart.
<b>S7COMM</b>	Shows the number of incidents occurring on S7COMM service with the percentage on a pie chart.
<b>BACNET</b>	Shows the number of incidents occurring on BACNET service with the percentage on a pie chart.
<b>IPMI</b>	Shows the number of incidents occurring on IPMI service with the percentage on a pie chart.
<b>TRICONEX</b>	Shows the number of incidents occurring on TRICONEX service with the percentage on a pie chart.
<b>GUARDIAN-AST</b>	Shows the number of incidents occurring on GUARDIAN-AST service with the percentage on a pie chart.
<b>IEC104</b>	Shows the number of incidents occurring on IEC104 service with the percentage on a pie chart.



Hover over the pie chart to see the percentage. Click the pie chart to split the particular service from the chart.

## Global Attacker Distribution

This widget displays the number of *Attackers* by country on a global map.



Hover over each country to see the number of Attackers from each country.



# Fabric

The *Fabric* tree menu enables you to manage and configure FortiGate information for integration with FortiDeceptor. This includes blocking settings and Security Fabric status information. Blocking from FortiGate is an API call from FortiDeceptor which allows instant quarantine from FortiGate once an incident is detected. The quarantined IP can be found under user quarantine in the FortiGate GUI.

The *Fabric* menu provides access to the following menus:

FortiGate Integration	Configure the FortiGate settings for FortiDeceptor integration.
Quarantine Status	Display the status of blocked IP addresses.
IOC Export	Export the IOC file in CSV format for a specified time period.

## Blocking

The *FortiGate Integration* menu allows you to configure FortiGate settings for integration with FortiDeceptor. The following options are available:

Add new block configuration	Select to create a new FortiGate integration setting.
Update	Save the modified FortiGate integration setting to a configuration file.
Cancel	Discard current change.
Edit	Allows you to edit the record.
Delete	Deletes the record after prompting.
Test	Manually send out the quarantine request to corresponding FortiGate.

The following information is displayed:

Name	The alias name for the integrated FortiGate.
IP	Mandatory option. The IP address of the integrated FortiGate.
User	Mandatory option. The login user of the integrated FortiGate.
Password	Password for the login user of the integrated FortiGate.
Port	The port number of integrated FortiGate REST API service. Default port number is 443.
Default Expiry	The default blocking time in second. Default is 3600 seconds.
Default VDOM	The default access VDOM of integrated FortiGate.
Type	FortiGate (read only value).
Enabled	Enable or disable the integration setting.

## Quarantine Status

The *Quarantine Status* menu displays the status of blocking/quarantine IP addresses. It also lets you manually block/unblock devices. Following options are available:

Refresh	Refresh the page to get latest data.
Block	Manually send a blocking request for the selected attacker IP addresses in the table.
Unblock	Manually send an unblocking request for the selected attack IP addresses in the table.

The following information is displayed:

Attacker IP	The IP addresses of blocked attacker.
Start	The start time of blocking behavior.
End	The end time of blocking behavior.
Handler Address	The IP address of the integrated FortiGate.
Handler	The integrated device type.
Handle Type	The blocking type, manual or automatic quarantine.
Time to Live	The blocking time period.
Status	The current status of the attacker.
Message	The related message for the blocking entry.

## IOC Export

The IOC Export function exports the IOC file in CSV format for a specified time period. The CSV file can be processed by third party Threat Intelligence Platforms. The file contains the TimeStamp, Incident time, Attacker IP, related files and WCF (Web Content Filtering) events. The export configuration includes MD5 checksums, WCF category and Reconnaissance Alerts.

# System

The *System* tree menu enables you to manage and configure the basic system options for the FortiDeceptor unit. This includes administrator configuration, mail server settings, and maintenance information.

The *System* menu provides access to the following menus:

<b>Administrators</b>	Configure administrator user accounts.
<b>Admin Profile</b>	Configure user profiles to define user privileges.
<b>Certificates</b>	Configure CA certificates.
<b>LDAP Servers</b>	Configure LDAP Servers.
<b>RADIUS Servers</b>	Configure RADIUS Servers.
<b>Mail Server</b>	Configure the Mail Server.
<b>SNMP</b>	Configure SNMP.
<b>Login Disclaimer</b>	Configure the Login Disclaimer.
<b>Settings</b>	Configure the idle timeout value for the GUI and CLI interface and GUI language. You can also toggle left-side menu mode and reset all widgets to their default state.
<b>Table Customization</b>	Define columns and orders of <i>Incident</i> and <i>Event</i> tables.

This section includes the following topics:

- [Administrators](#)
- [Admin Profiles](#)
- [Certificates](#)
- [LDAP Servers](#)
- [RADIUS Servers](#)
- [Mail Server](#)
- [SNMP](#)
- [FortiGuard](#)
- [Login Disclaimer](#)
- [Settings](#)

## Administrators

The *Administrators* menu allows you to configure administrator user accounts.

If the user whose Admin Profile does not have *Read Write* privilege under *System > Admin access*, the user will only be able to view and edit its own information.

The following options are available:

<b>Create New</b>	Select to create a new administrator account.
<b>Edit</b>	Select an administrator account from the list and select <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select an administrator account from the list and select <i>Delete</i> in the toolbar to delete the entry.
<b>Test Login</b>	Select a LDAP/RADIUS administrator account from the list and select <i>Test Login</i> to test the user's login settings. If an error occurs, a detailed debug message will display.

The following information is displayed:

<b>Name</b>	Displays the administrator account name.
<b>Type</b>	The administrator type: <ul style="list-style-type: none"><li>• Local</li><li>• LDAP</li><li>• RADIUS</li></ul>
<b>Profile</b>	The Admin Profile the user belongs to.

**To create a new user:**

1. Log in as a user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.
2. Select + *Create New* from the toolbar.

3. Configure the following:

<b>Administrator</b>	Enter a name for the new administrator account. The administrator name must be 1 to 30 characters long and may only contain upper-case letters, lower-case letters, numbers, and the underscore character <code>_</code> .
<b>Password</b>	Enter a password for the account. The password must be 6 to 64 characters long and may contain upper-case letters, lower-case letters, numbers, and special characters. This field is available when <i>Type</i> is set to <i>Local</i> .
<b>Confirm Password</b>	Confirm the password for the account. This field is available when <i>Type</i> is set to <i>Local</i> .
<b>Type</b>	Select either Local, LDAP, or RADIUS.
<b>LDAP Server</b>	When <i>Type</i> is <i>LDAP</i> , select the LDAP server from the drop-down list. For information on creating an LDAP server, see <a href="#">LDAP Servers on page 34</a> .
<b>RADIUS Server</b>	When <i>Type</i> is <i>RADIUS</i> , select the RADIUS server from the drop-down list. For information on creating a RADIUS server, see <a href="#">RADIUS Servers</a> .
<b>Admin Profile</b>	Select the Admin Profile the user belongs to.
<b>Trusted Host 1, Trusted Host 2, Trusted Host 3</b>	Enter up to three IPv4 trusted hosts. Only users from trusted hosts can access FortiDeceptor.
<b>Trusted IPv6 Host 1, Trusted IPv6 Host 2, Trusted IPv6 Host 3</b>	Enter up to three IPv6 trusted hosts. Only users from trusted hosts can access FortiDeceptor.
<b>Comments</b>	Enter an optional description comment for the administrator account.



Setting trusted hosts for administrators limits what computers an administrator can use to log into the FortiDeceptor unit. When you identify a trusted host, the FortiDeceptor unit will only accept the administrator's login from the configured IP address or subnet. Any attempt to log in with the same credentials from any other IP address or any other subnet will be dropped.

4. Select *OK* to create the new user.

**To edit a user account:**

1. Log in as a user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.
2. Select the name of the user you would like to edit and select *Edit* from the toolbar.
3. Edit the account as required and then re-type the new password in the confirmation field.
4. Click *OK* to apply the changes.



When editing the *admin* account, you will be required to type the old password before you can set a new password.



Only the *admin* user can edit its own settings.

#### To delete one or more user accounts:

1. Log in as a user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.
2. Select the user account you want to delete.
3. Select *Delete* from the toolbar.
4. Select *Yes, I'm sure* in the confirmation page to delete the selected user or users.

#### To test LDAP/RADIUS logins:

1. Log in as a user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.
  2. Select an LDAP/RADIUS user to test.
  3. Select *Test Login* from the toolbar.
  4. In the dialog box, enter the user's password.
  5. Click *OK*.
- If an error occurs, a detailed debug message will appear.



When a remote RADIUS server is configured for two-factor authentication, RADIUS users must enter a FortiToken pin code or the code from email/SMS to complete login. For example, after the user clicks *Login*, the user must enter the code, and click *Submit* to complete the login.

A pin code is also needed for the test login page.

## Admin Profiles

Administrator profiles are used to control administrator access privileges to system features. Profiles are assigned to administrator accounts when an administrator is created.

There are two predefined administrator profiles, which cannot be modified or deleted:

- Super Admin: All functionality is accessible
- Read only: Functionality is Read Only

Only the Super Admin user can create, edit, and delete administrator profiles. New users can create, edit, and delete administrator profiles if they are assigned the *Read Write* privilege in *System > Admin Profiles* page.

#### Settings for Menu Access:

**None**

The user cannot view or make changes to the system.

<b>Read only</b>	The user can view but not make any change to the system, except the session related user settings such as Table Customization/Dashboard/Attack Map filter
<b>Read Write</b>	The user can view and make changes to the system.

### Settings for CLI Commands:

<b>Execute</b>	User can execute the CLI command.
<b>None</b>	User cannot execute the CLI command.

### To create a new Administrator Profile:

1. Go to *System > Admin Profiles*.
2. Click *Create New*.
3. Specify the *Profile Name*.
4. Add a *Comment*.
5. Specify the privileges for the Menu Access. Select *None* or *Read Write* for the following features:
  - Dashboard
    - Dashboard
  - Deception
    - Deception OS
    - Deployment Network
    - Deployment Wizard
    - Decoy & Lure Status
    - Decoy Map
    - Whitelist
  - Incident
    - Analysis
    - Campaign
    - Attack Map
  - Fabric
    - FortiGate Integration
    - Quarantine Status
    - IOC Export
  - Network
    - Interfaces
    - System DNS
    - System Routing
  - System
    - Administrators
    - Admin Profiles
    - Certificates
    - LDAP Servers
    - RADIUS Servers
    - Mail Server

- SNMP
- FortiGuard
- Settings
- Login Disclaimer
- System Settings
- Table Customization
- test-network
- fdn-pkg
- Log
  - All Events
  - Log Servers

6. Specify the privileges for the CLI Commands. Select *None* or *Read Write* for the following features:

- Configuration
  - Set
  - Unset
- System
  - Reboot
  - Shutdown
  - Reset Configuration
  - Factory Reset
  - Firmware Upgrade
  - Reset Widgets
  - IP Tables
  - test-network
  - usg-license
  - Upload VM Firmware License
  - Resize VM Hard Disk
  - Set Confirm ID for Windows VM
  - List VM License
  - Show VM Status
  - VM reset
  - DC Image Status
  - Set Maintainer
  - Set Timeout for Remote Auth
  - Data Purge
  - Log Purge
  - DMZ Mode
  - fdn-pkg
- Utilities
  - TCP Dump
  - Trace Route
- Diagnostics
  - Disk Attributes
  - Disk Errors



- Disk Health
- Disk Info
- Raid Hardware Info

7. Click **Save**.

## Certificates

In this page you can import, view, and delete certificates. Certificates are used for secure connection to an LDAP server, system HTTPS and SSH services. The FortiDeceptor has one default certificate *firmware*, which means the certificate is installed on the unit by Fortinet.



FortiDeceptor does not support generating certificates, but importing certificates for SSH and HTTPS access to FortiDeceptor. `.crt`, `PKCS12`, and `.pem` formats are supported.

The following options are available:

<b>Import</b>	Import a certificate.
<b>Service</b>	Select to configure specific certificates for the HTTP and SSH servers.
<b>View</b>	Select a certificate in the list and select <i>View</i> in the toolbar to view the CA certificate details.
<b>Delete</b>	Select a certificate in the list and select <i>Delete</i> in the toolbar to delete the certificate.

The following information is displayed:

<b>Name</b>	The name of the certificate.
<b>Subject</b>	The subject of the certificate.
<b>Status</b>	The certificate status, active or expired.
<b>Service</b>	HTTPS or SSH service that is using this certificate.

### To import a certificate:

1. Go to *System > Certificates*.
2. Select *Import* from the toolbar.
3. Enter the certificate name in the text field.
4. Select *Choose File* and locate the certificate and key files on your management computer.
5. Select *OK* to import the certificate.



Users have the option to import a Password Protected PKCS12 Certificate. To import a PKCS12 Certificate, check the *PKCS12 Format* box upon importing a new certificate and writing down possible password.

**To view a certificate:**

1. Go to *System > Certificates*.
2. Select the certificate from the list and select *View* from the toolbar.
3. The following information is available:

<b>Certificate Name</b>	The name of the certificate.
<b>Status</b>	The certificate status.
<b>Serial number</b>	The certificate serial number.
<b>Issuer</b>	The issuer of the certificate.
<b>Subject</b>	The subject of the certificate.
<b>Effective date</b>	The date and time that the certificate became effective.
<b>Expiration date</b>	The date and time that the certificate expires.

4. Select *OK* to return to the Certificates page.

**To delete a CA certificate:**

1. Go to *System > Certificates*.
2. Select the certificate from the list and select *Delete* from the toolbar.
3. Select *Yes, I'm sure* in the *Are You Sure* confirmation page.



*Firmware* certificate(s) cannot be deleted.

## LDAP Servers

The FortiDeceptor system supports remote authentication of administrators using LDAP servers. To use this feature, you must configure the appropriate server entries in the FortiDeceptor unit for each authentication server in your network.

If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiDeceptor unit contacts the LDAP server for authentication. To authenticate with the FortiDeceptor unit, the user enters a user name and password. The FortiDeceptor unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the FortiDeceptor unit successfully authenticates the user. If the LDAP server cannot authenticate the user, the FortiDeceptor unit refuses the connection.

The following options are available:

<b>Create New</b>	Select to add an LDAP server.
<b>Edit</b>	Select an LDAP server in the list and select <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select an LDAP server in the list and select <i>Delete</i> in the toolbar to delete the entry.

The following information is displayed:

<b>Name</b>	The LDAP server name.
<b>Address</b>	The LDAP server address.
<b>Common Name</b>	The LDAP common name.
<b>Distinguished Name</b>	The LDAP distinguished name.
<b>Bind Type</b>	The LDAP bind type.
<b>Connection Type</b>	The LDAP connection type.

**To create a new LDAP server:**

1. Go to *System > LDAP Servers*.
2. Select + *Create New* from the toolbar.
3. Configure the following settings:

<b>Name</b>	Enter a name to identify the LDAP server. The name should be unique to FortiDeceptor.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the LDAP server.
<b>Port</b>	Enter the port for LDAP traffic. The default port is 389.
<b>Common Name</b>	The common name identifier for the LDAP server. Most LDAP servers use <i>cn</i> . However, some servers use other common name identifiers such as <i>uid</i> .
<b>Distinguished Name</b>	The distinguished name used to look up entries on the LDAP servers. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
<b>Bind Type</b>	Select the type of binding for LDAP authentication. The following options are available: <ul style="list-style-type: none"> <li>• Simple</li> <li>• Anonymous</li> <li>• Regular</li> </ul>
<b>Username</b>	When the <i>Bind Type</i> is set to <i>Regular</i> , type the user name.
<b>Password</b>	When the <i>Bind Type</i> is set to <i>Regular</i> , type the password.
<b>Enable Secure Connection</b>	Select to use a secure LDAP server connection for authentication.
<b>Protocol</b>	When <i>Enable Secure Connection</i> is selected, select either LDAPS or STARTTLS.
<b>CA Certificate</b>	When <i>Enable Secure Connection</i> is selected, select the CA certificate from the drop-down list.

4. Select *OK* to add the LDAP server.

## RADIUS Servers

The FortiDeceptor system supports remote authentication of administrators using RADIUS servers. To use this feature, you must configure the appropriate server entries in the FortiDeceptor unit for each authentication server in your network.

If you have configured RADIUS support and require a user to authenticate using a RADIUS server, the FortiDeceptor unit contacts the RADIUS server for authentication. To authenticate with the FortiDeceptor unit, the user enters a user name and password. The FortiDeceptor unit sends this user name and password to the RADIUS server. If the RADIUS server can authenticate the user, the FortiDeceptor unit successfully authenticates the user. If the RADIUS server cannot authenticate the user, the FortiDeceptor unit refuses the connection.

The following options are available:

<b>Create New</b>	Select to add a RADIUS server.
<b>Edit</b>	Select a RADIUS server in the list and select <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select a RADIUS server in the list and select <i>Delete</i> in the toolbar to delete the entry.

The following information is displayed:

<b>Name</b>	The RADIUS server name.
<b>Primary Address</b>	The primary server IP address.
<b>Secondary Address</b>	The secondary server IP address.
<b>Port</b>	The port used for RADIUS traffic. The default port is 1812.
<b>Auth Type</b>	The authentication type the RADIUS server requires. The default setting of ANY has the FortiDeceptor try all the authentication types. Select one of: <i>ANY</i> , <i>PAP</i> , <i>CHAP</i> , or <i>MSv2</i> .

### To add a RADIUS server:

1. Go to *System > RADIUS Servers*.
2. Select + *Create New* from the toolbar.

3. Configure the following settings:

<b>Name</b>	Enter a name to identify the RADIUS server. The name should be unique to FortiDeceptor.
<b>Primary Server Name/IP</b>	Enter the IP address or fully qualified domain name of the primary RADIUS server.
<b>Secondary Server Name/IP</b>	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
<b>Port</b>	Enter the port for RADIUS traffic. The default port is 1812.
<b>Auth Type</b>	Enter the authentication type the RADIUS server requires. The default setting of ANY has the FortiDeceptor try all the authentication types. Select one of: <i>ANY</i> , <i>PAP</i> , <i>CHAP</i> , or <i>MSv2</i> .
<b>Primary Secret</b>	Enter the primary RADIUS server secret.
<b>Secondary Secret</b>	Enter the secondary RADIUS server secret.
<b>NAS IP</b>	Enter the NAS IP address.

4. Select *OK* to add the RADIUS server.

## Mail Server

The Mail Server page allows you to adjust the mail server settings. Go to *System > Mail Server* to view the *Mail Server Settings* page. In this page you can configure notifications for malware detection and the weekly global email list.

The following options can be configured:

<b>Send Incidents Alerts</b>	Select to enable this feature. An email alert is sent to the <i>Receiver Email List</i> when an incident is detected.
<b>SMTP Server Address</b>	Enter the SMTP server address.
<b>Port</b>	Enter the SMTP server port number.
<b>E-Mail Account</b>	Enter the mail server email account. This will be used as the <i>from</i> address.
<b>Login Account</b>	Enter the mail server login account.
<b>Password</b>	Enter the password.
<b>Confirm Password</b>	Confirm the password.
<b>OK</b>	Select <i>OK</i> to apply any changes made to the mail server configuration.
<b>Send Test Email</b>	Select <i>Send Test</i> to send a test email to the global email list. If an error occurs, the error message will appear at the top of the page and be recorded in the System Logs.
<b>Reset</b>	Select <i>Reset</i> to restore the default mail server settings.

## SNMP

SNMP is a method for a FortiDeceptor system to monitor your FortiDeceptor system on your local computer. You will need an SNMP agent on your computer to read the SNMP information.

Using SNMP, your FortiDeceptor system monitors for system events including CPU usage, memory usage, log disk space, interface changes, and malware detection. Go to *System > SNMP* to configure your FortiDeceptor system's SNMP settings.

SNMP has two parts - the SNMP agent or the device that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on the monitored FortiDeceptor are hard coded and configured in the SNMP menu.

The FortiDeceptor SNMP implementation is read-only — SNMP v1, v2c, v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiDeceptor system information and can receive FortiDeceptor system traps.

From here you can also download FortiDeceptor and Fortinet core MIB files.

### Configure the SNMP agent

The SNMP agent sends SNMP traps that originate on the FortiDeceptor system to an external monitoring SNMP manager defined in one of the FortiDeceptor SNMP communities. Typically, an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiDeceptor system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiDeceptor system will be part of the information an SNMP manager will have. This information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiDeceptor system requires attention.

#### To configure SNMP agents:

1. Go to *System > SNMP* to configure the SNMP agent.
2. Configure the following settings:

<b>SNMP Agent</b>	Select to enable the FortiDeceptor SNMP agent. When this is enabled, it sends FortiDeceptor SNMP traps.
<b>Description</b>	Enter a description of this FortiDeceptor system to help uniquely identify this unit.
<b>Location</b>	Enter the location of this FortiDeceptor system to help find it in the event it requires attention.
<b>Contact</b>	Enter the contact information for the person in charge of this FortiDeceptor system.
<b>SNMP v1/v2c</b>	Create new, edit, or delete SNMP v1 and v2c communities. You can select to enable or disable communities in the edit page. The following columns are displayed: Community Name, Queries, Traps, Enable
<b>SNMP v3</b>	Create new, edit, or delete SNMP v3 entries. You can select to enable or disable queries in the edit page. The following columns are displayed: User Name, Security Level, Notification Host, Queries.

### To create a new SNMP v1/v2c community:

1. Go to *System > SNMP*.
2. In the SNMP v1/v2c section of the screen, select *Create New* from the toolbar.
3. Configure the following settings:

<b>Enable</b>	Select to enable the SNMP community.
<b>Community Name</b>	Enter a name to identify the SNMP community.
<b>Hosts</b>	The list of hosts that can use the settings in this SNMP community to monitor the FortiDeceptor system.
<b>IP/Netmask</b>	Enter the IP address and netmask of the SNMP hosts. Select the <i>Add</i> button to add additional hosts.
<b>Queries v1</b>	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiDeceptor system uses.
<b>Queries v2c</b>	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiDeceptor system uses.
<b>Traps v1</b>	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiDeceptor system uses.
<b>Traps v2c</b>	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiDeceptor system uses.
<b>SNMP Events</b>	Enable the events that will cause the FortiDeceptor unit to send SNMP traps to the community. <ul style="list-style-type: none"> <li>• CPU usage is high</li> <li>• Memory is low</li> <li>• Log disk space is low</li> <li>• Incident is detected</li> <li>• Power supply failure</li> </ul>

4. Select *OK* to create the SNMP community.

### To create a new SNMP v3 user:

1. Go to *System > SNMP*.
2. In the SNMP v3 section of the screen select *Create New* from the toolbar.

3. Configure the following settings:

<b>Username</b>	Enter the name of the SNMPv3 user.
<b>Security Level</b>	Select the security level of the user. Select one of the following: <ul style="list-style-type: none"> <li>• None</li> <li>• Authentication only</li> <li>• Encryption and authentication</li> </ul>
<b>Authentication</b>	Authentication is required when <i>Security Level</i> is either <i>Authentication only</i> or <i>Encryption and authentication</i> .
<b>Method</b>	Select the authentication method. Select either: <ul style="list-style-type: none"> <li>• MD5 (Message Digest 5 algorithm)</li> <li>• SHA1 (Secure Hash algorithm)</li> </ul>
<b>Password</b>	Enter the authentication password. The password must be a minimum of 8 characters.
<b>Encryption</b>	Encryption is required when <i>Security Level</i> is <i>Encryption and authentication</i> .
<b>Method</b>	Select the encryption method, either DES or AES.
<b>Key</b>	Enter the encryption key. The encryption key value must be a minimum of 8 characters.
<b>Notification Hosts (Traps)</b>	
<b>IP/Netmask</b>	Enter the IP address and netmask. Click the <i>Add</i> button to add additional hosts.
<b>Query</b>	
<b>Port</b>	Enter the port number. Select to <i>Enable</i> the query port.
<b>SNMP V3 Events</b>	Select the SNMP events that will be associated with that user. <ul style="list-style-type: none"> <li>• CPU usage is high</li> <li>• Memory is low</li> <li>• Log disk space is low</li> <li>• Incident is detected</li> <li>• Power supply failure</li> </ul>

4. Select *OK* to create the SNMP community.

## MIB files

To download MIB files, scroll to the bottom of the SNMP page, and select the MIB file that you would like to download to your management computer.



## FortiGuard

1. Go to *System > FortiGuard* to view the FortiGuard page.
2. The following options and information are available:

<b>Module Name</b>	The FortiGuard module name, including: AntiVirus Scanner, AntiVirus Extended Signature, AntiVirus Active Signature, AntiVirus Extreme Signature, IDS Engine, IDS Signature, Anti-Reconnaissance & Anti-Exploit Engine. All modules automatically install update packages when they are available on the FDN.
<b>Current Version</b>	The current version of the module.
<b>Release Time</b>	The time that module was released.
<b>Last Update Time</b>	The time that module was last updated.
<b>Last Check Status</b>	The status of the last update attempt.
<b>Upload Package File</b>	Select <i>Browse</i> to locate a package file on the management computer, then select <i>Submit</i> to upload the package file to the FortiDeceptor.  When the unit has no access to the Fortinet FDN servers, the user can go to the <a href="#">Customer Service and Support</a> site to download package files manually.
<b>FortiGuard Server Location</b>	Select FDN servers for package update and Web Filtering query. By default, the selection is <i>Nearest</i> , which means the closest FDN server according to the unit's time zone is used. When US Region is selected, only servers inside United States are used.
<b>FortiGuard Server Settings</b>	
<b>Use override FDN server to download module updates</b>	Select to enable an override FDN server, or FortiManager, to download module update, then enter the server IP address or FQDN in the text box. When an overridden FDN server is used, FortiGuard Server Location will be disabled.  Click <i>Connect FDN Now</i> button to schedule an immediate update check.
<b>Connect FDN Now</b>	Click the <i>Connect FDN Now</i> button to connect the override FDN server/Proxy.
<b>FortiGuard Web Filter Settings</b>	
<b>Use override server address for web filtering query</b>	Select to enable an override server address for web filtering query, then enter the server IP address (IP address or IP address:port) or FQDN in the text box. By default, the closest web filtering server according to the unit's time zone is used.  If port is not provided, target UDP port 53 will be used.

3. Click *Apply* to apply your changes.

## Login Disclaimer

Go to *System > Login Disclaimer* to customize the warning message, and to enable or disable the Login Disclaimer.

If enabled, the Login Disclaimer will appear when a user tries to log into the unit.

## Table Customization

**To customize the columns available for Incidents or Events:**

1. Go to *System > Table Customization*.
2. In the *Incident Columns* pane, drag and drop the columns from the *Available Column Headers* to the *Customized Column Headers and Orders*.
3. In the *Event Columns* pane, drag and drop the columns from the *Available Column Headers* to the *Customized Column Headers and Orders*.
4. In the *Table Settings* pane, specify the *Page Size* and select the *View Type*.
5. Click *Save* to save the setting.



Adjust the order of the columns in the *Customized Column Headers and Orders* as required.

---

## Settings

Go to *System > Settings* to configure idle timeout for the administrator account, which is the amount of time after which the user's login session will expire if there is no activity.

**To configure the idle timeout:**

1. Go to *System > Settings*.
2. Enter a value between 1 and 480 minutes.
3. Click *OK* to save the setting.

**To reset all widgets:**

You can reset all the widgets in the Dashboard by clicking the *Reset* button.

# System Settings

The System Settings explains the following topics:

- [Dashboard on page 43](#)
- [Basic System Settings on page 48](#)
- [Network on page 51](#)

## Dashboard

The System Status dashboard displays widgets that provide information and enable you to configure basic system settings. All of the widgets appear on a single dashboard, which can be customized as desired.

The following widgets are available:

<b>System Information</b>	Displays basic information about the FortiDeceptor system, such as the serial number, system up time, and license status information.
<b>System Resources</b>	Displays the real-time usage status of the CPU and memory.
<b>Incidents &amp; Events Distribution</b>	Displays a chart providing information about the number of incidents and events with the level of severity.
<b>Lure Distribution</b>	Displays the number of decoys deployed with the chart showing the type of service (SSH, Samba, SMB, SCADA or RDP).
<b>Decoy VM Distribution by OS</b>	Displays the number of VMs with a chart showing the type of VM. (Windows or Ubuntu).
<b>Incidents &amp; Events Count</b>	Displays a chart of events occurring each day.
<b>Top Critical Logs</b>	Displays the top logs that are classified as <i>Critical</i> .
<b>Disk Monitor</b>	Displays the RAID level and status, disk usage, and disk management information.
<b>TOP 10 Attackers by Incident</b>	Displays the top 10 attackers by the number of incidents.
<b>TOP 10 Attackers by Events</b>	Displays the top 10 attackers by the number of events.
<b>TOP 10 IPS attacks</b>	Displays the top 10 IPS attackers by the number of events.
<b>Global Incidents Distribution</b>	Displays the number of Attackers by country on a global map.

This section includes the following topics:

- [Customizing the dashboard on page 44](#)
- [System Information on page 45](#)
- [System Resources on page 46](#)
- [Decoy Distribution by OS on page 46](#)

- [Lure Distribution on page 47](#)
- [Top Critical Logs on page 48](#)
- [Disk Monitor on page 48](#)

## Customizing the dashboard

The FortiDeceptor system dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

### To move a widget:

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

### To refresh a widget:



Click *Refresh* in the widget's title bar to refresh the data presented in the widget.


### To reset all widgets to default settings:



Click *Reset* on the floating widget tool bar.

### To add a widget:



In the floating dashboard toolbar, click , then select the names of widgets that you want to add. To hide a widget, in its title bar, select the close icon.

The following is a list of widgets you can add to your dashboard:

- [System Information on page 45](#)
- [System Resources on page 46](#)
- [Decoy Distribution by OS on page 46](#)
- [Lure Distribution on page 47](#)
- [Incidents and Events Distribution on page 22](#)
- [Incidents and Events Count on page 22](#)
- [Top Critical Logs on page 48](#)
- [Disk Monitor on page 48](#)

### To go to the top of the dashboard:



After scrolling down the dashboard page, the  *Back to Top* button will appear in the floating widget tool bar. Click this button to go to the top of the dashboard.

**To edit a widget:**

1. Select the edit icon in the widget's title bar to open the edit widget window.
2. Configure the following information, and then select *OK* to apply your changes:

<b>Custom widget title</b>	Optionally, type a custom title for the widget. Leave this field blank to use the default widget title.
<b>Refresh interval</b>	<p>Enter a refresh interval for the widget, in seconds.</p> <p>Some widgets have default refresh values:</p> <ul style="list-style-type: none"> <li>• System Information: 90</li> <li>• System Resources: 10</li> <li>• Decoy Distribution by OS: 300</li> <li>• Lure Distribution: 300</li> <li>• Incidents and Events Distribution: 300</li> <li>• Incidents and Events Count: 300</li> <li>• Top Critical Logs: 3600</li> <li>• Disk Monitor: 3600</li> <li>• Top 10 Attackers by Events: 300</li> <li>• Top 10 Attackers by Incidents: 300</li> <li>• Incidents Distribution by Service: 300</li> <li>• Global Incidents Distribution: 600</li> <li>• Top 10 IPS attacks: 300</li> </ul>
<b>Top Count</b>	<p>Select the number of entries to display in the widget. The top count can be between 5 to 20 entries.</p> <p>This option is only available in the following widgets: <i>Top Critical Logs</i>.</p>
<b>Time Period</b>	<p>Select a time period to be displayed from the drop-down list. The options are: <i>Last 24 hours</i>, <i>Last 7 days</i>, <i>Last 4 weeks</i>. This option is only available for Incidents and Events Distribution, Incidents and Events Count, Top 10 Attackers by Events, and Top 10 Attackers by Incidents.</p>

## System Information

The *System Information* widget displays various information about the FortiDeceptor unit and enables you to configure basic system settings.

This widget displays the following information and options:

<b>Host Name</b>	The name assigned to this FortiDeceptor unit. Select <i>[Change]</i> to edit the FortiDeceptor host name.
<b>Serial Number</b>	The serial number of this FortiDeceptor unit. The serial number is unique to the FortiDeceptor unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
<b>System Time</b>	The current time on the FortiDeceptor internal clock or NTP server. Select <i>[Change]</i> to configure the system time.
<b>Firmware Version</b>	The version and build number of the firmware installed on the FortiDeceptor unit.

To update the firmware, you must download the latest version from the [Fortinet Customer Service & Support portal](#). Select *[Update]* and select the firmware image to load from the local hard disk or network volume.

<b>System Configuration</b>	The date and time of the last system configuration backup. Select <i>Backup/Restore</i> to browse to the <i>System Recovery</i> page.
<b>Current User</b>	The administrator that is currently logged on to the system.
<b>Uptime</b>	The duration of time that the FortiDeceptor unit has been running since it booted up.
<b>Deception OS</b>	<p>Deception OS license activation and initialization status.</p> <p>Displays an <i>up</i> icon if the Deception OS is activated and initialized. Displays a <i>Caution</i> icon if the Deception OS is initializing or having issues. Hover the mouse pointer on the status icon to view detailed information. More information can be found in the <i>Log &gt; All Events</i> page.</p> <p>Click <i>Deception OS</i> to go to the images available on FortiDeceptor.</p> <p>After purchase, you should download the license file from the <a href="#">Fortinet Customer Service &amp; Support</a> portal. Then, click the <i>[Upload License]</i> link next to the Deception OS field. Browse to the license file on the management computer, and click the <i>Submit</i> button. The system will reboot and activate the newly installed Deception OS.</p>



Select the *Edit* icon to type a custom widget title and enter the refresh interval. The default refresh interval is 300 seconds.

## System Resources

This widget displays the following information and options:

<b>CPU Usage</b>	Gauges the CPU percentage usage.
<b>Memory Usage</b>	Gauges the Memory percentage usage.
<b>Reboot/Shutdown</b>	Options to shut down or reboot the FortiDeceptor device.



Select the *Edit* icon to type a custom widget title and enter the refresh interval. The default refresh interval is 30 seconds.

## Decoy Distribution by OS

This widget displays the following information and options:

<b>Ubuntu</b>	Shows the number of Ubuntu Decoy VMs with the percentage on a pie chart.
<b>Windows</b>	Shows the number of Windows Decoy VMs with the percentage on a pie chart.
<b>SCADA</b>	Shows the number of SCADA Decoy VMs with the percentage on a pie chart.



Hover over the pie chart to see the percentage. Click the pie chart to split the Windows and Ubuntu VMs.

## Lure Distribution

This widget displays the number of lures deployed with the following information and options:

<b>SSH</b>	Shows the number of decoy images using SSH service with the percentage on a pie chart.
<b>SAMBA</b>	Shows the number of decoy images using SAMBA service with the percentage on a pie chart.
<b>SMB</b>	Shows the number of decoy images using SMB service with the percentage on a pie chart.
<b>RDP</b>	Shows the number of decoy images using RDP service with the percentage on a pie chart.
<b>HTTP</b>	Shows the number of decoy images using HTTP service with the percentage on a pie chart.
<b>FTP</b>	Shows the number of decoy images using FTP service with the percentage on a pie chart.
<b>TFTP</b>	Shows the number of decoy images using TFTP service with the percentage on a pie chart.
<b>SNMP</b>	Shows the number of decoy images using SNMP service with the percentage on a pie chart.
<b>MODBUS</b>	Shows the number of decoy images using MODBUS service with the percentage on a pie chart.
<b>S7COMM</b>	Shows the number of decoy images using S7COMM service with the percentage on a pie chart.
<b>BACNET</b>	Shows the number of decoy images using BACNET service with the percentage on a pie chart.
<b>IPMI</b>	Shows the number of decoy images using IPMI service with the percentage on a pie chart.
<b>TRICONEX</b>	Shows the number of decoy images using TRICONEX service with the percentage on a pie chart.

**Guardian-AST**

Shows the number of decoy images using Guardian-AST service with the percentage on a pie chart.

**IEC104**

Shows the number of decoy images using IEC104 service with the percentage on a pie chart.



Hover over the pie chart to see the percentage. Click the pie chart to split the particular service from the chart.

## Top Critical Logs

The *Top Critical Logs* widget displays recent critical logs, including the time they occurred and a brief description of the event.



Select the edit icon to type a custom widget title, enter the refresh interval, and top count. The default refresh interval is 3600 seconds.

## Disk Monitor

Displays the RAID level and status, disk usage, and disk management information. This widget is only available in hardware-based models.

This widget displays the following information:

<b>Summary</b>	Disk summary information including RAID level and status.
<b>RAID Level</b>	Displays the RAID level.
<b>Disk Status</b>	Displays the disk status.
<b>Disk Usage</b>	Displays the current disk usage.
<b>Disk Number</b>	Displays the disk number.
<b>Disk Size</b>	Displays the disk size.

## Basic System Settings

The following sections explain the how to configure basic system settings on FortiDeceptor:

- [Change the GUI idle timeout on page 49](#)
- [Microsoft Windows VM license activation on page 49](#)
- [Log out of the unit on page 49](#)
- [Refresh Current Web Page on page 49](#)



- [Table Customization on page 42](#)
- [Update the FortiDeceptor firmware on page 50](#)
- [Reboot and shut down the unit on page 50](#)
- [Back up or restore the system configuration on page 51](#)

## Change the GUI idle timeout

By default, the GUI disconnects administrative sessions if no activity takes place for five minutes. This idle timeout is recommended to prevent someone from using a logged-in GUI on a PC that has been left unattended.

**To change the idle timeout length:**

1. Go to *System > Settings*.
2. Change the idle timeout minutes (1 to 480 minutes) as required.
3. Select *OK* to save the setting. The setting will take affect only after logging out and logging back in.



In this page you can also reset all widgets to their default settings.

---

## Microsoft Windows VM license activation

When Fortinet ships FortiDeceptor, the default Windows guest VM image is activated. The Windows VM license will be in an unactivated state and need re-activation.



If you purchase a Windows or Ubuntu VM upgrade package, the downloaded license file should be uploaded here by clicking the *[Upload License]* link.

---

## Log out of the unit

**To log out of the unit:**

1. From the top-right corner of the banner, select your user name.
2. From the drop-down menu, select *Logout* to log out of your administrative session.

If you only close the browser or leave the GUI to browse another web site, you will remain logged in until the idle timeout period elapses.

## Refresh Current Web Page

Click the *Refresh* button on top of the web site, the current web page will be refreshed.

## Update the FortiDeceptor firmware

Before any firmware update, complete the following:

- Download the FortiDeceptor firmware image and Release Notes document from the [Fortinet Customer Service & Support](#) portal. Review the Release Notes, including the special notices, upgrade information, product integration and support, and resolved and known issues.
- Back up your configuration file. It is highly recommended that you create a system backup file and save it to your management computer. You can also schedule the system to back up system configurations to a remote server.
- Plan a maintenance window to complete the firmware update. If possible, you may want to set up a test environment to ensure that the update does not negatively impact your network.
- Once the update is complete, test your FortiDeceptor device to ensure that the update was successful.



Firmware best practice: Stay current on patch releases for your current major release. Only update to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiDeceptor Release Notes* or contact Technical Support.

---

### To update the FortiDeceptor firmware:

1. Go to *Dashboard > System Information > Firmware Version*.
2. Click *[Update]*.
3. Select *Choose File*, locate the firmware image on your management computer. Click *Submit* to start the upgrade. Alternatively, you can download the firmware by clicking the Download icon for the Firmware release you would like to install from the *Install* column of the *Available Firmware* table. If you choose this option, the system will upgrade and restart automatically.

## Reboot and shut down the unit

Always reboot and shut down the FortiDeceptor system using the options in the GUI or CLI to avoid potential configuration or hardware problems.

### To reboot the FortiDeceptor unit:

1. Go to *Dashboard > System Resources*.
2. Select *Reboot*.
3. Enter a reason for the reboot in the *Reason* field, and then select *OK* to reboot the unit. After reboot, the FortiDeceptor VM system will initialize again. This initialization can take up to 30 minutes. The Decoy VM icon in the *System Information* widget will show a warning sign before the process completes.



It is normal to see the following critical event log in *Log Access* after FortiDeceptor boots up: *The VM system is not running and might need more time to startup. Please check system logs for more details. If needed, please reboot system.*

---



After FortiDeceptor is upgraded to a new firmware version, the system might clean up data and a *Database is not ready message* will be displayed. The clean-up time depends on the size of historical data.

---

**To shut down the FortiDeceptor unit:**

1. Go to *Dashboard > System Resources widget*.
2. Select *Shutdown*.
3. Enter a reason for the shutdown in the *Reason* field.
4. Select *OK* to shutdown the unit.

## Back up or restore the system configuration

It is recommended that you create a system backup file as part of your maintenance plan. Always perform a backup before upgrading firmware or making major system configuration changes. Save these configuration backups to your management computer in the event that you need to restore the system after a network event.



The FortiDeceptor configuration file is in binary format and manual editing is not supported.

---

**To back up the FortiDeceptor configuration to your local management computer:**

1. Go to *Dashboard > System Information > System Configuration*.
2. Select *Backup/Restore*.
3. Click *Click here* to save your backup file to your management computer.

**To restore the FortiDeceptor configuration:**

1. Go to *Dashboard > System Information > System Configuration*.
2. Select *Backup/Restore*.
3. Click *Browse...*, locate the backup file on your management computer, then select *Restore* to load the backup file.
4. Select *OK* in the confirmation dialog box. When the system configuration restore process starts, you will be redirected to the login page once it has completed.



By performing a system restore, all of your current configurations will be replaced with the backup data. The system will reboot automatically to complete the restore operation. Only the backup configuration file from the previous or same release is supported.

---

## Network

The *Network* page provides interface, DNS, and routing management options.

This section includes the following topics:

- [Interfaces](#)
- [DNS Configuration](#)
- [System Routing](#)

## Interfaces

To view and manage interfaces, go to *Network > Interfaces*.

This page displays the following information and options:

<b>Interface</b>	The interface name and description, where applicable. Failover IP will be listed under this field with the following descriptor: <i>(cluster external port)</i> .
<b>port1 (administration port)</b>	port1 is hard-coded as the administration interface. You can select to enable or disable HTTP, SSH, Telnet access rights on port1. HTTPS is enabled by default. port1 can be used for Device mode, although a different, dedicated port is recommended.
<b>port2</b>	Decoy VM deployment.
<b>port3</b>	Decoy VM deployment.
<b>port4</b>	Decoy VM deployment.
<b>port5/port6</b>	Decoy VM deployment.
<b>port7/port8</b>	Decoy VM deployment.
<b>IPv4</b>	The IPv4 IP address and subnet mask of the interface.
<b>IPv6</b>	The IPv6 IP address and subnet mask of the interface.
<b>Interface Status</b>	The state of the interface, one of the following states: <ul style="list-style-type: none"> <li>Interface is up</li> <li>Interface is down</li> <li>Interface is being used by sniffer</li> </ul>
<b>Link Status</b>	The link status. <ul style="list-style-type: none"> <li>Link up</li> <li>Link down</li> </ul>
<b>Access Rights</b>	The access rights associated with the interface. HTTPS is enabled by default on port1. You can select to enable HTTP, SSH, and Telnet access on port1.
<b>Edit</b>	Select the interface and select <i>Edit</i> from the toolbar to edit the interface.

### To edit an interface:

1. Select the The *IPv4/IPv6* address of an interface name, and click the *Edit* button from the toolbar.
2. Edit the IP address as required.
3. Click *OK* to apply the changes.

You can also change the interface status from *Up* to *Down* by clicking the status icon.

### To edit administrative access:

The port1 interface is used for administrative access to the FortiDeceptor device. HTTPS is enabled by default, but you can edit this interface to enable HTTP, SSH, and Telnet support.

Edit the IP address and the access rights as required and click *OK* to apply the changes.

## DNS Configuration

The primary and secondary DNS server addresses can be configured from *Network > System DNS*.

## System Routing

The System Routing page allows you to manage static routes on your FortiDeceptor device. Go to *Network > System Routing* to view the routing list.

The following options are available:

<b>Create New</b>	Select to create a new static route.
<b>Edit</b>	Select a static route in the list and select <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select a static route in the list and select <i>Delete</i> in the toolbar to delete the entry.

The following information is displayed:

<b>IP/Mask</b>	Displays the IP address and subnet mask.
<b>Gateway</b>	Displays the gateway IP address.
<b>Device</b>	Displays the interface associated with the static route.
<b>Number of Routes</b>	Displays the number of static routes configured.

### To create a new static route:

1. Click *Create New* from the toolbar.
2. Enter a destination IP address, mask, and gateway in their requisite fields.



The destination IP/Mask can be entered in the format 192.168.1.2/255.255.255.0, 192.168.1.2/24, or fe80:0:0:0:0:c0a8:1fe.

3. Select a device (or interface) from the drop-down list.
4. Click *OK* to create the new static route.

### To edit a static route:

1. Select a Static Route
2. Click the *Edit* button.
3. Edit the destination IP address and mask, gateway, and device (or interface) as required.
4. Click *OK* to apply the edits to the static route.

### To delete a static route or routes:

1. Select one or more Static Routes.
2. Click the *Delete* button from the toolbar.

3. Select *Yes, I'm sure* on the confirmation page to delete the selected route or routes.

# System Log

The *Log* menu allows you to view and download all FortiDeceptor system logs collected by the device. You can log locally to FortiDeceptor or a remote log server.

This section includes the following topics:

- [Log Details](#)
- [Logging Levels](#)
- [Raw logs](#)
- [Log Categories](#)
- [Log Servers](#)

## Log Details

To view more details about a specific log in the log list, simply select that log. A log details pane displays at the bottom of the window.

The log details pane contains the same information as the log message list, except with a full message in lieu of a shortened one.

## Logging Levels

FortiDeceptor logs can be Emergency (reserved), Alert, Critical, Error, Warning, Information, or Debug. The following table provides example logs for each log level.

Log Level	Description	Example Log Entry
<b>Alert</b>	Immediate action is required.	Suspicious URL visit domain.com from 192.12.1.12 to 42.156.162.21:80.
<b>Critical</b>	Functionality is affected.	System database is not ready. A program should have started to rebuild it and it shall be ready after a while.
<b>Error</b>	An erroneous condition exists and functionality is probably affected.	Errors that occur when deleting certificates.

Log Level	Description	Example Log Entry
<b>Warning</b>	Functionality might be affected.	Submitted file AVSInstallPack.exe is too large: 292046088.
<b>Information</b>	General information about system operations.	LDAP server information that was successfully updated.
<b>Debug</b>	Detailed information useful for debugging purposes.	Launching job for file. jobid=2726271637747836543 filename=log md5=ebe5ae2bec3b653c2970e8cec9f5f1d9 sha1=06ea6108d02513f0d278ecc8d443df86dac2885b sha256=d678da5fb9ea3ee20af779a4ae13c402585ebb070edcf20091cb20509000f74b

## Raw logs

Raw logs can be downloaded and saved to the management computer using the *Download Log* button. The raw logs will be saved as a text file with the extension *.log.gz*. The user can search the system log for more information.

### Sample raw logs file content

```
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
Service=SSH AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
Operation=Established SSH connection Description=10.95.5.83 Username=NA Password=NA"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
Service=SSH AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
Operation=SSH connection closed Description=83ssh Username=83ssh Password=83ssh"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
Service=SSH AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
Operation=Authentication Failure Description=83ssh Username=83ssh Password=83ssh"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
Service=SAMBA AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
Operation=Change to dir Description=/home/share/samba Username=83samba Password=83samba"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
Service=SAMBA AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
Operation=Access path Description=samba Username=83samba Password=83samba"
itime=1535413204 date=2018-08-27 time=16:40:04 logid=0106000001 type=event subtype=system
pri=debug user=system ui=system action= status=success msg="SNMP TRAP sent out:
Service=SAMBA AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
Operation=Disconnect net share Description=samba Username=83samba Password=83samba"
itime=1535413201 date=2018-08-27 time=16:40:01 logid=0106000001 type=event subtype=system
pri=alert user=system ui=GUI action=update status=success msg="Service=SSH
AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22 Operation=SSH
connection closed Description=83ssh Username=83ssh Password=83ssh"
```



```

itime=1535413201 date=2018-08-27 time=16:40:01 logid=0106000001 type=event subtype=system
pri=alert user=system ui=GUI action=update status=success msg="Service=SSH
AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
Operation=Authentication Failure Description=83ssh Username=83ssh Password=83ssh"
itime=1535413198 date=2018-08-27 time=16:39:58 logid=0106000001 type=event subtype=system
pri=alert user=system ui=GUI action=update status=success msg="Service=SSH
AttackerIp=10.95.5.83 AttackerPort=57190 VictimIp=10.95.5.21 VictimPort=22
Operation=Established SSH connection Description=10.95.5.83 Username=NA Password=NA"
itime=1535413198 date=2018-08-27 time=16:39:58 logid=0106000001 type=event subtype=system
pri=alert user=system ui=GUI action=update status=success msg="Service=SAMBA
AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445
Operation=Disconnect net share Description=samba Username=83samba Password=83samba"
itime=1535413197 date=2018-08-27 time=16:39:57 logid=0106000001 type=event subtype=system
pri=alert user=system ui=GUI action=update status=success msg="Service=SAMBA
AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445 Operation=Change
to dir Description=/home/share/samba Username=83samba Password=83samba"
itime=1535413197 date=2018-08-27 time=16:39:57 logid=0106000001 type=event subtype=system
pri=alert user=system ui=GUI action=update status=success msg="Service=SAMBA
AttackerIp=10.95.5.83 AttackerPort=NA VictimIp=10.95.5.21 VictimPort=445 Operation=Access
path Description=samba Username=83samba Password=83samba"

```

## Log Categories

In FortiDeceptor, the following log category is displayed:

<b>All Events</b>	Shows all logs.
-------------------	-----------------

The following options are available:

<b>Download Log</b>	Select to download a file containing the raw logs to the management computer.
<b>History Logs</b>	Enable to include historical logs in Log Search.
<b>Refresh</b>	Select to refresh the log message list.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Users can select different categories to search the logs. The Search feature is not case sensitive.
<b>Pagination</b>	Use these controls to jump or scroll to other pages. The total number of pages and logs is also shown.

The following information is displayed:

<b>#</b>	Log number.
<b>Date/Time</b>	The time that the log message was created.
<b>Level</b>	The level of the log message. The available logging levels are: <ul style="list-style-type: none"> <li>Alert: Immediate action is required.</li> <li>Critical: Functionality is affected.</li> <li>Error: Functionality is probably affected.</li> <li>Warning: Functionality might be affected.</li> <li>Information: Information about normal events.</li> </ul>

	<ul style="list-style-type: none"><li>• <b>Debug:</b> Information used for diagnosis or debugging.</li></ul>
<b>User</b>	The user to which the log message relates. User can be a specific user or system.
<b>Message</b>	Detailing log message.

## Log Servers

FortiDeceptor logs can be sent to a remote syslog server or common event type (CEF) server. Go to *Log & Reports > Log Servers* to create new remote log servers as well as edit and delete remote log servers. You can configure up to 30 remote log server entries.

The following options are available:

<b>Create New</b>	Select to create a new log server entry.
<b>Edit</b>	Select a log server entry in the list and select <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select a log server entry in the list and select <i>Delete</i> in the toolbar to delete the entry.

This page displays the following information:

<b>Name</b>	The name of the server entry.
<b>Server Type</b>	The server type. One of the following options: CEF or syslog.
<b>Server Address</b>	The log server address.
<b>Port</b>	The log server port number.
<b>Status</b>	The status of the log server, <i>Enabled</i> or <i>Disabled</i> .

**To create a new server entry:**

1. Go to *Log & Reports > Log Servers*.
2. Select + *Create New* from the toolbar.

3. Configure the following settings:

<b>Name</b>	Enter a name for the new server entry.
<b>Type</b>	Select <i>Log Server Type</i> from the drop-down list.
<b>Log Server Address</b>	Enter the log server IP address or FQDN.
<b>Port</b>	Enter the port number. The default port is 514.
<b>Status</b>	Select to enable or disable sending logs to the server.
<b>Log Level</b>	Select to enable the logging levels to be forwarded to the log server. The following options are available: <ul style="list-style-type: none"><li>• Alert Logs.</li><li>• Critical Logs</li><li>• Error Logs</li><li>• Warning Logs</li><li>• Information Logs</li><li>• Debug Logs</li></ul>

4. Select *OK* to save the entry.

**To edit or delete a log server**

1. Go to *Log and Report > Log Servers*.
2. Select a syslog server or new common event entry.
3. Click the *Edit* or *Delete* button from the toolbar.



**FORTINET®**



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiDeceptor®, 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.