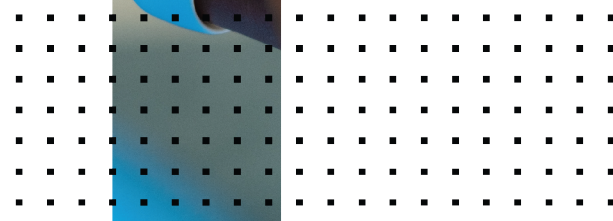


FortiDeceptor Customizaiton Guide

FortiDeceptor 5.0.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



December 16, 2022

FortiDeceptor 5.0.0 FortiDeceptor Customization Guide

50-500-868435-20221216

TABLE OF CONTENTS

Change Log	4
Introduction	5
1. Import the ISO image to FortiDeceptor	6
1.1 Prepare the import	6
1.2 Import the ISO image with the GUI	6
2. Customize the OS image	8
2.1 Initialize the OS instance	8
2.2 Customize the OS	10
2.3 (Optional) Install the Microsoft SQL Server	12
2.4 (Optional) Install the Internet Information Service (IIS)	13
2.5 (Optional) Join a domain	14
2.6 Install the FortiDeceptor customization toolkit	14
2.7 Save the customized image	16
2.8 Review the customization result	16
3. Use the custom images	18
3.1 Apply the custom images	18
3.2 Deploy decoys with custom images (Generic Image)	18
3.3 Deploy decoys with customized images (SQL Server)	19
4. Customize the Redhat Server OS image	22
4.1 Mount the device on your system	22
4.2 Configure network	22
4.3 Register the server	23
4.4 Install the required modules	23
4.5 Build the custom Linux tracer	25
4.6 Install the FDC toolkit	26
4.7 Save the custom Image	27
4.8 Review the result	28
5. Use the custom Redhat image	29
5.1 Apply the custom images	29
5.2 Deploy decoys with custom images (Generic Image)	29

Change Log

Date	Change Description
2022-12-14	Initial release.

Introduction

This document describes how to customize the deception base OS image via FortiDeceptor (FDC) GUI. This on-the-fly customization feature supports Windows 10 64-bits client, Windows Server 2016, Windows Server 2019 and Redhat Server 7.9.

1. Import the ISO image to FortiDeceptor

1.1 Prepare the import

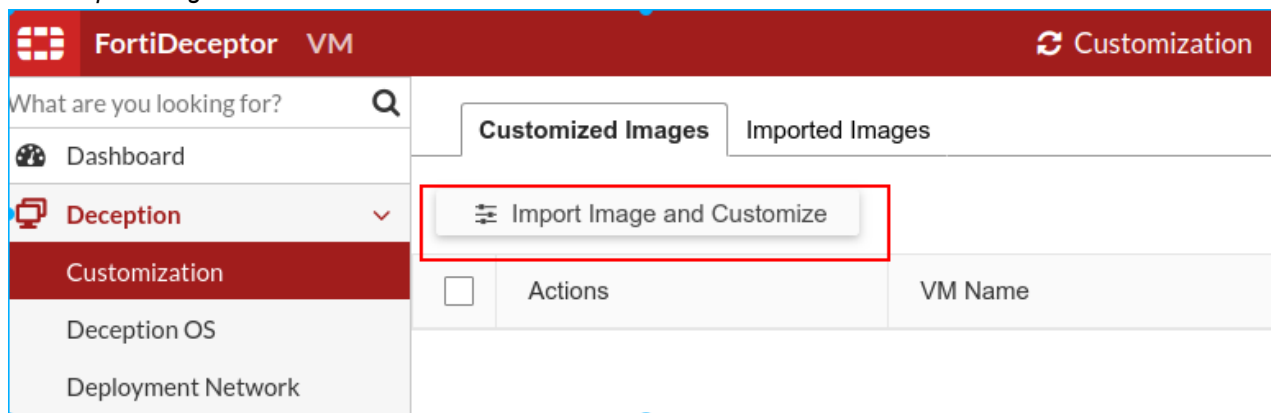
The customization feature requires you to bring your own license keys. Before importing the ISO image to FortiDeceptor, you should prepare the proper ISO images and proper license keys for their own environment. If you want to allow active domain (AD) accounts to access decoys, you should configure the related settings on you AD servers, (for example, create dummy accounts etc).

1.2 Import the ISO image with the GUI

Import the ISO with the GUI using either the *Customized Images* or the *Imported Images* page.

To import the ISO image with Customized Images:

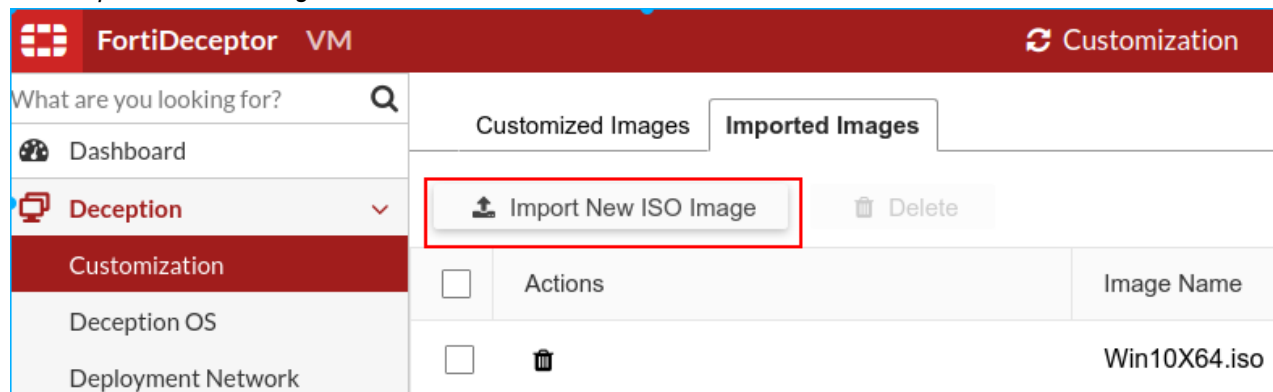
1. Go to *Deception > Customization > Customized Images*.
2. Click *Import Image and Customize*.



3. Drag or choose an image file to import.

To import the ISO image with Imported Images:

1. Go to *Deception > Customization > Imported Images*.
2. Click *Import New ISO Image*.



3. Drag or choose an image file to import.

To delete ISO images:

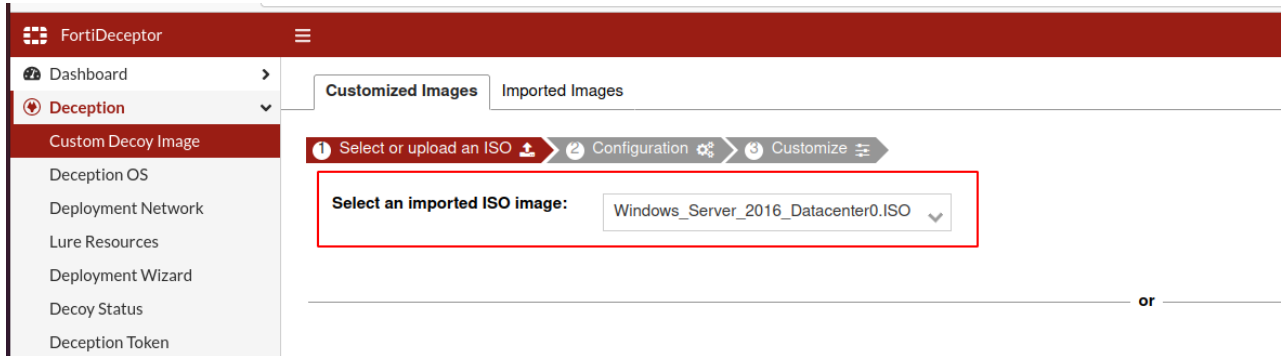
1. Go to *Deception > Customization > Customized Images*.
2. Click *Import Image and Customize*.
3. Choose an ISO image and click *Delete*.

2. Customize the OS image

2.1 Initialize the OS instance

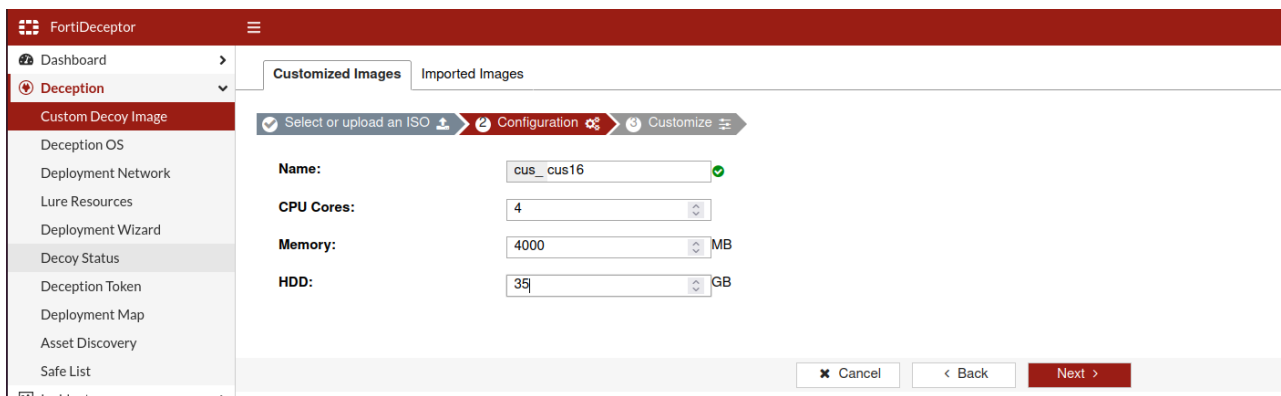
To initialize the OS instance:

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



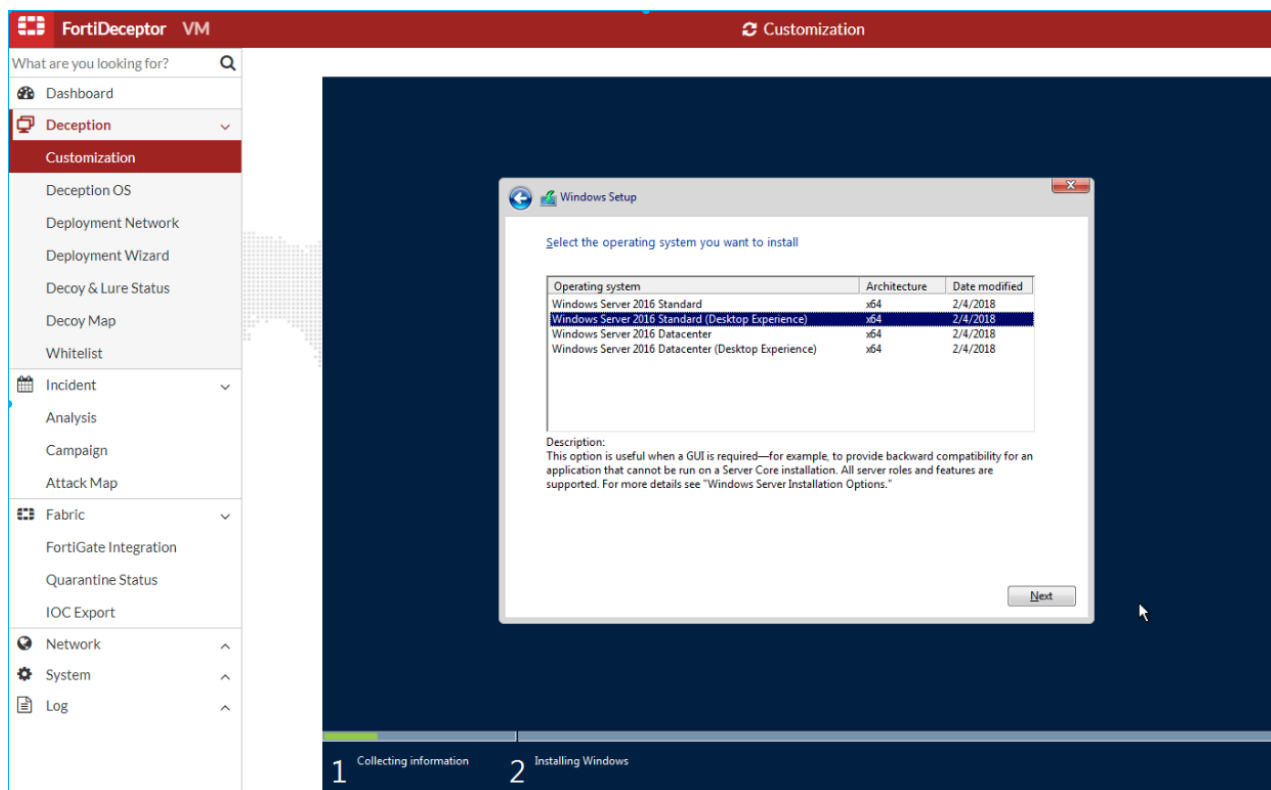
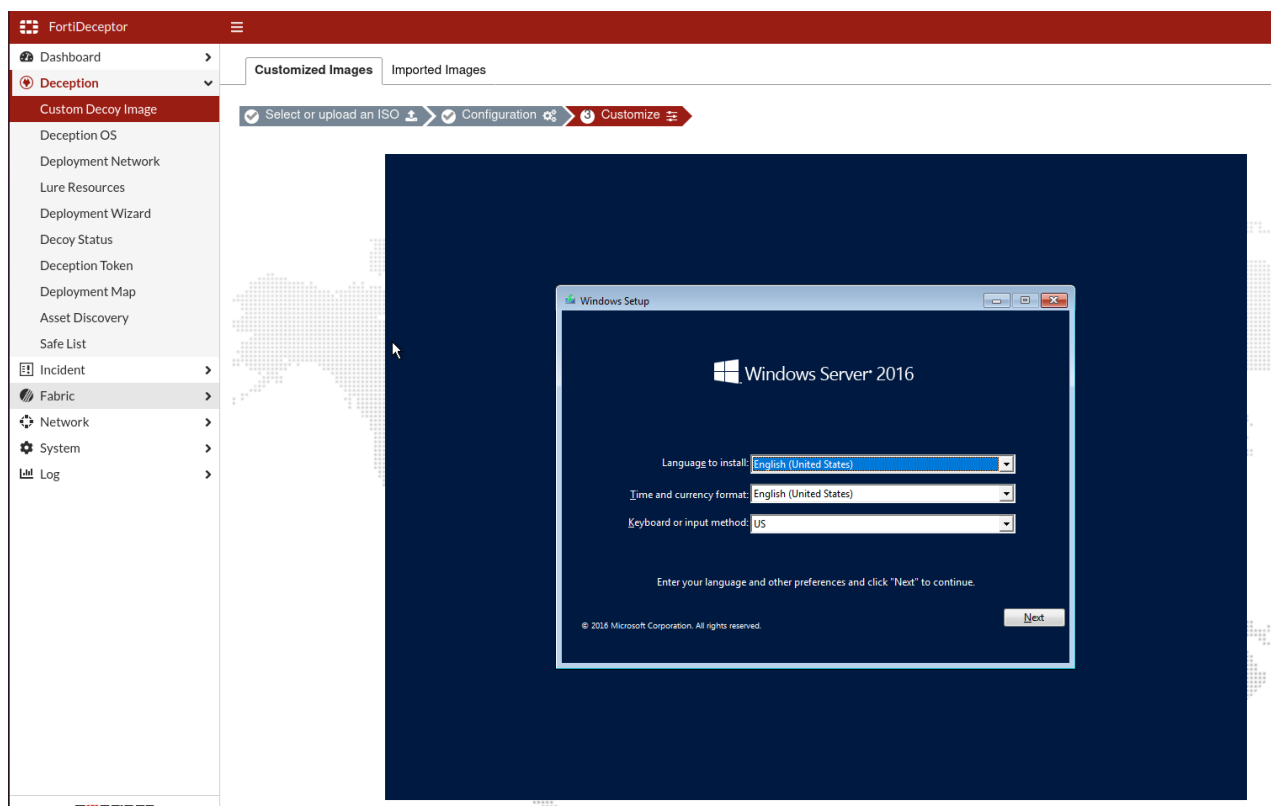
3. Choose an ISO image and click *Next*.
4. Configure the following settings and click *Next*.

Name	Characters in range “A-Za-z0-9-” , less than 48 characters.
CPU Cores	1-4
Memory	1024 – 8192 MB.
Storage	:20-50GB.Storage: 20-50GB.



2. Customize the OS image

5. In the VNC windows, install the OS from ISO image.

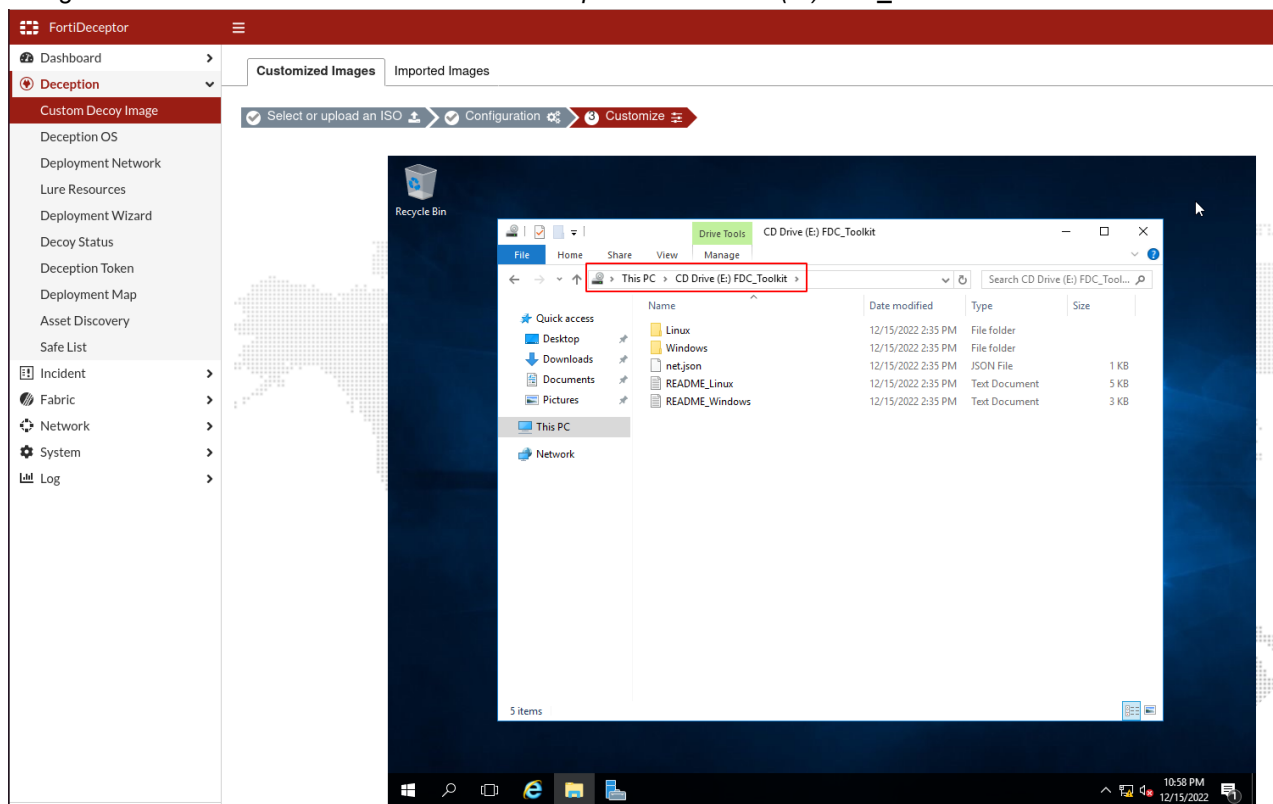


2.2 Customize the OS

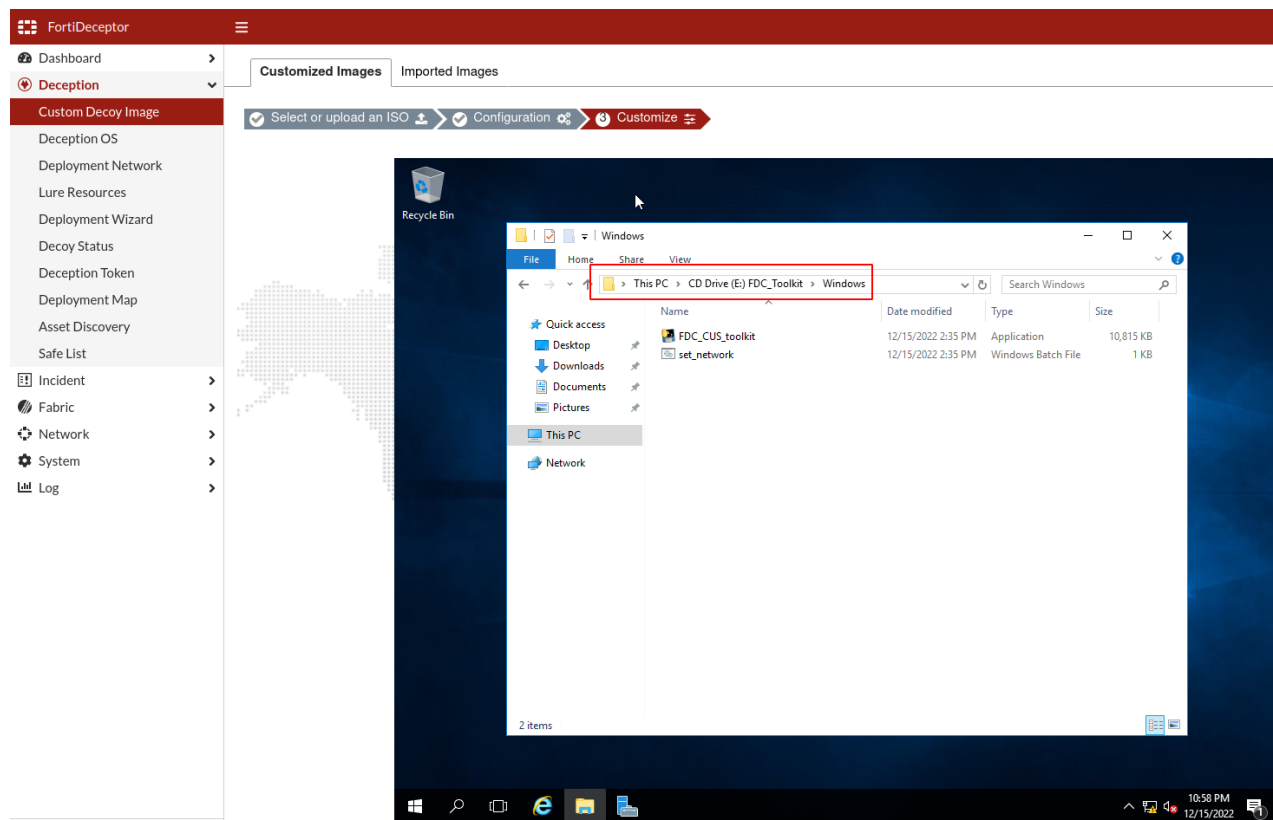
After the OS system is installed successfully, login with an account which has Windows administrator permission and follow below steps.

To locate the customization toolkit folder:

1. Navigate to FDC customization toolkit folder: *File Explorer > CD Drive (E:) FDC_Toolkit*.



2. Customize the OS image



2. Review and follow the guide in file `toolkit_README.txt`.

To configure the network:

To customize/configure	Description
Windows 10 OS	Right-click the file named <code>set_network.bat</code> , and choose <i>Run as Administrator</i> .
Windows server 2016/2019 OS	Double click it to run it directly if you logged on as <i>Administrator</i> .
IP, gateway and DNS	In Windows, go to <i>Control Panel > Network and Internet > Network Connections</i> . Follow the settings in file named <code>net.json</code> to configure the IP, gateway, and DNS.

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

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

Test network ...

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



The IP 10.254.253.0/24 set by the script is the internal NAT IP address, temporarily used by the customization OS to allow you to download files/access other network via FortiDeceptor default route.

To customize the system

1. If necessary, use your license to activate the system.
2. Customize the system to fit the deployment environment.
3. To avoid Lure configuration failure when using the decoy deployment wizard, remove the Password Complexity in the Windows Server 2016. To do this, copy and paste the command below into the PowerShell window:

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

To support decoys with AD accounts:

1. Configure the DNS in Windows manually.
2. Create a lure AD user account on your AD server.
3. Join the AD server with this AD user account.



You will need this AD account when deploy decoys based on this image.

2.3 (Optional) Install the Microsoft SQL Server

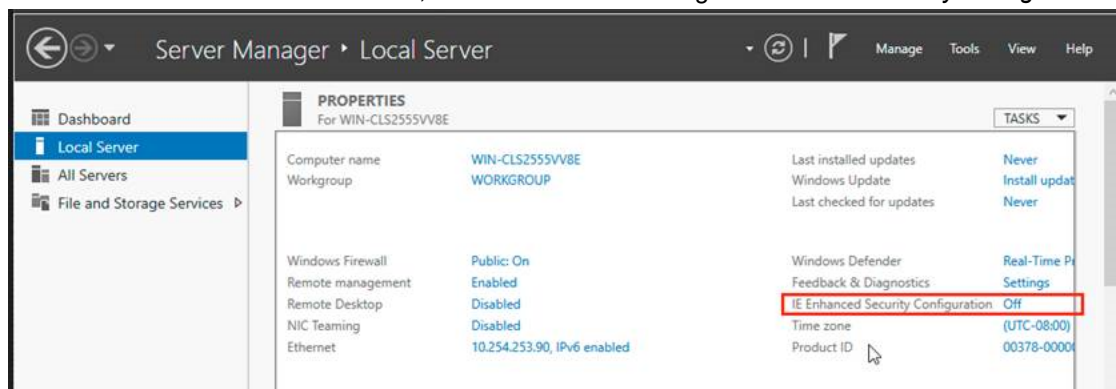
The following versions are supported:

Version	Download URL
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

Recommendations:

2. Customize the OS image

- To download files with the IE browser, we recommend disabling *IE Enhanced Security Configuration*.



- For Windows Server Core OS, you need to download the installation file onto another computer, and copy the installation file to Server Core OS over SMB service.

To install the Microsoft SQL Server:

- Download and install Microsoft SQL Server.
- When SQL server installation finished, click *Install SSMS* to download and install the SQL server management studio for SQL server management and customization.
- Download a database sample from this repository: <https://github.com/Microsoft/sql-server-samples/releases/download/wide-world-importers-v1.0/WideWorldImporters-Full.bak>
- Open the SQL management studio software on your windows server from the FortiDeceptor "*decoy customization*" console.
- Right-click the *Database* object and select *Restore database*.
- Select a database device and add the sample DB file you downloaded in Step 1.
- After restoring the database, right-click the sample database to change the DB permission access to make the Decoy DB more attractive to a threat actor.
- Choose *GRANT* permission for the *Select* and *Connect* options.
- Close the SQL management studio software and open a CMD.
- Run the command `netstat -an | findstr 1433` to verify that your DB is up and running.

2.4 (Optional) Install the Internet Information Service (IIS)

The following versions are supported:

- IIS 10 on Server 2016
- IIS 10 on Server 2019

To add IIS role and service:

- On the *Before you begin* page, click *Next*.
- On the *Installation Type* page, click *Next*.
- On the *Server Selection* page, click "Next" .
- In the pop-out page, select "*Web Server (IIS) > Add Features*", and click *Next*.
- On the *Select Features* page, click *Next*.

6. On the *Web Server Role (IIS)* page, click *Next*.
7. On the *Role Services* page, select *URL Authorization* and *Windows Authentication* then click *Next*.
8. On the *Confirmation* page, click *Install*.
9. On the *Results* page, wait for the installation to finish, then click *Close*.

2.5 (Optional) Join a domain

Before you join the customized windows OS to a domain, its DNS server should be changed to the DNS server of the domain. Otherwise, it will fail.

To join a domain:

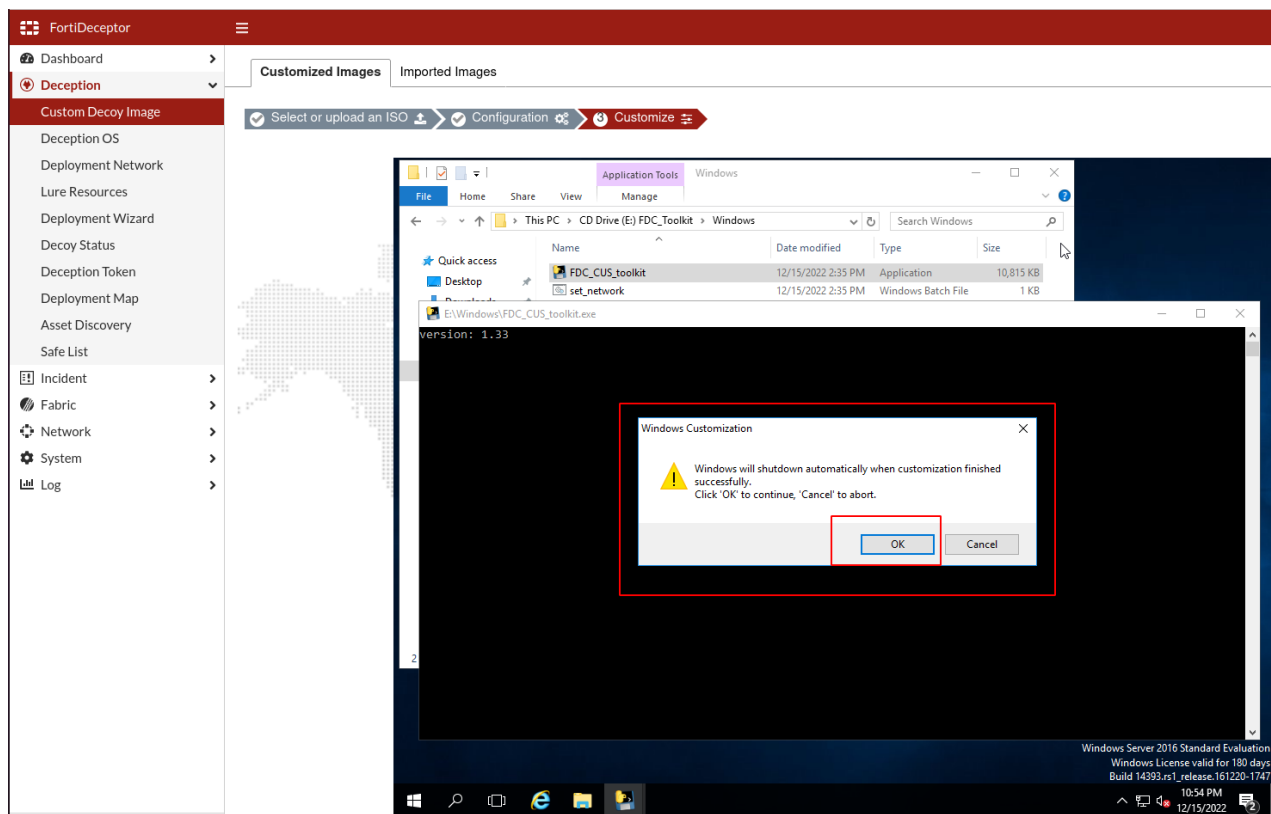
1. Go to *Control Panel > System*, and click *Change settings*.
2. On the *System Properties* page, click *Change*.
3. Input your domain info, and then click *OK*.
4. Input the domain account, click *OK*.
5. After joining the domain, a restart is required, click *Close*.
6. Click *Restart now*.
7. After Windows restarts, sign on as a local Administrator.

2.6 Install the FortiDeceptor customization toolkit

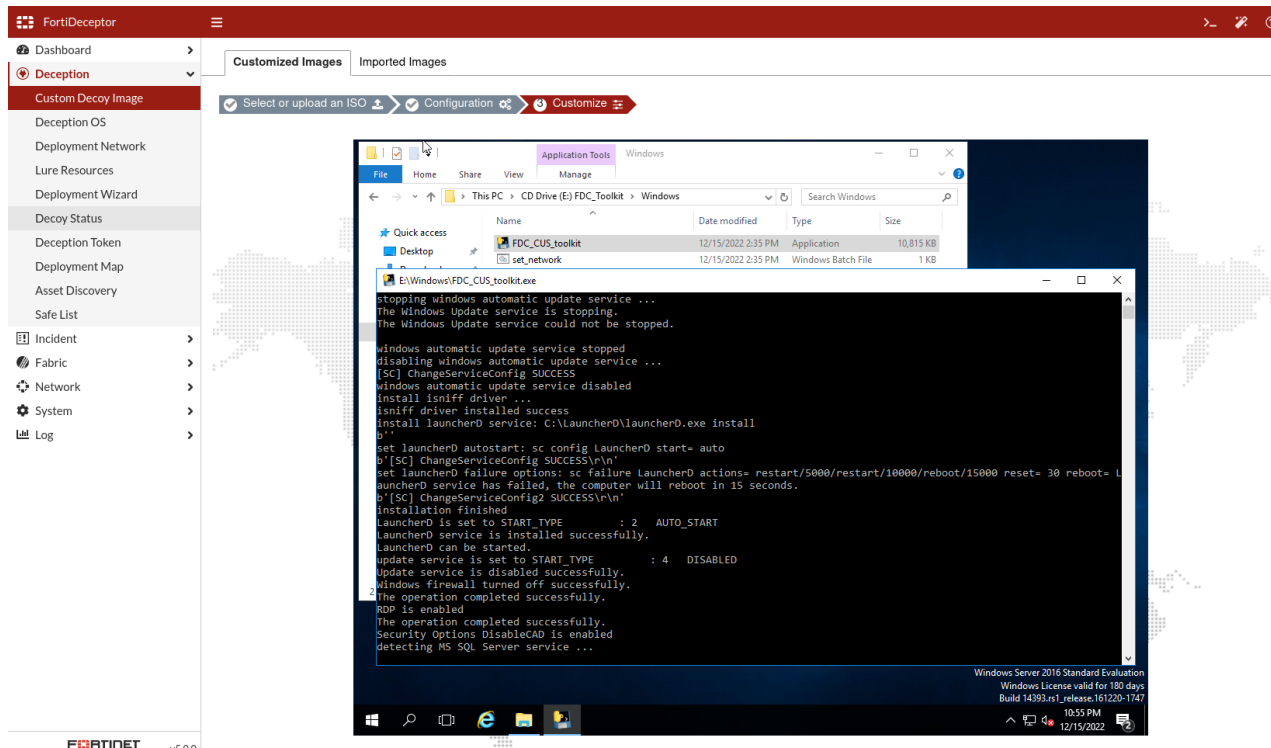
To install the customization toolkit:

1. After you are finished customizing the image, right-click the file `FDC_CUS_toolkit.exe`, and select *Run as Administrator*. The warning message *Windows will shut down automatically when customization finished successfully*, appears.

2. Customize the OS image

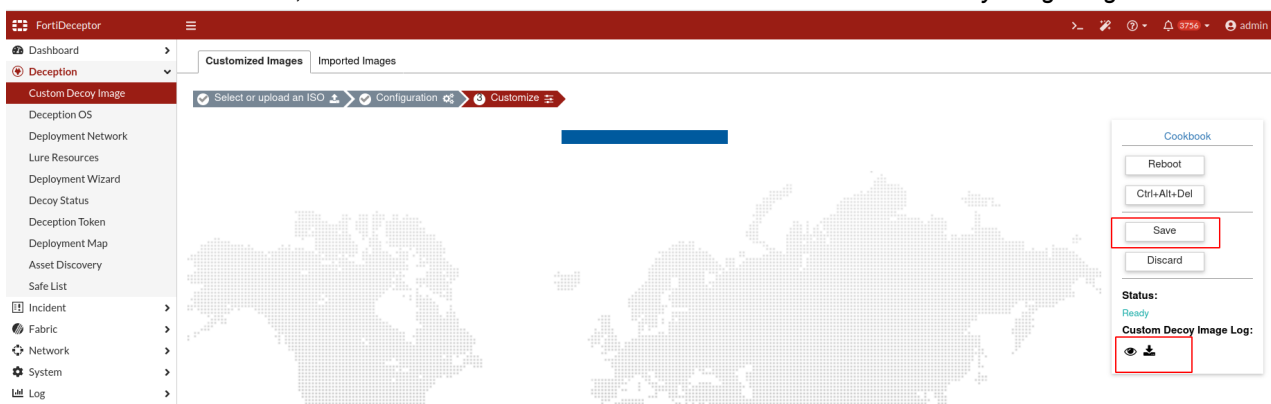


2. Click OK to continue, and wait for the installation to finish.



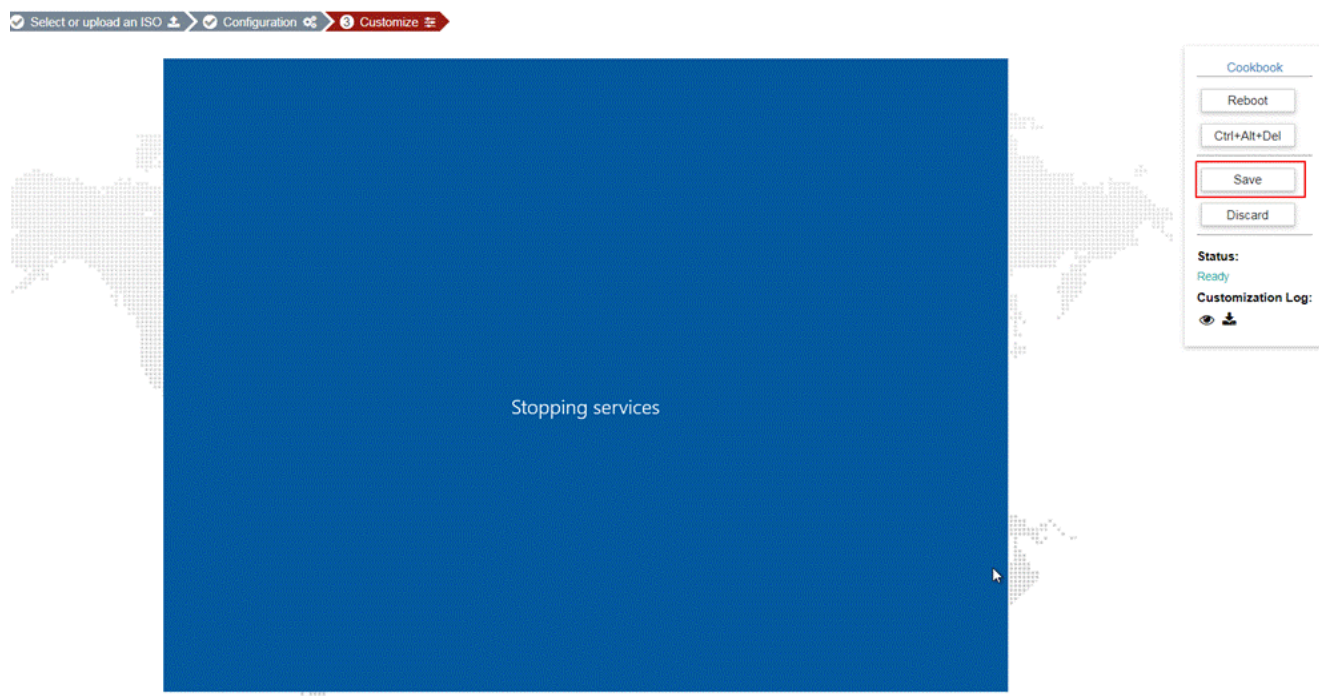
2. Customize the OS image

3. After the toolkit is installed, click **Save**. You can also *View* or *Download* the *Custom Decoy Image Log*.



2.7 Save the customized image

After Windows shuts down successfully, click **Save** to save this image. It may take several minutes to save the entire image. After it's finished, the page will display the *Customized Images* table with a new entry.



2.8 Review the customization result

Click the *View* icon to review the customization log for the customized image. Click the *Delete* icon to remove the customized image.

2. Customize the OS image

The screenshot shows the FortiDeceptor interface with the 'Customized Images' tab selected. The sidebar on the left contains the following menu items: Dashboard, Deception, Custom Decoy Image, Deception OS, Deployment Network, Lure Resources, Deployment Wizard, Decoy Status, Deception Token, Deployment Map, and Asset Discovery. The main content area has two tabs: 'Customized Images' (active) and 'Imported Images'. Below the tabs are buttons for 'Import Image and Customize', 'Apply', and 'Delete'. A table lists the customized images:

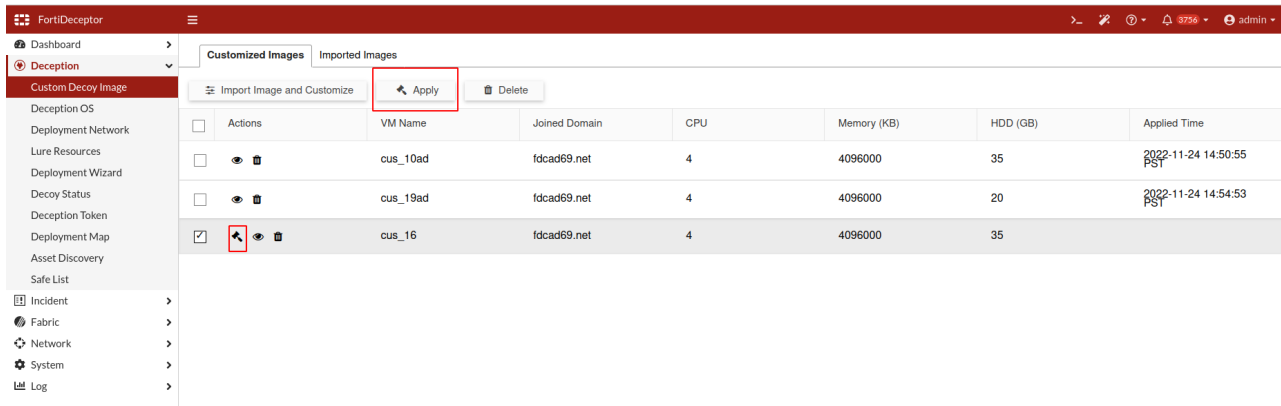
Actions	VM Name	Joined Domain	CPU	Memory (KB)	HDD (GB)	Applied Time
<input type="checkbox"/>	cus_10ad	fdcad69.net	4	4096000	35	2022-11-24 14:50:55 PST
<input type="checkbox"/>	cus_19ad	fdcad69.net	4	4096000	20	2022-11-24 14:54:53 PST
<input type="checkbox"/>	cus_16	fdcad69.net	4	4096000	35	

3. Use the custom images

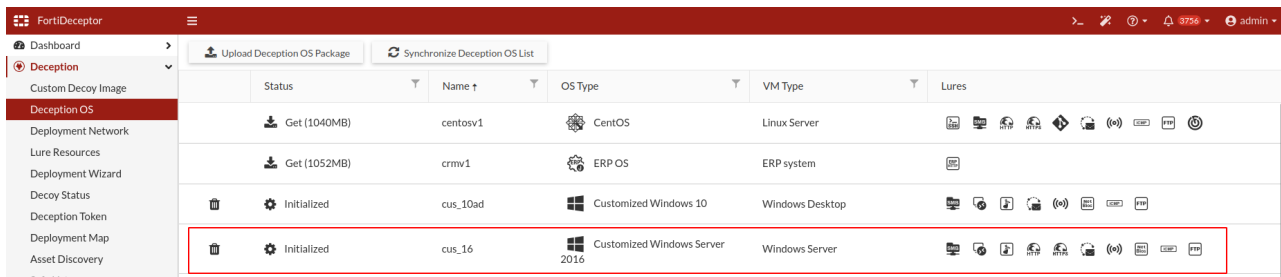
3.1 Apply the custom images

To apply a custom image:

1. In FortiDeceptor, go to *Deception > Customization* > *Customized Images*.



2. Choose a custom image and click *Apply*. The applied image is displayed in the *Deception OS* table. It may take several minutes for the image to appear in the table.



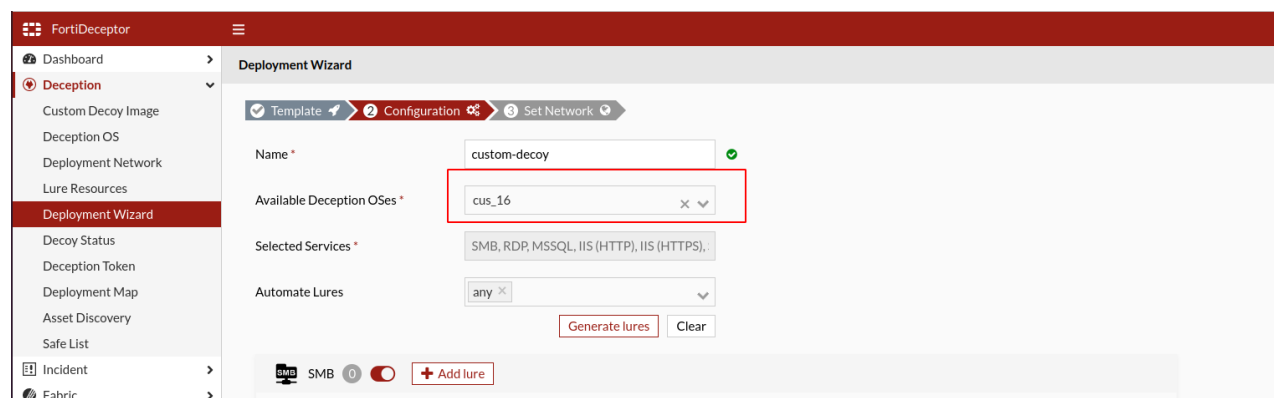
3.2 Deploy decoys with custom images (Generic Image)

To deploy decoys with generic custom images:

1. In FortiDeceptor, go to *Deception > Deployment Wizard* and create a new deployment.
2. In the *Configuration* step, choose a custom image and continue to follow the steps in the wizard to deploy the decoys.

3. Use the custom images

into the network.



The screenshot shows the FortiDeceptor web interface. On the left is a navigation menu with options: Dashboard, Deception (selected), Custom Decoy Image, Deception OS, Deployment Network, Lure Resources, Deployment Wizard (highlighted), Decoy Status, Deception Token, Deployment Map, Asset Discovery, Safe List, Incident, and Fabric. The main panel is titled 'Deployment Wizard' and shows three steps: 1. Template, 2. Configuration (active), and 3. Set Network. In the Configuration step, the 'Name' field contains 'custom-decoy'. The 'Available Deception OSes' dropdown menu is open, showing 'cus_16' selected and highlighted with a red box. Below this, the 'Selected Services' field lists 'SMB, RDP, MSSQL, IIS (HTTP), IIS (HTTPS)'. The 'Automate Lures' dropdown is set to 'any'. At the bottom of the configuration section are 'Generate lures' and 'Clear' buttons. At the very bottom of the interface, there is a status bar showing 'SMB' with a toggle switch and an '+ Add lure' button.



We highly recommend enabling the *RDP/SMB* services for decoys connected to a domain. Do not set any local lure accounts, because different domains have different policies for account name and password. This may cause the system to fail to initialize the decoys.

3.3 Deploy decoys with customized images (SQL Server)

To deploy decoys with SQL Server custom images:

1. In FortiDeceptor, go to *Deception > Deployment Wizard* and create a new deployment.
2. In the *Configuration* step, choose a custom image and continue to follow the steps in the wizard to deploy the decoys into the network.
3. Click *Sample* to download a sample DB that you can upload to any DB that already exists in the Customize Decoy image.

3. Use the custom images

FortiDeceptor

Dashboard >

Deception >

Custom Decoy Image

Deception OS

Deployment Network

Lure Resources

Deployment Wizard

Decoy Status

Deception Token

Deployment Map

Asset Discovery

Safe List

Incident >

Fabric >

Network >

System >

Log >

Name * custom-decoy ✓

Available Deception OSes * cus_16 x v

Selected Services * MSSQL, IIS (HTTP), IIS (HTTPS), SMTP, TCP

Automate Lures any x v

Generate lures Clear

SMB 0 0

RDP 0 0

MSSQL 0 1

Listening Port * 1433 ✓

Database Name * pubs ✓

The Database name must match the name of database in the uploaded SQL schema.

Database Content * Upload SQL schema Sample

Database File cannot be empty.

ODBC Lure 0 0

MSSQL Users

+ Add new user

Username	Password
----------	----------

4. To generate SQL alerts using the `SQLCMD` tool run the following command inside the command line:

```
sqlcmd -S "IP Address" -U "username" -P "password"
Use WideWorldImporters;
SELECT name
from SYSOBJECTS
WHERE
xtype = 'U'
ogo
```

Or

```
Use WideWorldImporters;
Select top 100 * from Sales.Orders;
go
```

3. Use the custom images

```
Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::58db:3388:eede:f9a%10
    IPv4 Address. . . . . : 172.18.18.12
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.18.18.254

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\Victor>sqlcmd -S 172.18.18.88 -U ricky -P P@ssw0rd
1>
```

In the image below, you can see the FortiDeceptor create an alerts for the SQL server attack.

The screenshot shows the FortiDeceptor web interface. On the left is a sidebar with navigation links: Dashboard, Deception, Incident (selected), Analysis, Campaign, Attack Map, MITRE ICS, Fabric, Network, System, and Log. The top header bar contains the FortiDeceptor logo, a menu icon, and user information (admin). Below the header is a toolbar with buttons for Refresh, PDF Report, Export to CSV, Mark all as read, and a Show dropdown menu set to Interaction Events Only. The main content area displays a table of incidents. The selected incident (ID 2938495035600220735) is highlighted, and its details are shown in a timeline view. The timeline includes the following events:

- 2022-12-14 10:35:11 PST**: Attacker User: ricky, Attacker IP: 10.11.4.24, Attacker Port: 1032, MITRE ICS Techniques: T0811, T0812, T0859, T0882.
- right after(2022-12-14 10:35:11 PST)**: Open Port: From 10.11.4.24:1032 To 10.11.4.121:1433. Download Traffic PCAP (MD5: 0db18af23a7b9927291312648ddc14b4, File Size: 6.8 KB, File Type: pcap).
- 2 seconds later(2022-12-14 10:35:13 PST)**: SQL Server Logon: User ricky login with password: Z2%V1%J1.
- 2 seconds later(2022-12-14 10:35:13 PST)**: (No details visible).

4. Customize the Redhat Server OS image

4.1 Mount the device on your system

To mount a device on the system:

1. Install the Redhat server 7.9
2. Set root password
3. Log in with root.
4. Run `mount /dev/sr1` to directory you prefer. (eg, / tmp / cus)
5. Check the file list in this mounted directory.

```
Red Hat Enterprise Linux Server 7.9 (Maipo)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

localhost login: root
Password:
[root@localhost ~]# ls
anaconda-ks.cfg
[root@localhost ~]# mkdir /tmp/cus
[root@localhost ~]# mount /dev/sr1 /tmp/cus
mount: /dev/sr1 is write-protected, mounting read-only
[root@localhost ~]# ls /tmp/cus/
FDC_Customization_Cookbook.pdf  Linux  net.json  README_Linux.txt  README_Windows.txt  Windows
[root@localhost ~]# ls /tmp/cus/Linux/
bash decoy_trace_installation.sh  install_redhat_modules.sh  redhat_cus_toolkit.sh  set_network.sh  sshd  strace.stp
[root@localhost ~]# _
```

4.2 Configure network

You can configure the network automatically or manually.

Option A: Configure the network by Linux/set_network.sh script automatically

```
bash set_network.sh
[root@localhost ~]# bash /tmp/cus/Linux/set_network.sh
found network interface ens3
set ip to 0.254.253.77
set 10.254.253.1 to 0.254.253.1
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/1)
[root@localhost ~]# subscription-manager register
```

Option B: Configure the network manually.

1. Open and read the setting file `net.json`.
2. Follow the settings to configure the IP, gateway, DNS

4. Customize the Redhat Server OS image

3. After you are done, verify your network can access the internet.

```
[root@localhost ~]# bash /tmp/cus/Linux/set_network.sh
found network interface ens3
set ip to 0.254.253.77
set 10.254.253.1 to 0.254.253.1
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/1)
[root@localhost ~]# subscription-manager register
```

4.3 Register the server

Register the server with your account, then customize your system customization to fit the deployment environment.

To register the server:

1. Run the following command: `subscription-manager register`
2. Enter your username and password.

```
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/1)
[root@localhost ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username:
Password:
The system has been registered with ID: d0b22383-7bad-47a1-a768-bb3296e9d503
The registered system name is: localhost.localdomain
```

4.4 Install the required modules

You can install all the modules and packages or install the modules manually.

Option A: install all required modules and packages

1. Make sure you have registered your server with redhat.com.
2. Run the following command: `bash install_redhat_modules.sh`

```
[root@localhost ~]# bash /tmp/cus/Linux/install_redhat_modules.sh
Going to enable repository: rhel-7-server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
Done!
Going to enable repository: rhel-7-server-debug-rpms
Repository 'rhel-7-server-debug-rpms' is enabled for this system.
Done!
Going to install yum-utils
Loaded plugins: product-id, search-disabled-repos, subscription-manager
rhel-7-server-debug-rpms | 3.2 kB 00:00:00
rhel-7-server-optional-rpms | 3.2 kB 00:00:00
rhel-7-server-rpms | 3.5 kB 00:00:00
(1/9): rhel-7-server-debug-rpms/7Server/x86_64/group | 124 B 00:00:01
(2/9): rhel-7-server-debug-rpms/7Server/x86_64/updateinfo | 2.7 MB 00:00:01
(3/9): rhel-7-server-optional-rpms/7Server/x86_64/group | 22 kB 00:00:01
(4/9): rhel-7-server-debug-rpms/7Server/x86_64/primary_db | 4.5 MB 00:00:01
(5/9): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo | 3.0 MB 00:00:02
(6/9): rhel-7-server-rpms/7Server/x86_64/group | 631 kB 00:00:02
(7/9): rhel-7-server-optional-rpms/7Server/x86_64/primary_db | 10 MB 00:00:02
(8/9): rhel-7-server-rpms/7Server/x86_64/updateinfo | 4.2 MB 00:00:03
(9/9): rhel-7-server-rpms/7Server/x86_64/primary_db | 91 MB 00:00:17
```



This script will take up to about one hour to run.

Option B: Install the modules manually

1. To enable the repository, run the following commands:

```
subscription-manager repos --enable=rhel-7-server-debug-rpms
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

```
[root@localhost cus]# subscription-manager repos --enable=rhel-7-server-debug-rpms
Repository 'rhel-7-server-debug-rpms' is enabled for this system.
[root@localhost cus]# subscription-manager repos --enable=rhel-7-server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
[root@localhost cus]#
```

2. Install the packages by running:

```
yum install -y yum-utils
yum install -y systemtap systemtap-runtime
yum install -y kernel-devel-$(uname -r)
yum install -y kernel-debuginfo-common-$(uname -m)-$(uname -r)
yum install -y kernel-debuginfo-$(uname -r)
yum -y install python3
yum install -y python3-devel-$(uname -m)
yum -y groupinstall 'Development Tools'
yum install -y net-tools
yum -y install samba samba-client
yum -y install httpd
yum -y install mod_ssl
pip3 install psutil
pip3 install requests
pip3 install sh
pip3 install netifaces
```



```

python-kitchen          noarch          1.1.1-5.el7             rhel-7-server-rpms      266 k
Transaction Summary
=====
Install 1 Package (+2 Dependent packages)

Total download size: 615 k
Installed size: 2.8 M
Downloading packages:
warning: /var/cache/yum/x86_64/7Server/rhel-7-server-rpms/packages/python-chardet-2.2.1-3.el7.noarch.rpm: Header U3 RSA/SHA256 Signature, key ID fd431d51: NOKEY
Public key for python-chardet-2.2.1-3.el7.noarch.rpm is not installed
(1/3): python-chardet-2.2.1-3.el7.noarch.rpm                | 227 kB  00:00:02
(2/3): python-kitchen-1.1.1-5.el7.noarch.rpm                | 266 kB  00:00:02
(3/3): yum-utils-1.1.31-54.el7_8.noarch.rpm                 | 122 kB  00:00:00
-----
Total                                                       188 kB/s | 615 kB  00:00:03
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Importing GPG key 0xFD431D51:
  Userid   : "Red Hat, Inc. (release key 2) <security@redhat.com>"
  Fingerprint: 567e 347a d004 4ade 55ba 8a5f 199e 2f91 fd43 1d51
  Package   : redhat-release-server-7.9-3.el7.x86_64 (@anaconda/7.9)
  From      : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Importing GPG key 0x2FA658E8:
  Userid   : "Red Hat, Inc. (auxiliary key) <security@redhat.com>"
  Fingerprint: 43a6 e49c 4a38 f4be 9abf 2a53 4568 9c88 2fa6 58e8
  Package   : redhat-release-server-7.9-3.el7.x86_64 (@anaconda/7.9)
  From      : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : python-chardet-2.2.1-3.el7.noarch                1/3
  Installing : python-kitchen-1.1.1-5.el7.noarch                2/3
  Installing : yum-utils-1.1.31-54.el7_8.noarch                 3/3
  Verifying  : python-kitchen-1.1.1-5.el7.noarch                1/3
  Verifying  : yum-utils-1.1.31-54.el7_8.noarch                 2/3
  Verifying  : python-chardet-2.2.1-3.el7.noarch                3/3
rhel-7-server-rpms/7Server/x86_64/productid                    | 2.1 kB  00:00:00

Installed:
  yum-utils.noarch 0:1.1.31-54.el7_8

Dependency Installed:
  python-chardet.noarch 0:2.2.1-3.el7                python-kitchen.noarch 0:1.1.1-5.el7

Complete!
[root@localhost cus]#

```

4.5 Build the custom Linux tracer

After installing all required modules, go to your mounted directory and run:

```
bash decoy_strace_installation.sh strace.stp
```

The script will check your build environment before building the tracer

```
ks-script-a0a12H system-private-13184e178ea04940a3f2ba0508b37848-chr0ngd.service-0x2f1f gum.log
[root@localhost cus]# cd /root
[root@localhost ~]# bash /mnt/cus/decoy_strace_installation.sh /mnt/cus/strace.stp
The systemtap building environment is ready
Loaded plugins: product-id, search-disabled-repos, subscription-manager
Installed Packages
Name       : systemtap
Arch       : x86_64
Version    : 4.0
Release    : 13.el7
Size       : 0.0
Repo       : installed
From repo  : rhel-7-server-rpms
Summary    : Programmable system-wide instrumentation system
URL        : http://sourceware.org/systemtap/
License    : GPLv2+
Description: SystemTap is an instrumentation system for systems running Linux.
           : Developers can write instrumentation scripts to collect data on
           : the operation of the system. The base systemtap package contains/requires
           : the components needed to locally develop and execute systemtap scripts.

Loaded plugins: product-id, search-disabled-repos, subscription-manager
```

If the build is successful, the output will look like this:

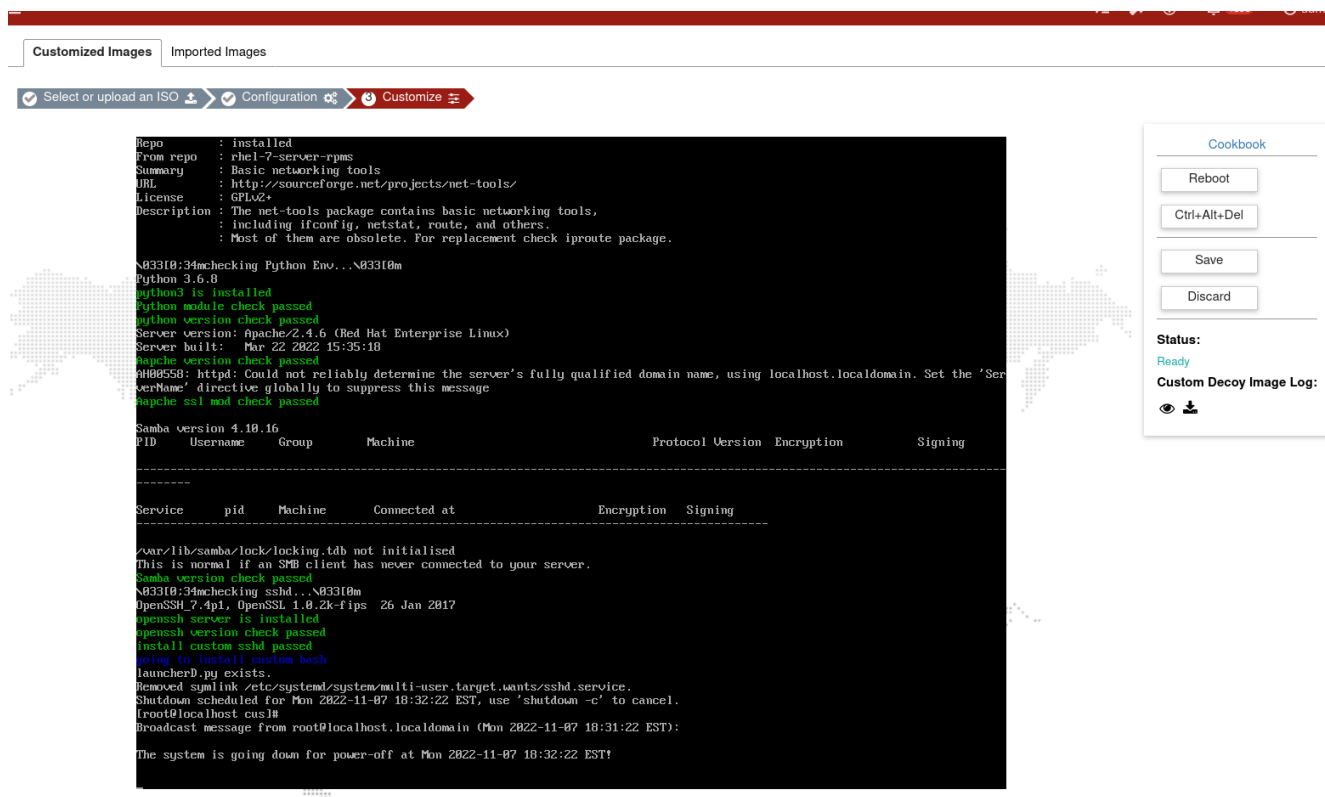
```
vmgfix.ko
Number of similar warning messages suppressed: 18.
Rerun with -v to see them.
'vmgfix.ko' -> '/usr/bin/vmgfix.ko'
[root@localhost ~]#
```

4.6 Install the FDC toolkit

To install the FDC toolkit:

1. Ensure the system customization is completed as expected.
2. Run the following command prompt you for missing packages: `bash redhat_cus_toolkit.sh`
3. Wait for the installation to finish. The system will:
 - Unregister from redhat.com
 - Shut down automatically if there are no errors

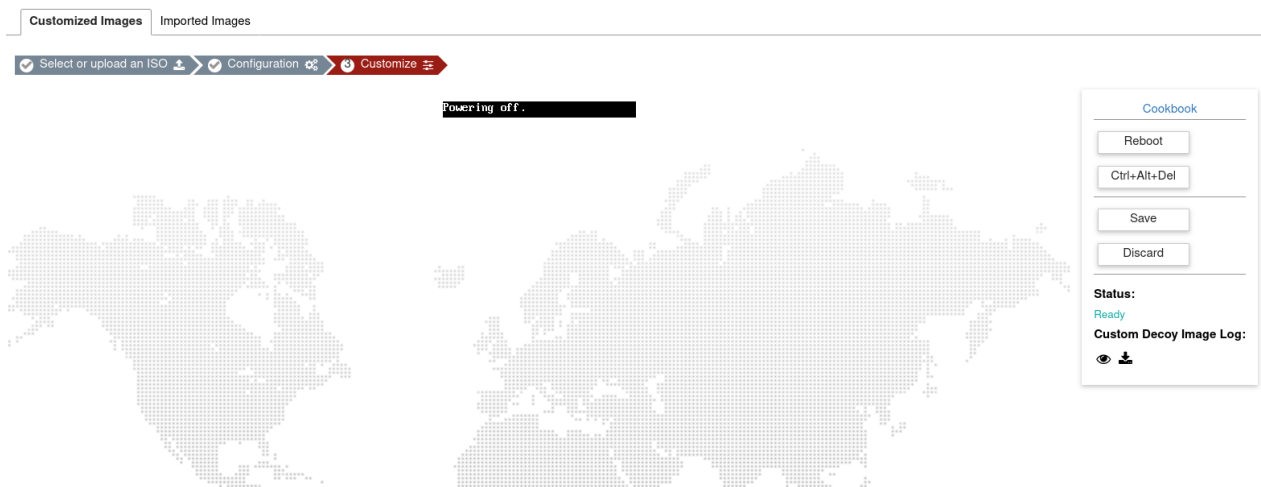
4. Customize the Redhat Server OS image



4.7 Save the custom Image

To save the custom image:

1. In the FortiDeceptor GUI, the image *Status*. You can continue when the status is *Ready*.









2. Click **Save** when the system is powered off.

4.8 Review the result

To review the result:

1. Click the *View* button to review the customization log for the customized image.

Customized Images Imported Images							
Import Image and Customize		Apply		Delete			
<input type="checkbox"/>	Actions	VM Name	Joined Domain	CPU	Memory (KB)	HDD (GB)	Applied Time
<input type="checkbox"/>	  	cus_redhat		2	1048576	20	N/A
<input type="checkbox"/>	  	cus_rhel		2	1048576	20	

2. (Optional) Click the *Delete* button to remove the custom image.

5. Use the custom Redhat image

5.1 Apply the custom images

To apply a custom image:

1. In FortiDeceptor, go to *Deception > Customization > Customized Images*.

Actions	VM Name	Joined Domain	CPU	Memory (KB)	HDD (GB)	Applied Time
<input checked="" type="checkbox"/>	cus_rehl		2	2097152	20	2022-10-31 22:37:39 UTC
<input checked="" type="checkbox"/>	cus_test		2	1048576	20	

2. Select a customized image and click *Apply*. The applied image is displayed in the *Deception OS* table. It may take several minutes for the image to appear in the table.

	Initialized	cus_rehl	RedHat	Linux Server	
	Initialized	cus_test	RedHat	Linux Server	

5.2 Deploy decoys with custom images (Generic Image)

To deploy decoys with a custom image:

1. In FortiDeceptor, go to *Deception > Deployment Wizard* and create a new deployment.
2. In the *Configuration* step, choose a custom image and continue to follow the steps in the wizard to deploy the decoys.

5. Use the custom Redhat image

into the network.

The screenshot shows the FortiDeceptor web interface. The top header bar is dark red with the text 'FDC-VM0000069086' and a hamburger menu icon. On the left is a sidebar with a 'Deception' section containing links to 'Custom Decoy Image', 'Deception OS', 'Deployment Network', 'Lure Resources', 'Deployment Wizard' (highlighted in red), 'Decoy Status', 'Deception Token', 'Deployment Map', 'Asset Discovery', and 'Safe List'. The main content area is titled 'Deployment Wizard' and shows a progress bar with three steps: '1 Template' (checked), '2 Configuration' (active), and '3 Set Network'. Below the progress bar are four configuration fields: 'Name *' with a text input containing 'new profile' and a red error message 'Please enter config name.'; 'Available Deception OSes *' with a dropdown menu showing 'cus_rehl'; 'Selected Services *' with a text box containing 'SSH, SAMBA, HTTP, HTTPS, GIT, TCPListen'; and 'Automate Lures' with a dropdown menu showing 'any'. At the bottom right are two buttons: 'Generate lures' and 'Clear'.

FDC-VM0000069086

Dashboard

Deception

- Custom Decoy Image
- Deception OS
- Deployment Network
- Lure Resources
- Deployment Wizard
- Decoy Status
- Deception Token
- Deployment Map
- Asset Discovery
- Safe List

Deployment Wizard

1 Template 2 Configuration 3 Set Network

Name * new profile
Please enter config name.

Available Deception OSes * cus_rehl

Selected Services * SSH, SAMBA, HTTP, HTTPS, GIT, TCPListen

Automate Lures any

Generate lures Clear



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.