



FortiDeceptor - Administration Guide

Version 2.0.0

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 COOKBOOK

<https://cookbook.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: techdocs@fortinet.com



April 1, 2019

FortiDeceptor 2.0.0 Administration Guide

50-200-548424-20190401

TABLE OF CONTENTS

Change Log	5
Introduction	6
Set up FortiDeceptor	7
Connect to the GUI	7
Change the system hostname	7
Change the administrator password	8
Configure the system time	8
Deploy Deception VM	10
View Available VM Images	10
Set up the Monitored Network	10
Deploy Deception VMs with the Deploy Wizard	11
Deploy the FortiDeceptor Token Package	13
Monitor Deception Status	13
View the Deception Map	14
Configure a Whitelist	15
DMZ Mode	16
Limitations of the DMZ Mode	17
Monitor Attacks	18
Analysis	18
Campaign	19
Attack Map	20
Incidents and Events Distribution	20
Incidents and Events Count	21
Top 10 Attackers by Events	21
Top 10 Attackers by Incidents	22
Top 10 IPS Attacks	22
Incidents Distribution by Service	22
Global Attacker Distribution	23
Fabric	24
Blocking	24
Fabric Status	25
System	26
Administrators	26
Admin Profiles	29
Certificates	31
LDAP Servers	33
RADIUS Servers	34
Mail Server	35
SNMP	36
FortiGuard	40
Login Disclaimer	41

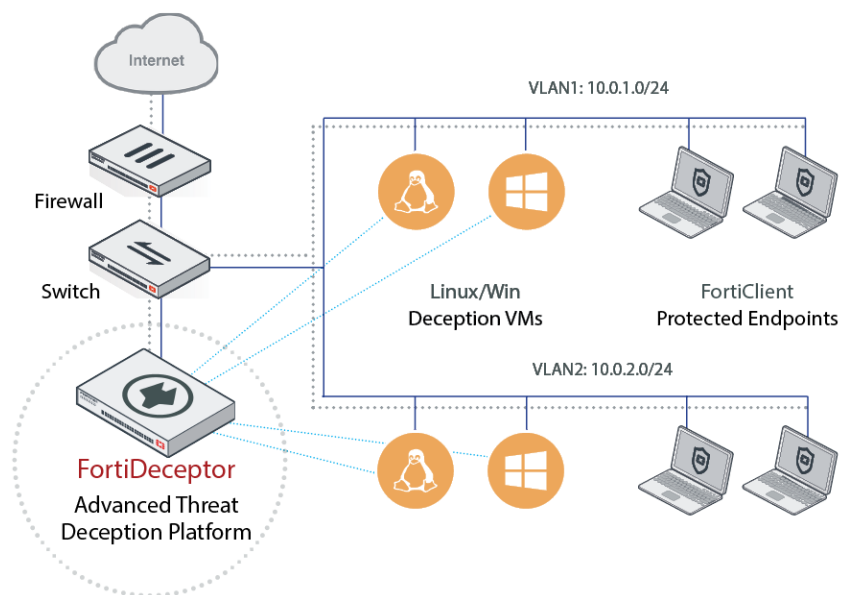
Table Customization	41
Settings	41
System Settings	42
Dashboard	42
Customizing the dashboard	43
System Information	44
System Resources	45
Deception VM Distribution	45
Decoy Service Distribution	46
Top Critical Logs	46
Disk Monitor	46
Basic System Settings	47
Change the GUI idle timeout	47
Microsoft Windows VM license activation	47
Log out of the unit	48
Refresh Current Web Page	48
Update the FortiDeceptor firmware	48
Reboot and shut down the unit	49
Back up or restore the system configuration	49
Network	50
Interfaces	50
DNS Configuration	51
System Routing	51
System Log	53
Log Details	53
Logging Levels	53
Raw logs	54
Log Categories	55
Log Servers	56

Change Log

Date	Change Description
2019-04-01	Initial release of FortiDeceptor 2.0.0.

Introduction

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



Key features of FortiDeceptor include:

- VM Images: Windows or Linux VM images are available to create Deception VMs.
- Deception VMs: Deception VMs that behave like real endpoints can be deployed through FortiDeceptor.
- Decoy: Decoys are services, applications, or users added to a Deception 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 Deception 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 7](#)
- [Change the system hostname on page 7](#)
- [Change the administrator password on page 8](#)
- [Configure the system time on page 8](#)

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:

System Time	The date and time according to the FortiDeceptor unit's clock at the time that this tab was loaded.
Time Zone	Select the time zone in which the FortiDeceptor unit is located.
Set Time	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> .
Synchronize with NTP Server	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 Deception VM

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

To use FortiDeceptor to monitor the network:

1. Go to *Deception > VM Images* to check the VM Images available. See [View Available VM Images on page 10](#)
2. Go to *Deception > Monitored Network* to Auto-Detect or specify the network where the Deception VMs will be deployed. See [Set up the Monitored Network on page 10](#)
3. Go to *Deception > Deploy Wizard* to deploy the Deception VM on the network. See [Deploy Deception VMs with the Deploy Wizard on page 11](#)
4. Go to *Deception > Deception Status* to see the Deception VM deployed, start, stop, or download the FortiDeceptor Token Package to manually install on computers. See [Monitor Deception Status on page 13](#)
5. Go to *Deception > Deception Map* to see the network of Deception VMs. See [View the Deception Map on page 14](#)
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 monitored network and not be flagged as an attacker. See [Configure a Whitelist on page 15](#)

View Available VM Images

The VM images available for creating Deception VMs are shown on the *VM Images* page. The following information is shown:

Column	Description
Status	Shows if the VM Image is <i>Initialized</i> or <i>Not Initialized</i> .
Name	Name of the VM Image.
OS Type	Shows the Operating System type (Ubuntu or Windows 7).
VM Type	Shows if the VM Image is a Linux or a Windows endpoint.
Services	Shows the services used by the Deception VM (SSH, SAMBA, SMB, or RDP).

Set up the Monitored Network

The *Monitored 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. Go to *Deception > Monitored Network*.
2. Select *Auto VLAN Detection* to automatically detect the VLANs on your network.

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:

Interface	The port that will connect to the VLAN or subnet.
VLAN ID	Specify an integer to assign a unique ID to the VLAN.
Deception Monitor IP/Mask	Specify an IP address to monitor. This is useful to mask the actual IP address.
Ref	Shows the number of objects referring to this object.
Status	Shows if the IP address is initialized.
Action	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 Deception VMs with the Deploy Wizard

The Deploy Wizard allows you to create and deploy Deception VMs on your network. These Deception 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 > Deploy Wizard*.
2. Click + to add a Deception VM.
3. Configure the following:

Profile Name	Specify the name of the deployment profile in 1-15 characters. <i>A-Z, a-z, 0-9</i> , dash or underscore allowed. Cannot be duplicate of the existing profile name.
Available VMs	Select one of the available VM Images. Windows or Ubuntu VM Images are available.
Selected Services	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.

- Click *Add Decoy* for the respective service and configure the following:

Username	Specify the username for the decoy in 1-19 characters. <i>A-Z</i> , <i>a-z</i> , or <i>0-9</i> , allowed.
Password	Specify the password for the decoy in 1-14 non-unicode characters.
Sharename	Specify a Sharename in 3-63 characters. <i>A-Z</i> , <i>a-z</i> , or <i>0-9</i> , allowed. This option is for a SAMBA (Ubuntu) or SMB (Windows).
Update or Cancel	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 decoy.

- Repeat step 5 to add more decoys.
- Switch *Launch Immediately* to *ON* to launch the Deception VMs.
- Click *Next*.
- 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.
- Click *Add Interface*.
- In the *Add Interface for Deception VM* screen, select the *Deploy Interface*. This is the VLAN or Subnet added in the following topic: [Set up the Monitored Network on page 10](#)
- Configure the following settings in the Add Interface for Deception VM screen:

Addressing Mode	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.
Network Mask	The network mask is shown automatically.
Gateway	Specify the gateway.
IP Count	Specify the number of IP address to be assigned. The maximum per Deception VM is 16 IPs. IP count will automatically switch to 1 if the addressing mode is DHCP.
Min	The minimum IP address in the IP range.
Max	The maximum IP address in the IP range.
IP Ranges	Specify the IP range between <i>Min</i> and <i>Max</i> .

- Click *Done*.
- Click *Template* to save as a template. The template is visible with the Profile Name in *Deception > Deploy Wizard*.
- 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 Deception VM. Tokens are normally distributed within the real endpoints and other IT assets on the network to maximize the deception surface.

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

1. Go to *Deception > Deception Status*.
2. Select the Deception VM.
3. Click *Download Package* to download the FortiDeceptor Token Package. Packages can only be downloaded from Deceptions VMs with valid IP and that are in the following status: *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 Deception VM.

To uninstall a FortiDeceptor Token Package:

1. Go to *Deception > Deception Status*.
2. Select the Deception 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 Deception Status

The *Deception Status* page shows the status of the decoys deployed on your network.

To view the Deception Status:

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

Action	Click <i>View</i> to view the decoy. Click <i>Start</i> or <i>Stop</i> to start or stop the decoy. Click <i>Delete</i> to delete the decoy.
Status	The current status of the decoy is shown as <i>Running</i> , <i>Stopped</i> , or <i>Cannot Start</i> . If the

	Deception VM cannot start, hover over the VM to see the reason for failure to start.
Name	Name of the decoy.
OS	Operating system of the decoy whether <i>Ubuntu</i> or <i>Windows</i> .
VM	The name of the Deception VM.
Enabled Decoys	The number of decoys enabled on this VM.
IP	The IP address of the Deception VM.
Network Type	Shows if the IP address is <i>Static</i> or <i>Dynamic</i> .
DNS	Shows the DNS.
Gateway	Shows the gateway.

To delete one or more Deception VMs:

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

To start one or more Deception VM:

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

To stop one or more Deception VMs:

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



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

View the Deception Map

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

To view the details of the node in Deception Map:

1. Click the node.
2. A dialog with the following information is shown:
 - IP
 - DNS
 - Gateway
 - OS
 - Status

To search for information about a node in Deception Map:

1. Click the *Search* field.
2. Specify the name of the node.

To change the mode:

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

To reset the Deception Map:

Click *Reset*.

To pause the visual representation of ongoing activity:

Click *Pause*.

To change display options:

1. Go to *Deception > Deception Map*.
2. Click *Options*. Configure one of the following options:
 - *Zoom controls* - select the check box to show zoom controls on the Deception 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:

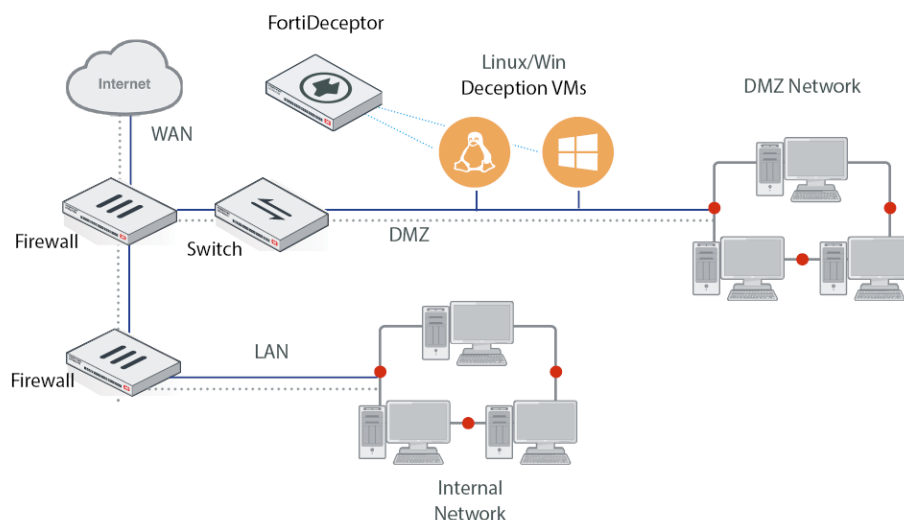
1. Go to *Deception > Whitelist*.
2. Click *Add New Whitelist IP*.
3. Configure the following settings:

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

```
dmz-mode enable
```




Enabling or disabling the DMZ mode will remove all previous configurations including Deception VMs, decoys, and tokens. Deception Images 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 Monitored Network view, Deception Monitor IP/Mask is hidden when in DMZ Mode. See [Set up the Monitored Network on page 10](#) for more information about Deception IP/Mask.
- Under Deception Status view, the Attack Test selection is disabled.
- When DMZ mode is enabled, Deception VMs are limited to 1 Deploy Interface with 16 Decoys. See [Deploy Deception VMs with the Deploy Wizard on page 11](#) 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 18](#)
- Campaign page lists the Attacks (related *Events*) detected by FortiDeceptor. See [Campaign on page 19](#)

To monitor Attacks from the Widgets:

- Incidents and Events Distribution widget. See [Incidents and Events Distribution on page 20](#).
- Incidents and Events Count widget. See [Incidents and Events Count on page 21](#).

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:

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

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

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:

Severity	Severity of the <i>Attack</i> is shown as Critical, High, Medium, Low, or Unknown.
Last Activity	Date and time of the last activity.
Start	Date and time when the attack started.
Attacker IP	IP mask of the attacker.
ID	ID of the campaign record.
Screenshot	Screenshot of the attack in progress.
Timeline	Click <i>Timeline</i> to see the entire timeline of the <i>Attack</i> from start to finish.
Table	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, Deception VMs, and ongoing attacks.

To change filtering arguments:

1. Go to *Incident > Attack Map*.
2. At the bottom of the Attack Map, click and drag in the timestamp indicator to identify a start and 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
- Deception VM IP

To locate the node in the map:

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

To save a snapshot of the map:

Click the *Save View* button, which has the icon of *Removable Disk*.

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:

Unknown	Shows the <i>Incident</i> or <i>Event</i> where the risk level is unknown. The entries are shown in grey color.
Low Risk	Shows the <i>Incident</i> or <i>Event</i> where the risk level is low. The entries are shown in green color.

Medium Risk	Shows the <i>Incident</i> or <i>Event</i> where the risk level is medium. The entries are shown in yellow color.
High Risk	Shows the <i>Incident</i> or <i>Event</i> where the risk level is high. The entries are shown in orange color.
Critical	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:

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

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



This widget is only available in DMZ Mode.

Top 10 Attackers by Incidents

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

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



This widget is only available in DMZ Mode.

Top 10 IPS Attacks

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

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

Incidents Distribution by Service

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

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

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

Blocking	Configure the FortiGate settings for FortiDeceptor integration.
Fabric Status	Display the status of blocked IP addresses.

Blocking

The *Blocking* 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.
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.

Fabric Status

The *Fabric 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 selected attacker IP addresses in below table.
Unblock	Manually send an unblocking request for selected attack IP addresses in below 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.

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:

Administrators	Configure administrator user accounts.
Admin Profile	Configure user profiles to define user privileges.
Certificates	Configure CA certificates.
LDAP Servers	Configure LDAP Servers.
RADIUS Servers	Configure RADIUS Servers.
Mail Server	Configure the Mail Server.
SNMP	Configure SNMP.
Login Disclaimer	Configure the Login Disclaimer.
Settings	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.
Table Customization	Define columns and orders of <i>Incident</i> and <i>Event</i> tables.



Some menus are not displayed on the Slave Nodes in a cluster.

This section includes the following topics:

- [Administrators](#)
- [Admin Profiles](#)
- [Certificates](#)
- [LDAP Servers](#)
- [RADIUS Servers](#)
- [Mail Server](#)
- [SNMP](#)
- [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:

Create New	Select to create a new administrator account.
Edit	Select an administrator account from the list and select <i>Edit</i> in the toolbar to edit the entry.
Delete	Select an administrator account from the list and select <i>Delete</i> in the toolbar to delete the entry.
Test Login	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:

Name	Displays the administrator account name.
Type	The administrator type: <ul style="list-style-type: none">• Local• LDAP• RADIUS
Profile	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:

Administrator	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 _.
Password	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> .
Confirm Password	Confirm the password for the account. This field is available when <i>Type</i> is set to <i>Local</i> .
Type	Select either Local, LDAP, or RADIUS.
LDAP Server	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 LDAP Servers on page 33 .
RADIUS Server	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 RADIUS Servers .
Admin Profile	Select the Admin Profile the user belongs to.
Trusted Host 1, Trusted Host 2, Trusted Host 3	Enter up to three IPv4 trusted hosts. Only users from trusted hosts can access FortiDeceptor.
Trusted IPv6 Host 1, Trusted IPv6 Host 2, Trusted IPv6 Host 3	Enter up to three IPv6 trusted hosts. Only users from trusted hosts can access FortiDeceptor.
Comments	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 is one predefined administrator profile, which cannot be modified or deleted:

- Super Admin: All functionality is accessible

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:

Read Write	User can view and make changes to the system.
None	User cannot view or make changes to the system.

Settings for CLI Commands:

Execute	User can execute the CLI command.
None	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
 - VM Images
 - Monitored Network
 - Wizard
 - Deception Status
 - Deception Map
 - Whitelist
 - Incident
 - Analysis
 - Campaign
 - Attack Map
 - Fabric
 - Blocking
 - Fabric Status
 - Network
 - Interfaces
 - System DNS
 - System Routing
 - System
 - Administrators
 - Admin Profiles
 - Certificates
 - LDAP Servers
 - RADIUS Servers
 - Mail Server
 - SNMP
 - 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
 - Set Confirm ID for Windows VM
 - List VM License
 - Show VM Status
 - VM reset
 - Set Maintainer
 - Set Timeout for Remote Auth
 - Log Purge
 - 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:

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

The following information is displayed:

Name	The name of the certificate.
Subject	The subject of the certificate.
Status	The certificate status, active or expired.
Service	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:

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

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

The following information is displayed:

Name	The LDAP server name.
Address	The LDAP server address.
Common Name	The LDAP common name.
Distinguished Name	The LDAP distinguished name.
Bind Type	The LDAP bind type.
Connection Type	The LDAP connection type.
Number of LDAP servers	The number of LDAP server configured on the device.

To create a new LDAP server:

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

3. Configure the following settings:

Name	Enter a name to identify the LDAP server. The name should be unique to FortiDeceptor.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Common Name	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> .
Distinguished Name	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.
Bind Type	Select the type of binding for LDAP authentication. The following options are available: <ul style="list-style-type: none"> • Simple • Anonymous • Regular
Username	When the <i>Bind Type</i> is set to <i>Regular</i> , type the user name.
Password	When the <i>Bind Type</i> is set to <i>Regular</i> , type the password.
Enable Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	When <i>Enable Secure Connection</i> is selected, select either LDAPS or STARTTLS.
CA Certificate	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:

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

Delete	Select a RADIUS server in the list and select <i>Delete</i> in the toolbar to delete the entry.
---------------	---

The following information is displayed:

Name	The RADIUS server name.
Primary Address	The primary server IP address.
Secondary Address	The secondary server IP address.
Port	The port used for RADIUS traffic. The default port is 1812.
Auth Type	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:

Name	Enter a name to identify the RADIUS server. The name should be unique to FortiDeceptor.
Primary Server Name/IP	Enter the IP address or fully qualified domain name of the primary RADIUS server.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Port	Enter the port for RADIUS traffic. The default port is 1812.
Auth Type	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> .
Primary Secret	Enter the primary RADIUS server secret.
Secondary Secret	Enter the secondary RADIUS server secret.
NAS IP	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:

Send Incidents Alerts	Select to enable this feature. An email alert is sent to the <i>Receiver Email List</i> when an incident is detected.
SMTP Server Address	Enter the SMTP server address.
Port	Enter the SMTP server port number.
E-Mail Account	Enter the mail server email account. This will be used as the <i>from</i> address.
Login Account	Enter the mail server login account.
Password	Enter the password.
Confirm Password	Confirm the password.
OK	Select <i>OK</i> to apply any changes made to the mail server configuration.
Send Test Email	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.
Reset	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:

SNMP Agent	Select to enable the FortiDeceptor SNMP agent. When this is enabled, it sends FortiDeceptor SNMP traps.
Description	Enter a description of this FortiDeceptor system to help uniquely identify this unit.
Location	Enter the location of this FortiDeceptor system to help find it in the event it requires attention.
Contact	Enter the contact information for the person in charge of this FortiDeceptor system.
SNMP v1/v2c	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
SNMP v3	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:

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

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:

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

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:

Module Name	The FortiGuard module name, including: <i>AntiVirus Scanner</i> , <i>AntiVirus Extreme Signature</i> , <i>AntiVirus Active Signature</i> , <i>AntiVirus Extended Signature</i> , <i>Network Alerts Signature</i> , <i>Sandbox System Tools</i> , <i>Sandbox Rating Engine</i> , <i>Sandbox Tracer Engine</i> , <i>Android Analytic Engine</i> , <i>Android Analytic Rating Engine</i> and <i>Traffic Sniffer</i> . All modules automatically install update packages when they are available on the FDN.
Current Version	The current version of the module.
Release Time	The time that module was released.
Last Update Time	The time that module was last updated.
Last Check Status	The status of the last update attempt.
Upload Package File	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 Customer Service and Support site to download package files manually.
FortiGuard Server Location	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.
FortiGuard Server Settings	
Use override FDN server to download module updates	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.
Connect FDN Now	Click the <i>Connect FDN Now</i> button to connect the override FDN server/Proxy.
FortiGuard Web Filter Settings	
Use override server address for web filtering query	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 42](#)
- [Basic System Settings on page 47](#)
- [Network on page 50](#)

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:

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

This section includes the following topics:

- [Customizing the dashboard on page 43](#)
- [System Information on page 44](#)
- [System Resources on page 45](#)
- [Deception VM Distribution on page 45](#)

- [Decoy Service Distribution on page 46](#)
- [Top Critical Logs on page 46](#)
- [Disk Monitor on page 46](#)


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 44](#)
- [System Resources on page 45](#)
- [Deception VM Distribution on page 45](#)
- [Decoy Service Distribution on page 46](#)
- [Incidents and Events Distribution on page 20](#)
- [Incidents and Events Count on page 21](#)
- [Top Critical Logs on page 46](#)
- [Disk Monitor on page 46](#)

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:

Custom widget title	Optionally, type a custom title for the widget. Leave this field blank to use the default widget title.
Refresh interval	<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"> • System Information: 90 • System Resources: 10 • Deception VM Distribution: 300 • Decoy Service Distribution: 300 • Incidents and Events Distribution: 300 • Incidents and Events Count: 300 • Top Critical Logs: 3600 • Disk Monitor: 3600 • Top 10 Attackers by Events: 300 • Top 10 Attackers by Incidents: 300 • Incidents Distribution by Service: 300 • Global Incidents Distribution: 600 • Top 10 IPS attacks: 300
Top Count	<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>
Time Period	<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:

Host Name	The name assigned to this FortiDeceptor unit. Select <i>[Change]</i> to edit the FortiDeceptor host name.
Serial Number	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.
System Time	The current time on the FortiDeceptor internal clock or NTP server. Select <i>[Change]</i> to configure the system time.
Firmware Version	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.

System Configuration	The date and time of the last system configuration backup. Select <i>Backup/Restore</i> to browse to the <i>System Recovery</i> page.
Current User	The administrator that is currently logged on to the system.
Uptime	The duration of time that the FortiDeceptor unit has been running since it booted up.
Deception VM	<p>Deception VM license activation and initialization status.</p> <p>Displays an <i>up</i> icon if the Deception VM is activated and initialized. Displays a <i>Caution</i> icon if the Deception VM 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 > All Events</i> page.</p> <p>Click the <i>VM Images</i> to go to the images available on FortiDeceptor.</p> <p>After purchase, you should download the license file from the Fortinet Customer Service & Support portal. Then, click the <i>[Upload License]</i> link next to the Deception VM 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 VMs.</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:

CPU Usage	Gauges the CPU percentage usage.
Memory Usage	Gauges the Memory percentage usage.
Reboot/Shutdown	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.

Deception VM Distribution

This widget displays the following information and options:

Ubuntu	Shows the number of Ubuntu Deception VMs with the percentage on a pie chart.
Windows	Shows the number of Windows Deception 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.

Decoy Service Distribution

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

SSH	Shows the number of decoy images using SSH service with the percentage on a pie chart.
SAMBA	Shows the number of decoy images using SAMBA service with the percentage on a pie chart.
SMB	Shows the number of decoy images using SMB service with the percentage on a pie chart.
RDP	Shows the number of decoy images using RDP 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:

Summary	Disk summary information including RAID level and status.
RAID Level	Displays the RAID level.
Disk Status	Displays the disk status.
Disk Usage	Displays the current disk usage.
Disk Number	Displays the disk number.
Disk Size	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 47](#)
- [Microsoft Windows VM license activation on page 47](#)
- [Log out of the unit on page 48](#)
- [Refresh Current Web Page on page 48](#)
- [Table Customization on page 41](#)
- [Update the FortiDeceptor firmware on page 48](#)
- [Reboot and shut down the unit on page 49](#)
- [Back up or restore the system configuration on page 49](#)

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.
4. Click *Submit* to start the upgrade.

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 Deception 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:

Interface	The interface name and description, where applicable. Failover IP will be listed under this field with the following descriptor: <i>(cluster external port)</i> .
port1 (administration port)	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.
port2	Deception VM deployment.
port3 (VM outgoing interface)	Deception VM deployment.
port4	Deception VM deployment.
port5/port6	Deception VM deployment.
port7/port8	Deception VM deployment.
IPv4	The IPv4 IP address and subnet mask of the interface.

IPv6	The IPv6 IP address and subnet mask of the interface.
Interface Status	The state of the interface, one of the following states: <ul style="list-style-type: none"> Interface is up Interface is down Interface is being used by sniffer
Link Status	The link status. <ul style="list-style-type: none"> Link up Link down
Access Rights	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.
Edit	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:

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

The following information is displayed:

IP/Mask	Displays the IP address and subnet mask.
----------------	--

Gateway	Displays the gateway IP address.
Device	Displays the interface associated with the static route.
Number of Routes	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
Alert	Immediate action is required.	Suspicious URL visit domain.com from 192.12.1.12 to 42.156.162.21:80.
Critical	Functionality is affected.	System database is not ready. A program should have started to rebuild it and it shall be ready after a while.
Error	An erroneous condition exists and functionality is probably affected.	Errors that occur when deleting certificates.

Log Level	Description	Example Log Entry
Warning	Functionality might be affected.	Submitted file AVSInstallPack.exe is too large: 292046088.
Information	General information about system operations.	LDAP server information that was successfully updated.
Debug	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:

All Events	Shows all logs.
-------------------	-----------------

The following options are available:

Download Log	Select to download a file containing the raw logs to the management computer.
History Logs	Enable to include historical logs in Log Search.
Refresh	Select to refresh the log message list.
Add Search Filter	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.
Pagination	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:

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

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

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

Name	The name of the server entry.
Server Type	The server type. One of the following options: CEF or syslog.
Server Address	The log server address.
Port	The log server port number.
Status	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:

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

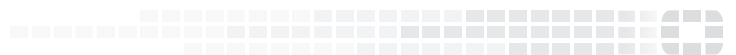
4. Select *OK* to save the entry.

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®, 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.