

Administration Guide

FortiDeceptor 4.2.0



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/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



October 31, 2022

FortiDeceptor 4.2.0 Administration Guide

50-420-801591-20221025

TABLE OF CONTENTS

Change Log	6
Introduction	7
Set up FortiDeceptor	8
Connect to the GUI	8
Connect to the CLI	9
Change the system hostname	9
Change the administrator password	10
Configure the system time	10
Upload license file to FortiDeceptor	10
Default port information	10
Central Management	11
Remote Client	12
Configuring Central Management	13
Deploy Decoy VM	16
Custom Decoy Image	16
Customize the deception base OS image	17
Deception OS	39
Deployment Network	40
Setting up the deployment network	41
Deploy Decoy VMs with the Deployment Wizard	42
Lure Settings	44
Deploy the FortiDeceptor token package	48
Decoy Status	51
Deployment Map	53
Discover & Deploy	54
Asset Discovery	55
Configure a Safe List	57
Lure Resources	57
Uploading lure resources	57
Importing users from LDAP	58
DMZ Mode	59
Limitations of the DMZ Mode	60
Monitor Attacks	61
Analysis	62
Table settings	63
Viewing the incident details	65
Campaign	66
Attack Map	68
Incidents and Events Distribution	69
Incidents and Events Count	70
Top 10 Attackers by Events	70
Top 10 Attackers by Incidents	70

Top 10 IPS Attacks	71
Incidents Distribution by Service	71
Supported services	71
Global Attacker Distribution	72
Fabric	73
Detection Devices	73
FortiSandbox	74
Cuckoo Sandbox	74
Virus Total	75
Quarantine Integration	75
FortiDeceptor on FortiGate Security Fabric topology map	75
FortiDeceptor integration for threat response mitigation	79
Integrate Method settings	82
Quarantine Status	85
IOC Export	86
System	88
Administrators	88
Admin Profiles	90
Certificates	92
LDAP Servers	94
RADIUS Servers	95
Mail Server	97
SNMP	98
FortiGuard	101
FDC License	103
Settings	104
Login Disclaimer	104
Table Customization	105
System Settings	106
Dashboard	106
Customizing the dashboard	108
System Information	109
System Resources	110
Decoy Distribution by OS	110
Lure Distribution	111
Top Critical Logs	112
Disk Monitor	112
Basic System Settings	113
Change the GUI idle timeout	113
Log out of the unit	113
Update FortiDeceptor firmware	113
Reboot or shut down the unit	114
Back up or restore the system configuration	114
Network	115
Interfaces	115
DNS Configuration	116

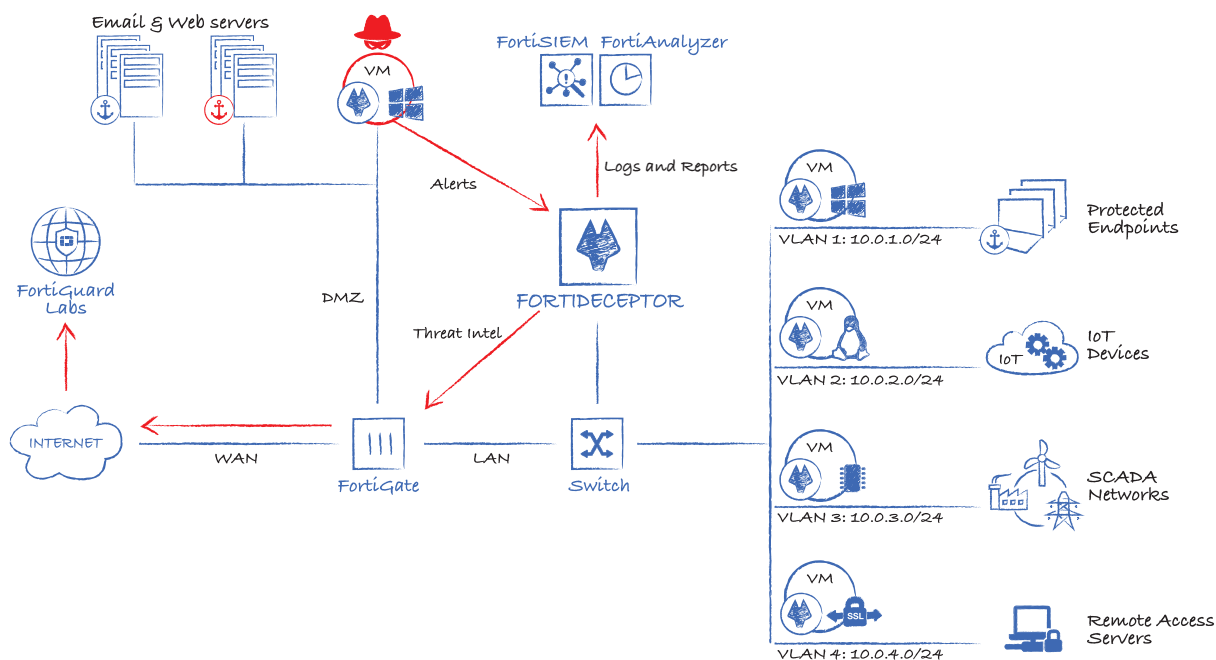
System Routing	116
System Log	118
Logging Levels	118
Raw logs	118
Log Categories	120
Log Servers	120
Deploying FortiDeceptor in offline or air-gapped networks	122
Deception VM security	122
Applying the license in an offline or air-gapped network	122
Importing deception VMs in an offline or air-gapped network	124
Importing firmware in an offline or air-gapped network	126
Importing an FDS package via FDC GUI in an offline or air-gapped network	126
Importing FDS package and license file via FortiManager in an offline or air-gapped network	127
Appendix A - Deception deployment best practices	130
Deception strategy	130
Deception strategy components	131
Deception strategy goals	131
Deception philosophy	131
Deception light stack vs full stack	132
FortiDeceptor platform	132
FortiDeceptor components	133
FortiDeceptor Token Package	133
FortiDeceptor decoys	134
Decoy services details	135
Deploying deception	143
Deception decoy best practices	144
Deception token best practices	147
AD integration best practices	148
Deployment best practices checklist	149
Network topology best practices	150
Attack vectors vs deception	154
Compromised internal endpoint using lateral movement	154
Lateral movement based on AD mapping	156
Lateral movement based on Mimikatz / PTH	157
Deploying tokens using AD GPO logon script	158
Configuring the GPO logon script	160
Configuring trunk ports on FortiDeceptor VM	163
Configuring FortiDeceptor	167
Configuring the vSwitch	170
How to setup and use LDAP/RADIUS servers	174

Change Log

Date	Change Description
2022-04-28	Initial release.
2022-05-10	Updated Deploy the FortiDeceptor token package on page 48 , Lure Settings on page 44 , Admin Profiles on page 90 , Detection Devices on page 73 , Deploying tokens using AD GPO logon script on page 158 . Added FDC License on page 103 .
2022-05-11	Updated Deployment Network on page 40 . Added Asset Discovery on page 55 .
2022-05-13	Updated Integrate Method settings on page 82 , Deploy Decoy VMs with the Deployment Wizard on page 42 , Analysis on page 62 , Quarantine Integration on page 75 Added Detection Devices on page 73 , Integrate Method settings on page 82
2022-05-25	Updated Deployment Network on page 40 .
2022-05-31	Updated FortiDeceptor decoys on page 134 Added How to setup and use LDAP/RADIUS servers on page 174 .
2022-05-31	Updated FDC License on page 103 .
2022-06-14	Updated Deployment Map on page 53 .
2022-06-28	Updated Set up FortiDeceptor on page 8 , Default port information on page 10 , Central Management on page 11 , Custom Decoy Image on page 16 , DMZ Mode on page 59 , Attack Map on page 68 , Mail Server on page 97 , Admin Profiles on page 90 , Mail Server on page 97 , SNMP on page 98 , FortiGuard on page 101 , Settings on page 104 , Customizing the dashboard on page 108 , System Information on page 109 , Update FortiDeceptor firmware on page 113 , Reboot or shut down the unit on page 114 , Deploying FortiDeceptor in offline or air-gapped networks on page 122 , Applying the license in an offline or air-gapped network on page 122 , Importing an FDS package via FDC GUI in an offline or air-gapped network on page 126 , Importing an FDS package via FDC GUI in an offline or air-gapped network on page 126 ,
2022-06-29	Updated FortiGuard on page 101 and Central Management on page 11
2022-07-25	Updated Custom Decoy Image on page 16 .
2022-10-31	Updated Basic System Settings on page 113

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, SCADA OS, IoT OS, ERP OS, Medical OS, SSL-VPN OS, or POS OS images are available to create Decoy VMs.
- **Decoy VMs:** Decoy VMs that behave like real network assets can be deployed via FortiDeceptor.
- **Deception Lures:** Deception 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 all actions taken by a hacker on a single decoy/victim host. Examples include, 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 hacker logs on to a system using the credentials found on another system.
- **Log Events:** Log all FortiDeceptor system events.

Set up FortiDeceptor

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

Task	Description
<input type="checkbox"/> Connect to the GUI	Connect the administration interface to a management computer with an Ethernet cable, then configure the management computer to be on the same subnet as the internal interface of the FortiDeceptor unit.
<input type="checkbox"/> Connect to the CLI	If necessary, connect to the CLI console.
<input type="checkbox"/> Change the system hostname	Change the full host name in the <i>System Information</i> widget.
<input type="checkbox"/> Change the administrator password	For security purposes, it is highly recommended you add a password to the admin account.
<input type="checkbox"/> Configure the system time	Configure the FortiDeceptor system time manually or synchronize with an NTP server from the <i>System Information</i> widget.
<input type="checkbox"/> Upload the license file to FortiDeceptor	Go to <i>Dashboard > System Information</i> widget, click <i>Upload License</i> beside <i>Firmware License</i> .
<input type="checkbox"/> Review the default port information	FortiDeceptor reserves Port1 for device management. The other ports are used to deploy deception decoys.
<input type="checkbox"/> Configure Central Management on the manager	Configure the Central Management console to manage remote FortiDeceptor appliances including Decoy VMs deployment, system configuration, and incident alert monitoring.

Connect to the GUI

Use the GUI to configure and manage FortiDeceptor.

To connect to the FortiDeceptor GUI:

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



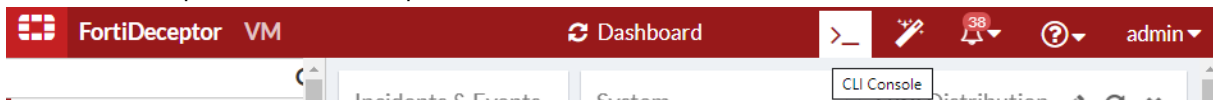
If the network interfaces have been configured differently during installation, the URL and administrative access protocols might not be in their default state.

Connect to the CLI

You can use CLI commands to configure and manage FortiDeceptor.

To connect to the FortiDeceptor CLI:

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



The *CLI Console* pane opens.

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

Change the system hostname

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

To change the host name:

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

Change the administrator password

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 better 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 an administrator and click *Edit*.
3. 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* widget and click *Change* beside *System Time*.
2. Select the *Time Zone* and wait for the widget to refresh.
3. Check that the *System Time* is correct. If necessary, click *Set Time* and manually set the time and date.
4. Click *Apply*.

You might need to log in again.

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

Upload license file to FortiDeceptor

To upload the license to FortiDeceptor:

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

Default port information

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

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

FortiDeceptor default ports:

Configure the FortiDeceptor management IP address on port1.

Configure the FortiDeceptor management IP address on port1.

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



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

Central Management

Central Management allows you to manage remote FortiDeceptor appliances including Decoy VM deployments, system configuration, and incident alert monitoring.

You can configure a FortiDeceptor hardware or VM appliance to be a Management Device or Remote Client. The Management Device has deception capabilities. You can use the Management Device to deploy decoys and lures to the Remote Clients on the network.



Network communication requirements:

Communication between:	From:
Management device and	Client to manager port1 IP and 8443 port

Communication between: **From:**

regular client appliance

Management device and cloud client appliance Management device to cloud client port1 public IP and 8443 port

FortiDeceptor VM Appliances										
Central Management Appliances										
Add Cloud Appliance + Approve Hold Delete Refresh ▶ Restart										
<input type="checkbox"/>	Action	SN ↑	IP ↑	Name ↑	Approval St...	Live Status	Version ↑	Enroll Time ↑	Last Activity ↑	
<input type="checkbox"/>	 	FDC-VM000...		C239	Approved	Online	v4.1.0.build02...	2022-06-16 15:18:05 PDT	2022-06-20 15:31:47 PDT	

Use the buttons in the *Central Management Appliances* pane to manage Remote Clients.

Button	Description
Approve	Allow the selected clients to participate in Central Management.
Hold	Pause the selected clients' participation in Central Management.
Delete	Pause the selected clients and then permanently delete related data in the Manage Device's local database, including OS, network settings, decoys, and lures. This action does not: <ul style="list-style-type: none"> • Delete or change any data in the Remote Client. • Change incident and campaign data generated in the past.
Refresh	Force re-sync all data between manager and selected clients.
Restart	Send signal to selected clients to reboot.

Remote Client

When a FortiDeceptor is managed as a Remote Client the navigation pane will only displays the *Network*, *System* and *Log* modules.

FortiDeceptor VM Interfaces						
Edit						
Interface	IPv4	IPv6	Interface Status	Link Status	Access Rights	
port1 (administration port)	/255.255.255.0		Online	Online	HTTPS,SSH	
port2	/255.255.255.0		Online	Online		
port3	/255.255.255.0		Online	Online		
port4	/255.255.255.0		Online	Online		
port5	/255.255.255.0		Online	Online		
port6	/255.255.255.0		Online	Online		

To prevent access to a Remote Client outside the Central Management or other trusted IP addresses, go to System > Administrators. See [Administrators on page 88](#).

When the Remote Client is a cloud device, configure the trusted host with the Management Device's IP to ensure only the Management Device can access itself.

On the Management Device, configure the trusted host with regular client IPs to ensure regular clients can access Management Device.

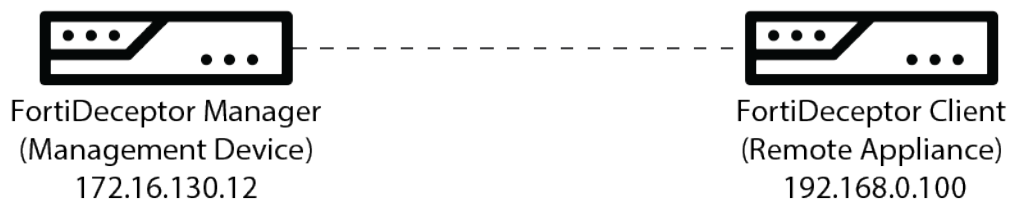
When you deploy a decoy or network, select the local or Remote Client name. Use the local configuration to deploy decoys and lures from the Management Device.

Configuring Central Management

To configure Central Management :

1. [Enable Central Management on the Management Device.](#)
2. [Enable Central Management the Remote Clientt.](#)
3. [Approve the Remote Client on the Management Device.](#)
4. [Configure the Remote Client with the Management Device.](#)

The tasks below are based on the following topology:



To enable Central Management on the Management Device:

```
cm -sc -mM -nManager -a<password>
```

Example:

```
cm -sc -mM -nManager -a1234567890
```

To enable Central Management on the Remote Client:



Before configuring FortiDeceptor as a Remote Client, perform a `factory reset` and basic network configuration to avoid data incompatibility between the Management Device and Remote Client. For more information on manager and client configuration, see the [CLI Reference](#).

```
cm -sc -mC -nAppliance1 -a<password> -i<manager_ip_address>
```

Example:

```
cm -sc -mC -nAppliance1 -a1234567890 -i172.16.130.12
```

To approve a Remote Client with the Management Device:

1. On the Management Device, go to *Central Management > Appliances*. The *Approval Status* for the Remote Client will display *On-Hold*.

Appliances									
Central Management Appliances									
Add Cloud Appliance + Approve Hold Delete Refresh Restart									
<input type="checkbox"/>	Action	SN ↑	IP ↑	Name ↑	Approval St...	Live Status	Version ↑	Enroll Time ↑	Last Activity ↑
<input type="checkbox"/>		FDC-VM000...	172.16.69...	C239	On-Hold	Online	v4.1.0,build02...	2022-06-16 15:18:05 PDT	2022-06-20 15:35:11 PDT

2. Select the appliance and click *Approve*. The *Approval Status* changes to *Approved*.

Request sent successfully.									
Central Management Appliances									
Add Cloud Appliance + Approve Hold Delete Refresh Restart									
<input type="checkbox"/>	Action	SN ↑	IP ↑	Name ↑	Approval St...	Live Status	Version ↑	Enroll Time ↑	Last Activity ↑
<input type="checkbox"/>		FDC-VM000...	172.16.69...	C239	Approved	Online		2022-06-16 15:17:53 PDT	2022-06-16 15:17:53 PDT

To configure the Remote Client with the Management Device:

1. On the Management Device, go to *Central Management > Appliances*.
2. In the *Action* column, click the *Config* icon . The Appliance - <name> page displays the following tabs.

Firmware	Push FortiDeceptor firmware updates and upgrades to the Remote Client. Synchronization can be immediate or scheduled.										
Deception OS	Push deception VM images from the Management Device to the Remote Client. Synchronization can be immediate or scheduled.										
	<table> <tr> <td>Status</td><td>Current status of deception OS image.</td></tr> <tr> <td>Name</td><td>Name of deception OS.</td></tr> <tr> <td>OS Type</td><td>Type of this deception OS.</td></tr> <tr> <td>VM Type</td><td>Category of this deception OS.</td></tr> <tr> <td>Lures</td><td>Lure services can be provided by this deception OS.</td></tr> </table>	Status	Current status of deception OS image.	Name	Name of deception OS.	OS Type	Type of this deception OS.	VM Type	Category of this deception OS.	Lures	Lure services can be provided by this deception OS.
Status	Current status of deception OS image.										
Name	Name of deception OS.										
OS Type	Type of this deception OS.										
VM Type	Category of this deception OS.										
Lures	Lure services can be provided by this deception OS.										
Interfaces	Configure the Remote Client network interfaces.										
Routing	Configure the Remote Client network routing table.										
DNS	Configure the Remote Client DNS configuration.										
FortiGuard	Configure the Remote Client FortiGuard configuration.										

- To synchronize the firmware, click the *Firmware* tab and select one of the following options and then click *Apply*:

Synchronize firmware image from manager now Click to synchronize the firmware immediately.

Synchronize firmware image from manager at Click to schedule the synchronization.

The screenshot shows the FortiDeceptor web interface for an appliance named 'Appliance - C239'. The 'Firmware' tab is selected. The interface displays the following information:

- SERIAL NUMBER:** FDC-VM00000
- FIRMWARE VERSION:** v4.1.0.build0225 (Interim) *The appliance firmware need to be synchronized.*
- AVAILABLE VERSION:** v4.2.0.build226 (GA)

There are two radio button options for synchronization:

- ☐ Synchronize firmware image from manager now
- ☒ Synchronize firmware image from manager at

Below the radio buttons, there are input fields for scheduling:

- Date:** 2022/06/20 (with a calendar icon)
- Time:** 10:00:00 (with a clock icon)

At the bottom, there are two buttons: **Apply** (with a checkmark icon) and **Cancel** (with an 'X' icon).

To remove a client from Central Management:

- On the Remote Client, run the following CLI command:

```
cm -sc -mN
```

After a client leaves Central Management, its status on the manager changes to *Wait*.
- On the Management Device, select that client and click *Delete*.

To remove the Management Device from Central Management:

- On the Management Device, run the following CLI command:

```
cm -sc -mN
```

Deploy Decoy VM

Use the *Deception* pages 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.

To use FortiDeceptor to monitor the network:

Task	Location in GUI	More information
Check the Deception OS is available	Go to Deception > Deception OS	See Deception OS on page 39 .
Auto-detect or specify the network where the Decoy VMs are deployed	Go to <i>Deception > Deployment Network</i>	See Deployment Network on page 40 .
Deploy the Decoy VM on the network	Go to <i>Deception > Deployment Wizard</i>	See Deploy Decoy VMs with the Deployment Wizard on page 42 .
Start or stop the deployed Decoy VMs, or download the FortiDeceptor token package to manually install it on computers	Go to <i>Deception > Decoy Status</i>	See Decoy Status on page 51 .
Specify the IP address that is to be considered safe	Go to <i>Deception > Safe List</i>	See Configure a Safe List on page 57 . This is useful when you want to log in to the deployment network without being flagged as an attacker.
View and work with lure resources	Go to <i>Deception > Lure Resources</i>	See Lure Resources on page 57 .

For more information, see [Deception deployment best practices on page 130](#).

Custom Decoy Image

For most deployments, the decoys included with FortiDeceptor are enough and are easier to deploy. However, you have the option to build a decoy from your gold image using the custom decoy feature that is included under the subscription license.

Some examples of using Decoy Customization include:

- Windows 10/2016/2019 decoy joining AD.
- Windows Server 2016/2019 Enterprises users with SQL Server, web applications using an IIS server, and more.



This version only supports Decoy Customization for Windows 10 and Windows Server 2016/2019. Windows Server 2016/2019 supports customized MSSQL and IIS services.

Overview of implementing Decoy Customization:

1. Order the FDC Custom Decoy Subscription for FDC HW appliance only.
The Decoy Customization subscription is for FortiDeceptor hardware appliances only. This subscription license is already included in the FortiDeceptor VM bundle.
2. Install FortiDeceptor.
After installing FortiDeceptor with the Decoy Customization subscription, the *Help* menu in the toolbar will display an option for the *Custom Decoy Image Cookbook*.
3. Follow the instructions in the *Customization Cookbook*. The high-level instructions are:
 - a. Upload an ISO image.
 - b. Install ARAE engine on image.
 - c. Use the Deployment Wizard to install the customized decoy.

Customize the deception base OS image

Overview of customizing the deception base OS image:

1. [Import Windows ISO image.](#)
2. [Customize VM image.](#)
3. [Deploy custom image.](#)

Import Windows ISO image

Before importing an ISO image into FortiDeceptor, ensure you have completed the following:

- Purchased a FDC Custom Decoy Subscription
The FDC Custom Decoy Subscription is for FortiDeceptor hardware appliances only. This subscription license is already included in the FortiDeceptor VM bundle.
- Set up an ISO image with the licenses for your environment. For example, if you want to allow Active Domain (AD) accounts to access decoys, configure the settings on the AD servers, such as create dummy accounts, and so on.

To import an ISO image using the Imported Images page:

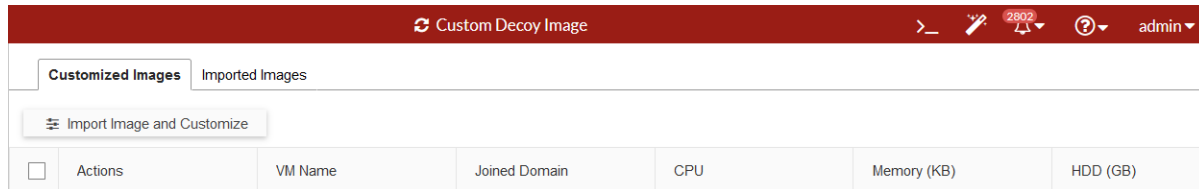
1. Go to *Deception > Custom Decoy Image* and click the *Imported Images* tab.



2. Click *Import New ISO Image*.
3. Click *Choose a file* or drag and drop an image file into that pane.

To import an ISO image using the Customized Images page:

1. Go to *Deception > Custom Decoy Image* and click the *Customized Images* tab.



2. Click *Import Image and Customize*.
3. Click *Choose a file* or drag and drop an image file into that pane.

To delete an ISO image:

1. Go to *Deception > Custom Decoy Image* and click the *Imported Images* tab.
2. Select one or more images and then click *Delete*.

Customize VM image

To initialize the VM instance:

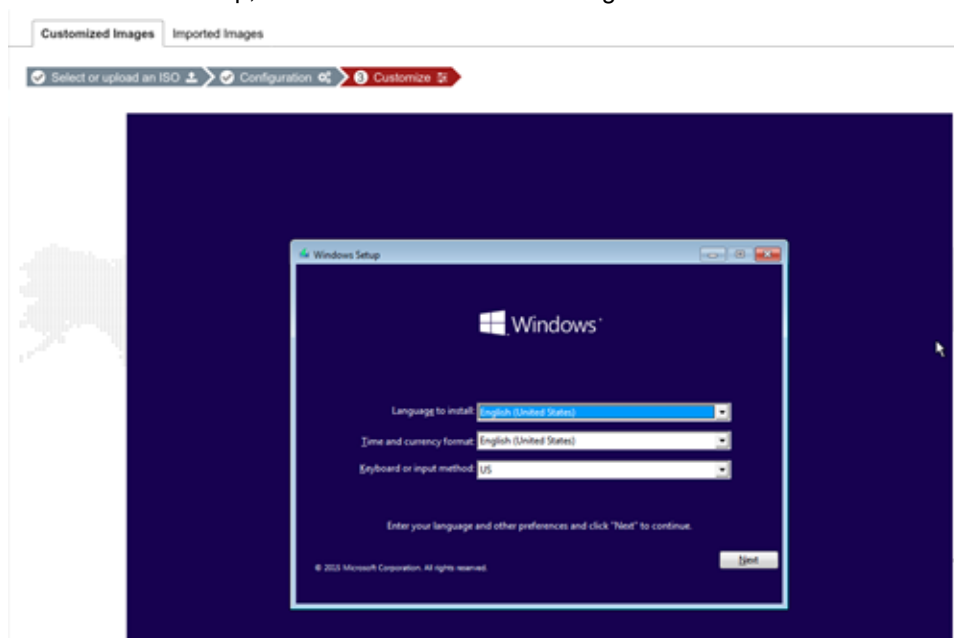
1. Go to *Deception > Custom Decoy Image* and click the *Customized Images* tab.
2. Click *Import Image and Customize*. The custom image wizard opens.
3. In the *Select an imported ISO image* dropdown list, select an ISO image. Then click *Next*.
4. In the *Configuration* step, specify the following and then click *Next*.

Name	Upper and lowercase letters and numbers totaling under 48 characters.
CPU Cores	1–4 cores.
Memory	1024–8192 MB.
Storage	20–50 GB.

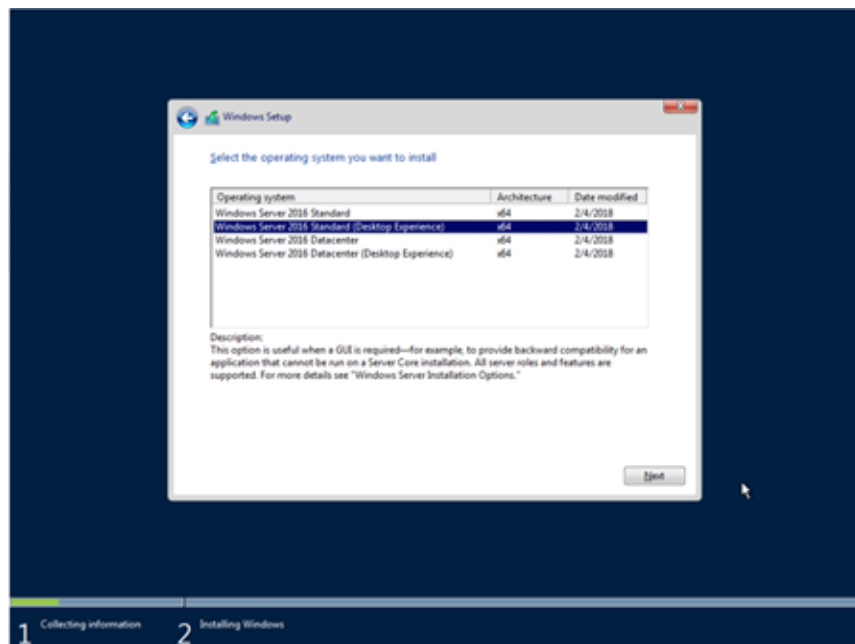
 A screenshot of the 'Configuration' step in the custom image wizard. It shows a progress bar with three steps: 'Select or upload an ISO' (completed), 'Configuration' (current), and 'Customize' (disabled). Below the progress bar, there are four configuration fields: 'Name' (text input), 'CPU Cores' (dropdown menu set to 1), 'Memory' (dropdown menu set to 1024 MB), and 'HDD' (dropdown menu set to 20 GB).


This configuration is applied to the VM instance for customizing the image, This configuration is **not** applied to decoys.

5. In the *Customize* step, install the OS from the ISO image.

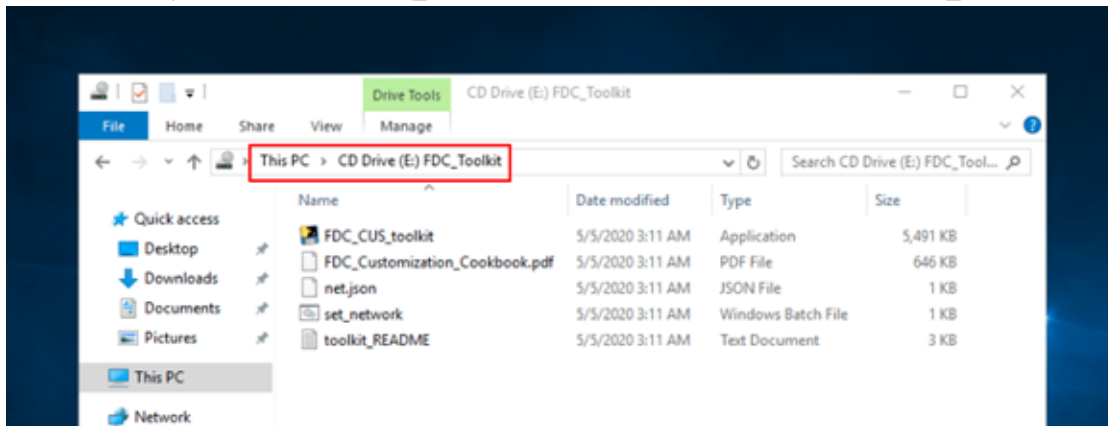


Follow the prompts until the installation is complete.



To customize the VM:

1. Ensure the OS is installed and then log in with an admin account.
2. In Windows Explorer, locate the *FDC_Toolkit* folder and read the instructions in *toolkit_README.txt*.



3. Configure the network using one of the following options.
 - Right-click *set_network.bat* and then click *Run as Administrator*.
 - Follow the instructions in *net.json* to configure the IP address, gateway, and DNS in Windows *Control Panel > Network and Internet > Network Connections*.

```
C:\Windows\System32\cmd.exe
Find proper interface: "Ethernet"
Enable interface: "Ethernet"

Set interface: "Ethernet" IP:10.254.253.83 gateway:10.254.253.1

Test network ...

Pinging 10.254.253.1 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
Reply from 10.254.253.1: bytes=32 time<1ms TTL=64
```



10.254.253.0/24 set by the script is the internal NAT IP address that is temporarily used by the customization VM to allow downloading files and accessing other network resources via the FortiDeceptor default route.

To customize the system for Windows 2016:

1. Ensure your license is activated.
2. If you are using Windows 2016, enter the following commands in the PowerShell window to prevent lure configuration failures in the Decoy Deployment wizard.


```
secedit /export /cfg c:\secpol.cfg
(gc C:\secpol.cfg).replace("PasswordComplexity = 1", "PasswordComplexity = 0") | Out-File C:\secpol.cfg
secedit /configure /db c:\windows\security\local.sdb /cfg c:\secpol.cfg /areas SECURITYPOLICY
rm -force c:\secpol.cfg -confirm:$false
```

To customize the system for standalone Windows Server 2016:

1. Go to *Server Manager > Tools > Local Security Policy*. The *Local Security Policy* directory opens.
2. In the Security Settings folder, open the *Password Policy* folder, and double-click *Password must meet complexity requirements*.
3. Select *Disabled* and then click *OK*.
4. Open a Command Prompt as an Administrator and type the following command to update the group policy:

```
gpupdate /force
```

You should get the following response:

```
C:\Users\Administrator>gpupdate /force
Updating policy...
Computer policy update has completed successfully.
```

To customize the system for Server 2016 Domain Controller :

1. In the *Domain Controller*, go to *Server Manager > Tools > Group Policy Management*.
2. Right-click *Default Domain Policy* and click *Edit*. The *Group Policy Management Editor* opens.
3. In the *Computer Configuration* folder, go to *Policies > Windows Settings > Security Settings\Account Policies > Password Policy > Password must meet complexity requirements*.
4. Select *Disabled* and click *OK*.
5. Open a Command Prompt as Administrator and type the following command to update the group policy:

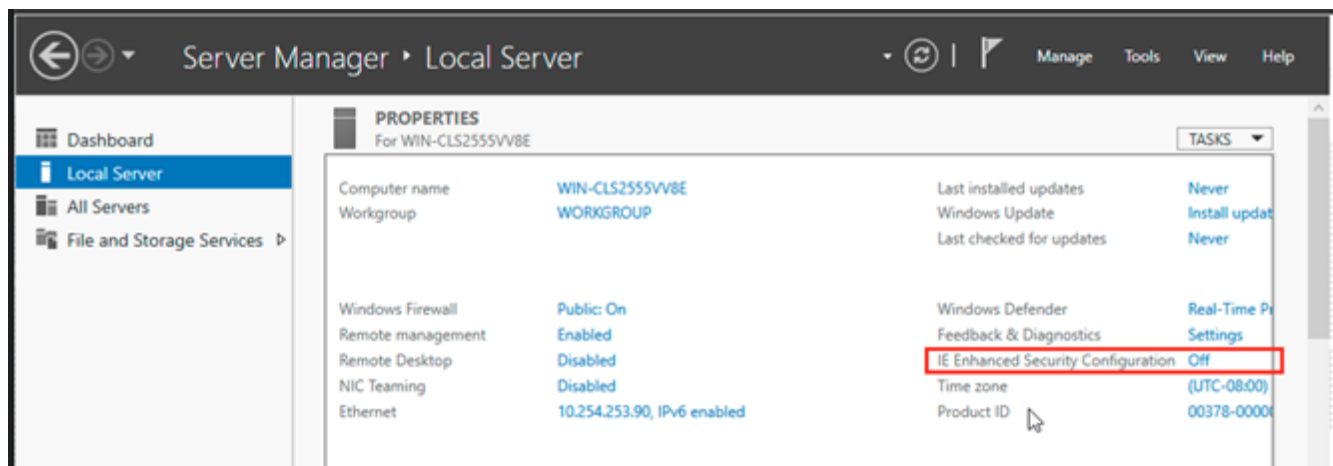
```
gpupdate /force
```

Optional: install the Microsoft SQL Server

The following SQL Server versions are supported.

- SQL Server 2016. <https://www.microsoft.com/en-us/download/details.aspx?id=56840>
- SQL Server 2017. <https://www.microsoft.com/en-us/download/details.aspx?id=55994>
- SQL Server 2019. <https://www.microsoft.com/en-us/sql-server/sql-server-downloads>
- SQL Server Management Studio for SQL server management and customization. <https://aka.ms/ssmsfullsetup>

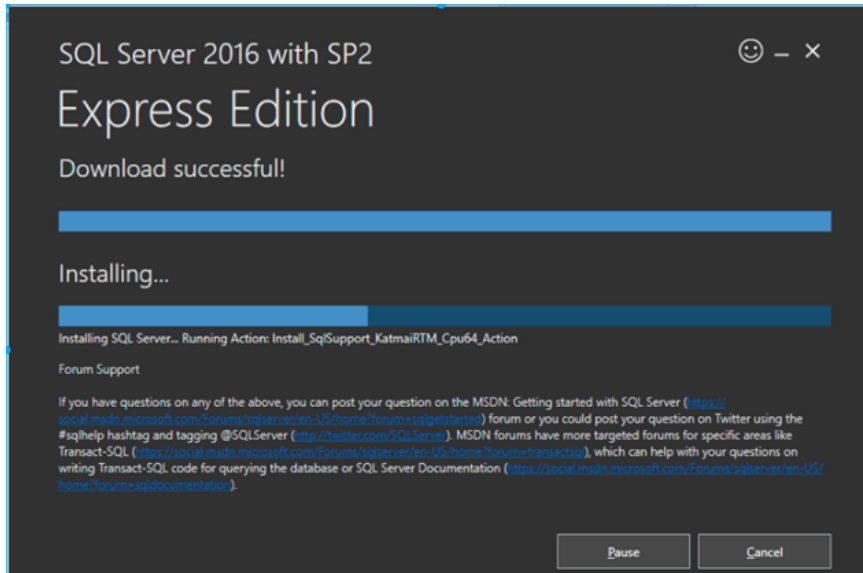
If you are downloading with Internet Explorer, it is recommended you disable *IE Enhanced Security Configuration*.



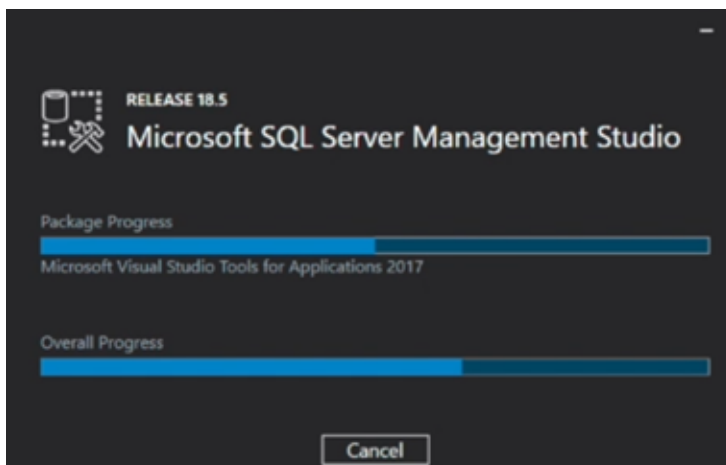
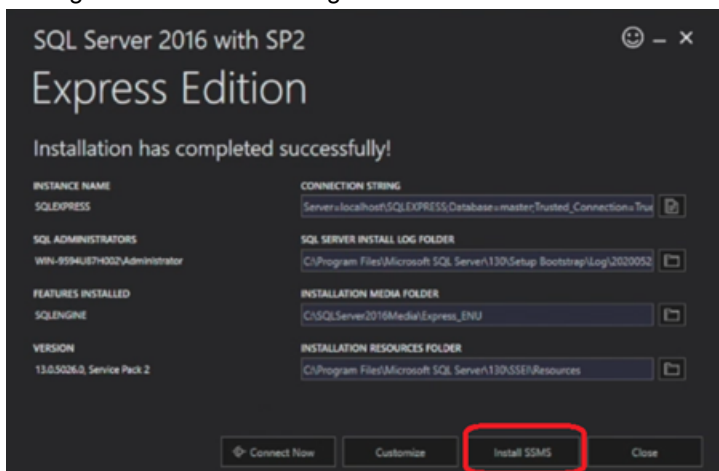
Since there is no desktop for Windows Server core OS, you must download the installation file on another computer and then use SMB to install the SQL Server.

To install SQL server:

1. Download and install the SQL server on another computer.

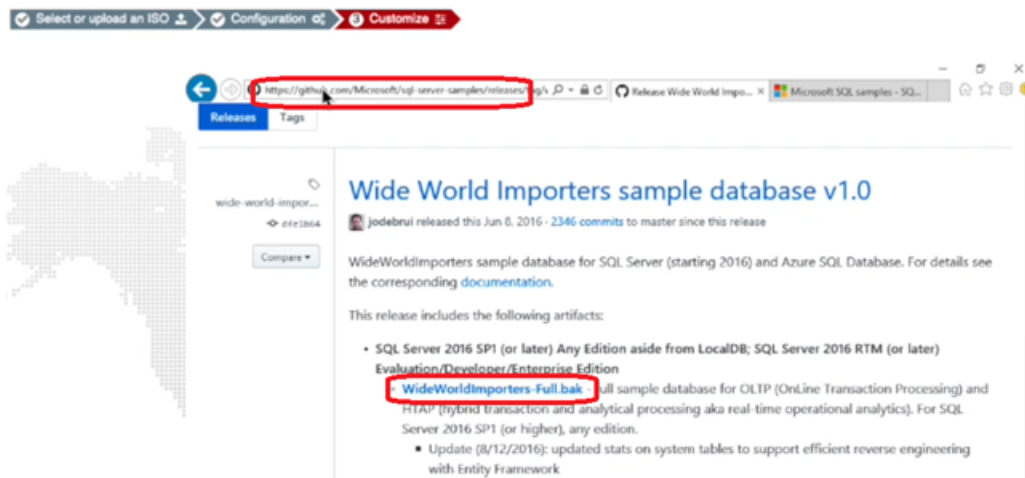


2. When the SQL Server installation is complete, click *Install SSMS* to download and install the SQL Server Management Studio to manage and customize the SQL Server.

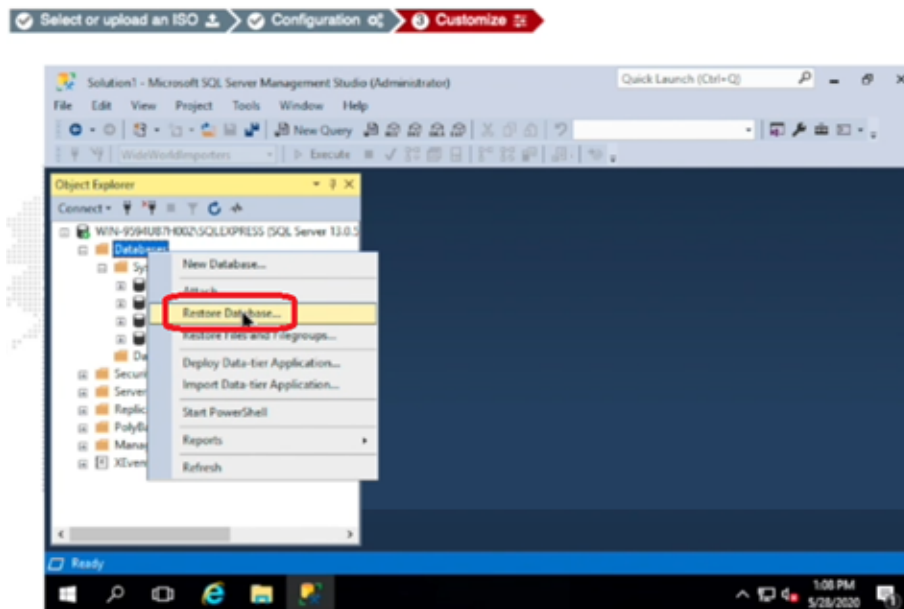


To further customize the SQL database:

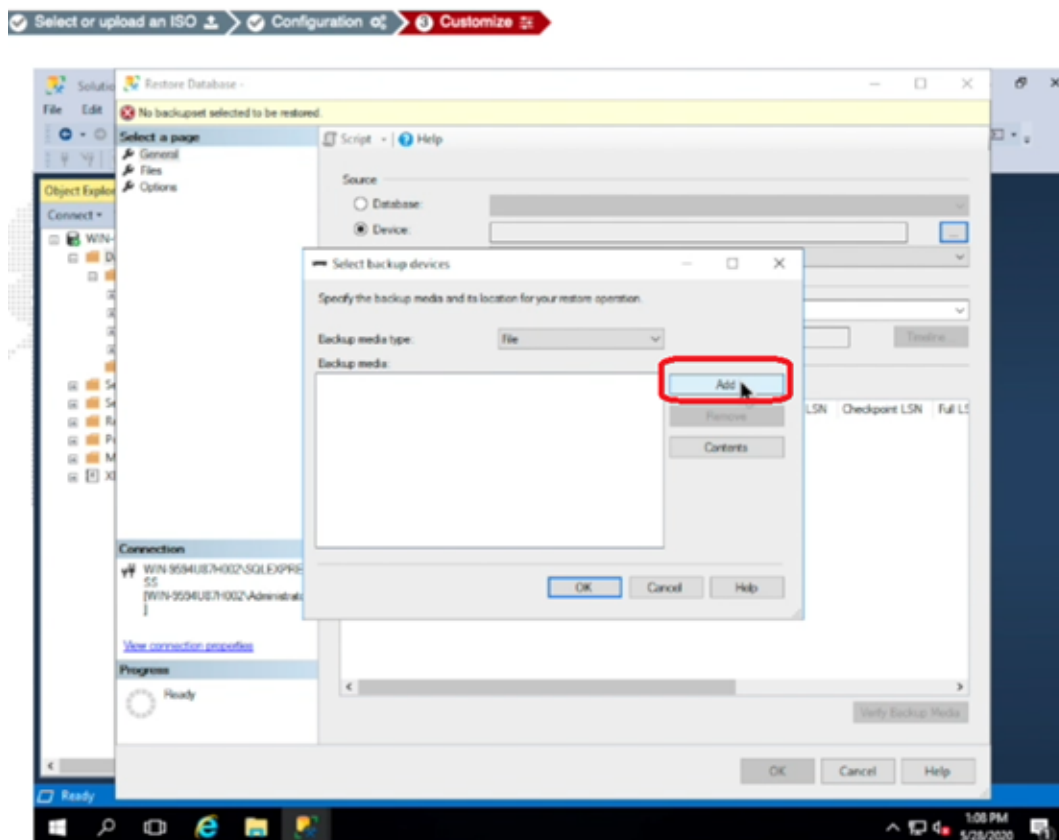
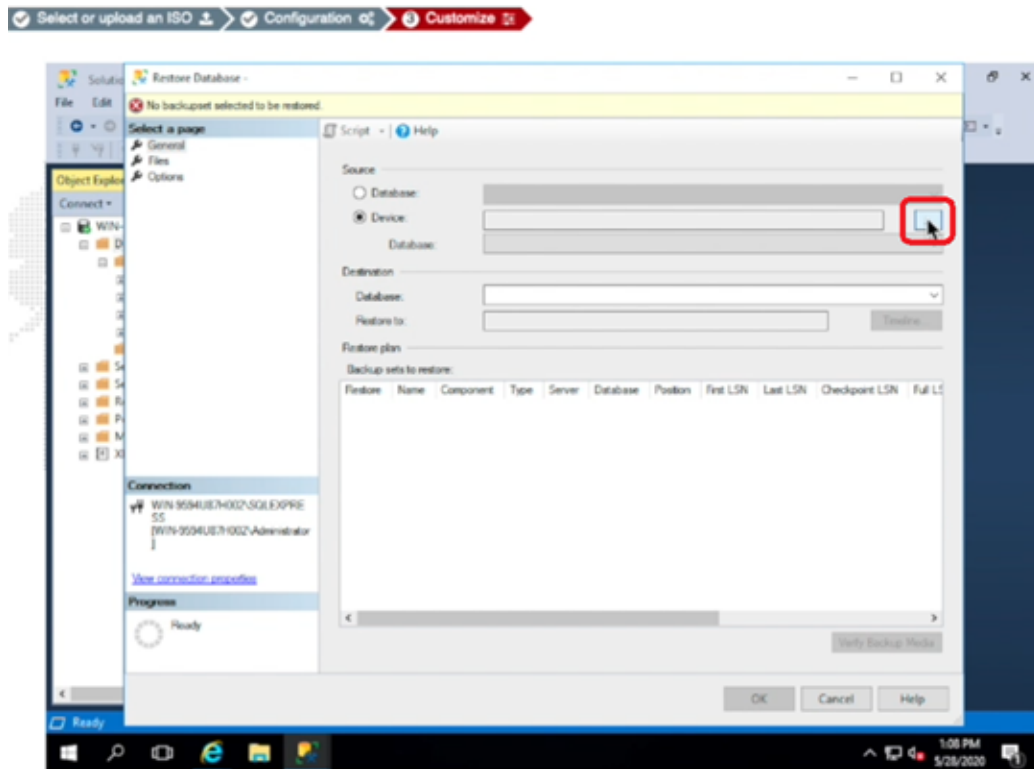
1. Download a sample database from <https://github.com/Microsoft/sql-server-samples/releases/download/wide-world-importers-v1.0/WideWorldImporters-Full.bak>.



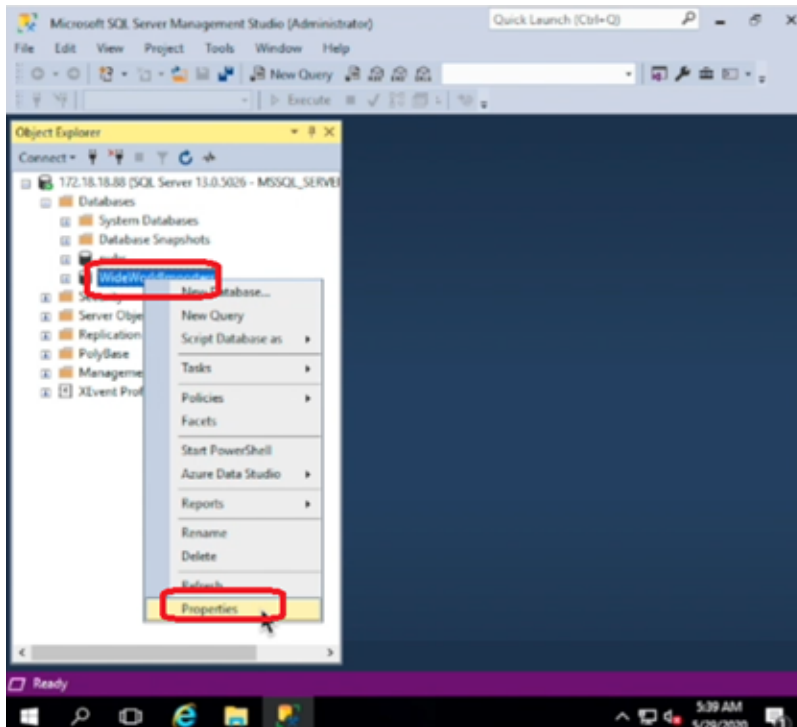
2. In the FortiDeceptor Customize Decoy console, open SQL Server Management Studio.
3. Right-click the database object and select *Restore Database*.



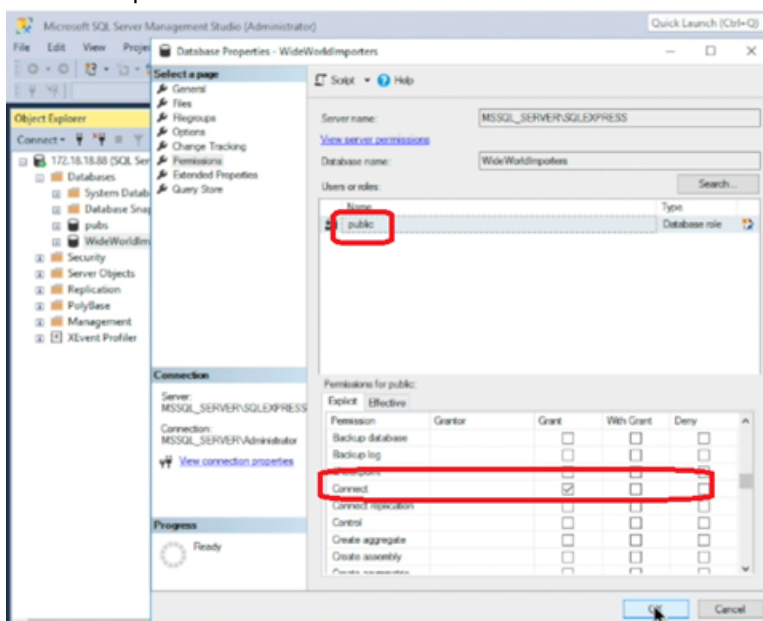
4. Locate and add the sample DB you downloaded.



5. When the sample DB is restored, right-click that DB and select *Properties* to change access permission to make the decoy DB more attractive to attackers.



6. Give *Grant* permission to *Select* and *Connect*.



7. Close SQL Server Management Studio.
8. Verify that your DB is up using the command `netstat -an | findstr 1433`.
9. The listening port on the SQL Express Database is disabled by default. To enable the port:
 - a. Click *Start > Programs > Microsoft SQL Server 20XX* and select *SQL Server Configuration Manager*.
 - b. Select *SQL Server Network Configuration*.
 - c. Double-click *Protocols for SQLEXPRESS*

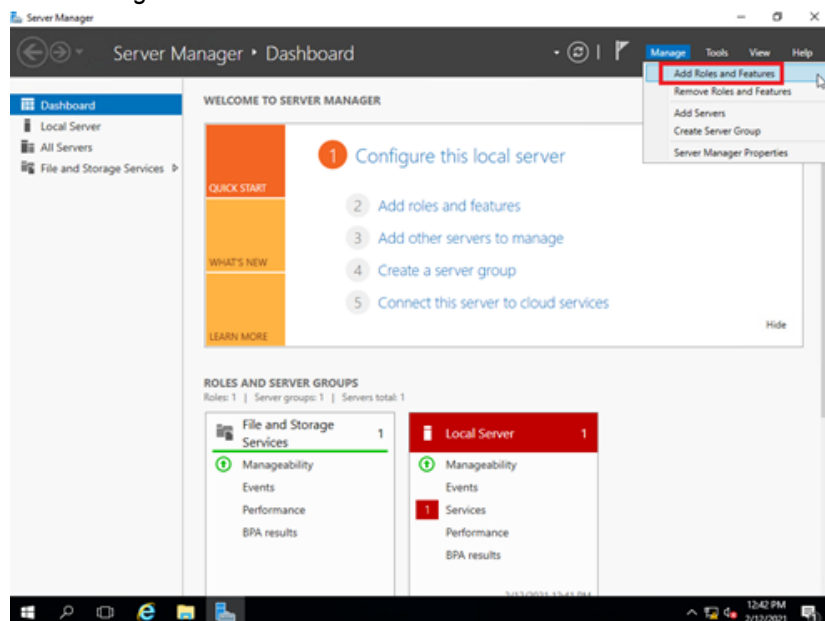
- d. Right-click *TCP/IP* and select *Properties*. If necessary, first enable *TCP/IP*.
- e. Scroll down to *IPAll* and verify *TCP Dynamic Ports* is blank and that *TCP Port* is set to *1433*.
- f. Click *OK*.

Optional: install Internet Information Service (IIS)

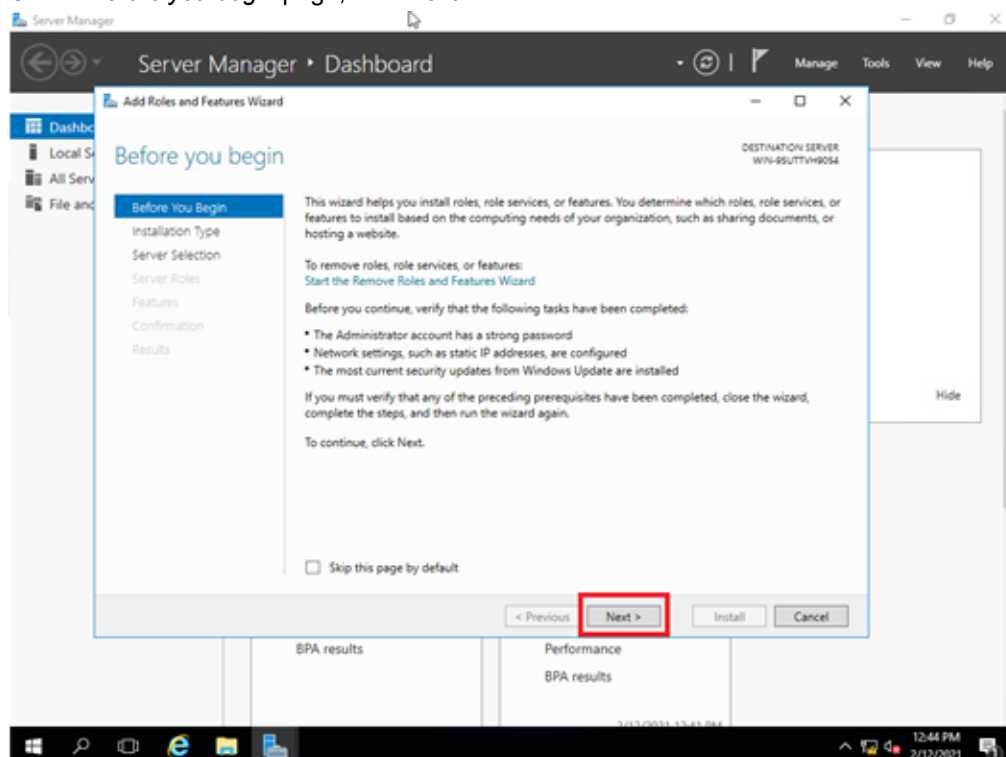
IIS 10 is supported on Windows Server 2016/2019.

To add the IIS role and service:

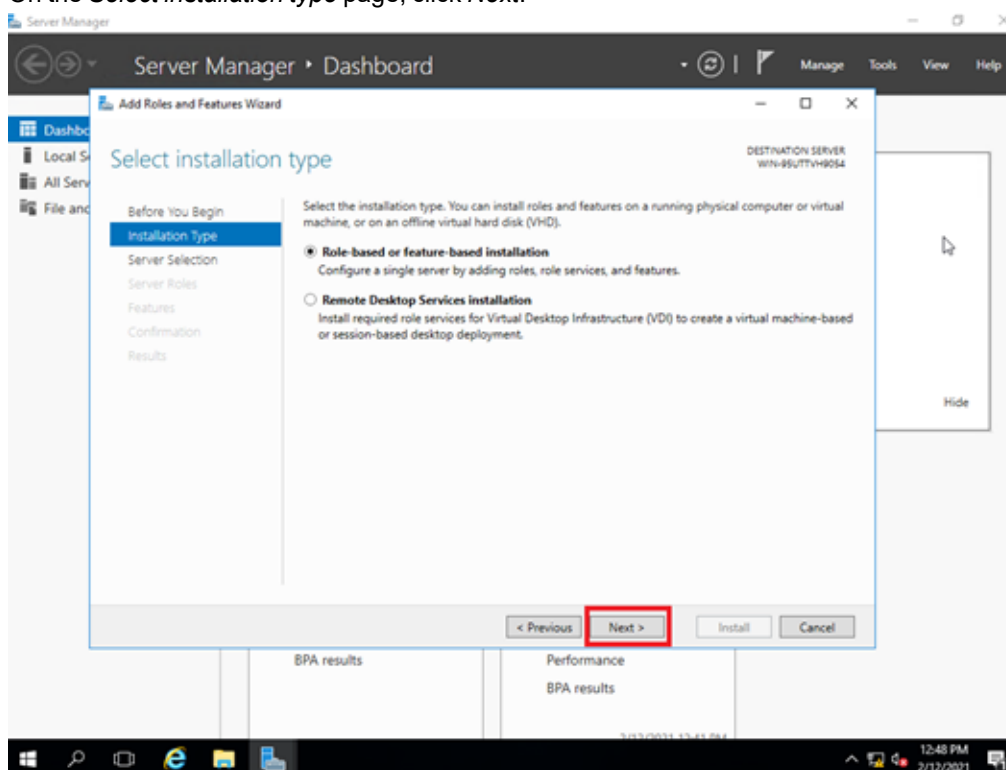
1. Go to *Server Manager > Dashboard*.
2. Click *Manage > Add Roles and Features*.



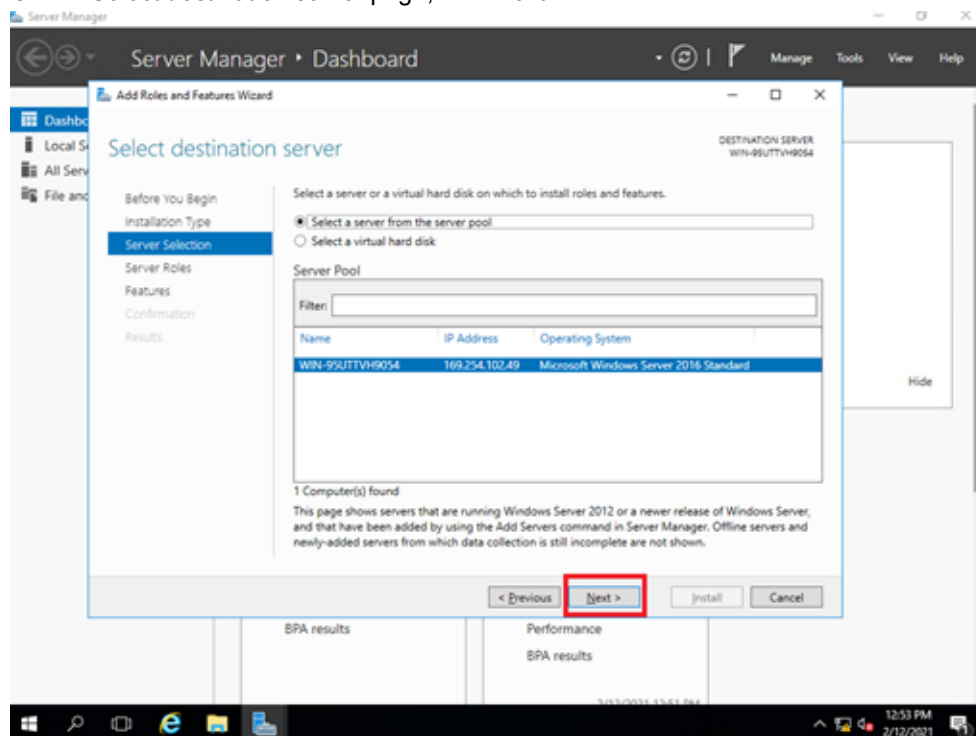
3. On the *Before you begin* page, click *Next*.



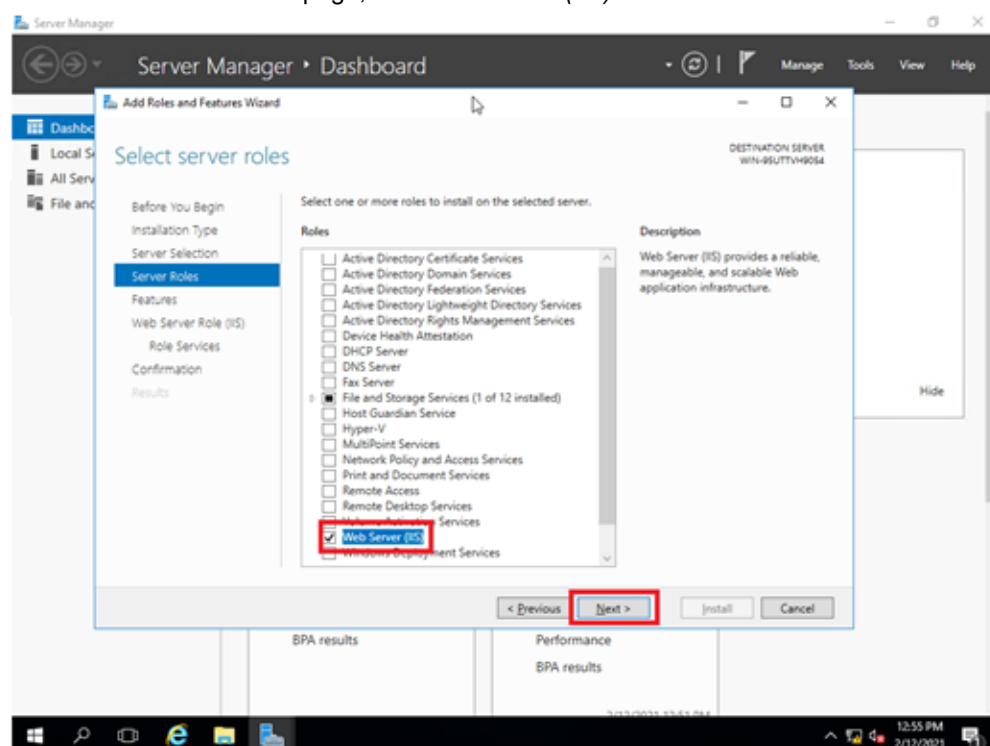
4. On the *Select installation type* page, click *Next*.



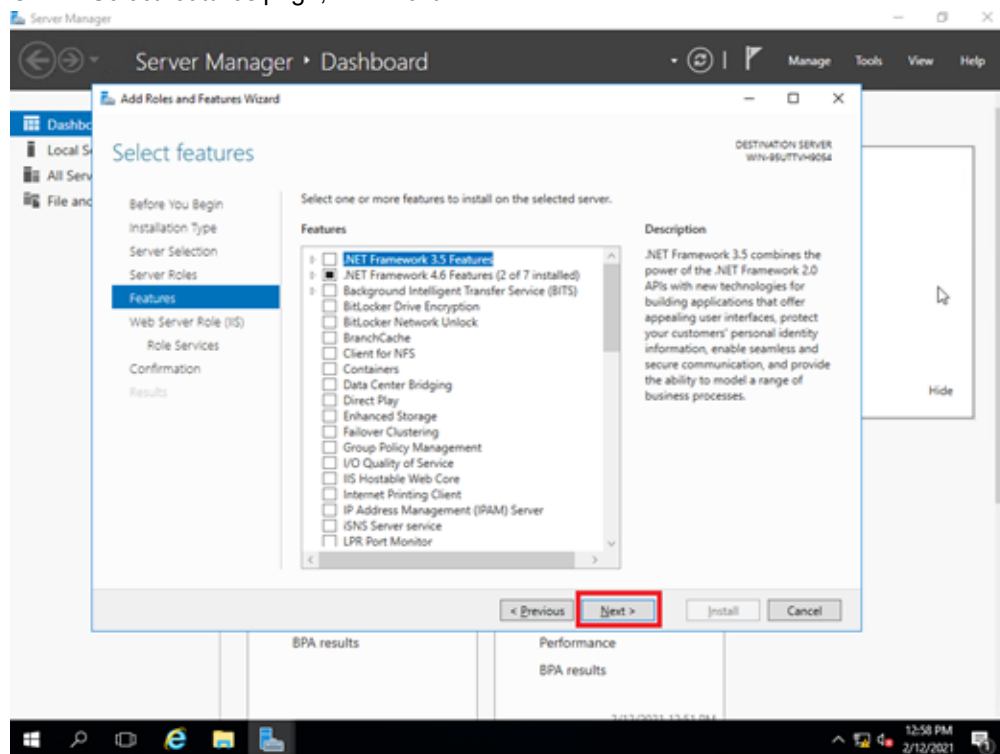
5. On the *Select destination server* page, click *Next*.



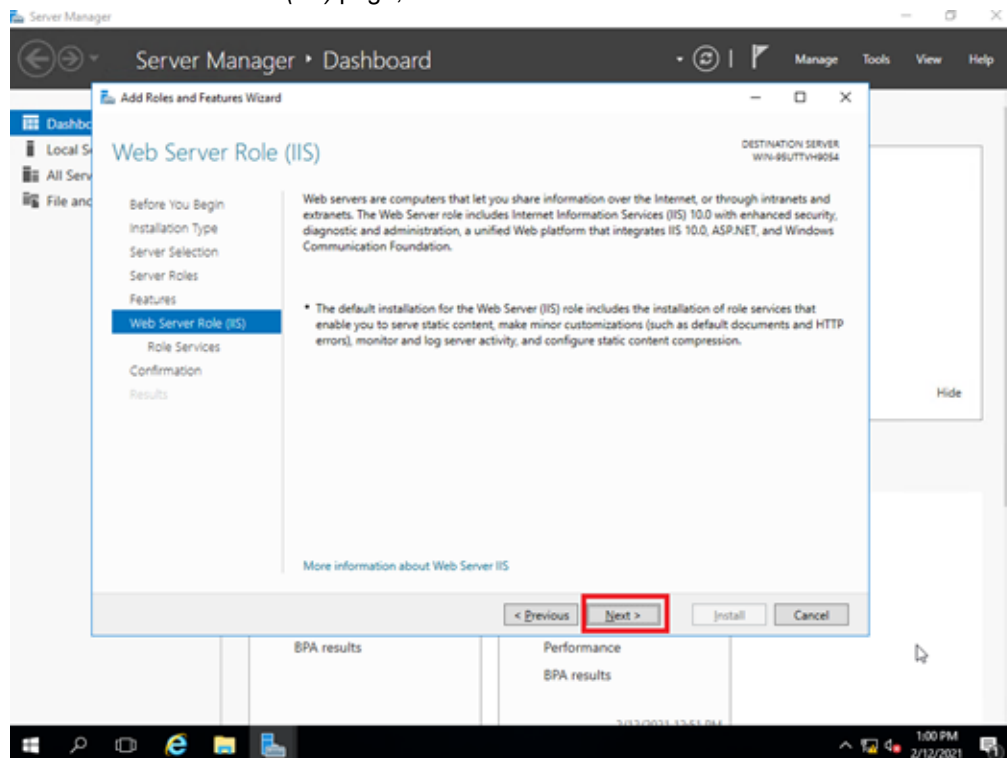
6. On the *Select server roles* page, click *Web Server (IIS)*.



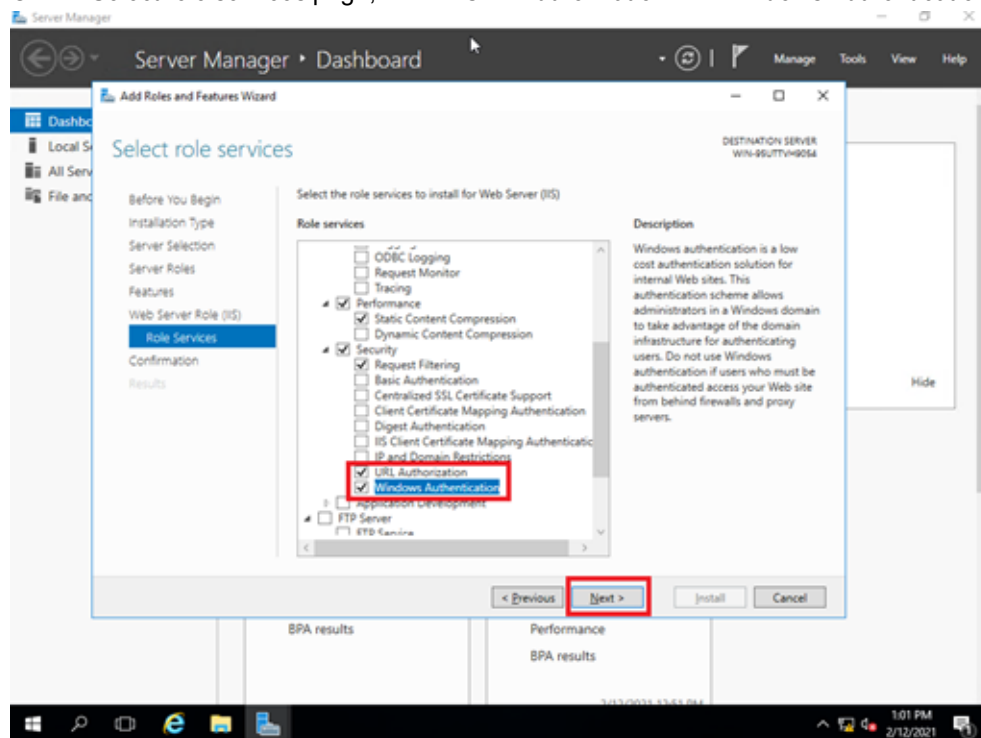
7. In the pop-up dialog box, click *Add Features*.
8. On the *Select features* page, click *Next*.



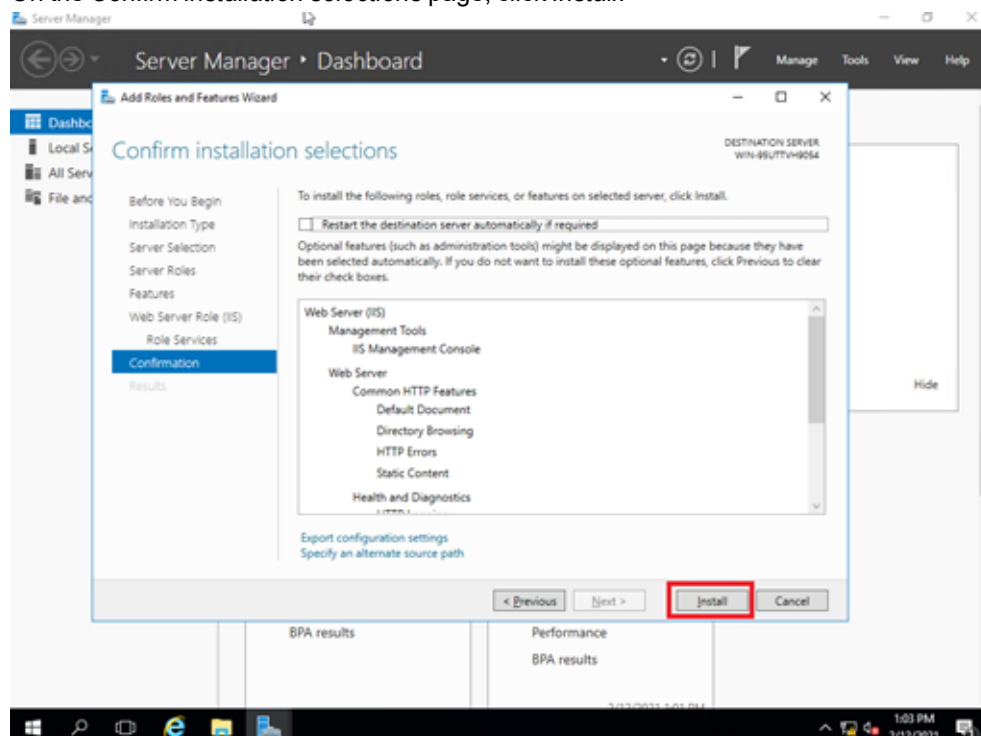
9. On the *Web Server Role (IIS)* page, click *Next*.



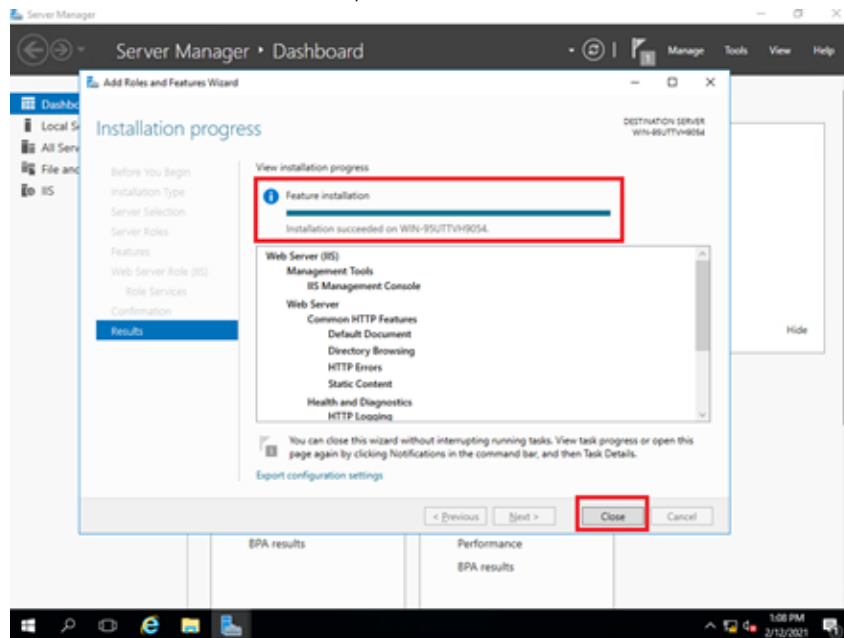
10. On the *Select role services* page, enable *URL Authorization* and *Windows Authentication*, then click *Next*.



11. On the *Confirm installation selections* page, click *Install*.



12. Wait for the installation to finish, then check the results and click *Close*.



Join a domain

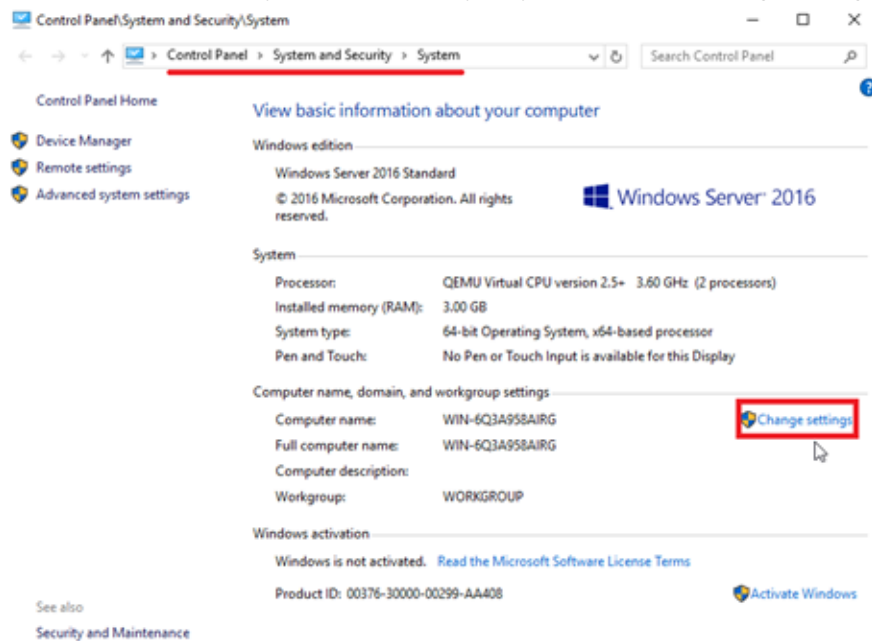
Before joining a custom Windows OS to a domain, change its DNS server to the DNS server of the domain.



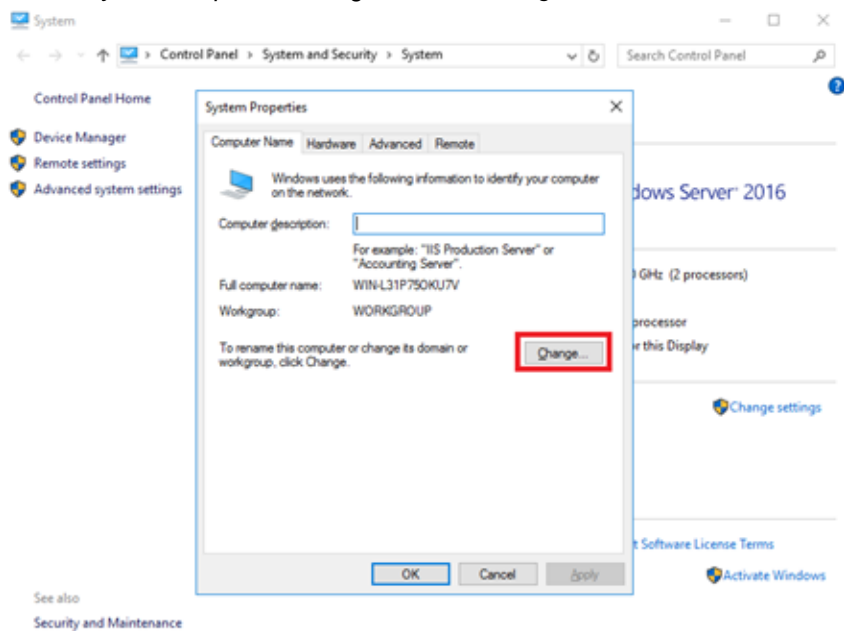
This task is optional.

To join a domain:

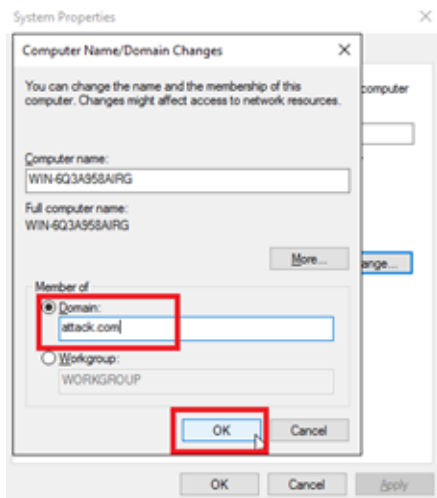
1. Go to *Control Panel > System and Security > System* and click *Change settings*.



2. On the *System Properties* dialog box, click *Change*.



3. Enter the *Domain* and click *OK*.



4. Click *Close* and restart the computer to join the domain.

Install the FortiDeceptor customization toolkit

When system customization is complete, right-click *FDC_CUS_toolkit.exe* and select *Run as Administrator* and wait for the installation to finish.

Another option is to run the CLI command `FDC_CUS_toolkit.exe` as an administrator.

Save the custom image

When the customization status in the GUI displays *Ready*, click *Start -> Power > Shut down* to shut down Windows and then click *Save* to save this image.

If the Windows Server is connected to a domain, there may not be a *Power* option in the GUI. In this case, run the command `shutdown /s /t 1 /f` as administrator.


It might take several minutes to save the entire image. When the image is saved, the page lists the image in *Customized Images*.

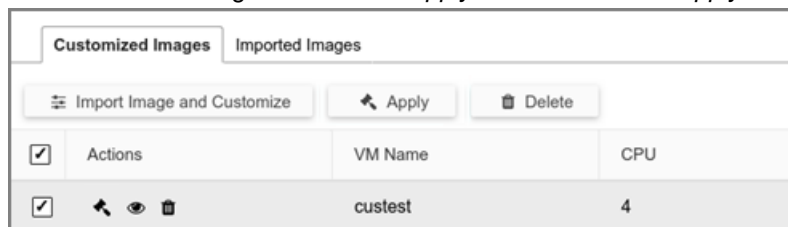
In *Deception > Customization*, the *Customized Images* tab lists the custom images.

The *Actions* column has icons for you to view logs, apply the image, or delete the image.




Deploy custom image

To apply a custom image:

1. Go to *Deception > Custom Decoy Image* and click the *Customized Images* tab.
2. Select a custom image and click the *Apply* button or click the *Apply* icon  beside a custom image.



It might take a few minutes to apply the custom image. When applied, the custom image is listed in *Deception > Deception OS*.

Status	Name	OS Type	VM Type	Lures
Initialized	custest	Customized Windows 10	Windows End Point	
Get	scadav1	Scada	SCADA/IOT device	
Initialized	ubuntu16v1	Ubuntu	Linux End Point	


To deploy decoys with custom images—generic image:

1. Go to *Deception > Deployment Wizard*.
2. Click a custom image and deploy it like a standard decoy.
3. Select whether to domain users to access RDP and SMB.

For normal users:

 RDP (2) ☒ + Add Lure

Username	Password
loretta	<input type="password"/>
lawrence	<input type="password"/>

 SMB (2) ☒ + Add Lure

Username	Password	Sharename
rhonda	<input type="password"/>	<input type="password"/>
maurice	<input type="password"/>	<input type="password"/>

For domain users:

 RDP (2) ☒ + Add Lure

Allow domain user to access RDP ☒

Username	Password
david@name.com	<input type="password"/>
ethan@name.com	<input type="password"/>

 SMB (1) ☒ + Add Lure

Allow domain user to access SMB ☒

Username	Password	Sharename
robert@name.com	<input type="password"/>	<input type="password"/>



We highly recommend enabling RDP and SMB services for decoys joined in the domain and not set in any local lure accounts. Many domains have different policies for account name and password which may cause the decoy to fail to initialize.

To deploy decoys with custom images–SQL Server:

1. Go to *Deception > Deployment Wizard*.
2. Click a custom SQL server image.

The screenshot shows the FortiDeceptor VM Deployment Wizard interface. The left sidebar contains navigation links: Dashboard, Deception (expanded), Customization, Deception OS, Deployment Network, Deployment Wizard (selected), Decoy & Lure Status, Decoy Map, Whitelist, Incident, Fabric, Network, System, and Log. The main panel displays the 'Configuration' step of the wizard. The 'Name' field is set to 'MSSQL_Server'. The 'Available Deception OSes' dropdown is set to 'cus_WinSrv16_MSSQL'. The 'Selected Services' dropdown is set to 'SQLSERVER, TCPLISTENER'. The 'SQLSERVER (0)' section is expanded, showing fields for 'Listening Port' (1433), 'Database Name' (pubs), and 'Database Content' (Upload SQL Schema). A red box highlights the 'Sample' button next to the 'Upload SQL Schema' field. The 'TCPLISTENER (0)' section is also visible with a 'Listening Ports' field. The 'Launch Immediately' and 'Reset Decoy' options are at the bottom.

3. (Optional) Click *Sample* to download a sample .sql file.

- Click *Upload SQL Schema* to upload your own custom .sql file .

Deployment Wizard

1 Template 2 Configuration 3 Set Network

Name: win2016svr-sql ✓

Available Deception OSes: cus_16ad ✕

Selected Services: MSSQL ✓

Automate Lures: any ✕ Generate Lures Clear

SMB (0) ☐

RDP (0) ☐

MSSQL (1) ☒

Listening Port: 1433 ✓

Database Name: pubs ✓

Database Content: Upload SQL Schema ✓ Sample

MSSQL Users: + Add User

Username	Password	
susan	ZsabcZo	✕ Delete

To generate SQL alerts:

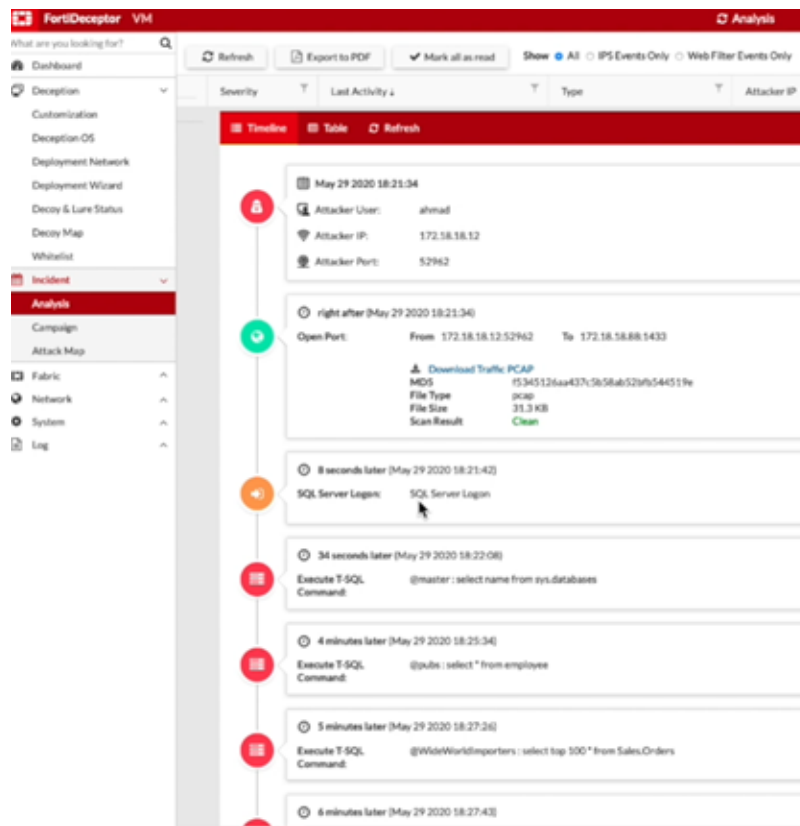
- You can generate SQL alerts using the SQLCMD tool or using WideWorldImporters.

- To use SQLCMD, run the following commands.

```
sqlcmd -S "IP Address" -U "username" -P "password"
use WideWorldImporters;
SELECT name
from SYSOBJECTS
WHERE
xtype = 'U'
go
```
- To use WideWorldImporters, run the following commands.

```
use WideWorldImporters;
select top 100 * from Sales.Orders;
go
```

The *Incident > Analysis* page displays the alerts for the SQL server attack.



To deploy decoys with custom images—IIS (HTTP/HTTPS):

1. Go to *Deception > Deployment Wizard*.
2. Click a custom IIS image.

IIS (HTTP) (1)

Listening Port: 80 ✓

IIS (HTTP) Users: + Add User

IIS (HTTPS) (1)



Listening Port: 443 ✓


SSL Certificate (optional): Upload certificate/key zip file ✓
The .zip file should contain both SSL certificate and key files.


IIS (HTTPS) Users: + Add User

To deploy decoys with custom images—NBNSpoofSpotter:


1. Go to *Deception > Deployment Wizard*.
2. Click a custom NBNSpoofSpotter image.


 NBNSpoofSpotter (0) 


Username 

Password 

Domain (optional)

Hostname 

 Please provide a fake hostname for NBNS request.


















Interval seconds 



NBNSpoofSpotter feature detects attacks using the *Responder* tool and includes a link to <https://github.com/SpiderLabs/Responder> with more information about the attack.

Deception OS

The *Deception OS* page displays the deception OSes available for creating Decoy VMs. Use this page to upload a deception OS package or to synchronize the deception OS list.

Deception OS admin					
 Upload Deception OS Package		 Synchronize Deception OS List			
Status	Name	OS Type	VM Type	Lures	
 Initialized	centosv1	 CentOS	Linux Server		
 Initialized	crmv1	 ERP OS	ERP system		
 Initialized	fgt601v1	 FortiGate	Fortinet device		
 Initialized	iotv1	 IoT OS	IoT system		
 Initialized	medicalv1	 Medical OS	Medical IoT system		

The *Deception OS* page displays the following information:

Column	Description
Status	Status of the Deception OS.
Name	Name of the Deception OS.
OS Type	Operating System type.
VM Type	VM type of the Deception OS endpoint.

Column	Description
Lures	Lures used by the Decoy VM such as SSH, SAMBA, SMB, RDP, TCPLISTENER, HTTP, NBNSSpoofSpotter, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, Guardian-AST, IEC104, DNP3, ENIP, KAMSTRUP, Infusion Pump (Telnet), Infusion Pump (FTP), PACS, PACS-WEB, DICOM server, POS-WEB, ERP-WEB, and SSLVPN

To upload a deception package:

1. Go to *Deception > Deception OS*.
2. Click *Upload Deception OS Package*.
3. Click *Choose a file* or drag and drop the file onto the field.

To synchronize the list:

Click *Synchronize Deception OS List*.

Deployment Network

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

Deployment Network										
Auto Vlan Detection <input type="text" value="port2"/>										
OK										
+ Add New Vlan / Subnet										
Action	Status	Name	Interface	VLAN ID	Deploy Monitor IP/Mask	Tag	Gateway	Ref.	Arp Protec...	
Edit Delete	Initialized	deploynet1	port2	0		any	10.10.2.1	9	No	
Edit Delete	Initialized	deploynet3	port3	0		any	0.0.0.1	2	No	
Edit Delete	Initialized	deploynet4	port4	0		any12	10.12.2.1	7	No	
Edit Delete	Initialized	deploynet5	port5	0		any	0.0.0.1	2	No	
Edit Delete	Initialized	deploynet6	port6	0		any	0.0.0.1	0	Yes	

The *Deployment Network* page displays the following information:


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. Click <i>Delete</i> to remove a VLAN or Subnet.
Status	Status of the IP address, such as if it is initialized.
Name	Name of the VLAN or subnet.

Interface	The port that connects to the VLAN or subnet.
VLAN ID	The VLAN's unique integer ID.
Deploy Monitor IP/Mask	The IP address to monitor.
Tag	The tag for the VLAN or subnet.
Gateway	The gateway IP address of the deployment network.
ARP Protection	Indicates ARP Protection is enabled (Yes) or disabled (No).

Setting up the deployment network

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. Configure the following settings:

Name	Name of the VLAN or subnet.
Interface	The port that connects to the VLAN or subnet.
VLAN ID	The VLAN's unique integer ID.
Deploy Monitor	The IP address to monitor.
<div style="display: flex; align-items: center;">  <div> <p>The deploy monitor IP/Mask must be an IP address and not a subnet.</p> <p>You must use the following guidelines to set the network IP/mask:</p> <ul style="list-style-type: none"> • Interface name and VLAN ID must be unique among all network IP/masks. • If VLAN ID is 0, the network IP/mask must be unique among all the network IP/masks without VLAN and all system interfaces. • If VLAN is not 0, the network IP/mask must be unique among all subnets in the same VLAN. </div> </div>	
Gateway	The gateway IP address of the deployment network.
ARP Protection	Select to enable ARP poisoning detection. ARP Protection is disabled by default. Upgrading FortiDeceptor will disable this setting.
Tag	You can specify a tag for the VLAN or subnet.
Ref	The number of objects referring to this object.



Each *VLAN/Subnet* with a network mask of /24 and higher is counted as one seat of the VLAN license.

Each *VLAN/Subnet* with a network mask less than /24 is counted as two seats of the VLAN license.

5. Click Save.

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 + *Create a new decoy* 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.
Appliance Name	Destination of the Decoy VM. This can be local (manager) or remote client (remote appliance). This column only shows in Central Management mode on manager.
Available Deception OSES	Select a Deception OS. The OS you select determines the services that are available.
Available Deception Decoys	This only supports SCADA V3/IoT deception OS. The decoy you select determines the specific services set.

Selected Services

Displays the services available for the Deception OS you selected.

Services for Windows include RDP, SMB, NBNSSpoofSpotter (responder tool detection), TCPLISTENER, ICMP, IIS(HTTP), and IIS(HTTPS).

Services for SCADA include HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, ENIP, DNP3, KAMSTRUP, and IEC104.

Services for Ubuntu include SSH, SAMBA, TCPLISTENER, HTTP, HTTPS, GIT, ICMP, FTP.

Services for Medical OS include Infusion Pump (Telnet), Infusion Pump (FTP), PACS, PACS-WEB, and DICOM server

Services for POS OS include POS-WEB.

Services for ERP OS include ERP-WEB.

Services for FortiGate include SSLVPN.

Services for Cisco Router include Telnet, HTTP, SNMP and CDP.

Services for HP Printer include Jetdirect, Printer-WEB and SNMP.

Services for SAP include SAP ROUTER, SAP DISPATCHER and SAP WEB

Services for IoT include SNMP, Jetdirect, Printer-WEB, Telnet, HTTP, CDP, TP-LINK WEB, CWMP, IP Camera-WEB, UPnP and RTSP.

Services for IP Camera include IP Camera-Web, UPnP, SNMP and RTSP.

CentOS include SSH, SAMBA, TCPLISTENER, HTTP, HTTPS, GIT, ICMP, FTP.

Automate Lures

Select one or more tag names to automate lure generation and to generate related contents. Selecting *any* and *all* generate random content.

Click *Generate Lures* to automatically generate lures and list them in the panes below.

Click *Clear* to delete the lures on this page.

4. If applicable, click *Generate lures* or *Add Lure* for the service and configure the lure settings. See, [Lure Settings on page 44](#).
5. To launch the decoy VM immediately, scroll to the bottom of the page and enable *Launch Immediately*.
6. To reset the decoy VM after it detects incidents, enable *Reset Decoy* and specify the *Reset Interval* value in seconds.
7. Click *Next*. The *Set Network* tab opens.
8. Configure the network IP and Hostname. You can enter up to two DNS IP addresses.

DNS

Enter the network IP address.

You must set Domain DNS server IP to be the 1st DNS when custom Windows decoys are in the domain(s).

DNS2

(Optional) Enter a second network IP address.

Two DNS IP addresses are not supported in the FortiGate SSLVPN decoy deployments.

Hostname

Enter the hostname for the network.

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 supported.

The *Hostname* cannot conflict with decoy names.

9. Click *Deploy Into Network*.
10. Select the *Deploy Interface*. Set this to the VLAN or subnet added in [Deployment Network on page 40](#)
11. 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.
MAC Address OUI	The first three octets of the MAC address for the device vendor. Only the xx:xx:xx format is supported.
IP Count	Specify the number of IP addresses to be assigned, up to 24 (for both STATIC and 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> .

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



For deception strategies and examples, see [Deployment best practices checklist on page 149](#) and [Deception decoy best practices on page 144](#)

Lure Settings

The lure settings will vary depending on the service. The character limits and requirements in FortiDeceptor may differ from the requirements implemented in the service.

Character restrictions and guidelines

Lure setting	Service	Requirements
Client Number	SAP DISPATCHER	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), commas (,), hyphens (-), underscores (_), and spaces are supported.

Lure setting	Service	Requirements
DICOM Listening Port	Medical	Enter a value between 1-65535. Default is 4242.
DICOM Server Name	Medical	Maximum of 16 characters. Name cannot begin with a digit. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
Domain (optional)	Windows: NBNSSpoofSpotter	Alphanumeric characters (A-Z, a-z, 0-9) and periods (.), are supported.
DSN Description	Windows: ODBC lure	Maximum of 256 characters. Alphanumeric characters (A-Z, a-z, 0-9), special characters (.-_!@(~)?[: +;*"/)" and spaces are supported.
DSN Name	Windows: ODBC lure	Maximum of 32 characters. Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
FTP Banner	SCADA3, Ubuntu, Centos	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
Hostname	Windows: NBNSSpoofSpotter SAP DISPATCHER	Maximum of 15 characters. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
HTTP Listening Port	Ubuntu, Centos	Enter a value between 1-65535. Default is 80.
HTTPS Listening Port	Ubuntu, Centos	Enter a value between 1-65535. Default is 443.
HTTPS SSL Certificate	Ubuntu, Centos	Optional. Upload using default settings is supported.
Instance Name	SAP DISPATCHER	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), commas (,), hyphens (-), underscores (_), and spaces are supported.
Interval(sec)	Windows: NBNSSpoofSpotter	Enter a value between 60-3600.
Listening Port	ERP (CRM), POS, SAP Router, SAP DISPATCHER, TP-LINK, CWMP	Enter a value between 1-65535. <ul style="list-style-type: none"> ERP (CRM), POS, and TP-LINK: Default is 80. SAP Router: Default is 3299 SAP DISPATCHER: Default is 3200 CWMP: Default is 7547
Listening Port Over HTTPS	SAP WEB	Enter a value between 1-65535. Default is 443
Module type	SCADA3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.

Lure setting	Service	Requirements
PACS Listening Port	Medical	Enter a value between 1-65535.Default is 80.
PACS System Name	Medical	Maximum of 16 characters. Name cannot start with a digit. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), and underscores (_) are supported.
Page title	SCADA V3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
Password	Windows: RDP & SMB, Ubuntu and Centos: SSH & SAMBA, NBNSSpoofSpotter GIT Users, ERP (CRM), Medical, POS, FortiGate, Cisco Router (Telnet/HTTP), HP Printer (HTTP), IP Camera (HTTP), Centos, SAP Router, SAP WEB, Brother MFC Printer (HTTP), Lexmark Printer (HTTP), TP-LINK	Maximum of 32 characters. Alphanumeric characters (A-Z, a-z, 0-9) and special characters (!@#\$%&~)^*<?: +;*/,." _) are supported. The password is optional in <i>GIT repository import</i> .
Plant Identification	SCADA V3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
PLC name	SCADA V3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
Repository Name	GIT Users	Maximum of 100 characters. Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
Serial number	SCADA V3	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), underscores (_), and spaces are supported.
Serial number for ENIP	SCADA V3	Only 0-9 allowed
Sharename	Windows:RDP & SMB, Ubuntu Centos-SSH & SAMBA Centos	This option is only available for SAMBA (Ubuntu) or SMB (Windows). Enter a Sharename between 3-63 characters. Alphanumeric characters (a-z, 0-9) and hyphens are supported.
SID	SAP DISPATCHER	Alphanumeric characters (A-Z, a-z, 0-9), periods (.), commas (,), hyphens (-), underscores (_), and spaces are supported.

Lure setting	Service	Requirements
SNMP	SCADA V3, Cisco Router (Telnet/HTTP), HP Printer (HTTP), IP Camera (HTTP), Brother MFC Printer (HTTP), Lexmark Printer (HTTP)	Alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_) are supported.
SSLVPN Bookmarks Name	FortiGate	Maximum of 15 characters. Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-), underscores (_), and spaces are supported.
SSLVPN Bookmarks URL	FortiGate	Required field. Alphanumeric characters (A-Z, a-z, 0-9), spaces, and special characters (-@#~?:./_=) are supported.
SSLVPN Listening Port	FortiGate	Enter a value between 1-65535. Default is 10443.
TCP Listener	Windows: TCP Listener Ubuntu, Centos	Separate multiple ports with a comma (,).
Telnet	SCADA V3	Telnet username password is the same as ERP
Token	GitHub repository import	Alphanumeric characters (A-Z, a-z, 0-9), and periods (.) are supported.
Update or Cancel	Windows: RDP & SMB, Ubuntu and Centos: SSH & SAMBA	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.
URL	GitHub repository import	Required field. Alphanumeric characters (A-Z, a-z, 0-9), spaces, and special characters (-@#~?:./_=) are supported.
Username	Windows: RDP & SMB, Ubuntu and Centos- SSH & SAMBA, NBNSSpoofSpotter. GIT Users, ERP (CRM), Medical, POS, FortiGate, Cisco Router (Telnet/HTTP), HP Printer (HTTP), IP Camera (HTTP), Centos, SAP Router, SAP WEB, Brother MFC Printer (HTTP), Lexmark Printer (HTTP), TP-LINK	Maximum of 64 characters. Alphanumeric characters (A-Z, a-z, 0-9), periods (.), hyphens (-) and underscores (_) are supported.

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.


For information about using FortiDeceptor to generate a deception lure package based on the decoy service configuration, see [Deploying tokens using AD GPO logon script on page 158](#).

The following token types are available:

Token type	Description
SMB (hidden mapped network disk)	Map the shared directory to a remote decoy that acts as file server while the shared disk is hidden. The username and password are saved in the Windows Vault (Credentials Manager). SMB remote folders are Windows folders.
SAMBA (hidden mapped network disk)	Same as SMB but for Linux SAMBA shares. SAMBA remote folders are Linux folders.
RDP (Remote Desktop)	The username, password and the windows Decoy IP are saved in the Windows Vault (Credentials Manager). Additionally, it creates RDP shortcuts in %USERPROFILE%\Documents. The file name format is rdp_USERNAME_IP.rdp and created files are hidden. The RDP Lure username and password are saved in Windows Vault.
SSH (Secure Shell)	Create a hidden Putty shortcut in %USERPROFILE%\Documents. If Putty (putty.exe) is not installed in the specified directory, no shortcut is created.
Credential Cache Lure	In Domain environment, add a new credentials entry to the real desktop or server process lsass.exe.
HoneyDocs	Add fake files (Word & PDF) to Windows directories. The default is to the most recent folder. You can specify the location in the Windows directory.
ODBC	The ODBC lure saves a DSN connection string using the Trusted Connection mechanism. To deploy an effective ODBC token, the following is required: <ul style="list-style-type: none"> • Deploy with domain DNS and SQL SERVER service based on a custom windows image joining a domain. See, Custom Decoy Image on page 16 > <i>To deploy decoys with custom images–SQL Server</i>. • Install ODBC lures into domain user accounts that are on the same domain as the custom Windows server.
SAP token	Add fake SAP configuration files to Windows SAP installation path that contains decoy IP and other SAP related configuration data.

To create a FortiDeceptor token campaign:

1. Go to *Deception > Deception Token > Token Campaign*.
2. Click **+Campaign**.
3. Configure the campaign *Name* and *Mode*.

Name	Enter the campaign name.
Mode	<ul style="list-style-type: none"> • Offline: The complete Deception Tokens package will be downloaded from the FDC manager and copied to the endpoint using the external distribution system like the A/D logon script for deployment. • Online: A light Deception Tokens package will download from the FDC manager and copied to the endpoint using the external distribution system like the A/D logon script. The package will have the binary file and one configuration file that points to the endpoint to download the deception campaign from the FDC manager over a secure port. <hr/> <div>  <p>Use <i>Online</i> mode to change the campaign at any time on the FortiDeceptor server. Any changes you make will be applied to the endpoint.</p> </div>

4. Select the lures. At least one lure must be selected.



You can only select lures with valid Static IP addresses.

The related decoys must have a status of *Initialized*, *Stopped*, *Running*, or *Failed*. We recommend keeping the related decoys with a status of *Running* for successful lure deployment.

5. (Optional) Click *Generate API Auth Key* to generate an API key.
6. Click **Save**.

Campaign

Campaign Name:
Mode: Online ▾

<input type="checkbox"/>	Lure Type ↑ ▾	Decoy ↑ ▾	IP Address ↑ ▾	IP Mode ↑ ▾
<input type="checkbox"/>	RDP	w7-r12734	<input type="text"/>	Static
<input type="checkbox"/>	SMB	w7-r12734	<input type="text"/>	Static

« 1 » 20 ▾
1 - 2 of 2 Items

























It is required to select one Lure at least.

Generate API Auth Key

Save Cancel

To view campaign list:

1. Go to *Deception > Deception Token*.
2. Select a campaign from the list. In the column:
 - Click *Edit* icon to edit the campaign.
 - Click *Delete* icon to delete the campaign.
 - Click *Download* icon to download the campaign.

Token Campaign		Token Deployment Status					
+ Campaign		Delete					
<input type="checkbox"/>	Action	Campaign Name ↑	Online/Offline	Created By	Created At	Lure Services List	API Token
<input type="checkbox"/>	  	██████████	Offline	admin	2022-03-16 13:48:07 PDT	SAMBA, RDP, Cached Credential, HoneyDoc, HTTP, SSH, SMB	████████████████████████████████████████████████████████████████████████████████
<input type="checkbox"/>	  	██████████	Offline	admin	2022-03-29 16:21:49 PDT	RDP	████████████████████████████████████████████████████████████████████████████████
<input type="checkbox"/>	  	██████████	Offline	admin	2022-03-17 11:34:59 PDT	RDP, SMB	████████████████████████████████████████████████████████████████████████████████
<input type="checkbox"/>	  	██████████	Online	admin	2022-03-29 16:23:09 PDT	RDP	████████████████████████████████████████████████████████████████████████████████
<input type="checkbox"/>	  	██████████	Offline	admin	2022-03-17 11:35:55 PDT	SAMBA	████████████████████████████████████████████████████████████████████████████████
<input type="checkbox"/>	  	██████████	Offline	admin	2022-03-17 15:34:36 PDT	SMB	████████████████████████████████████████████████████████████████████████████████
<input type="checkbox"/>	  	██████████	Online	sally	2022-03-29 16:25:03 PDT	SMB	████████████████████████████████████████████████████████████████████████████████
<input type="checkbox"/>	  	██████████	Online	sally	2022-03-17 14:29:25 PDT	SSH	████████████████████████████████████████████████████████████████████████████████

To deploy FortiDeceptor token campaign on an existing endpoint:

1. Download FortiDeceptor token campaign package
2. Copy the downloaded FortiDeceptor token campaign package to an endpoint such as a Windows or Linux endpoint.
3. Unzip the FortiDeceptor token campaign package.
4. In the OS folder, follow the instructions in README.txt file to install the token package.
 - **Windows:** Open the windows folder, and double-click the *windows_token.exe* to run it.
 - **Ubuntu:** Open Terminal and run python script *./ubuntu_token.py*.
5. In the OS folder, uninstall the token campaign package.
 - By default, the new token installation process will automatically clear the lure information before installing the new ones.

When the FortiDeceptor token package is installed on a real Windows or Ubuntu endpoint, it increases the deception attack surface and lures the attacker to a Decoy VM

To review Token Deployment Status:

1. Go to *Deception > Deception Token > Token Deployment Status*.
2. Expand the *Endpoint Name* to view the *Token Deployment Details* for the endpoint.

Endpoint Name	IP Address	Last Deployment Date	Campaign Name	Success/Failure
GPO16102	10.10.2.57	2022-05-11 12:32:07 PDT	72-B223-online	Success

Deployment Details	
<p>✓ Cached Credential</p> <ul style="list-style-type: none"> Decoy: [redacted] Lure User: adlure7@fdcad69.net / Lure Password: lure123# Decoy: [redacted] Lure User: adlure6@fdcad69.net / Lure Password: lure123# Decoy: [redacted] Lure User: adlure7@fdcad69.net / Lure Password: lure123# Decoy: [redacted] Lure User: adlure6@fdcad69.net / Lure Password: lure123# 	
<p>✓ HoneyDoc</p> <ul style="list-style-type: none"> Decoy: [redacted] 	
<p>✓ ODBC</p> <ul style="list-style-type: none"> Decoy: [redacted] 	
<p>✓ RDP</p> <ul style="list-style-type: none"> Decoy: [redacted] Lure User: kari / Lure Password: [redacted] Decoy: [redacted] Lure User: alvin / Lure Password: [redacted] Decoy: [redacted] Lure User: adlure7@fdcad69.net / Lure Password: [redacted] Decoy: [redacted] Lure User: adlure3 / Lure Password: [redacted] Decoy: [redacted] Lure User: albert / Lure Password: [redacted] Decoy: [redacted] Lure User: erik / Lure Password: [redacted] Decoy: [redacted] Lure User: mariah / Lure Password: [redacted] Decoy: [redacted] Lure User: adlure6@fdcad69.net / Lure Password: [redacted] 	

Decoy Status

The *Decoy Status* page shows the status of the Decoys on your network. Use the page to start, stop or delete a decoy. You can also view the decoy's configuration details and copy the decoy template.

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


Decoy Status							
Refresh		Delete	Start	Stop			
<input type="checkbox"/>	Action	Appliance ↑	Status	Decoy Name ↑	MAC	Network Type	IP
<input type="checkbox"/>		C239	Stopped	B119-239w	52:94:74:74:fa:1a	Static	10.10.2.60
<input type="checkbox"/>		C239	Stopped	B119-239w	52:3a:33:b3:75:4b	Static	10.10.2.61
<input type="checkbox"/>		C239	Stopped	B212	52:ed:5d:ae:7d:89	DHCP	10.10.2.25
<input type="checkbox"/>		C239	Stopped	c239-ubuntu	52:29:0d:3e:ef:98	Static	10.10.2.108
<input type="checkbox"/>		C239	Stopped	c239-ubuntu	52:4e:0d:8d:8d:bb	Static	10.10.2.105

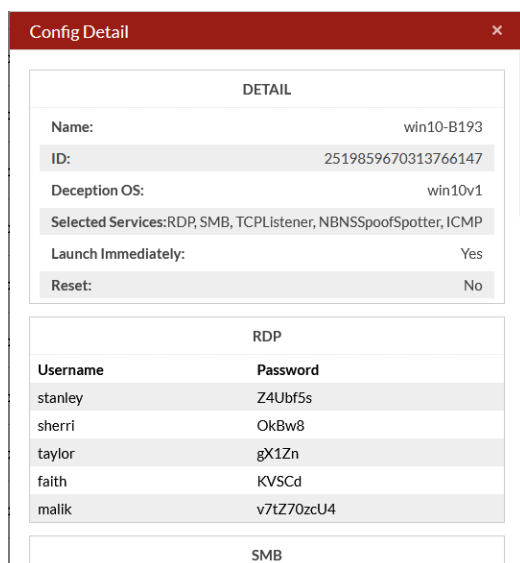
The *Decoy Status* page displays the following information:

Status The status of the decoy can be *Initializing*, *Running*, *Stopped*, or *Cannot Start*. If the Decoy VM cannot start, hover over the VM to see the reason.

Decoy Name	Name of the decoy.
Initialize Time and Start Time	The decoy's initialization time and its last start time.
OS	Operating system of the decoy.
VM	The name of the Decoy 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 view the decoy configuration details:

1. Go to *Deception > Decoy Status* and select a decoy.
2. In the *Action* column, click *View Details* . The *Config Detail* page opens.



The screenshot shows a window titled "Config Detail" with a close button. It contains two main sections: "DETAIL" and "RDP".

DETAIL Section:


- Name: win10-B193
- ID: 2519859670313766147
- Deception OS: win10v1
- Selected Services: RDP, SMB, TCPListener, NBNSspoofer, ICMP
- Launch Immediately: Yes
- Reset: No

RDP Section:


Username	Password
stanley	Z4Ubf5s
sherri	OkBw8
taylor	gX1Zn
faith	KVSCd
malik	v7tZ70zcU4

Below the RDP section is a section for SMB.

To copy a decoy the Deployment Wizard:

1. Go to *Deception > Decoy Status* and select a decoy.
2. Click *Copy to Template* . The template is copied to the *Deployment Wizard*.

To delete Decoy VMs:

1. Go to *Deception > Decoy Status* and select one more decoys.
2. In the *Action* column, click *Delete* .
3. Click *OK*.

To start a Decoy VM:

1. Go to *Deception > Decoy Status* and select one more decoys that are stopped.
2. In the *Action* column, click *Start* ►.

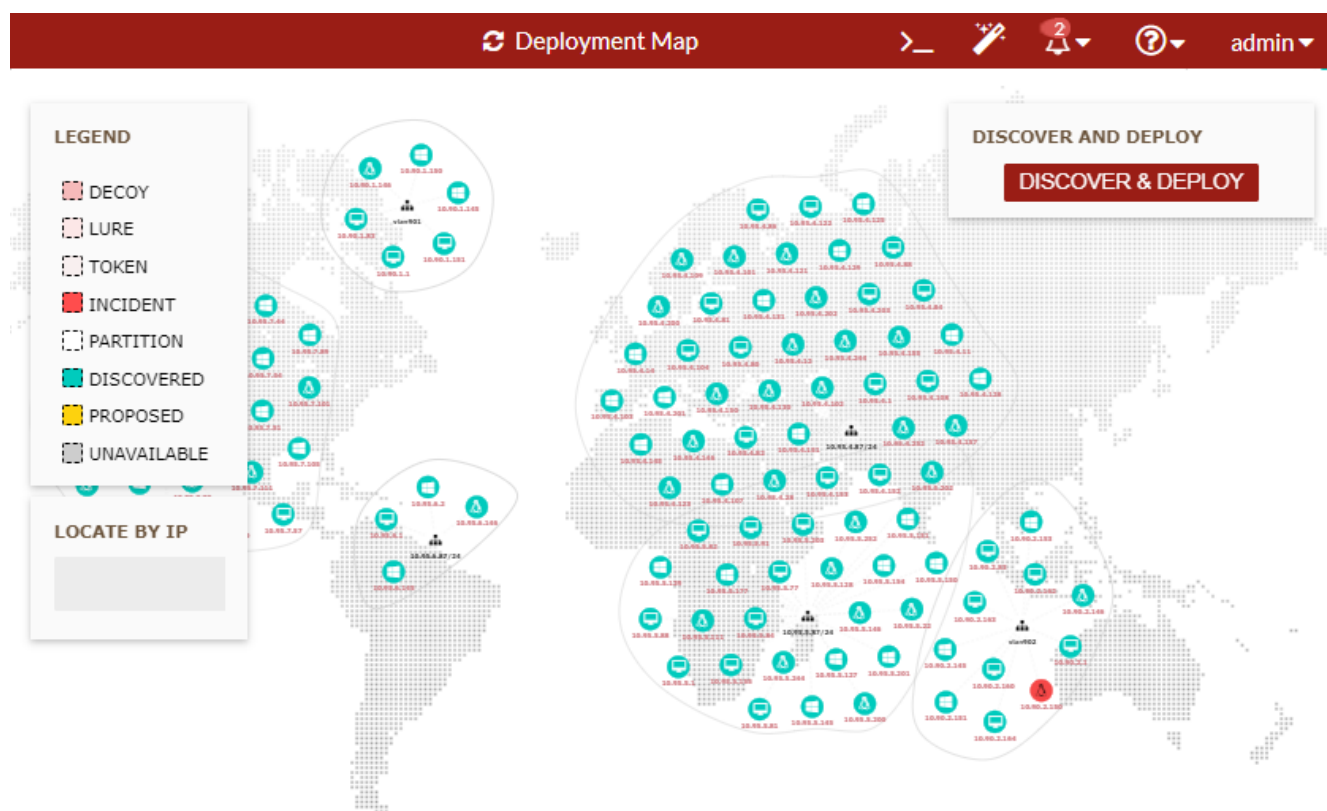
To stop a Decoy VM:

1. Go to *Deception > Decoy Status* and select one more decoys that are running.
2. In the toolbar, click *Stop*. The decoy status changes to *Stopped* ■.

Deployment Map

The *Deployment Map* is a visual representation of the entire network showing real endpoints and decoy VMs. Click a node on the map to view its details. Use *Discover & Deploy* to detect the OSES for all the assets on the network and automatically deploy decoys for those OSES.

If you know the IP of an endpoint or partition, you can search for it with the *Locate By IP* box.



The nodes on the map are color-coded by importance:

Node	Color	Description
Partition	White	Click the node to view the Network Partition ID, Interface port, and subnet.
Incident	Red	A glowing red node indicates the decoys have been attacked. Click the node to view the Decoy ID, view incidents in the <i>Analysis</i> page.
Decoy	Pink	Click to start or stop the, view its configuration, save the decoy as a template, or delete it.
Lure	Coral	Click to view the Decoy type, Service, and data such as the username and password.
Endpoint	Green	Click to view the IP, MAC address, and OS.
Proposed	Yellow	Click a yellow node to edit its settings, generate lures, duplicate, or delete it.
Unavailable	Grey	FortiDeceptor cannot retrieve data for the asset.

Discover & Deploy

Use *Discover & Deploy* to detect the OSes for all the assets on the network. After the OSes are discovered, FortiDeceptor will attempt to create decoys to auto-fit the assets in the network.

To discover OSes and auto-deploy decoys:

1. Click *Discover & Deploy*. The *Discovery & Deployment* dialog opens.
2. Configure the discover settings.

Select Networks to Scan	Select the ports on the network you want to discover.
Add Deployment Network	Click to open the <i>Add New Vlan/Subnet</i> dialog. See Deployment Network on page 40 .
Additional TCP Scan Port	Enter the additional scan ports. The default scan ports are 21, 22, 23, 25, 53, 69, 80, 110, 135, 137, 1378, 139, 143, 443, 445, 993, 995, 1433, 3306, 3389, 5900, 8080.
Decoys per VLAN/Subnet	Enter the number of decoys per VLAN based on the asset discovery results.

- Click *Discover* and wait a few minutes for the system to complete the discovery. The results are displayed.

OS Covered	The OSes FortiDeceptor can cover with a suitable decoy for auto-deployment.
Total auto-deploy decoys	The number of decoys that are suitable for auto-deployment.
Total coverage	The percentage of assets that will be covered by the deployment.
Download assets list CSV	Click to download the asset list as CSV file.

- Click *Accept & Deploy*. FortiDeceptor deploys the decoys.

Asset Discovery

The *Asset Discovery* module generates Asset Inventory by passively fingerprinting the OS and other parameters for the assets in OT/IT/IoT networks. This improves threat visibility for the networks and helps with optimizing decoy placement.

Asset Discovery									
Asset discovery setting Export to CSV Delete									
<input type="checkbox"/>	Action	IP Address	MAC	Vendor	Network	Hostname	Device OS	Device Fir...	Device Ty...
<input type="checkbox"/>		[REDACTED]	00:0c:29:88:...		deploynet1		Windows 7 E...	6.1.7601	
<input type="checkbox"/>		[REDACTED]	00:0c:29:62:...		deploynet1		Windows 10 ...	10.0.19041	
<input type="checkbox"/>		[REDACTED]	00:0c:29:62:...		10.11.2.0/24		Windows 10 ...	10.0.19041	

The Asset Discovery page displays the following information:

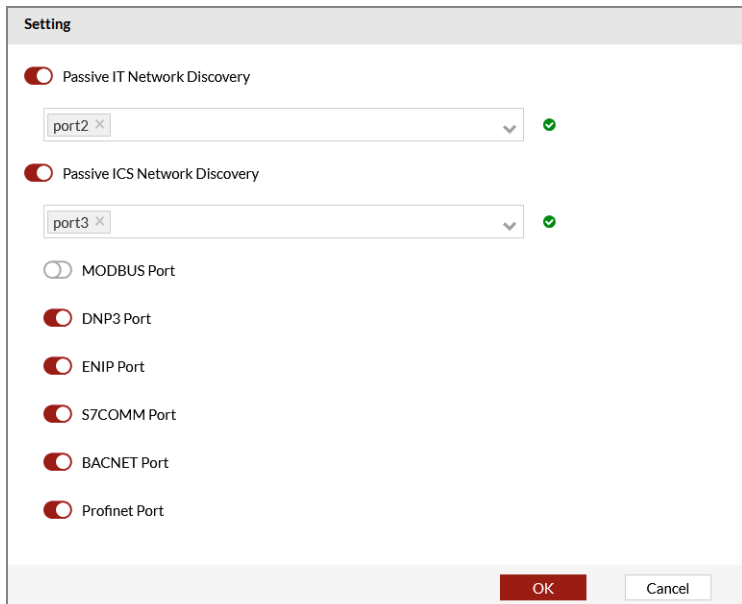
Action	Click <i>Delete</i> to remove the asset.
IP Address	The IP address of the asset.
MAC	The MAC address of the asset.
Vendor	The vendor identified by the asset MAC address.
Network	The network this asset was discovered.
Hostname	The hostname of the asset.
Device OS	The Device OS of the asset.
Device Firmware	The firmware version of the asset.
Device Type	The type of the asset.

To enable Asset Discovery:

- Go to *Deception > Asset Discovery*.
- Click *Asset discovery setting*.
- Enable the following the settings:

Passive IT Network Discovery	Enable to allow FortiDeceptor to identify common IT devices such as servers, laptops, and routers by sniffing network traffic.
-------------------------------------	--------------------------------------------------------------------------------------------------------------------------------

Select all the ports connected to the network for discovery.	
Passive ICS Network Discovery	Enable to allow FortiDeceptor to identify industrial control devices such as PLC controllers.
	Select all the ports connected to the network and ICS protocols for discovery.



The screenshot shows a 'Setting' dialog box with the following content:

- Passive IT Network Discovery:** A dropdown menu showing 'port2' with a green checkmark to its right.
- Passive ICS Network Discovery:** A dropdown menu showing 'port3' with a green checkmark to its right.
- MODBUS Port:** A red toggle switch.
- DNP3 Port:** A red toggle switch.
- ENIP Port:** A red toggle switch.
- S7COMM Port:** A red toggle switch.
- BACNET Port:** A red toggle switch.
- Profinet Port:** A red toggle switch.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

4. Click *OK*.

To delete multiple assets at the same time:

1. Select the assets you want to delete.
2. In the toolbar, click *Delete*.

To export the asset details as a CSV file:

In the toolbar, click *Export CSV*.

Configure a Safe List

Use the *Deception > Safe List* page to add an IP address that is considered legitimate so that it does not generate an *Event* or *Incident* when accessing decoys. For example, the IP address of a monitoring system that is polling the network.

To add a new Safe List IP address:

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

IP/Mask	Specify the IP address or subnet from where the connection originate.
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> .
Action	Click <i>Update</i> or <i>Cancel</i> .

Lure Resources

Use the *Lure Resources* page to view the current lure, upload resources such as Word and PDF files to automatically generate lures, and import a user name list from an LDAP server.

Lure Resources				
<div> + Upload Import Users from LDAP </div>				
Action	Type	Tag	File Name ↑	Upload Time
✕ Delete	Documents - Template (doc,docx,pdf,zip)	any	Competitive Research.docx	2022-06-15 14:29:55 PDT
✕ Delete	Documents - Fake Content (zip)	any	Human Resources.zip	2022-06-15 14:43:15 PDT
<div> 1 50 1 - 2 of 2 items </div>				

Uploading lure resources

Upload a lure resource to automatically generate lures. There are two types of lure resource

- **Documents:** Word and PDF files that generate authentic directories and files over the Decoy network shares.
- **Credential:** Username (with password) list files that generate authentic credentials access to the network Decoys.

To upload a lure resource:

1. Go to *Deception > Lure Resources*.
2. Click *Upload*. The *Upload New Lure Resource* dialog opens.
3. From the *Lure Type* dropdown, select the lure type.
 - **Credential - Fake Users (txt)**: Upload a list file with fake users and passwords.
 - **Documents - Template (doc,docx,pdf,zip)**: Upload files as a template. FortiDeceptor will insert content to build honey docs.
 - **Documents - Fake Content (zip)**: Upload files directly to FortiDeceptor.



The *Credential - Fake Users (txt)* and *Documents - Template (doc,docx,pdf,zip)* options include sample files to help you create a resource.

4. Enter an optional *Tag*, such as *any*.
5. In the *Resource File* field, click *Choose a file* to upload the resource, or drag and drop it onto the field.
6. Click *Save*.

Importing users from LDAP

To import an LDAP user list:

1. Go to *Deception > Lure Resources*.
2. Click *Import Users from LDAP*.

3. Configure the import settings.

Version	Select the version from the dropdown.
Bind DN	Username used to connect to the LDAP service on the specified LDAP Server.
LDAP URL	Enter the LDAP URL using the following format: [protocol:///]host[:port] [/basedn[?attribute,...] [?scope] [?filter]]
Bind Password	Enter the Bind DN's password.
CA Certificates	Select a certificate from the dropdown.
Search Limit	Search sub-tree depth.
TCP Timeout	Enter the TCP connection timeout in seconds.
Search Timeout	Enter the search timeout in seconds.
SASL Bind User	The username to authenticate a DN on the directory server using SASL.
SASL Bind Mechanism	The username and password for authentication.
Tag	Enter a tag for the import.

4. Click Save.

Examples: Import Users from LDAP

Open LDAP example:

```
"dn": "uid=test,o=org,dc=example,dc=com",
"url": "ldap://192.168.0.100/o=org,dc=example,dc=com?uid?sub?(objectclass=*)",
"password": "password"
```

Windows AD example:

```
"version": "3",
"dn": "cn=users,cn=usergroup,dc=example,dc=com",
"url": "ldap:192.168.0.100/cn=usergroup,dc=example,dc=com?sAMAccountName?sub?
(objectClass=user)",
"password": "password"
```

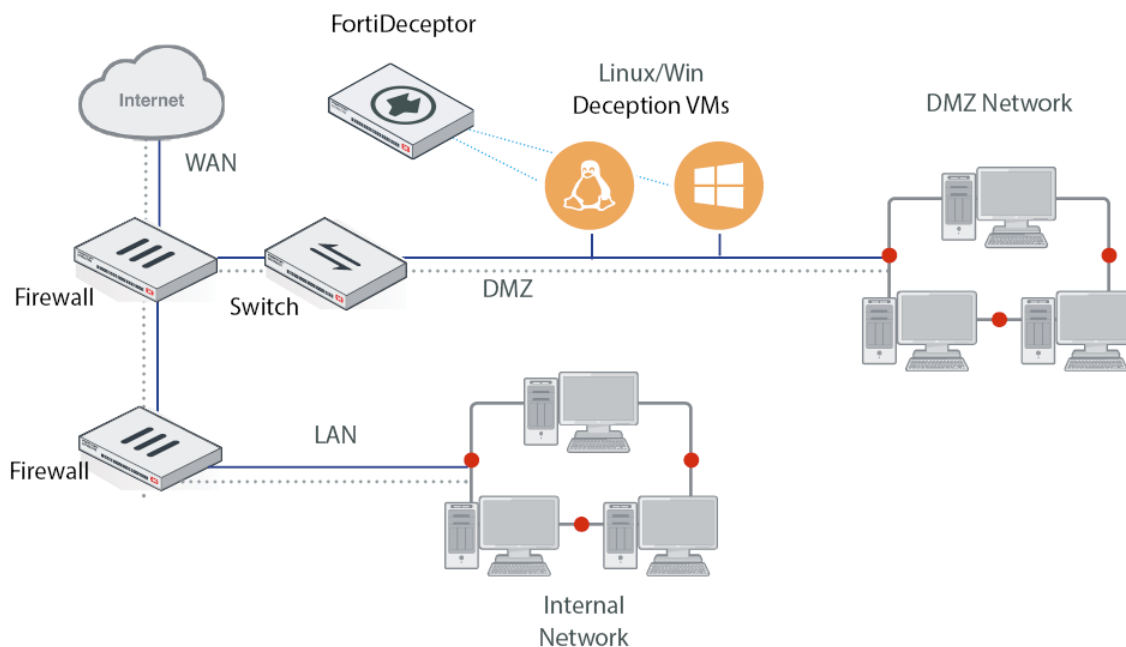
Support is offered if the format of the tree can parse uid/sAMAccountName in the search results. Ensure the URL queries the proper data.

DMZ Mode

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

DMZ mode is useful when you want to deploy decoys to a segment of the network that hosts critical services. When a threat actor attacks a server and attempts to move laterally inside the DMZ segment they are detected by the decoys

without exposing the decoys on the Internet.



Limitations of the DMZ Mode

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

- When DMZ mode is enabled, the banner displays *DMZ-MODE*.
- In *Deception > Deployment Network*, *Deception Monitor IP/Mask* is hidden. See [Deployment Network on page 40](#).
- 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 42](#).

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 62](#).
- *Incident > Campaign* lists attacks and related events detected by FortiDeceptor. See [Campaign on page 66](#).
- *Incident > Attack Map* shows attacks and related events detected by FortiDeceptor. See [Attack Map on page 68](#).

To monitor attacks using Dashboard widgets:

- Use the *Dashboard Incidents & Events Distribution* widget. See [Incidents and Events Distribution on page 69](#).
- Use the *Dashboard Incidents & Events Count* widget. See [Incidents and Events Count on page 70](#).

Analysis

The *Analysis* page displays the list of incidents detected by FortiDeceptor. Use this page to generate the *Incidents Report* PDF. You can also export the list as a CSV file.

When you expand an incident to the view the details, the incident is marked as *read*. Newly-detected incidents are in bold to indicate they are unread.

Analysis 1759 admin									
				Show Interaction Events Only					
	Protocol	Severity	Last Activity	Type	Attacker IP	Victim IP	Vi		
5	SMB	4	2022-05-11 16:16:30 PDT	Interaction			445		
11	SMB	4	2022-05-11 16:00:45 PDT	Interaction			445		
10	RDP	4	2022-05-11 15:39:51 PDT	Interaction			3385		
3	SMB	2	2022-05-11 12:28:36 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:28:05 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:27:35 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:27:06 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:26:36 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:23:50 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:23:21 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:22:50 PDT	Interaction			445		
3	SMB	2	2022-05-11 12:22:16 PDT	Interaction			445		
3	SMB	2	2022-05-11 10:28:36 PDT	Interaction			445		
3	SMB	2	2022-05-11 10:28:06 PDT	Interaction			445		
<div> 1 2 3 4 5 50 </div> <div>1 - 50 of 227 items</div>									

The *Analysis* page displays the following information:

Severity	Severity of the event.	
Protocol	Network protocol the attacker used to perform the attack.	
Last Activity	Date and time of the last activity.	
Type	Event Type	Triggered By
	Connection	<ol style="list-style-type: none"> 1. Port scan (SYNConnection). 2. Ping. 3. SYN connection. 4. Access to the service with no other interaction like accessing a web server without entering any credentials.

		Event Type	Triggered By
		Reconnaissance	<ol style="list-style-type: none"> 1. Port scan (Full TCP Connection). 2. Access the decoy network share and browse files. 3. Access the decoy web application and browse the web application. 4. Access decoy FTP server and browse files.
		Interaction	<ol style="list-style-type: none"> 1. The attacker accesses the decoy and passes the log in phase. 2. Attacker logs into a decoy and runs commands inside the session like RDP.
		Infection	<ol style="list-style-type: none"> 1. Attacker copies files to the decoy. 2. Attacker accesses the decoy and downloads files from the internet. 3. The attacker runs an exploit against the decoy and injects a binary file.
Attacker IP	Attacker IP address.		
Attacker User	Attacker username.		
Victim IP	IP address of the victim.		
Victim Port	Port of the victim.		
Decoy ID	Unique ID of the Decoy VM.		
ID	ID of the incident.		
Attacker IP	Attacker IP address and domain name.		
Attacker Port	Port where the attack originated.		
Tag Key	Unique key string for the incident.		
Attacker Password	Password used by the attacker.		
Start	Date and time when the attack started.		



The infected files captured by the decoy are saved as a password protected .zip file you can download. The password for the file is `FortiDeceptor`.

Table settings

Use the Actions menu at the top of the page to export the incidents table and sort the events. The table settings allow you to show or hide columns and set the order of the column headings in the table.

The following options are available in the Actions menu:

Action	Description
Refresh	Click to refresh the data.
PDF Report	Click to download the <i>detailed analysis</i> report in PDF format.
Export to CSV	Click to export the list as a CSV file. Depending on the number of incidents, the file may take some time to generate and export.
Mark all as read	Click to mark all the incidents as read.
Show	Click to display the incident events by type: <i>Interaction Events Only</i> (default), <i>IPS Events Only</i> , <i>Web Filter Events Only</i> , or <i>All</i> .

To generate the Incidents Report PDF:

1. Go to *Incident > Analysis*.
2. In the Actions menu, click *PDF Report*. The *Generate PDF Report* dialog opens.
3. In the *From* and *To* fields, specify the time range for the report.
4. (Optional) In the *Mail Address (optional)* enter an email address to send the report. Separate multiple email addresses with a semi-colon (;).
5. Click *Generate*.

To configure the table settings:

1. Go to *System > Table Customization*. The *Table Customization* dialog opens.
2. In the *Incident Columns* pane:
 - To show a column: Drag and drop the headers from the *Available Column Headers* to *Customized Column Headers and Orders*.
 - To hide a column: Drag and drop the headers from the *Customized Column Headers and Orders* to *Available Column Headers*.
 - To change the column order: Drag and drop the position of the headers in *Customized Column Headers and Orders*.
3. In the *Table Settings* pane, configure the table size and view.

Page Size	Enter the number of incidents to display per page when <i>View Type > Pagination</i> is selected.
View Type	Select <i>Pagination</i> , <i>Infinite Scroll</i> or <i>Both</i> .

Table View Settings

Incident Columns

Customized Column Headers and Orders

Severity Last Activity Type Attacker IP Attacker User Victim IP Victim Port

Available Column Headers

Protocol Decoy ID ID Attacker Port Tag Key Attacker Password Start

Table Settings

Page Size: 50

View Type: ☐ Pagination ☒ Infinite Scroll ☐ Both

Apply Reset Cancel

4. Click *Apply*.

Viewing the incident details

You can view the incident details in timeline or table view.

To view the incident details:

1. Go to *Incident > Analysis*.
2. Click the arrow » to expand the incident. The *Timeline* tab opens.

2022-05-11 10:15:06 PDT Interaction 10.10.2.16 N/A 10.10.2.54 445

Timeline **Table** Refresh

2022-05-11 10:10:33 PDT

Attacker User: N/A

Attacker IP: [Redacted]

Attacker Port: 53350

[Download lures](#)

right after(2022-05-11 10:10:33 PDT)

Open Port: From [Redacted] To [Redacted]

[Download Traffic PCAP](#)

MD5: 7dffe697a9856ceffa09356915cef9ca







File Size: 3.3 KB

File Type: pcap

4 seconds later(2022-05-11 10:10:37 PDT)










SAMBA logon failure: Wrong Username

3. Click the *Table* tab to view the incident details as a table.

Timeline Table Refresh				
Severity	PCAP	Time Stamp	Event Type	Detail
		2022-05-11 10:10:33 PDT	Open Port	From [redacted] on port 53350 to [redacted] on port 445.
		2022-05-11 10:10:37 PDT	SAMBA logon failure	Wrong Username
		2022-05-11 10:15:06 PDT	Close Port	From [redacted] on port 53350 to [redacted] on port 445.

Campaign

The *Campaign* page displays a list of attacks detected by FortiDeceptor. An attack consists of multiple incidents.

Campaign						
Refresh						
	Severity	Start	Attacker IP	ID	Last Activity	
2		2022-06-13 12:24:33 PDT	[redacted]	116	2022-06-13 12:24:33 PDT	
117		2022-06-12 22:15:36 PDT	[redacted]	115	2022-06-13 02:19:38 PDT	
194		2022-06-12 21:11:33 PDT	[redacted]	113	2022-06-13 00:05:05 PDT	
3		2022-06-12 21:15:15 PDT	[redacted]	114	2022-06-12 21:15:45 PDT	
1		2022-06-10 12:23:33 PDT	[redacted]	112	2022-06-10 12:23:33 PDT	
5		2022-06-09 22:54:29 PDT	[redacted]	111	2022-06-09 22:57:38 PDT	
1		2022-06-08 09:32:44 PDT	[redacted]	110	2022-06-08 09:32:44 PDT	
80		2022-06-07 22:46:22 PDT	[redacted]	109	2022-06-07 23:24:51 PDT	
14		2022-06-07 22:21:34 PDT	[redacted]	108	2022-06-07 22:25:59 PDT	

The *Campaign* page displays the following information:

Severity	Severity of the event.
Start	Date and time when the attack started.
Attacker IP	IP mask of the attacker.
ID	ID of the campaign record.
Last Activity	Date and time of the last activity.

To view the attack details:

1. Go to *Incident > Campaign*.
2. Expand an attack in the list. The campaign *Timeline* is displayed.

3. Click table to view the attack *Severity*, *Last Activity*, *Type*, *Attacker IP*, *Attacker User*, *Victim IP*, and *Victim Port*.

Timeline Table Refresh					
Severity	Last Activity	Type	Attacker IP	Attacker User	Victim IP
■	2022-06-13 12:24:33 PDT	Connection	[Redacted]	N/A	[Redacted]
■	2022-06-13 12:24:33 PDT	Connection	[Redacted]	N/A	[Redacted]

4. (Optional) Click *Refresh* to refresh the data.

To configure the table settings:

1. Go to *System > Table Customization*. The *Table Customization* dialog opens.
2. In the *Incident Columns* pane:
 - To show a column: Drag and drop the headers from the *Available Column Headers* to *Customized Column Headers and Orders*.
 - To hide a column: Drag and drop the headers from the *Customized Column Headers and Orders* to *Available Column Headers*.
 - To change the column order: Drag and drop the position of the headers in *Customized Column Headers and Orders*.
3. In the *Table Settings* pane, configure the table size and view.

Page Size	Enter the number of incidents to display per page when <i>View Type > Pagination</i> is selected.
View Type	Select <i>Pagination</i> , <i>Infinite Scroll</i> or <i>Both</i> .

Table View Settings

Incident Columns

Customized Column Headers and Orders

SeverityLast ActivityTypeAttacker IPAttacker UserVictim IPVictim Port

Available Column Headers

ProtocolDecoy IDIDAttacker PortTag KeyAttacker PasswordStart

Table Settings

Page Size

50

View Type

PaginationInfinite ScrollBoth

Apply

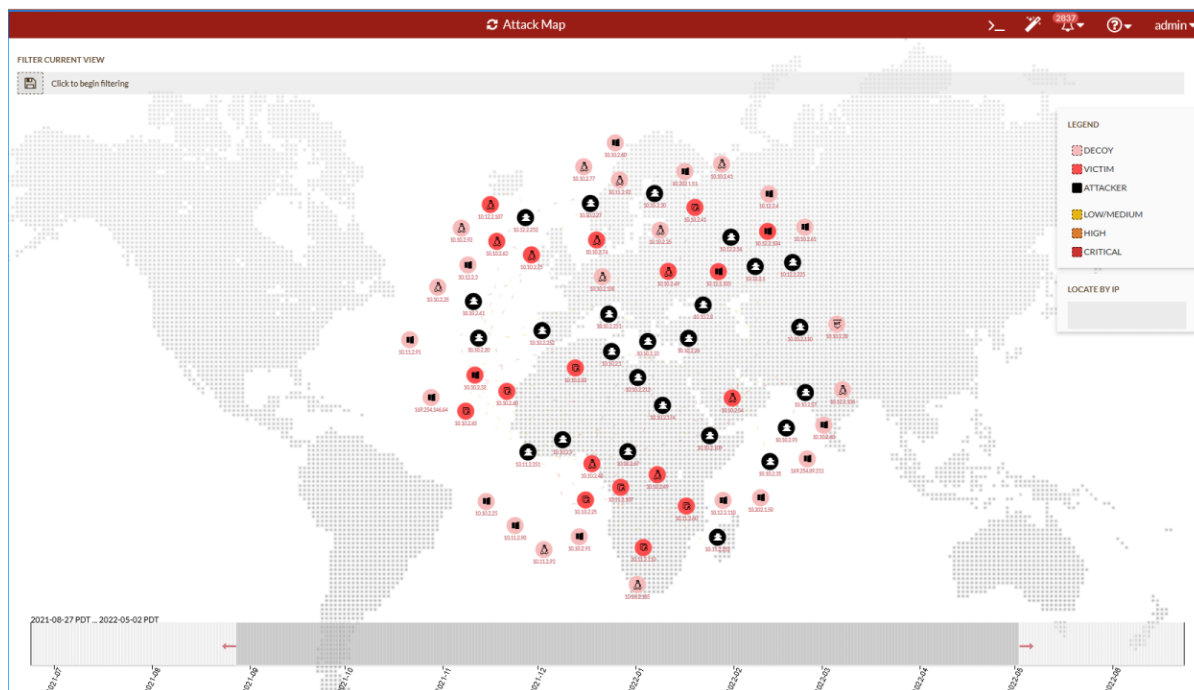
Reset

Cancel

4. Click *Apply*.

Attack Map

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




The nodes on the map are color-coded by severity.

Node	Color	Description
Decoy	Pink	Click to view the <i>Name</i> , <i>MAC address</i> , <i>IP</i> , <i>DNS</i> , and <i>Gateway</i> .
Victim	Red	Click to view the attack history including <i>Attacker</i> , <i>Start Time</i> and <i>Incident ID</i> . When a node is both Victim and Attacker, the node will appear as Attacker.
Attacker	Black	Click to view the attacker's history including <i>Attacker</i> , <i>Start Time</i> and <i>Incident ID</i> .

To filter the Attack Map by IP:

1. Under *Filter Current View*, click in inside *Click to begin filtering*. The options menu is displayed.
2. Select one of the following options:
 - *Attacker IP*
 - *Victim IP*
 - *Decoy IP*
3. Enter the IP address. FortiDeceptor sorts the nodes on the map.

To save the current view of the map:

Under *Filter Current View*, click the *Save View* icon .

To filter the map by date:

Drag the red arrows at the bottom of the page to set the start and end dates.



To search for a node by IP:

In the *Locate by IP* box, enter the IP address.

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 red.

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

To customize this widget:

- Click the edit icon to 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.

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:

- Click the edit icon to 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> .

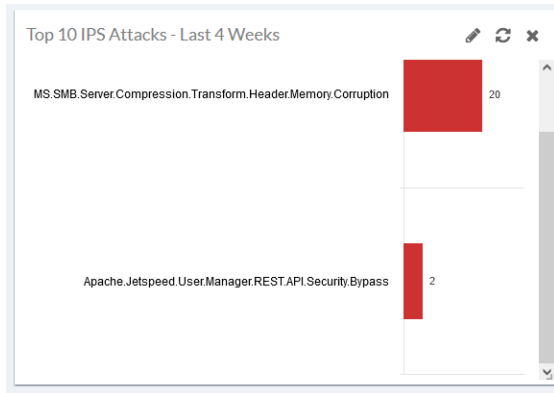
Top 10 Attackers by Incidents

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> .

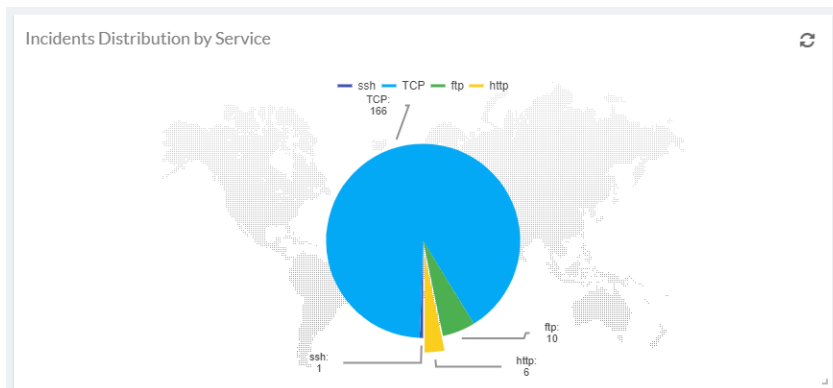
Top 10 IPS Attacks

The Top 10 IPS displays the IPS attack name and number of events for the selected time period (24 hours, 7 Days, or 4 weeks)



Incidents Distribution by Service

This dashboard widget displays the number of *Incidents* occurring by service with the percentage on a pie chart.



Supported services

Incidents Distribution by Service widget displays incidents occurring for the following services:

SSH, SAMBA, SMB, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, HTTPS, PACSWEB, POSWEB, AST, IPCAMERA, JETIRECT, TELNET, SSLVPN, KAMSTRUP, DICOM, ENIP, UPNP_HTTP, GIT, RTSP, PRINTER, DNP3, SAP_DISPATCHER, SAP_WEB_HTTPS, SAP_WEB, SAP_ROUTER, NETBIOS-NS, and ERPWEB.



Hover over the pie chart to see the percentage. Click the pie chart to split that 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 is under user quarantine in the FortiGate GUI.

Fabric provides access to the following pages:

Detection Devices	Configure the third-party malware detection devices for FortiDeceptor integration. When FortiDeceptor detects a suspicious file transfer in an incident, FortiDeceptor will send raw files to those detection devices for malware inspection and display the result along side the Incident.
Quarantine Integration	Configure the quarantine devices for FortiDeceptor integration
Quarantine Status	Status of blocked IP addresses.
IOC Export	Export the IOC file in CSV format for a specified time period.

Detection Devices

The *Detection Devices* page allows you to configure integrations with FortiSandbox, Cuckoo Sandbox, and Virus Total devices.

Detection Devices

Fabric Detection

FortiSandbox

Test

IP/URL: *

Port: *

Username: *

Password:

CuckooSandbox

Test

IP/URL: *

Port: *1337

API Token: *

Virus Total

VT API Key: *

Save

Reset

FortiSandbox

The integration between FortiDeceptor and FortiSandbox will provide a complete static and dynamic analysis against malicious code captured by the network decoys. The malware analysis report will be available on the FortiDeceptor admin console.

To configure integration with FortiSandbox:

1. Go to *Fabric > Detection Devices*.
2. Enable *FortiSandbox*.
3. Configure the following parameters:

Name	The Fabric connector name
IP/URL	Type the FortiSandbox IP address or URL
Port	Type the FortiSandbox API port. (default is 443)
Username	Type the API username. (please configure it on the Sandbox Console)
Password	Type the API password. (please configure it on the Sandbox Console)

4. Click on the *Test* button to ensure the API connection is working properly.
5. Click *Save* to store the configuration

Cuckoo Sandbox

The integration between FortiDeceptor and Cuckoo Sandbox will provide a complete static and dynamic analysis against malicious code captured by the network decoys. The malware analysis report will be available on the FortiDeceptor admin console.

To configure integration with Cuckoo Sandbox:

1. Go to *Fabric > Detection Devices*.
2. Enable *Cuckoo Sandbox*.
3. Configure the following parameters:

Name	The Fabric connector name
IP/URL	Type the Cuckoo Sandbox IP address or URL
Port	Type the Cuckoo Sandbox API port. (default is 1337)
API Token	Type the API Token located in the Cuckoo Sandbox's configuration file.

4. Click on the *Test* button to ensure the API connection is working properly.
5. Click *Save* to store the configuration

Virus Total

The integration between FortiDeceptor and the well-known Virus Total service allows the submission of suspicious files (MD5) for malware analysis. When integrated, Virus Total detection ratios will be displayed in the incident analysis alert Workflow for relevant events.

Virus Total engages with multiple service providers to perform the same file inspection. Some service providers return a score of *0*, meaning it is not malware, whereas other providers return a score of *1*, meaning it is malware. Virus Total then returns a ratio such as *15/36* that indicates *15* out of *36* service providers determined the file is malware.

To configure integration with VirusTotal:

1. Join the [VirusTotal Community](#).
2. In your personal settings section find your personal API key in your personal settings section.
3. Go to *Fabric > Detection Devices*.
4. Enable *VirusTotal*.
5. In *VT API Key* field enter the your Virus Total personal API key.
6. Click *Save*.

Quarantine Integration

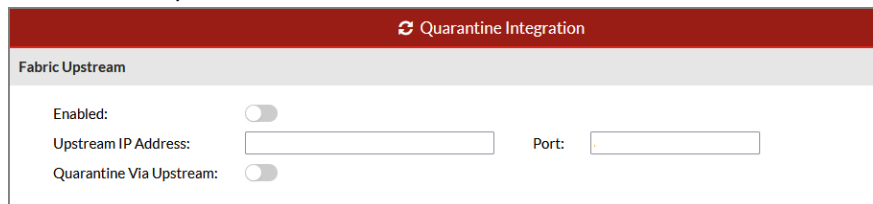
FortiDeceptor on FortiGate Security Fabric topology map

Security Fabric integration allows FortiDeceptor and deception decoys to be visible through the Fabric network topology map.

To configure Security Fabric integration, enter the upstream device IP in Port in FortiDeceptor. Next you will add the FortiDeceptor fabric connector in FortiGate.

To configure FortiGate for Security Fabric integration in FortiDeceptor:

1. In FortiDeceptor, go to *Fabric > Quarantine Integration*.
2. Under *Fabric Upstream* section, select *Enabled*.



The screenshot shows the 'Quarantine Integration' configuration page in FortiDeceptor. The page has a red header bar with a refresh icon and the text 'Quarantine Integration'. Below the header is a section titled 'Fabric Upstream'. Inside this section, there are three configuration items: 'Enabled:' with a toggle switch, 'Upstream IP Address:' with a text input field, and 'Quarantine Via Upstream:' with a toggle switch. A 'Port:' label is also present next to the 'Upstream IP Address' field, but it does not have an associated input field in the visible area.

- Enter the FortiGate IP address in *Upstream IP Address* and the FortiGate connector port in *Port*.

Fabric Upstream

Enabled:

☐

Upstream IP Address:

Port:

Quarantine Via Upstream:

☐

Quarantine Severity:

Low

Medium

High

Critical

Quarantine Expiry:

seconds

Apply

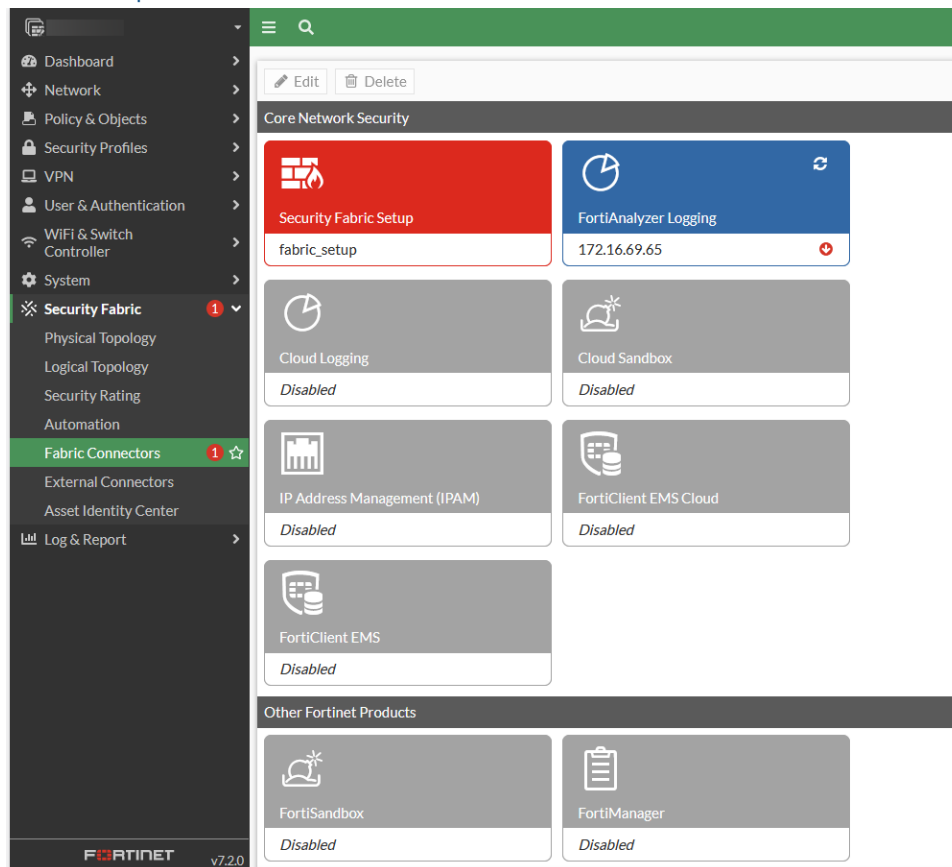
Cancel

+ Quarantine Integration With New Device

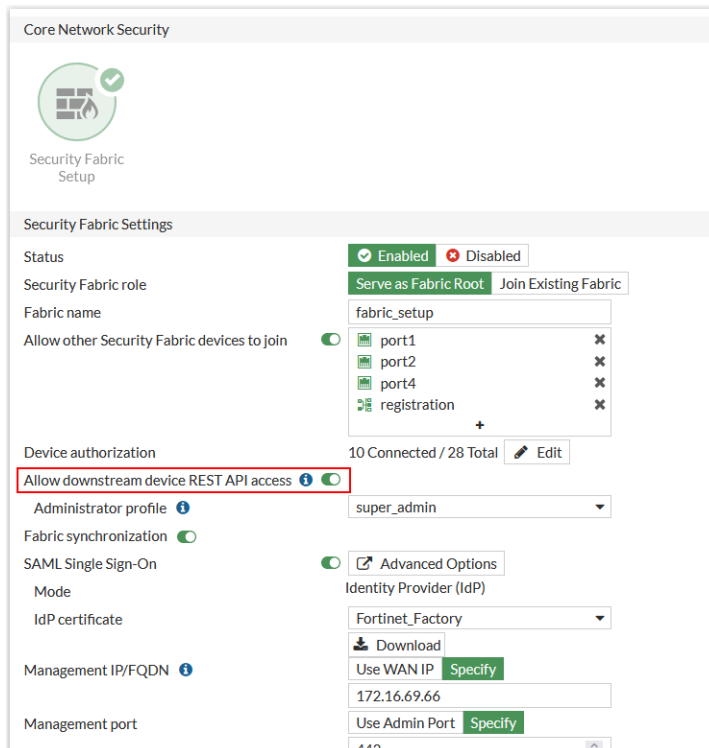
Action	Enabled	Status	Name	Integrate Method ↑	Severity	Detail
--------	---------	--------	------	--------------------	----------	--------

To add the FortiDeceptor fabric connector in FortiGate:

- In FortiGate, log in as an admin and go to *Security Fabric > Fabric Connectors*.
- Add the FortiDeceptor connector for this integration. For information, see [Configuring other Security Fabric devices > FortiDeceptor](#) in the *FortiGate Administration Guide*.



When configuring the Fabric Connector in FortiGate, you must enable *Allow downstream device REST API*.



FortiDeceptor supports the CSF protocol that triggers automatic mitigation/isolation of the infected endpoint from the network and prevents the attack from moving laterally.

The CSF integration provides access to more fabric devices for isolation like FortiSwitch through the FortiGate. SAML support between FortiGate WEB-UI to FortiDeceptor to allows SSO login from FortiGate to FortiDeceptor.



Cooperative Security Fabric (CSF), also known as a Fortinet Security Fabric, spans across an entire network linking different security sensors and tools together to collect, coordinate, and respond to malicious behavior in real time. CSF can be used to coordinate the behavior of different Fortinet products in your network, including FortiGate, FortiAnalyzer, FortiClient, FortiSandbox, FortiAP, FortiSwitch, and FortiClient Enterprise Management Server (EMS).

3. To trigger automatic mitigation using the CSF:
 - a. In FortiGate, log in as an admin and go to *Security Fabric > Automation*.
 - b. Click *Trigger > Create New*.
 - c. Configure the *Fabric Connector Event*:
 - i. Enter the *Name* of the event.
 - ii. Enter a *Description* of the event.
 - iii. Select a *FDC* appliance from the connector menu.
 - iv. Select an event.
 - v. Select the *Event Severity*.

- vi. Click OK.

Create New Automation Trigger

Fabric Connector Event A specified Fabric Connector's event has occurred.

Name: FDC

Description: FDC Mitigation 14/255

Fabric Connector Event

Connector: FDCVM-LAB

Event name:
 Search
 + Create
 Insider Threat
 Notify Ban
 Notify Unban

Event severity: Search

4. In the same screen, go to *Action > Create New* and choose any mitigation response you would like to execute once the FortiDeceptor pushes an incident alert to FortiGate.

Create New Automation Action

Search

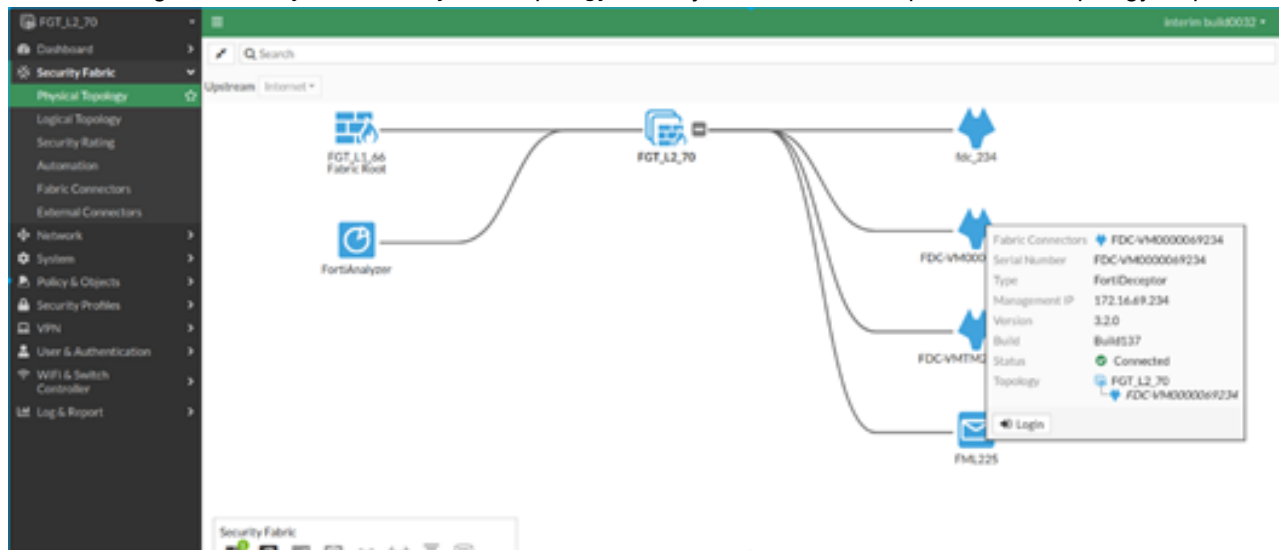
Security Response

- Access Layer Quarantine**
Quarantine the MAC address on access layer devices (FortiSwitch and FortiAP).
- FortiClient Quarantine**
Use FortiClient EMS to quarantine the endpoint device.
- FortiNAC Quarantine**
Use FortiNAC to quarantine the endpoint device.
- VMware NSX Security Tag**
Assign a specified security tag to a VMware endpoint device.
- IP Ban**
Ban the IP address specified in the automation trigger event.

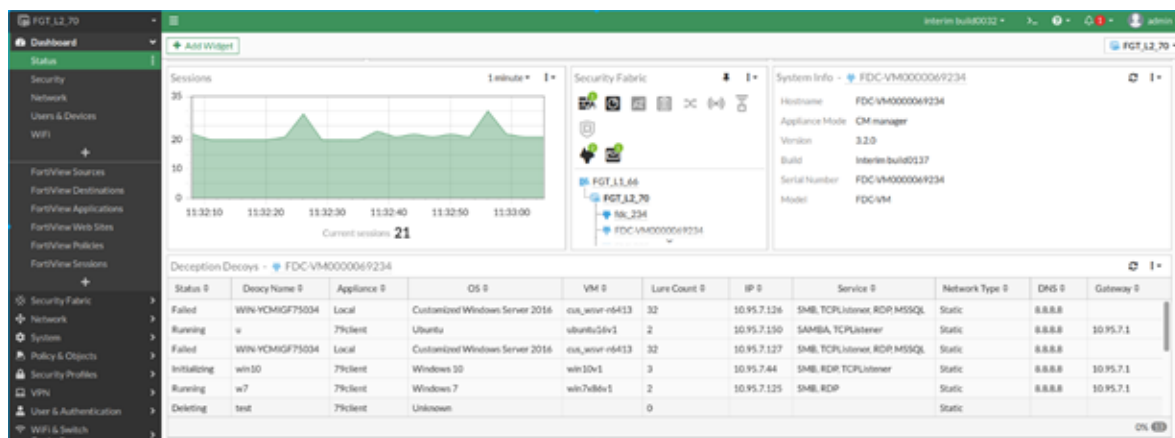
Notifications

- Email**
Send a custom email to the specified recipient(s).
- FortiExplorer Notification**

5. In FortiGate, go to *Security Fabric > Physical Topology* to verify that the FortiDeceptor is on the topology map.



6. In FortiGate, go to *Dashboard > Status* to view FortiDeceptor information and deception decoys configuration status.



FortiDeceptor integration for threat response mitigation

Use *Fabric > Quarantine Integration* to view and configure FortiGate and other device settings for integration with FortiDeceptor. Integration uses REST APIs, XML APIs, or webhooks. When decoys are accessed, FortiDeceptor makes quarantine calls and attackers are immediately quarantined on the device for further analysis.

The following information is displayed:

Action	Click <i>Edit</i> to edit the integration settings. Click <i>Delete</i> to delete the device.
Enabled	Shows if the device is enabled or disabled.
Status	Device status.
Name	Alias of the integrated device.

Integrate Method	<ul style="list-style-type: none">• FGT-REST-API• FGT-WEBHOOK• PAN-XMLAPI• GEN-WEBHOOK• FNAC-WEBHOOK• WMI-Disable• FortEDR-Isolation• Cisco-ISE• Microsoft-ATP• CrowdStrike-Isolation• FSM-Watch-List
Severity	Security level. The selected level and all levels above it are blocked. For example, if you select <i>Medium</i> , then when any attack reaches medium, high, or critical levels, the attacker IP address is blocked. If you select <i>Critical</i> , then only the critical level is blocked.
Detail	Device integration details.

To integrate a device:

1. Go to *Fabric > Integration Devices*.
2. Click *Quarantine Integration With New Device*.

3. Configure the device for integration. Then click **Save**.

Enabled	Enable or disable this device.
Name	Specify a name for this device.
Block Severity	The selected level and all levels above it are blocked. For example, if you select <i>Medium</i> , then when any attack reaches medium, high, or critical levels, the attacker IP address is blocked. If you select <i>Critical</i> , then only the critical level is blocked.
Appliance	Option for Central Management manager device to integrate the incidents from the specified appliances only.
Integrate Method	<p>The integration method of this device:</p> <ul style="list-style-type: none"> • FGT-REST-API (Default) • FGT-WEBHOOK • PAN-XMLAPI • GEN-WEBHOOK • FNAC-WEBHOOK • WMI-Disable • FortEDR-Isolation • Cisco-ISE • Microsoft-ATP • CrowdStrike-Isolation • FSM-Watch-List <p>Different integration methods have different settings. To view the settings for each integration type, see Integrate Method settings on page 82</p>
IP or Device IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username and Password	Username and password of the integrated device.
VDOM	For FortiGate devices, the default access VDOM.
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in second. Default is 3600 seconds.

Integrate With New Device

Enabled:

Name: *

fgtblocker6

Block Severity:

Low

Medium

High

Critical

Integrate Method:

FGT-REST-API

Compatible FortiGate version: 6.0.4 or later

IP: *

IP

Port: *

443

Username: *

Username

Password:

Password

Vdom: *

root

Expiry: *

3600

seconds

Save

Cancel

Integrate Method settings

FGT-REST-API

Compatible FortiGate version: 6.0.4 or later

IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username	Username of the integrated device.
Password	Password of the integrated device.
VDOM	For FortiGate devices, the default access VDOM.
Expiry	Default blocking time in second. Default is 3600 seconds.

FGT-WEBHOOK

Compatible FortiGate version: 6.4.0 or later

Block Action	Expiry	Default blocking time in seconds. Default is 3600 seconds.
	URL	Enter the request API URI.
	Authorization	Enter the API key.
Unblock Action	Expiry	Default blocking time in seconds. Default is 3600 seconds.
	URL	Enter the request API URI.
	Authorization	Enter the API key.

PAN-XMLAPI

Compatible PAN-device version: 10.0.0 or later

Device IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username	Username of the integrated device.
Password	Password of the integrated device.
Vsys	The virtual system which is configured on PAN
Policy Index	Select <i>Top</i> or <i>Bottom</i> .
Expiry	Default blocking time in seconds. Default is 3600 seconds.

GEN-WEBHOOK

Compatible FortiNAC version: 8.8 or later (Firmware: 8.8.2.1714)

Block Action:	Expiry	Default blocking time in seconds. Default is 3600 seconds.
	Http Method	Select GET, POST, PUT, or PATCH
	URL	Enter the request API URI.
	Authorization	Enter the API key.
	HTTP Header	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.
Unblock Action:	HTTP Data	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.
	Http Method	Select GET, POST, PUT, or PATCH
	URL	Enter the request API URI.
	Authorization	Enter the API key.
	HTTP Header	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.
	HTTP Data	Select Empty, Hacker-IP, Hacker-MAC, or Expiry-Time.

FNAC-WEBHOOK

Compatible FortiNAC version: 8.8.2.1714 or later.

IP:	IP address of the integrated device.
Port:	Port number of the integrated device API service. Default is 8443.

Authorization Token:	The FortiNAC-WEBHOOK authorization token generated by FNAC.
Expiry:	Default blocking time in seconds. Default is 3600 seconds.

WMI-Disable

Domain	The device domain.
Username	Username of the integrated device.
Password	Password of the integrated device.

FortiEDR-Isolation

Compatible FortiEDR version: 5.0.2.305 or later.

IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Organization\Username	The FortiEDR organization and username.
Password	Password of the integrated device.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

Cisco-ISE

Compatible Cisco ISE version: 2.7 or later.

Server URL/IP	The Cisco server URL and IP address.
Port	Port number of the integrated device API service. Default is 8443.
Username	Username of the integrated device.
Password	Password of the integrated device.
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

Microsoft-ATP

Server URL	Service base URI to connect and perform the automated operations. For example, https://api.securitycenter.microsoft.com .
Client ID	Client ID of the Azure application that is used to access Windows Defender ATP
Client Secret	Secret string that the application (used to access Windows Defender ATP) uses to prove its identity
Tenant ID	Tenant ID of the Azure application
Verify SSL	Enable to verify SSL.

Expiry	Default blocking time in seconds. Default is 3600 seconds.
---------------	------------------------------------------------------------

CrowdStrike-Isolation

Server URL	CrowdStrike server URL.
Client ID	Client ID of the CrowdStrike application which is used to access CrowdStrike isolation service.
Client Secret	Secret string of the CrowdStrike application which is used to access CrowdStrike isolation service.
Verify SSL	Enable to verify SSL.
Expiry	Default blocking time in seconds. Default is 3600 seconds.

FSM-Watch-List

IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 8443.
Username:	Username of the integrated device.
Password:	Password of the integrated device.
Organization	Type the organization name for the integration device.
Verify SSL	Enable to verify SSL.
Watch-List Name	Type Watch-List Name as defined in FortiSIEM.
Lure Users-Manual Mode	Type the other lures you want to watch.
Polling Time Interval	Default polling time in seconds. Default is 3600 seconds.

Quarantine Status

The *Fabric > Quarantine Status* page displays the status of blocked 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	IP addresses of blocked attacker.
Start	Start time of blocking behavior.

End	End time of blocking behavior.
Type	Blocking type, manual, or automatic quarantine.
Integrated Device	Alias of the device which blocks the <i>Attacker IP</i> address. This is the <i>Name</i> field in <i>Fabric > Integration Devices</i> .
Time Remaining	The remaining blocking time.
Status	Current status of the attacker.
Message	Additional message for the quarantine operation.

IOC Export

The *IOC Export* page allows you to export the IOC file in CSV or STIX format for a specified time period. The CSV file can be processed by third party Threat Intelligence Platforms. The file contains the TimeStamp, Incident ID, Attacker IP, related files, and WCF (Web Content Filtering) events. You can include MD5 checksums, WCF category, and reconnaissance alerts.

The screenshot shows the 'IOC Export' page. The header is red with the title 'IOC Export' and icons for navigation, search, notifications (1803), help, and a user dropdown 'admin'. The main content area has a light gray background. It contains two date/time pickers for 'From' and 'To'. Below these are three toggle switches: 'Include File MD5', 'Include WCF Category', and 'Exclude Reconnaissance Alerts'. At the bottom of the main area are three buttons: 'Reset', 'Export as CSV', and 'Export as STIX'. Below this is a section for 'STIX/TAXII Integration' with a toggle switch, and at the very bottom are 'Reset' and 'Save' buttons.

To export the IOC as a CSV file:

1. Go to *Fabric > IOC Export*.
2. Specify the date range by setting the date and time in the *From* and *To* fields.
3. (Optional) Include or exclude the following files and alerts:
 - *Include File MD5*
 - *Include WCF Category*
 - *Exclude Reconnaissance Alerts*
4. Click *Export as CSV*

To Push the IOC over STIX/TAXII server

1. Go to *Fabric > IOC Export*.
2. Specify the date range by setting the date and time in the *From* and *To* fields.
3. Enable *STIX/TAXII Integration*.
4. Configure the export settings:

API Root URL	Enter the API Root URL.
TAXII Username	Enter the TAXII username.
TAXII Password	Enter the TAXII password.
Collection ID	Enter the Collection ID.
Certificate File	Click Upload a certificate file to upload the certificate file.
Key File	Click to upload the API key file.
Certificate/Key Verification	Enable Certificate/Key Verification.
Include File MD5	Enable to include the MD5 file.
Include WCF Category	Enable to include the WCF category.
Include IPS Category	Enable to include the IPS category.

☒ STIX/TAXII Integration

API Root URL *
This field cannot be empty.

TAXII Username *
This field cannot be empty.

TAXII Password *
This field cannot be empty.

Collection ID *
This field cannot be empty.

Certificate File

Key File

Certificate/Key Verification ☐

Include File MD5 ☐

Include WCF Category ☐

Include IPS Category ☐

5. Click *Export as STIX* to push the export over the protocol in real time.

System

Use the *System* pages to manage and configure the basic system options for FortiDeceptor. This includes administrator configuration, mail server settings, and maintenance information.

The *System* menu provides access to the following:

Administrators	Configure administrator user accounts.
Admin Profile	Configure admin profiles to define admin privileges.
Certificates	Configure CA certificates.
LDAP Servers	Configure LDAP servers.
RADIUS Servers	Configure RADIUS servers.
Mail Server	Configure the mail server.
SNMP	Configure SNMP.
FortiGuard	Configure FortiGuard settings and upgradeable packages.
FDC License	Upload license files and input confirmation ID.
Settings	Configure the idle timeout or reset all widgets to their default state.
Login Disclaimer	Configure the Login Disclaimer.
Table Customization	Define columns and order of <i>Incident</i> and <i>Event</i> tables.

Administrators

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

If the admin user's Admin Profile does not have *Read Write* privilege under *System > Admin Profiles*, 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 using an account with *Read/Write* 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 upper-case letters, lower-case letters, numbers, or the underscore character (_) for <i>Local</i> and LDAP administrators. The character limit for RADIUS server administrators is 64 characters.
Password, Confirm Password	Password of the account. The password must be 6 to 64 characters using upper-case letters, lower-case letters, numbers, or special characters. This field is available when <i>Type</i> is set to <i>Local</i> .
Type	Select <i>Local</i> , <i>LDAP</i> , or <i>RADIUS</i> .
LDAP Server	When <i>Type</i> is <i>LDAP</i> , select an <i>LDAP Server</i> . For more information, see LDAP Servers on page 94 .
RADIUS Server	When <i>Type</i> is <i>RADIUS</i> , select a <i>RADIUS Server</i> . For more information, 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 the 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 using an account with *Read/Write* access and go to *System > Administrators*.
2. Select an account and click *Edit*.
Only the *admin* user can edit its own settings.

You must enter the 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 using an account with *Read/Write* 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 or RADIUS logins:

1. Log in using an account with *Read/Write* access and go to *System > Administrators*.
2. Select an LDAP or 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 or to 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:

- *Read Write* has access to all functionality. This includes creating, editing, and deleting administrator profiles
- *Read only* has read-only access.

The *Menu Access* section has the following settings:

None	User cannot view or make changes to that page.
Read Only	User can view but not make any change to that page, except session-related user settings such as Table Customization, Dashboard, or Attack Map filter.
Read Write	User can view and make changes to that page.

The *CLI Commands* section has the following settings:

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

To create an 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
Central Management	Appliances
Deception	<ul style="list-style-type: none"> • Custom Decoy Image • Deception OS • Deployment Network • Deployment Wizard • Decoy Status • Deployment Map • Asset Discovery • Safe List • Lure Resources • Deception Token
Incident	<ul style="list-style-type: none"> • Analysis • Campaign • Attack Map
Fabric	<ul style="list-style-type: none"> • Integration Devices • Quarantine Status • IOC Export • Detection Devices
Network	<ul style="list-style-type: none"> • Interfaces • System DNS • System Routing
System	<ul style="list-style-type: none"> • Administrators • Admin Profiles • Certificates • LDAP Servers • RADIUS Servers • Mail Server • SNMP • Login Disclaimer • FortiGuard • FDC License • System Settings • Table Customization
Log	<ul style="list-style-type: none"> • All Events • Log Servers

6. Specify the privileges for *CLI Commands*:

Configuration	<ul style="list-style-type: none"> • Set • Unset
System	<ul style="list-style-type: none"> • Reboot • Shutdown • Reset Configuration • Factory Reset • Firmware Upgrade • Reset Widgets • IP Tables • test-network • usg-license • 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 Package Information • Fabric Binding • Central Management Settings
Utilities	<ul style="list-style-type: none"> • 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 named *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.

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 users 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 users 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 Mail Server page to send incident alerts. You can also create custom delivery rules.

Mail Server

Send Incidents Alerts *

SMTP Server Address *

Port: *

From: *

Login User

Login Password

0.0.0.0

25

user@fortinet.com

optional

optional

Invalid email.

Reset

Save

Send Test Email

+ Custom Alert Delivery Rule

Edit

Delete

Rule Name	Status
-----------	--------

To send incident alerts:

1. Go to *System > Mail Server*. The *Mail Server* page opens.
2. Enable *Send Incidents Alerts*.
3. Configure the mail server settings.

SMTP Server Address	SMTP server address.
Port	SMTP server port number.
From	The mail server email account. This is the "from" address.
Login User	The mail server login account.
Login Password	Enter and confirm the password.

4. (Optional) Click *Send Test Email* to send a test email to one or more email addresses. If an error occurs, the error message appears at the top of the page and is recorded in the System Logs.
5. Click *Save*.
6. Click *Reset* to restore the default settings.

To create a custom alert delivery rule:

1. Click *Customer Alert Deliver Rule*. The *Custom Alert Rule* dialog opens.
2. *Enable* the rule. When enabled, FortiDeceptor sends an email alert to the Receiver Email List according to the rule

3. Configure the rule settings.

Name	Enter a name for the rule.
Alert Severity	Select <i>Low</i> , <i>Medium</i> , <i>High</i> , or <i>Critical</i> .
Alert Type	Select <i>Connection</i> , <i>Reconnaissance</i> , <i>Interaction</i> , or <i>Infection</i> .
Incident Alert Section	Select <i>All</i> , <i>Interaction Events Only</i> , <i>IPS events only</i> , or <i>Web filter events only</i> .
Binary Infection	This options is available when the <i>Alert Type</i> is <i>Interaction</i> or <i>Infection</i> . Select <i>Yes</i> to be alerted when an attacker drops or downloads suspicious files into decoys.
Attacker IP	Enter the attacker IP address
Victim Decoy Service	Enter one or more decoy service port numbers.
Recipients	Enter one or more receiver email addresses.

Custom Alert Rule ×

Enabled ☐

Name *
Please enter a rule name.

Alert Severity * Low Medium High Critical

Alert Type * Connection Reconnaissance Interaction Infection

Incident Alert Section * All Interaction Events Only IPS events only Web filter events only

Binary Infection * Yes × ✓

Attacker IP (0) +

Victim Decoy Service (0) +

Recipients (0) * +
Recipients list cannot be empty.

Cancel Save

4. Click Save.

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.

SNMP has two parts:

- The SNMP agent or the device that is sending traps.
- The SNMP manager that monitors those traps.

The SNMP communities on the monitored FortiDeceptor are configured in the SNMP page.

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</i> , <i>Queries</i> , <i>Traps</i> , <i>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</i> , <i>Security Level</i> , <i>Notification Host</i> , and <i>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, Queries v2c	Port number and if it is enabled. Enable queries for each SNMP version that FortiDeceptor uses.
Traps v1, Traps v2c	Local port number, remote port number, and if it is enabled. 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. Go to *System > SNMP*.
2. Scroll down to *FortiDeceptor SNMP MIB* and click one of the following links:
 - *Download FortiDeceptor MIB File*
 - *Download Fortinet Core MIB File*

FortiGuard

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiDeceptor system. The FDN is a worldwide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your

FortiDeceptor system on a regular basis so that your FortiDeceptor system is protected against the latest threats.

The FortiGuard services available on the FortiDeceptor system include:

Service	Description
Antivirus	Malware scanning against files that get captured by the decoys.
IDS engines	<ul style="list-style-type: none"> Scanning the traffic between the threat actor and the decoys to detect network attacks Contain the industrial signature pack for the ICS network .
Web filtering engine	Databases and look-ups against access from the decoy to the internet.
Anti-Recon and Anti-Exploit Service	The Anti-Reconnaissance and Anti-Exploit Service (ARAE) service is available on FortiDeceptor and is responsible for tracking hackers' activities on decoys with real-time alerts. Similar to how FortiSandbox traces malware behavior activities, ARAE will record malicious activities such as files extracted, intrusions activities, planted malware, and web sites visited. ARAEs goal is to Deceive, Expose and Eliminate threats.

To configure FortiGuard updates:

1. Go to *System > FortiGuard*.
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 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. The default port on FDN server is 443 and can be changed to 53 or 8888.

Use Proxy	Select to use a proxy. Configure the <i>Proxy Type</i> (<i>HTTP Connect</i> , <i>SOCKS v4</i> , or <i>SOCKS v5</i>), <i>Server Name/IP</i> , <i>Port</i> , <i>Proxy Username</i> , and <i>Proxy Password</i> .
FortiGuard Web Filter Settings	
Use override server address for web filtering query	<p>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.</p> <p>By default, the closest web filtering server according to the unit's time zone is used.</p> <p>The default port on FDN server is 443.</p>
Use Proxy	Select to use a proxy. Configure the <i>Proxy Type</i> (<i>HTTP Connect</i> , <i>SOCKS v4</i> , or <i>SOCKS v5</i>), <i>Server Name/IP</i> , <i>Port</i> , <i>Proxy Username</i> , and <i>Proxy Password</i> .
VM Image Download Proxy Settings	
Use Proxy	Select to use a proxy. Configure the <i>Proxy Type</i> (<i>HTTP Connect</i> , <i>SOCKS v4</i> , or <i>SOCKS v5</i>), <i>Server Name/IP</i> , <i>Port</i> , <i>Proxy Username</i> , and <i>Proxy Password</i> .

- Click *Connect FDN Now* to connect the override FDN server/proxy.
 - Click *Test Connection* to test your connection.
 - Click *Apply* to apply your changes.

FDC License

FortiDeceptor is a subscription-based model that calculates the amount of Network VLANs the system can connect to. Single Class C (/24) will consume 1 VLAN, while other network classes with /23 and below will consume 2 VLANs (max).

To upload a FortiDeceptor license:

- Go to *System > FDC License*.
- Click *License Upload*. The *Firmware License Upload* page opens.
- Click *Browse* and navigate to the license file on your computer.
- Click *Submit*.



FortiDeceptor will reboot after the license file is installed.

To input the confirmation ID for Windows:

- Go to *System > FDC License*.
- Click *Input Confirmation ID for Windows*. The *Input Confirmation ID for Windows* dialog opens.
- From the *Windows Key* dropdown, select a Windows key.
- In the *Confirmation ID* field, enter the confirmation ID.

5. Click OK.

Module Name	License Details	Module version	Status
FDC Platform	FDCVM	4.0.0	Active
Network Segment Coverage			Active
Deception Lure			Active



Do not reboot FortiDeceptor until the activation is complete.

Settings

Go to *System > Settings* to configure the idle timeout for the administrator account.

To configure idle timeout:

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

To reset all widgets:

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

Click the *Reset* button to revert the *Dashboard* to the default settings. This remove any widgets you added to the Dashboard and restore the widget settings.

Login Disclaimer

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

If enabled, the disclaimer appears when a user tries to log into the unit.

Table Customization

You can customize the page layout for the *Incidents* and *Events* pages.

To customize the columns available for Incidents or Events:

- In the *Incident Columns* pane:
 - To show a column: Drag and drop the headers from the *Available Column Headers* to *Customized Column Headers and Orders*.
 - To hide a column: Drag and drop the headers from the *Customized Column Headers and Orders* to *Available Column Headers*.
 - To change the column order: Drag and drop the position of the headers in *Customized Column Headers and Orders*.
- In the *Table Settings* pane, configure the table size and view.

Page Size Enter the number of incidents to display per page when *View Type > Pagination* is selected.

View Type Select *Pagination*, *Infinite Scroll* or *Both*.

- Click *Apply*.

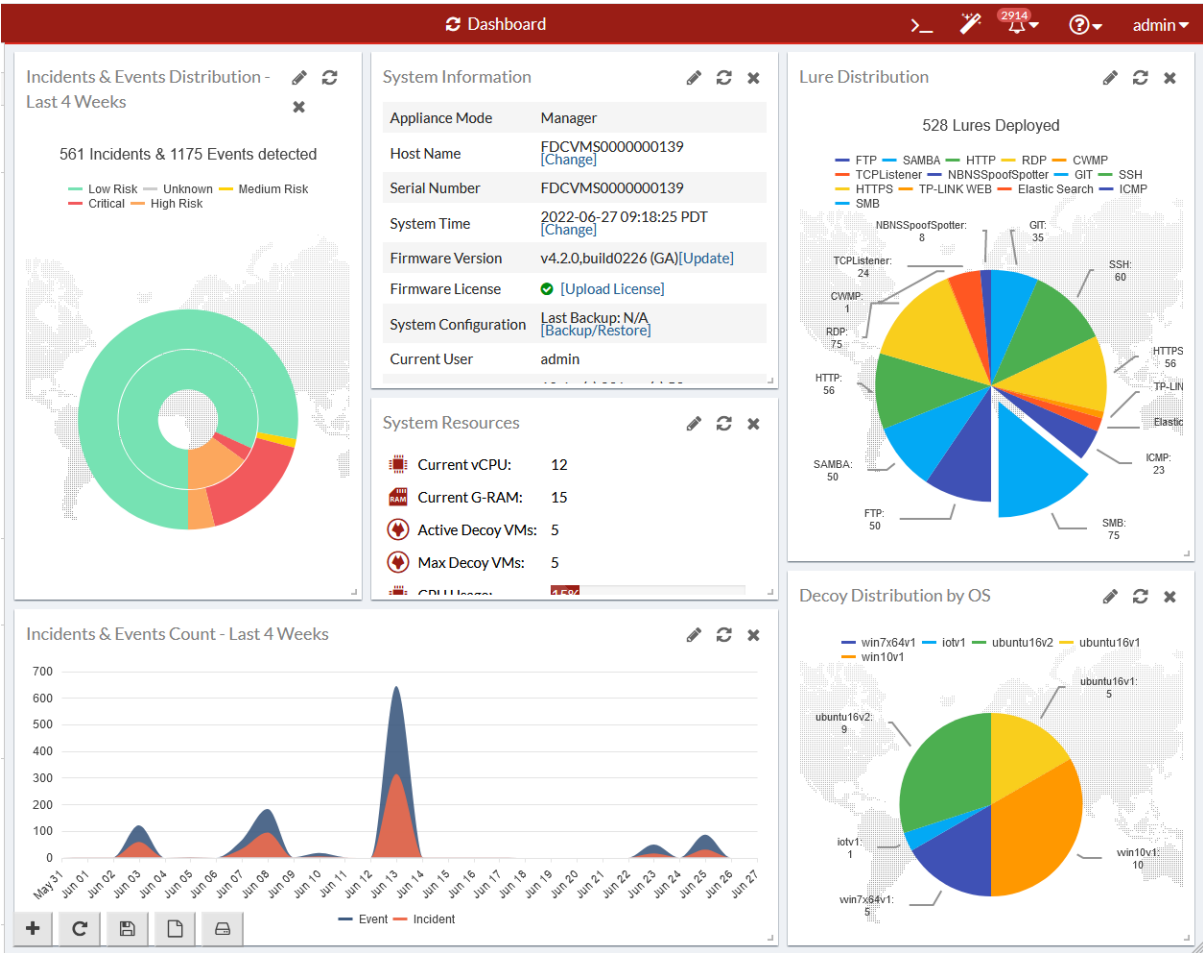


You may need to refresh the page to see your changes.

System Settings

Dashboard

The *Dashboard* contains system information widgets that allow you to monitor the performance of the FortiDeceptor. The Dashboard also includes widgets that provide overview incidents and events in the last 24 hours to 7 days. You can customize the Dashboard by adding and removing widgets.



The default Dashboard view displays the following widgets:

Widget	Description
Incidents & Events Distribution	Information about the number of incidents and events, and their level of severity. You can configure the time period to display the Last 24 hours, 7 Days or 4 Weeks.

Widget	Description
System Information	Basic information about the FortiDeceptor system, such as the serial number, system up time, and license status information.
Lure Distribution	Number of decoys deployed with the chart showing the type of service such as SSH, SAMBA, SMB, SCADA, RDP, HTTP, HTTPS, IIS (HTTP, HTTPS), or MSSQL.
System Resources	Hardware requirements benchmark for FortiDeceptor Virtual appliances only. This widget provides real-time guidelines for system performance and increasing vCPU & RAM resources during deployment and ongoing maintenance. The widget also provides the overall Real-time usage status of the CPU and memory.
Incidents & Events Count	Number of events occurring each day. You can configure the time period to display the Last 24 hours, 7 Days or 4 Weeks.
Decoy Distribution by OS	Number of decoys with a chart showing the OS such as Windows or Ubuntu.

The following widgets are available to add to the Dashboard:

Widget	Description
Top Critical Logs	The top logs that are classified as <i>Critical</i> .
License Information	The list of VM license keys and their expiry dates.
Disk Monitor	For hardware models: <ul style="list-style-type: none"> The RAID level and status, disk usage, and disk management information. For VM models: <ul style="list-style-type: none"> Disk usage.
Incidents Distribution by Service	Information about the number and types of incidents, such as SMB, HTTP, TCP, and so on.
Top 10 Attackers by Incidents	The top 10 attackers by the number of incidents. You can configure the time period to display the Last 24 hours, 7 Days or 4 Weeks.
Top 10 Attackers by Events	The top 10 attackers by the number of events. You can configure the time period to display the Last 24 hours, 7 Days or 4 Weeks.
Global Incidents Distribution	Displays the number of Attackers by country on a global map.
Top 10 IPS attacks	Displays the top 10 IPS attackers by the number of events. You can configure the time period to display the Last 24 hours, 7 Days or 4 Weeks.





For information about adding widgets, see [Customizing the dashboard on page 108](#).

Customizing the dashboard

You can select which widgets to display on the Dashboard and where they are located on the page. You can also configure the time period and refresh interval for individual widgets.

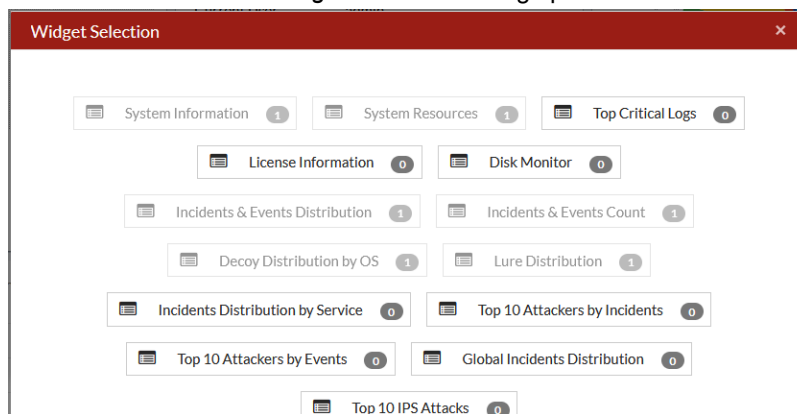
Dashboard toolbar

The dashboard toolbar is located near the bottom of the pages. You can perform the following tasks:

	Click to add a widget to the dashboard.
	Click to restore the dashboard settings. This will remove any widgets you added to Dashboard and revert any changes you made to the widget settings.
	Click to save the current Dashboard view.
	Click to save the current layout as the default Dashboard view.

To add a widget to the Dashboard:




1. Click the Add icon. The *Widget Selection* dialog opens.



2. Select the widget you want to add to the Dashboard.

Widget toolbar

The widget tools are located in the widget header.

	Click to configure the widget Time Period and Refresh Interval. The widgets setting will vary depending on the widget.
	Click to refresh the widget data.
	Click to remove a widget from the Dashboard.

System Information

The *System Information* widget displays information about the FortiDeceptor device. Use this widget to quickly configure the device host name, update the firmware version, upload a license or back up the system configuration.

This widget displays the following information and options.

Appliance Mode	The mode of the appliance: Manager, Client, or standalone.
Appliance CM Status	Optional for client appliance. Display the status in Central Management.
Appliance CM Live Time	Optional for client appliance. The last live timestamp in Central Management.
Host Name	The name assigned to this FortiDeceptor unit. Click <i>Change</i> to edit the FortiDeceptor host name.
Serial Number	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. Click <i>Change</i> to configure the system time.
Firmware Version	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 . Click <i>Update</i> or <i>UPDATE AVAILABLE</i> and select the firmware image to load from the local hard disk or network volume.
Firmware License	To load a firmware license, click <i>Upload License</i> and select a license file.
System Configuration	Date and time of the last system configuration backup. Click <i>Backup/Restore</i> to go to the <i>System Recovery</i> page.
Current User	The administrator that is currently logged into the system.
Uptime	Duration that the FortiDeceptor unit has been running since it booted up.
Deception OS	Deception OS license activation and initialization status. Displays a green check mark if the Deception OS is activated and initialized. Displays a <i>Caution</i> icon if the Deception OS is initializing or having issues. Hover the mouse pointer on the status icon to view detailed information. For more information, see <i>Log > All Events</i> . To go to <i>Deception > Deception OS</i> to see the images available on FortiDeceptor, click <i>Update</i> or <i>UPDATE AVAILABLE</i> . After purchase, download the license file from the Fortinet Customer Service & Support portal . Then click <i>Upload License</i> to select the license file. The system reboots and activates the newly-installed Deception OS.
FDN Download Server	Shows if the FDN download server is accessible. When the FDN download server is inaccessible, no update packages are downloaded.
Web Filtering Server	Shows if the web filtering query server is accessible.
Antivirus DB Contract	Brief information about this contract.

Antivirus Engine Contract	Brief information about this contract.
IDS Engine/DB Contract	Brief information about this contract.
Web Filtering Contract	Brief information about this contract.
ARAE Engine Contract	Brief information about this contract.
Custom VM Contract	Brief information about this contract. This is displayed when FortiDeceptor is running a v1 license.
SSL VPN Contract	Brief information about this contract. These is displayed when FortiDeceptor is running a v4 license.

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.

Decoy Distribution by OS

This widget displays the following information in a pie chart.

Ubuntu	Number and percentage of Ubuntu Decoy VMs.
Windows	Number and percentage of Windows Decoy VMs.
SCADA V3	Number and percentage of SCADA Decoy VMs.
SSLVPN	Number and percentage of SSLVPN Decoy VMs.
Medical	Number and percentage of Medical Decoy VMs.
ERP	Number and percentage of ERP Decoy VMs.
POS	Number and percentage of POS Decoy VMs.
IoT	Number and percentage of IoT Decoy VMs.
SAP	Number and percentage of SAP Decoy VMs.

Hover over the pie chart to see the percentage. Click the pie chart to split out a Decoy from the pie chart.

Lure Distribution

This widget displays the number of lures deployed with the following information in a pie chart.

SSH	Number and percentage of decoy images using SSH service.
SAMBA	Number and percentage of decoy images using SAMBA service.
SMB	Number and percentage of decoy images using SMB service.
TCPLISTENER	Number and percentage of decoy images using TCPLISTENER service.
NBNSSpoofSpotter	Number and percentage of decoy images using NetBios Name Service Spoof Spotter .
RDP	Number and percentage of decoy images using RDP service.
HTTP	Number and percentage of decoy images using HTTP service.
FTP	Number and percentage of decoy images using FTP service.
TFTP	Number and percentage of decoy images using TFTP service.
SNMP	Number and percentage of decoy images using SNMP service.
MODBUS	Number and percentage of decoy images using MODBUS service.
S7COMM	Number and percentage of decoy images using S7COMM service.
BACNET	Number and percentage of decoy images using BACNET service.
IPMI	Number and percentage of decoy images using IPMI service.
TRICONEX	Number and percentage of decoy images using TRICONEX service.
Guardian-AST	Number and percentage of decoy images using Guardian-AST service.
IEC104	Number and percentage of decoy images using IEC104 service.
MSSQL	Number and percentage of decoy images using MSSQL service.
IIS	Number and percentage of decoy images using IIS service.
GIT	Number and percentage of decoy images using GIT service.
ENIP	Number and percentage of decoy images using ENIP service.
Infusion Pump Telnet	Number and percentage of decoy images using Infusion Pump Telnet service.
Infusion Pump FTP	Number and percentage of decoy images using Infusion Pump Ftp service.
POS-WEB	Number and percentage of decoy images using POS-WEB service.
ERP-WEB	Number and percentage of decoy images using ERP-WEB service.
PACS	Number and percentage of decoy images using PACS service.
PACS-WEB	Number and percentage of decoy images using PACS-WEB service.
DICOM	Number and percentage of decoy images using DICOM service.
SSLVPN	Number and percentage of decoy images using SSLVPN service.

DNP3	Number and percentage of decoy images using DNP3 service.
Telnet	Number and percentage of decoy images using Cisco-Telnet service.
Printer-WEB	Number and percentage of decoy images using HP Printer-WEB service.
JETDIRECT	Number and percentage of decoy images using HP Printer-JETDIRECT service.
IP CAMERA-WEB	Number and percentage of decoy images using IP CAMERA-WEB service.
UPNP	Number and percentage of decoy images using IP CAMERA-UPNP service.
RTSP	Number and percentage of decoy images using IP CAMERA-RTSP service.
SAP WEB	Number and percentage of decoy images using SAP WEB service.
SAP ROUTER	Number and percentage of decoy images using SAP ROUTER service.
SAP DISPATCHER	Number and percentage of decoy images using SAP DISPATCHER service.
TP-LINK WEB	Number and percentage of decoy images using TP-LINK WEB service.
CWMP	Number and percentage of decoy images using CWMP service.

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

Top Critical Logs

This widget displays recent critical logs including the time and a brief description of the event.

Click the edit icon to change the refresh interval and top count.

Disk Monitor

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

This widget displays the following information.

Summary	Disk summary information including RAID level and status.
RAID Level	The RAID level.
Disk Status	The disk status.
Disk Usage	The current level of disk usage.
Disk Number	The disk number.
Disk Size	The disk size.

Basic System Settings

Change the GUI idle timeout

By default, the GUI disconnects administrative sessions if there is no activity for five minutes.

To change the idle timeout length:

1. Go to *System > Settings*.
 2. Change the *Idle timeout* minutes (1 to 480 minutes).
 3. Click *OK*.
- The setting takes affect after you log out and log back in.



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

Log out of the unit

To log out of the unit:

1. In the FortiDeceptor banner at the top-right, click the user name and select *Logout*.

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

Update FortiDeceptor firmware

A best practice is to stay up-to-date on patch releases for currently deployed 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.

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. See, [Back up or restore the system configuration on page 114](#).
- Plan a maintenance window for the firmware update. If possible, consider setting up a test environment to check that the update does not negatively impact your network.

To update the FortiDeceptor firmware:

1. Go to *Dashboard > System Information > Firmware Version*.
2. In the *System Information* widget beside *Firmware Version*, click *Update* or *UPDATE AVAILABLE*.

3. Click *Choose File* and locate the previously downloaded firmware image on your management computer; then click *Submit* to start the upgrade.
Alternatively, in the *AVAILABLE FIRMWARE* pane *Install* column, click the download icon beside the firmware release you want. The system upgrades and restarts automatically.

When the update is complete, test your FortiDeceptor device to ensure that the update was successful.

Reboot or shut down the unit

To avoid potential configuration or hardware problems, always use the GUI or CLI to reboot or shut down FortiDeceptor.

To reboot the FortiDeceptor unit:

1. Go to *Dashboard > System Resources*.
2. Click *Reboot*.
3. Enter a reason for the reboot in the *Reason* field.
4. Click *OK*.

After reboot, the FortiDeceptor VM initialization requires approximately 30 minutes. The Decoy VM icon in the *System Information* widget shows a warning sign until the process completes.

When FortiDeceptor boots or reboots, the following critical event log message is normal:

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 upgrading FortiDeceptor to a new firmware version, the system might clean up data and a *Database is not ready* message displays. The clean up time depends on the size of historical data.

To shut down the FortiDeceptor unit:

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

Back up or restore the system configuration

We recommend that your regular maintenance includes system backups. Always backup before upgrading firmware or making major system configuration changes. Save configuration backups to a management computer in case 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. Click *Backup/Restore*.

3. Click *Click here* to save your backup file.

To restore the FortiDeceptor configuration:

1. Go to *Dashboard > System Information > System Configuration*.
2. Click *Backup/Restore*.
3. Click *Choose File* and locate the backup file on your management computer.
4. Click *Restore* to load the backup file.
5. Click *OK*.

When the system configuration restore process completes, the login page appears.



When you do a system restore, all configurations are replaced with the backup data. The system reboots automatically to complete the restore. Only the backup configuration file from the previous or the current release is supported.

Network

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

Interfaces

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

This page displays the following information and options:

Interface	The interface name and description. Failover IP is listed under this field with the descriptor: <i>(cluster external port)</i> .
port1 (administration port)	Port1 is hard-coded as the administration interface. You can enable or disable HTTP, SSH, and Telnet access rights on port1. HTTPS is enabled by default and cannot be disabled. You can use port1 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: <ul style="list-style-type: none"> • Interface up

	<ul style="list-style-type: none"> • Interface 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 enable HTTP, SSH, and Telnet access on port1.
Edit	Select the interface and click <i>Edit</i> in the toolbar to edit the interface.

To edit an interface:

1. Select the *IPv4* or *IPv6* address of an interface name and click *Edit* in the toolbar.
2. Edit the *IP Address / Netmask*. The Confirmation dialog opens.
3. (Optional) Change the *Interface Status*.
4. In the *IP Address / Netmask* pane, update the IPv4 and IPv6 address.
5. Click *OK*.

To edit administrative access:

1. Select *port1 (administration port)* and click *Edit* in the toolbar.
2. Edit the *Access Rights*.
HTTPS is enabled by default. You can also enable HTTP, SSH, and Telnet support.
3. If necessary, edit the *IP Address / Netmask*.
4. Click *OK*.

DNS Configuration

You can configure the primary and secondary DNS server addresses in *Network > System DNS*.

System Routing

Use the *Network > System Routing* page to manage static routes of your FortiDeceptor device.

The following options are available:

Create New	Create a new static route.
Edit	Edit the selected static route.
Delete	Delete the selected static route.

The following information is displayed:

IP/Mask	IP address and subnet mask.
Gateway	Gateway IP address.
Device	The interface associated with the static route.

To create a new static route:

1. Click *Create New*.
2. Enter the *Destination IP* address, *Mask*, and *Gateway*.



You can enter the *Destination IP/Mask* in the format 192.168.1.2/255.255.255.0, 192.168.1.2/24, or fe80:0:0:0:0:0:c0a8:1fe.

3. Select a *Device* (or interface).
4. Click *OK*.

To edit a static route:

1. Select a Static Route
2. Click *Edit*.
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 *Delete*.
3. Confirm the deletion.

System Log

Use the *Log* pages to view and download FortiDeceptor system logs. You can put logs locally on FortiDeceptor or on a remote log server.

Logging Levels

FortiDeceptor log level 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.
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 for debugging.	Launching job for file. jobid=2726271637747836543 filename=log md5=ebe5ae2bec3b653c2970e8cec9f5f1d9 sha1=06ea6108d02513f0d278ecc8d443df86dac2885b sha256=d678da5fb9ea3ee20af779a4ae13c402585 ebb070edcf20091cb20509000f74b

Raw logs

You can download and save raw logs to the management computer. Raw logs are saved as a text file with the extension *.log.gz*.

To download raw logs:

1. Go to *Log > All Events* and select a log.
2. In the toolbar, click *Download Log*.

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

Log > All Events shows all logs.

The following options are available.

Download Log	Download the raw log file to the management computer.
History Logs	Enable to include historical logs in Log Search.
Refresh	Refresh the log message list.
Filter	Click <i>Filter</i> to add search filters. You can select different categories to search the logs. Search is not case sensitive.

The following information is displayed.

#	Log number.
Date/Time	Date and time the log message was created.
Level	Level of the log message. For logging levels, see Logging Levels on page 118 .
User	The user to which the log message relates. User can be a specific user or system.
Message	Detailed log message.
Appliance	The appliance name to which the log belongs.

Log Servers

You can send FortiDeceptor logs to a remote syslog server, FortiAnalyzer, or common event type (CEF) server. In *Log > Log Servers*, you can create new remote log servers, and edit and delete remote log servers. You can configure up to 30 remote log server entries.

The following options are available:

Create New	Create a log server entry.
Edit	Edit the selected log server entry.
Delete	Delete the selected log server entry.

This page displays the following information:

Name	Name of the server entry.
Type	Server type: syslog or CEF.
Log Server Address	Log server address.
Port	Log server port number.
Status	Log server status, <i>Enabled</i> or <i>Disabled</i> .

To create a server entry:

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

Name	Name of the new server entry.
Type	Select <i>Syslog Protocol</i> , <i>FortiAnalyzer</i> , or <i>Common Event Format</i> .
Log Server Address	Log server IP address or FQDN.
Port	Port number. The default port is 514.
Status	Enable or disable sending logs to the server.
Log Level	Select the logging levels to forward to the log server. For logging levels, see Logging Levels on page 118 .

4. Click *OK*.

To edit or delete a log server

1. Go to *Log > Log Servers*.
2. Select an entry and click *Edit* or *Delete*.

Deploying FortiDeceptor in offline or air-gapped networks

This section shows how to deploy FortiDeceptor in an offline or air-gapped network with no internet access, using the following procedures.

- [Applying the license in an offline or air-gapped network on page 122](#)
- [Importing deception VMs in an offline or air-gapped network on page 124](#)
- [Importing firmware in an offline or air-gapped network on page 126](#)
- [Importing an FDS package via FDC GUI in an offline or air-gapped network on page 126](#)
- [Importing FDS package and license file via FortiManager in an offline or air-gapped network on page 127](#)

FortiDeceptor uses deception VMs to deploy decoys across the network. Deploying FortiDeceptor VMs in a closed network requires downloading the required images directly from the FortiDeceptor VM external repository and manually uploading the deception VMs. For information about downloading the deception VMs, see [Importing deception VMs in an offline or air-gapped network on page 124](#)

You can also use the *Deception > Deception OS* page or the `fw-upgrade` CLI command to download and import packages.

Because FortiDeceptor also uses FDS services (IPS/AV/WEB) in offline and air-gapped networks, you must also import these packages.

Deception VM security

You can download deception VMs via the HTTPS protocol. Each image is compressed, encrypted, and packed by the FDC tool separately. The metafile describes the MD5 of each VM image.

The security layers that protect deception images are:

- Download via HTTPS.
- Deception VMs do not have any Fortinet proprietary software.
- We provide the file's MD5 so that you can confirm the MD5 checksum for the downloaded files.
- FortiDeceptor always verifies the VM image by encryption and multiple layer checksum inside the package before installing it.

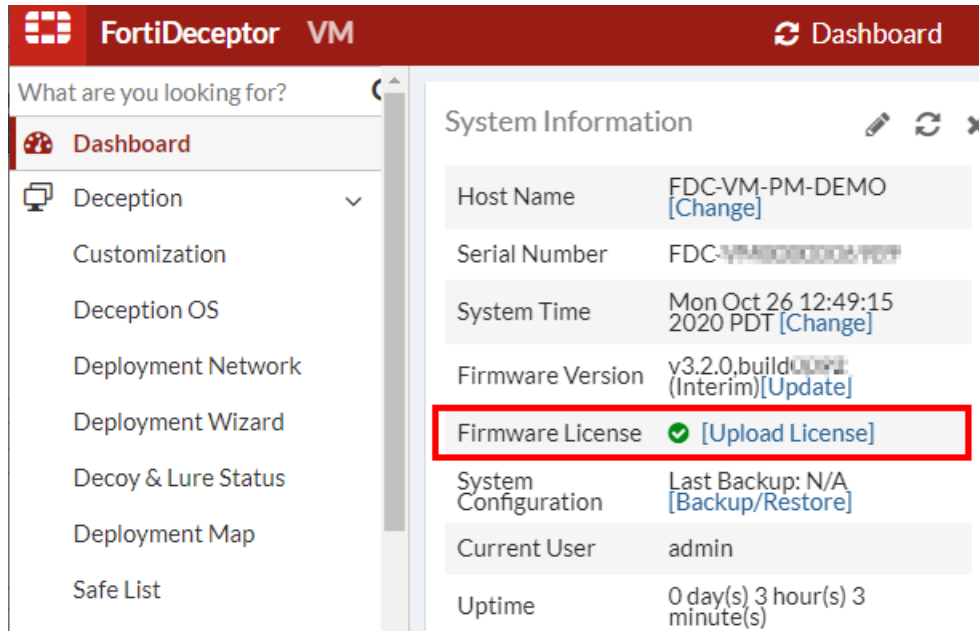
Applying the license in an offline or air-gapped network

To download the FortiDeceptor license file from the Fortinet support site:

1. Log into [Customer Service and Support](#). The Asset Portal opens.
2. Go to *My Assets* and locate the device then click the *Serial Number*. The product details page opens.
3. In the *License & Key* widget, click *Get The License File* and save it to the local disk.

To upload the license file to FortiDeceptor:

1. Log into FortiDeceptor.
2. Configure the management IP address on port1.
3. In the *Dashboard System Information* widget, click *Upload License* beside *Firmware License*.



4. Locate the license and click *Submit*.

FortiDeceptor extracts the serial number, IP addresses, decoy keys, expiry date; and then performs the following verifications.

- Verify the expiration time of the license.
- Verify that the embedded management IP address is the same as the current management IP address. You can view the IP address in the *Product Information* widget in the product details page.
- Verify the expiration time of the decoys keys if the keys are subscription type.

If all the verifications pass, the unit is ready to import deception images.



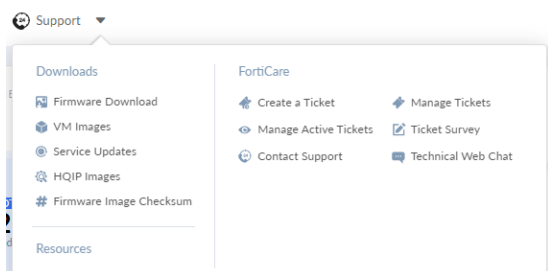
- FortiDeceptor decoy WCF lookup (any URLs visiting from decoys) are **not** categorized.
 - You can use FortiManager to resolve this. Because FortiDeceptor supports override FDS server, you can enter the FortiManager IP address there.
- Subscription-based decoys, that is, SSL VPN Windows customization, is in the `*.lic` file from the support site, which you can run offline.
- FortiDeceptor Custom Decoy Subscription Service includes:
 - FC-10-FDCVM-292-02-DD (for VM).
 - FC-10-FDC1K-292-02-DD (for HW).

Importing deception VMs in an offline or air-gapped network

This topic shows how to download and import deception VMs in an offline or air-gapped network.

To download and import a deception VM:

1. Log into [Customer Service and Support](#). The *Asset Portal* opens.
2. In the banner, click *Support > Downloads > Firmware Download*.



3. In the *Select Product* dropdown list, select FortiDeceptor and then click *Download*.

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiDeceptor ▼

Release Notes Download

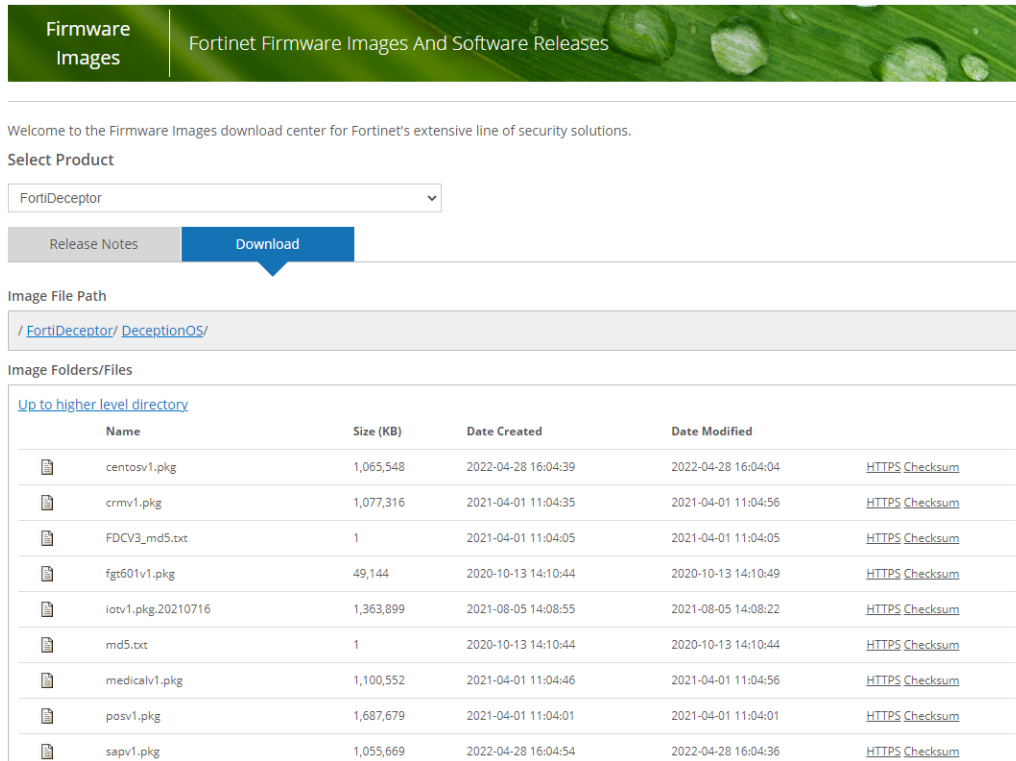
Image File Path

/ FortiDeceptor/

Image Folders/Files

	Name	Size (KB)	Date Created	Date Modified
📁	DeceptionOS	Directory	2020-10-13 14:10:39	2022-04-28 16:04:39
📁	v3.00	Directory	2019-12-24 08:12:03	2022-06-20 12:06:08
📁	v4.00	Directory	2021-07-30 13:07:35	2022-04-28 17:04:19

- Click *Deception OS* to see the list of deception OS VM files.



Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiDeceptor

Release Notes Download

Image File Path

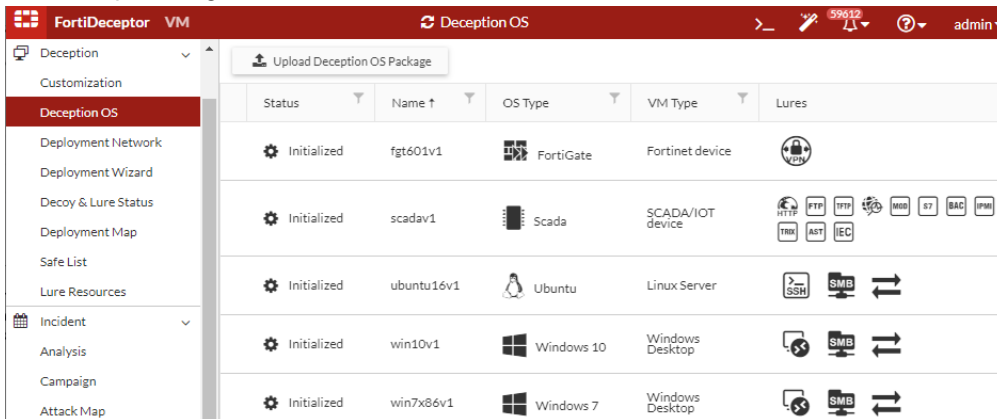
/ FortiDeceptor/ DeceptionOS/

Image Folders/Files

[Up to higher level directory](#)

Name	Size (KB)	Date Created	Date Modified	
centosv1.pkg	1,065,548	2022-04-28 16:04:39	2022-04-28 16:04:04	HTTPS Checksum
crmv1.pkg	1,077,316	2021-04-01 11:04:35	2021-04-01 11:04:56	HTTPS Checksum
FDCV3_md5.txt	1	2021-04-01 11:04:05	2021-04-01 11:04:05	HTTPS Checksum
fgt601v1.pkg	49,144	2020-10-13 14:10:44	2020-10-13 14:10:49	HTTPS Checksum
iotv1.pkg.20210716	1,363,899	2021-08-05 14:08:55	2021-08-05 14:08:22	HTTPS Checksum
md5.txt	1	2020-10-13 14:10:44	2020-10-13 14:10:44	HTTPS Checksum
medicalv1.pkg	1,100,552	2021-04-01 11:04:46	2021-04-01 11:04:56	HTTPS Checksum
posv1.pkg	1,687,679	2021-04-01 11:04:01	2021-04-01 11:04:01	HTTPS Checksum
sapv1.pkg	1,055,669	2022-04-28 16:04:54	2022-04-28 16:04:36	HTTPS Checksum

- Download all the deception OS VM .pkg files in this directory.
- Copy the downloaded files to the offline or air-gapped network.
- In FortiDeceptor, go to *Deception > Deception OS* and click *Upload Deception OS Package* to import the FortiDeceptor images.



FortiDeceptor VM Deception OS

Upload Deception OS Package

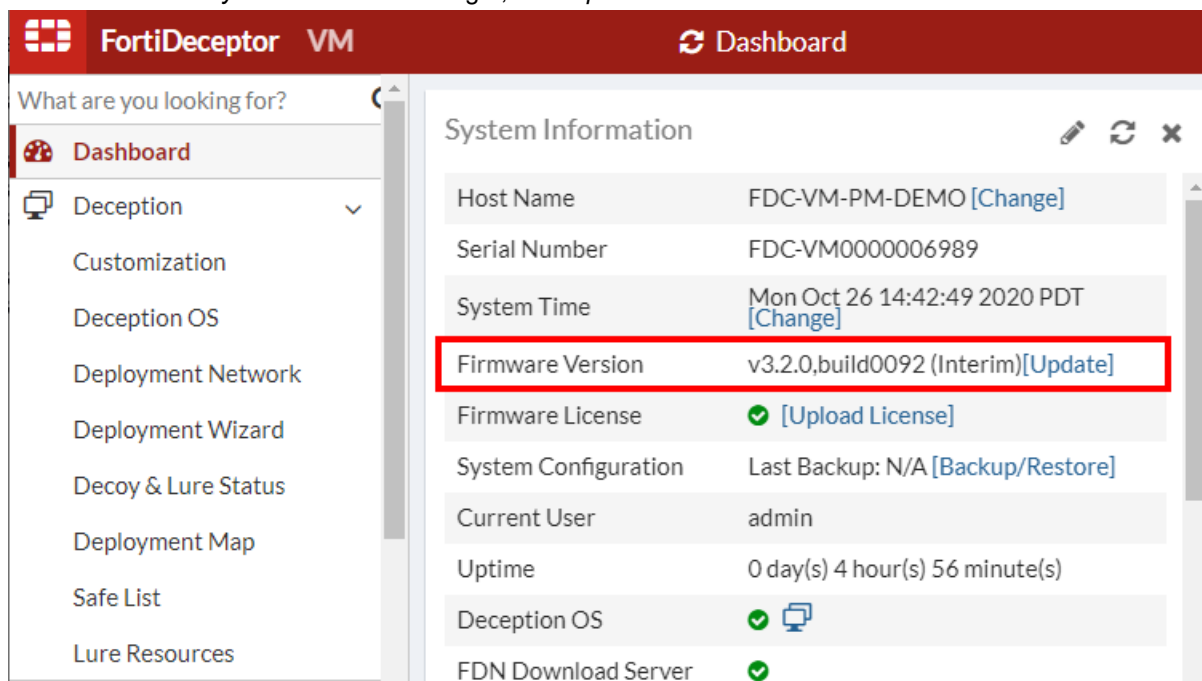
Status	Name	OS Type	VM Type	Lures
Initialized	fgt601v1	FortiGate	Fortinet device	VPN
Initialized	scadav1	Scada	SCADA/IOT device	FTP, TFTP, SSH, RDP, SMB, ST, BAC, IPsec, TRIP, AST, IEC
Initialized	ubuntu16v1	Ubuntu	Linux Server	SSH, SMB, RDP
Initialized	win10v1	Windows 10	Windows Desktop	SMB, RDP
Initialized	win7x86v1	Windows 7	Windows Desktop	SMB, RDP

FortiDeceptor imports the images, verifies image integrity and other security layers, confirms that the images are the originals, and then initializes them. After initialization the *Deception OS* window *Status* column shows these images as *Initialized*.

Importing firmware in an offline or air-gapped network

To download and import FortiDeceptor firmware:

1. Log into [Customer Service and Support](#).
2. Go to *Download > Firmware Images*.
3. In the *Select Product* dropdown list, select FortiDeceptor and then click *Download*.
4. Click the version you want.
5. Download the FortiDeceptor firmware file (the `.out` file).
6. Copy the downloaded file to the offline or air-gapped network.
7. Log into FortiDeceptor.
8. In the *Dashboard System Information* widget, click *Update* beside *Firmware Version*.



9. Click *Choose file*, then locate the firmware file and click *Submit*.
FortiDeceptor reboots after the update.

Importing an FDS package via FDC GUI in an offline or air-gapped network

To download and import a FortiDeceptor FDS package:

1. Log into [Customer Service and Support](#).
2. Go to *Download > FortiGuard Service Updates*.
3. Locate and download the FortiDeceptor FDS package (the `.pkg` file).
4. Copy the downloaded file to the offline or air-gapped network.

5. In FortiDeceptor, go to *System > FortiGuard*; then beside *Upload Package File*, click *Choose File* and locate the FDS package.

The screenshot shows the FortiDeceptor VM interface with the FortiGuard tab selected. On the left is a navigation menu with options: Administrators, Admin Profiles, Certificates, LDAP Servers, RADIUS Servers, Mail Server, SNMP, and FortiGuard (highlighted). The main area displays a table of installed modules:

Module Name	Current Version	Release Time	Last Update Time
AntiVirus Scanner	00006.00009	2018-05-01 17:45:00	2020-10-26 14:15:43
AntiVirus Extended Signature	00000.00000	Unknown	2020-10-26 14:15:43
AntiVirus Active Signature	00008.00777	2016-11-05 00:23:00	2020-10-26 14:15:43
AntiVirus Extreme Signature	00000.00000	Unknown	2020-10-26 14:15:43
IDS Engine	00004.00025	2018-10-12 16:54:00	2020-10-26 14:15:43
IDS Signature	00015.00853	2020-05-29 12:03:00	2020-10-26 14:15:43
Anti-Reconnaissance & Anti-Exploit Engine	01000.00011	2020-10-26 09:59:00	2020-10-26 14:15:43

Below the table, the 'Upload Package File:' section is highlighted with a red box. It contains a 'Choose File' button and the text 'No file chosen'. A 'Submit' button is located to the right of this section.

6. Click *Submit*.
Ensure you receive a confirmation that installation is successful.

Importing FDS package and license file via FortiManager in an offline or air-gapped network

This topic shows how to download and import a FortiDeceptor license in an offline or air-gapped network using FortiManager.

When FortiManager is operating in a closed network, you can create a support ticket to request account entitlement files from Fortinet Customer Service & Support for devices, and then upload the files to FortiGuard. This allows devices in the closed network to check licenses.

To request the FortiDeceptor entitlement license file for FortiManager:

1. Log into [Customer Service and Support](#).
2. Go to *Assistance > Create a Ticket*.
3. Expand *Customer Service* and click *Submit Ticket*.
4. Enter the required information.
 - For *Subject*, enter *Entitlement file*.
 - For *Category*, select *CS Contract/License*.
5. Complete and submit the ticket.
6. When you receive the entitlement file via email, download it to your computer.

Without a connection to a FortiGuard server, update packages and licenses must be manually downloaded from support, and then uploaded to FortiManager.

To upload the FortiDeceptor entitlement license file to FortiManager:

1. In FortiManager, go to *FortiGuard > Settings*.
2. Set *Enable Communication with FortiGuard Server* to *OFF* so that you can configure FortiManager as a local FDS server.

3. In the *Upload Options for FortiGate/FortiMail* section, click *Upload* besides *Service License*.

FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server

Enable Antivirus and IPS Service

FortiGate	<input type="checkbox"/> All v4	<input type="checkbox"/> 5.0	<input type="checkbox"/> 5.2	<input type="checkbox"/> 5.4	<input type="checkbox"/> 5.6
FortiClient	<input type="checkbox"/> All v4	<input type="checkbox"/> 5.0	<input type="checkbox"/> 5.2	<input type="checkbox"/> 5.4	
FortiAnalyzer	<input type="checkbox"/> All v4	<input checked="" type="checkbox"/> 5.0	<input checked="" type="checkbox"/> 5.2	<input checked="" type="checkbox"/> 5.4	
FortiMail	<input type="checkbox"/> All v4	<input type="checkbox"/> All v5			

Enable Web Filter Service

Enable Email Filter Service

Upload Options for FortiGate/FortiMail

Antivirus/IPS Packages	<input type="button" value="Upload"/>
Web Filter Database	<input type="button" value="Upload"/>
Email Filter Database	<input type="button" value="Upload"/>
Service License	<input type="button" value="Upload"/>

Upload Options for FortiClient

Antivirus/IPS Packages	<input type="button" value="Upload"/>
------------------------	---------------------------------------

Enable Communication with FortiGuard Server

Toggle *OFF* to disable communication with FortiGuard servers.

Enable AntiVirus and IPS Service

Toggle *ON* to enable antivirus and intrusion protection service. When on, select the versions of FortiGate, FortiClient, FortiAnalyzer, and FortiMail to download updates.

Enable Web Filter Service

Toggle *ON* to enable web filter services. When uploaded to FortiManager, the web filter database displays.

AntiVirus/IPS Packages

Click *Upload* to upload antivirus and IPS packages you downloaded from the Customer Service & Support portal.

Web Filter Database

Click *Upload* to upload the web filter database you downloaded from the Customer Service & Support portal. As the database can be large, uploading with CLI is recommended.

Service License

Click *Upload* to import the FortiGate license. You can get a license file from support by requesting your account entitlement for the device.

To configure FortiDeceptor to use FortiManager for FortiGuard services:

1. Go to *System > FortiGuard*.
2. In the *FortiGuard Server Settings* section, select *Use override FDN server to download module updates* and enter the FortiManager IP address.
3. In the *FortiGuard Web Filter Settings* section, select *Use override server for web filtering query (address or address:port)* and enter the FortiManager IP address.

4. In the *FortiGuard Server Settings* section, click *Connect FDN Now* to test the FDN connection.

The screenshot shows the FortiGuard configuration page within the FortiDeceptor VM interface. The left sidebar contains a menu with 'System' expanded, showing options like Administrators, Admin Profiles, Certificates, LDAP Servers, RADIUS Servers, Mail Server, SNMP, FortiGuard, and Settings. The main content area is titled 'FortiGuard' and contains three sections: 'FortiGuard Server Settings', 'FortiGuard Web Filter Settings', and 'VM Image Download Proxy Settings'. In the 'FortiGuard Server Settings' section, the checkbox 'Use override FDN server to download module updates' is checked, and the text field next to it contains 'fds1.fortinet.com'. A red box highlights this checkbox and text field. Below this, there is an unchecked checkbox for 'Use Proxy' and a red button labeled 'Connect FDN Now'. The 'FortiGuard Web Filter Settings' section has the checkbox 'Use override server for web filtering query (address or address:port)' checked, with the text field containing 'service.fortiguard.net'. A red box highlights this checkbox and text field. To the right of the text field are two small red boxes containing the numbers '53' and '8888'. Below this is an unchecked checkbox for 'Use Proxy'. The 'VM Image Download Proxy Settings' section has an unchecked checkbox for 'Use Proxy'. At the bottom right of the configuration area is a red button labeled 'Apply'.

5. If the test passes, click *Apply*.

Appendix A - Deception deployment best practices

This section provides best practices principles and use cases on how to deploy FortiDeceptor in different network topologies.

The section covers the following topics:

[Deception strategy on page 130](#)

[FortiDeceptor platform on page 132](#)

[Deploying deception on page 143](#)

[Attack vectors vs deception on page 154](#)

[Deploying tokens using AD GPO logon script on page 158](#)

[Configuring trunk ports on FortiDeceptor VM on page 163](#)

Deception strategy

The ancient war strategies by Sun Tzu says: "Know thy self, know thy enemy. A thousand battles, a thousand victories."

This means if you know the strengths and weaknesses of your enemy, and if you know the strengths and weaknesses in your defense system, you can win any battle. To win against cyber attackers and hackers or users with malicious intention, the cyber security team needs to understand the attacker's techniques and tools, as well as shortfalls in the organization's defense system.

To understand the attack techniques and hackers' interests in your environment, we need to understand three tools that can help security professionals stop attackers before a data breach happens.

- **Sandboxing:** This technique allows the malware to install and run in an enclosed environment where the security team can monitor the malware's actions to identify potential risks and countermeasures.
- **Honeypots:** These are intentionally vulnerable systems that are meant to attract attackers. Honeypots entice attackers to attempt to steal valuable data or further scope out the target network. Honeypots help you to understand the process and strategy of attackers.
- **Deception technologies:** These are more advanced honeypot and honeynet products that offer more automation for both detection and implementation of defenses based on the data they gather.

Deception technology is like honeypots on steroids. It has more advanced capabilities like deception lure, deception automation, threat analysis, threat hunting, and more.

The core technology behind deception is the decoy. In general, there are several kinds: low, medium, and high. To align with FortiDeceptor technology, let's focus on two types of decoys: Low Interaction and High Interaction.

- **Low interaction honeypot:** This decoy has limited capability of emulating enterprise applications and is used only to detect from where the attackers are coming and what they attempt to exploit. These are easy for attackers to fingerprint and bypass.
- **High interaction honeypot:** This decoy is identical to the enterprise systems and can run real operating systems, applications, and services with dummy data. They allow the attacker to log in and they respond to the attacker's

request. In this way, the decoy helps you understand the attacker's intentions, lures them for a long time to identify how command and control infrastructure is set up.

Deception technology systems are more advanced and have more components, breadcrumbs, baits, and lures. Deception systems are implemented alongside enterprise systems but still remain in an isolated environment.

Deception technology systems are used to interrupt the attacker's kill chain, prolong the attack either to exhaust the attacker's resources or encourage attackers by providing obvious vulnerabilities to help identify the details of their network and arsenals.

Deception strategy components

Deployment of enterprise-scale deception includes the following components:

- Medium interaction decoy and high interaction decoy that are deployed everywhere.
- Customizable decoys to match infrastructure and applications.
- Create and deploy lures to redirect attackers toward decoys.
- Create and deploy lures with trackable misinformation.
- Threat analysis capabilities.
- Integration with existing security infrastructure for mitigation and remediation (Security Fabric and third-party).

Deception strategy goals

Deployment of enterprise-scale deception should achieve the following cybersecurity requirements and goals:

- Generate actionable, high-fidelity alerts.
- Reduce the “dwell time” of an initial compromise.
- Confuse the attacker with false assets and misinformation.
- Block the human attacker or Advanced Persistent Threat (APT).
- Collect threat intelligence regarding tactics, techniques, and procedures.
- Integrate with existing defense-in-depth architecture.

Deception philosophy

Deception philosophy is a straightforward concept. You deploy deception across the whole network infrastructure and location which generates a fake virtual network layer that masks the real assets with a fake one.

The networks today are fluid and dynamic, so we need to be sure that every network segment and location has this deception layer and capability.

For example:

- **IT Endpoint segment** — Requires deployment of lures and decoys.
- **IT Servers segment** — Requires deployment of lures and decoys.
- **Network Devices** — Requires deployment of decoys.
- **IoT Devices** — Requires deployment of decoys.
- **OT Devices** — Requires deployment of decoys.
- **Data Repository** — Requires deployment of honey files and decoys.
- **Application segment** — Requires deployment of lures and decoys.

- **Network Traffic** — Require decoys that generates fake network traffic and lure that creates fake network connections and entries on the endpoint level.
- **Public/Private Cloud** — Requires deployment of decoys.

Deception light stack vs full stack

Deception light stack concept

The light deception concept uses a combination of endpoint lures with several high interaction decoys only as destination targets.

Using the light deception concept against a sophisticated adversary has some significant drawbacks:

- Deception lures reside on the endpoint and if there is no in-depth customization, this can be fingerprinted.
- A sophisticated adversary that controls several endpoints might fail once and learn the deception lure logic so that the adversary will not make the same mistake next time.
- A sophisticated adversary might not touch the deception lures if it can get high privilege at the beginning of the attack, and the probability of finding several decoys from several thousand assets is non-existent.
- Lack of visibility around unmanaged devices (IoT/OT) where an adversary has plenty of time and space to attack without detection.
- Simple malware spread vectors like pass the hash / single vulnerability attacks are not detected due to a lack of decoys in the network segment level. For example, the Wannacry malware will not get detected using this deployment stack.

Deception full stack concept

A simple explanation of the deception full stack concept is “do not let the sophisticated adversary / malware fingerprint your fake story!”

The deception full stack addresses the drawback of the light deception concept using several deception layers' architectures:

- Server / endpoint lures are the first layer that engages with the adversary / APT.
- A large scale of decoys that creates a fake network surface on top of the real one offering false endpoints, servers, network devices, IoT/OT, database, files, applications, cloud, and more. This is the deception everywhere concept.
- Some of the decoys are generated from a customer “gold image” and are part of the network domain to increase the authentic deception level.

The dynamic deception decoys module prevents the sophisticated adversary from fingerprinting the decoys by changing the decoys' IP addresses and profile based on time or trigger.

The FortiDeceptor full stack deception concept runs deception lures with a large scale of decoys using a hybrid mode engine that provides medium and high-level interaction decoys against the adversary / APT malware.

FortiDeceptor platform

The FortiDeceptor platform includes the following:

- [FortiDeceptor components on page 133](#)
- [FortiDeceptor Token Package on page 133](#)

- [FortiDeceptor decoys on page 134](#)

FortiDeceptor components

The FortiDeceptor platform includes the following components:

- The FortiDeceptor management console manages and operates the whole platform including deployment, configuration, alerting, analysis, and ECO system integration.
- FortiDeceptor offers a highly-scalable three-tier architecture that combines three levels of deception:
 - Server / endpoint lures.
 - Medium interaction decoys (IoT / OT).
 - High interaction decoys.

You can deploy deception lures using existing infrastructure tools such as A/D GPO, MS SCCM, and so on.

A single FortiDeceptor appliance can run up to 16 deception VMs that support a total of 256 IP addresses. Each IP address represents a single decoy.

You can download a deception VM from the FortiDeceptor marketplace. You can also allow the end user admin bring their own gold image and convert it to a decoy using the FortiDeceptor decoy customization wizard.

FortiDeceptor Token Package

The FortiDeceptor Token package adds breadcrumbs on real endpoints and servers, and redirects an attacker to engage with a decoy instead of a real asset. Deception tokens are typically distributed within real endpoints and servers on the network to expand the deception surface.

Effective deception lure technology should support the following:

- Deploy deception lure data and configurations where attackers collect information.
- Deception lure location must be invisible to end users, and doesn't affect endpoint functionality.
- Deception lure is accessible with user level permissions so that attackers can access it early on and get detected. This saves the privileged escalation attack time.

The current FortiDeceptor token packages are:

Windows	<ul style="list-style-type: none">• SMB• RDP• SSH• HoneyDocs• Network Connection (static MAC address)
Linux	<ul style="list-style-type: none">• SMB (SAMBA)• RDP (xfreerdp)• SSH
MAC	<ul style="list-style-type: none">• SMB (SAMBA)• RDP (xfreerdp)• SSH
SAP	<ul style="list-style-type: none">• SAP

When the FortiDeceptor token package is installed on a real Windows, Linux, or MAC endpoint, it increases the deception surface and redirects an attacker to engage with a decoy instead of a real asset.

FortiDeceptor decoys

FortiDeceptor creates a network of decoys to lure attackers and monitor their activities on the network. When a hacker attacks a decoy, an alert is generated and their malicious activities are captured and analyzed in real-time. This analysis generates a mitigation and remediation response that protects the network.

The current FortiDeceptor decoy OS are:

Windows	Windows 7, Windows 10, Windows 2016 and Windows 2019
Linux	Ubuntu Desktop, CentOS, ESXi and ELK
IoT/OT	SCADA version 3, Medical OS, and IoT OS.
VPN	Fortinet SSL-VPN (FG-60E, FG-100F, FG-1500D, FG-2000E, FG-3700D)
Customized Windows	Windows 10, Windows Server 2016, Windows Sever 2019

The current FortiDeceptor application decoys are:

Application Decoys	POS OS, ERP OS PACS and SAP
---------------------------	-----------------------------

The current FortiDeceptor lure services are:

Windows	RDP, SMB, TCPLListener, NBNSSpoofSpotter, ICMP and FTP
Linux	SSH, SAMBA, TCPLListener, HTTP, HTTPS, GIT, ICMP and FTP
IoT/OT	HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, ENIP, Kamstrup, DNP3, Telnet, PACS-WEB, PACS, DICOM server, Infusion Pump (TELNET), Infusion Pump (FTP), POS-WEB, ERP-WEP, GUARDIAN-AST, IEC104, Jetdirect, Printer-WEB, IP Camera-WEB, UPnP, RTSP, CDP, TP-link WEB, CWMP, SAP DISPATCHER and SAP WEB
SSL VPN	HTTPS
Customized Windows	RDP, SMB, NBNSSpoofSpotter, MSSQL, IIS (HTTP/HTTPS) and ICMP

The current FortiDeceptor IP address capacity are:

- A single EOL can host up to 16 deception VMs.
- A single FDCIKG can host up to 20 deception VMs.
- A single FDCVMS can host up to 20 deception VMs.
- A single deception VM supports up to 24 IP addresses or decoys. Each IP represents a decoy.
- A single FortiDeceptor appliance (HW/VM) can support up to 480 IP addresses.
- A single FortiDeceptor appliance (HW/VM) can support up to 128 segments (VLANs).



VPN only supports 8 IPs.
Cisco Decoy only supports 1VLAN.

Decoy services details

- [IoT OS on page 135](#)
- [Medical on page 137](#)
- [POS on page 138](#)
- [CRM\(ERP\) on page 138](#)
- [SAP on page 138](#)
- [SCADA](#)

IoT OS

Brother MFC Printer Decoy

Service	Description
SNMP	<ul style="list-style-type: none"> • Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for Brother MFC Printer decoy.
Jetdirect	Enable this service to open port 9100 on the decoy VM and respond to PJJ (Printer Job Language) requests.
Printer-WEB	A web GUI that simulates the administration GUI of Brother NC-340h printer.

Cisco router decoy

Service	Description
Models*	4 Cisco images (models) are supported: 2691, 3660, 3725 and 3745. An error is displayed if you upload an image that is not supported.
Router Running-Config (optional)	Allows you to upload a customized Cisco <i>config</i> file to predefine the Cisco router setting
Telnet service	A login-required service that enables attackers to utilize all Cisco router functions.
HTTP service	A login-required GUI service similar to the telnet service but with less functionality.
SNMP service	<ul style="list-style-type: none"> • Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Cisco router decoy.
CDP service	Enable this service to allow the decoy VM to send CDP traffic within the network.

*Please provide Cisco IOS software to run the Cisco decoy. You can copy the IOS from any Cisco router/switch flash by using TFTP server and running the `copy flash tftp:` command on the Cisco router/switch side, and then completing the deployment wizard.

HP printer decoy

Service	Description
SNMP service	<ul style="list-style-type: none"> • Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) requests from within network • Community name is user-defined • SNMP response is customized for HP printer decoy.
Jetdirect	<ul style="list-style-type: none"> • Enable this service to open port 9100 on the decoy VM, and respond to PJJ (Printer Job Language) requests.
Printer-WEB	<ul style="list-style-type: none"> • A web GUI that simulates the administration GUI of HP Officejet Pro X451dw printer.

IP camera decoy

Service	Description
IP Camera-WEB	<ul style="list-style-type: none"> • A login-required service that displays videos to simulate IP cameras. Default videos are available. However, we strongly recommend uploading 1-8 .mp4 videos that fit best with the working environment.
SNMP service	<ul style="list-style-type: none"> • Enable this service to open port 161 on the decoy VM, and respond to SNMP (v1 or v2c) requests from within the network • Community name is user-defined. • SNMP response is customized for IP camera decoy.
UPnP service	<ul style="list-style-type: none"> • Enable this service to open port 8080 on the decoy VM and simulate UPnP service. • A UPnP msg will broadcast within the network. Within the msg there is a URL for the attacker to download a .xml file showing device information.
RTSP service	<ul style="list-style-type: none"> • When this service is enabled, you will also need to upload a video to a predefined location so the attacker can watch the video. • The RTSP port can be adjusted. • To upload the video, you can use <i>ffmpeg</i>, or any other method to infinitely loop a video so it is available to the attacker <p>Example:</p> <p>To infinitely loop a video: <code>sudo ffmpeg -re -stream_loop -1 -i {path_to_local_video} -c copy -f rtsp rtsp://{ip}:{port}/{name_you_choose};</code></p> <p>From the attacker perspective, the live camera stream is available at <code>rtsp://{ip}:{port}/{name_you_choose}</code></p>

Lexmark Printer decoy

Service	Description
SNMP	<ul style="list-style-type: none"> • Enable this service to open port 161 on decoy VM, and respond to SNMP(v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for Lexmark Printer decoy
Jetdirect	Enable this service to open port 9100 on the decoy VM and respond to PJL (Printer Job Language) requests.
Printer-WEB	A web GUI that simulates the administration GUI of Lexmark MX410de printer.

TP-LINK decoy

Service	Description
TP-LINK WEB	Enable this service to allow attackers to login to a fake TP-link setting site.
CWMP	Enable this service to send data using CWMP protocol to <i>{ip}:{port}/cpe</i> .

Medical

Service	Description
Infusion Pump (Telnet) service	<ul style="list-style-type: none"> • Simulates Infusion Pump (telnet) • A username/password is required to login.
Infusion Pump (FTP)	<ul style="list-style-type: none"> • Simulates Infusion Pump (FTP) • A username/password is required to login.
PACS service	<ul style="list-style-type: none"> • A user-defined name for the PACS system.
PACS-WEB service	<ul style="list-style-type: none"> • Login-required web GUI for PACS, with existing medical data • Port can be adjusted
DICOM Server service	<ul style="list-style-type: none"> • Server port can be adjusted • Server name can be adjusted • DICOM operations (e.g. C-STORE, C-FIND) are supported
B. Braun Infusomat service	<ul style="list-style-type: none"> • HTTP/S: Built-in web services to retrieve medical data • CAN Bus Protocol (enable/disable) • B.BRAUN (port 8080): Login-required web GUI for the B.Braun Infusomat device

POS

Service	Description
POS-WEB service	<ul style="list-style-type: none"> Login-required web GUI simulate POS website Port can be adjusted

CRM(ERP)

Service	Description
ERP-WEB service	<ul style="list-style-type: none"> Login-required web GUI simulates ERP website Port can be adjusted

SAP

Service	Description
SAP ROUTER	<ul style="list-style-type: none"> Enable SAP ROUTER Service so SAP Logon can configure the SAProuter String. Use the default port to ensure SAP Logon can connect.
SAP DISPATCHER	<ul style="list-style-type: none"> Enable SAP DISPATCHER so SAP Logon can get responses from the SAP decoy. Use the default port to ensure SAP Logon can connect.
SAP WEB	A fake SAP HTTP and HTTPS GUI for SAP Fiori Launchpad or Legacy WebGUI.

SCADA (version3) OS

Ascent Compass MNG decoy

Service	Description
HTTP service	<ul style="list-style-type: none"> Enable this service to capture attacks through HTTP on the default HTTP port.
FTP service	<ul style="list-style-type: none"> Enable this service to capture attacks through FTP on the default FTP port FTP banner is user-defined.
SNMP service	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) request from within the network Community name is user-defined SNMP response is customized for Ascent Compass MNG decoy.
BACNET service	<ul style="list-style-type: none"> Enable this service to capture attacks through BACNET on the default BACNET port.

Guardian-AST decoy

Service	Description
Guardian-AST service	<ul style="list-style-type: none"> • Enable this service to simulate an AST's satellite communications remote asset tracking system named <i>Guardian</i>. • To deploy a Guardian-AST decoy, this service must be enabled since it is the only service available

IPMI Device decoy

Service	Description
HTTP service	<ul style="list-style-type: none"> • Enable this service to capture attacks through HTTP on the default HTTP port.
SNMP service	<ul style="list-style-type: none"> • Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for IPMI Device decoy.
FTP service	<ul style="list-style-type: none"> • Enable this service to capture attacks through FTP on the default FTP port. • FTP banner is user-defined.
IPMI service	<ul style="list-style-type: none"> • Enable this service to capture attack through IPMI on the default IPMI port.

KAMSTRUP 382 decoy

Service	Description
KAMSTRUP service	<ul style="list-style-type: none"> • Toggle to enable/disable this service. Enable this service to simulate a Kamstrup device • To deploy a KAMSTRUP decoy, this service must be enabled since it is the only service available

Liebert Spruce UPS decoy

Service	Description
TFTP	Enable this to service capture attacks through TFTP on default TFTP port
SNMP	<ul style="list-style-type: none"> • Enable this service to open port 161 on decoy VM and respond to SNMP(v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Liebert Spruce UPS decoy.
HTTP	Enable this service to capture attacks through HTTP on default HTTP port.

Niagara4 Station decoy

Service	Description
SNMP	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. Community name is user-defined. SNMP response is customized for IPMI Device decoy.
HTTP	Enable this service to capture attacks through HTTP on default HTTP port.
BACNET	Enable this service capture attack through BACNET on default BACNET port.

NiagaraAX Station decoy

Service	Description
SNMP	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. Community name is user-defined. SNMP response is customized for IPMI Device decoy.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.
BACNET	Enable this service capture attacks through BACNET on the default BACNET port.

PowerLogic ION7650 decoy

Service	Description
SNMP	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. Community name is user-defined. SNMP response is customized for PowerLogic ION7650 decoy.
MODBUS	Enable this service capture attacks through MODBUS on the default MODBUS port.
DNP3	Enable this service capture attacks through DNP3 on the default DNP3 port.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.

Rockwell 1769-L16ER/BLOGIX5316ER decoy

Service	Description
SNMP	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. Community name is user-defined. SNMP response is customized for Rockwell 1769-L16ER/B LOGIX5316ER decoy.

Service	Description
ENIP	Enable this service to capture attacks through ENIP on the default ENIP port.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.

Rockwell 1769-L35E Ethernet Port decoy

Service	Description
SNMP	<ul style="list-style-type: none"> • Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Rockwell 1769-L35E Ethernet Port decoy.
ENIP	Enable this service to capture attacks through ENIP on the default ENIP port.
HTTP	Enable this service to capture attacks through HTTP on the default HTTP port.

Rockwell PLC decoy

Service	Description
HTTP service	<ul style="list-style-type: none"> • Enable s this service capture attack through HTTP on the default HTTP port. • HTTP page title is user defined.
TFTP service	<ul style="list-style-type: none"> • Enable this service to capture attacks through TFTP on the default TFTP port.
SNMP service	<ul style="list-style-type: none"> • Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) request from within the network. • Community name is user-defined. • SNMP response is customized for Siemens Rockwell PLC decoy.
ENIP service	<ul style="list-style-type: none"> • Enable this service capture attack through ENIP on the default ENIP port. • ENIP serial number is user-defined.

Schneider EcoStruxure BMS server decoy

Service	Description
SNMP service	<ul style="list-style-type: none"> • Enable this service to open port 161 on decoy VM and respond to SNMP (v1 or v2c) requests from within the network. • Community name is user-defined. • SNMP response is customized for Schneider EcoStruxure BMS server decoy.
BACNET service	<ul style="list-style-type: none"> • Enable this service to capture attacks through BACNET on the default BACNET port.

Service	Description
HTTP service	<ul style="list-style-type: none"> Enable this service to capture attacks through HTTP on the default HTTP port.
TRICONEX service	<ul style="list-style-type: none"> Enable this service to capture attacks with the TRICONEX service.

Schneider Power Meter - PM5560 decoy

Service	Description
SNMP service	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network Community name is user-defined. SNMP response is customized for Schneider Power Meter - PM5560 decoy.
BACNET service	<ul style="list-style-type: none"> Enable this service to capture attacks through BACNET on the default BACNET port.
HTTP service	<ul style="list-style-type: none"> Enable this service to capture attacks through HTTP on default HTTP port.
DNP3 service	<ul style="list-style-type: none"> Enable this service capture attacks through DNP3 on the default DNP3 port.
ENIP service	<ul style="list-style-type: none"> Enable this service to capture attacks through ENIP on the default ENIP port.

Schneider SCADAPack 333E decoy

Service	Description
SNMP service	<ul style="list-style-type: none"> Enable this service to open port 161 on decoy VM, and respond to SNMP(v1 or v2c) requests from within the network. Community name is user-defined. SNMP response is customized for Schneider SCADAPack 333E decoy.
DNP3 service	<ul style="list-style-type: none"> Enable this service to capture attacks through DNP3.
Telnet service	<ul style="list-style-type: none"> Login-required telnet service simulates SCADAPack E Smart RTU command line environment.

Siemens S7-200 PLC decoy

Service	Description
HTTP service	<ul style="list-style-type: none"> Enable this service capture attacks through HTTP on the default HTTP port. HTTP page title is user defined. Plant Identification is user-defined. Serial Number is user-defined.
TFTP service	<ul style="list-style-type: none"> Enable this to service capture attacks through TFTP on the default TFTP port.
SNMP service	<ul style="list-style-type: none"> Enable this service to open port 161 on decoy VM, and respond to SNMP(v1

Service	Description
	<ul style="list-style-type: none"> or v2c) request from within the network. Community name is user-defined. SNMP response is customized for Siemens S7-200 PLC decoy.
MODBUS service	<ul style="list-style-type: none"> Enable this service to capture attacks through MODBUS on the default MODBUS port.
S7COMM service	<ul style="list-style-type: none"> Enable this service capture attacks through S7COMM on the default S7COMM port. Module Type is user-defined. PLC Name is user-defined.

Siemens S7-300 PLC decoy

TFTP service	<ul style="list-style-type: none"> Enable this service to capture attacks through TFTP on the default TFTP port.
SNMP service	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. Community name is user-defined. SNMP response is customized for Siemens S7-300 PLC decoy.
IEC104 service	<ul style="list-style-type: none"> Enable this service capture attacks through IEC104 on the default IEC104 port.

VAV-DD BACNET controller decoy

Service	Description
SNMP service	<ul style="list-style-type: none"> Enable this service to open port 161 on the decoy VM and respond to SNMP (v1 or v2c) requests from within the network. Community name is user-defined. SNMP response is customized for VAV-DD BACNET controller decoy.
BACNET service	<ul style="list-style-type: none"> Enable this service to capture attacks through BACNET on the default BACNET port.

Deploying deception

To deploy FortiDeceptor to optimize the deception surface, see the following best practices.

[Deception decoy best practices on page 144](#)

[Deception token best practices on page 147](#)

[AD integration best practices on page 148](#)

[Deployment best practices checklist on page 149](#)

[Network topology best practices on page 150](#)

Deception decoy best practices

Deception effectiveness requires deployment across all network segments and locations.

This topic provides deception deployment best practices for the decoy layer, including deployment guidelines for each kind of network VLAN that can exist on an enterprise network.

Example of 5-8 decoys per data-center segment (VLAN)

OS

Deploy a matching decoy OS for each type of critical / sensitive IT system in this segment.

Services

Enable matching services for each type of critical / sensitive IT system in this segment and customize the services:

- Apply banner matching the network.
- Apply user access rule such as fake user and password.
- Upload fake data (SMB, FTP, HTTP).

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure.

Application

Enable a false matching application for each type of critical / sensitive IT system on this segment. If you do not have a matching application, enable high profile fake applications like ERP, POS, or PACS, and so on..

Hostname

Follow corporate standard server's names for half the decoys and assign enticing names to the remaining half, such as JumpHost001, ERP-XXX, MNG-XXX, Net-Monitor, and so on. Remember that we need to configure these hostnames on the AD level as we use single deception VM across 16 IP address and we can have just one real hostname per OS. For the rest of the IP address, we should have it virtual on the DNS level.

Attackers also like to attack servers with a hostname that has names like "-test" or "-dev" as attackers assume that these servers are less protected.

Gold Image

Ensure you use at least two Windows servers as customer gold images that host critical applications and data. To increase authenticity, configure them to be part of the organization domain.

STATIC / DHCP IP Address

For datacenter segment hosting servers that always use static IP addresses, also use static IP configuration for the decoys.

Example of 2-4 decoys per endpoint segment (VLAN)

OS

Deploy a matching decoy OS and also an “old” OS like Win7.

Services

Enable matching services for the endpoint on this segment.

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure.

Hostname

Follow corporate standard server’s names for half the decoys and assign enticing names to the remaining half, such as IT Admin, HelpDesk, DBA, Finance, and so on. Remember that we need to configure these hostnames on the AD level as we use single deception VM across 16 IP address and we can have just one real hostname per OS. For the rest of the IP address, we should have it virtual on the DNS level.

Gold Image

Ensure you use at least 3–4 Windows servers as customer gold images. To increase authenticity, configure them to be part of the organization domain.

STATIC / DHCP IP Address

For endpoints segment hosting desktops that always use DHCP IP addresses, also use the DHCP IP configuration for the decoys. The DHCP configuration in FortiDeceptor 3.1 and 3.2 allows us to configure one IP per segment, so use the static configuration in this stage to have more decoys per segment.

Example of 7-10 decoys per OT segment (VLAN)

OS

Deploy a matching decoy SCADA OS.

Deploy a matching regular IT OS such as Win7, Win10, or Win2016.

Services

Enable matching services for the OT assets on this segment and customize the services.

- Apply banner matching the network.
- Apply access rule such as fake user and password.
- Upload fake data (SMB, FTP, HTTP).

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure. You can also use a search engine like SHODAN.IO to find this data on the Internet and use it to customize the decoys.

Hostname

Follow the OS SCADA names for half the decoys and assign enticing names to the remaining half, such as IT Admin, SCADA-MNG, PLC_ADMIN, HMI_SERVER, NET-MONITOR, and so on.

Application

Check if the customer is willing to provide you access to his OT software. Otherwise, use open-source OT software or use the customize decoy option to generate this kind of decoy.

MAC ADDRESS

Ensure the OT decoy uses the appropriate MAC ADDRESS per vendor.

STATIC / DHCP IP Address

OT networks are mainly a static environment that does not has a DHCP server, so use static IP configuration as well for the decoys.

Example of 8-10 decoys per cloud segment (VPC, VNET)

OS

Deploy a matching decoy OS for each type of critical / sensitive IT system in this segment.

Services

Enable matching services for each type of critical / sensitive IT system in this segment and customize the services:

- Apply banner matching the network.
- Apply user access rule such as fake user and password.
- Upload fake data (SMB, FTP, HTTP).

If you do not have out-of-the-box matching services, you can use the custom TCP port listener.

Data

Upload fake data to the decoys to provide authentic engagement. If you do not have matching files, ask the customer to provide a public files package that you can upload and generate fake data using the same structure.

Application

Enable a false matching application for each type of critical / sensitive IT system on this segment. If you do not have a matching application, enable high profile fake applications like ERP, POS, or PACS, and so on.

Hostname

Follow corporate standard server's names for half the decoys and assign enticing names to the remaining half, such as JumpHost001, WEB-XXX, DB-XXX, Sec-Monitor, and so on. Remember that we need to configure these hostnames on the AD level as we use single deception VM across 16 IP address and we can have just one real hostname per OS. For the rest of the IP address, we should have it virtual on the DNS level.

Attackers also like to attack servers with a hostname that has names like "-test" or "-dev" as attackers assume that these servers are less protected.

Gold Image

Ensure you use at least two Windows servers as customer gold images that host critical applications and data. To increase authenticity, configure them to be part of the organization domain.

STATIC / DHCP IP Address

Cloud environments mainly host servers that always use static IP addresses, so use static IPs configuration as well for the decoys.

Deception token best practices

Deception effectiveness requires deployment across all managed endpoints and servers.

This topic provides deception deployment best practices for the deception token layer. For token deployment over AD logon script, see appendix A.

Example of deception tokens on Windows, MAC, or Linux endpoint segment (VLAN)

RDP token

- Set up several Windows server decoys that support RDP access.
- Set up appropriate decoy hostnames like Terminal-XX, VDI-XX, and so on. This increases the level of authenticity when you add the Windows server decoys to the company domain.
- Follow company username and password policy.
- Generate 2-3 deception lures and deploy them over several different AD user groups.

SMB token

For Windows endpoints, use either SMB token or SAMBA token. Do not use both.

- Set up at least two Windows server decoys that support two fake network share access.
- Generate at least two tokens with two different share names.
- Use a share name similar to the company structure.
- Set up appropriate hostnames like FileSRV-XX, File-Server, and so on. This increases the level of authenticity when you add the Windows server decoy to the company domain.
- Follow company username and password policy.
- Generate a single deception token package and deploy it over all the network endpoints.

SAMBA token

For Windows endpoints, use either SMB lure or SAMBA token. Do not use both.

- Set up at least two Linux server decoys that support network share access.
- Set up appropriate hostnames like Storage-XX, Backup-Server, and so on.
- Generate at least two tokens with two different share names.
- Use a share name similar to the company structure.
- Follow company username and password policy.
- Generate a single deception token package and deploy it over all the network endpoints.

SSH lure

- Set up several Linux server decoys that support SSH access.
- Set up appropriate hostnames like JumpHost-XX, Control-XX, Cloud-XXX, and so on.
- Use a complicated password. This gives the attacker the impression that this is a critical server.
- Generate 2-3 deception tokens and deploy them over the IT endpoints group only. Attackers do not expect to see SSH clients on a regular desktop.

AD integration best practices

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and allows administrators to manage permissions and access to network resources. Active Directory stores data as objects. An object is a single element, such as a user, group, application; or device, such as a printer.

To detect AD attack using deception technology, use the following deception configuration example.

- Deploy custom Windows decoys (Windows 10, 2016, 2019) and add them to the customer network domain.

Example of custom decoys in customer network domain

- Add several custom Windows decoys to the customer network domain.
- On the Windows domain, configure schedule task scripts to run using the fake users, such as the one from the cache credentials lure.
- Add to each domain decoy the maximum number of IP addresses and ensure they are static IP addresses.
- On the network DNS server, configure a decoy DNS.
 - Add DNS records to each decoy IP address.
 - Set up attractive hostnames for each decoy IP address. For more information, see [Deception decoy best practices on page 144](#).
- Deploy the SMB lure front in a domain decoy to avoid detection by tools like HoneyBuster.

Deployment best practices checklist

This checklist is an example of a deception deployment profiling and sizing. This example is based on a company with one headquarters (HQ) site and two remote sites, one of which is a manufacturing site.

Deception Items	Customer Requirements	Deployment
FortiDeceptor appliance HW/VM	VM	The VM support VMware or KVM.
HQ site installation	Yes	Deploy on the company ESXi where you have access to most of the network VLANs.
Number of remote sites	2	<p>If the primary and remote locations are connected by FortiGate firewall, configure the VXLAN tunnel between firewalls to publish decoys over the L2 tunnel from the HQ to the remote sites. For details on setting up the VXLAN, see https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD47325&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=163742631&stateId=1%200%20163740760%27.</p> <p>If the firewalls are different, check with Customer Support on how to configure an L2 Tunnel.</p>
Remote sites are office / OT network	1 remote office + 1 manufacture site	<p>For remote office site, deploy Windows / Linux desktop decoys and deception lures like SMB, RDP and cache credentials.</p> <p>For remote OT site, deploy Windows / Linux and SCADA decoys.</p>
Number of segments (VLANs) to cover	30	
Number of DC segments to cover	2	Deploy Windows / Linux server decoys.
Customer's server OS	Windows, Linux	Deploy Windows / Linux server decoys.
Critical services in the DC segments	SAP, web logistic app	Deploy ERP decoy, Windows decoy with a web app.
Number of endpoint segments to cover	25	Deploy Windows / Linux desktop decoys.
Customer's endpoint OS	Windows, MAC	Deploy deception lures such as SMB, RDP, and cache credentials for both Windows and MAC.

Deception Items	Customer Requirements	Deployment
Customer's most important asset to protect	SAP	Deploy Windows decoy with SQL that uses SAP fake data.
Attack vectors customer is facing	Phishing, PTH, lateral movement based on AD	Deploy deception lures like SMB, RDP, and cache credentials. Follow cache credentials best practice.
Customer network's IoT devices	Printer, camera, temp sensors	
Customer network's OT devices	SCADA PLC, HMI	Deploy Windows / Linux and SCADA decoys.
Customer FortiGate firewall solution	Yes	Configure Security Fabric integration for isolation mitigation response.
Customer SIEM solution	Yes	Send SYSLOG from the FDC. Configure a correlation rule to detect lateral movement based on cache credentials lure.

Network topology best practices

For effective deception, you must also understand the customer's network topology, company security risks, where his most important assets are located, and what kind of attack vectors they face or have concerns.

Several common network topologies require different deception deployment approaches.

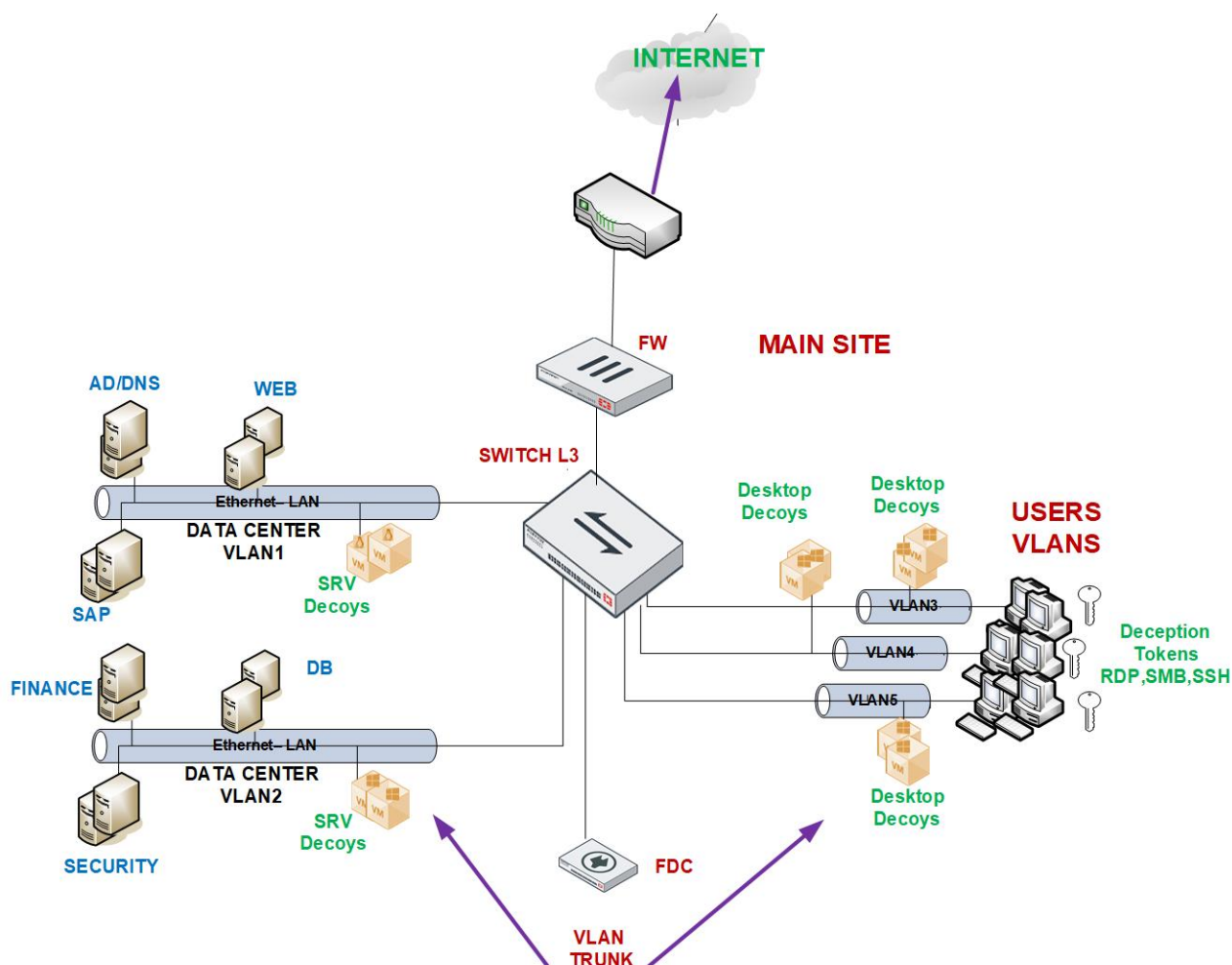
This topic provides best practices for the following scenarios:

1. [Network with data center and users at the same location.](#)
2. [Network with a data center, users at the same location, and users at remote offices.](#)
3. [Network with a data center, users at the same location, users at remote offices, and remote OT sites.](#)

Deception deployment in HQ only

A network topology without remote location is less common today. The reasoning might be that the most important assets are in HQ only and there is no need to deploy deception in remote sites.

This scenarios shows deploying deception in the main HQ only even if there are also remote locations.

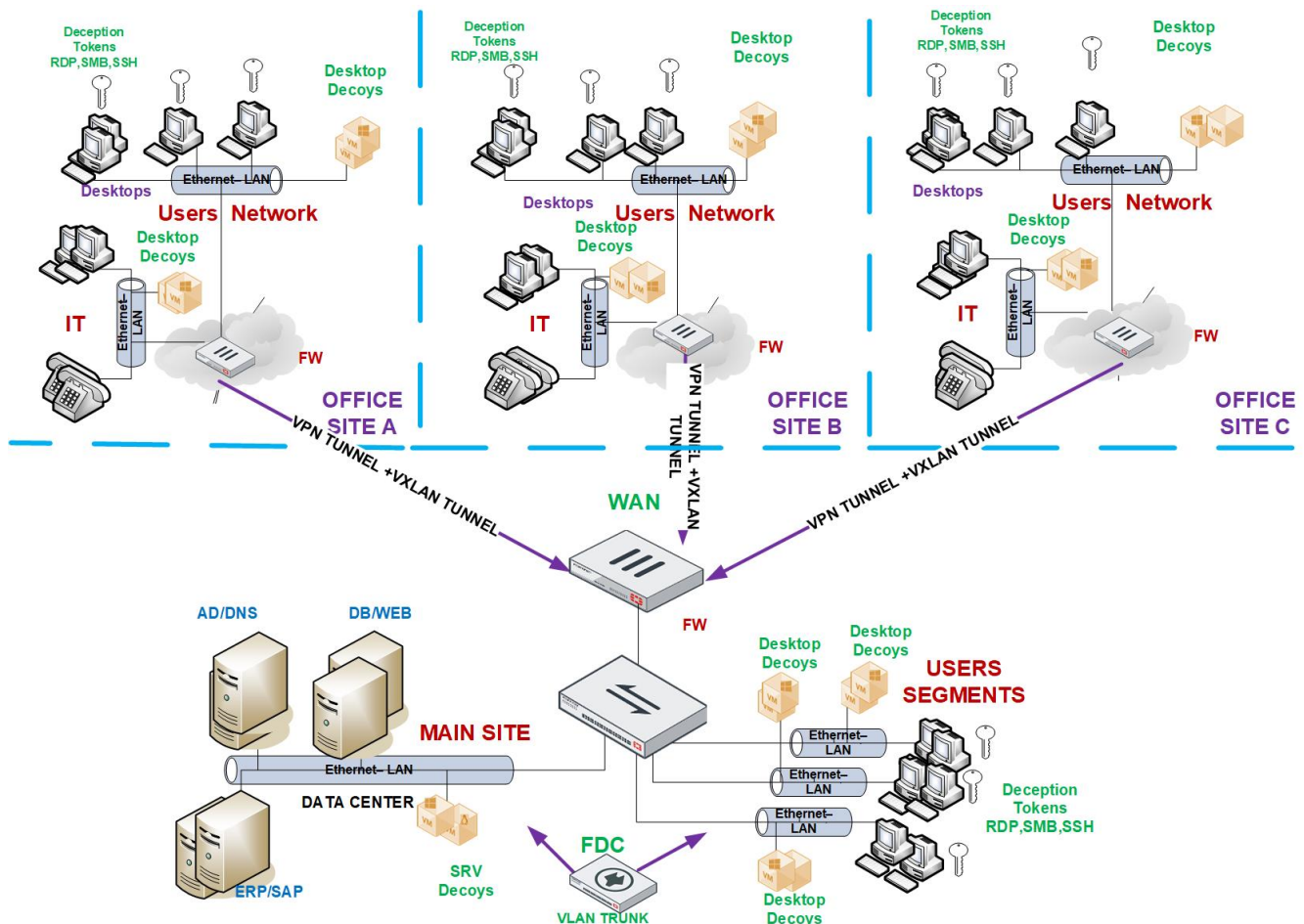


In this scenario, follow these best practice recommendations:

Deception deployment in HQ and remote offices

Network topology with remote locations is the most common enterprise network topology for installations that want to provide the same security protection across all sites.

The level of connectivity required by remote office users is broader and will lead to a data breach if the security level is not similar to the HQ security.



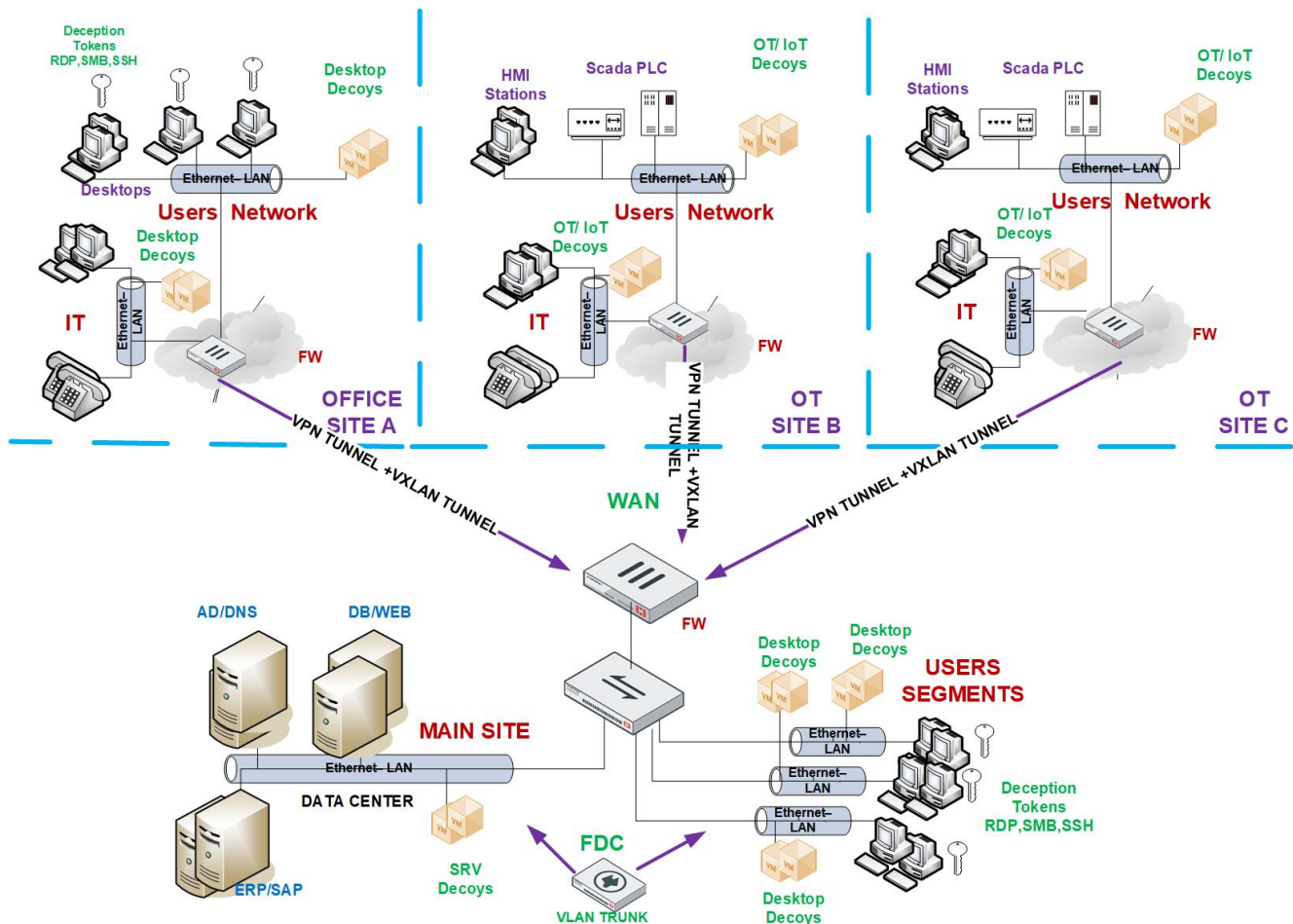
In this scenario, follow these best practice recommendations:

- Deploy a single FortiDeceptor appliance and connect it to the network via trunk to cover most of the HQ network VLANs.
- Deploy decoys following the best practice recommendation in [Deception decoy best practices on page 144](#).
 - On data center VLANs: 5-7 decoys per VLAN.
 - On endpoint VLANs: 2-4 decoys per VLAN.
- Deploy deception lures across all manageable endpoints even if some of them are in remote sites.
 - RDP
 - SMB
 - Cached credentials
 - HoneyDocs
 - SSH (on IT department desktops only)

- Fabric integration.
 - If you have FortiGate, consider the integration value between FortiDeceptor and FortiGate for alert mitigation by isolating the infected machine.
 - Send SYSLOG to SIEM or any logger solution in place.
 - Send SYSLOG to SOAR solution for Deception playbooks. For example, FortiSOAR has pre-built deception playbooks for FortiDeceptor.

Deception deployment in HQ, remote offices, and OT sites

Network topology with remote location (offices + OT sites) is very common for manufacturing, critical infrastructure, and energy companies. The OT site presents a security challenge due to its environmental complexity, such as legacy OSes, non-standard devices and protocols, and so on.



In this scenario, follow these best practice recommendations:

- Deploy a single FortiDeceptor appliance and connect it to the network via trunk to cover most of the HQ network VLANs.
- Deploy decoys following the best practice recommendation in [Deception decoy best practices on page 144](#).
 - On data center VLANs: 5-7 decoys per VLAN.
 - On endpoint VLANs: 2-4 decoys per VLAN.

- Deploy deception lures across all manageable endpoints even if some of them are in remote sites.
 - RDP
 - SMB
 - Cached credentials
 - HoneyDocs
 - SSH (on IT department desktops only)
- Fabric integration.
 - If you have FortiGate, consider the integration value between FortiDeceptor and FortiGate for alert mitigation by isolating the infected machine.
 - Send SYSLOG to SIEM or any logger solution in place.
 - Send SYSLOG to SOAR solution for Deception playbooks. For example, FortiSOAR has pre-built deception playbooks for FortiDeceptor.

Attack vectors vs deception

This section shows the best practices for attack vectors vs deception.

[Compromised internal endpoint using lateral movement on page 154](#)

[Lateral movement based on AD mapping on page 156](#)

[Lateral movement based on Mimikatz / PTH on page 157](#)

Compromised internal endpoint using lateral movement

This scenario shows a human attacker trying to compromise an internal endpoint using lateral movements.

Attack vector scenario

An attacker uses a phishing email to compromise the internal user and get access to an internal endpoint.

The attacker then explores the compromised endpoint and collect intelligence on the network before running any privileged escalation or lateral movement.

Attacker's possible first steps on the compromised endpoint:

- Use network commands to understand the network environment and the endpoint location, such as getting information on critical servers and sensitive application locations.
- Access the local / network drive to find information like sensitive files, credentials, and more. The attacker is building the lateral movement route.
- Extract / dump saved password from Windows Credential Manager, browser, or memory, whether in clear text or hashed.

Deception layer

Use SMB deception lures that generate fake network drive fronts with a file server decoy with fake files. The fake network drive configuration is hidden to avoid users from opening it and generating false alerts. Keep in mind that the

SMB lure also inserts fake credentials to the Windows credentials manager as well.

Use RDP deception lures that store saved usernames and passwords in the Windows Credential Manager that provides access to a Windows / Linux server decoy.

Use Cached credentials lures that inject saved usernames and passwords in the Windows memory to detect attacks using password dump like Mimikatz. Use a real domain user with IP restrictions.

Early breach detection

Since most users store data on the network drive, when an attacker finds that the compromised endpoint has a local disk and network drive, the attacker will likely access the fake network drive and generate alerts.

Attackers might use a tool like MIMIKATZ to extract clear-text password. An attacker engaging with a decoy using the extracted password generates alerts.

Alert details

The FortiDeceptor console presents the alert as a kill chain flow and presents a profile of the attacker. The alert data includes:

- Attacker username.
 - One of the most critical indicators that provide a quick answer regarding the attacker, attack stage, and phase.
 - A standard user means that the attacker / attack is in the early stage. Admin-level credentials means that the attacker / attack is in the privilege escalation phase or the attack was directed against high profile users from the IT department.
- Compromised IP address.
 - This is a critical indicator that points directly to the compromised host. Early detection prevents more persistent points by the attacker.
- Data that has been accessed by the attacker.
 - To see what data an attacker wants to access and steal, one way is to deploy interesting fake data that resembles your organization's real data.
 - Another way is to deploy a decoy file server with a structure that contains at least ten fake directories that resemble your organization's real server.
 - You can monitor what data the attacker accesses or copies to assess the attacker's goal.
- Malicious binary.
 - For example, if the attacker engages with a decoy over RDP, the attacker will likely use malicious code to get more persistent and privilege access. So having malicious binary as a piece of evidence with the full binary analysis helps IOC look across the network for more compromised endpoints. You can use an IOC scanner or AV/EDR API to find the indicators across network endpoints and servers.

ECO system flow:

- Send alerts to your SIEM solution.
- Use your FortiGate Fabric integration to isolate the compromised endpoint from the network.
- Deploy more decoys on the isolated segment to keep monitoring the compromised endpoint.

Lateral movement based on AD mapping

This scenario shows a human attacker trying to compromise an internal endpoint using lateral movements based on AD mapping.

Attack vector scenario

An attacker uses a phishing email to compromise the internal user and get access to an internal endpoint.

The attacker uses the compromised user credentials to passively map the network and collect information without generating network noise.

The attacker uses the compromised user credentials to run LDAP queries against the AD to retrieve asset inventory since all users have read-only access on AD objects.

Leveraging the AD asset inventory saves the attacker from running active port scan mapping that generates network noise that can expose his malicious activity.

Attacker's toolkit for AD attack:

- PS script or LDAP query command tools to extract company endpoint and server assets.
- Analyze the hostname to find assets where the hostname reflects their role or dev / test servers that might not be protected like the rest of the network.

Deception layer

- Deploy Windows decoys and add them to the network Domain
- Add DNS A record using attractive hostnames for all domain decoys' IP address. Each decoy supports up to 24 IPs.
- Use SMB deception lures that generate a fake network drive share on the endpoint that mapped front a file server decoy with fake files. The fake network drive configuration is hidden to prevent users from opening it and generating false alerts. Keep in mind that the SMB lure also inserts fake credentials to the Windows credentials manager as well.
- Use RDP deception lures that store saved usernames and passwords in the Windows Credential Manager that provides access to a Windows / Linux server decoy.
- Use Cached credentials lures that inject saved usernames and passwords in the Windows memory to detect attacks using password dump like Mimikatz. Use a real domain user with IP restrictions.

Early breach detection

When the attacker retrieves asset inventory from the AD and starts probing the attractive servers based on their hostname or the fake network connection, these activities generate alerts.

Alert details

The FortiDeceptor console presents the alert as a kill chain flow and presents a profile of the attacker. The alert data includes:

- Attacker username.
 - One of the most critical indicators that provide a quick answer regarding the attacker, attack stage, and phase.

- A standard user means that the attacker / attack is in the early stage. Admin-level credentials means that the attacker / attack is in the privilege escalation phase or the attack was directed against high profile users from the IT department.
- Compromised IP address.
 - This is a critical indicator that points directly to the compromised host. Early detection prevents more persistent points by the attacker.
- Malicious binary.
 - For example, if the attacker engages with a decoy over RDP, the attacker will likely use malicious code to get more persistent and privilege access. So having malicious binary as a piece of evidence with the full binary analysis helps IOC look across the network for more compromised endpoints. You can use an IOC scanner or AV/EDR API to find the indicators across network endpoints and servers.

ECO system flow:

- Send alerts to your SIEM solution.
- Use your FortiGate Fabric integration to isolate the compromised endpoint from the network. FortiDeceptor offers more fabric connectors for isolation.
- Deploy more decoys on the isolated segment to keep monitoring the compromised endpoint.

Lateral movement based on Mimikatz / PTH

This scenario shows a human attacker trying to compromise an internal endpoint using lateral movements based on Mimikatz / PTH.

Attack vector scenario

An attacker uses a phishing email to compromise the internal user and get access to an internal endpoint.

The attacker looks for any powerful user in the compromised endpoint.

The attacker / APT uses an advanced tool like Mimikatz to run several attacks to extract clear text passwords from memory or Windows Credential Manager, AD Kerberos tickets, Windows local hash, and so on.

The Mimikatz tool's goal is to get administrator-level permission and run in-depth lateral movement across the network.

Attacker's toolkit:

- Tools like Mimikatz, Meterpreter, password dump, and so on.
- Leverage services like RDP, RPC, WMI, VNC, SSH, and WINRM for lateral movement.

Deception layer

- Deploy Windows decoys and add them to the network Domain.
- Add DNS A record using attractive hostnames for all domain decoys' IP addresses. Each decoy supports up to 24 IPs.
- Use SMB deception lures that generate a fake network drive share on the endpoint that mapped front a file server decoy with fake files. The fake network drive configuration is hidden to prevent users from opening it and generating false alerts. Keep in mind that the SMB lure also inserts fake credentials to the Windows Credential Manager as well.

- Use RDP deception lures that store saved usernames and passwords in the Windows Credential Manager that provides access to a Windows / Linux server decoy.
- Use Cached credentials lures that inject saved usernames and passwords in the Windows memory to detect attacks using password dump like Mimikatz. Use a real domain user with IP restrictions.

Early breach detection

An attacker using fake credentials in the sRDP lure to engage with a decoy generates alerts.

An attacker engaging with a real asset using the fake username and password (in the cache credential lure) generate an alert on the SIEM solution. This requires a SIEM correlation rule.

Alert details

The FortiDeceptor console presents the alert as a kill chain flow and presents a profile of the attacker. The alert data includes:

- Attacker username.
 - One of the most critical indicators that provide a quick answer regarding the attacker, attack stage, and phase.
 - A standard user means that the attacker / attack is in the early stage. Admin-level credentials means that the attacker / attack is in the privilege escalation phase or the attack was directed against high profile users from the IT department.
- Compromised IP address.
 - This is a critical indicator that points directly to the compromised host. Early detection prevents more persistent points by the attacker.
- Malicious binary.
 - For example, if the attacker engages with a decoy over RDP, the attacker will likely use malicious code to get more persistent and privilege access. So having malicious binary as a piece of evidence with the full binary analysis helps IOC look across the network for more compromised endpoints. You can use an IOC scanner or AV/EDR API to find the indicators across network endpoints and servers.

ECO system flow:

- For SIEM:
 - Send alerts to your SIEM solution.
 - Create a correlation rule that creates an alert on using the fake username (cache credential lure).
- Use your FortiGate Fabric integration to isolate the compromised endpoint from the network. FortiDeceptor offers more fabric connectors for isolation.
- Deploy more decoys on the isolated segment to keep monitoring the compromised endpoint.

Deploying tokens using AD GPO logon script

FortiDeceptor generates a deception lure package based on the decoy service configuration. For example, deploying a Windows server decoy with the services RDP and SMB, and Linux desktop decoy with the services SSH and SAMBA generates a deception lure package named `FDC_TokenPKG_XXXXXXXXXX` that contains the deception lure files.

The deception lure package is a zip file that has three directories containing all the relevant data and configuration for each OS.

The deception lure for each OS uses the same concept: binary files with several JSON files that provide the decoy fake access parameters for the lure.

There are two ways to assign logon scripts. The first is on the *Profile* tab of the user properties dialog in the Active Directory Users and Computers (ADUC). The second is via Group Policy Objects (GPO).

This section provides in-depth instructions on how to deploy Windows lures using the second option via AD GPO logon script.

The main idea for the GPO logon script distribution is:

- Place the deception lure package in a network directory that is accessible to all endpoints.
- Generate a batch file that runs under the logon script and runs each time the end user logs into the network domain.
- The batch file copies the deception lure package to the endpoint and executes it.
- After execution, the endpoint has the deception lure in place.

To prepare the GPO logon script:

1. Download the deception lure package from the FortiDeceptor Admin Console.
2. Unzip the downloaded file to a temporary location.
3. Open the unzipped file and access the `windows` directory.
4. Copy all the files and directories, except `uninstall.bat`, from the `windows` directory::
 - `windows_token.exe`
 - `Config.json`
 - `res` directory (if it is there)
 - `Honeydocs` directory (if it is there)
5. On the AD server, go to `\\%UserDNSDomain%\SysVol\domain\scripts`
In this example, the domain is FDC.COM so the location is `\\FDC.COM\SysVol\FDC.COM\scripts`.
6. In the `scripts` directory, create a new directory and name it `MyFiles`.
7. Copy `windows_token.exe` and the `res` directory to the `MyFiles` directory.
8. Create a batch file named `Lure.bat` with the following commands. In this example, the domain is FDC.com.


```
set SFolder=\\FDC.COM\SysVol\FDC.COM\scripts\MyFiles
set DFolder=%UserProfile%
xcopy /E /S /H /K /F /C /Y /I "%SFolder%" "%DFolder%\MyFiles"
start /B /WAIT /MIN "windows_token" "%DFolder%\windows_token.exe" "--non-interactive"
exit
```

A similar script for token installation is:

```
set SFolder=\\FDC.COM\SysVol\FDC.COM\scripts\MyFiles
start /B /WAIT /MIN "windows_token" "%SFolder%\windows_token.exe" "--keep-files" "--non-interactive"
exit
```

Syntax example:

```
windows_token.exe "[optional command]" "<optional parameters>"...
```

Command

- (blank): The default command both uninstalls previous lures (if applicable), and installs the new lures.
- `uninstall`: Uninstalls all previous installed lures (if applicable) for the current user.

Parameters

--non-interactive: (Optional) Used with any command, this parameter prevents any user interface from being displayed while the command is being executed.

--keep-files (Optional) Keep the installation files/directories. Otherwise, all files and directories in the current folder will be wiped out.

9. (Optional) *The default installation process both uninstalls previous lures (if applicable), and installs the new lures. To uninstall tokens without installation:

- a. Copy `windows_token.exe` from the `windows` directory to the `MyFiles\Uninstall` directory.
- b. Create a batch file named `uninstall_lure.bat` with the following commands.

In the following example, the domain is *FDC.com*:

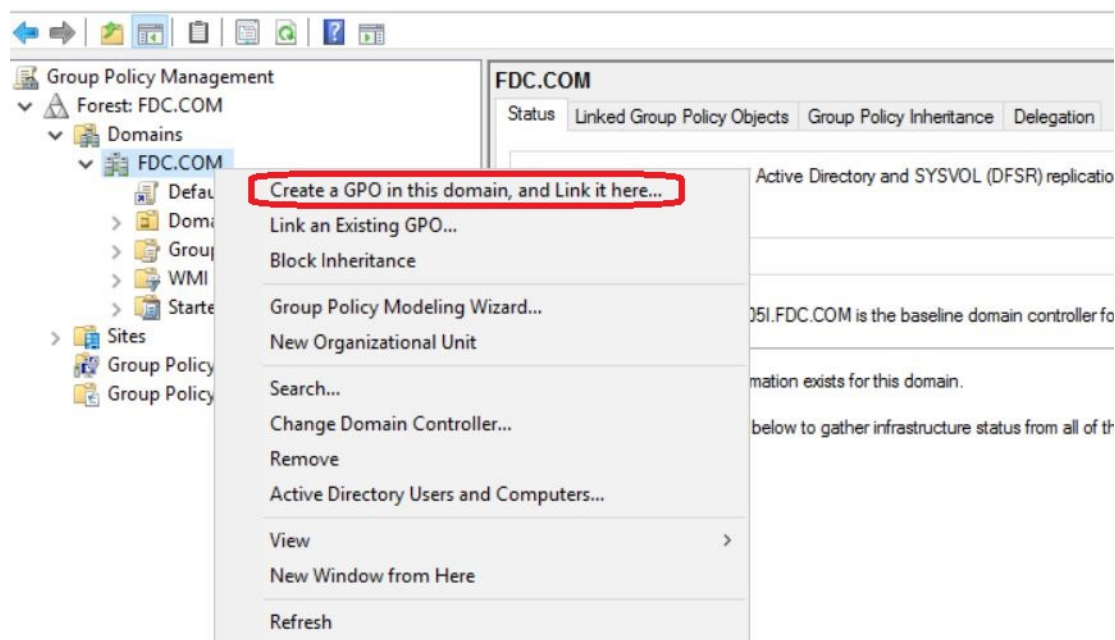
```
set SFolder=\\fdc.com\SYSVOL\fdc.com\scripts\MyFiles\Uninstall
start /B /WAIT /MIN "uninstall_windows_token" "%SFolder%\windows_token.exe"
"uninstall" "-non-interactive"
exit
```

Configuring the GPO logon script

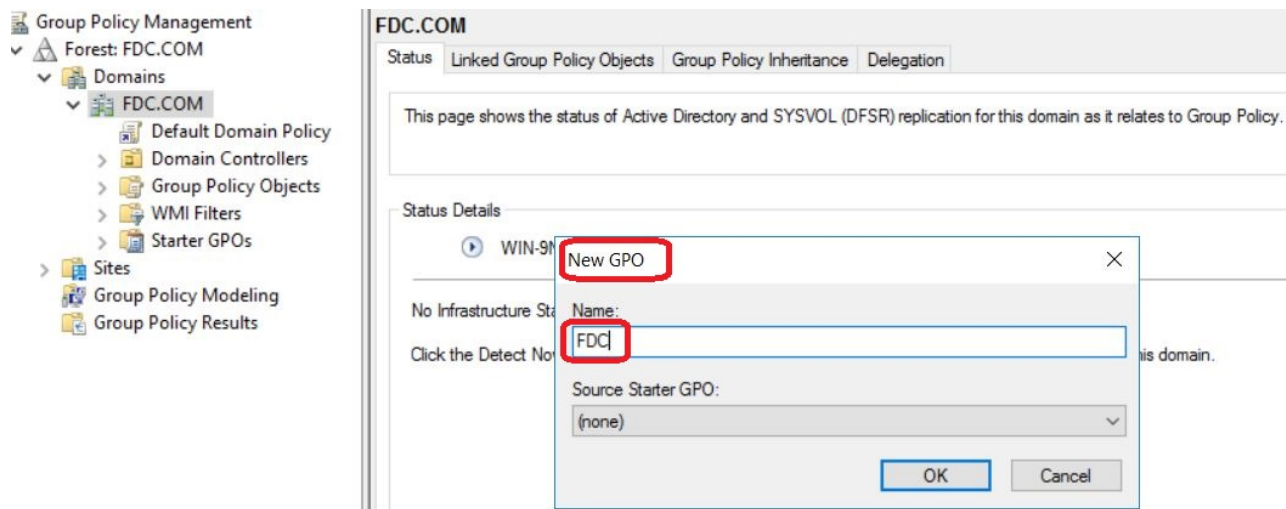
To configure the GPO logon script:

- Log into the AD server and open the Group Policy Management tool.
You can also open this tool using the CLI `gpmc.msc`.
- Right-click the top-level domain object (in this example, *FDC.COM*) and select *Create a GPO in this domain, and link it here*.

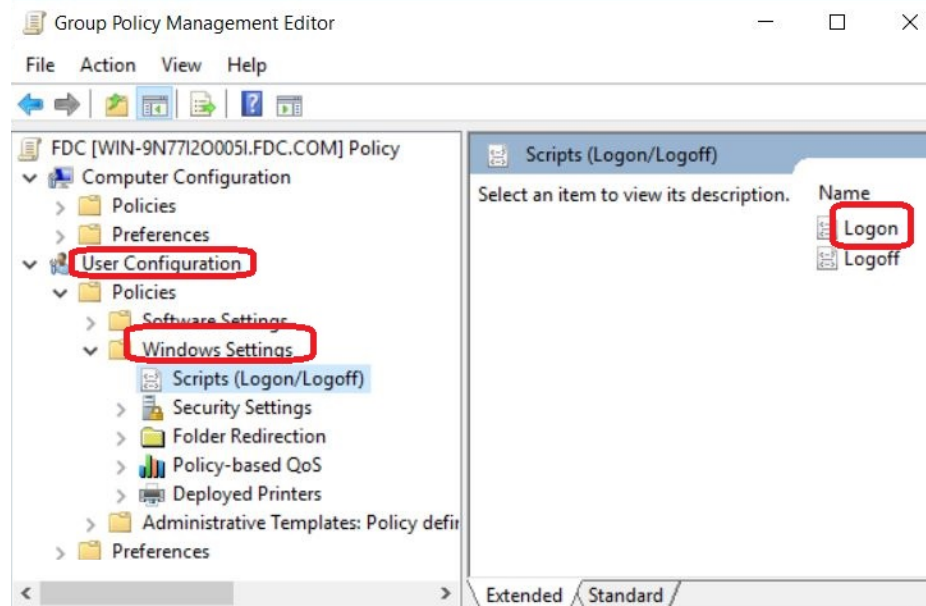
This creates a new group policy object.



- Enter a name for the new group policy object. Do not use a name that has any association with a deception technology.

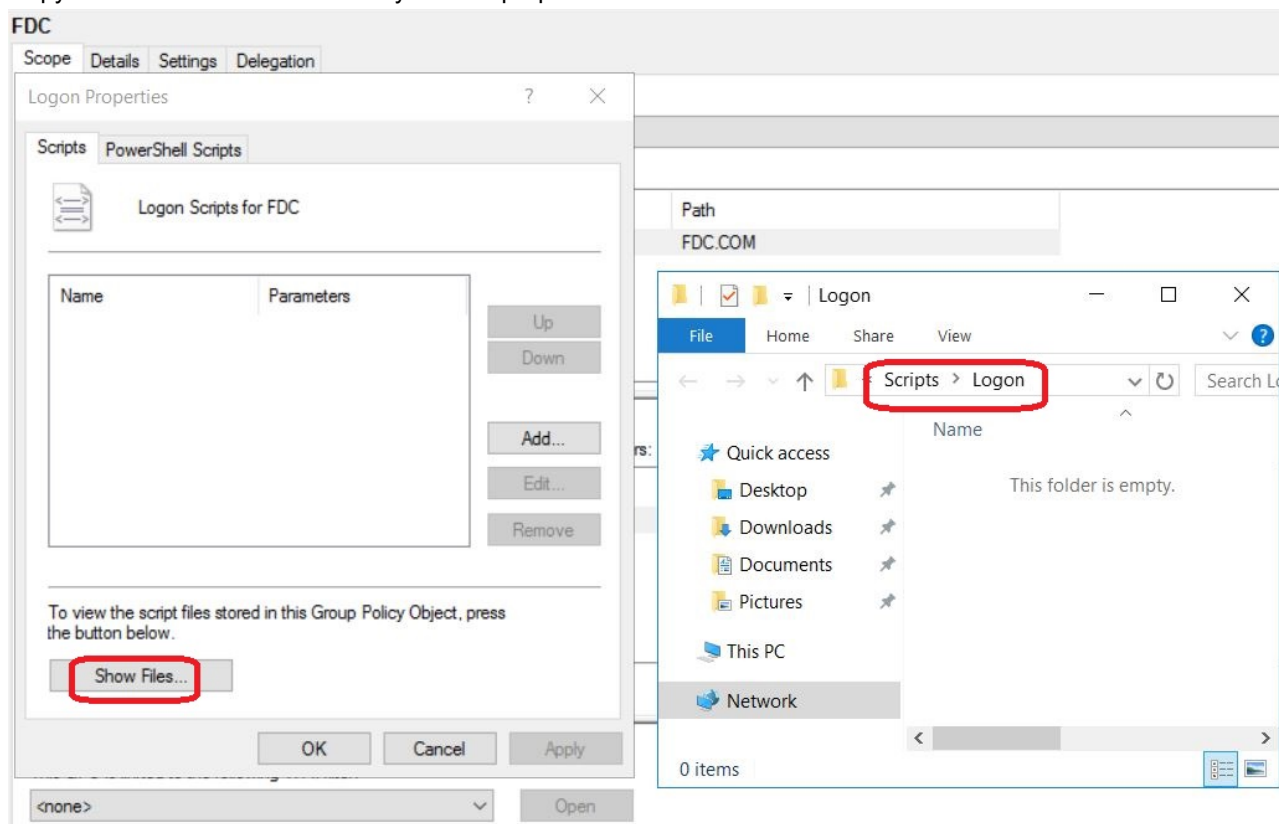


4. Right-click the new group policy object and select *Edit*.
5. Go to *User configuration > Policies > Windows Settings > Scripts (Logon/Logoff)*.
6. In the right pane, double click the *Logon* script to configure the Logon script properties.

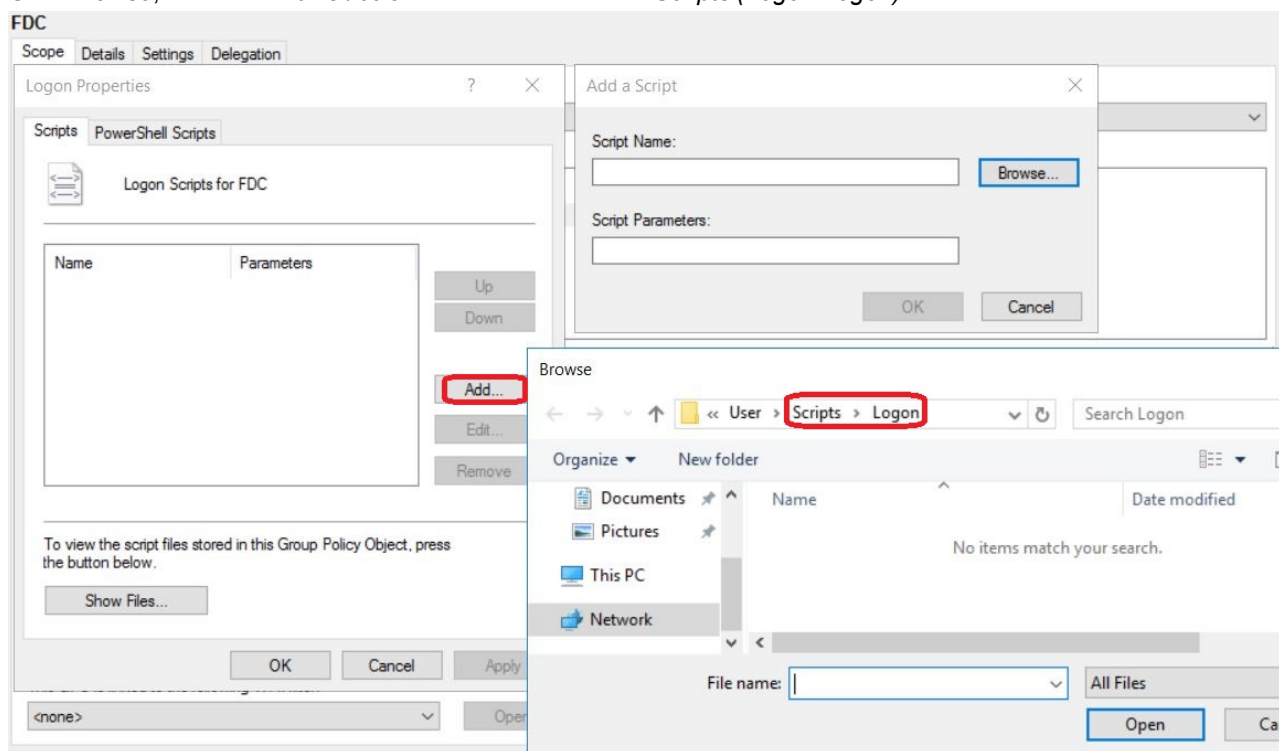


7. In the *Logon Properties* dialog box, click *Show Files*.

8. Copy the batch file `Lure.bat` that you have prepared.



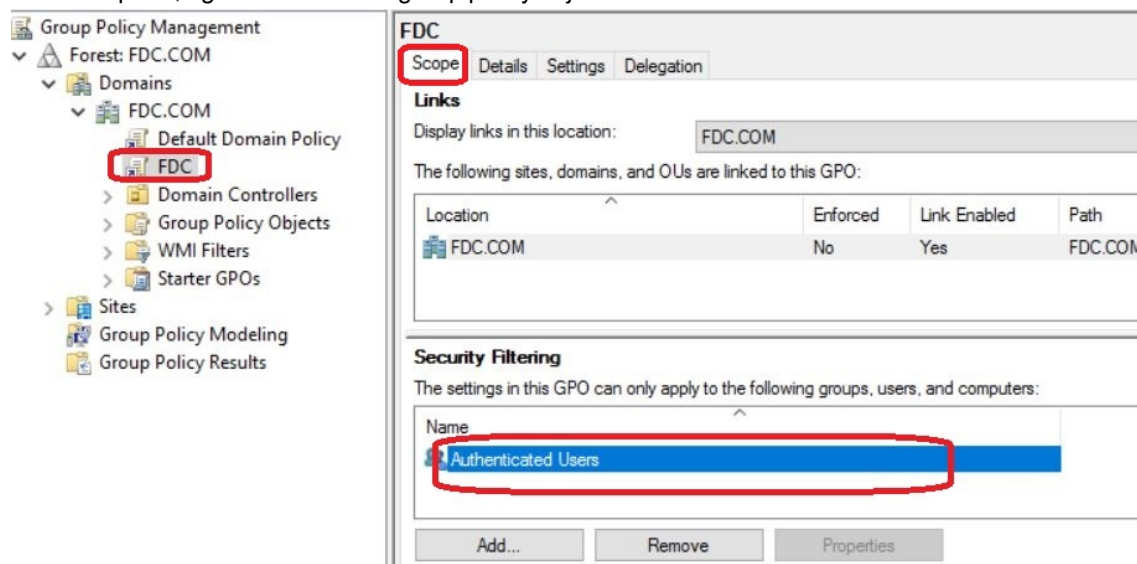
9. In the *Logon Properties* dialog box, click *Add* to open the *Add a Script* dialog box.
10. Click *Browse*, locate the `Lure.bat` batch file and add it to *Scripts (Logon/Logoff)*.



11. Click *Apply* and then click *OK* to close this window.

To enforce the group policy:

1. In the *Group Policy Management* console, select the new group policy object. In this example, *FDC.COM*.
2. In the *Scope* tab, verify that *FDC.COM* is linked.
3. In the *Security Filtering* section, add and remove the user groups to get the deception lure package through the logon script.
4. In the left pane, right-click the *FDC* group policy object and select *Enforced*.



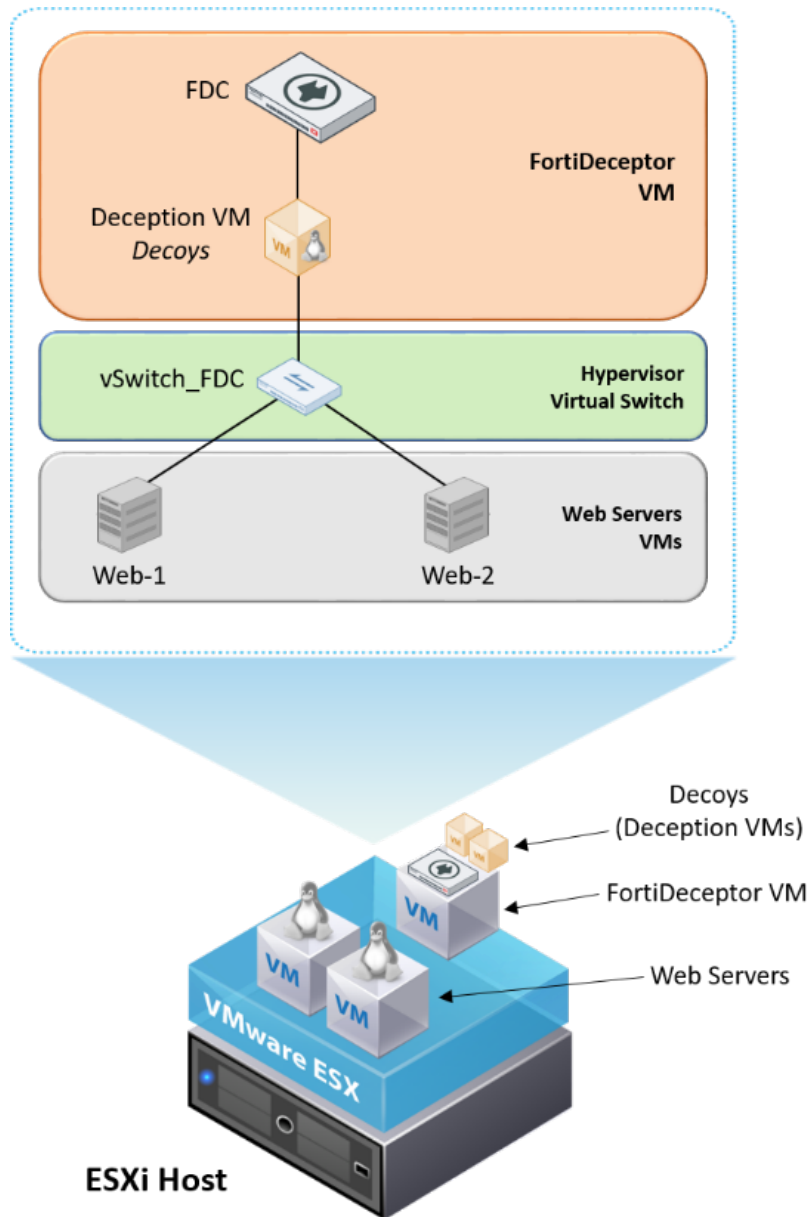
Configuring trunk ports on FortiDeceptor VM

This section describes how to configure trunk ports to extend VLANs between FortiDeceptor VM and ESXi vSwitch using a single interface.

This setup requires FortiDeceptor VM v3.1 build 0061 and vSwitch ESXi v6.7.0 build 13006603.

Set up a single ESXi host with the following workloads.

- 1 FortiDeceptor VM with one decoy monitoring two network segments.
- 2 web servers in different VLANs / network segments.
- 1 vSwitch dedicated to connecting the FortiDeceptor decoy to the network segments.



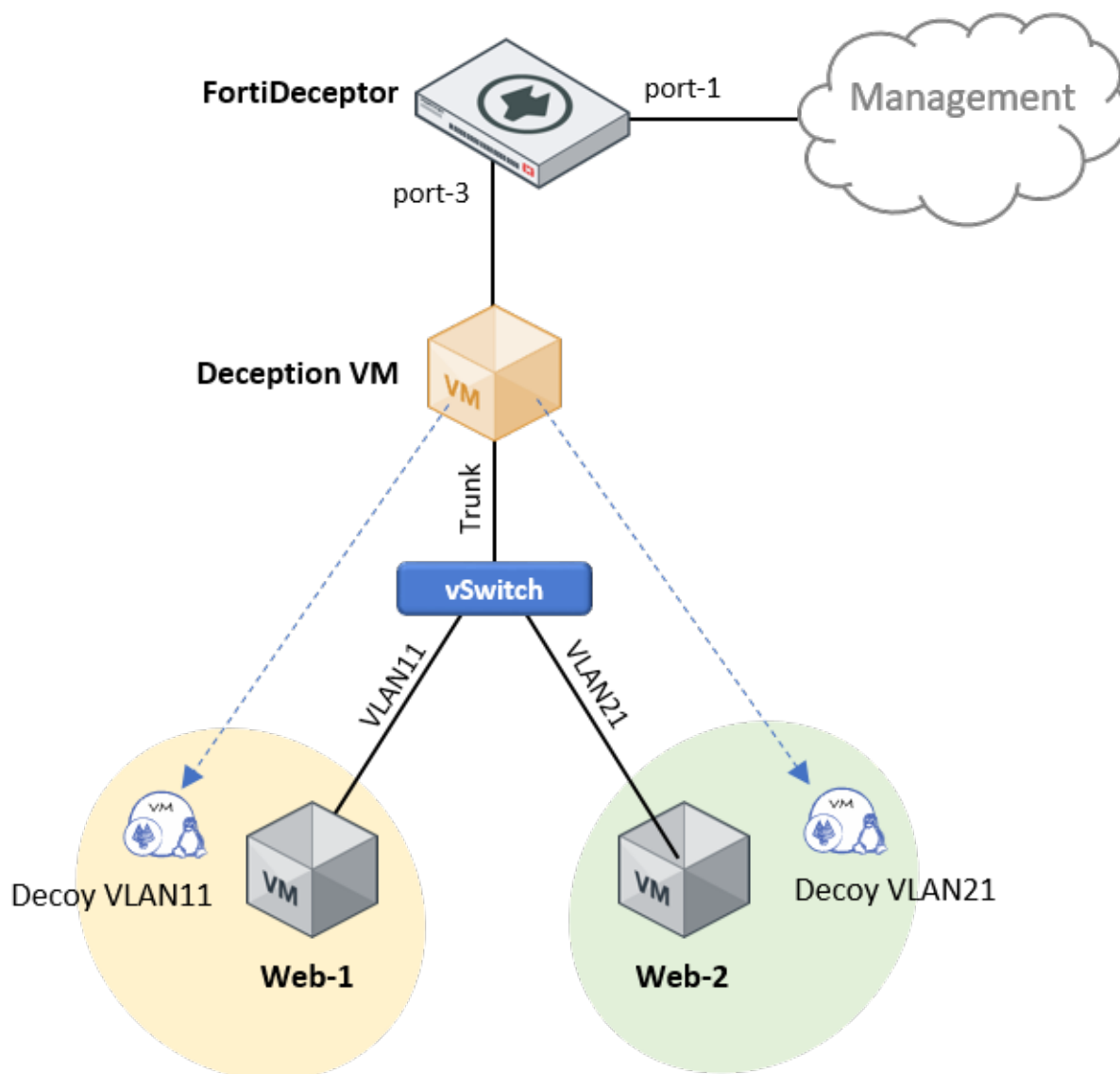
FortiDeceptor VM has internal network ports. Set up FortiDeceptor VM with the following.

- Reserve port1 for device management.
- Use the other ports to deploy deception decoys.

FortiDeceptor VM		Interfaces					admin	
What are you looking for?		Edit						
Dashboard								
Deception								
Customization								
Deception OS								
Deployment Network								
Deployment Wizard								
Decoy & Lure Status								
Decoy Map								
Whitelist								
Incident								
Fabric								
Network								
Interfaces								
		Interface	IPv4	IPv6	Interface Status	Link Status	Access Rights	
		port1 (administration port)	192.168.0.36/255.255.255.0		🟢	🟢	HTTPS,SSH	
		port2	192.168.1.9/255.255.255.0		🟢	🟢		
		port3	192.168.2.99/255.255.255.0		🟢	🟢		
		port4	192.168.3.99/255.255.255.0		🟢	🟢		
		port5	192.168.4.99/255.255.255.0		🟢	🟢		
		port6	192.168.5.99/255.255.255.0		🟢	🟢		

When you initially set up FortiDeceptor, the interface configuration in *Network > Interfaces* is provisioned automatically. You do not need to change this section as these network settings are just for internal use. The actual deception network interfaces that connect to the monitored segments are configured under *Deception > Deployment Network*.

In this environment, port3 is used to deploy a Linux-based deception VM (decoy). The goal is to monitor network activity in two different VLANs where the production servers reside: WebServer-1 (192.168.11.11/24) in VLAN11 and WebServer-2 (192.168.21.21/24) in VLAN21.



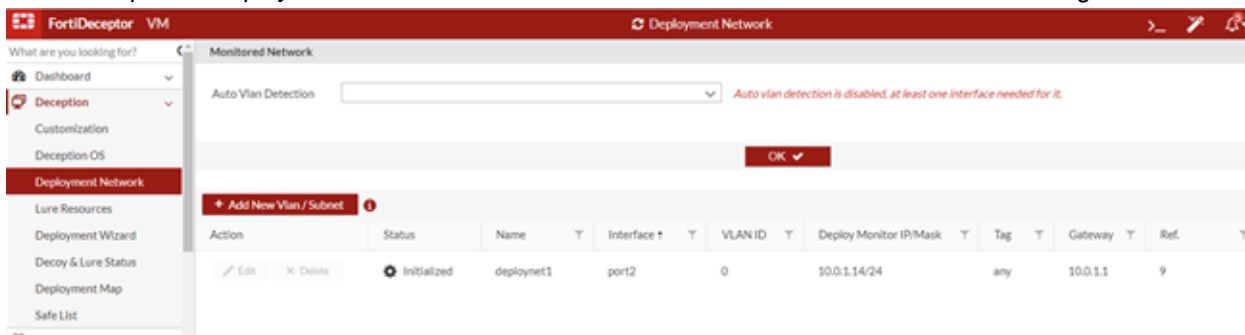
The deception VM has a single network interface to monitor two different VLANs so it is necessary to configure VLAN trunking between port3 and the ESXi vSwitch port. There is only one vSwitch to connect all the devices together using different virtual ports for each device.

Configuring FortiDeceptor

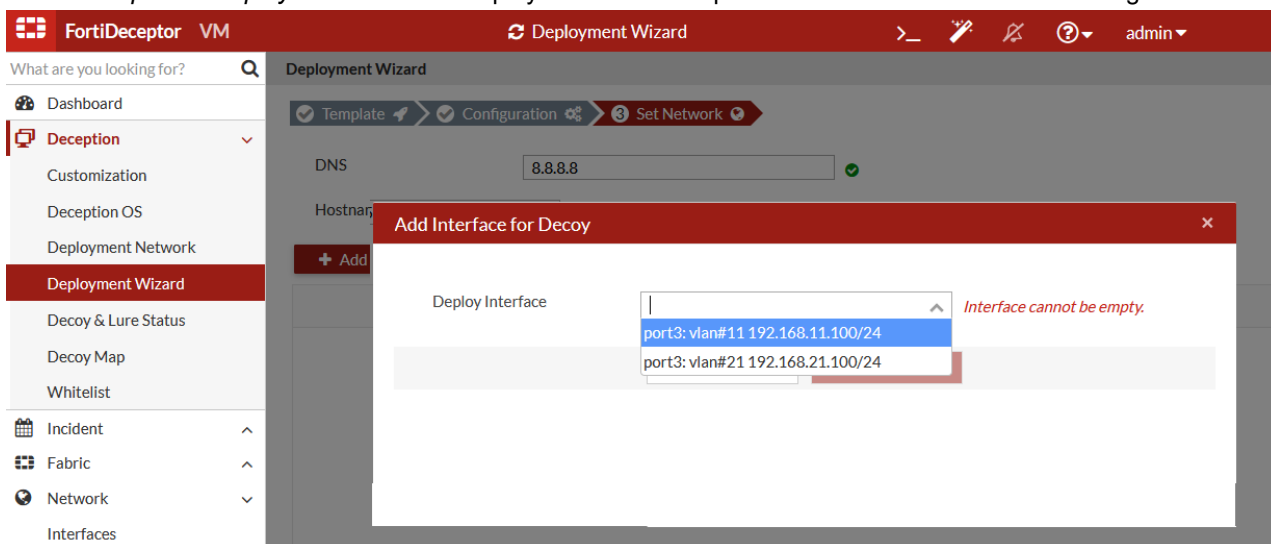
Configure FortiDeceptor to monitor the subnet networks, one for each VLAN, using the same network port3.

To configure FortiDeceptor:

1. Go to *Deception > Deployment Network* and click *Add New Vlan / Subnet* to add the monitored segments.

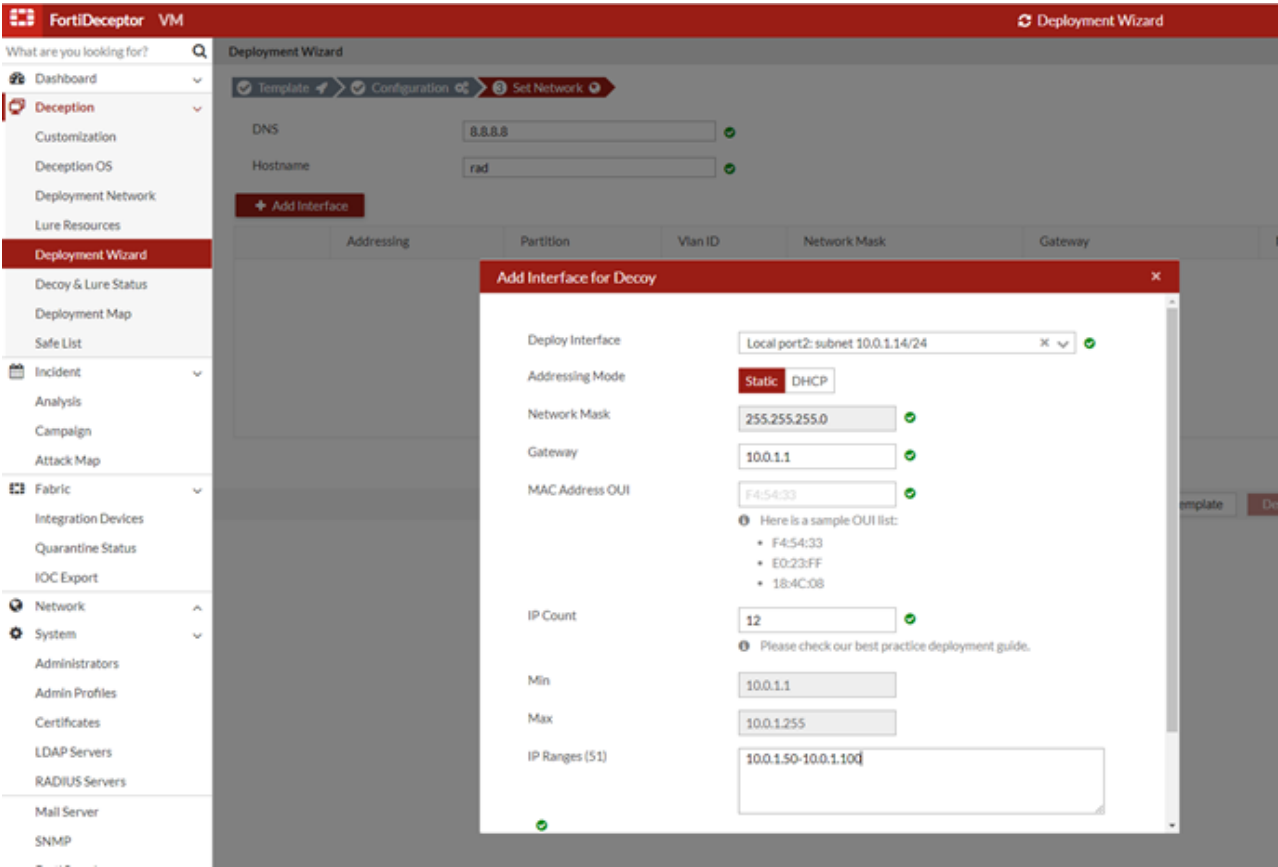


2. Use the VLAN tag for each monitored subnet so that FortiDeceptor can differentiate the traffic between them. Verify that both VLANs use port3.
3. Specify the *Deploy Network IP/Mask* that the deception VM use to monitor its decoys on each segment. Ensure these IP addresses are unique and belong to the monitored subnets.
4. Go to *Deception > Deployment Wizard* to deploy the actual deception VM and attach the monitored segments.

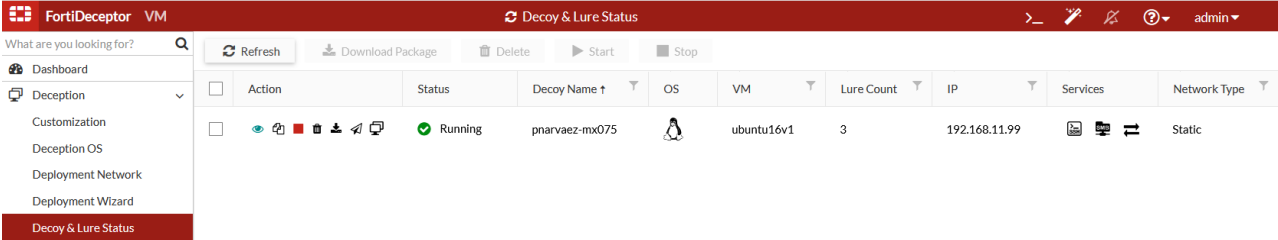


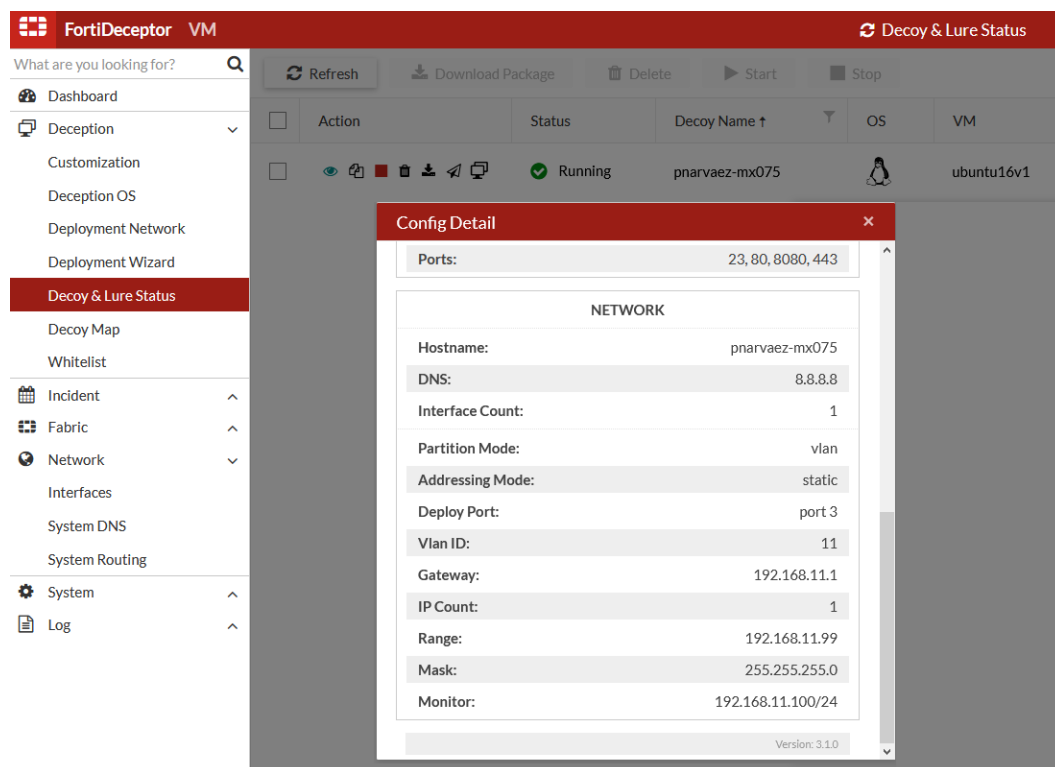
5. Specify the network settings for the decoys.
FortiDeceptor automates the creation of deception VMs and decoy services to lure and expose attackers; so decoy services on each segment require dedicated IP addresses to interact with attackers.

If you want to use a static IP address for the decoy services, click *Static*, then specify a single IP address or IP address range in *IP Ranges*.

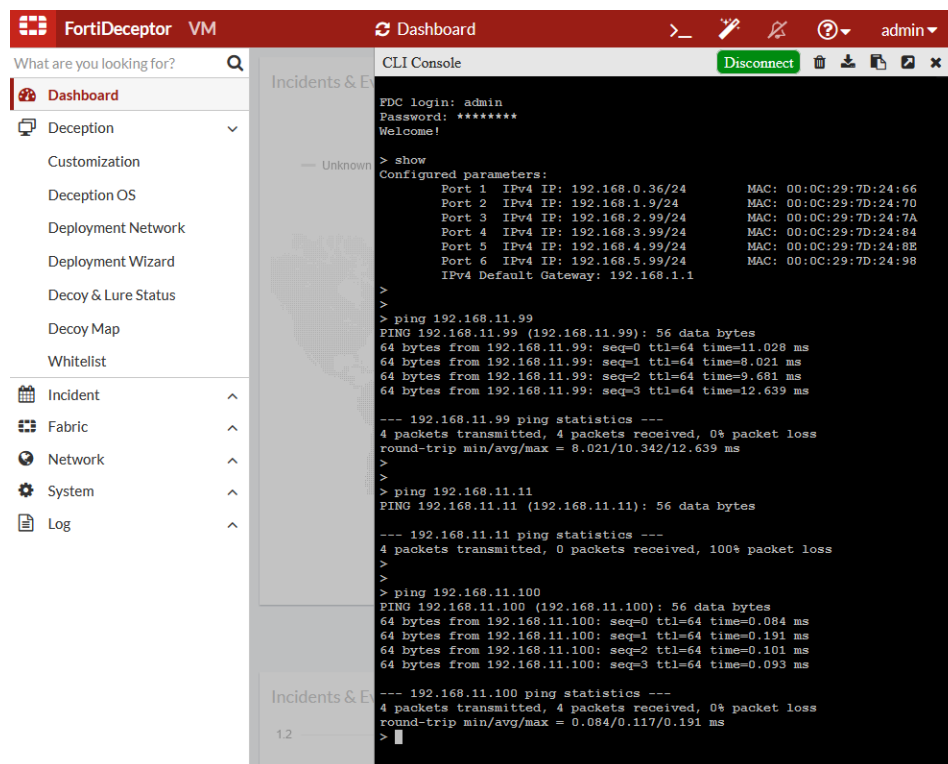


6. After completing VM deployment, go to *Decoy & Lure Status* to validate the configuration.





- Test connectivity by pinging the decoy and the monitoring IP addresses and verify that they are reachable. The web servers are not reachable as ESXi is not configured yet.



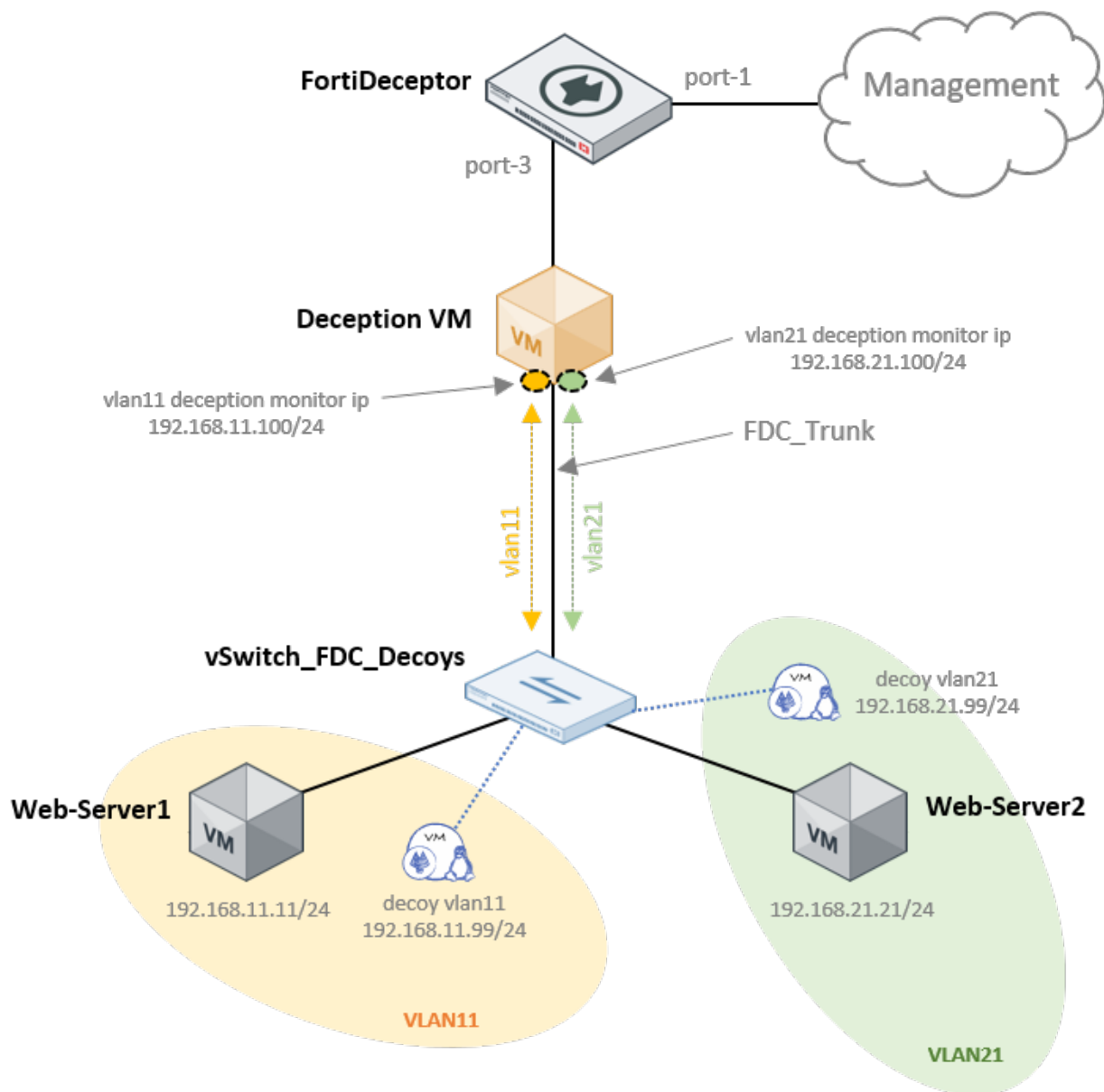
From the networking perspective, FortiDeceptor is ready to monitor both VLANs over port3. However, to activate the logical trunk interface, FortiDeceptor needs to receive VLAN trunking traffic from the vSwitch port.

If you have a physical switch connected to the ESXi host, you must configure 802.1Q on the switch port that is connected to the host uplink.

Configuring the vSwitch

To simplify configuration, we recommend using a dedicated vSwitch for the decoy and monitored segments.

The following diagram shows the vSwitch ports relationship.





On ESXi, configure the `vSwitch_FDC_Decoys` vSwitch to connect both VLANs to FortiDeceptor. Then configure three network port-groups:

1. `FDC_Trunk` – Port-group for the actual trunk interface between FortiDeceptor and vSwitch.
2. `VLAN11` – Port-group to connect VLAN11 to vSwitch.
3. `VLAN21` – Port-group to connect VLAN21 to vSwitch.

To configure the vSwitch:


1. On the ESXi client, go to *Networking > Virtual Switches* and add a standard virtual switch. Just configure the *vSwitch Name*, remove the uplink (unless you need it), and use default values for the other options.

 **Add standard virtual switch - vSwitch_FDC_Decoys.**

 **Add uplink**

vSwitch Name	<input type="text" value="vSwitch_FDC_Decoys."/>
MTU	<input type="text" value="1500"/>
▶ Link discovery	Click to expand
▶ Security	Click to expand

2. Go to *Networking > Port groups* and add the port groups. Port groups for VLAN11 and VLAN21 are similar. For each port group, specify a *Name*, configure the *VLAN ID*, and select the *Virtual switch*.


 **Add port group - VLAN11.**

Name	<input type="text" value="VLAN11."/>
VLAN ID	<input type="text" value="11"/>
Virtual switch	<input type="text" value="vSwitch_FDC_Decoys"/>
▶ Security	Click to expand

3. For the FDC Trunk port, configure a special port-group.

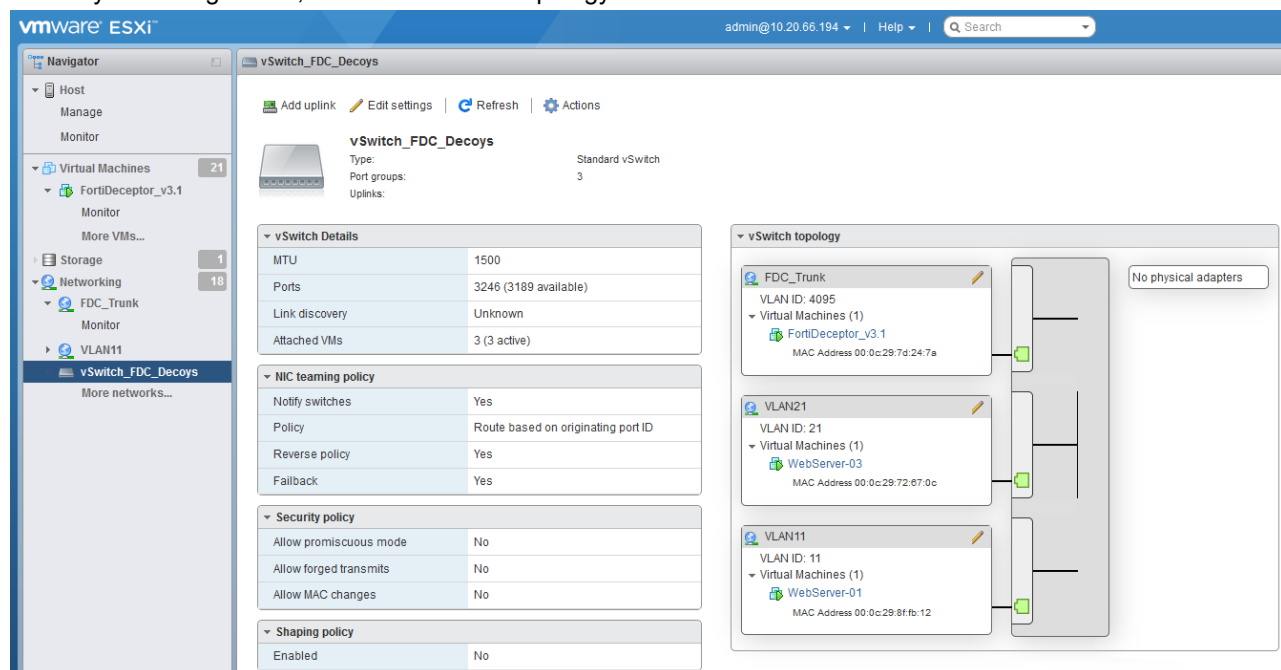
On ESXi, you do not need to configure 802.1Q. You only need to set the port group to be a promiscuous interface and specify 4095 for the *VLAN ID* so the vSwitch can send and receive traffic from the VLANs configured on FortiDeceptor.

Select the *Virtual switch* and set all *Security* options to *Accept*.

 Add port group - FDC_Trunk.

Name	FDC_Trunk.
VLAN ID	4095
Virtual switch	vSwitch_FDC_Decoys
▼ Security	
Promiscuous mode	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
MAC address changes	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
Forged transmits	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch

4. To verify the configuration, check the vSwitch topology and ensure all devices are connected to this switch.



The screenshot shows the VMware ESXi interface for configuring and verifying the vSwitch_FDC_Decoys. The left sidebar shows the navigation tree with 'vSwitch_FDC_Decoys' selected under 'Networking'. The main panel displays the vSwitch configuration details, including MTU (1500), Ports (3246), and attached VMs (3 active). The 'vSwitch topology' section on the right shows the connection diagram, including the FDC_Trunk port group (VLAN ID: 4095) and three virtual machines (VLAN ID: 21, 11, and 10) connected to the vSwitch. The 'Security policy' section shows that promiscuous mode, MAC address changes, and forged transmits are all set to 'No'.

5. Test connectivity from FortiDeceptor to the web servers, and from each web server to the decoys connected to the same VLAN.

- From FortiDeceptor.

The screenshot shows the FortiDeceptor VM interface with the CLI Console open. The console displays the login process and three ping tests performed from the FortiDeceptor to web servers at 192.168.11.100, 192.168.11.99, and 192.168.11.11. All tests show 0% packet loss and successful round-trip times.

```

FortiDeceptor VM Dashboard
What are you looking for?
Dashboard
Deception
Customization
Deception OS
Deployment Network
Deployment Wizard
Decoy & Lure Status
Decoy Map
Whitelist
Incident
Fabric
Network
System
Log

CLI Console
Disconnect
FDC login: admin
Password: *****
Welcome!

> ping 192.168.11.100
PING 192.168.11.100 (192.168.11.100): 56 data bytes
64 bytes from 192.168.11.100: seq=0 ttl=64 time=0.102 ms
64 bytes from 192.168.11.100: seq=1 ttl=64 time=0.075 ms
64 bytes from 192.168.11.100: seq=2 ttl=64 time=0.079 ms
64 bytes from 192.168.11.100: seq=3 ttl=64 time=0.085 ms

--- 192.168.11.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.075/0.085/0.102 ms
>
> ping 192.168.11.99
PING 192.168.11.99 (192.168.11.99): 56 data bytes
64 bytes from 192.168.11.99: seq=0 ttl=64 time=15.623 ms
64 bytes from 192.168.11.99: seq=1 ttl=64 time=11.914 ms
64 bytes from 192.168.11.99: seq=2 ttl=64 time=12.291 ms
64 bytes from 192.168.11.99: seq=3 ttl=64 time=12.310 ms

--- 192.168.11.99 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 11.914/13.034/15.623 ms
>
> ping 192.168.11.11
PING 192.168.11.11 (192.168.11.11): 56 data bytes
64 bytes from 192.168.11.11: seq=0 ttl=64 time=2.814 ms
64 bytes from 192.168.11.11: seq=1 ttl=64 time=1.908 ms
64 bytes from 192.168.11.11: seq=2 ttl=64 time=1.448 ms
64 bytes from 192.168.11.11: seq=3 ttl=64 time=6.773 ms

--- 192.168.11.11 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.448/3.235/6.773 ms
>

```

- From web server 1.

The screenshot shows a terminal window on a web server (Web1) with the IP 192.168.11.99. It displays two ping tests: one to the FortiDeceptor at 192.168.11.99 and another to a web server at 192.168.11.100. Both tests show 0% packet loss and successful round-trip times.

```

fortinet@Web1:~$
fortinet@Web1:~$ ping 192.168.11.99
PING 192.168.11.99 (192.168.11.99) 56(84) bytes of data.
64 bytes from 192.168.11.99: icmp_seq=1 ttl=64 time=12.3 ms
64 bytes from 192.168.11.99: icmp_seq=2 ttl=64 time=43.2 ms
64 bytes from 192.168.11.99: icmp_seq=3 ttl=64 time=12.5 ms
64 bytes from 192.168.11.99: icmp_seq=4 ttl=64 time=12.6 ms
64 bytes from 192.168.11.99: icmp_seq=5 ttl=64 time=12.0 ms
^C
--- 192.168.11.99 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4017ms
rtt min/avg/max/mdev = 12.077/18.577/43.294/12.360 ms
fortinet@Web1:~$
fortinet@Web1:~$ ping 192.168.11.100
PING 192.168.11.100 (192.168.11.100) 56(84) bytes of data.
64 bytes from 192.168.11.100: icmp_seq=1 ttl=64 time=1.72 ms
64 bytes from 192.168.11.100: icmp_seq=2 ttl=64 time=0.894 ms
64 bytes from 192.168.11.100: icmp_seq=3 ttl=64 time=2.14 ms
64 bytes from 192.168.11.100: icmp_seq=4 ttl=64 time=1.15 ms
64 bytes from 192.168.11.100: icmp_seq=5 ttl=64 time=1.32 ms
^C
--- 192.168.11.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.894/1.448/2.146/0.440 ms
fortinet@Web1:~$

```

How to setup and use LDAP/RADIUS servers

1. Set up the LDAP server

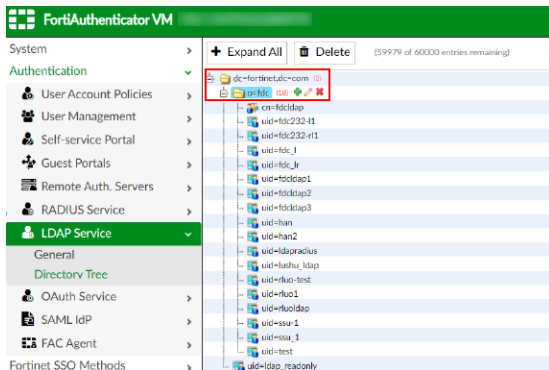
Requirements:

- FortiAuthenticator login credentials

To set up the LDAP server:

1. In FortiDeceptor Go to *System > LDAP Servers*.
2. Click *Create New*. The *New LDAP Server* window opens.
3. Configure the LDAP server settings, see [LDAP Servers on page 94](#).

You must use the following format for the *Distinguished Name* field :<root_node>,<subordinate_node>. To find the names of the Root and Subordinate nodes in FortiAuthenticator, by go to *LDAP Service > Directory Tree*.



Setup the RADIUS server

Requirements:

- FortiAuthenticator login credentials

To set up the RADIUS server in FortiDeceptor:

1. Go to *System > RADIUS Servers*.
2. Click *Create New*. The *New RADIUS Server* window opens.

3. Configure the RADIUS server settings. See [RADIUS Servers on page 95](#).



In the *Primary Secret* field enter, *fortinet*.

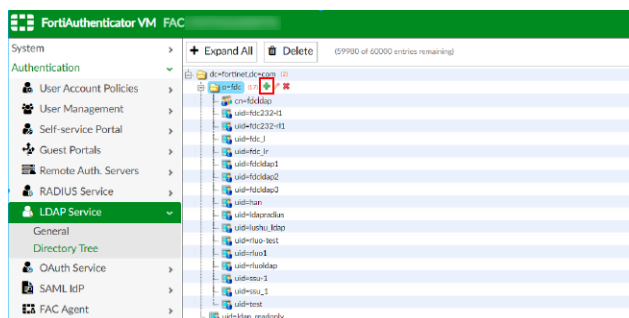
3. Create an account in FortiAuthenticator and enable LDAP/RADIUS

You do not need to complete this step if you already have a FortiAuthenticator account.

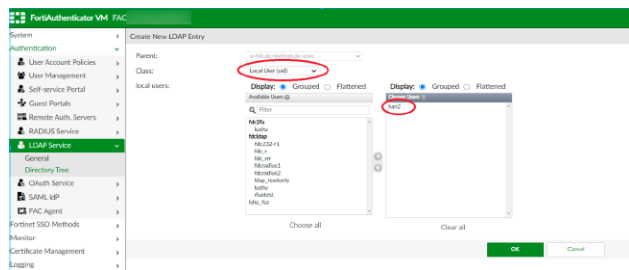
To enable LDAP/RADIUS:

1. In FortiAuthenticator, go to *User Management > Local Users* and create a new account.
 - a. Enable *Allow RADIUS authentication*.
 - b. In the *Password* and *Password confirmation* fields, enter *fortinet*.

2. Go *LDAP Service > Directory Tree* to enable LDAP.
3. Expand the Root node, and then click the green plus symbol next to the Subordinate node. The *Create New LDAP entry* window opens.



4. From the *Class* dropdown, select *Local User (uid)*.



5. Go to *User Management > Local Users* to verify the RADIUS and LDAP servers are enabled. To do this, check that the *Authentication Methods* column shows *RADIUS and LDAP*.

Username	First name	Last name	Email address	Status	Type	Value	Value Required	Group	Authentication Methods
admin				✓	Local User		✓		RADIUS and LDAP
admin1				✓	Local User		✓		RADIUS and LDAP
admin2				✓	Local User		✓		RADIUS and LDAP
admin3				✓	Local User		✓		RADIUS and LDAP
admin4				✓	Local User		✓		RADIUS and LDAP
admin5				✓	Local User		✓		RADIUS and LDAP
admin6				✓	Local User		✓		RADIUS and LDAP
admin7				✓	Local User		✓		RADIUS and LDAP
admin8				✓	Local User		✓		RADIUS and LDAP
admin9				✓	Local User		✓		RADIUS and LDAP
admin10				✓	Local User		✓		RADIUS and LDAP
admin11				✓	Local User		✓		RADIUS and LDAP
admin12				✓	Local User		✓		RADIUS and LDAP
admin13				✓	Local User		✓		RADIUS and LDAP
admin14				✓	Local User		✓		RADIUS and LDAP
admin15				✓	Local User		✓		RADIUS and LDAP
admin16				✓	Local User		✓		RADIUS and LDAP
admin17				✓	Local User		✓		RADIUS and LDAP
admin18				✓	Local User		✓		RADIUS and LDAP
admin19				✓	Local User		✓		RADIUS and LDAP
admin20				✓	Local User		✓		RADIUS and LDAP

4. Create login account using LDAP/RADIUS accounts from FortiAuthenticator

To create a login account with LDAP/RADIUS:

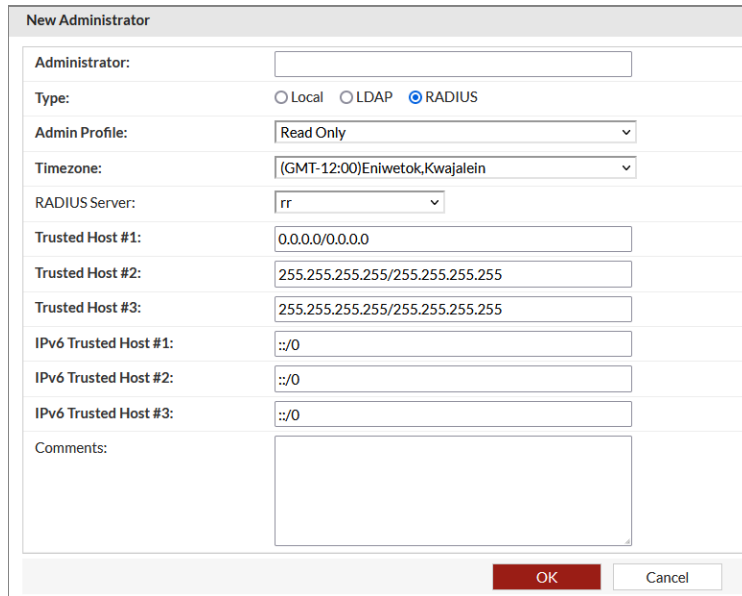
1. In FortiAuthenticator, go to *User Management > Local Users* and locate an account that has LDAP/RADIUS enabled. To do this, look in the *Authentication Methods* column for *RADIUS and LDAP*.
2. In FortiDeceptor, go to *System > Administrators* and click + *Create New* to create a new administrator. The *New Administrator* window opens.
3. Configure the administrator settings.



The values for the *Administrator*, *Type*, and *LDAP Server* fields must match the user's settings in FortiAuthenticator.

4. Log in to FortiDeceptor with the administrator account you created.
5. Go to *System > Administrators* and click + *Create New*. The *New Administrator* window opens.

6. Create a new administrator and set the *Type* to *RADIUS*.



The image shows a 'New Administrator' configuration window. It contains the following fields and options:

- Administrator:** A text input field.
- Type:** Radio buttons for ☐ Local, ☐ LDAP, and ☒ RADIUS.
- Admin Profile:** A dropdown menu with 'Read Only' selected.
- Timezone:** A dropdown menu with '(GMT-12:00)Eniwetok,Kwajalein' selected.
- RADIUS Server:** A dropdown menu with 'rr' selected.
- Trusted Host #1:** A text input field with '0.0.0.0/0.0.0.0'.
- Trusted Host #2:** A text input field with '255.255.255.255/255.255.255.255'.
- Trusted Host #3:** A text input field with '255.255.255.255/255.255.255.255'.
- IPv6 Trusted Host #1:** A text input field with '::/0'.
- IPv6 Trusted Host #2:** A text input field with '::/0'.
- IPv6 Trusted Host #3:** A text input field with '::/0'.
- Comments:** A large text area.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

7. Log in to FortiDeceptor with the RADIUS administrator account you created.



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.