



FortiDeceptor - Administration Guide

Version 3.0.0

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 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



December 23, 2019

FortiDeceptor 3.0.0 Administration Guide

50-300-599498-20191223

TABLE OF CONTENTS

Change Log	5
Introduction	6
Set up FortiDeceptor	8
Connect to the GUI	8
Connect to the CLI	8
Change the system hostname	9
Change the administrator password	9
Configure the system time	9
Deploy Decoy VM	10
View available Deception OS	10
Set up the Deployment Network	11
Deploy Decoy VMs with the Deployment Wizard	11
Deploy the FortiDeceptor Token Package	13
Monitor Decoy & Lure Status	13
Decoy Map	15
Configure a Whitelist	15
DMZ Mode	16
Limitations of the DMZ Mode	16
Monitor Attacks	17
Analysis	17
Campaign	18
Attack Map	19
Incidents and Events Distribution	19
Incidents and Events Count	20
Top 10 Attackers by Events	20
Top 10 Attackers by Incidents	20
Top 10 IPS Attacks	20
Incidents Distribution by Service	21
Global Attacker Distribution	22
Fabric	23
Blocking	23
Quarantine Status	24
IOC Export	24
System	25
Administrators	25
Admin Profiles	27
Certificates	30
LDAP Servers	31
RADIUS Servers	32
Mail Server	34
SNMP	34

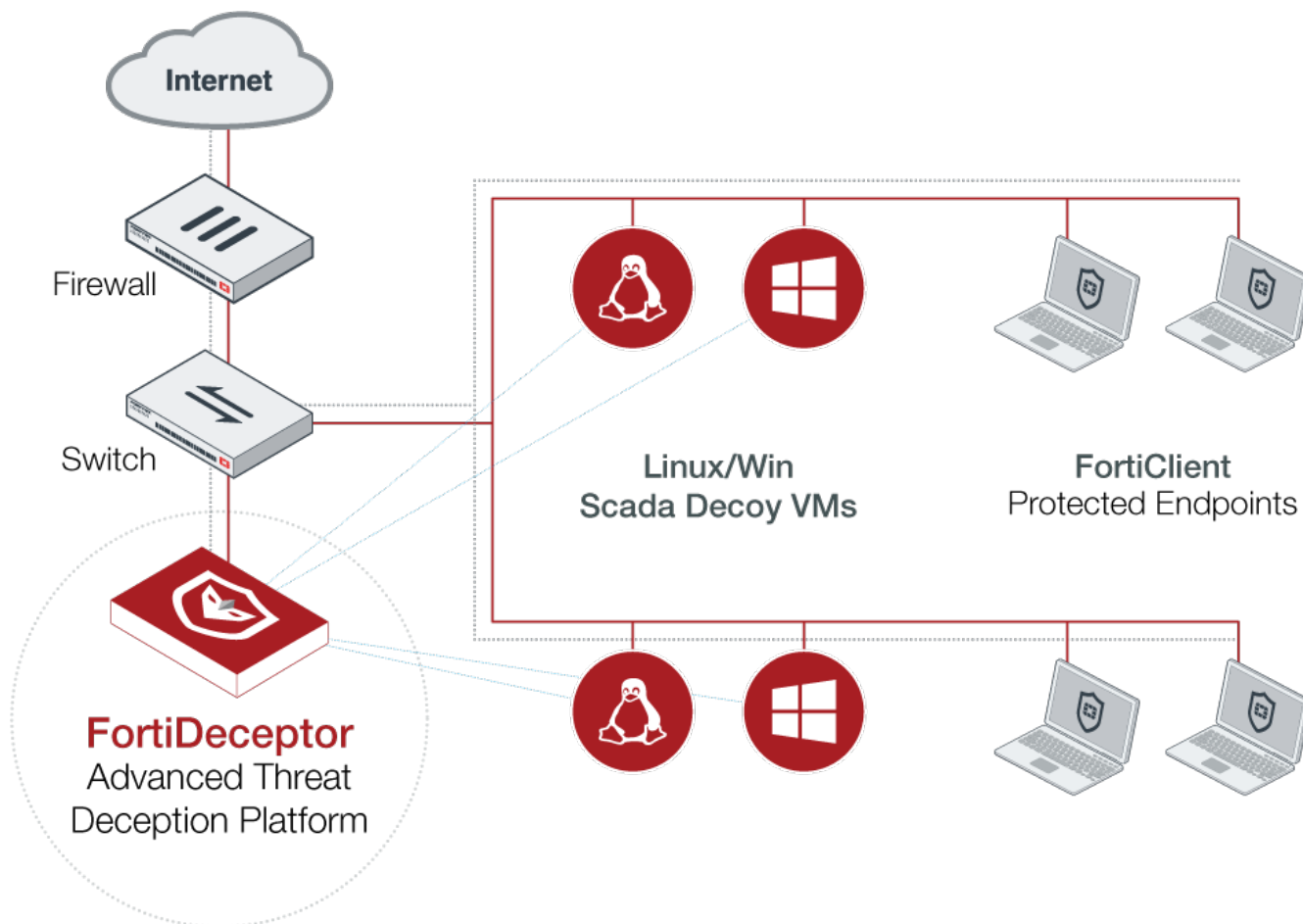
FortiGuard	37
Login Disclaimer	38
Table Customization	38
Settings	38
System Settings	39
Dashboard	39
Customizing the dashboard	39
System Information	41
System Resources	42
Decoy Distribution by OS	42
Lure Distribution	43
Top Critical Logs	44
Disk Monitor	44
Basic System Settings	44
Change the GUI idle timeout	44
Microsoft Windows VM license activation	45
Log out of the unit	45
Refresh Current Web Page	45
Update the FortiDeceptor firmware	45
Reboot and shut down the unit	46
Back up or restore the system configuration	47
Network	47
Interfaces	47
DNS Configuration	48
System Routing	49
System Log	50
Log Details	50
Logging Levels	50
Raw logs	51
Log Categories	52
Log Servers	53

Change Log

Date	Change Description
2019-12-23	Initial release.

Introduction

FortiDeceptor creates a network of decoy VMs to lure attackers and monitor their activities on the network. When 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. Use tokens to influence attackers' lateral movements and activities. Examples of what you can use in a token include: cached credentials, database connections, network share, data files, and configuration files.
- Monitor the hacker's actions: Monitor *Incidents*, *Events*, and *Campaign*.
 - An *Event* represents a single action, for example, a login-logout event 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 related *Incidents* 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 section explains the initial set up of FortiDeceptor such as connecting to the GUI and CLI, changing the hostname, changing the administrator password, and configuring the system time.

Connect to the GUI

Use the GUI to configure and manage FortiDeceptor.

To connect to the FortiDeceptor GUI:

1. Connect the port1 (administration) interface of the device to a management computer using an 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. Use web browser to go to `https://192.168.0.99`.
4. Type `admin` in the *Name* field, leave the *Password* field blank, and click *Login*.
You can now proceed with configuring your FortiDeceptor unit.



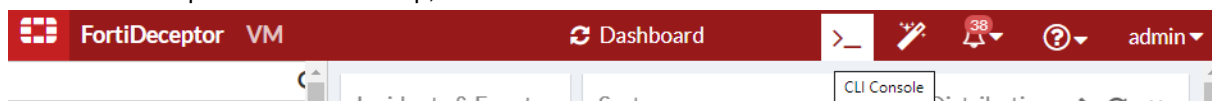
If the network interfaces have been configured differently during installation, the URL and administrative access protocols might not be in their default state.

Connect to the CLI

You can use CLI commands to configure and manage FortiDeceptor. This topic shows how to connect to the unit using the CLI.

To connect to the FortiDeceptor CLI:

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



The *CLI Console* pane opens.

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

Change the system hostname

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

To change the host name:

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

Change the administrator password

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

To change the password of the logged in administrator:

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

To change the administrator password in the Administrators page:

1. Go to *System > Administrators*.
2. Select the administrator account you want to edit.
3. Click *Edit*.
4. Change the password and click *OK*.

Configure the system time

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

To configure the system time:

1. Go to *Dashboard > System Information > System Time*.
2. Click *Change*.
3. Set the system time and click *Apply*.
You might need to log in again.

Deploy Decoy VM

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

Apart from the default decoy Windows, Linux, or SCADA OS images, FortiDeceptor supports custom OS images with a purchased subscription service. You can upload your custom ISO images and install the FortiDeceptor Toolkit on the image. For instructions, click the Help icon in the toolbar and select Customization.

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 10](#).
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 11](#).
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 13](#).
5. Go to *Deception > Decoy Map* to see the network of Decoy VMs. See [Decoy Map on page 15](#).
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 15](#).

View available Deception OS

The *Deception OS* page lists the deception OSes available for creating Decoy VMs.

Column	Description
Delete	Delete a custom OS that you have applied.
Status	Status of the Deception OS is <i>Initialized</i> or <i>Not Initialized</i> .
Name	Name of the Deception OS.
OS Type	Operating System type.
VM Type	VM type of the Deception OS endpoint.
Lures	Lures 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

Use the *Deployment Network* page to set up a monitoring interface into a VLAN or a subnet.

To add a VLAN or subnet to FortiDeceptor:

1. Go to *Deception > Deployment Network*.
2. Enable *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* and click *OK*.
You can select multiple ports.
4. Click *Add New VLAN/Subnet* to manually add a VLAN or a subnet to FortiDeceptor. Configure the following settings:

Interface	The port that connects to the VLAN or subnet.
VLAN ID	A unique integer ID of the VLAN.
Deploy Network IP/Mask	The IP address to monitor. This is useful to mask the actual IP address.
Ref	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 network IP/mask must be an IP address and not a subnet.

You must use the following guidelines to set the network IP/mask:

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

Deploy Decoy VMs with the Deployment Wizard

Use the *Deployment Wizard* to create and deploy Decoy VMs on your network. Decoy VMs appear as real endpoints to hackers 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:


Name	Specify the name of the deployment profile. Maximum 15 characters using A-Z, a-z, 0-9, dash, or underscore. No duplicate profile names.
Available Deception OSes	Select a Deception OS.
Selected Services	Displays the selected services. You cannot edit this field.

4. For an Ubuntu VM, turn on SSH or SAMBA.

For Windows, turn on RDP or SMB.

For SCADA, turn on HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, or IEC104.

5. Click *Add Lure* for the service and configure the following:

Username	Specify the username for the decoy. Maximum 19 characters using A-Z, a-z, or 0-9.
<div>  <p>Do not set the username of the lures to be the same as existing usernames 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> </div>	
Password	Specify the password for the decoy in 1-14 non-unicode characters.
Sharename	This option is only available for SAMBA (Ubuntu) or SMB (Windows). Specify a Sharename in 3-63 characters using A-Z, a-z, or 0-9.
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 lure.

6. To launch the decoy VM immediately, enable *Launch Immediately*.7. To reset the decoy VM after it detects incidents, enable *Reset Decoy* and specify the *Reset Interval* value in seconds.8. Click *Next*.9. The *Hostname* can start with an English character or a digit, and must not end with a hyphen. Maximum 15 characters using A-Z, a-z, 0-9, or hyphen (case-sensitive). Other symbols, punctuation, or white space are not allowed. The *Hostname* cannot conflict with decoy names.10. Click *Add Interface*.11. In the *Add Interface for Decoy* pane, select the *Deploy Interface*. Set this to the VLAN or subnet added in [Set up the Deployment Network on page 11](#)12. Configure the following settings in the *Add Interface for Decoy* pane:

Addressing Mode	Select <i>Static</i> or <i>DHCP</i> . <i>Static</i> allows you to configure the IP address for all the decoys. <i>DHCP</i> allows the decoys to receive IP address from the DHCP server. If you select <i>DHCP</i> , <i>IP Count</i> is automatically set to 1 and all other fields are not applicable.
Network Mask	This field is set automatically.

Gateway	Specify the gateway.
IP Count	Specify the number of IP addresses to be assigned, up to 16. If <i>Addressing Mode</i> is DHCP, <i>IP Count</i> is automatically set to 1.
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> .

13. Click *Done*.
14. To deploy the decoys on the network, click *Deploy*.
15. To save this as a template in *Deception > Deployment Wizard*, click *Template*.

Deploy the FortiDeceptor Token Package

Use a FortiDeceptor Token Package to add breadcrumbs on real endpoints and lure an attacker to a Decoy VM. Tokens are normally distributed within 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 > Decoy & Lure Status*.
2. Select the Decoy VM by clicking its checkbox.
3. To download the FortiDeceptor Token Package, click *Download Package*.
You can only download packages with valid IP addresses. A package must have a status of *Initialized*, *Stopped*, *Running*, or *Failed*.
4. Copy the FortiDeceptor Token Package to an endpoint such as a Windows or Linux endpoint.
5. Unzip the FortiDeceptor Token Package:
 - For Windows, copy the file in the *Windows* directory and run *windows_token.exe* by double-clicking the file.
 - For Ubuntu, open Terminal and run *python ./ubuntu_token.py*.

When 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.

Monitor Decoy & Lure Status

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



We recommend operating Decoy VMs with the same status for expected behavior.

To view the Deception Status:

1. Go to *Deception > Decoy & Lure Status*.

Action	Click <i>View detail</i> to see the decoy's configuration details. Click <i>Copy to Template</i> to duplicate the decoy as a template. Click <i>Start</i> or <i>Stop</i> to start or stop the decoy. Click <i>Delete</i> to delete the decoy. Click <i>Download</i> to download the FortiDeceptor Token Package. Click <i>VNC</i> to open a VNC of the decoy.
Status	The current status of the decoy can be <i>Initializing</i> , <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.
Decoy Name	Name of the decoy.
OS	Operating system of the decoy.
VM	The name of the Decoy VM.
Enabled Services	The number of decoy services enabled on this VM.
IP	The IP address of the Decoy VM.
Services	List of services enabled. Hover over an icon to see a text list.
Network Type	Shows if the IP address is <i>Static</i> or <i>DHCP</i> .
DNS	DNS of the Decoy VM.
Gateway	Gateway of the Decoy VM.

To delete one or more Decoy VMs:

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

Decoy Map

Deception > Decoy Map is a visual representation of the entire network showing real endpoints and Decoy VMs. You can apply filters to focus on specific decoys.

To work with the Decoy Map:

1. Go to *Deception > Decoy Map*.
2. To change the display, drag items to another location, and scroll to zoom in or out.
3. Click a node to see its information.
4. Click *Click to begin filtering* to select a different filter type and type values.
Filter types include *Decoy Name*, *Decoy IP*, and *Lure Type*.
You can use multiple arguments with different filter types. All filter arguments and time indicator arguments are considered "AND" conditions.
5. To locate the node on the map, use the *LOCATE BY IP* box.
6. To save a snapshot of the map, click *Save view* .

Configure a Whitelist

Use the *Whitelist* page to add an IP address for an administrator to log into the network. User actions from a whitelisted IP address are recorded as an *Event* or *Incident*.

To add a new whitelist IP:

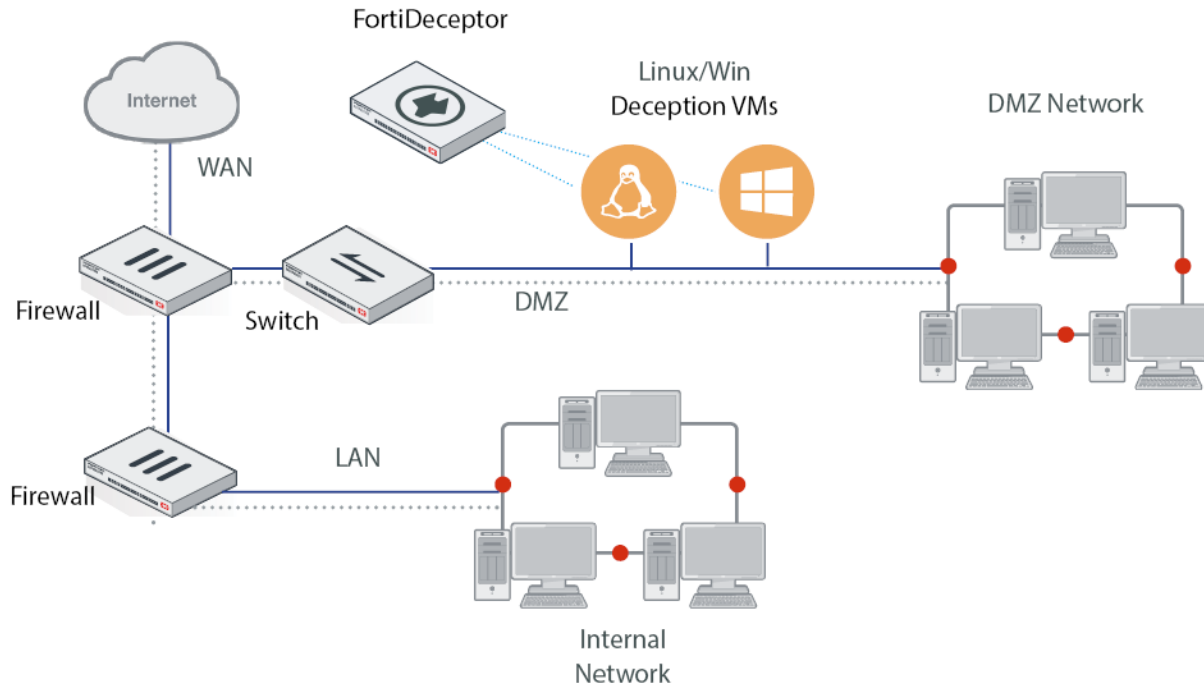
1. Go to *Deception > Whitelist*.
2. Click *Add New Whitelist IP* and configure its settings:

IP Address	Specify the IP address from where the connection originates.
Source Ports	Specify the source ports from where the connection originates.
Destination Ports	Specify the destination ports 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> .

3. Click *Update*.

DMZ Mode

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



Limitations of the DMZ Mode

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

- When DMZ mode is enabled, the banner displays *DMZ-MODE*.
- In *Deception > Deployment Network*, *Deception Monitor IP/Mask* is hidden. See [Set up the Deployment Network on page 11](#).
- In *Deception > Decoy & Lure Status* in the Deception Status view, the Attack Test selection is disabled.
- Decoy VMs are limited to one deploy Interface. For information about IP address range, see [Deploy Decoy VMs with the Deployment Wizard on page 11](#).

To enable DMZ mode in the CLI:

```
dmz-mode -e
```

To disable DMZ mode in the CLI:

```
dmz-mode -d
```



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

Monitor Attacks

Administrators can monitor attacks in two ways:

To monitor attacks using Incident pages:

- *Incident > Analysis* lists incidents and related events detected by FortiDeceptor. See [Analysis on page 17](#).
- *Incident > Campaign* lists attacks and related events detected by FortiDeceptor. See [Campaign on page 18](#).
- *Incident > Attack Map* shows attacks and related events detected by FortiDeceptor. See [Attack Map on page 19](#).

To monitor attacks using widgets:

- Use the *Incidents and Events Distribution* widget. See [Incidents and Events Distribution on page 19](#).
- Use the *Incidents and Events Count* widget. See [Incidents and Events Count on page 20](#).

Analysis

Incident > Analysis lists the *Incidents* detected by FortiDeceptor. You can download the detailed analysis report by clicking *Export to PDF*.

To use the Analysis page:

1. Go to *Incident > Analysis*.
2. The *Analysis* page displays the list of events:

Severity	Severity of the event.
Last Activity	Date and time of the last activity.
Type	Type of event.
Attacker IP	Attacker IP mask.
Attacker User	Attacker username.
Victim IP	IP address of the victim.
Start	Date and time when the attack started.
Attacker Port	Port 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	If the Decoy VM captured network traffic or files, download the PCAP files or dumped 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 table view.

3. To refresh the data, click *Refresh*.
4. To download the detailed analysis report in PDF format, click *Export to PDF*.
5. To mark items as read, expand the incident details or click *Mark all as read*.
Newly-detected incidents are in bold to indicate they are unread.
6. To display specific types of events, click *Show All*, *IPS Events Only*, or *Web Filter Events Only*.

Campaign

Incident > Campaign lists the *Attacks* detected by FortiDeceptor. An *Attack* consists of multiple *Incidents*.

To use the Campaign page:

1. Go to *Incident > Campaign*.
2. The *Campaign* page displays the list of attacks:


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

3. To refresh the data, click *Refresh*.
4. To export the data, click *Export to PDF*.

Attack Map

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

To work with the Attack Map:

1. Go to *Incident > Attack Map*.
2. At the bottom of the Attack Map, drag the timeline indicator to set the 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. To change the display, drag items to another location, and scroll to zoom in or out.
4. Click *Click to begin filtering* to select a different filter type and type values.
Filter types include *Attacker IP*, *Victim IP*, and *Decoy IP*.
You can use multiple arguments with different filter types. All filter arguments and time indicator arguments are considered "AND" conditions.
5. To locate the node on the map, use the *LOCATE BY IP* box.
6. To save a snapshot of the map, click *Save view* .

Incidents and Events Distribution

This dashboard widget displays the number of incidents and events with the following risk level information and options:

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

Hover over the pie chart to see the number of *Incidents* or *Events* and their percentage.

To customize this widget:

1. Click the edit icon where you can make the following changes:
 - Enter a *Customized Widget Title*.
 - Change the *Refresh Interval*.
 - Select a *Time Period*: *Last 24 hours*, *Last 7 days*, or *Last 4 weeks*.

Incidents and Events Count

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

Event	Click <i>Event</i> to show or hide the number of events in the time period. Events are in blue.
Incidents	Click <i>Incident</i> to show or hide the number of incidents in the time period. Incidents are in orange.
Time/Date	The time or date the <i>Incident</i> or <i>Event</i> occurred.

To customize this widget:

1. Click the edit icon where you can make the following changes:
 - Enter a *Customized Widget Title*.
 - Change the *Refresh Interval*.
 - Select a *Time Period*: *Last 24 hours*, *Last 7 days*, or *Last 4 weeks*.

Top 10 Attackers by Events

This dashboard widget displays the top ten attackers by the number of events.

IP Address	IP address of the attacker.
Number of Events	Hover over an IP address to see the total number of <i>Events</i> .

Top 10 Attackers by Incidents

This dashboard widget displays the top ten attackers by the number of incidents.

IP Address	IP address of the attacker.
Number of Incidents	Hover over an 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:

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

Use the *Fabric* pages 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.

Fabric provides access to the following pages:

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

Use *FortiGate Integration* to configure FortiGate settings for integration with FortiDeceptor. FortiDeceptor uses FortiGate REST APIs to make quarantine calls when decoys are accessed. Attackers are immediately quarantined on the FortiGate for further analysis.

The following options are available:

Severity level	Select the security level. The selected level and all levels above it are blocked. For example, if you select <i>Medium</i> , then medium, high, and critical levels are blocked. If you select <i>Critical</i> , then only the critical level is blocked.
Add new block configuration	Create a new FortiGate integration setting.
Update	Save the modified FortiGate integration setting to a configuration file.
Cancel	Discard current changes.
Edit	Edit the record.
Delete	Delete the record.
Test	Manually send quarantine request to the corresponding FortiGate.

The following information is displayed:

Name	Alias name of the integrated FortiGate.
IP	IP address of the integrated FortiGate.
User	Username of the integrated FortiGate.
Password	Password of that username.

Port	Port number of the integrated FortiGate REST API service. Default port number is 443.
Default Expiry	Default blocking time in second. Default is 3600 seconds.
Default VDOM	The default access VDOM of the integrated FortiGate.
Type	FortiGate (read only value).
Enabled	Enable or disable the integration setting.

Quarantine Status

The *Quarantine Status* page displays the status of blocking and quarantined IP addresses. It also lets you manually block or unblock devices. The following options are available:

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

The following information is displayed:

Attacker IP address	IP addresses of blocked attacker.
Start	Start time of blocking behavior.
End	End time of blocking behavior.
Handler Address	IP address of the integrated FortiGate.
Handler	The integrated device type.
Handle Type	Blocking type, manual, or automatic quarantine.
VDOM	VDOM of the integrated FortiGate.
Time Remaining	The remaining blocking time.
Status	Current status of the attacker.
Message	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. You can choose to include MD5 checksums, WCF category, and reconnaissance alerts.

System

Use the *System* pages 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 Login Disclaimer.
Settings	Configure the idle timeout for GUI and CLI, configure GUI language, toggle left menu mode, and reset all widgets to their default state.
Table Customization	Define columns and order of <i>Incident</i> and <i>Event</i> tables.

Administrators

Use the *Administrators* page to configure administrator user accounts.

If the user whose Admin Profile does not have *Read Write* privilege under *System > Admin access*, the user can only view and edit their own information.

The following options are available:

Create New	Create a new administrator account.
Edit	Edit the selected entry.
Delete	Delete the selected entry.
Test Login	Test the selected user's login settings. If an error occurs, a debug message appears.

The following information is displayed:

Name	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. Click *Create New*.
3. Configure the following:

Administrator	Name of the administrator account. The name must be 1 to 30 characters using only upper-case letters, lower-case letters, numbers, or the underscore character (_).
Password	Password of the account. The password must be 6 to 64 characters using only upper-case letters, lower-case letters, numbers, or special characters. This field is available when <i>Type</i> is set to <i>Local</i> .
Confirm Password	Confirm the password for the account.
Type	Select <i>Local</i> , <i>LDAP</i> , or <i>RADIUS</i> .
LDAP Server	When <i>Type</i> is <i>LDAP</i> , select a <i>LDAP Server</i> . For information on creating an LDAP server, see LDAP Servers on page 31 .
RADIUS Server	When <i>Type</i> is <i>RADIUS</i> , select a <i>RADIUS Server</i> . For information on creating a RADIUS server, see RADIUS Servers .
Admin Profile	Select the Admin Profile.
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 comment.



Setting trusted hosts for administrators limits what computers an administrator can use to log into FortiDeceptor. When you identify a trusted host, FortiDeceptor only accepts the administrator's login from the configured IP address or subnet. Attempts to log in with the same credentials from another IP address or subnet are dropped.

4. Click *OK*.

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 want to edit and click *Edit*.
Only the *admin* user can edit its own settings.
You must enter old password before you can set a new password.
3. Edit the account and click *OK*.

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. Click *Delete* and confirm that you want to delete the user.

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. Click *Test Login*.
4. Enter the user password.
5. Click *OK*.

If an error occurs, a debug message appears.



When a remote RADIUS server is configured for two-factor authentication, RADIUS users must enter a FortiToken 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.

You also need a code for the test login.

Admin Profiles

Use administrator profiles to control administrator access privileges to system features. When you create an administrator account, you assign a profile to the account.

You cannot modify or delete the following predefined administrator profiles:

- *Super Admin* has access to all functionality.
- *Read only* has read-only access.

Only the Super Admin 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*.

The *Menu Access* section has the following settings:

None	User cannot view or make changes to the system.
-------------	---

Read Only	User can view but not make any change to the system, except session-related user settings such as Table Customization/Dashboard/Attack Map filter.
Read Write	User can view and make changes to the system.

The *CLI Commands* section has the following settings:

None	User cannot execute CLI commands.
Execute	User can execute CLI commands.

To create a new Administrator Profile:

1. Go to *System > Admin Profiles*.
2. Click *Create New*.
3. Specify the *Profile Name*.
4. If you wish, add a *Comment*.
5. Specify the privileges for *Menu Access*:
 - Dashboard
 - Dashboard
 - Deception
 - Customization
 - 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
- Log
 - All Events
 - Log Servers

6. Specify the privileges for *CLI Commands*:

- 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

7. Click *Save*.

Certificates

Use this page to import, view, and delete certificates. Certificates are used for secure connection to an LDAP server, system HTTPS and SSH services. FortiDeceptor has one default certificate *firmware*.

FortiDeceptor does not support generating certificates. FortiDeceptor supports importing certificates for SSH and HTTPS access using `.crt`, `PKCS12`, or `.pem` format.

The following options are available:

Import	Import a certificate.
Service	Configure specific certificates for HTTP and SSH servers.
View	View the selected CA certificate details.
Delete	Delete the selected certificate.

The following information is displayed:

Name	Name of the certificate.
Subject	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. Click *Import*.
3. Enter the *Certificate Name*.
4. If you want to import a password protected PKCS12 certificate, select *PKCS12 Format*.
5. Click *Choose File* and locate the certificate and key files on your management computer.
6. Click *OK* to import the certificate.

To view a certificate:

1. Go to *System > Certificates*.
2. Select a certificate and click *View*.

The following information is available:

Certificate Name	Name of the certificate.
Status	Certificate status.
Serial number	Certificate serial number.
Issuer	Issuer of the certificate.
Subject	Subject of the certificate.

Effective date	Date and time that the certificate became effective.
Expiration date	Date and time that the certificate expires.

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

To delete a CA certificate:

1. Go to *System > Certificates*.
2. Select the certificate you want to delete.
3. Click *Delete* and confirm you want to delete the certificate.



You cannot delete the *firmware* certificate.

LDAP Servers

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

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

The following options are available:

Create New	Add an LDAP server.
Edit	Edit the selected LDAP server.
Delete	Delete the selected LDAP server.

The following information is displayed:

Name	LDAP server name.
Address	LDAP server address.
Common Name	LDAP common name.
Distinguished Name	LDAP distinguished name.
Bind Type	LDAP bind type.
Connection Type	LDAP connection type.

To create a new LDAP server:

1. Go to *System > LDAP Servers*.
2. Click *Create New*.
3. Configure the following settings:

Name	A unique name to identify the LDAP server.
Server Name/IP	IP address or FQDN of the LDAP server.
Port	The port for LDAP traffic. The default port is 389.
Common Name	Common name identifier of the LDAP server. Most LDAP servers use <code>cn</code> . Some servers use other common name identifiers such as <code>uid</code> .
Distinguished Name	Distinguished name used to look up entries on LDAP servers. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
Bind Type	The type of binding for LDAP authentication: <ul style="list-style-type: none"> • <i>Simple</i> • <i>Anonymous</i> • <i>Regular</i>
Username	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the user name.
Password	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the password.
Enable Secure Connection	Use a secure LDAP server connection for authentication.
Protocol	When <i>Enable Secure Connection</i> is selected, select <i>LDAPS</i> or <i>STARTTLS</i> .
CA Certificate	When <i>Enable Secure Connection</i> is selected, select a <i>CA Certificate</i> .

4. Click *OK*.

RADIUS Servers

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

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

The following options are available:

Create New	Add a RADIUS server.
-------------------	----------------------

Edit	Edit the selected RADIUS server.
Delete	Delete the selected RADIUS server.

The following information is displayed:

Name	RADIUS server name.
Primary Address	Primary server IP address.
Secondary Address	Secondary server IP address.
Port	Port used for RADIUS traffic. The default port is 1812.
Auth Type	The authentication type the RADIUS server requires. Select <i>Any</i> , <i>PAP</i> , <i>CHAP</i> , or <i>MSv2</i> . <i>Any</i> means FortiDeceptor tries all authentication types.

To add a RADIUS server:

1. Go to *System > RADIUS Servers*.
2. Click *Create New*.
3. Configure the following settings:

Name	A unique name to identify the RADIUS server.
Primary Server Name/IP	IP address or FQDN of the primary RADIUS server.
Secondary Server Name/IP	IP address or FQDN of the secondary RADIUS server.
Port	Port for RADIUS traffic. The default port is 1812.
Auth Type	Authentication type the RADIUS server requires. Select <i>Any</i> , <i>PAP</i> , <i>CHAP</i> , or <i>MSv2</i> . <i>Any</i> means FortiDeceptor tries all authentication types.
Primary Secret	Primary RADIUS server secret.
Secondary Secret	Secondary RADIUS server secret.
NAS IP	NAS IP address.

4. Click *OK*.

Mail Server

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

You can configure the following options:

Send Incidents Alerts	When enabled, FortiDeceptor sends an email alert to the <i>Receiver Email List</i> when it detects an incident.
SMTP Server Address	SMTP server address.
Port	SMTP server port number.
E-Mail Account	The mail server email account. This is the "from" address.
Login Account	The mail server login account.
Password and Confirm Password	Enter and confirm the password.
Receiver Email List	Enter one or more receiver email addresses.
Send Test Email	Send a test email to the global email list. If an error occurs, the error message appears at the top of the page and is recorded in the System Logs.

SNMP

SNMP is a method to monitor your FortiDeceptor system on your local computer. You 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.

You can also download FortiDeceptor and Fortinet core MIB files.

Configure the SNMP agent

The SNMP agent sends SNMP traps that originate on FortiDeceptor 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 then generate reports or graphs.

The SNMP manager can monitor FortiDeceptor to determine if it is operating properly or if critical events are occurring. The description, location, and contact information for this FortiDeceptor system is part of the information an SNMP

manager collects. This information is useful if the SNMP manager is monitoring many devices, and it enables a faster response when FortiDeceptor requires attention.

To configure SNMP agents:

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

SNMP Agent	When enabled, the FortiDeceptor SNMP agent sends FortiDeceptor SNMP traps.
Description	Description of this FortiDeceptor to identify this unit.
Location	Location of this FortiDeceptor if it requires attention.
Contact	Contact information of the person in charge of this FortiDeceptor.
SNMP v1/v2c	Create, edit, or delete SNMP v1 and v2c communities. You can enable or disable communities in the edit page. Columns include: <i>Community Name, Queries, Traps, Enable</i> .
SNMP v3	Create, edit, or delete SNMP v3 entries. You can enable or disable queries in the edit page. Columns include: <i>Username, Security Level, Notification Host, Queries</i> .

To create an SNMP v1/v2c community:

1. Go to *System > SNMP*.
2. In the SNMP v1/v2c section, click *Create New*.
3. Configure the following settings:

Enable	Enable the SNMP community.
Community Name	The name that identifies the SNMP community.
Hosts	The list of hosts that can use the settings in this SNMP community to monitor FortiDeceptor.
IP/Netmask	IP address and netmask of the SNMP hosts. Click <i>Add</i> to add additional hosts.
Queries v1	Port number and if it is enabled.
Queries v2c	Enable queries for each SNMP version that FortiDeceptor uses.
Traps v1	Local port number, remote port number, and if it is enabled.
Traps v2c	Enable traps for each SNMP version that FortiDeceptor uses.
SNMP Events	Events that cause FortiDeceptor 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

4. Click *OK*.

To create an SNMP v3 user:

1. Go to *System > SNMP*.
2. In the SNMP v3 section, click *Create New*.
3. Configure the following settings:

Username	Name of the SNMPv3 user.
Security Level	Security level of the user: <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	Authentication method: <ul style="list-style-type: none"> • MD5 (Message Digest 5 algorithm) • SHA1 (Secure Hash algorithm)
Password	Authentication password of at least eight characters.
Encryption	Encryption is required if <i>Security Level</i> is <i>Encryption and authentication</i> .
Method	Encryption method: <ul style="list-style-type: none"> • DES • AES
Key	Encryption key of at least eight characters.
Notification Hosts (Traps)	
IP/Netmask	IP address and netmask. Click <i>Add</i> to add more hosts.
Query	
Port	Port number and if it is enabled.
SNMP V3 Events	SNMP events 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

4. Click *OK*.

To download MIB files:

1. At the bottom of the SNMP page, select the MIB file you want 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: 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.
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

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.
Lure Distribution	Displays the number of decoys deployed with the chart showing the type of service (SSH, Samba, SMB, SCADA or RDP).
Decoy VM Distribution by OS	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.

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 *Add*, 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 41](#)
- [System Resources on page 42](#)
- [Decoy Distribution by OS on page 42](#)
- [Lure Distribution on page 43](#)
- [Incidents and Events Distribution on page 19](#)
- [Incidents and Events Count on page 20](#)
- [Top Critical Logs on page 44](#)
- [Disk Monitor on page 44](#)

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	Enter a refresh interval for the widget, in seconds. Some widgets have default refresh values: <ul style="list-style-type: none"> • System Information: 90 • System Resources: 10 • Decoy Distribution by OS: 300

	<ul style="list-style-type: none"> • Lure 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 <i>[Update]</i> 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 OS	Deception OS license activation and initialization status.

Displays an *up* icon if the Deception OS is activated and initialized. Displays a *Caution* 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 *Log > All Events* page.

Click *Deception OS* to go to the images available on FortiDeceptor.

After purchase, you should download the license file from the [Fortinet Customer Service & Support](#) portal. Then, click the *[Upload License]* link next to the Deception OS field. Browse to the license file on the management computer, and click the *Submit* button. The system will reboot and activate the newly installed Deception OS.



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.

Decoy Distribution by OS

This widget displays the following information and options:

Ubuntu	Shows the number of Ubuntu Decoy VMs with the percentage on a pie chart.
Windows	Shows the number of Windows Decoy VMs with the percentage on a pie chart.
SCADA	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:

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.
HTTP	Shows the number of decoy images using HTTP service with the percentage on a pie chart.
FTP	Shows the number of decoy images using FTP service with the percentage on a pie chart.
TFTP	Shows the number of decoy images using TFTP service with the percentage on a pie chart.
SNMP	Shows the number of decoy images using SNMP service with the percentage on a pie chart.
MODBUS	Shows the number of decoy images using MODBUS service with the percentage on a pie chart.
S7COMM	Shows the number of decoy images using S7COMM service with the percentage on a pie chart.
BACNET	Shows the number of decoy images using BACNET service with the percentage on a pie chart.
IPMI	Shows the number of decoy images using IPMI service with the percentage on a pie chart.
TRICONEX	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:

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 44](#)
- [Microsoft Windows VM license activation on page 45](#)
- [Log out of the unit on page 45](#)
- [Refresh Current Web Page on page 45](#)
- [Table Customization on page 38](#)
- [Update the FortiDeceptor firmware on page 45](#)
- [Reboot and shut down the unit on page 46](#)
- [Back up or restore the system configuration on page 47](#)

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:

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	Decoy VM deployment.
port3	Decoy VM deployment.
port4	Decoy VM deployment.
port5/port6	Decoy VM deployment.
port7/port8	Decoy 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© 2020 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.