FortiDeceptor - Administration Guide

Version 3.2.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 17, 2020
FortiDeceptor 3.2.1 Administration Guide
50-321-683346-20201217

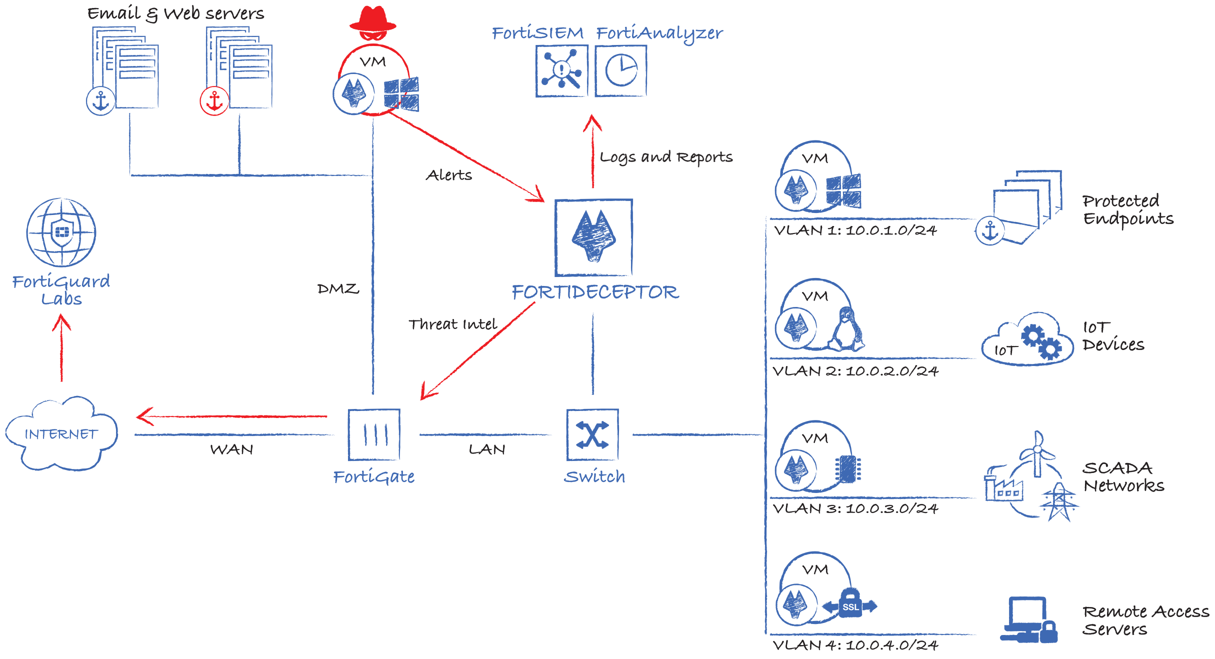
TABLE OF CONTENTS

Change Log

Date	Change Description
2020-12-17	Initial release.

Introduction

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



Key features of FortiDeceptor include:

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

Set up FortiDeceptor

This section explains the initial set up of FortiDeceptor.

Connect to the GUI

Use the GUI to configure and manage FortiDeceptor.

To connect to the FortiDeceptor GUI:

1. Connect the port1 (administration) interface of the device to a management computer using an Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiDeceptor unit:
    - 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.

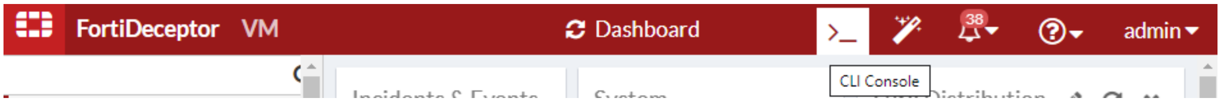
If the network interfaces have been configured differently during installation, the URL and administrative access protocols might not be in their default state.

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.
2. Click *Change* beside *System Time*.
3. Set the system time and click *Apply*.
   You might need to log in again.

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 1000F default ports:

Port (Interface)	Default Open Ports
Port1	TCP ports 22 (SSH), 23 (Telnet), 80 and 443 (GUI). FortiGuard Distribution Servers (FDS) use TCP port 8890 for download. FortiDeceptor uses a random port picked by the kernel. FortiGuard Web Filtering servers use UDP port 53 or 8888. FortiDeceptor uses a random port picked up by the kernel. FortiDeceptor deception VM download uses TCP port 443 for download. FortiDeceptor uses a random port picked by the kernel.
Port2 to port8	Each FortiDeceptor port can be directly connected to a specific VLAN or use the network trunk to communicate with multiply VLANs from a single interface. In DMZ mode, no service listens. In regular mode, token communication service listens on deployment interface monitor IP with port 1443. The token communication uses HTTPS protocol.

Deploy Decoy VM

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

To use FortiDeceptor to monitor the network:

- Go to *Deception* > *Deception OS* to check the Deception OS available. See View available Deception OS on page 23.
- Go to *Deception* > *Deployment Network* to auto-detect or specify the network where the Decoy VMs are deployed. See Set up the Deployment Network on page 24.
- Go to *Deception* > *Deployment Wizard* to deploy the Decoy VM on the network. See Deploy Decoy VMs with the Deployment Wizard on page 25.
- Go to *Deception* > *Decoy & Lure Status* to start or stop deployed Decoy VMs, or download the FortiDeceptor Token Package to manually install on computers. See Monitor Decoy & Lure Status on page 27.
- Go to *Deception* > *Deployment Map* to see the network of Decoy VMs. See Deployment Map on page 28.
- Go to *Deception* > *Safe List* to specify the network that is to be considered safe. This is useful if the administrator wants to log into the deployment network and not be flagged as an attacker. See Configure a Safe List on page 29.
- Go to *Deception* > *Lure Resources* to view and work with lure resources. See Lure Resources on page 30.

For more information, see Deception deployment best practices on page 75.

Customize Decoy VMs

For most deployments, the decoys included with FortiDeceptor are enough and are easier to deploy. However, if you want to use your own custom OS images for the decoy, FortiDeceptor supports Decoy Customization with a purchased subscription service.

Some examples of using Decoy Customization include:

- Windows 10 decoy joining AD.
- Windows Server 2016/2019 Enterprises users with their standard server management tools.

This version only supports Decoy Customization for Windows 10 and Windows Server 2016/2019.

Overview of implementing Decoy Customization:

1. Order the license with Decoy Customization subscription-based SKU.
2. Install FortiDeceptor.
   After installing FortiDeceptor with the Decoy Customization subscription, the Help icon in the toolbar has a *Customization 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.

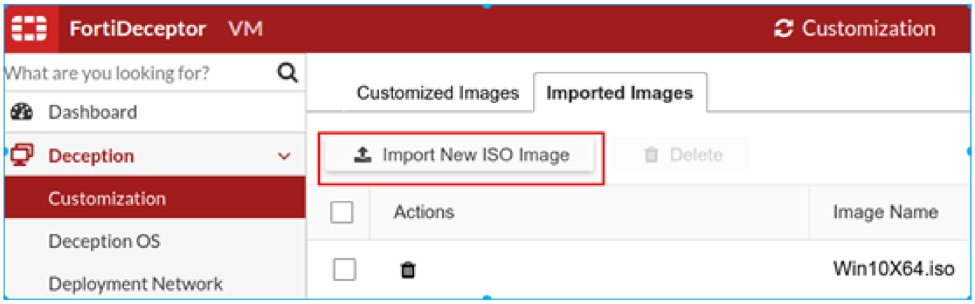
Import Windows ISO image

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

- Purchased a license with Decoy Customization subscription-based SKU.
- 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:

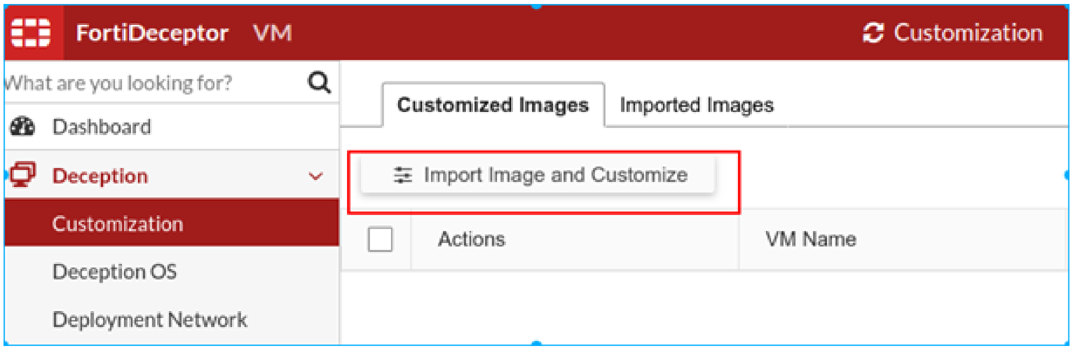
1. Go to *Deception* > *Customization* and click the *Imported Images* tab.
2. Click *Import New ISO Image*.
3. Click *Choose a file* or drag and drop an image file into that pane.



To import an ISO image using the Customized Images page:

1. Go to *Deception* > *Customization* 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:

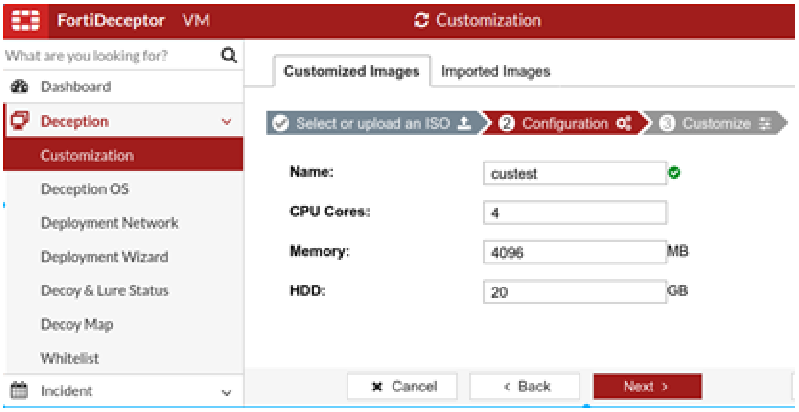
1. Go to *Deception* > *Customization* and click the *Imported Images* tab.
2. Select one or more images and then click *Delete*.

Customize VM image

To initialize the VM instance:

1. Go to *Deception* > *Customization* and click the *Customized Images* tab.
2. Click *Import Image and Customize*.
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.



Name: custest

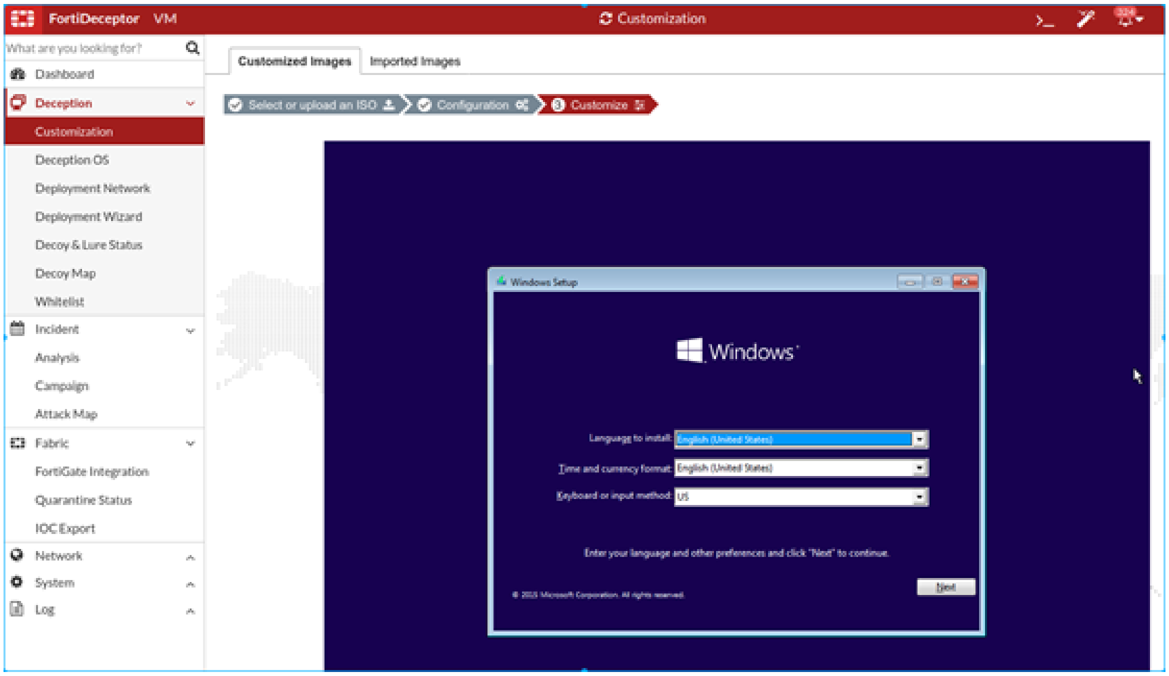
CPU Cores: 4

Memory: 4096 MB

HDD: 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.



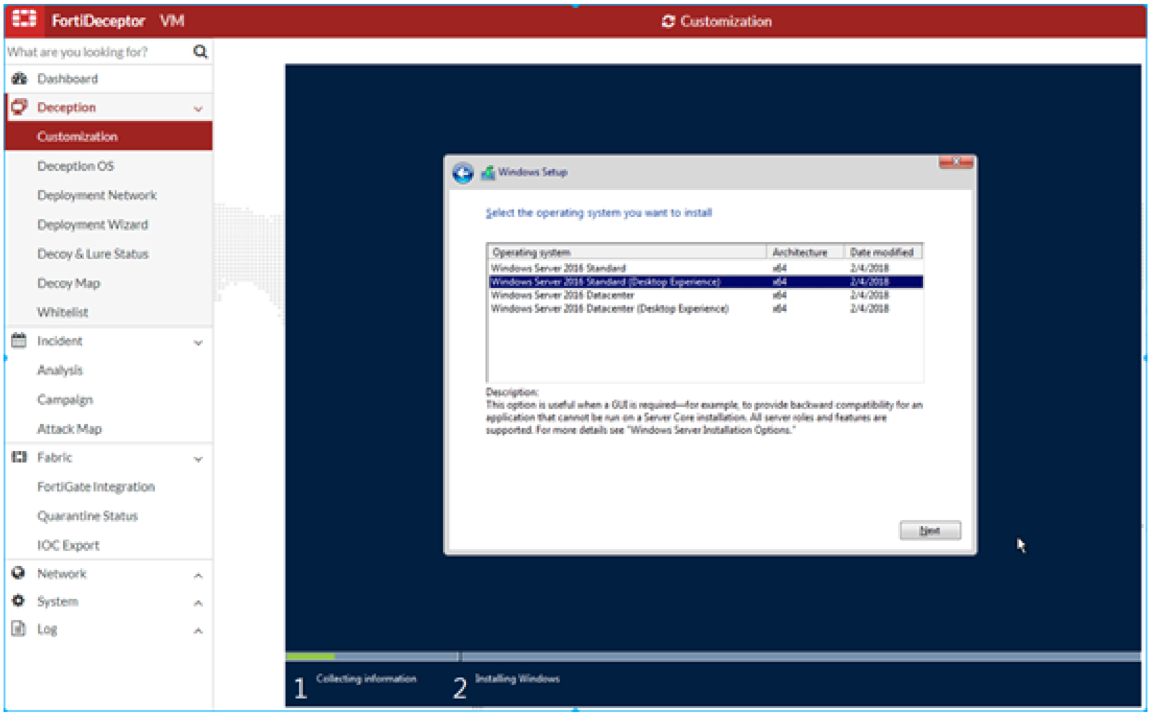
Language to install: English (United States)

Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

© 2016 Microsoft Corporation. All rights reserved.



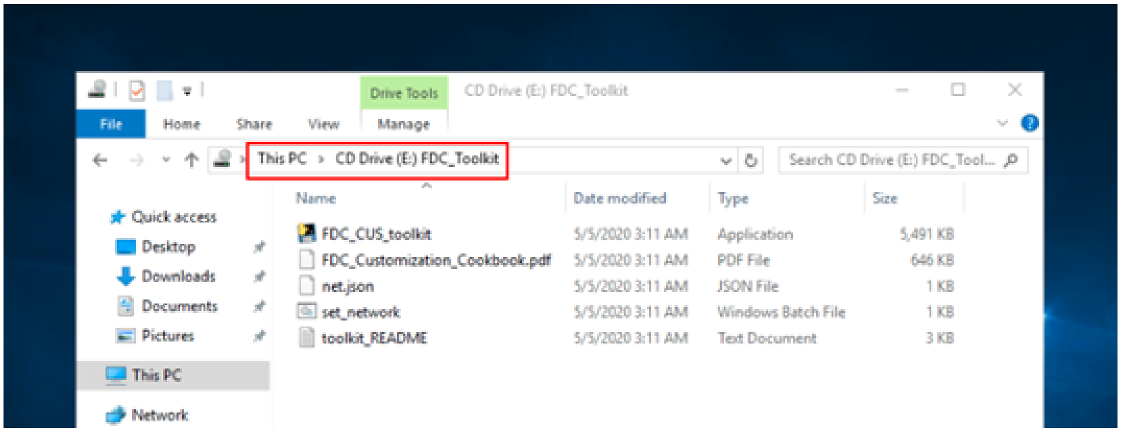
Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2016 Standard	x64	2/4/2018
Windows Server 2016 Standard (Desktop Experience)	x64	2/4/2018
Windows Server 2016 Datacenter	x64	2/4/2018
Windows Server 2016 Datacenter (Desktop Experience)	x64	2/4/2018

Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."

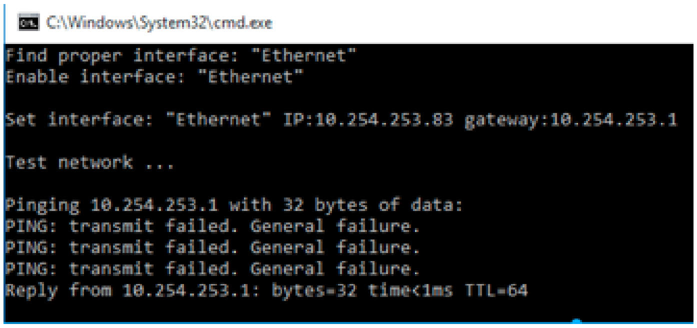
To customize the VM:

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*.



Name	Date modified	Type	Size
FDC_CUS_toolkit	5/5/2020 3:11 AM	Application	5,491 KB
FDC_Customization_Cookbook.pdf	5/5/2020 3:11 AM	PDF File	646 KB
net.json	5/5/2020 3:11 AM	JSON File	1 KB
set_network	5/5/2020 3:11 AM	Windows Batch File	1 KB
toolkit_README	5/5/2020 3:11 AM	Text Document	3 KB

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*.



```
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:

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
```

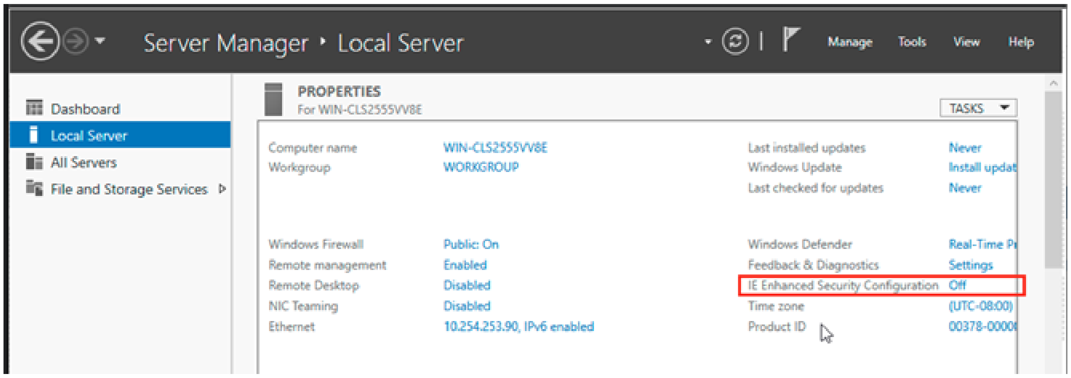
3. If you want to support decoys with AD accounts, do the following:
   a. Manually configure the DNS in Windows.
   b. Create a lure AD user account on your AD server.
      You will need this AD user account when you deploy decoys based on this image.
   c. Join the AD server with this AD user account.

Install the Microsoft SQL Server (optional)

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*.



PROPERTIES
For WIN-CLS2555VV8E

Computer name WIN-CLS2555VV8E
Workgroup WORKGROUP

Last installed updates Never
Windows Update Install updat
Last checked for updates Never

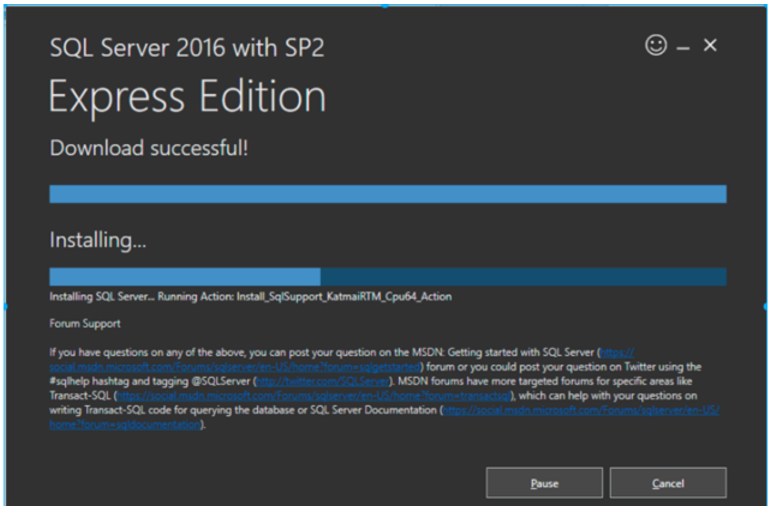
Windows Firewall Public: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet 10.254.253.90, IPv6 enabled

Windows Defender Real-Time P
Feedback & Diagnostics Settings
IE Enhanced Security Configuration Off
Time zone (UTC-08:00)
Product ID 00378-0000

For Windows Server core OS, because there is no desktop, 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.



SQL Server 2016 with SP2
Express Edition
Download successful!

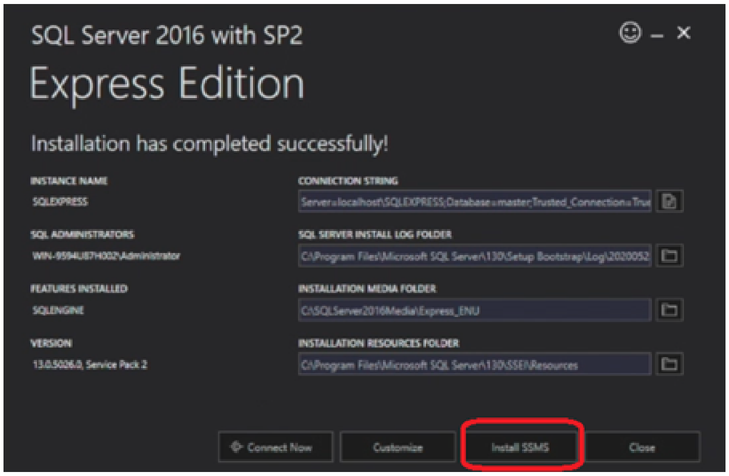
Installing...

Installing SQL Server... Running Action: Install_SqlSupport_KatmaiRTM_Cpu64_Action

Forum Support

If you have questions on any of the above, you can post your question on the MSDN: Getting started with SQL Server (https://social.msdn.microsoft.com/Forums/sqlserver/en-US/home?forum=sqlgetstarted) forum or you could post your question on Twitter using the #sqlhelp hashtag and tagging @SQLServer (http://twitter.com/SQLServer). MSDN forums have more targeted forums for specific areas like Transact-SQL (https://social.msdn.microsoft.com/Forums/sqlserver/en-US/home?forum=transactsql), which can help with your questions on writing Transact-SQL code for querying the database or SQL Server Documentation (https://social.msdn.microsoft.com/Forums/sqlserver/en-US/home?forum=sqldocumentation).

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



SQL Server 2016 with SP2

Express Edition

Installation has completed successfully!

INSTANCE NAME
SQLEXPRESS

SQL ADMINISTRATORS
WIN-9594U87H002\Administrator

FEATURES INSTALLED
SQLENGINE

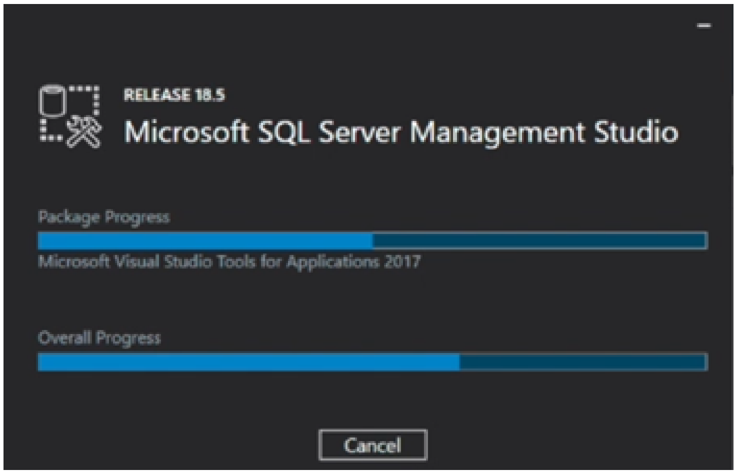
VERSION
13.0.5026.0, Service Pack 2

CONNECTION STRING
Server=localhost\SQLEXPRESS;Database=master;Trusted_Connection=True

SQL SERVER INSTALL LOG FOLDER
C:\Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\2020052

INSTALLATION MEDIA FOLDER
C:\SQLServer2016Media\Express_ENU

INSTALLATION RESOURCES FOLDER
C:\Program Files\Microsoft SQL Server\130\SSEI\Resources



RELEASE 18.5

Microsoft SQL Server Management Studio

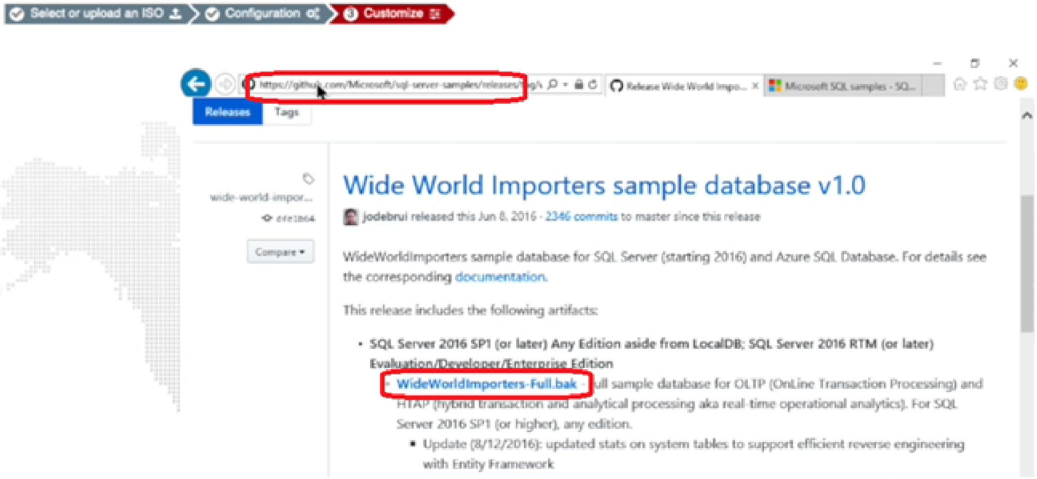
Package Progress

Microsoft Visual Studio Tools for Applications 2017

Overall Progress

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.



Select or upload an ISO
Configuration
3 Customize
https://github.com/Microsoft/sql-server-samples/releases/tag/
Release Wide World Impo...
Microsoft SQL samples - SQ...
Releases
Tags
wide-world-impor...
Compare ▾

Wide World Importers sample database v1.0

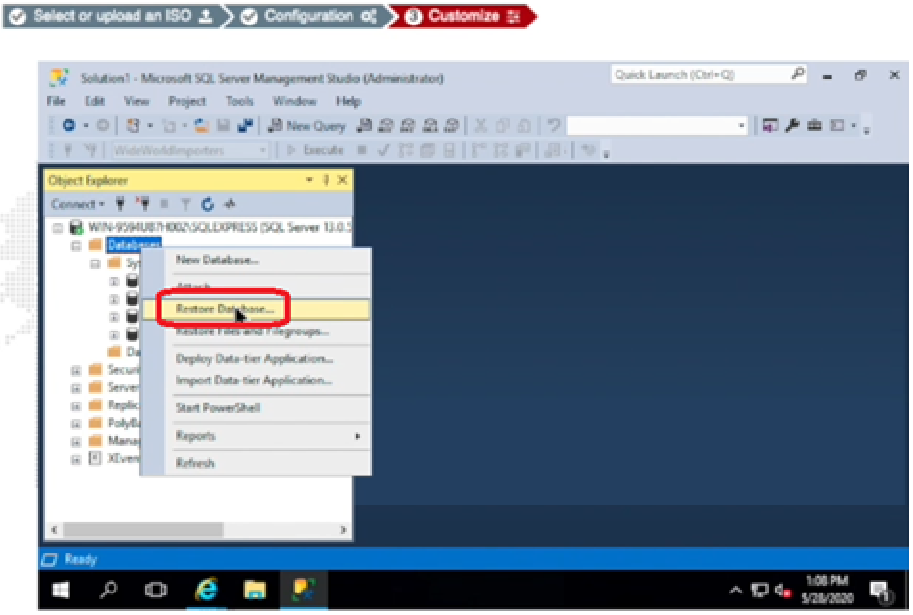
jodebrui released this Jun 8, 2016 · 2346 commits to master since this release

WideWorldImporters sample database for SQL Server (starting 2016) and Azure SQL Database. For details see the corresponding documentation.

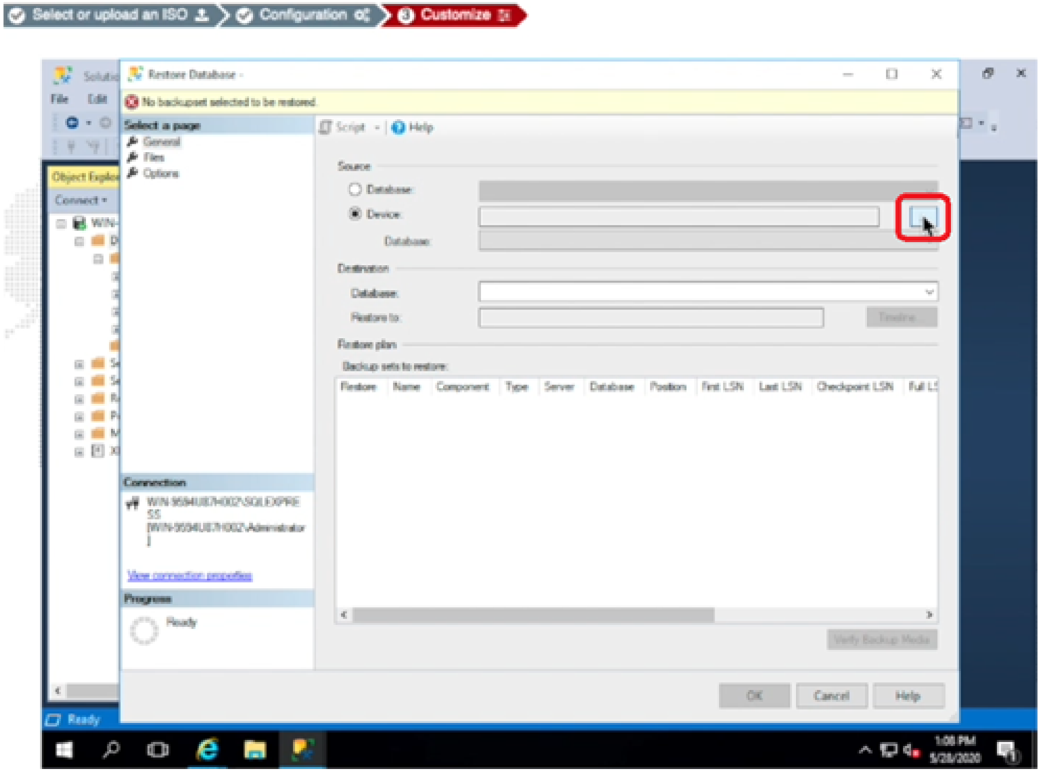
This release includes the following artifacts:

- SQL Server 2016 SP1 (or later) Any Edition aside from LocalDB; SQL Server 2016 RTM (or later) Evaluation/Developer/Enterprise Edition
  - WideWorldImporters-Full.bak - full sample database for OLTP (OnLine Transaction Processing) and HTAP (hybrid transaction and analytical processing aka real-time operational analytics). For SQL Server 2016 SP1 (or higher), any edition.
    - Update (8/12/2016): updated stats on system tables to support efficient reverse engineering with Entity Framework

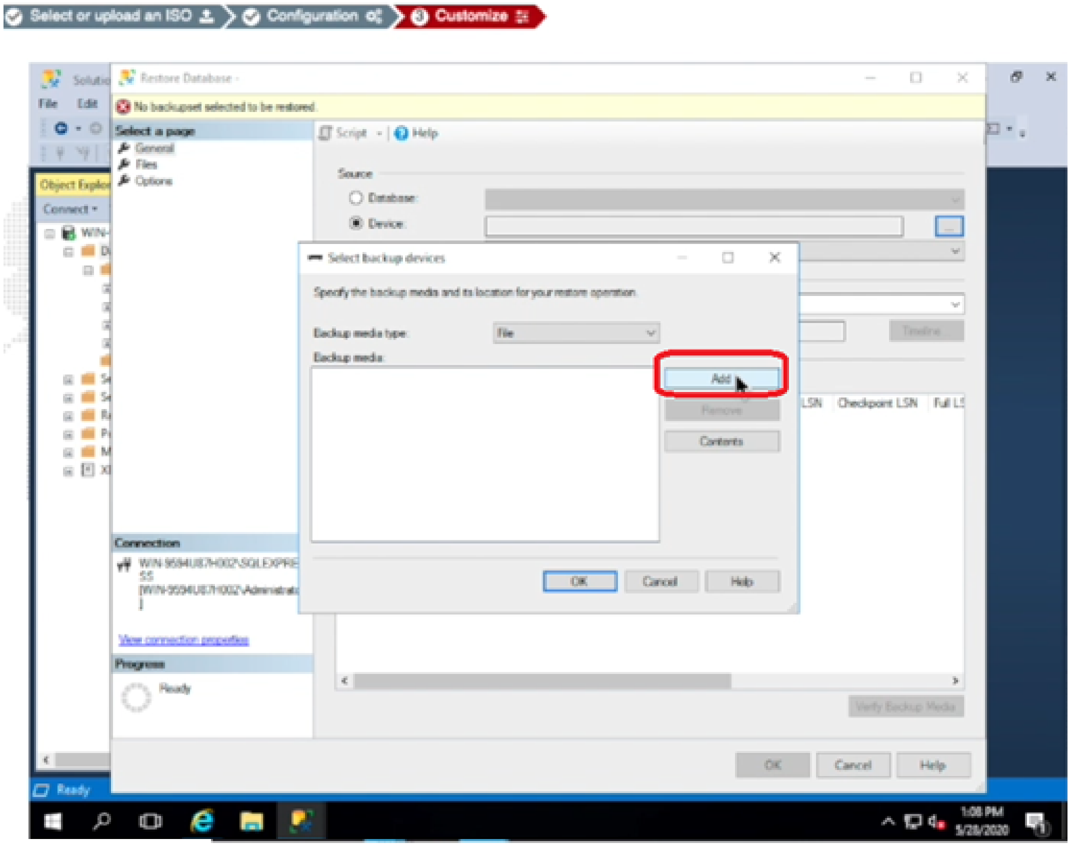
2. In the FortiDeceptor Customize Decoy console, open SQL Server Management Studio.
3. Right-click the database object and select *Restore Database*.


Select or upload an ISO
Configuration
3 Customize
Solution1 - Microsoft SQL Server Management Studio (Administrator)
Quick Launch (Ctrl+Q)
File Edit View Project Tools Window Help
New Query
Execute
Object Explorer
Connect
WIN-9594U87H002\SQLEXPRESS (SQL Server 13.0.5
Databases
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Deploy Data-tier Application...
Import Data-tier Application...
Start PowerShell
Reports
Refresh
Ready
1:08 PM
5/28/2020

4. Locate and add the sample DB you downloaded.



No backupset selected to be restored.



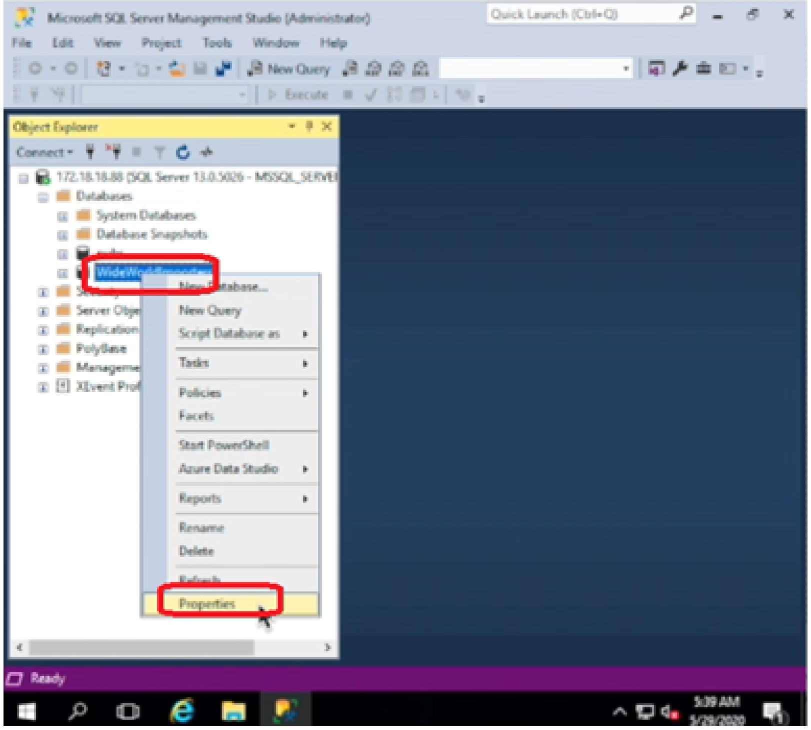
No backupset selected to be restored

Source: ● Device

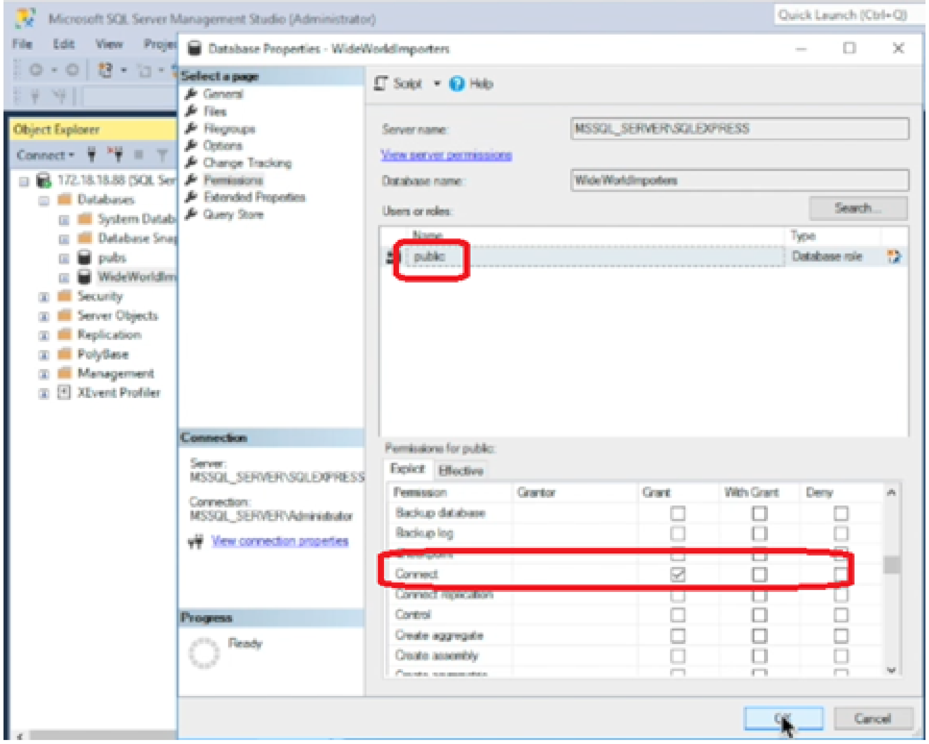
Specify the backup media and its location for your restore operation.

Backup media type: File

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*.



Server name: MSSQL_SERVER\SQLEXPRESS

Database name: WideWorldImporters

Users or roles:

Name	Type
public	Database role

Server: MSSQL_SERVER\SQLEXPRESS

Connection: MSSQL_SERVER\Administrator

Permissions for public:

Permission	Grantor	Grant	With Grant	Deny
Backup database		□	□	□
Backup log		□	□	□
Connect		☑	□	□
Control		□	□	□
Create aggregate		□	□	□
Create assembly		□	□	□

7. Close SQL Server Management Studio.
8. Verify that your DB is up using the command `netstat -an | findstr 1433`.

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.

Save the custom image

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

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

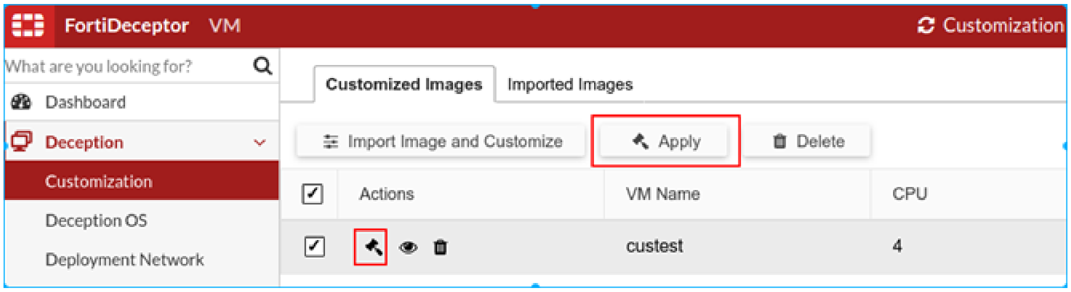
In *Deception > Customization*, the *Customized Images* tab lists the custom images.

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

Deploy custom image

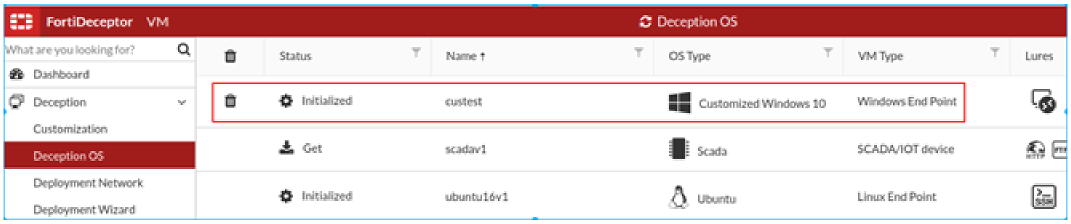
To apply a custom image:

1. Go to *Deception* > *Customization* 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.



☑	Actions	VM Name	CPU
☑		custest	4

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	

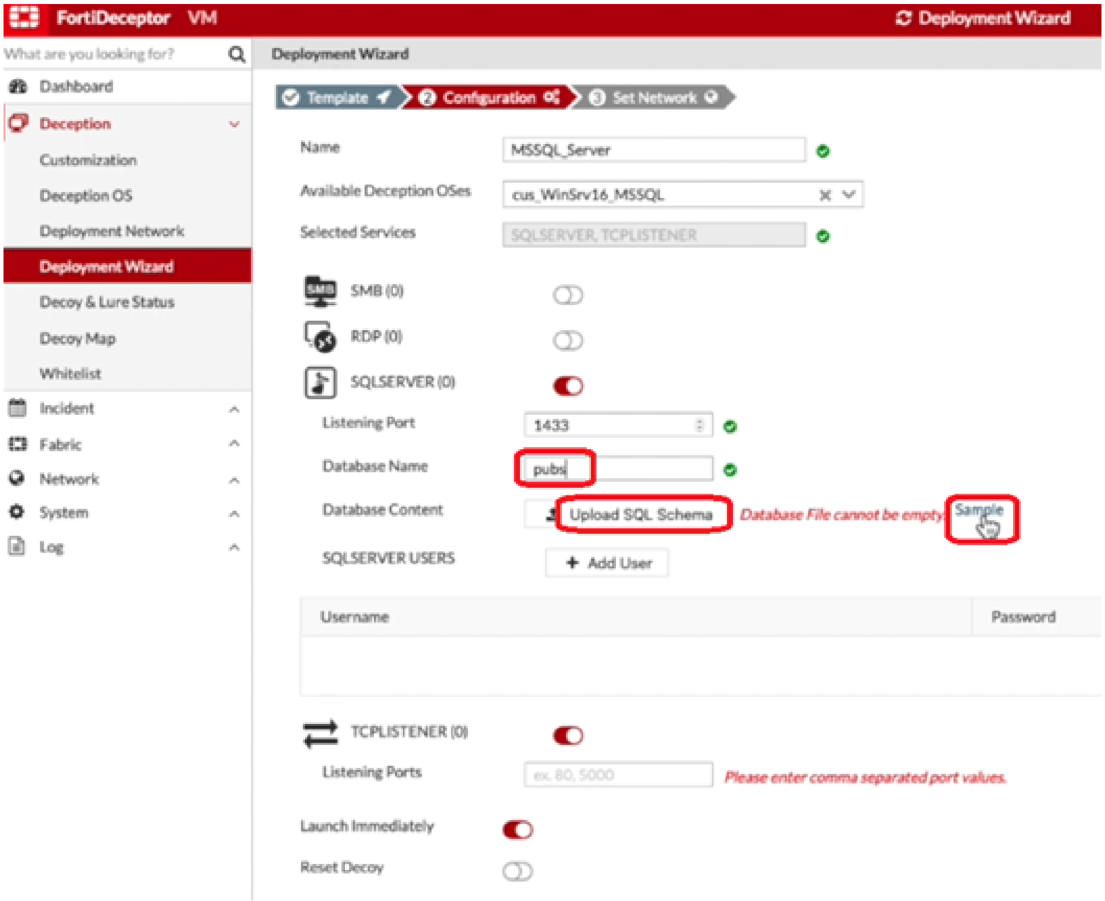
To deploy decoys with custom images–generic image:

1. Go to *Deception* > *Deployment Wizard*.
2. Click a custom image and deploy it like a standard decoy.

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.



Name: MSSQL_Server

Available Deception OSes: cus_WinSrv16_MSSQL

Selected Services: SQLSERVER, TCPLISTENER

SMB (0)

RDP (0)

SQLSERVER (0)

Listening Port: 1433

Database Name: pubs

Database Content: Database File cannot be empty

SQLSERVER USERS

TCPLISTENER (0)

Listening Ports: ex. 80, 5000 Please enter comma separated port values.

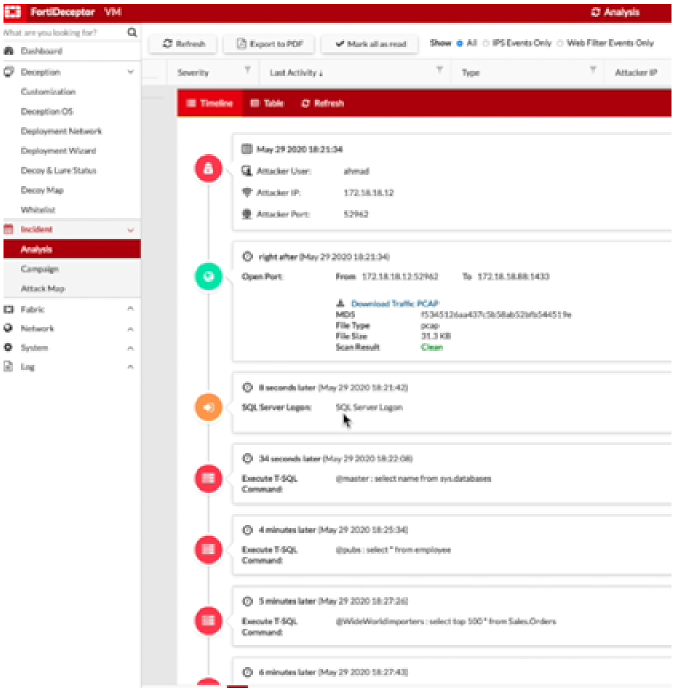
Launch Immediately

Reset Decoy

To generate SQL alerts:

1. 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.



May 29 2020 18:21:34
Attacker User: ahmad
Attacker IP: 172.18.18.12
Attacker Port: 52962

right after (May 29 2020 18:21:34)
Open Port: From 172.18.18.12:52962 To 172.18.18.88:1433
Download Traffic PCAP
MD5 f5345126aa437c5b58ab52bfb544519e
File Type pcap
File Size 31.3 KB
Scan Result Clean

8 seconds later (May 29 2020 18:21:42)
SQL Server Logon: SQL Server Logon

34 seconds later (May 29 2020 18:22:08)
Execute T-SQL Command: @master : select name from sys.databases

4 minutes later (May 29 2020 18:25:34)
Execute T-SQL Command: @pubs : select * from employee

5 minutes later (May 29 2020 18:27:26)
Execute T-SQL Command: @WideWorldImporters : select top 500 * from Sales.Orders

6 minutes later (May 29 2020 18:27:43)

View available Deception OS

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

Column	Description
Upload Deception OS Package	Upload a deception OS package.
Delete 🗑	Delete a custom OS that you have applied.
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.
Lures	Lures used by the Decoy VM such as SSH, SAMBA, SMB, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, Guardian-AST, or IEC104.

Set up the Deployment Network

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

To add a VLAN or subnet to FortiDeceptor:

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

Action	Click *Edit* to edit the VLAN or subnet entry. The *Edit* button is visible only after the entry is saved.
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. This is useful to mask the actual IP address. Mask must be 16 or higher.
Tag	You can specify a tag for the VLAN or subnet.
Ref	The number of objects referring to this object.

5. Click *Save*.

The network IP/mask must be an IP address and not a subnet.

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

- Interface name and VLAN ID 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.

Deploy Decoy VMs with the Deployment Wizard

Use the *Deception > Deployment Wizard* page to create and deploy Decoy VMs on your network. Decoy VMs appear as real endpoints to hackers and can collect valuable information about attacks.

To deploy Decoys on the network:

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

Name	Specify the name of the deployment profile. Maximum 15 characters using A-Z, a-z, 0-9, dash, or underscore. No duplicate profile names.
Available Deception OSes	Select a Deception OS. The OS you select determines the services that are available.
Selected Services	Displays the services available for the Deception OS you selected. Services for Windows include RDP, SMB, and TCPLISTENER. Services for SCADA include HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, and IEC104. Services for ubuntu include SSH, SAMBA, and TCPLISTENER.
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 *Add Lure* for the service and configure the following:

Username	Specify the username for the decoy. Maximum 19 characters using A-Z, a-z, or 0-9. Do not set the username of the lures to be the same as existing usernames in the decoy, such as *administrator* for RDP/SMB services on Windows, or *root* for SSH/SAMBA services on Linux.
Password	Specify the password for the decoy in 1-14 non-unicode characters.
Sharename	This option is only available for SAMBA (Ubuntu) or SMB (Windows). Specify a Sharename in 3-63 characters using A-Z, a-z, or 0-9.
Update or Cancel	Click *Update* to save the username and password. Click *Cancel* to discard the username and password. Click *Delete* to delete an existing lure.

5. To launch the decoy VM immediately, 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*.

8. Specify the *DNS* and *Hostname*. The *Hostname* can start with an English character or a digit, and must not end with a hyphen. Maximum 15 characters using A-Z, a-z, 0-9, or hyphen (case-sensitive). Other symbols, punctuation, or white space are not allowed. The *Hostname* cannot conflict with decoy names.
9. Click *Add Interface*.
10. Select the *Deploy Interface*. Set this to the VLAN or subnet added in Set up the Deployment Network on page 24
11. Configure the following settings in the *Add Interface for Decoy* pane:

Addressing Mode	Select *Static* or *DHCP*. *Static* allows you to configure the IP address for all the decoys. *DHCP* allows the decoys to receive IP address from the DHCP server. If you select *DHCP*, *IP Count* is automatically set to 1 and all other fields are not applicable.
Network Mask	This field is set automatically.
Gateway	Specify the gateway.
IP Count	Specify the number of IP addresses to be assigned, up to 16. If *Addressing Mode* is DHCP, *IP Count* is automatically set to 1.
Min	The minimum IP address in the IP range.
Max	The maximum IP address in the IP range.
IP Ranges	Specify the IP range between *Min* and *Max*.

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*.

Deploy the FortiDeceptor Token Package

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

To download a FortiDeceptor Token Package:

1. Go to *Deception* > *Decoy & Lure Status*.
2. Select the Decoy VM by clicking its checkbox.
3. To download the FortiDeceptor Token Package, click *Download Package*.
   You can only download packages with valid IP addresses. A package must have a status of *Initialized*, *Stopped*, *Running*, or *Failed*.

To deploy or uninstall a FortiDeceptor Token Package on an existing endpoint:

1. Copy the downloaded FortiDeceptor Token Package to an endpoint such as a Windows or Linux endpoint.
2. Unzip the FortiDeceptor Token Package.
3. In the folder for the OS, such as *windows* or *ubuntu*, follow the instructions in *README.txt* to install or uninstall the Token Package.

- For Windows, open the *windows* folder, right-click *windows_token.exe* and select *Run as administrator*.
- For Ubuntu, open Terminal and run *python ./ubuntu_token.py*.

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

Monitor Decoy & Lure Status

The *Deception* > *Decoy & Lure Status* page shows the status of the Decoys on your network.

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

To view the Deception Status:

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

Action	Click *View detail* to see the decoy's configuration details. Click *Copy to Template* to duplicate the decoy as a template. Click *Start* or *Stop* to start or stop the decoy. Click *Delete* to delete the decoy. Click *Download* to download the FortiDeceptor Token Package. Click *Attack Test* to test the decoy. Click *VNC* to open a VNC of the decoy.
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.
Enabled Services	The number of decoy services enabled on this VM.
IP	The IP address of the Decoy VM.
Services	List of services enabled. Hover over an icon to see a text list.
Network Type	Shows if the IP address is *Static* or *DHCP*.
DNS	DNS of the Decoy VM.
Gateway	Gateway of the Decoy VM.

To delete one or more Decoy VMs:

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

3. Click *OK*.

To start one or more Decoy VM:

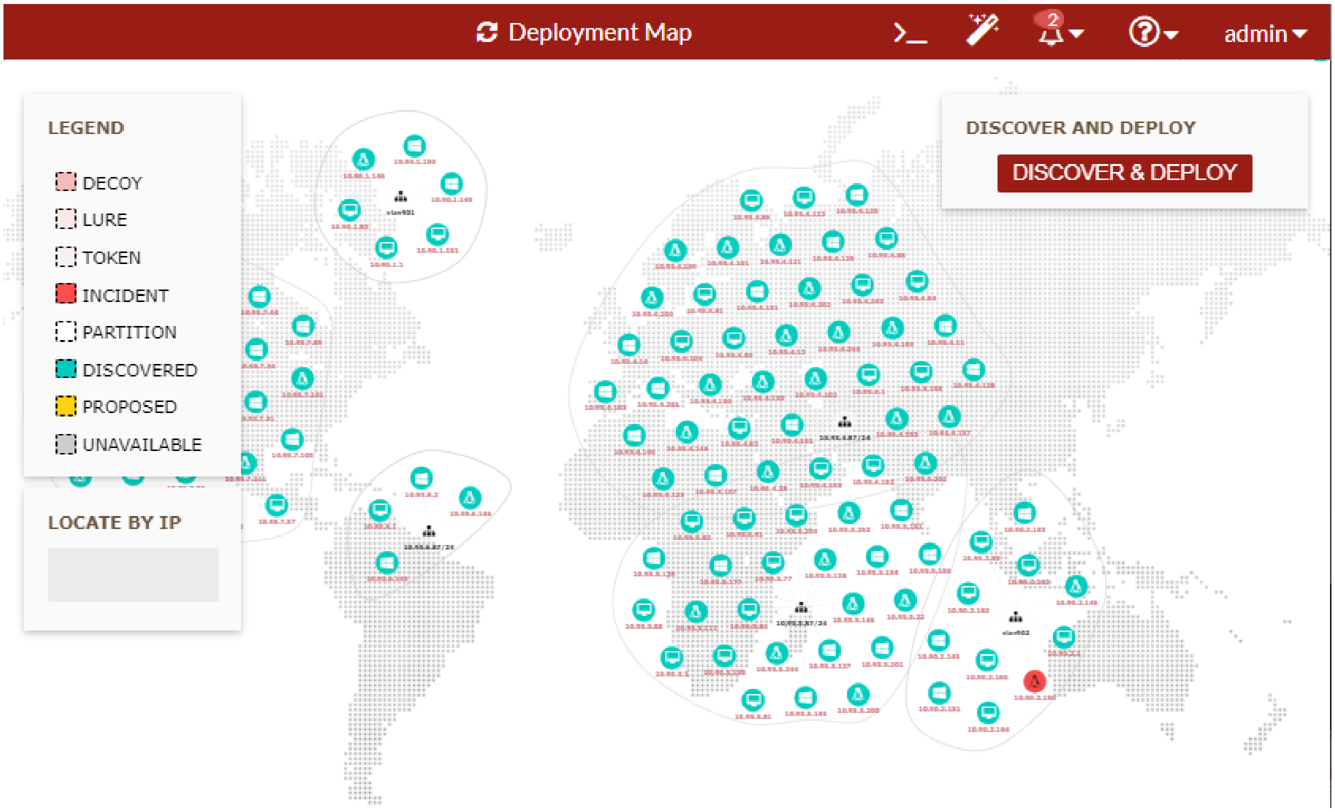
1. Go to *Deception* > *Decoy & Lure Status*.
2. Select one or more Decoy VMs that are stopped.
3. Click *Start*.

To stop one or more Decoy VMs:

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

Deployment Map

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



- To start automatic discovery and deployment, click *DISCOVER & DEPLOY* to display the *Discovery & Deployment* popup dialog box.

The *Discovery & Deployment* dialog box has the following options:

  - Select deployment networks to scan.
  - Add deployment networks to scan.
  - Add TCP scan ports for discovery.
  - Specify the number of decoys per OS per VLAN/subnet.

When you click *DISCOVER*, the automatic deployment purges the existing auto-deployed decoys and uses the same license for the new settings. It starts the discover and deploy process and discovered endpoints appear on the *Deployment Map*.

- If the *DISCOVER & DEPLOY* dialog box displays *ACCEPT & DEPLOY*, check the settings to see if you want to accept the proposal and start auto-deployment.
  - The top of this dialog box displays the proposal showing the OSes covered, total decoys, and total coverage.
  - Click the link to download the asset list.
- To change the display, drag items to another location.
- Scroll to zoom in or out.
- To locate the node on the map, use the *LOCATE BY IP* box.
- Click a node to see more information.
- Green nodes are the discovered endpoints.
- Pink nodes are decoys.
  Click a pink node to start or stop it, view its configuration, save it as a template, view the VNC interface, or delete it.
- Yellow nodes are proposal decoys.
  Click a yellow node to edit its settings, generate lures, duplicate, or delete it.

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 Address	Specify the IP address from where the connection originates.
Source Ports	Specify the source ports from where the connection originates.
Destination Ports	Specify the destination ports on the network where the connection terminates.
Description	Specify a description. For example, you can name it as *Safe_Network*.
Services	Select the name of the services used to connect to the network.
Status	Select *Enabled* or *Disabled*.
Action	Click *Update* or *Cancel*.

Lure Resources

The *Deception* > *Lure Resources* page allows you to:

- View current lures.
- Upload a lure resource to automatically generate lures.
- Import a user name list from an LDAP server and save the file in the backend.

To upload a lure resource:

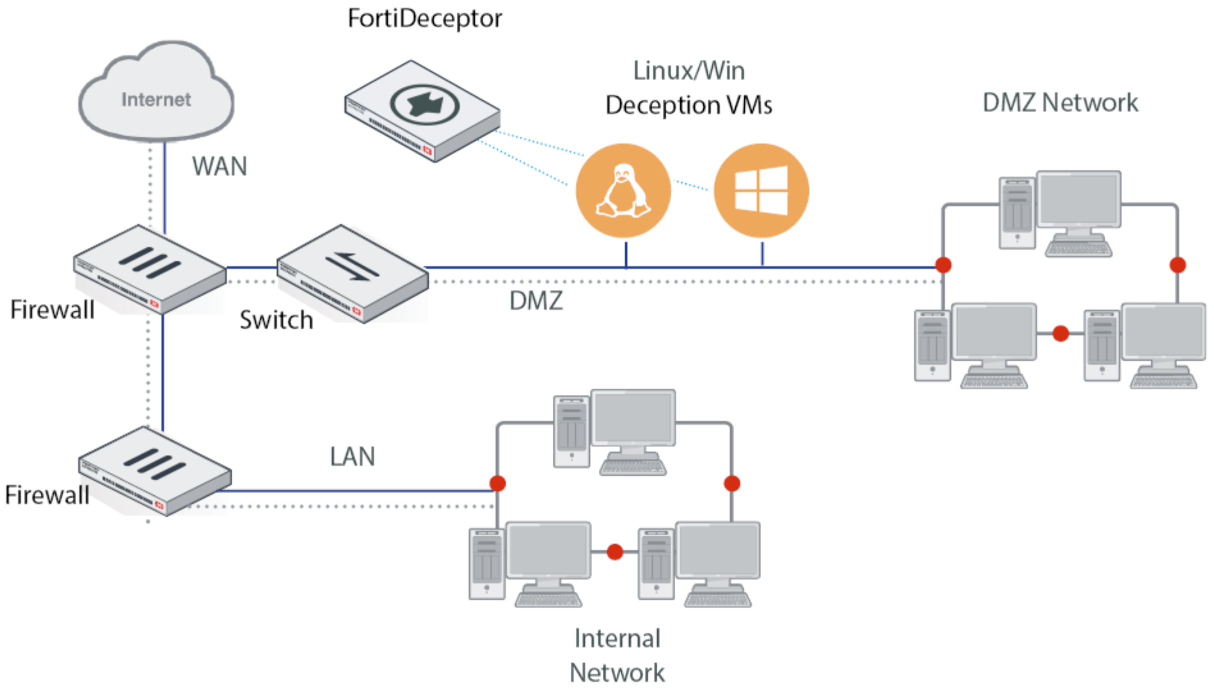
1. Go to *Deception* > *Lure Resources*.
2. Click *Upload*.
3. Select the *Lure Type* from the dropdown list.
4. Enter an optional *Tag*, such as *any*.
5. Specify a *Resource File* and click *Save*.

To import an LDAP user list:

1. Go to *Deception* > *Lure Resources*.
2. Click *Import Users from LDAP*.
3. Specify the import settings and click *Save*.

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.



Limitations of the DMZ Mode

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

- When DMZ mode is enabled, the banner displays *DMZ-MODE*.
- In *Deception* > *Deployment Network*, *Deception Monitor IP/Mask* is hidden. See Set up the Deployment Network on page 24.
- 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 25.

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 32.
- *Incident* > *Campaign* lists attacks and related events detected by FortiDeceptor. See Campaign on page 33.
- *Incident* > *Attack Map* shows attacks and related events detected by FortiDeceptor. See Attack Map on page 33.

To monitor attacks using Dashboard widgets:

- Use the *Dashboard Incidents & Events Distribution* widget. See Incidents and Events Distribution on page 34.
- Use the *Dashboard Incidents & Events Count* widget. See Incidents and Events Count on page 34.

Analysis

Incident > *Analysis* lists the *Incidents* detected by FortiDeceptor.

To use the Analysis page:

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

Severity	Severity of the event.
Last Activity	Date and time of the last activity.
Type	Type of event.
Attacker IP	Attacker IP mask.
Attacker User	Attacker username.
Victim IP	IP address of the victim.
Victim Port	Port of the victim.
Lure	Name of the lure service.
Decoy ID	Unique ID of the Decoy VM.
ID	ID of the incident.
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.

3. To refresh the data, click *Refresh*.
4. To download the detailed analysis report in PDF format, click *Export to PDF*.
5. To mark items as read, expand the incident details or click *Mark all as read*.
   Newly-detected incidents are in bold to indicate they are unread.
6. To display specific types of events, click *Show Interaction Events Only* (default), *IPS Events Only*, *Web Filter Events Only*, or *All*.
7. To specify columns and table settings, use the Settings icon at the bottom right.

Campaign

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

To use the Campaign page:

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

Severity	Severity of the event.
Start	Date and time when the attack started.
Last Activity	Date and time of the last activity.
Attacker IP	IP mask of the attacker.
ID	ID of the campaign record.
Timeline	Click *Timeline* to see the timeline of the *Attack* from start to finish.
Table	Click *Table* to see all the *Events* in table view.

3. To refresh the data, click *Refresh*.
4. To export the data, click *Export to PDF*.
5. To specify columns and table settings, use the Settings icon at the bottom right.

Attack Map

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

To work with the Attack Map:

1. Go to *Incident* > *Attack Map*.
   - To change the display, drag items to another location.
   - Scroll to zoom in or out.

- Click a node to see its information.

2. At the bottom of the Attack Map, use the timeline indicator to set the start and end time.
3. Click *Click to begin filtering* to select a different filter type and type values.
   Filter types include *Attacker IP*, *Victim IP*, and *Decoy IP*.

   You can use multiple arguments with different filter types. All filter arguments and time indicator arguments are considered "AND" conditions.
4. To locate the node on the map, use the *LOCATE BY IP* box.
5. To save a snapshot of the map, click *Save view* 💾.

Incidents and Events Distribution

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

Unknown	*Incident* or *Event* where the risk level is unknown. Entries are in grey.
Low Risk	*Incident* or *Event* where the risk level is low. Entries are in green.
Medium Risk	*Incident* or *Event* where the risk level is medium. Entries are in yellow.
High Risk	*Incident* or *Event* where the risk level is high. Entries are in orange.
Critical	*Incident* or *Event* 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:

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

To customize this widget:

1. 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 *Events*.

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 *Incidents*.

Top 10 IPS Attacks

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

IPS attack name	IP address of the attacker.
Number of attack events	Hover over an IPS attack name to see the total number of attack events.

Incidents Distribution by Service

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

SSH	Number of incidents occurring on SSH service with the percentage on a pie chart.
SAMBA	Number of incidents occurring on SAMBA service with the percentage on a pie chart.
SMB	Number of incidents occurring on SMB service with the percentage on a pie chart.

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

Hover over the pie chart to see the percentage. Click the pie chart to split 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:

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

Integration Devices

Use *Fabric > Integration Devices* 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 *Edit* to edit the integration settings. Click *Delete* to delete the device.
Enabled	Shows if the device is enabled or disabled.
Status	Device status.
Name	Alias of the integrated device.
Integrate Method	The integration method of this device.
Severity	Security level. The selected level and all levels above it are blocked. For example, if you select *Medium*, then medium, high, and critical levels are blocked. If you select *Critical*, then only the critical level is blocked.
Detail	Device integration details.

To integrate a device:

1. Go to *Fabric > Integration Devices*.
2. Click *Integrate 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	Select the security level. The selected level and all levels above it are blocked. For example, if you select *Medium*, then medium, high, and critical levels are blocked. If you select *Critical*, then only the critical level is blocked.
Integrate Method	The integration method of this device. Different integration methods have different settings.
IP or Device IP	IP address of the integrated device.
Port	Port number of the integrated device API service. Default is 443.
Username and Password	Username and password of the integrated device.
VDOM	For FortiGate devices, the default access VDOM.
Expiry	Default blocking time in second. Default is 3600 seconds.
Block Action	For integration by webhook, specify the *Expiry*, *URL*, *Authorization*, *HTTP Method*, *HTTP Header*, and *HTTP Data* for the block action. *HTTP Header* and *HTTP Data* allow you to use field names and values. You can also add multiple HTTP header and data fields.
Unblock Action	For integration by webhook, specify the *URL*, *Authorization*, *HTTP Method*, *HTTP Header*, and *HTTP Data* for the unblock action.

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 *Attacker IP* address. This is the *Name* field in *Fabric > Integration Devices*.
Time Remaining	The remaining blocking time.
Status	Current status of the attacker.

Message	Related message for the blocking entry.

IOC Export

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

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 user profiles to define user privileges.
Certificates	Configure CA certificates.
LDAP Servers	Configure LDAP servers.
RADIUS Servers	Configure RADIUS servers.
Mail Server	Configure the mail server.
SNMP	Configure SNMP.
FortiGuard	Configure FortiGuard settings and upgradeable packages.
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 *Incident* and *Event* tables.

Administrators

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

If the user whose 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: • 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 (_).
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 *Type* is set to *Local*.
Type	Select *Local*, *LDAP*, or *RADIUS*.
LDAP Server	When *Type* is *LDAP*, select an *LDAP Server*. For more information, see LDAP Servers on page 46.
RADIUS Server	When *Type* is *RADIUS*, select a *RADIUS Server*. 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 what computers an administrator can use to log into FortiDeceptor. When you identify a trusted host, FortiDeceptor only accepts the administrator’s login from the configured IP address or subnet. Attempts to log in with the same credentials from another IP address or subnet are dropped.

4. Click *OK*.

To edit a user account:

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

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

Only users with the Super Admin profile can create, edit, and delete administrator profiles. Users can create, edit, and delete administrator profiles if they have *Read Write* privilege in their profile.

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
    - Deception
        - Customization
        - Deception OS
        - Deployment Network
        - Deployment Wizard
        - Decoy & Lure Status
        - Deployment Map
        - Safe List
    - Incident
        - Analysis
        - Campaign
        - Attack Map
    - Fabric
        - Integration Devices
        - Quarantine Status
        - IOC Export
    - Network
        - Interfaces
        - System DNS
        - System Routing
    - System
        - Administrators
        - Admin Profiles
        - Certificates
        - LDAP Servers
        - RADIUS Servers
        - Mail Server
        - SNMP
        - FortiGuard
        - Settings
        - Login Disclaimer
        - System Settings
        - Table Customization
    - Log
        - All Events
        - Log Servers

6. Specify the privileges for *CLI Commands*:
   - Configuration
     - Set
     - Unset
   - System
     - Reboot
     - Shutdown
     - Reset Configuration
     - Factory Reset
     - Firmware Upgrade
     - Reset Widgets
     - IP Tables
     - test-network
     - usg-license
     - Upload VM Firmware License
     - Resize VM Hard Disk
     - Set Confirm ID for Windows VM
     - List VM License
     - Show VM Status
     - VM reset
     - DC Image Status
     - Set Maintainer
     - Set Timeout for Remote Auth
     - Data Purge
     - Log Purge
     - DMZ Mode
     - fdn-pkg
   - Utilities
     - TCP Dump
     - Trace Route
7. Click *Save*.

Certificates

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

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

The following options are available:

Import	Import a certificate.

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

The following information is displayed:

Name	Name of the certificate.
Subject	Subject of the certificate.
Status	The certificate status, active or expired.
Service	HTTPS or SSH service that is using this certificate.

To import a certificate:

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

To view a certificate:

1. Go to *System* > *Certificates*.
2. Select a certificate and click *View*.
   The following information is available:

Certificate Name	Name of the certificate.
Status	Certificate status.
Serial number	Certificate serial number.
Issuer	Issuer of the certificate.
Subject	Subject of the certificate.
Effective date	Date and time that the certificate became effective.
Expiration date	Date and time that the certificate expires.

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 `cn`. Some servers use other common name identifiers such as `uid`.
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: • *Simple* • *Anonymous* • *Regular*
Username	When the *Bind Type* is set to *Regular*, enter the user name.
Password	When the *Bind Type* is set to *Regular*, enter the password.
Enable Secure Connection	Use a secure LDAP server connection for authentication.
Protocol	When *Enable Secure Connection* is selected, select *LDAPS* or *STARTTLS*.
CA Certificate	When *Enable Secure Connection* is selected, select a *CA Certificate*.

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 *Any*, *PAP*, *CHAP*, or *MSv2*. *Any* 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 *Any*, *PAP*, *CHAP*, or *MSv2*. *Any* means FortiDeceptor tries all authentication types.
Primary Secret	Primary RADIUS server secret.
Secondary Secret	Secondary RADIUS server secret.
NAS IP	NAS IP address.

4. Click *OK*.

Mail Server

Use the *System* > *Mail Server* page to adjust mail server settings.

You can configure the following options:

Send Incidents Alerts	When enabled, FortiDeceptor sends an email alert to the *Receiver Email List* when it detects an incident.
SMTP Server Address	SMTP server address.

Port	SMTP server port number.
E-Mail Account	The mail server email account. This is the "from" address.
Login Account	The mail server login account.
Password, Confirm Password	Enter and confirm the password.
Receiver Email List	Enter one or more receiver email addresses.
Send Test Email	Send a test email to the global email list. If an error occurs, the error message appears at the top of the page and is recorded in the System Logs.

SNMP

SNMP is a method to monitor your FortiDeceptor system on your local computer. You need an SNMP agent on your computer to read the SNMP information. Using SNMP, your FortiDeceptor system monitors for system events including CPU usage, memory usage, log disk space, interface changes, and malware detection. Go to *System* > *SNMP* to configure your FortiDeceptor system's SNMP settings.

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

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

You can also download FortiDeceptor and Fortinet core MIB files.

Configure the SNMP agent

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

The SNMP manager can monitor FortiDeceptor to determine if it is operating properly or if critical events are occurring. The description, location, and contact information for this FortiDeceptor system is part of the information an SNMP manager collects. This information is useful if the SNMP manager is monitoring many devices, and it enables a faster response when FortiDeceptor requires attention.

To configure SNMP agents:

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

SNMP Agent	When enabled, the FortiDeceptor SNMP agent sends FortiDeceptor SNMP traps.
Description	Description of this FortiDeceptor to identify this unit.

Location	Location of this FortiDeceptor if it requires attention.
Contact	Contact information of the person in charge of this FortiDeceptor.
SNMP v1/v2c	Create, edit, or delete SNMP v1 and v2c communities. You can enable or disable communities in the edit page. Columns include: *Community Name*, *Queries*, *Traps*, *Enable*.
SNMP v3	Create, edit, or delete SNMP v3 entries. You can enable or disable queries in the edit page. Columns include: *Username*, *Security Level*, *Notification Host*, and *Queries*.

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 *Add* 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: • 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: • None • Authentication only • Encryption and authentication
Authentication	Authentication is required when *Security Level* is either *Authentication only* or *Encryption and authentication*.
Method	Authentication method: • MD5 (Message Digest 5 algorithm) • SHA1 (Secure Hash algorithm)
Password	Authentication password of at least eight characters.
Encryption	Encryption is required if *Security Level* is *Encryption and authentication*.
Method	Encryption method: • DES • AES
Key	Encryption key of at least eight characters.
Notification Hosts (Traps)	
IP/Netmask	IP address and netmask. Click *Add* to add more hosts.
Query	
Port	Port number and if it is enabled.
SNMP V3 Events	SNMP events associated with that user: • CPU usage is high • Memory is low • Log disk space is low • Incident is detected

4. Click *OK*.

To download MIB files:

1. At the bottom of the SNMP page, select the MIB file you want to download to your management computer.

FortiGuard

1. Go to *System* > *FortiGuard*.
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 *Browse* to locate a package file on the management computer, then select *Submit* to upload the package file to the FortiDeceptor. When the unit has no access to the Fortinet FDN servers, the user can go to the Customer Service and Support site to download package files manually.
FortiGuard Server Location	Select FDN servers for package update and Web Filtering query. By default, the selection is *Nearest*, which means the closest FDN server according to the unit's time zone is used. When US Region is selected, only servers inside Unite States are used.
FortiGuard Server Settings	
Use override FDN server to download module updates	Select to enable an override FDN server, or FortiManager, to download module update, then enter the server IP address or FQDN in the text box. When an overridden FDN server is used, FortiGuard Server Location will be disabled. Click *Connect FDN Now* button to schedule an immediate update check.
Use Proxy	Select to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
FortiGuard Web Filter Settings	
Use override server address for web filtering query	Select to enable an override server address for web filtering query, then enter the server IP address (IP address or IP address:port) or FQDN in the text box. By default, the closest web filtering server according to the unit's time zone is used. If port is not provided, target UDP port 53 will be used.
Use Proxy	Select to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
VM Image Download Proxy Settings	
Use Proxy	Select to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.

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

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.

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

To customize the columns available for Incidents or Events:

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

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

System Settings

Dashboard

The System Status dashboard displays widgets that provide information and enable you to configure basic system settings. All the widgets appear on a single dashboard. You can select which widgets to display and you can customize the widgets.

The following widgets are available.

System Information	Basic information about the FortiDeceptor system, such as the serial number, system up time, and license status information.
System Resources	Real-time usage status of the CPU and memory.
Top Critical Logs	The top logs that are classified as *Critical*.
Deception VM License	The list of VM license keys and their expiry dates.
Disk Monitor	The RAID level and status, disk usage, and disk management information.
Incidents & Events Distribution	Information about the number of incidents and events, and their level of severity.
Incidents & Events Count	Number of events occurring each day.
Decoy Distribution by OS	Number of decoys with a chart showing the OS such as Windows or Ubuntu.
Lure Distribution	Number of decoys deployed with the chart showing the type of service such as SSH, Samba, SMB, SCADA, or RDP.
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.
Top 10 Attackers by Events	The top 10 attackers by the number of events.
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.

Customizing the dashboard

You can customize the FortiDeceptor system dashboard. You can select which widgets to display and where they are located on the page.

- To add a widget, click *Add Widget* + in the Dashboard’s floating toolbar at the bottom, and then select the widgets you want to add.
- To edit a widget, click the Edit icon ✎ in the in the widget’s title bar, change the settings, and click *OK*.
- To move a widget, click and drag the widget's title bar.

- To refresh a widget's data, click *Refresh* ↻ in the widget’s title bar.
- To reset all widgets to their default settings, click *Reset* ↻ in the Dashboard’s floating toolbar at the bottom.
- To hide a widget, click the Close icon in the widget's title bar.

System Information

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

This widget displays the following information and options.

Host Name	The name assigned to this FortiDeceptor unit. Click *Change* 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 *Change* 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 *Update* or *UPDATE AVAILABLE* and select the firmware image to load from the local hard disk or network volume.
Firmware License	To load a firmware license, click *Upload License* and select a license file.
System Configuration	Date and time of the last system configuration backup. Click *Backup/Restore* to go to the *System Recovery* 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 an *up* icon if the Deception OS is activated and initialized. Displays a *Caution* icon if the Deception OS is initializing or having issues. Hover the mouse pointer on the status icon to view detailed information. For more information, see *Log > All Events*. To go to *Deception > Deception OS* to see the images available on FortiDeceptor, click *Update* or *UPDATE AVAILABLE*. After purchase, download the license file from the Fortinet Customer Service & Support portal. Then click *Upload License* 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.

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	Number and percentage of SCADA 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.
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.

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.

Microsoft Windows VM license activation

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

If you purchase a Windows or Ubuntu VM upgrade package, put the downloaded license file here using the *Upload License* link.

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

Before any firmware update, complete the following:

- Download the FortiDeceptor firmware image and Release Notes document from the Fortinet Customer Service & Support portal. Review the Release Notes, including the special notices, upgrade information, product integration and support, and resolved and known issues.
- Back up your configuration file. It is highly recommended that you create a system backup file and save it to your management computer. You can also schedule the system to back up system configurations to a remote server.
- Plan a maintenance window 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 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 might about 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 yous 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 same 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: *(cluster external port)*.
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. 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: • Interface up • Interface down • Interface is being used by sniffer

Link Status	The link status: - 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 *Edit* 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*.
3. If you want, you can change the *Interface Status*.
4. 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 by clicking *Download Log*. Raw logs are saved as a text file with the extension *.log.gz*. You can search the system log for more details.

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* show 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 *Filter* 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 63.
User	The user to which the log message relates. User can be a specific user or system.
Message	Detailed log message.

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.
Server Type	Server type: syslog or CEF.
Server Address	Log server address.
Port	Log server port number.
Status	Log server status, *Enabled* or *Disabled*.

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 *Syslog Protocol*, *FortiAnalyzer*, or *Common Event Format*.
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 63.

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 67
- Importing deception VMs in an offline or air-gapped network on page 69
- Importing firmware in an offline or air-gapped network on page 71
- Importing an FDS package via FDC GUI in an offline or air-gapped network on page 72
- Importing FDS package and license file via FortiManager in an offline or air-gapped network on page 72

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. The FortiDeceptor hardware appliance already has deception VMs pre-configured and loaded. For new deception VMs, update the hardware appliance.

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 propriety 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.

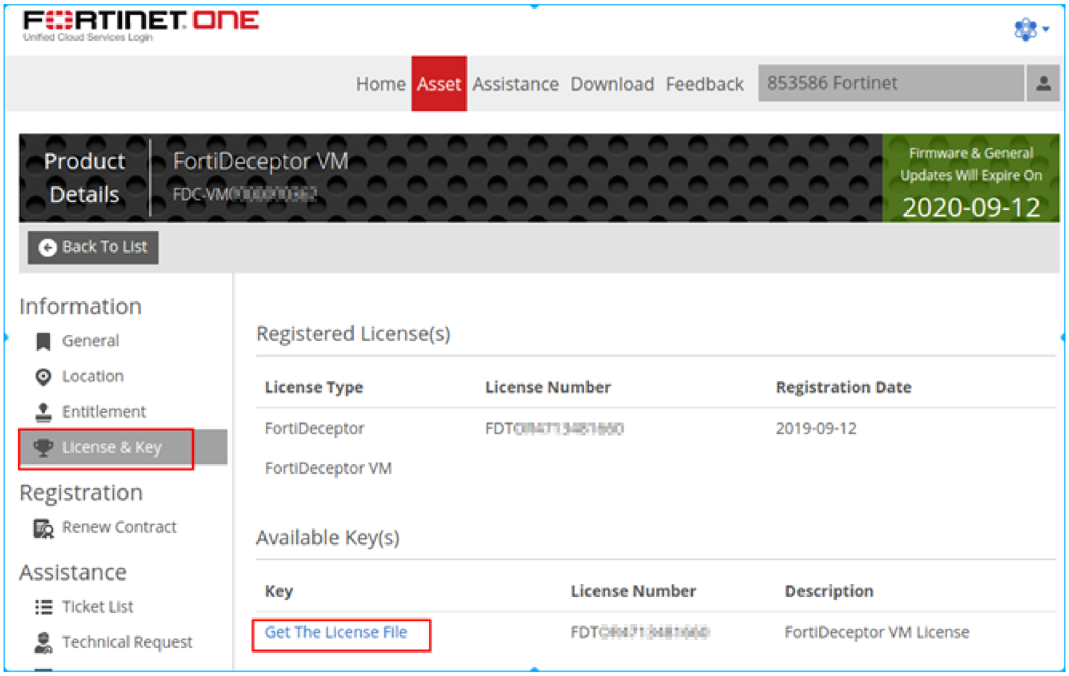
Applying the license in an offline or air-gapped network

This topic shows how to apply for a FortiDeceptor 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.
2. Go to *Asset* > *Information* > *License & Key*.

3. In the *Available Key(s)* section, click *Get The License File* and save it to the local disk.



Product Details — FortiDeceptor VM, FDC-VM[redacted]

Firmware & General Updates Will Expire On 2020-09-12

Registered License(s)

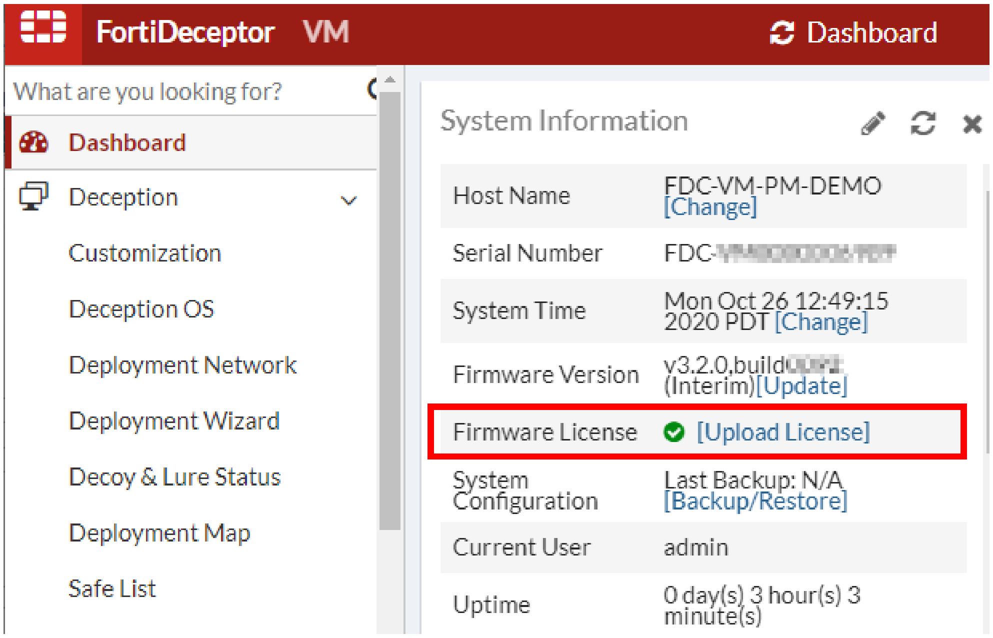
License Type	License Number	Registration Date
FortiDeceptor	FDT[redacted]	2019-09-12
FortiDeceptor VM		

Available Key(s)

Key	License Number	Description
Get The License File	FDT[redacted]	FortiDeceptor VM License

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*.



System Information

Host Name	FDC-VM-PM-DEMO [Change]
Serial Number	FDC-[redacted]
System Time	Mon Oct 26 12:49:15 2020 PDT [Change]
Firmware Version	v3.2.0,build[redacted] (Interim)[Update]
Firmware License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 3 hour(s) 3 minute(s)

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.
- 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 FortiManaager 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).

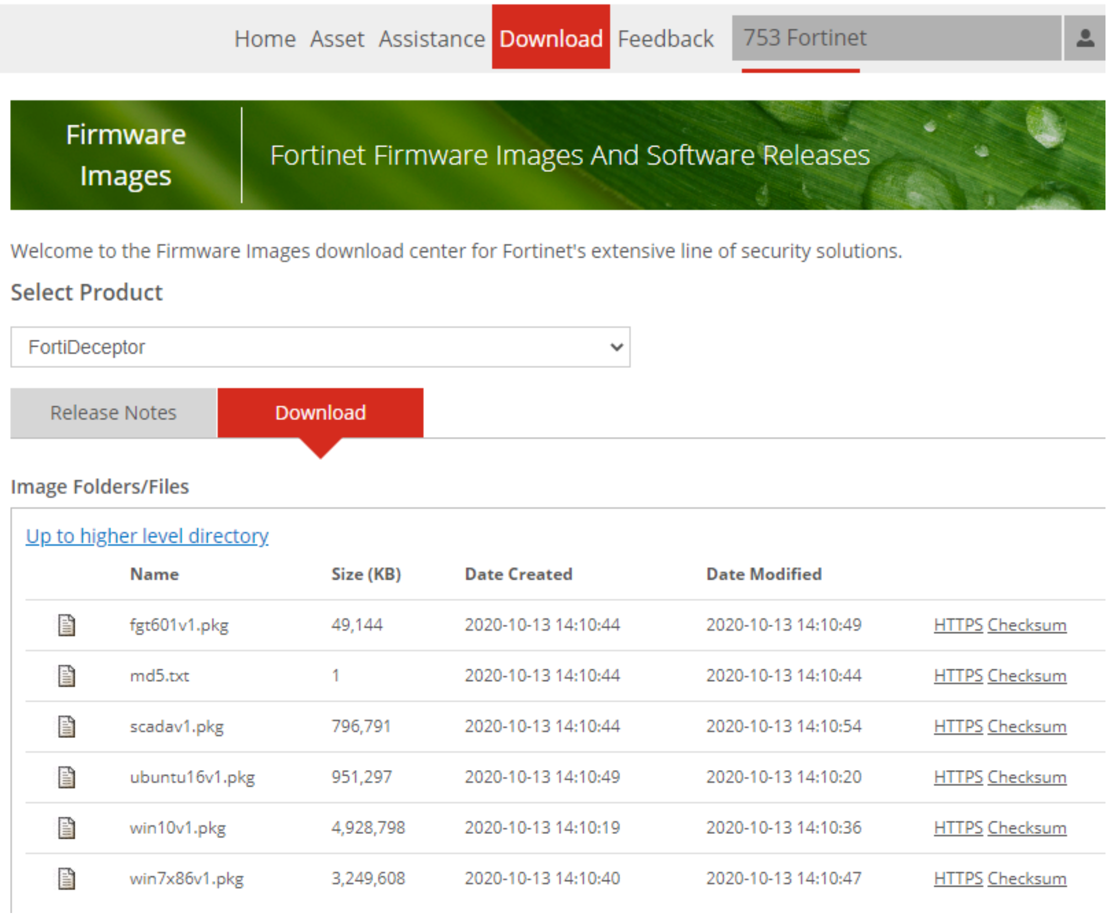
Importing deception VMs in an offline or air-gapped network

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.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select FortiDeceptor and then click *Download*.

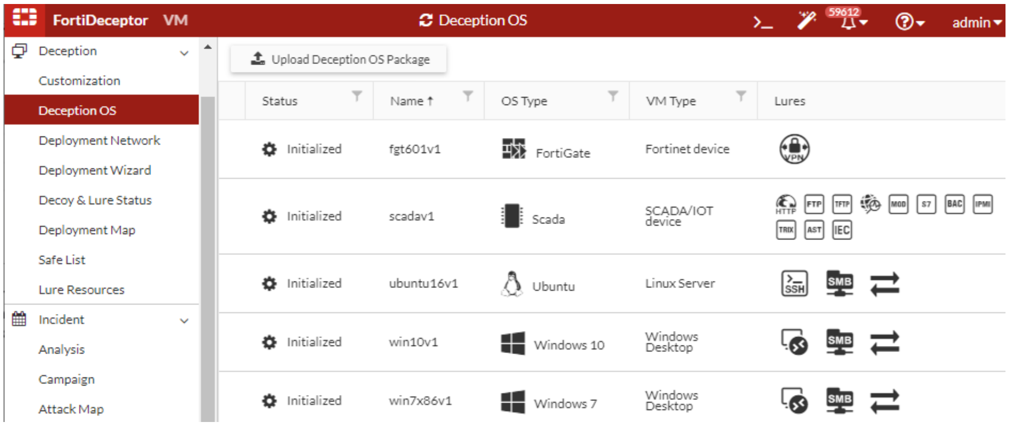
4. Click *v.3.00* to see the list of deception OS VM files.



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

Name	Size (KB)	Date Created	Date Modified	
fgt601v1.pkg	49,144	2020-10-13 14:10:44	2020-10-13 14:10:49	HTTPS Checksum
md5.txt	1	2020-10-13 14:10:44	2020-10-13 14:10:44	HTTPS Checksum
scadav1.pkg	796,791	2020-10-13 14:10:44	2020-10-13 14:10:54	HTTPS Checksum
ubuntu16v1.pkg	951,297	2020-10-13 14:10:49	2020-10-13 14:10:20	HTTPS Checksum
win10v1.pkg	4,928,798	2020-10-13 14:10:19	2020-10-13 14:10:36	HTTPS Checksum
win7x86v1.pkg	3,249,608	2020-10-13 14:10:40	2020-10-13 14:10:47	HTTPS Checksum

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



Status	Name ↑	OS Type	VM Type	Lures
Initialized	fgt601v1	FortiGate	Fortinet device	VPN
Initialized	scadav1	Scada	SCADA/IOT device	HTTP FTP TFTP MOD S7 BAC IPMI TRIX AST IEC
Initialized	ubuntu16v1	Ubuntu	Linux Server	SSH SMB ⇄
Initialized	win10v1	Windows 10	Windows Desktop	SMB ⇄
Initialized	win7x86v1	Windows 7	Windows Desktop	SMB ⇄

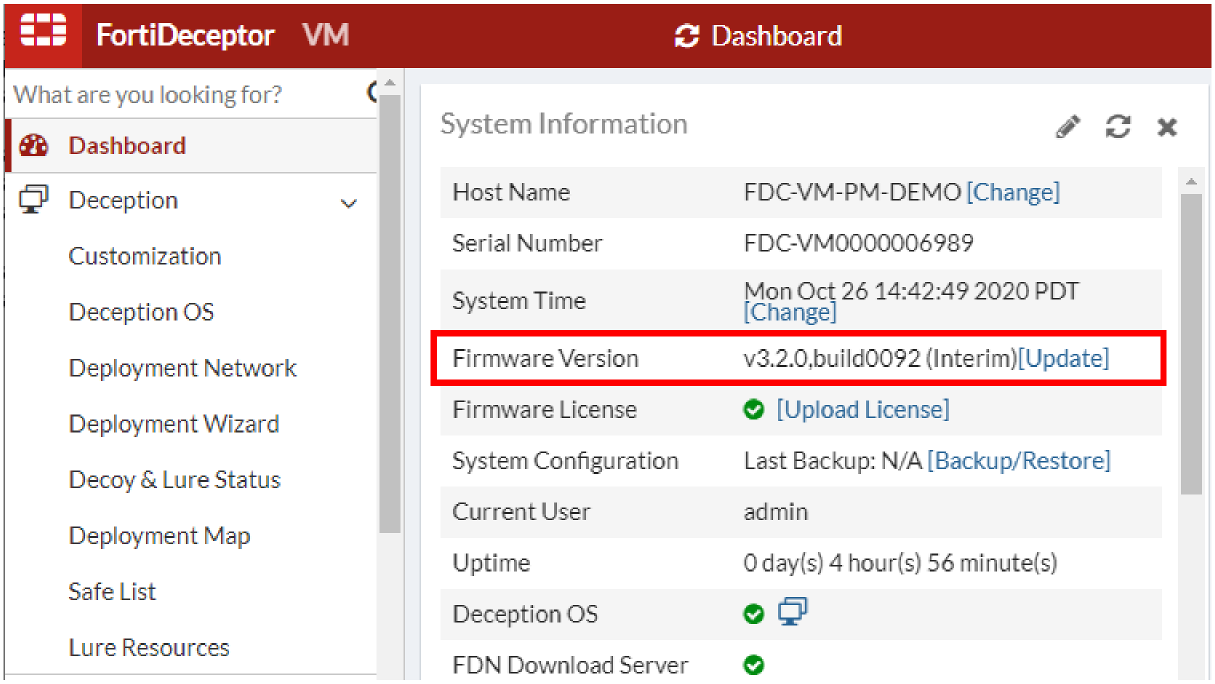
FortiDeceptor imports the images, verifies image integrity and other security layers, confirms that the images are the originals, and then initializes them. After initialization the *Deception OS* window *Status* column shows these images as *Initialized*.

Importing firmware in an offline or air-gapped network

This topic shows how to download and import FortiDeceptor 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*.



Host Name	FDC-VM-PM-DEMO [Change]
Serial Number	FDC-VM0000006989
System Time	Mon Oct 26 14:42:49 2020 PDT [Change]
Firmware Version	v3.2.0,build0092 (Interim)[Update]
Firmware License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 4 hour(s) 56 minute(s)
Deception OS	✓
FDN Download Server	✓

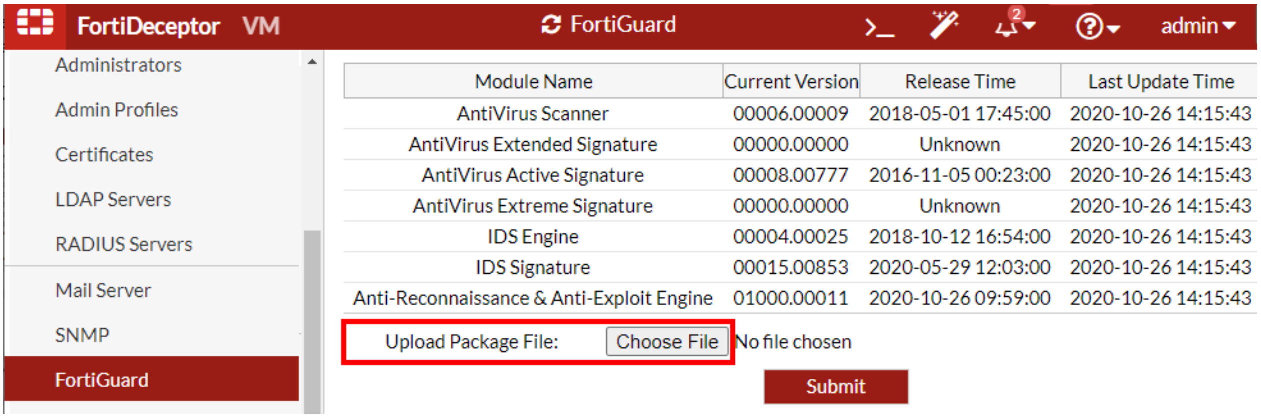
9. Locate the firmware file and click *Submit*.
   FortiDeceptor reboots after the update.

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

This topic shows how to download and import a FortiDeceptor FDS package 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.



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

Upload Package File: Choose File No file chosen

Submit

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:

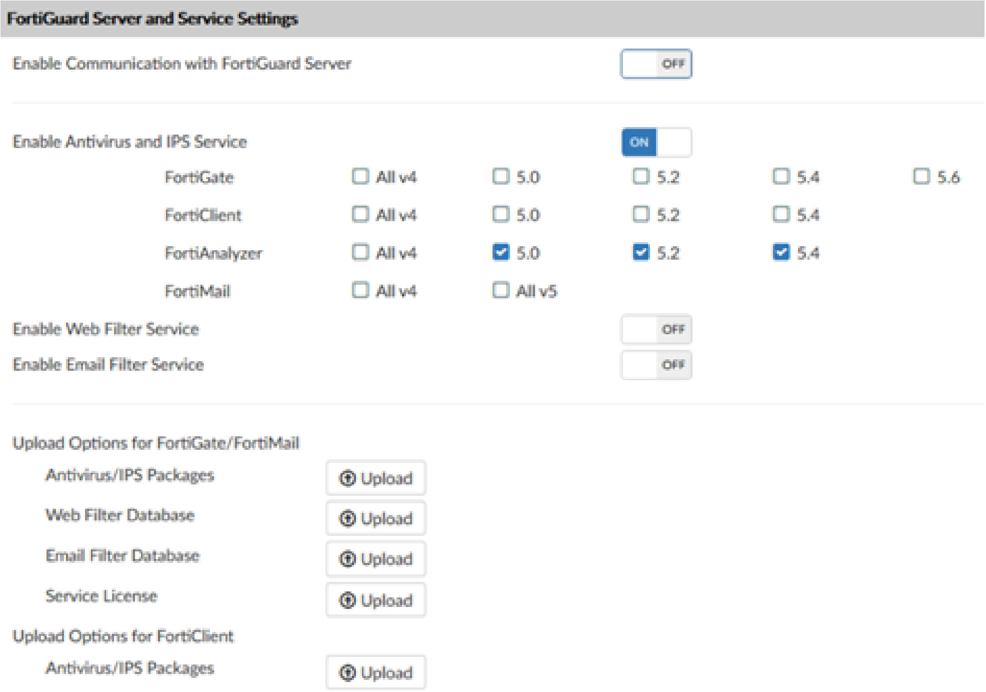
1. Log into Customer Service and Support.
2. Go to *Assistance* > *Create a Ticket*.
3. Expand *Customer Service* and click *Submit Ticket*.

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: OFF

Enable Antivirus and IPS Service: ON

FortiGate	□ All v4	□ 5.0	□ 5.2	□ 5.4	□ 5.6
FortiClient	□ All v4	□ 5.0	□ 5.2	□ 5.4	
FortiAnalyzer	□ All v4	☑ 5.0	☑ 5.2	☑ 5.4	
FortiMail	□ All v4	□ All v5			

Enable Web Filter Service: OFF

Enable Email Filter Service: OFF

Upload Options for FortiGate/FortiMail
- Antivirus/IPS Packages: Upload
- Web Filter Database: Upload
- Email Filter Database: Upload
- Service License: Upload

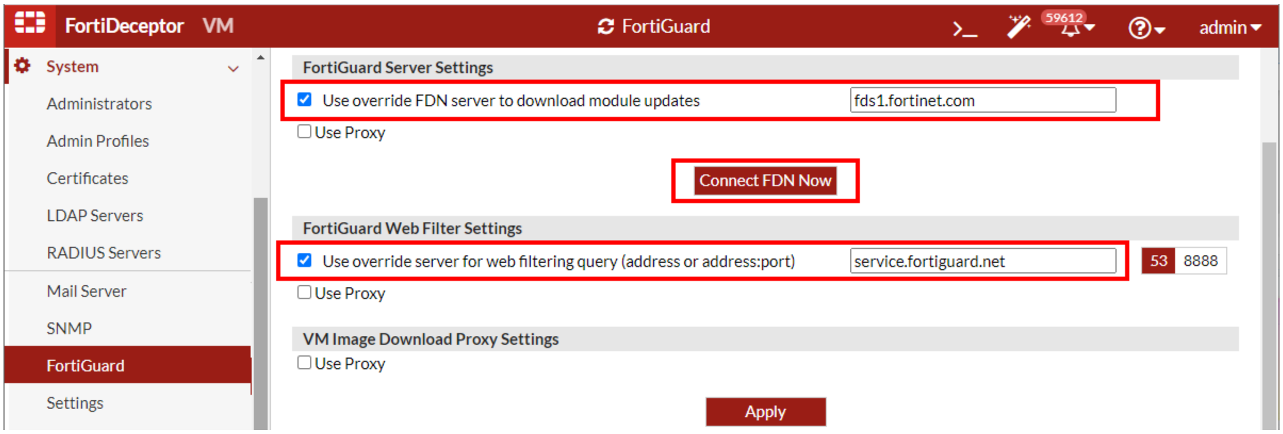
Upload Options for FortiClient
- Antivirus/IPS Packages: Upload

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.



☑ Use override FDN server to download module updates: fds1.fortinet.com

□ Use Proxy

☑ Use override server for web filtering query (address or address:port): service.fortiguard.net 53 8888

□ Use Proxy

□ Use Proxy

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

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 techniques 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, 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 be used only for detection from where the attackers are coming and what they want 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 parts, breadcrumbs, baits, and lures. Deception systems are implemented alongside enterprise systems but they are still 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 oblivious vulnerabilities to know the identity and 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 traps.
- 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.
- Tackle the human attacker or APT.
- 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 engageswith 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 79
- FortiDeceptor lures on page 79
- FortiDeceptor decoys on page 80

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 lures

The role of the FortiDeceptor lure package is to add breadcrumbs on real endpoints and servers, and redirect an attacker to engage with a decoy instead of a real asset. Deception lures 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:
  - SMB
  - RDP
  - SSH
- Linux:
  - SMB (SAMBA)
  - RDP (xfreerdp)
  - SSH

- MAC:
  - SMB (SAMBA)
  - RDP (xfreerdp)
  - SSH

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 attackers attack a decoy, first, an alert is generated; second, their malicious activities are captured and analyzed in real-time to generate a mitigation and remediation response that protects the network.

The current FortiDeceptor decoys are:

- Windows:
  - Windows 7
  - Windows 10 (can be deployed as a gold image)
  - Windows 2016 (deployed as a gold image)
  - Windows 2019 (deployed as a gold image)
- Linux:
  - Ubuntu Desktop
- IoT/OT:
  - SCADA
  - 8 OT protocols
- VPN:
  - Fortinet SSL-VPN (FG-60E, FG-100F, FG-1500D, FG-2000E, FG-3700D)

The current FortiDeceptor monitor services are:

- Windows:
  - RDP
  - SMB
- Linux
  - SSH
  - SAMBA
- IoT/OT:
  - HTTP
  - FTP
  - TFTP
  - SNMP
  - MODBUS
  - S7COMM
  - BACNET
  - IPMI
  - TRICONEX

  - GUARDIAN-AST
  - IEC104
- SSL VPN:
  - HTTPS

The current FortiDeceptor IP address capacity are:

- A single FortiDeceptor appliance (HW/VM) can host up to 16 deception VMs.
- A single deception VM supports up to 16 IP addresses or decoys, Each IP represent a decoy.
- A single FortiDeceptor appliance (HW/VM) can support up to 256 IP addresses.
- With 4 decoys per segment on average, a single FortiDeceptor appliance (HW/VM) can support up to 64 segments (VLANS).

Deploying deception

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

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 lure best practices

Deception effectiveness requires deployment across all managed endpoints and servers.

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

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

RDP lure

- 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 lure

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

- Set up at least two Windows server decoys that support two fake network share access.
- Generate at least two lures 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 lures package and deploy it over all the network endpoints.

SAMBA lure

For Windows endpoints, use either SMB lure or SAMBA lure. 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 lures with two different share names.
- Use a share name similar to the company structure.
- Follow company username and password policy.
- Generate a single deception lures 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 lures 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 82.
- 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	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. If the firewalls are different, check with Customer Support on how to configure an L2 Tunnel.

Deception Items	Customer Requirements	Deployment
Remote sites are office / OT network	1 remote office + 1 manufacture site	For remote office site, deploy Windows / Linux desktop decoys and deception lures like SMB, RDP and cache credentials. For remote OT site, deploy Windows / Linux and SCADA decoys.
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.
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.

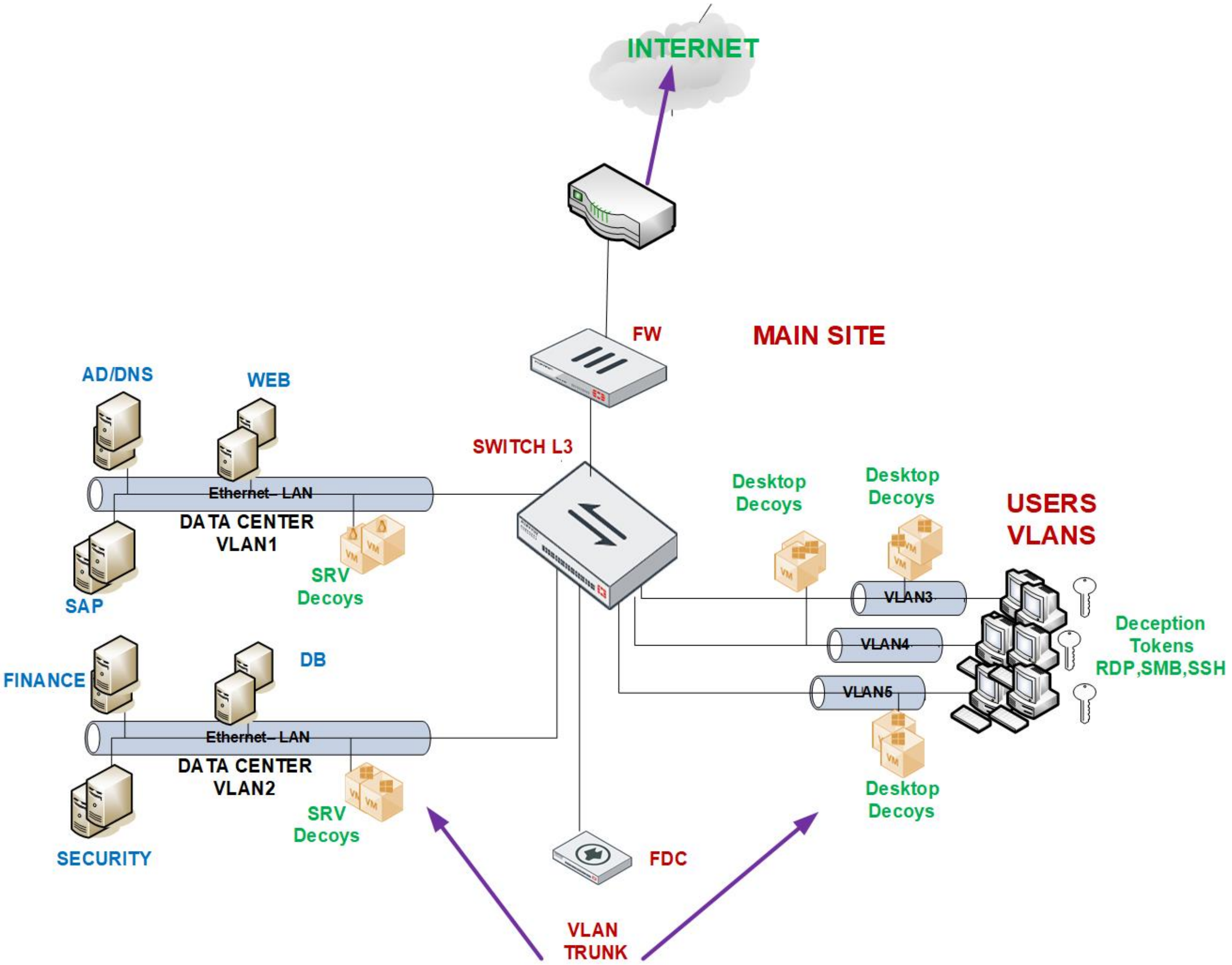
This topic provides best practices for the following scenarios:

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.



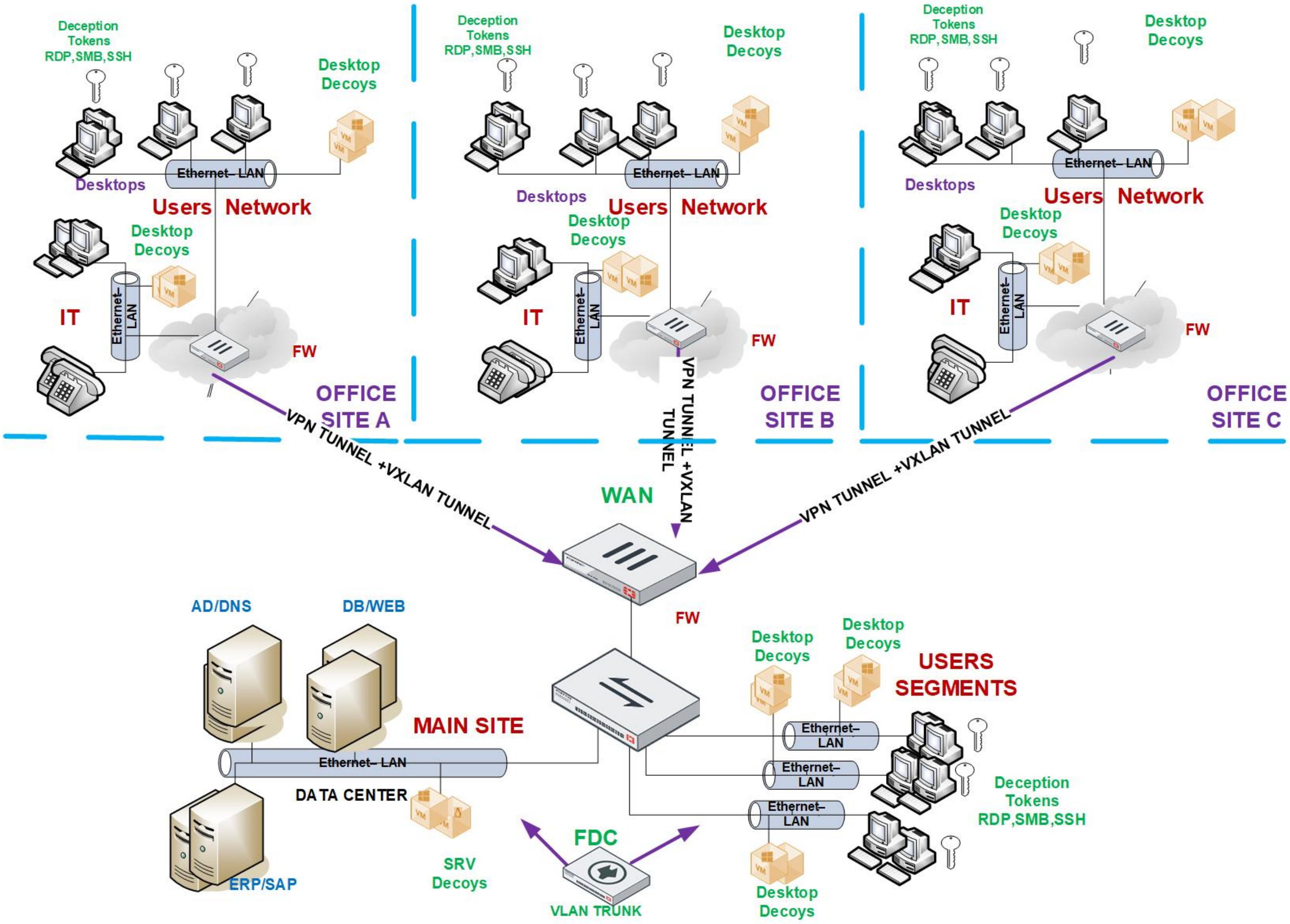
In this scenario, follow these best practice recommendations:

- 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 82.
  - 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.
    - 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.

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.



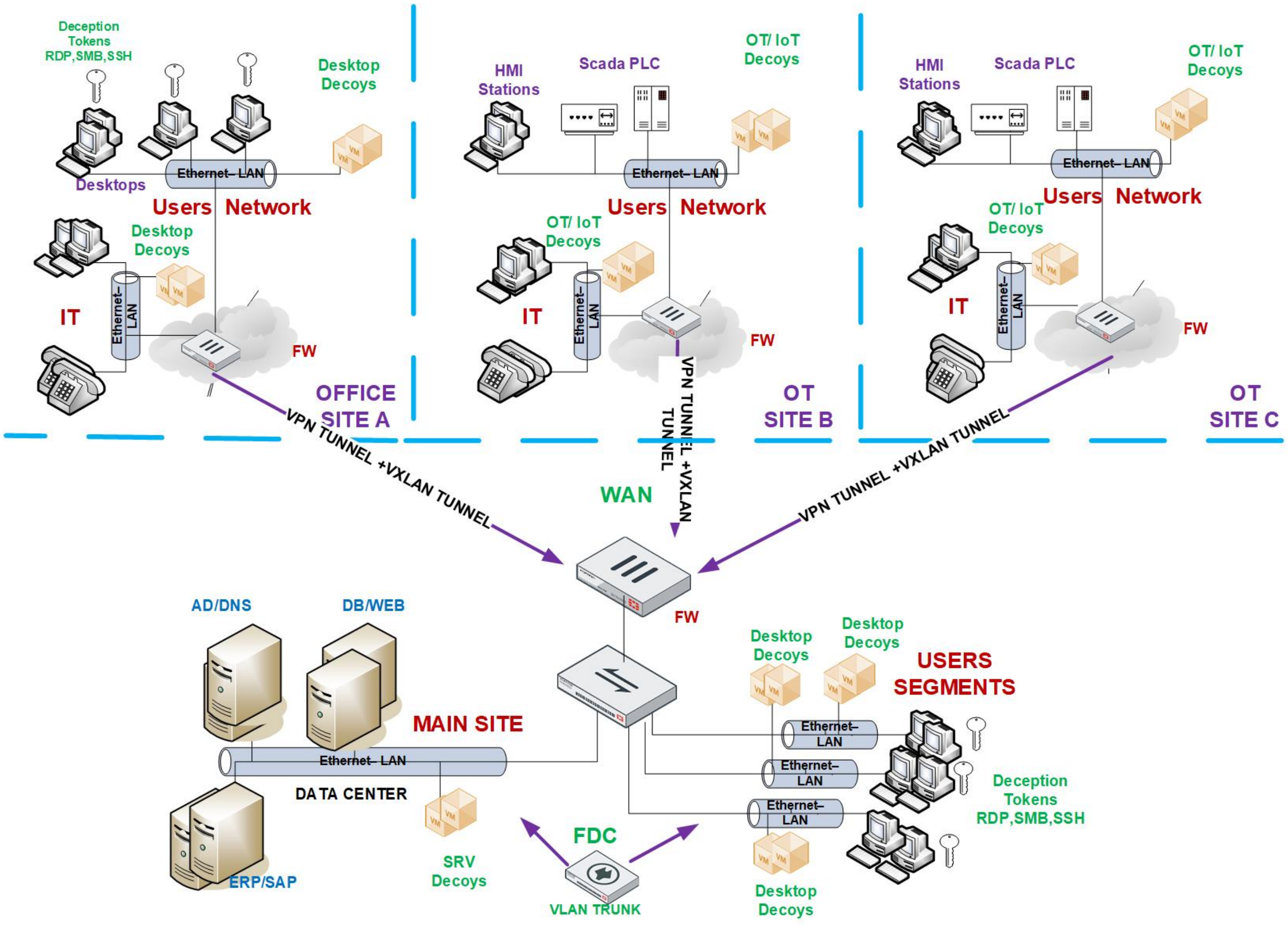
In this scenario, follow these best practice recommendations:

- Deploy a single FortiDeceptor appliance and connect it to the network via trunk to cover most of the HQ network VLANs.
- FortiDeceptor currently does not have a central management capability so you must configure the VXLAN tunnel between the HQ firewall and each of the remote office firewall. 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.
- These are the requirements for deploying deception lures in remote desktops:
  - No VXLAN tunnel between both firewalls.
  - The remote site has only 1-2 VLANS (risk vs. cost).
- Deploy decoys following the best practice recommendation in Deception decoy best practices on page 82.
  - 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.
  - 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.

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.

- FortiDeceptor currently does not have a central management capability so you must configure the VXLAN tunnel between the HQ firewall and each of the remote office firewall. See https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/22733/virtual-wire-pair-with-vxlan.
- These are the requirements for deploying deception lures in remote desktops:
  - No VXLAN tunnel between both firewalls, that is, no deception lures on OT site desktops.
    If you must install FortiDeceptor at OT sites, you must deploy FortiDeceptor as a standalone device and forward the SYSLOG to a central SIEM or any logger solution.
  - The remote site has only 1-2 VLANS (risk vs. cost).
- Deploy decoys following the best practice recommendation in Deception decoy best practices on page 82.
  - On data center VLANs: 5-7 decoys per VLAN.
  - On endpoint VLANs: 2-4 decoys per VLAN on HQ and remote offices.
  - On OT VLANs: 7-10 decoys (OT decoys and IT decoys for HMI/SCADA management systems.
  - Deploy deception lures across all manageable endpoints even if some of them are in remote sites.
    - RDP.
    - SMB.
    - 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.

Attack vectors vs deception

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

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.

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 web browser deception lures that store fake URLs and bookmarks with saved usernames and passwords in the browser. Browser lures cannot be hidden from the user so you might get false alerts from a legitimate user.

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

Use AD lures that register all decoys at the AD or DNS level.

Use decoy hostname features to configure attractive hostnames.

Use network connection deception lures to inject fake ARP entries and TCP connections to a fake decoy.

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.
- 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

Use RDP lures that save usernames, passwords, and IP addresses in the Windows Credential Manager.

Deploy at least 5-7 Windows decoys on each server VLAN.

Deploy 2-4 endpoint decoys on each endpoint VLAN.

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.
- 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_XXXXXXXXX` 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:

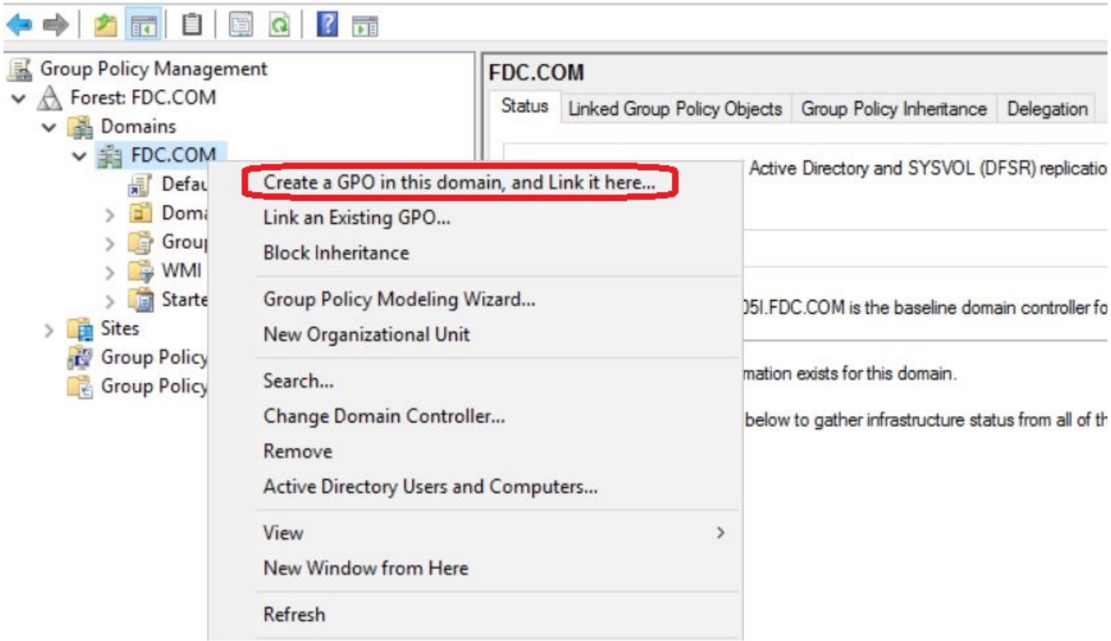
1. Download the deception lure package from the FortiDeceptor Admin Console.
2. Unzip the downloaded file to a temporary location.
3. Open the unzipped file and access the `windows` directory.
4. Copy the following from the `windows` directory:
   - `windows_token.exe`
   - `res` directory.
5. On the 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 /H /K /F /C /Y /I "%SFolder%\windows_token.exe" "%DFolder%\windows_token.exe*"
xcopy /E /S /H /K /F /C /Y /I "%SFolder%\res" "%DFolder%\res"
start /B /WAIT /MIN "windows_token" "%DFolder%\windows_token.exe" )
exit
```

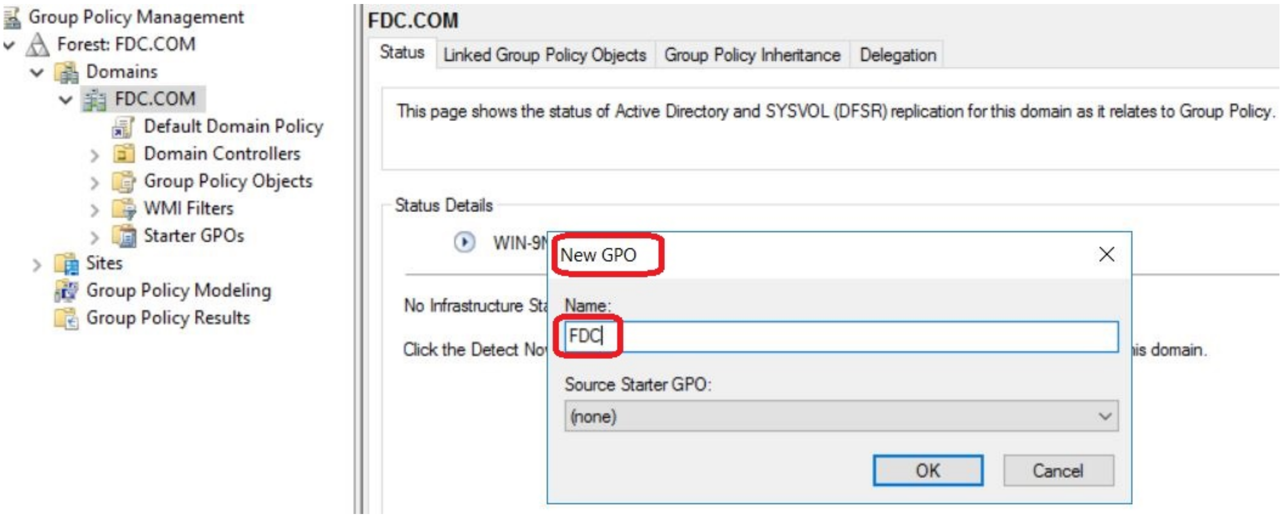
Configuring the GPO logon script

To configure the GPO logon script:

1. Log into the AD server and open the Group Policy Management tool.
   You can also open this tool using the CLI `gpmc.msc`.
2. 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.


Group Policy Management
Forest: FDC.COM
Domains
FDC.COM
Defau
Doma
Grou
WMI
Starte
Sites
Group Policy
Group Policy
FDC.COM
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
View
New Window from Here
Refresh
Active Directory and SYSVOL (DFSR) replicatio
)5I.FDC.COM is the baseline domain controller fo
mation exists for this domain.
below to gather infrastructure status from all of th

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



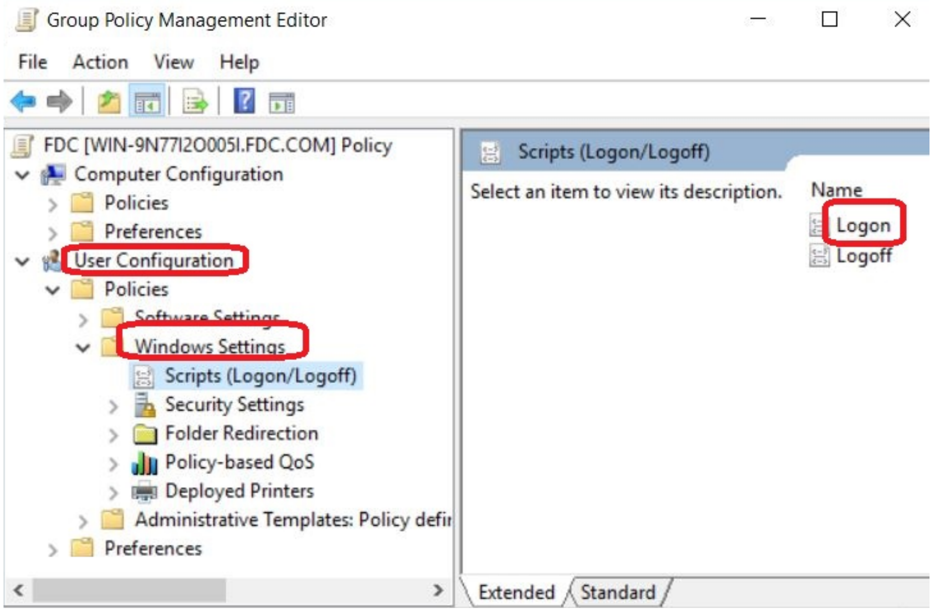
This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.

Name: FDC

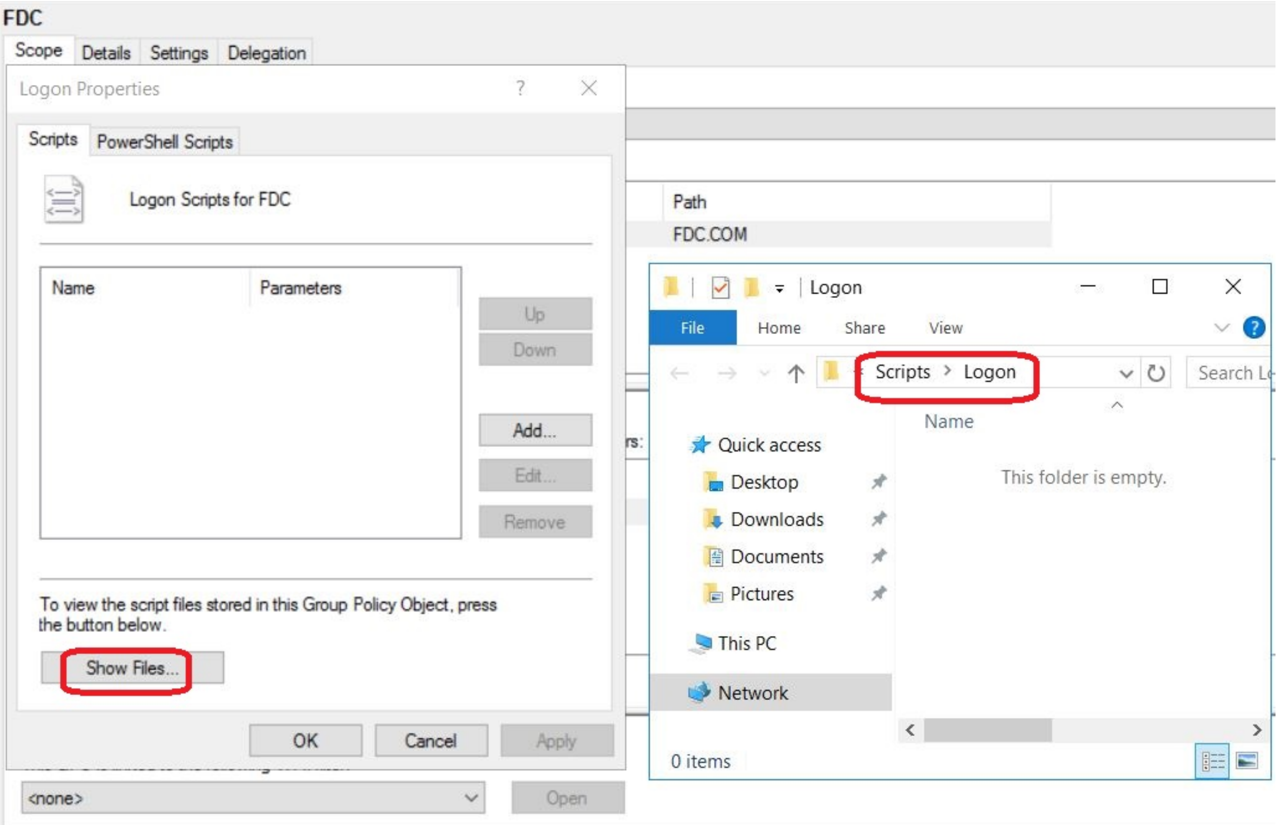
Source Starter GPO: (none)

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.

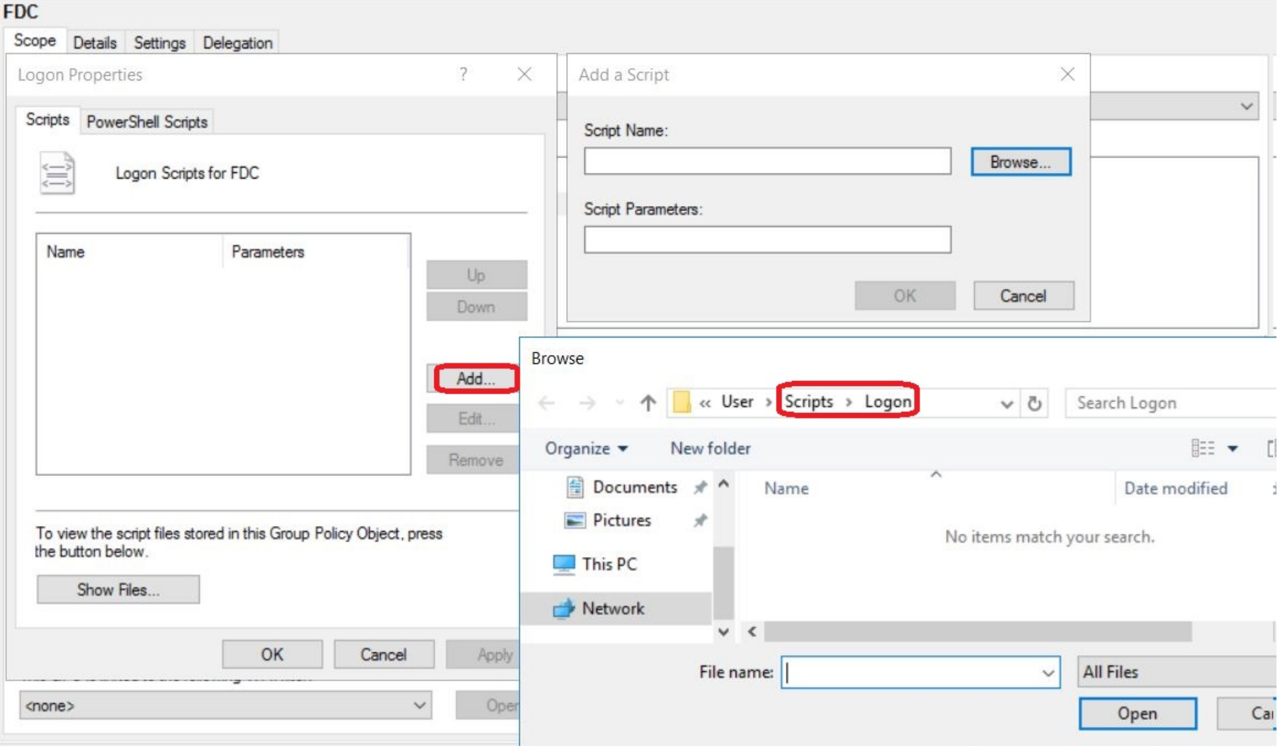


7. In the *Logon Properties* dialog box, click *Show Files*.
8. Copy the batch file `Lure.bat` that you have prepared.



9. In 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)*.



Logon Scripts for FDC

To view the script files stored in this Group Policy Object, press the button below.

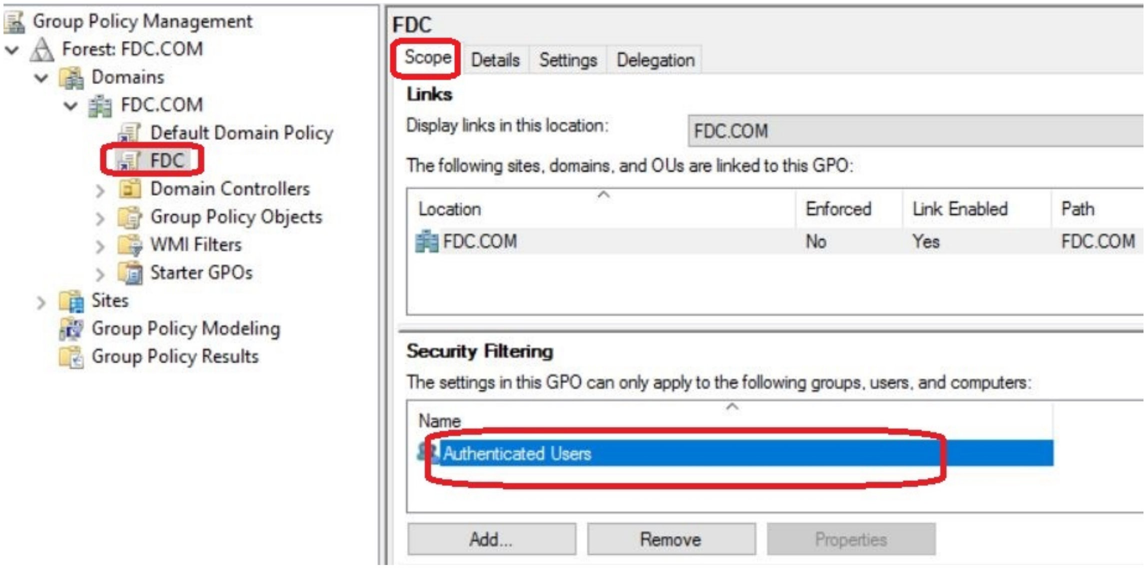
No items match your search.

<none>

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*.



Links

Display links in this location: FDC.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
FDC.COM	No	Yes	FDC.COM

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

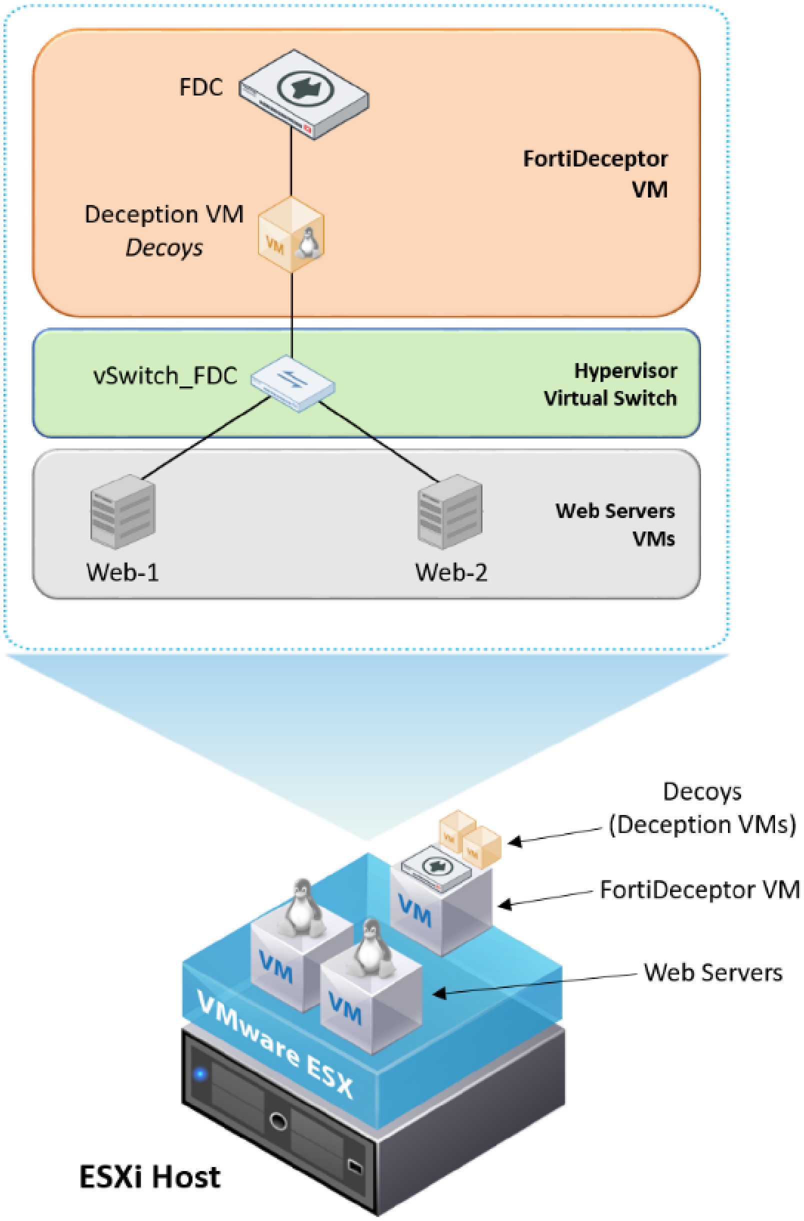
Configuring trunk ports on FortiDeceptor VM

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.

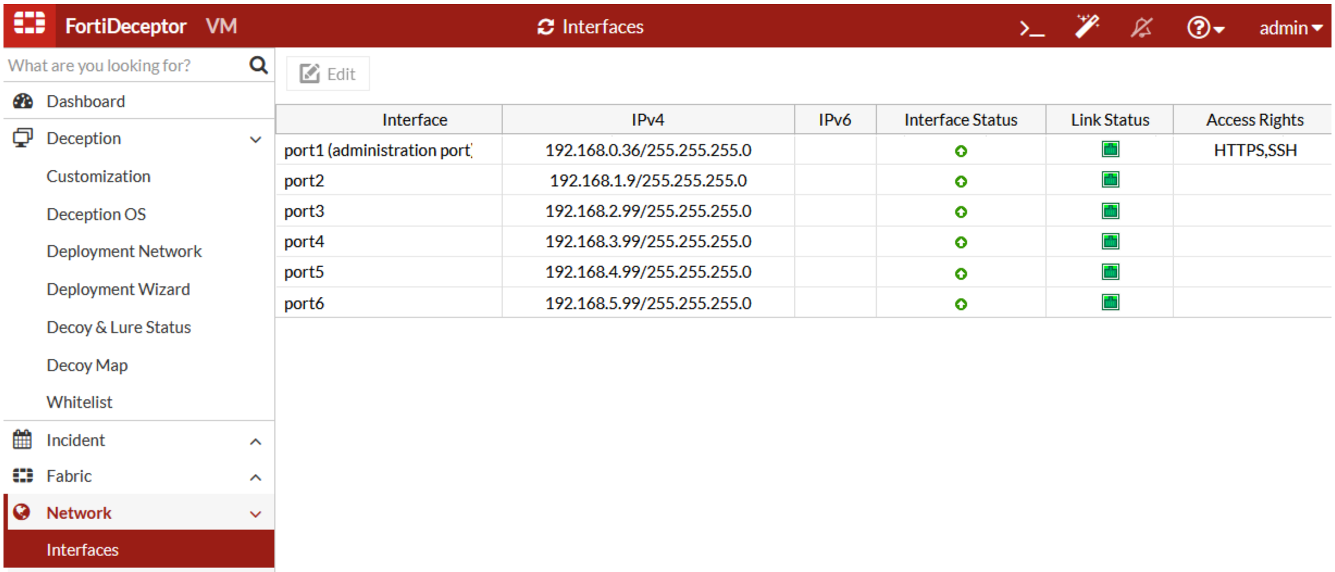
Set up a single ESXi host with the following workloads.

- 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.

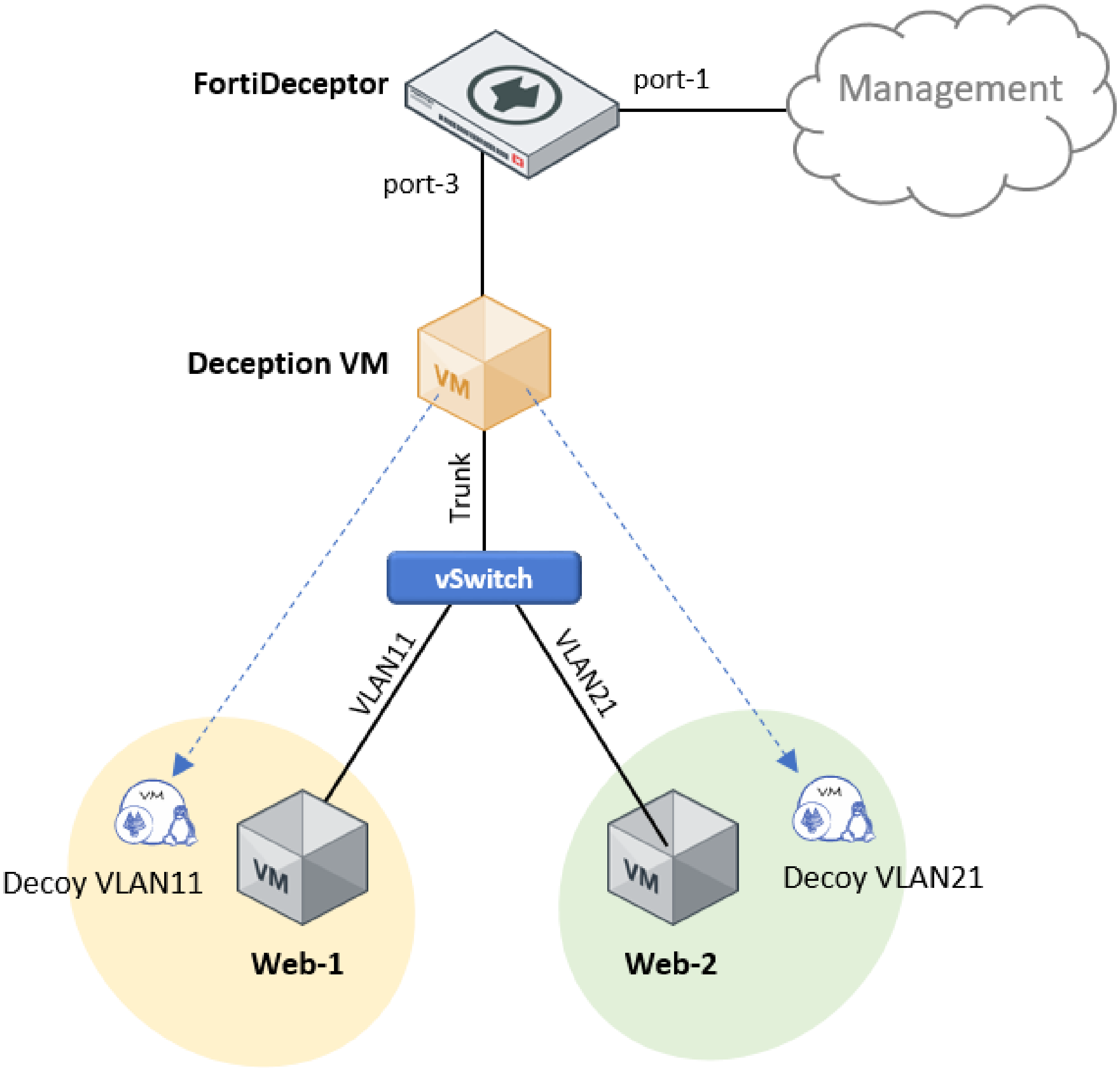
- Reserve port1 for device management.
- Use the other ports to deploy deception decoys.



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.



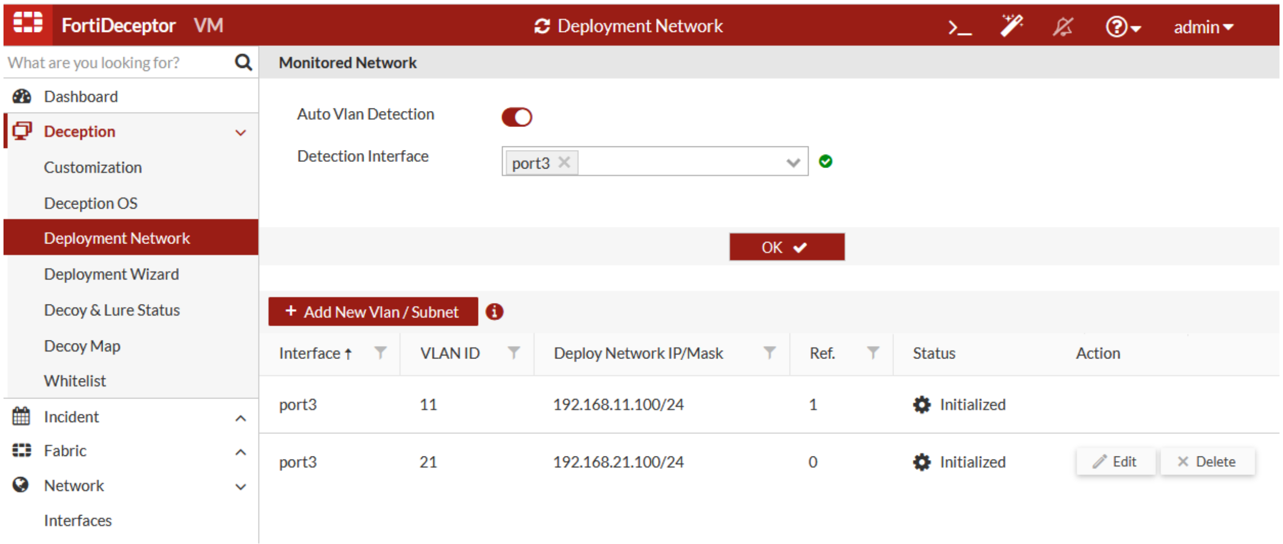
The deception VM has a single network interface to monitor two different VLANs so it is necessary to configure VLAN trunking between port3 and the ESXi vSwitch port. There is only one vSwitch to connect all the devices together using different virtual ports for each device.

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.



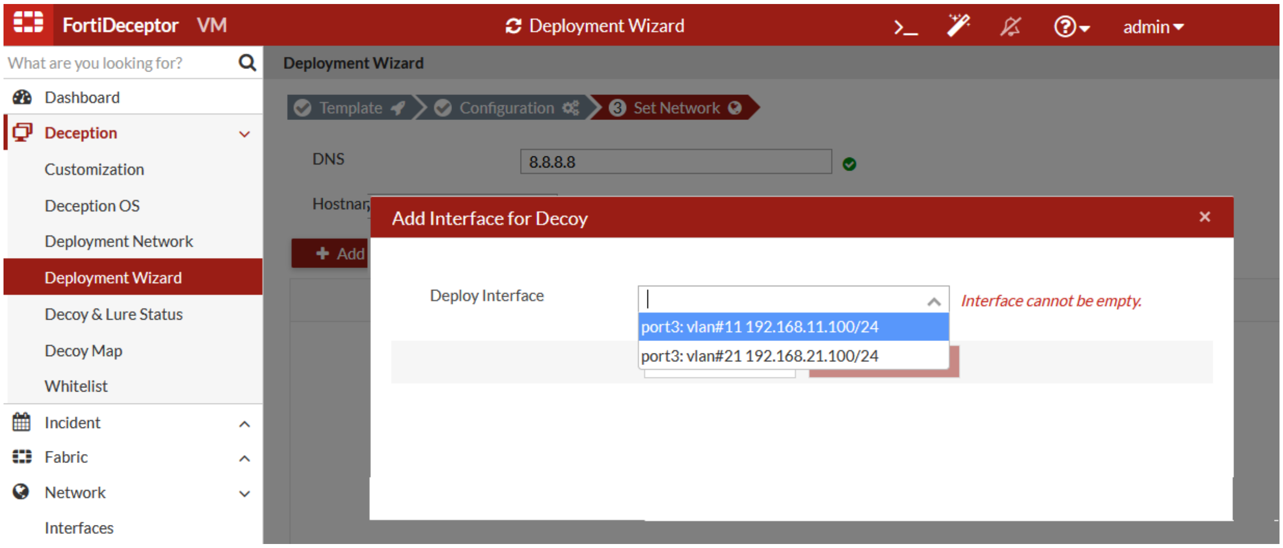
Monitored Network

Auto Vlan Detection: on

Detection Interface: port3

Interface	VLAN ID	Deploy Network IP/Mask	Ref.	Status	Action
port3	11	192.168.11.100/24	1	Initialized	
port3	21	192.168.21.100/24	0	Initialized	Edit Delete

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.



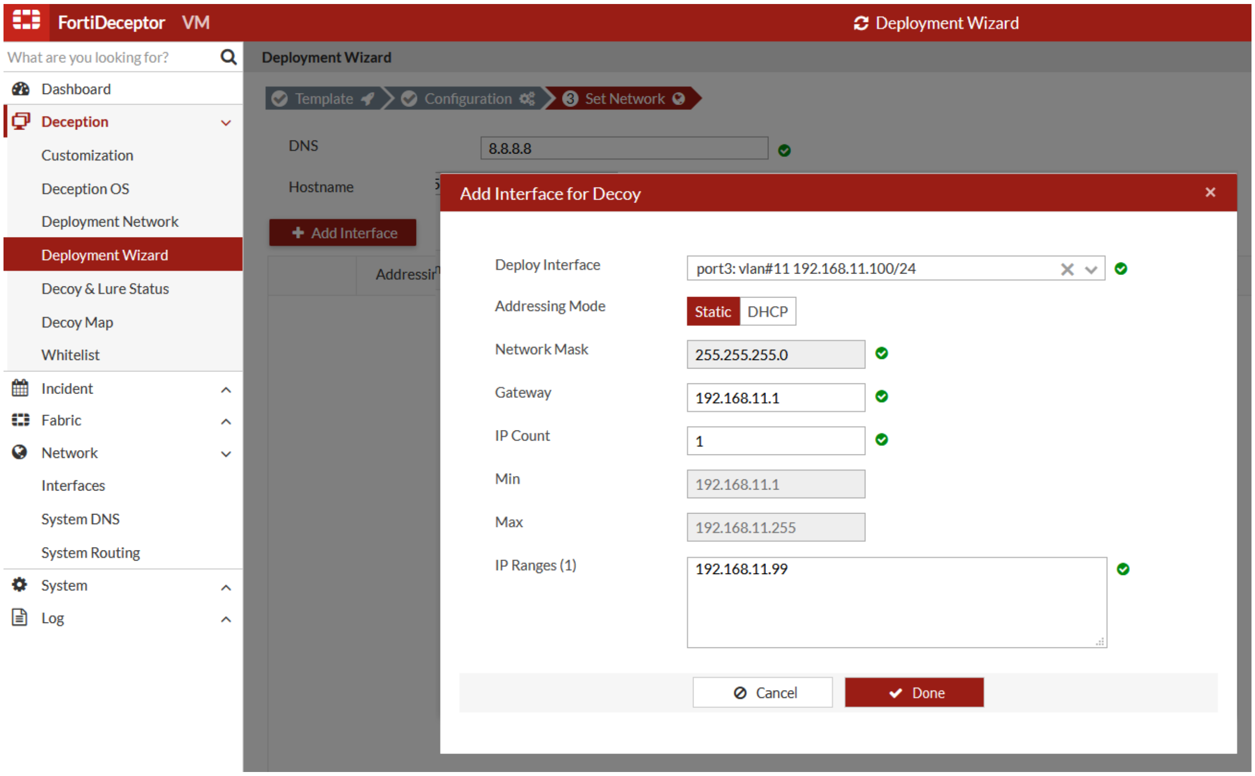
DNS: 8.8.8.8

Deploy Interface:

- port3: vlan#11 192.168.11.100/24
- port3: vlan#21 192.168.21.100/24

Interface cannot be empty.

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*.

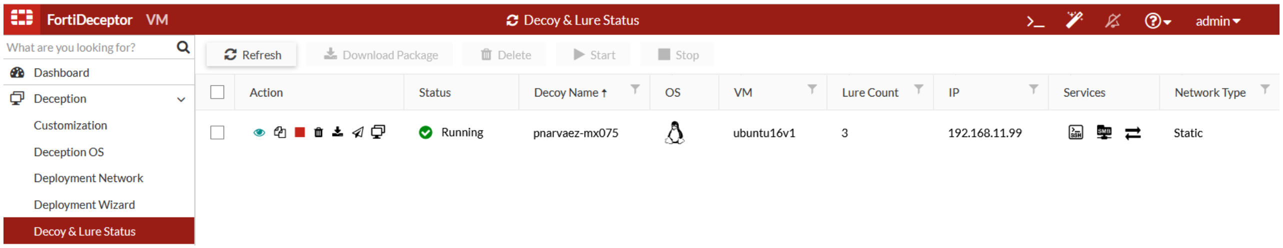


DNS	8.8.8.8
Hostname	

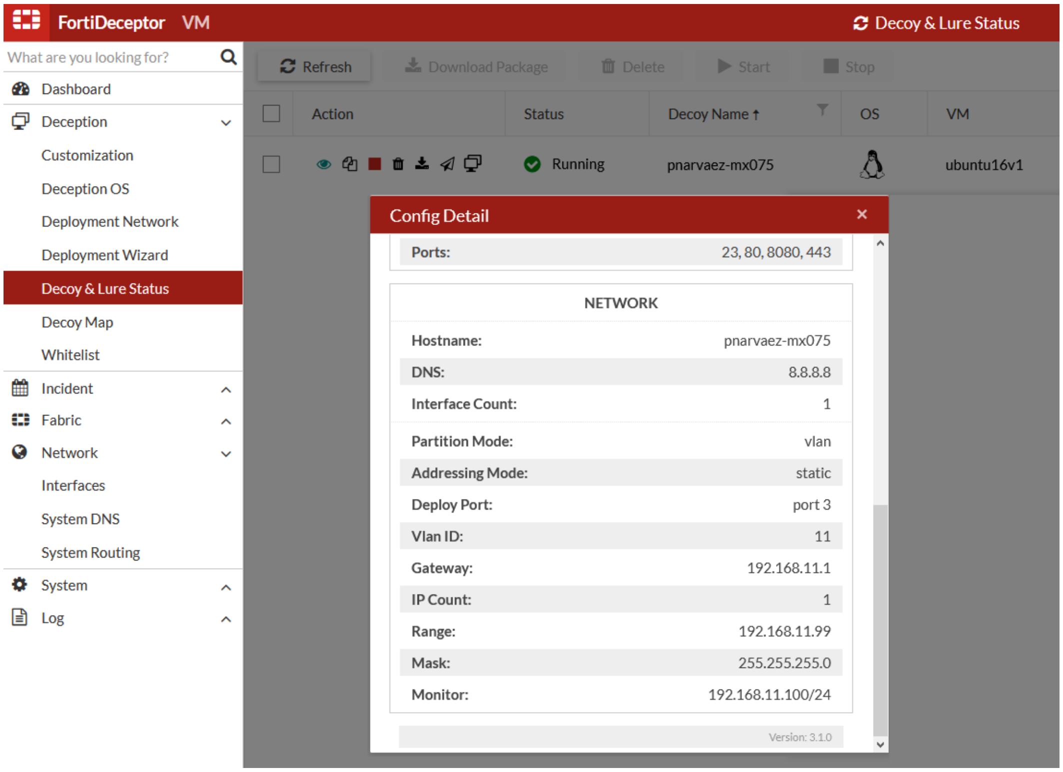
Add Interface for Decoy

Deploy Interface	port3: vlan#11 192.168.11.100/24
Addressing Mode	Static DHCP
Network Mask	255.255.255.0
Gateway	192.168.11.1
IP Count	1
Min	192.168.11.1
Max	192.168.11.255
IP Ranges (1)	192.168.11.99

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



□	Action	Status	Decoy Name ↑	OS	VM	Lure Count	IP	Services	Network Type
□		✓ Running	pnarvaez-mx075		ubuntu16v1	3	192.168.11.99		Static



Action	Status	Decoy Name ↑	OS	VM
	Running	pnarvaez-mx075		ubuntu16v1

Config Detail

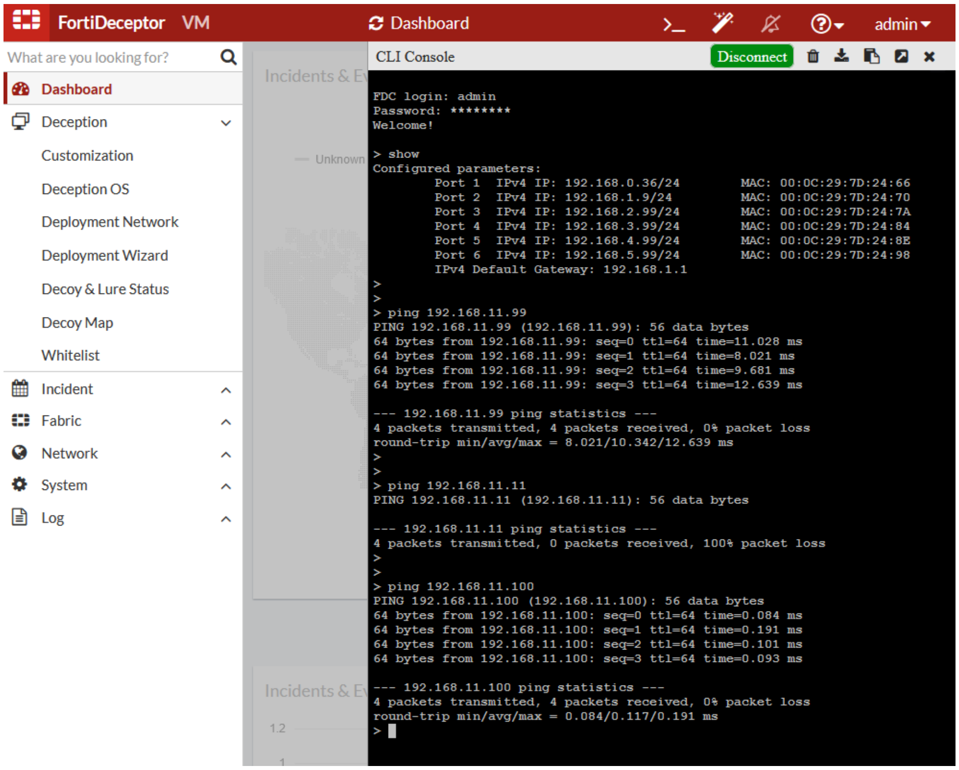
Ports:	23, 80, 8080, 443

NETWORK

Hostname:	pnarvaez-mx075
DNS:	8.8.8.8
Interface Count:	1
Partition Mode:	vlan
Addressing Mode:	static
Deploy Port:	port 3
Vlan ID:	11
Gateway:	192.168.11.1
IP Count:	1
Range:	192.168.11.99
Mask:	255.255.255.0
Monitor:	192.168.11.100/24

Version: 3.1.0

7. 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.



```
FDC login: admin
Password: ********
Welcome!

> show
Configured parameters:
        Port 1  IPv4 IP: 192.168.0.36/24        MAC: 00:0C:29:7D:24:66
        Port 2  IPv4 IP: 192.168.1.9/24         MAC: 00:0C:29:7D:24:70
        Port 3  IPv4 IP: 192.168.2.99/24        MAC: 00:0C:29:7D:24:7A
        Port 4  IPv4 IP: 192.168.3.99/24        MAC: 00:0C:29:7D:24:84
        Port 5  IPv4 IP: 192.168.4.99/24        MAC: 00:0C:29:7D:24:8E
        Port 6  IPv4 IP: 192.168.5.99/24        MAC: 00:0C:29:7D:24:98
        IPv4 Default Gateway: 192.168.1.1
>
>
> 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=11.028 ms
64 bytes from 192.168.11.99: seq=1 ttl=64 time=8.021 ms
64 bytes from 192.168.11.99: seq=2 ttl=64 time=9.681 ms
64 bytes from 192.168.11.99: seq=3 ttl=64 time=12.639 ms

--- 192.168.11.99 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 8.021/10.342/12.639 ms
>
>
> ping 192.168.11.11
PING 192.168.11.11 (192.168.11.11): 56 data bytes

--- 192.168.11.11 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
>
>
> 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=0.084 ms
64 bytes from 192.168.11.100: seq=1 ttl=64 time=0.191 ms
64 bytes from 192.168.11.100: seq=2 ttl=64 time=0.101 ms
64 bytes from 192.168.11.100: seq=3 ttl=64 time=0.093 ms

--- 192.168.11.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.084/0.117/0.191 ms
>
```

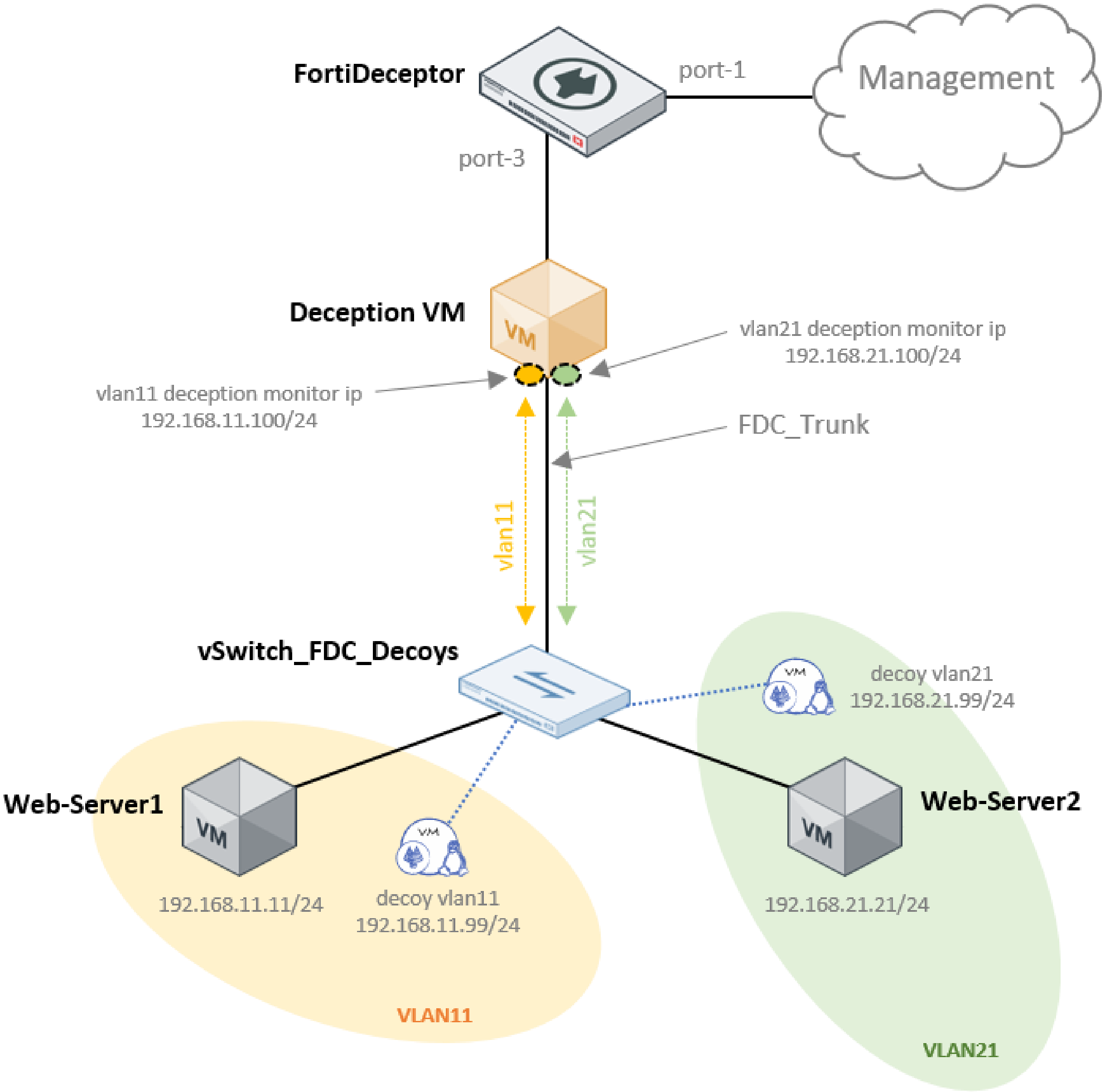
From the networking perspective, FortiDeceptor is ready to monitor both VLANs over port3. However, to activate the logical trunk interface, FortiDeceptor needs to receive VLAN trunking traffic from the vSwitch port.

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.

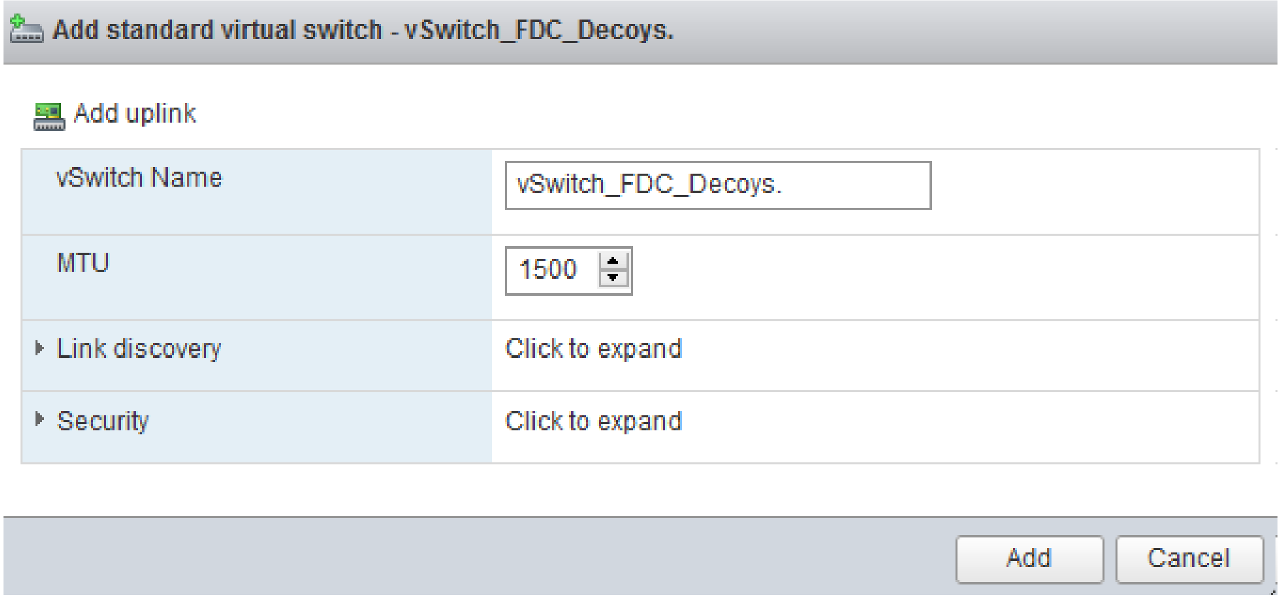


On ESXi, configure the *vSwitch_ FDC_Decoys* vSwitch to connect both VLANs to FortiDeceptor. Then configure three network port-groups:

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:

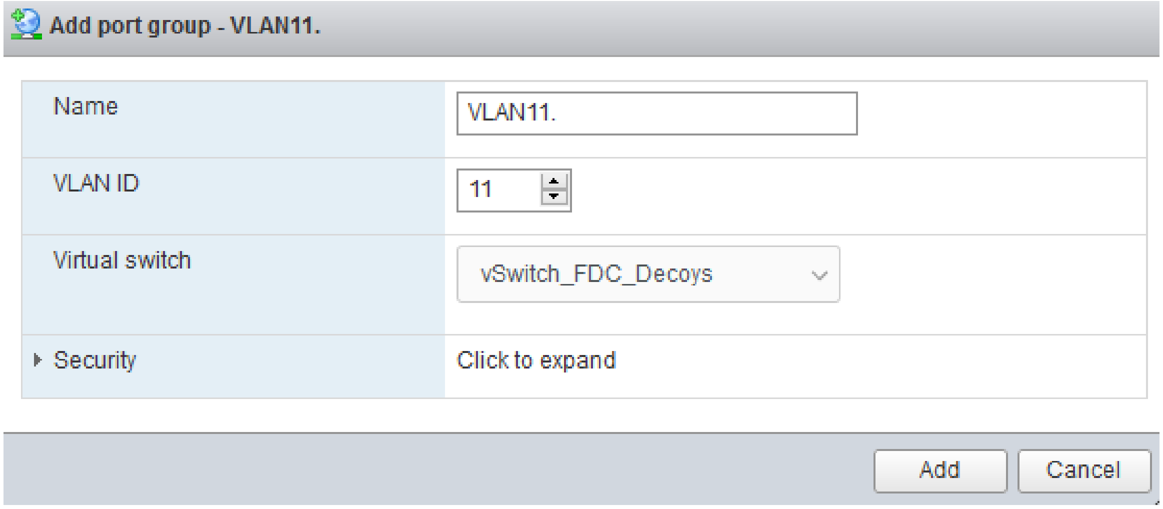
1. On the ESXi client, go to *Networking* > *Virtual Switches* and add a standard virtual switch.
   Just configure the *vSwtich Name*, remove the uplink (unless you need it), and use default values for the other options.



Add standard virtual switch - vSwitch_FDC_Decoys.

vSwitch Name	vSwitch_FDC_Decoys.
MTU	1500
▸ Link discovery	Click to expand
▸ Security	Click to expand

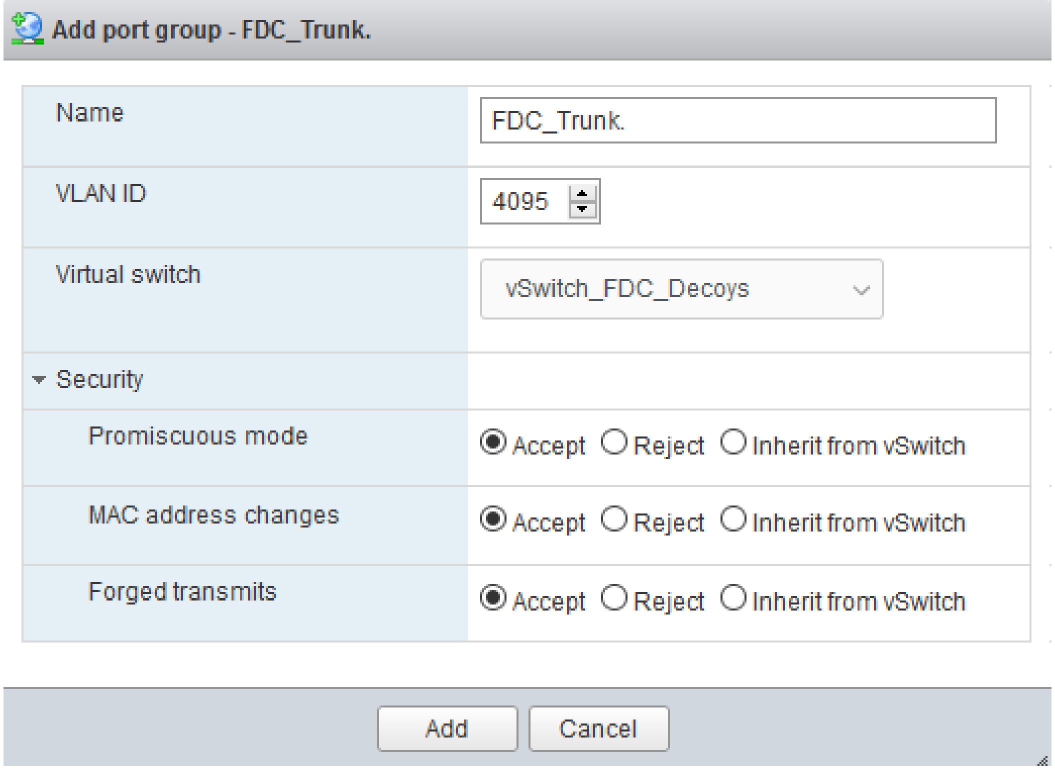
2. Go to *Networking* > *Port groups* and add the port groups.
   Port groups for VLAN11 and VLAN21 are similar. For each port group, specify a *Name*, configure the *VLAN ID*, and select the *Virtual switch*.



Add port group - VLAN11.

Name	VLAN11.
VLAN ID	11
Virtual switch	vSwitch_FDC_Decoys
▸ Security	Click to expand

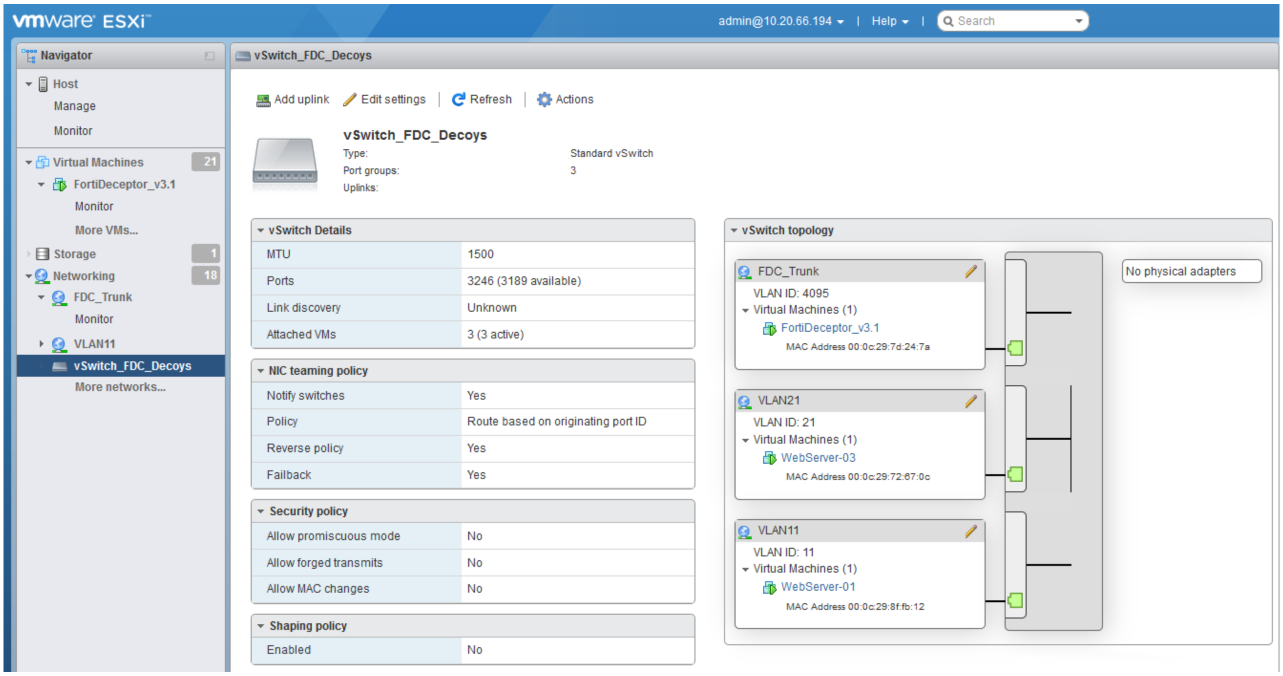
3. For the FDC Trunk port, configure a special port-group.
   On ESXi, you do not need to configure 802.1Q. You only need to set the port group to be a promiscuous interface and specify *4095* for the *VLAN ID* so the vSwitch can send and receive traffic from the VLANs configured on FortiDeceptor.
   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	● Accept ○ Reject ○ Inherit from vSwitch
MAC address changes	● Accept ○ Reject ○ Inherit from vSwitch
Forged transmits	● Accept ○ Reject ○ Inherit from vSwitch

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



vSwitch_FDC_Decoys

Type: Standard vSwitch
Port groups: 3
Uplinks:

vSwitch Details	
MTU	1500
Ports	3246 (3189 available)
Link discovery	Unknown
Attached VMs	3 (3 active)

NIC teaming policy	
Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes
Failback	Yes

Security policy	
Allow promiscuous mode	No
Allow forged transmits	No
Allow MAC changes	No

Shaping policy	
Enabled	No

vSwitch topology

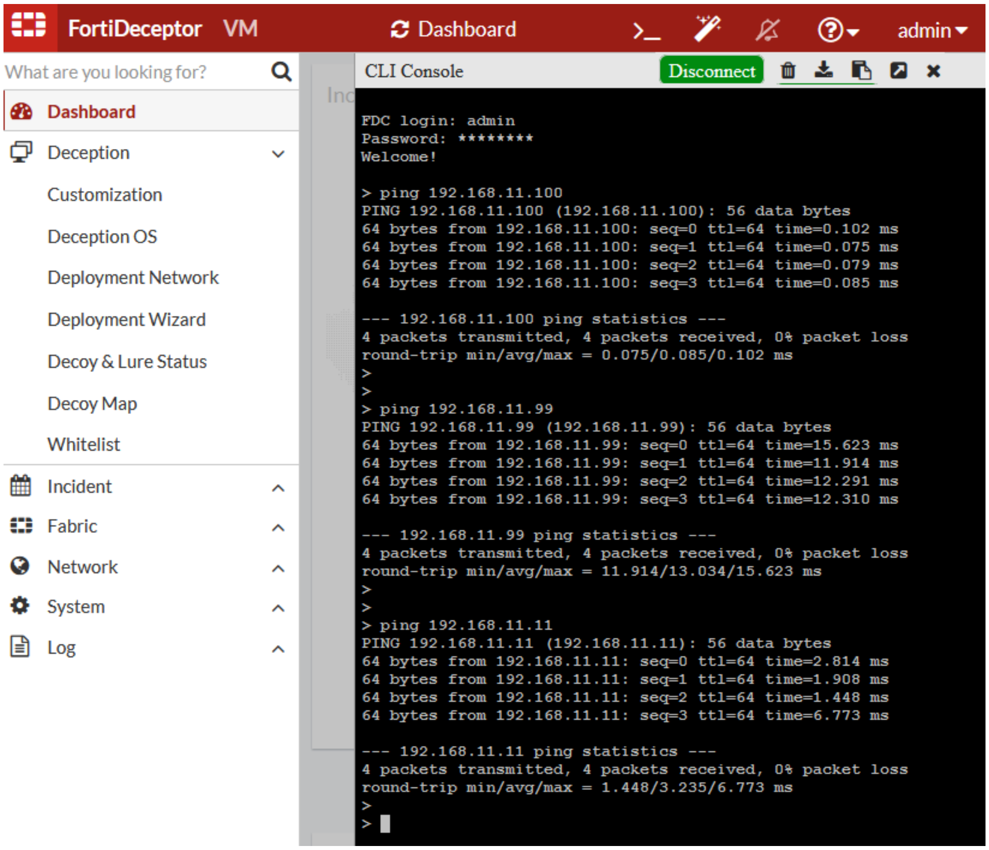
FDC_Trunk
VLAN ID: 4095
Virtual Machines (1)
FortiDeceptor_v3.1
MAC Address 00:0c:29:7d:24:7a

VLAN21
VLAN ID: 21
Virtual Machines (1)
WebServer-03
MAC Address 00:0c:29:72:67:0c

VLAN11
VLAN ID: 11
Virtual Machines (1)
WebServer-01
MAC Address 00:0c:29:8f:fb:12

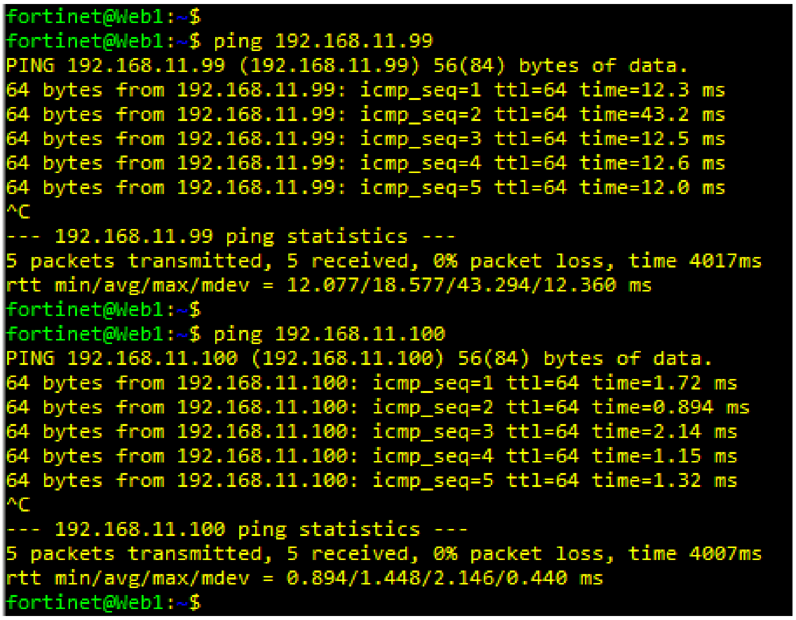
No physical adapters

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



```
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.



```
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:~$
```