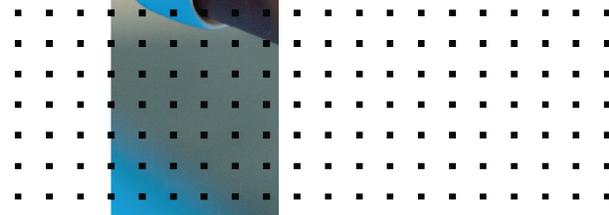


FortiDeceptor Customizaiton Guide

FortiDeceptor 6.2.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



October 7, 2025

FortiDeceptor 6.2.0 FortiDeceptor Customization Guide

50-520-948429-20251007

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported OS types	6
Import the ISO image to FortiDeceptor	8
1. Prepare the import	8
Licenses	8
2. Import the ISO image with the GUI	8
3. (Optional) Re-customizing existing images	9
Windows OS	11
1. Initialize the OS instance	11
2. Customize the OS	13
Windows 2016	16
Windows Server 2016	16
Server 2016 Domain Controller	17
AD accounts	17
3. (Optional) Install the Microsoft SQL Server	17
4. (Optional) Install the Internet Information Service (IIS)	21
5. (Optional) Join a domain	24
6. Install the FortiDeceptor customization toolkit	26
7. (Optional) Turn on Active Directory (AD) controller	29
8. Save the customized image	58
9. Review the customization result	59
10. Use the custom Windows image	60
Apply the custom images	60
Deploy decoys with custom generic Image	60
Deploy decoys with a customized SQL Server image	62
Deploy decoys with a custom IIS (HTTP/HTTPS) image	65
Deploy decoys with a custom NBNSSpoofSpotter image	65
Deploy decoys with a custom SWIFT Lite2 image	65
Troubleshooting	66
The PC does not meet the Windows 11 minimum system requirements	66
Redhat OS	73
1. Initialize the OS instance	73
2. Mount the device on your system	82
3. Configure network	82
4. Register the server	83
5. Install the required modules	83
6. Build the custom Linux tracer	85
7. Install the FDC toolkit	86
8. Save the custom Image	87
9. Review the result	88
10. Use the custom Redhat image	88

Apply the custom images	88
Deploy decoys with custom images (Generic Image)	89
Ubuntu OS	90
1. Initialize the OS instance	90
2. Mount the device on your system	92
3. Configure network	93
Option A: Configure the network by Ubuntu/set_network.sh script automatically	93
Option B: Configure the network manually.	93
4. Install the required modules	93
Option A: install all required modules and packages	94
Option B: Install the modules manually	94
5. Build the custom Ubuntu tracer	95
6. Install the FDC toolkit	97
7. Save the custom Image	98
8. Review the result	98
9. Use the custom Ubuntu image	99
Apply the custom images	99
Deploy decoys with custom Ubuntu images	99
Debian OS	101
1. Initialize the OS instance	101
2. Mount the device on your system	111
3. Configure the network	112
4. Install the required modules	112
5. Build the custom Debian tracer	113
6. Install the FDC toolkit	116
7. Save the custom Image	116
8. Review the result	117
9. Apply the custom images	117
10. Deploy decoys with custom Debian images	118

Change Log

Date	Change Description
2025-10-07	Initial release v6.2.0.
2025-10-27	Added Debian OS on page 101.

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 (English and French), Windows Server (English and French), Redhat Server, and Ubuntu.

For more additional information about custom decoy images, see the [Custom Decoy Image](#) topic in the *FortiDeceptor Administration Guide*.

Supported OS types

FortiDeceptor v6.2.0 supports the following OS types:

OS	OS version		
Windows	Language	Supported versions	Notes
	English	Windows 10	Supports custom MSSQL
		Windows 11 version 23H2	<ul style="list-style-type: none">Supports custom MSSQLFortiDeceptor v6.1.0 does not support Windows 11 version 24H2.
	French	Windows 10	Supports custom MSSQL
Windows Server	Language	Supported versions	Notes
	English	<ul style="list-style-type: none">Windows Server 2016Windows Server 2019Windows Server 2022	<ul style="list-style-type: none">Supports custom MSSQLSupports custom IIS Service
	French	French Windows Server 2016	<ul style="list-style-type: none">Supports custom MSSQLSupports custom IIS Service
RedHat Enterprise Linux	<ul style="list-style-type: none">RedHat Enterprise Linux 7.9RedHat Enterprise Linux 8.8RedHat Enterprise Linux 8.10RedHat Enterprise Linux 9.4RedHat Enterprise Linux 9.6		

OS	OS version
Ubuntu	<ul style="list-style-type: none">• Ubuntu 20.04
Debian	<ul style="list-style-type: none">• Debian 11.7• Debian 11.9

Import the ISO image to FortiDeceptor

1. Prepare the import

To use the customization feature, you will need to provide your own license keys. Before importing the ISO image to FortiDeceptor, ensure you have the correct ISO images and license keys for your environment. If you want Active Directory (AD) accounts to access decoys, configure the necessary settings on your AD servers, such as creating dummy accounts.

Licenses

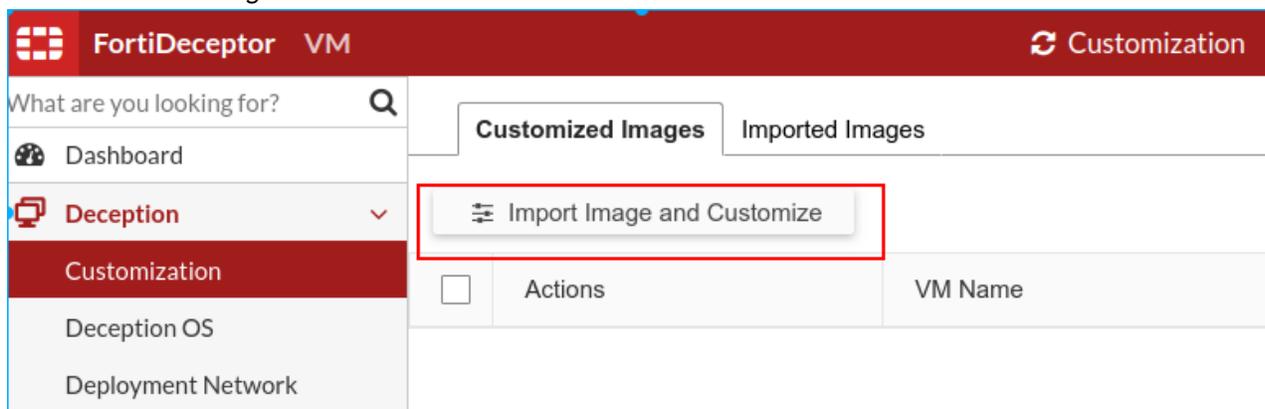
- The FortiDeceptor Custom Decoy Subscription bundle for FDC1000G, FDR100G, FDC-VMS, includes the custom decoy feature and does not require a license.
- The FortiDeceptor Custom Decoy license is required for the old perpetual license for FDC-VM and FDC1000F. This license is no longer being sold but is maintained for customers.

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:

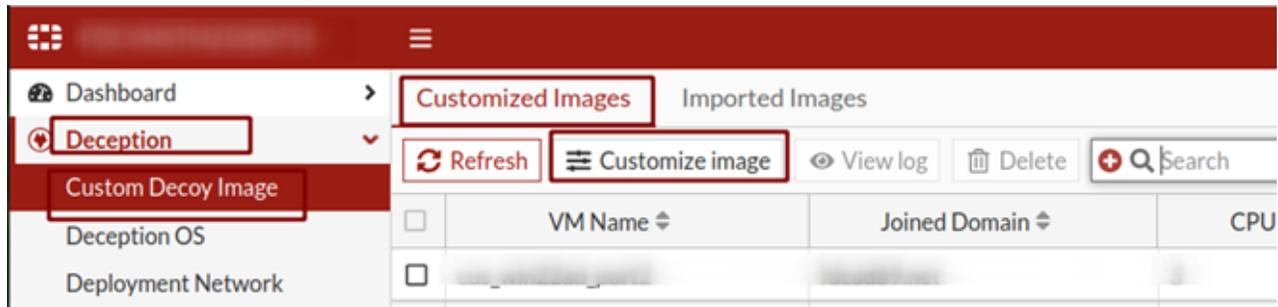
1. Go to *Deception > Custom Decoy Image > Customized Images*.
2. Click *Customize Image*.



3. Drag or choose an image file to import.

To import the ISO image with Imported Images:

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



3. Drag or choose an image file to import.

To delete ISO images:

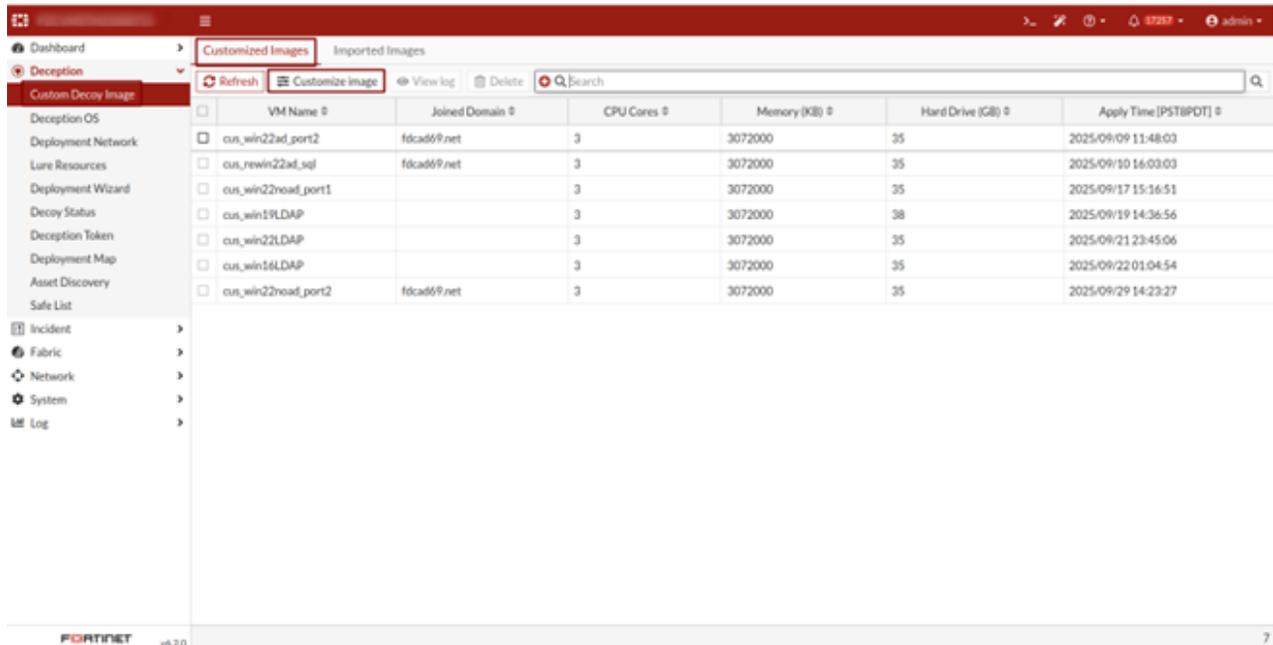
1. Go to *Deception > Customization > Customized Images*.
2. Click *Import Image and Customize*.
3. Choose an ISO image and click *Delete*.

3. (Optional) Re-customizing existing images

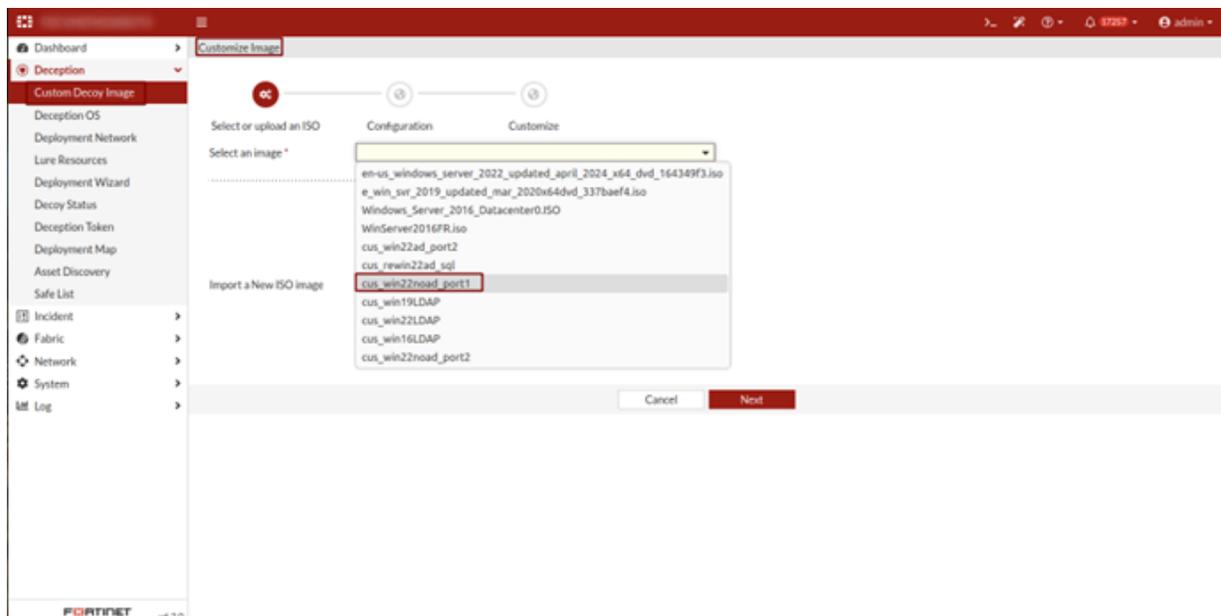
You can update customized images to expand the virtual hard disk (HDD) or apply new configurations.

To re-customize an existing image:

1. Go to *Deception Custom Decoy Image > Customized Images*.
2. Click *Customize Image*.



3. Choose an existing customized image from the dropdown list
4. Configure the following settings and click *Next*. Storage must be equal to or greater than the current size.



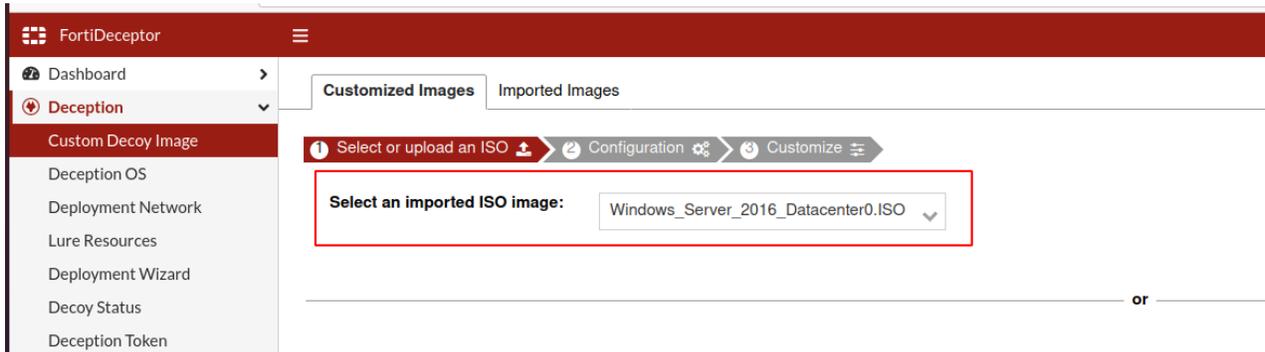
It may take more than 10 minutes for the VNC to load. Please do not customize another image during this process.

Windows OS

1. Initialize the OS instance

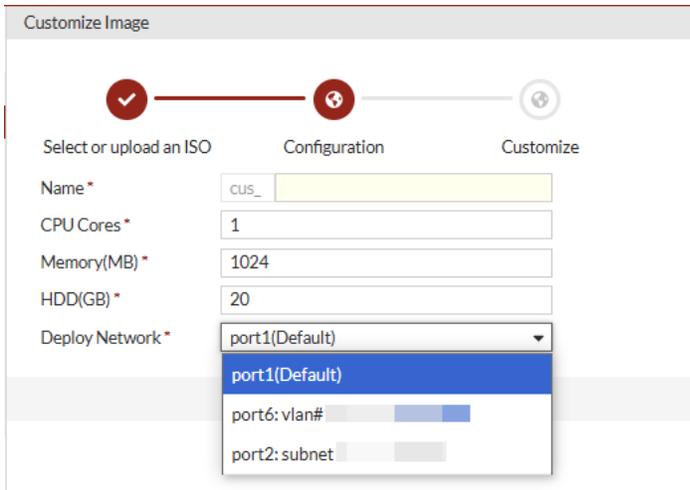
To initialize the OS instance:

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

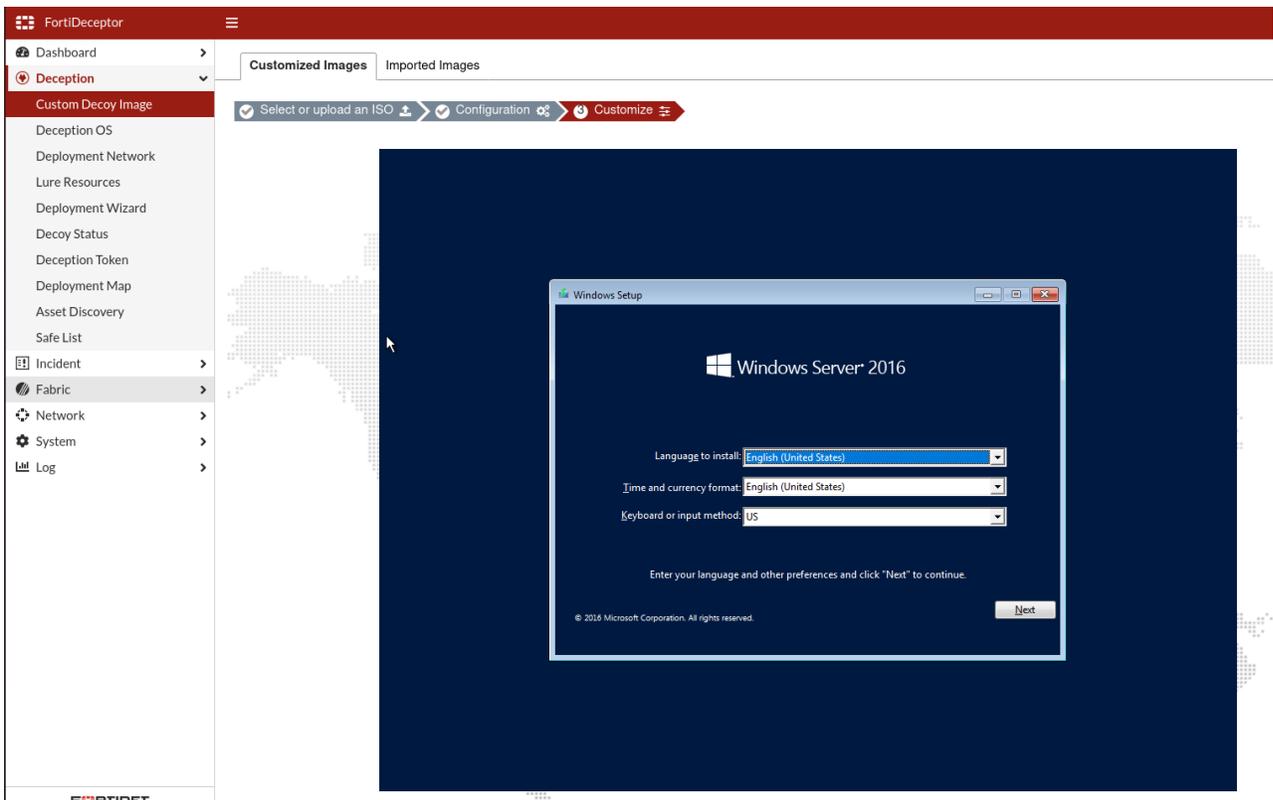


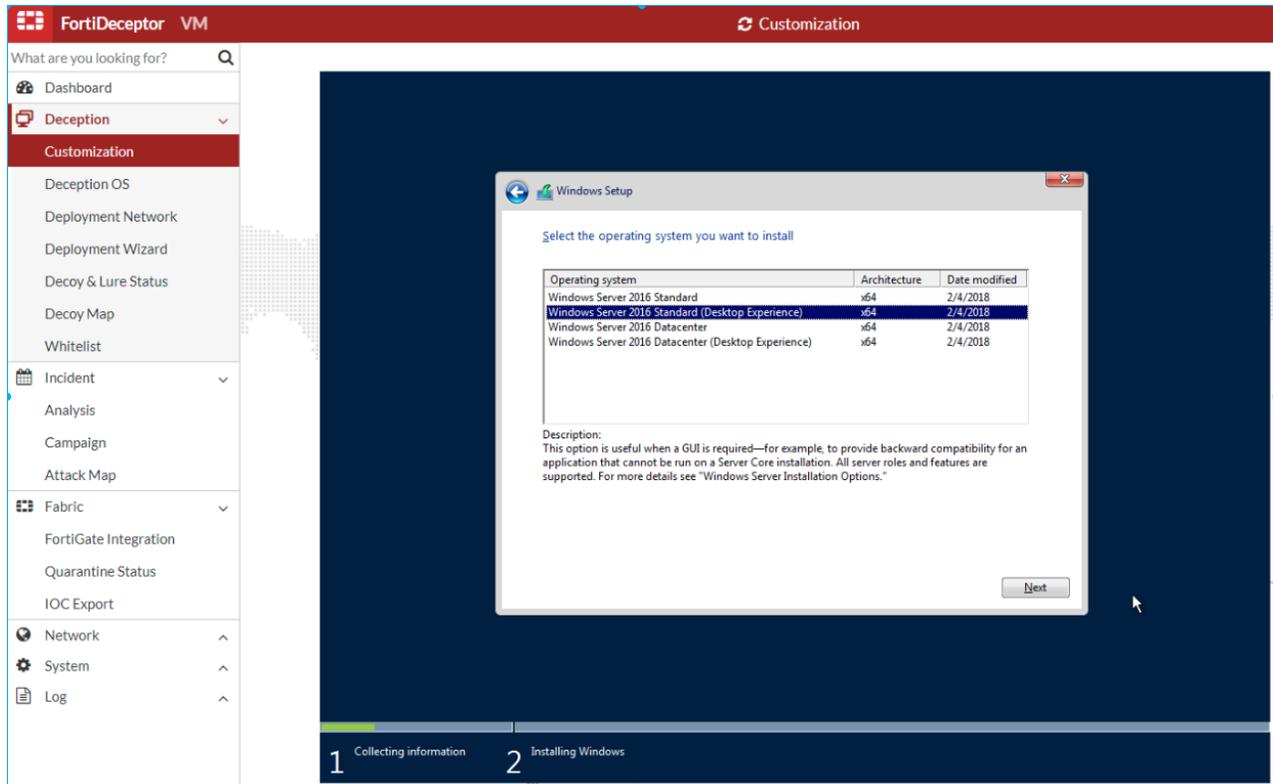
3. Choose an ISO image and click *Next*.
4. Configure the following settings and click *Next*.

Name	Alphanumeric characters (A-Z, a-z, 0-9) are supported. Maximum 48 characters.	
CPU Cores	2-4	
Memory	4000– 8192 MB.	
Storage	25-50GB.	
Deploy Network	Port1	Default
	PortX	Select the deployment network. Ensure the specified IP is not already in use and the following settings align with the PortX configuration: <ul style="list-style-type: none"> • IP/Mask • Gateway • DNS



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



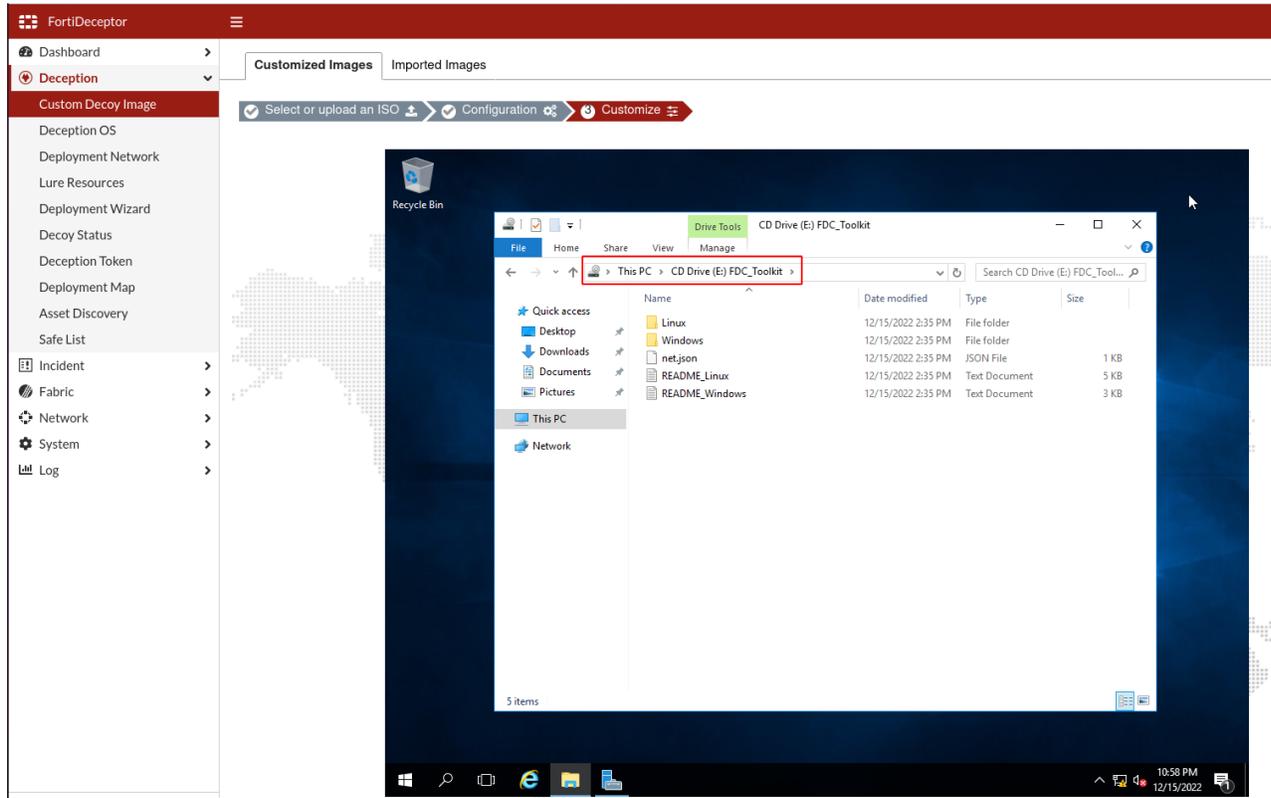


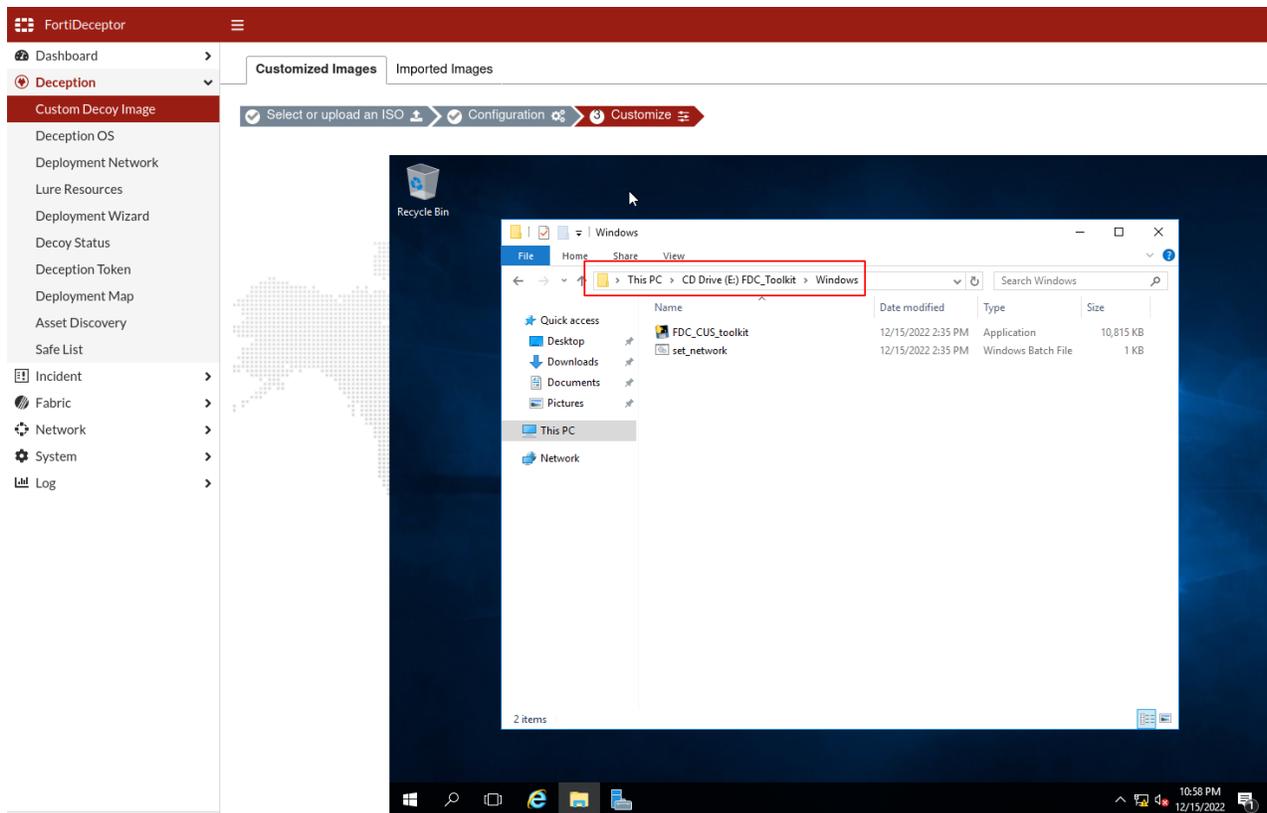
2. Customize the OS

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

To configure the network:

To customize/configure	Description
Windows 10/11, French Windows10 OS	Right-click the file named <code>set_network.bat</code> , and choose <i>Run as Administrator</i> .
Windows server 2016/2019/2022, French Windows server 2016 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.

Windows 2016

To customize Windows 2016:

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

```

Windows Server 2016

To customize Windows Server 2016:

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


```

gpupdate /force

```

 You should get the following response:


```

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

```

Server 2016 Domain Controller

To customize Server 2016 Domain Controller:

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

AD accounts

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.

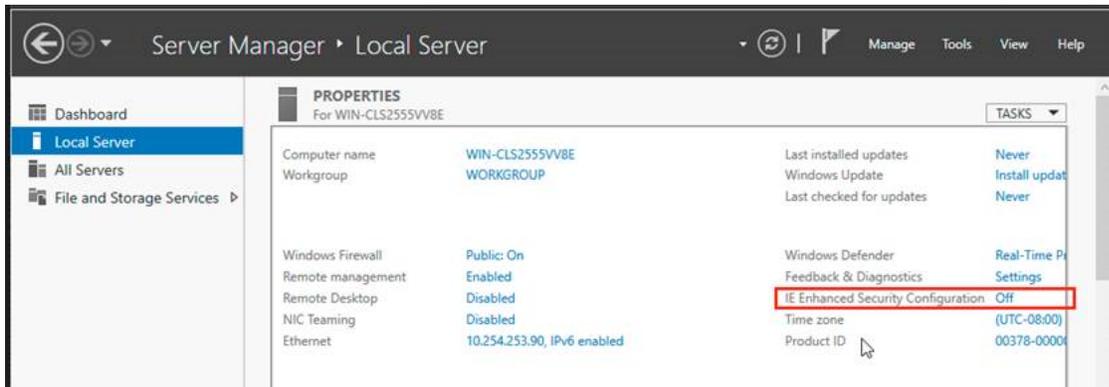
3. (Optional)Install the Microsoft SQL Server

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
SQL Server 2022	https://www.microsoft.com/en-ca/sql-server/sql-server-downloads
SQL Server Management Studio for SQL server management and customization.	https://aka.ms/ssmsfullsetup

Recommendations:

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

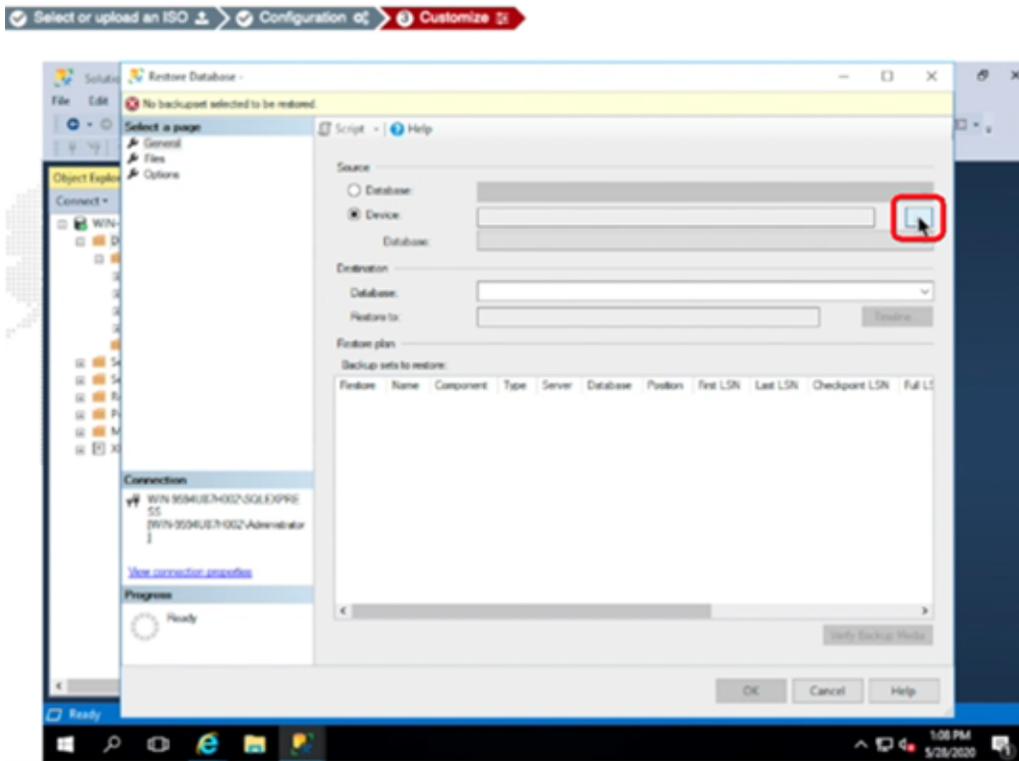


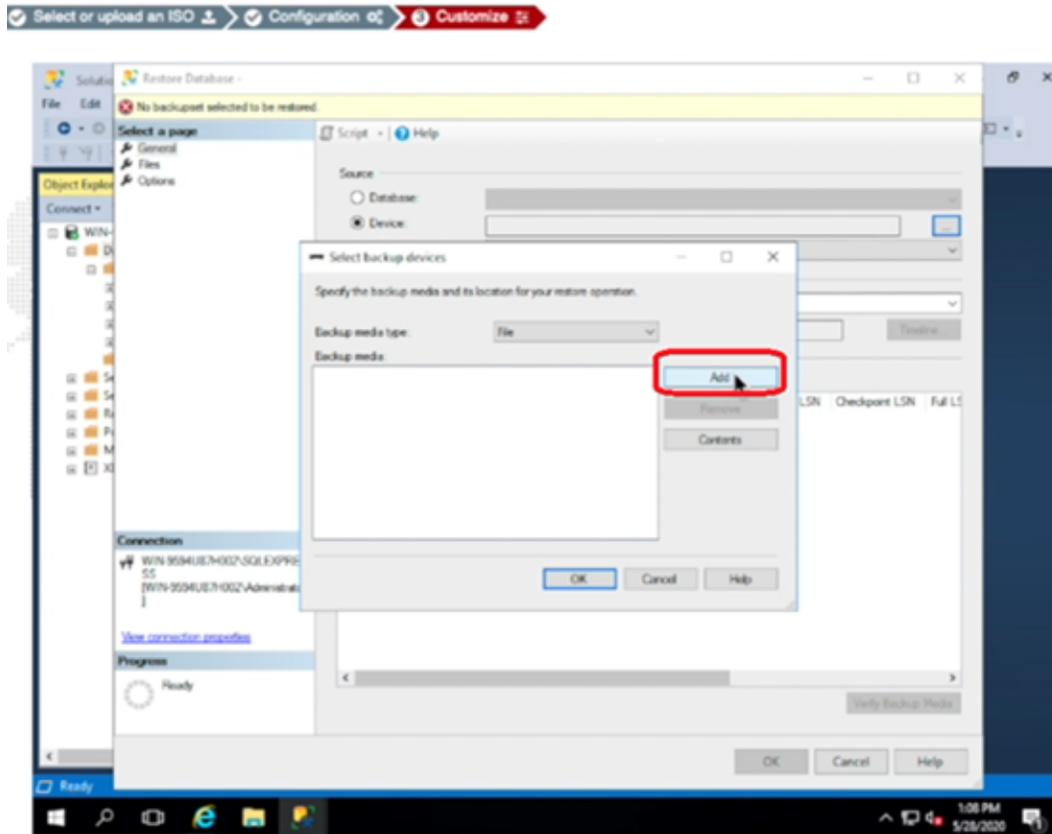
- For Windows Server Core OS, you need to download the installation file onto another computer, and copy the installation file to Server Core OS over SMB service.

To install the Microsoft SQL Server:

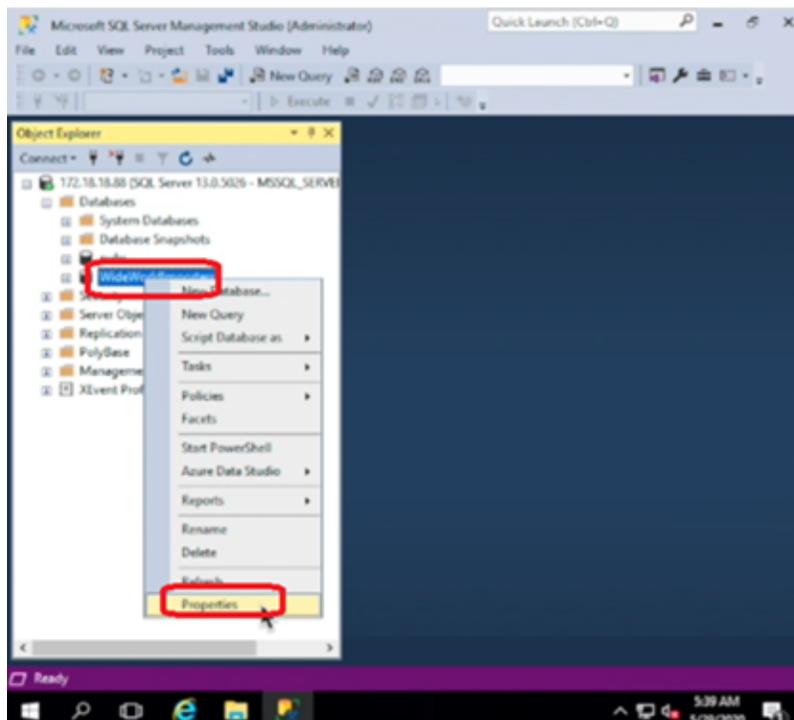
- Download and install Microsoft SQL Server.
- When SQL server installation finished, click *Install SSMS* to download and install the SQL server management studio for SQL server management and customization.
- Download a database sample from this repository: <https://github.com/Microsoft/sql-server-samples/releases/download/wide-world-importers-v1.0/WideWorldImporters-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*.

6. Select a database device and add the sample DB file you downloaded in Step 1.





7. 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.



8. Choose *Grant* permission for the *Select* and *Connect* options.
9. Close the SQL management studio software and open a CMD.
10. Run the command `netstat -an | findstr 1433` to verify that your DB is up and running.
11. The listening port on the SQL Express Database is disabled by default. To enable the port:
 - a. Click *Start > Programs > Microsoft SQL Server 20XX* and select *SQL Server Configuration Manager*.
 - b. Select *SQL Server Network Configuration*.
 - c. Double-click *Protocols for SQLEXPRESS*.
 - d. Right-click *TCP/IP* and select *Properties*. If necessary, enable *TCP/IP*.
 - e. Scroll down to *IPAll* and verify *TCP Dynamic Ports* is blank and that *TCP Port* is set to 1433.
 - f. Click *OK*.

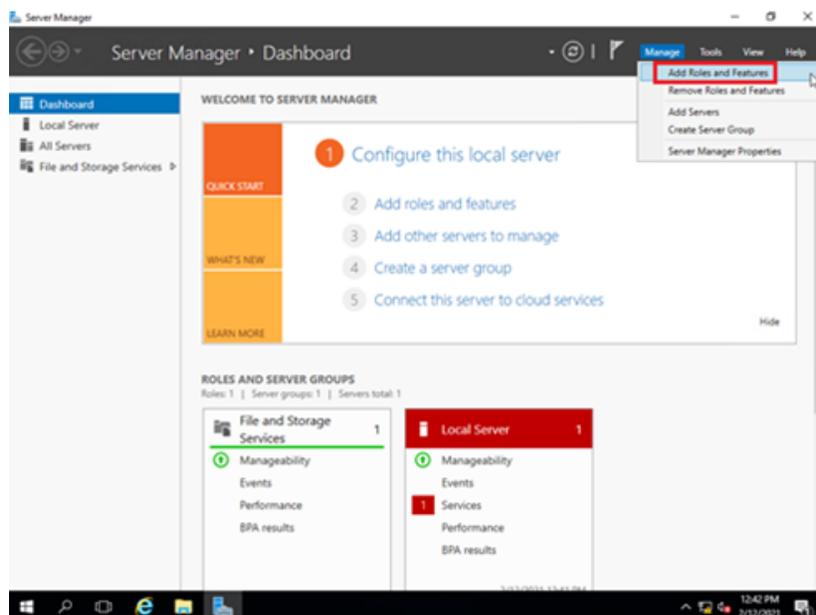
4. (Optional) Install the Internet Information Service (IIS)

The following versions are supported:

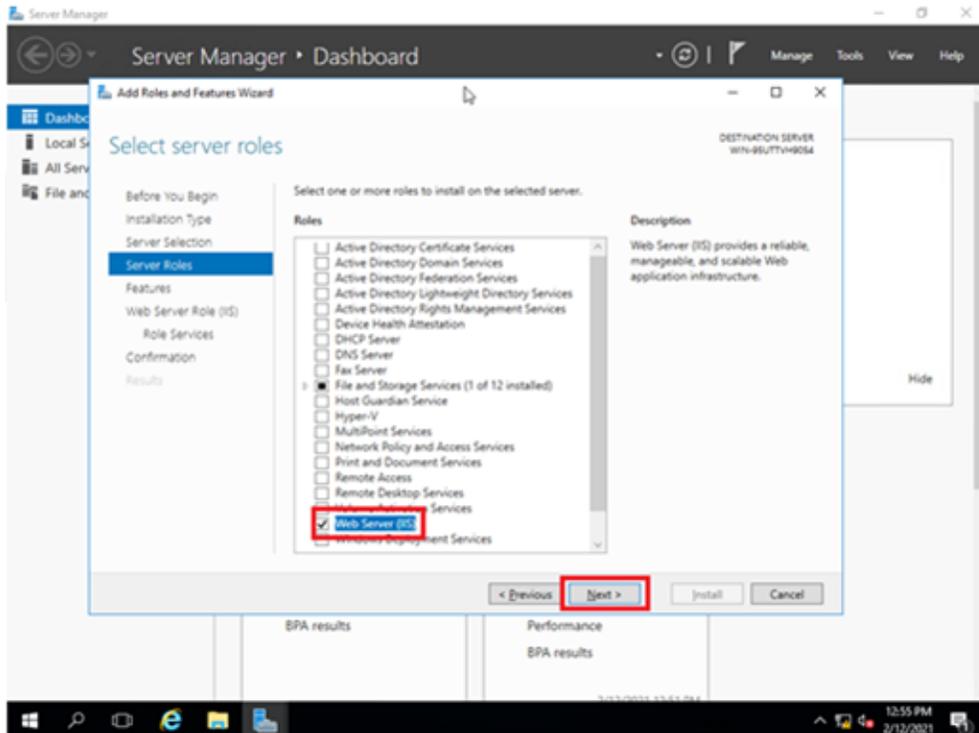
- IIS 10 on Server 2016
- IIS 10 on Server 2019
- IIS 10 on Server 2022
- IIS 10 on French Windows Server 2016

To add IIS role and service:

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

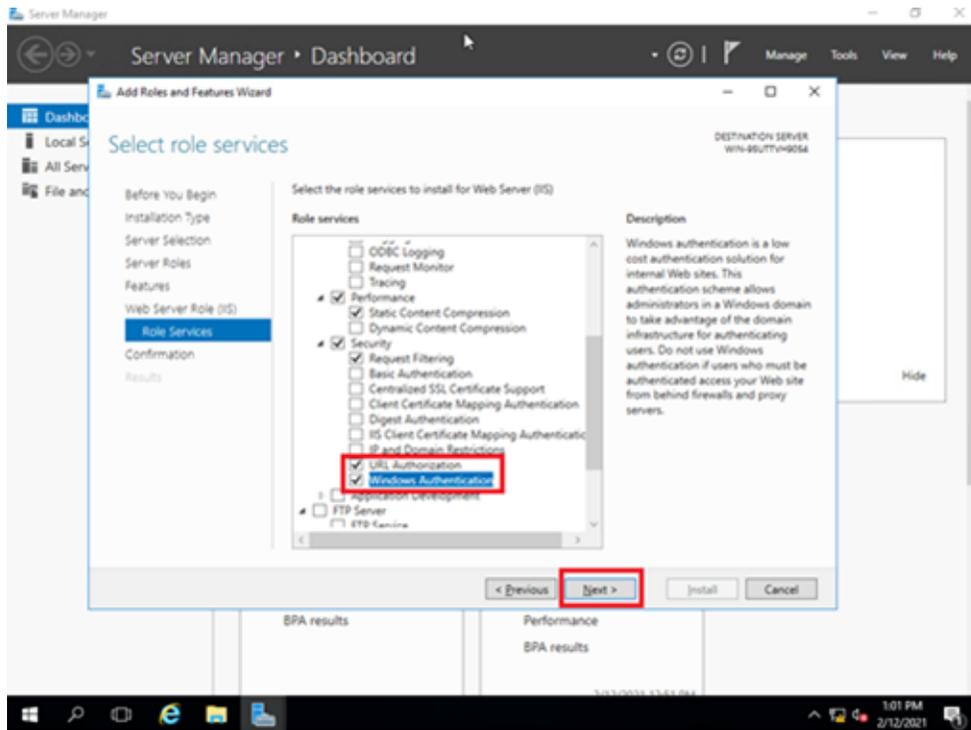


3. On the *Before you begin* page, click *Next*.
4. On the *Installation Type* page, click *Next*.
5. On the *Server Selection* page, click *Next*.
6. In the *Select server roles* dialog, select *Web Server (IIS) > Add Features*, and click *Next*.

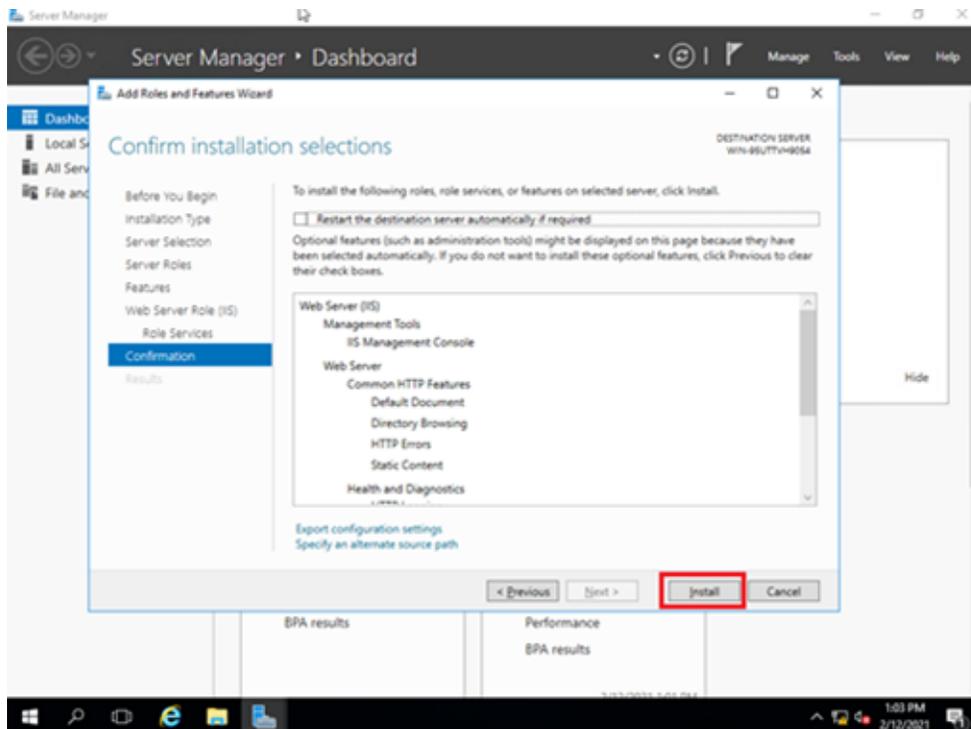


7. On the *Select Features* page, click *Next*.
8. On the *Web Server Role (IIS)* page, click *Next*.

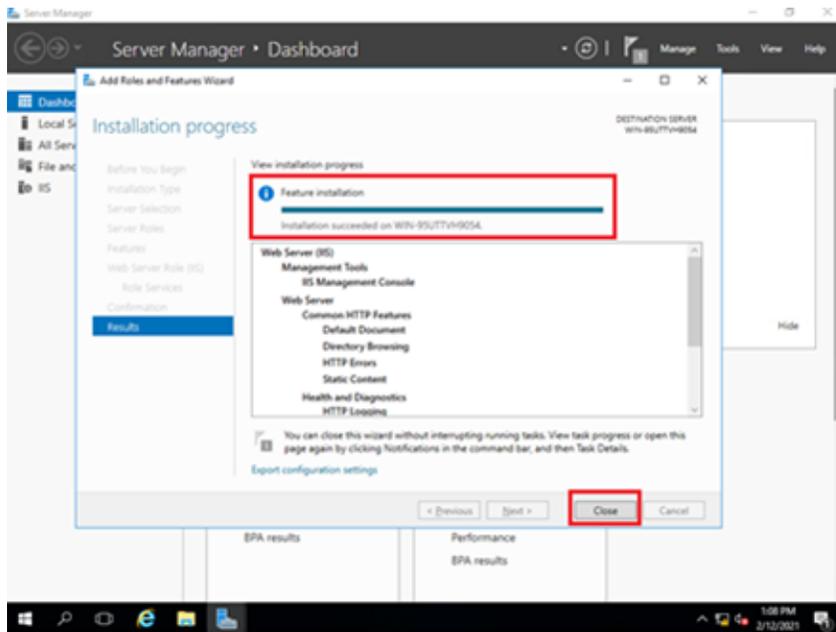
9. On the *Role Services* page, select *URL Authorization* and *Windows Authentication* then click *Next*.



10. On the *Confirmation* page, click *Install*.



11. On the *Results* page, wait for the installation to finish, then click *Close*.

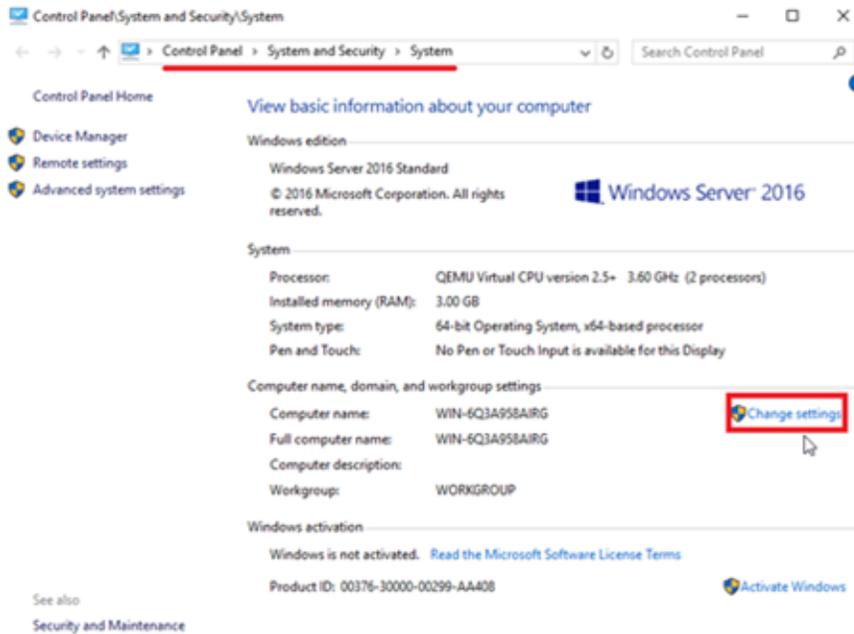


5. (Optional) Join a domain

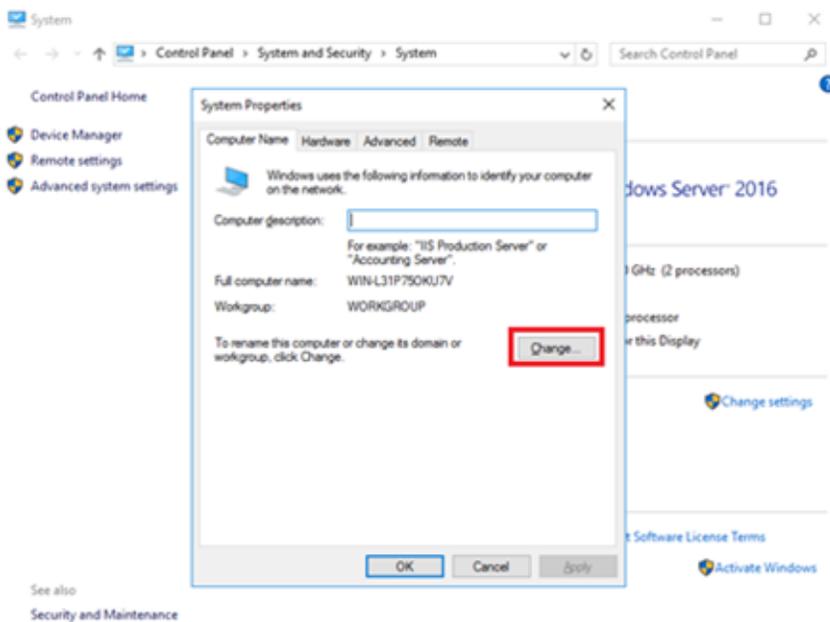
Before you join the customized windows OS to a domain, its DNS server should be changed to the DNS server of the domain. Otherwise, it will fail.

To join a domain:

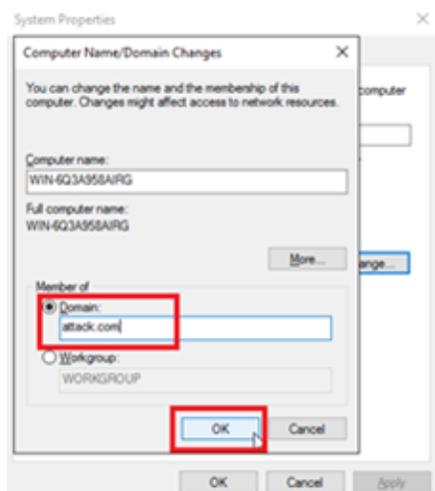
1. Go to *Control Panel > System*, and click *Change settings*.



2. On the *System Properties* page, click *Change*.



3. Input your domain information and then click *OK*.

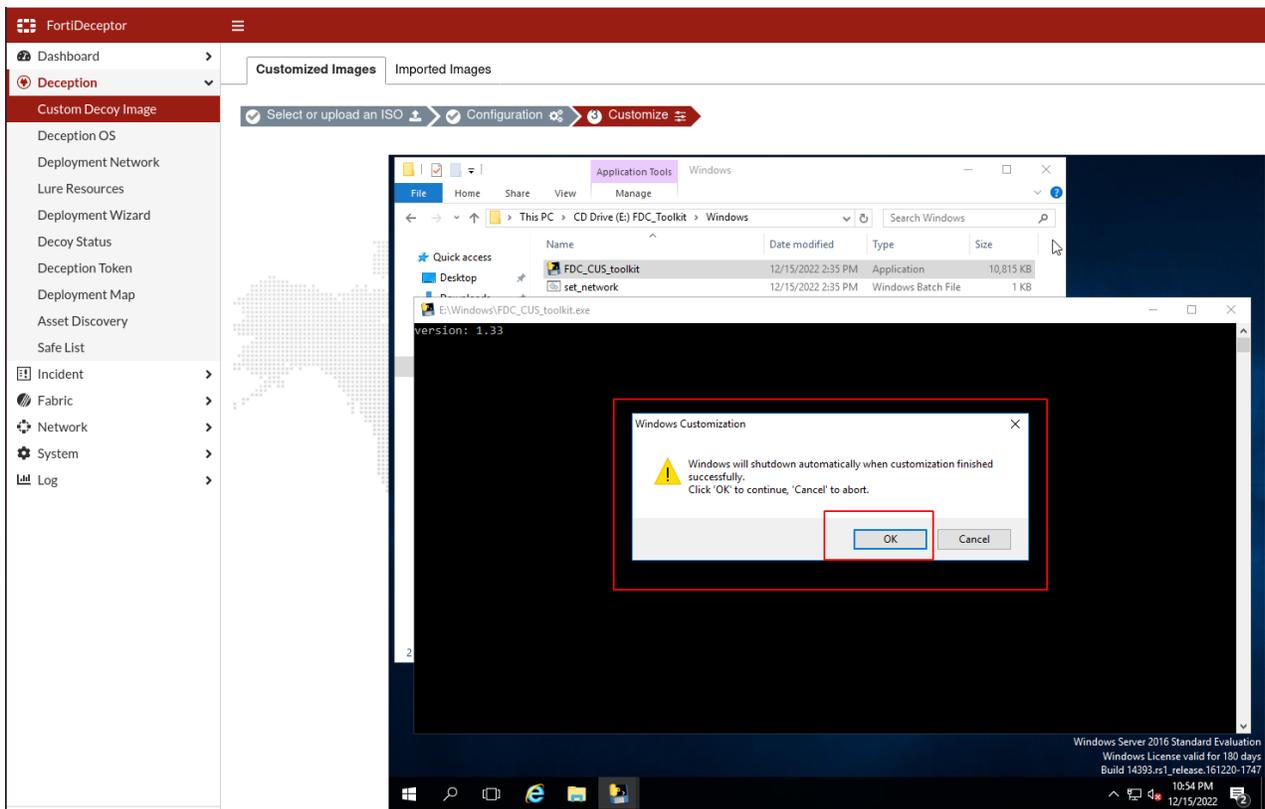


4. Input the domain account, click *OK*.
5. After joining the domain, a restart is required, click *Close*.
6. Click *Restart now*.
7. After Windows restarts, sign on as a local Administrator.

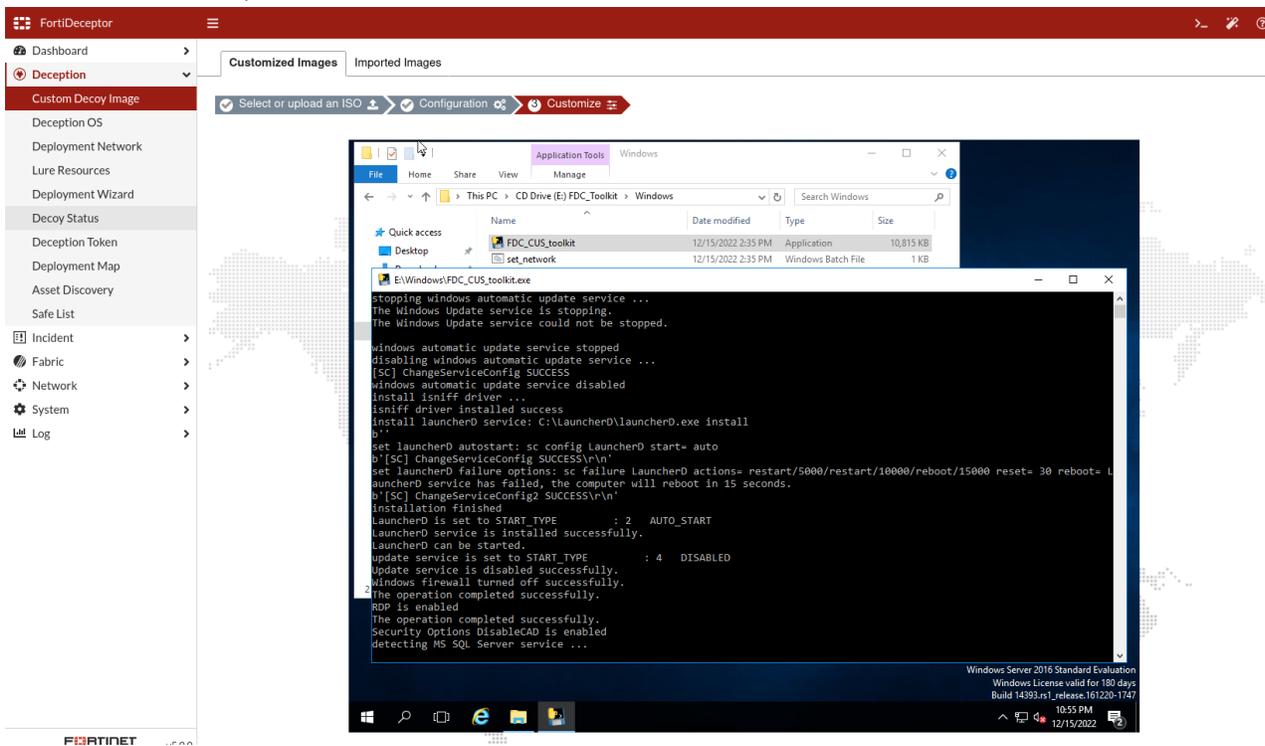
6. Install the FortiDeceptor customization toolkit

To install the customization toolkit:

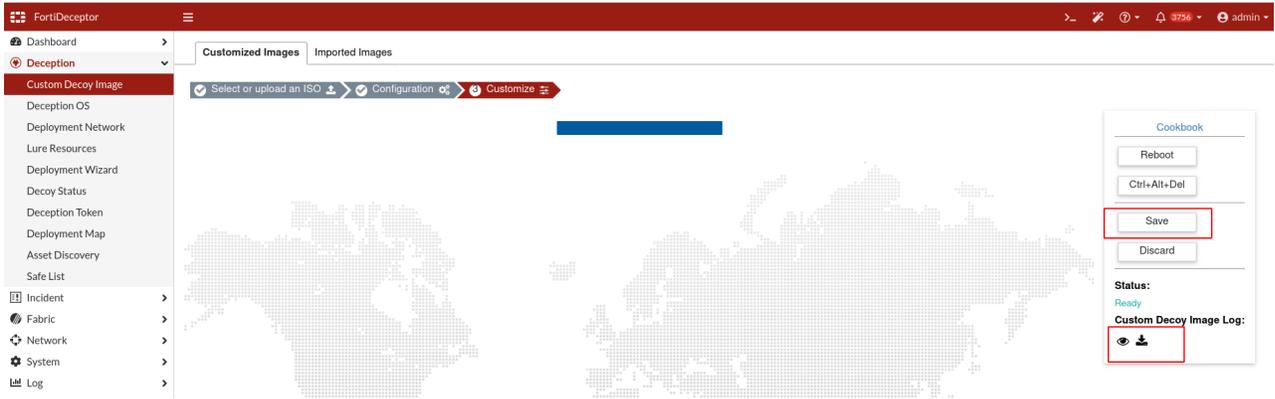
1. After you are finished customizing the image, right-click the file `FDC_CUS_toolkit.exe`, and select *Run as Administrator*. The warning message *Windows will shut down automatically when customization finished successfully*, appears.



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



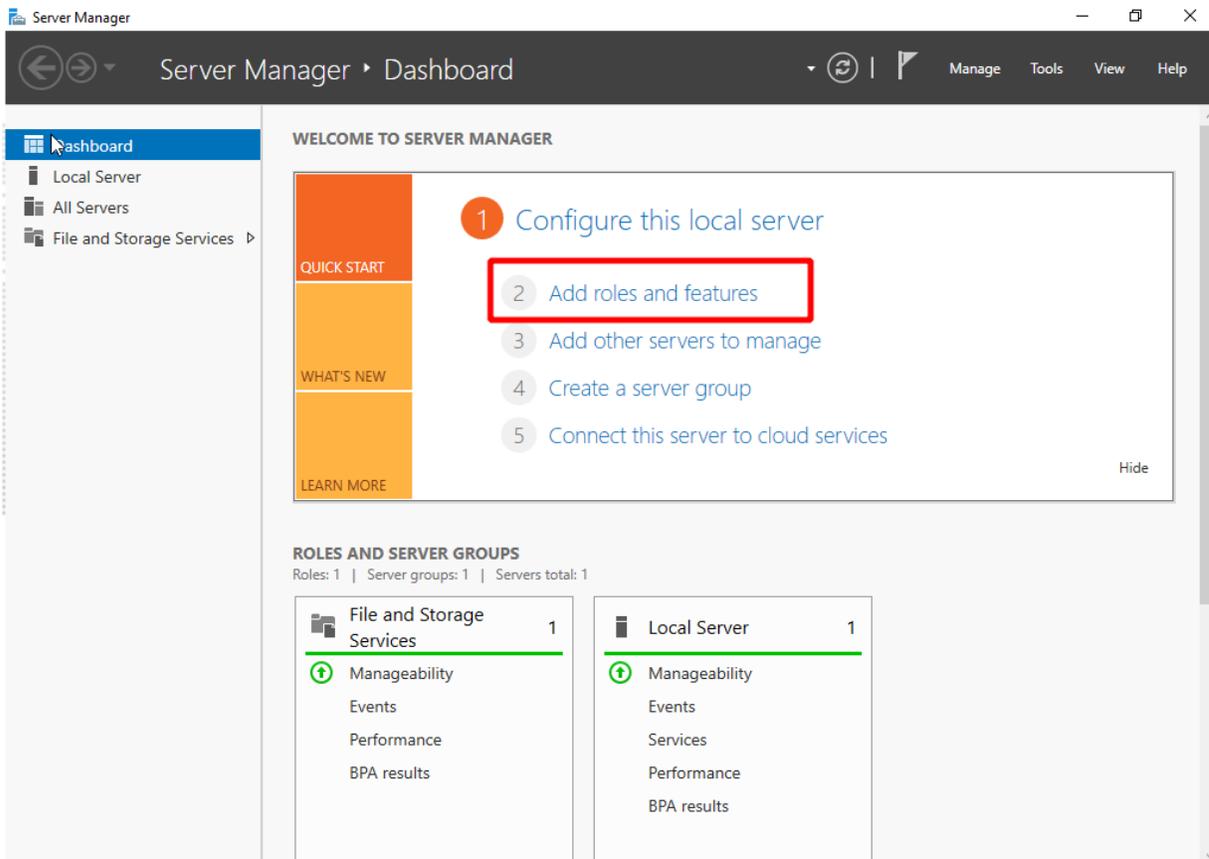
3. After the toolkit is installed, click Save. You can also View or Download the Custom Decoy Image Log.

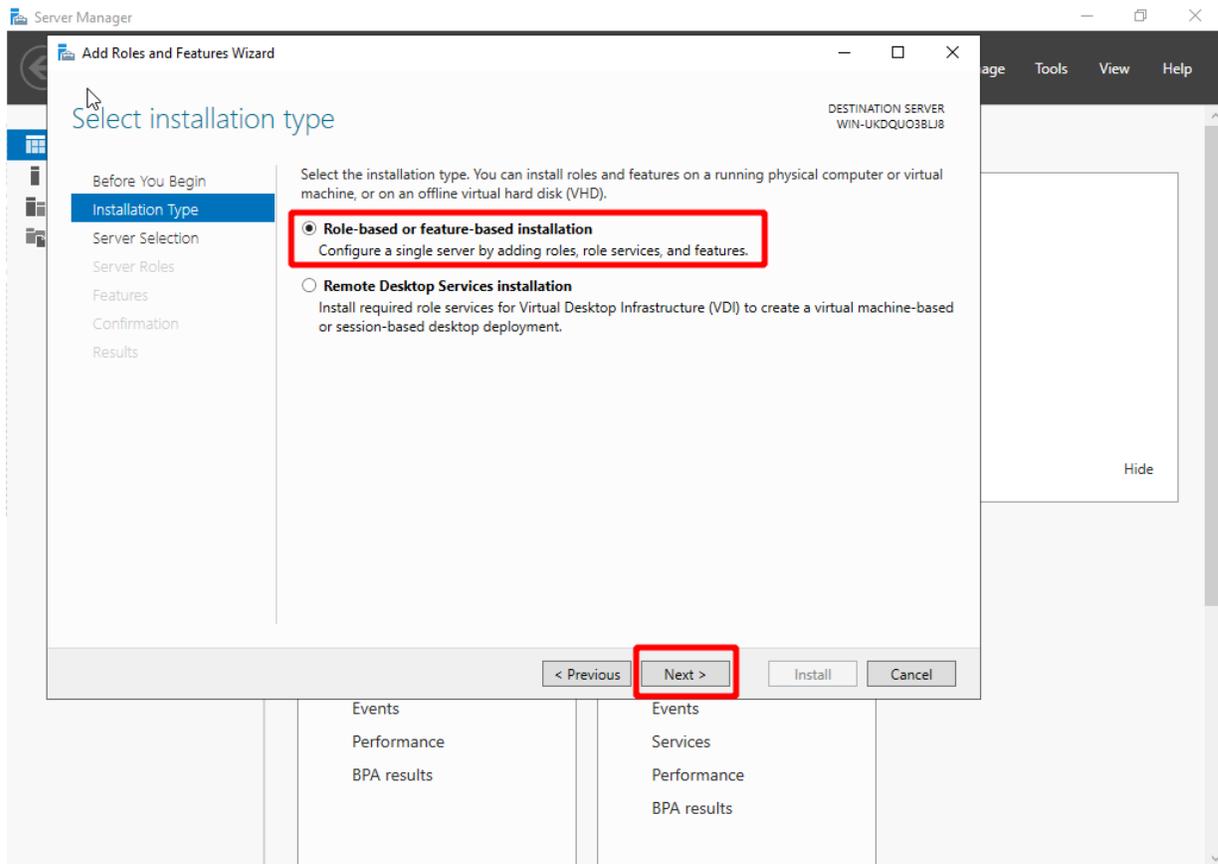


7. (Optional) Turn on Active Directory (AD) controller

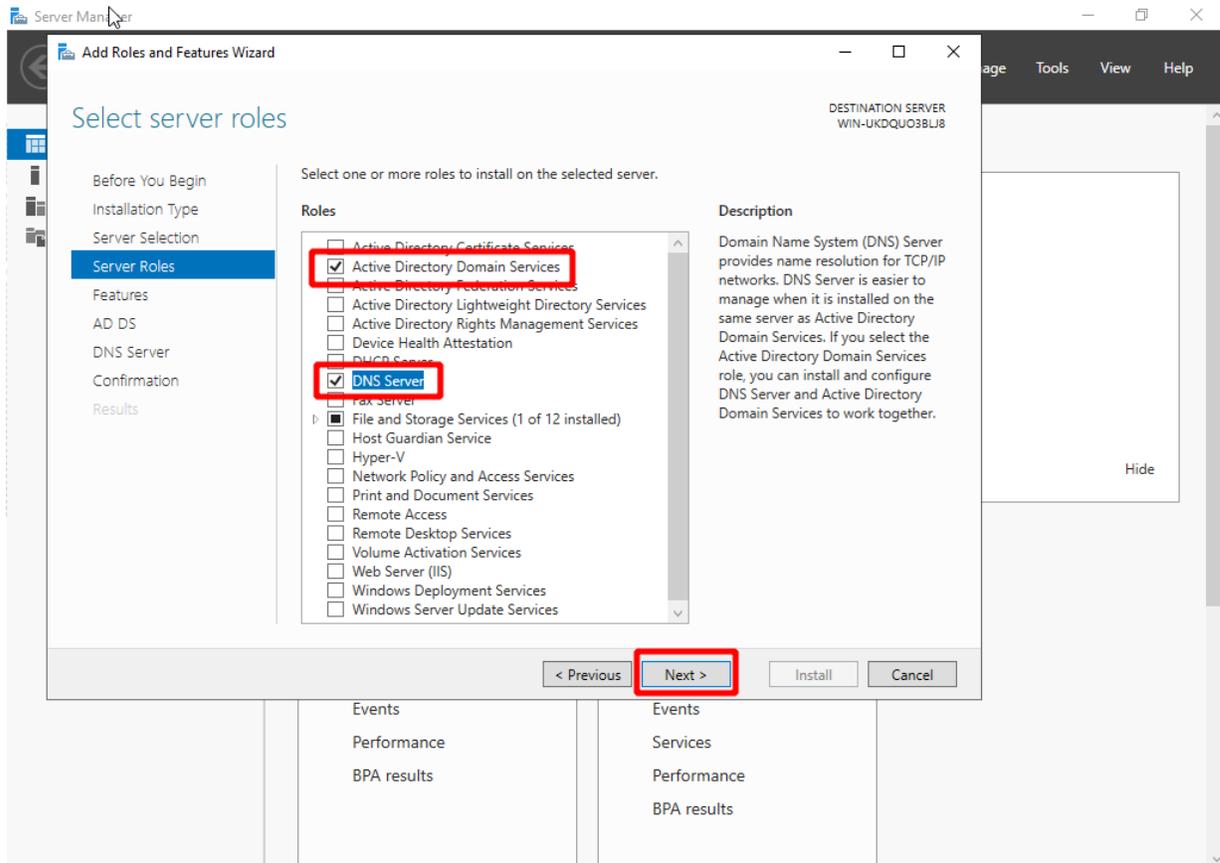
1. Setup the new domain controller for the new domain forest.

- 1. Install Active Directory Domain Services and DNS Servers
 - a. Open the Server Manager go to *Dashboard > Roles Summary > Add roles and features.*

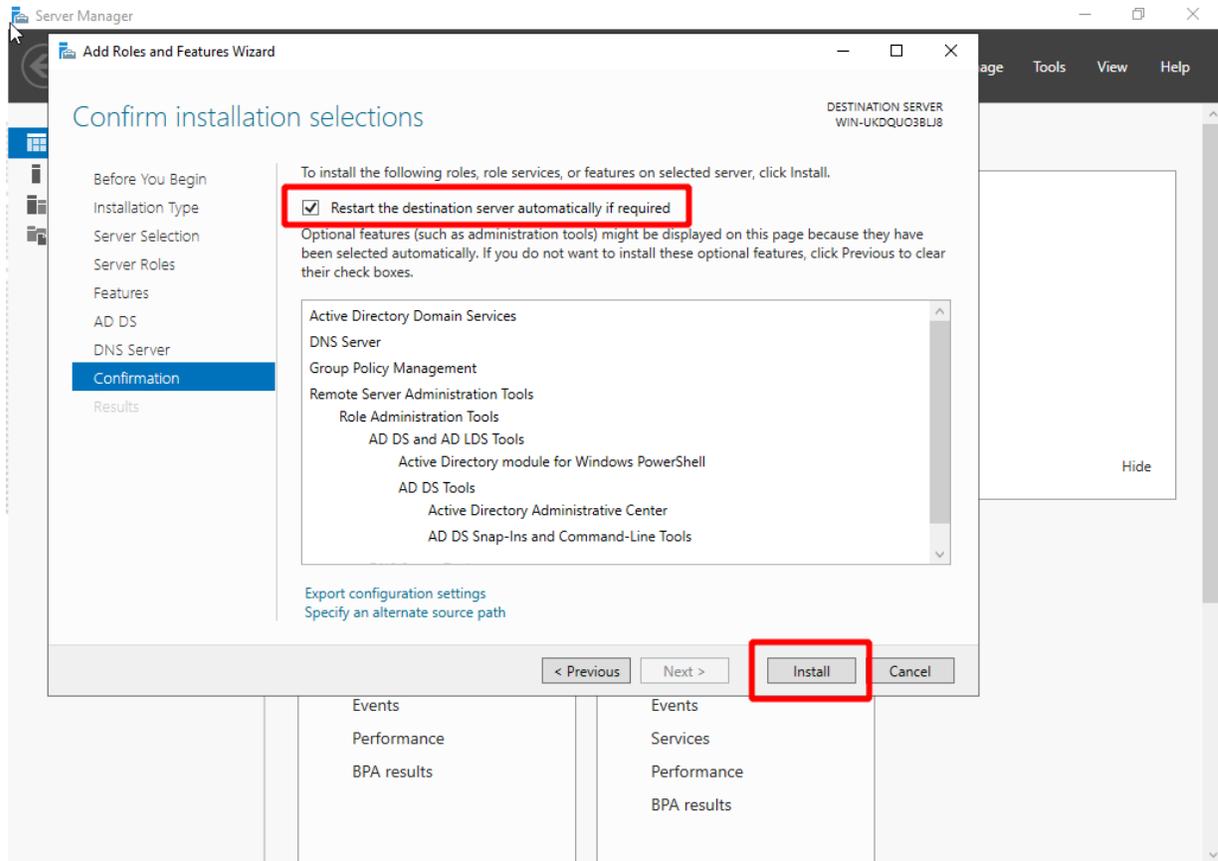


b. Select *Role-based or Feature-based installation*.**c. Click *Server Role* and select *Active Directory Domain Services* and click *Next*.**

The DNS Server role is no longer supported in the version 6.2 GA. For domain name resolution, use a standalone third-party DNS server, such as a Linux-based dnsmasq server or a Windows DNS server hosted on a separate machine.

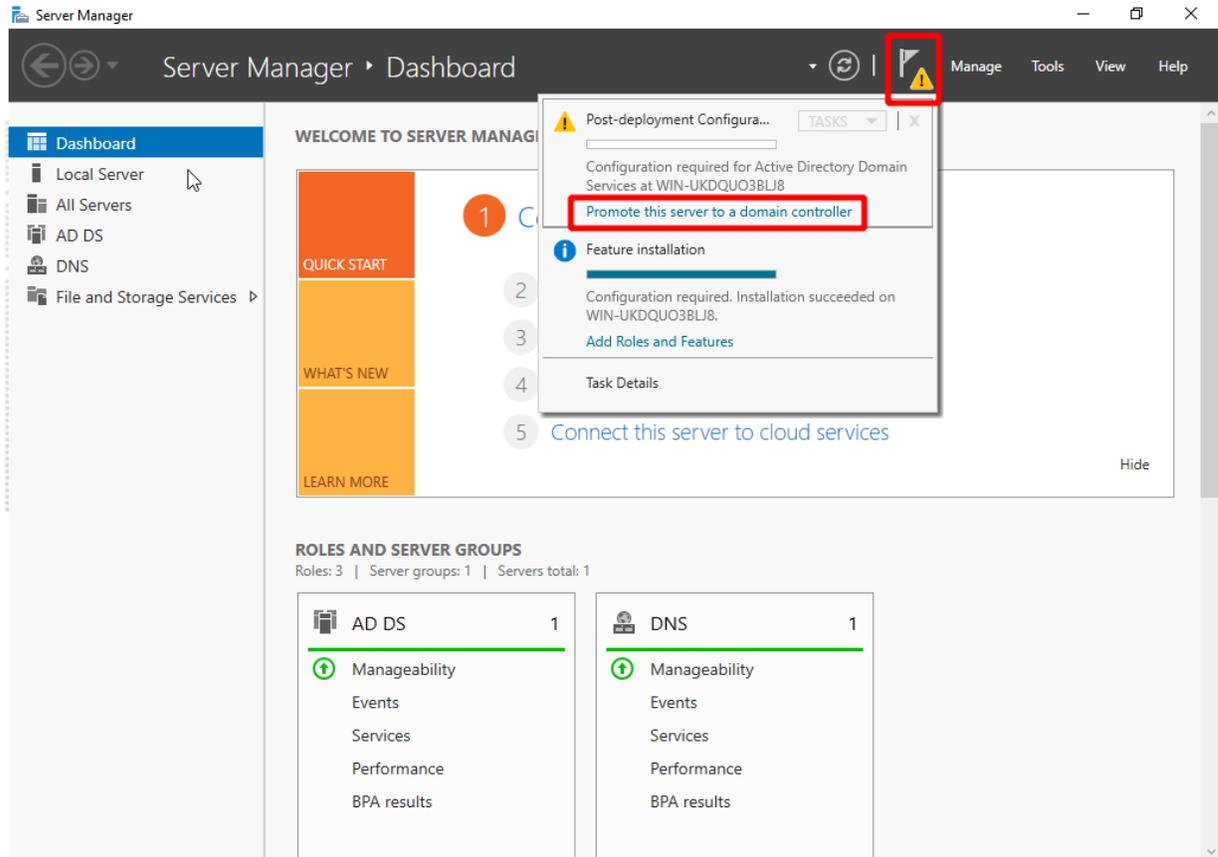


- d. Keep clicking *Next* until you reach the *Confirmation* page. Select *Restart the destination server automatically if required*, and click *Install*.

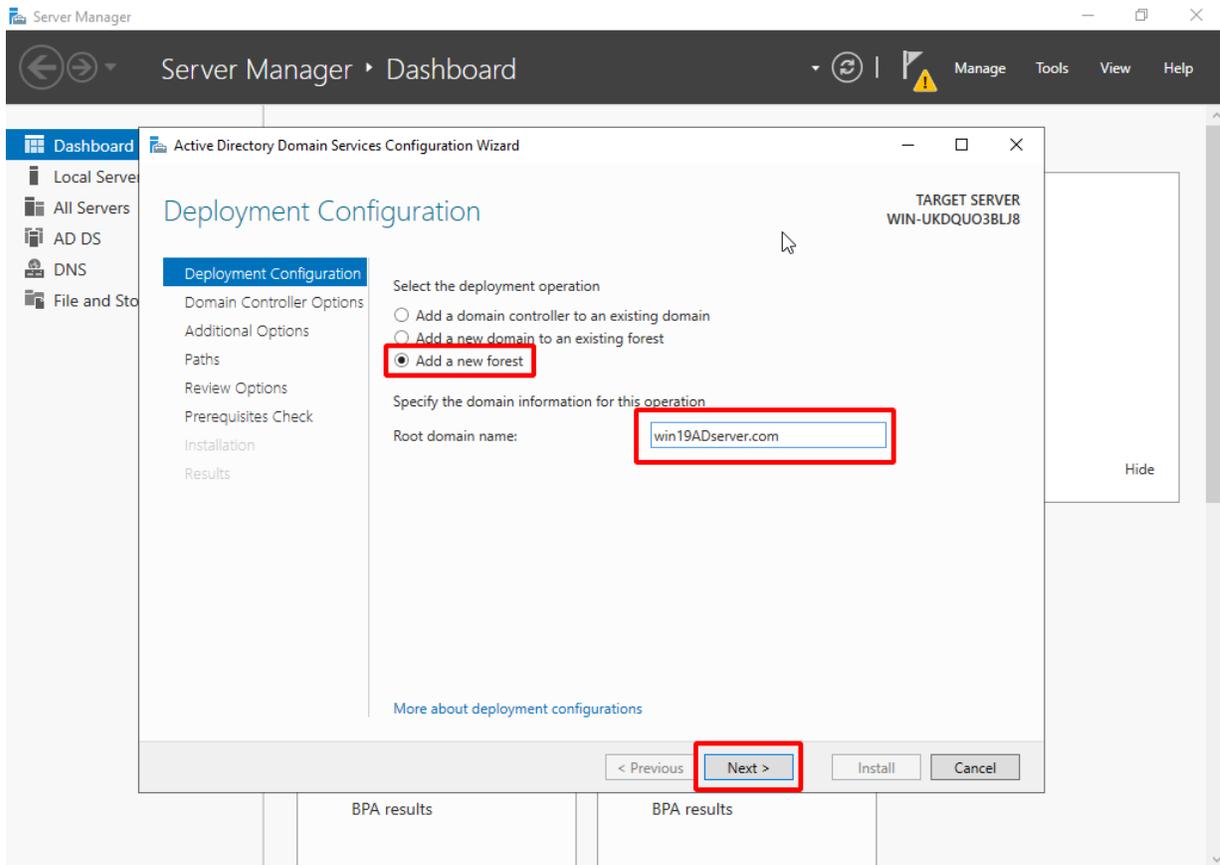


2. Promote the server into a domain controller.

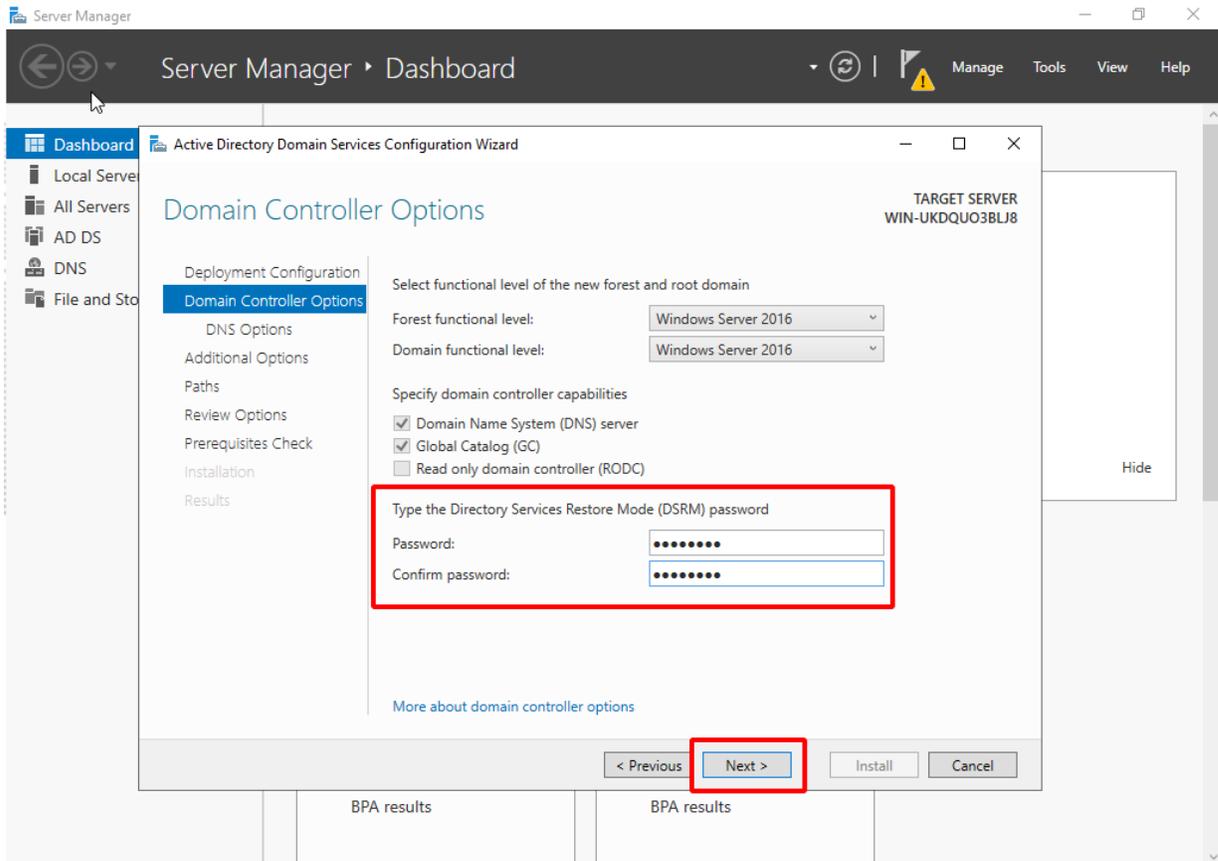
- a. Click the notification flag next to the *Manage* menu and click *Promote this server to a domain controller*. The configuration wizard opens.



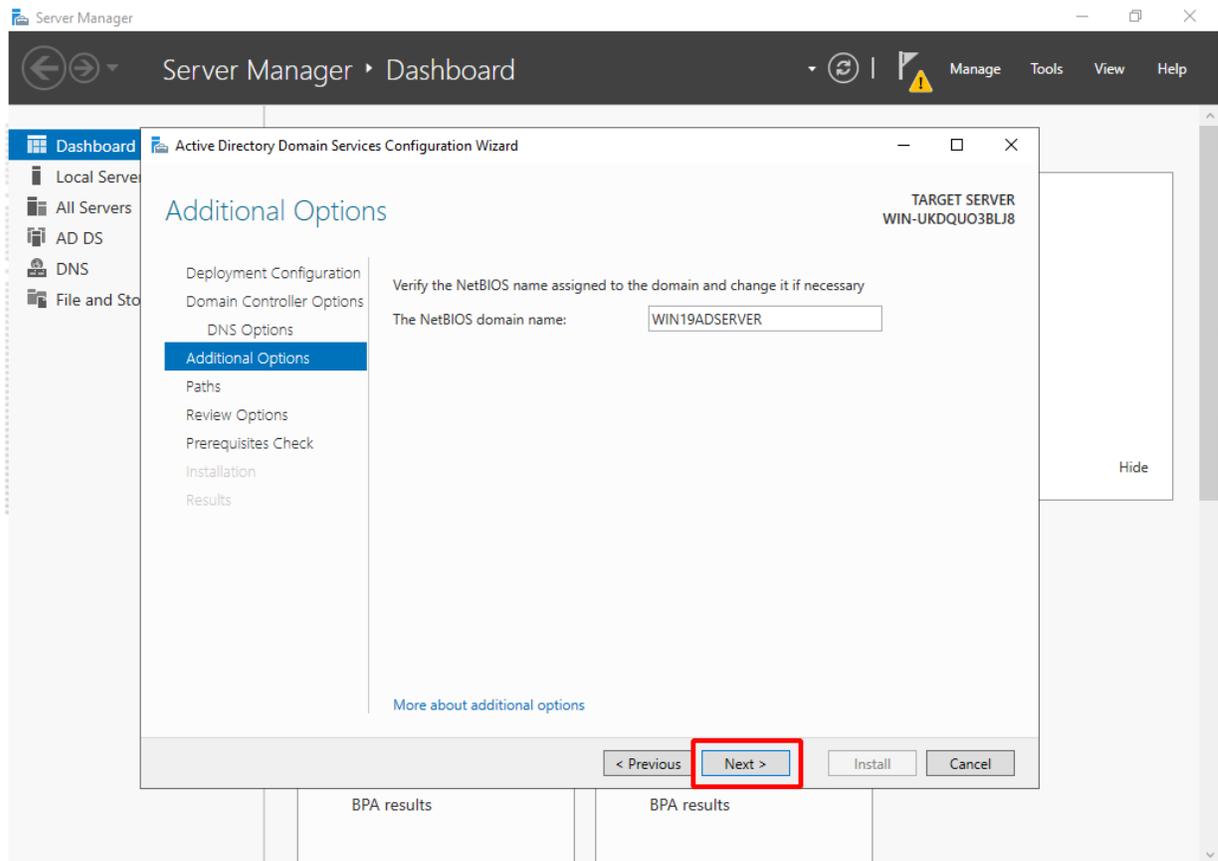
- b. In *Deployment Configuration*, select *Add a new forest* and enter the *Root domain name*.



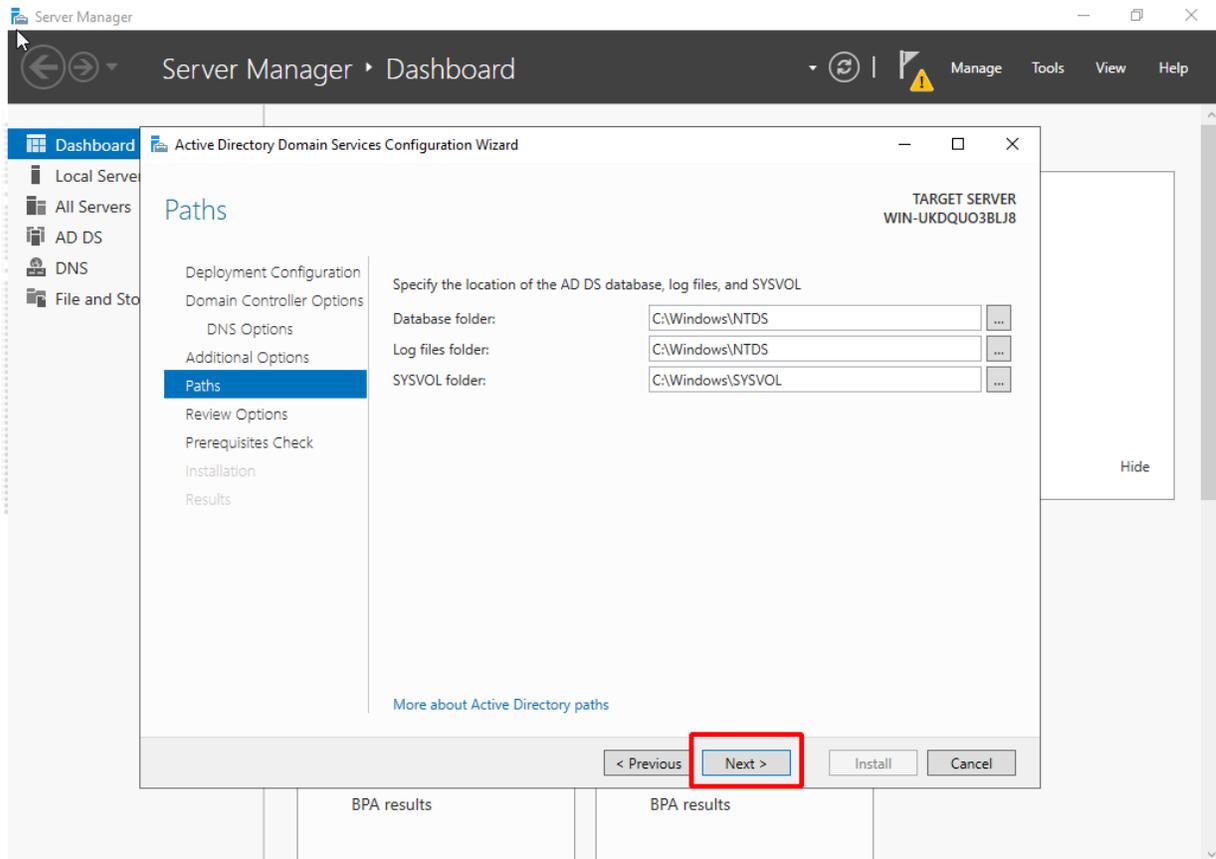
c. In *Domain Controller Options*, enter a password for the domain.



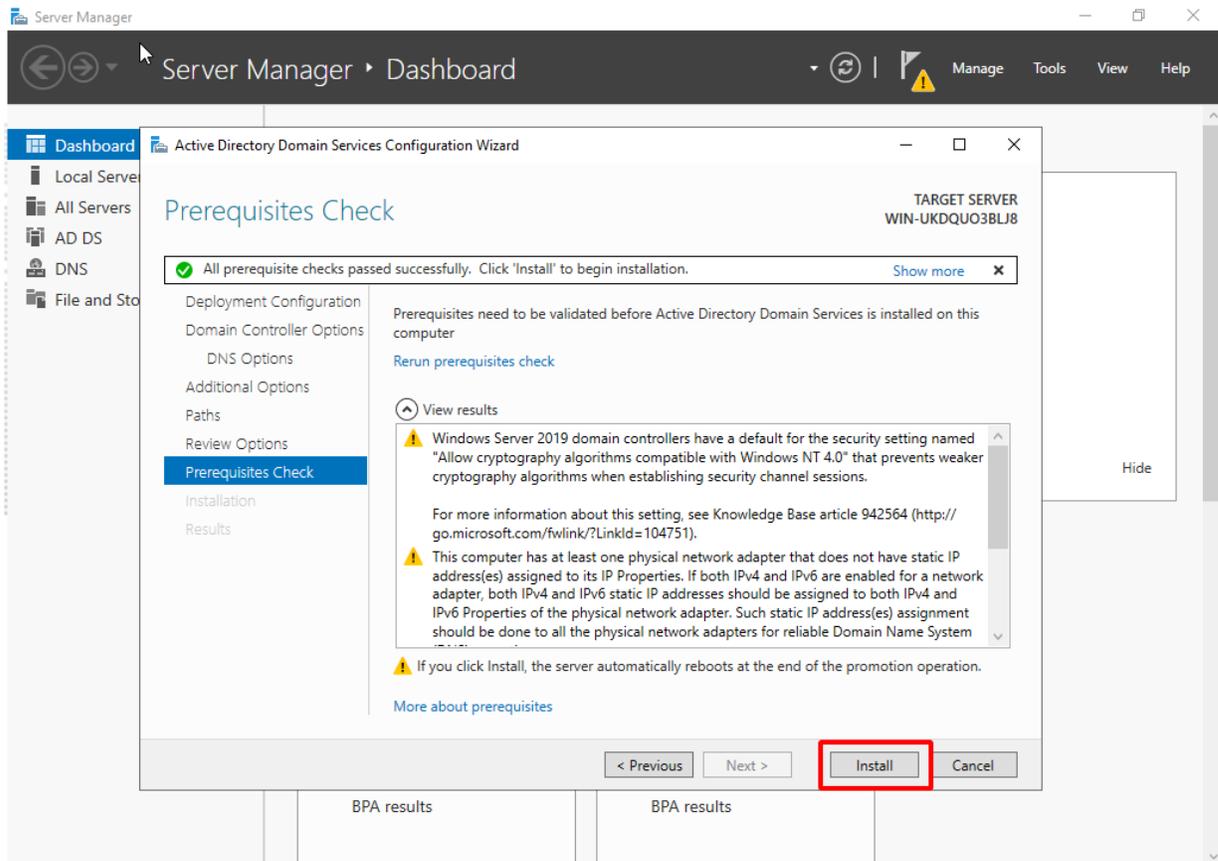
- d. In *Additional Options*, enter a NetBIOS name for your domain (the default name is recommended).



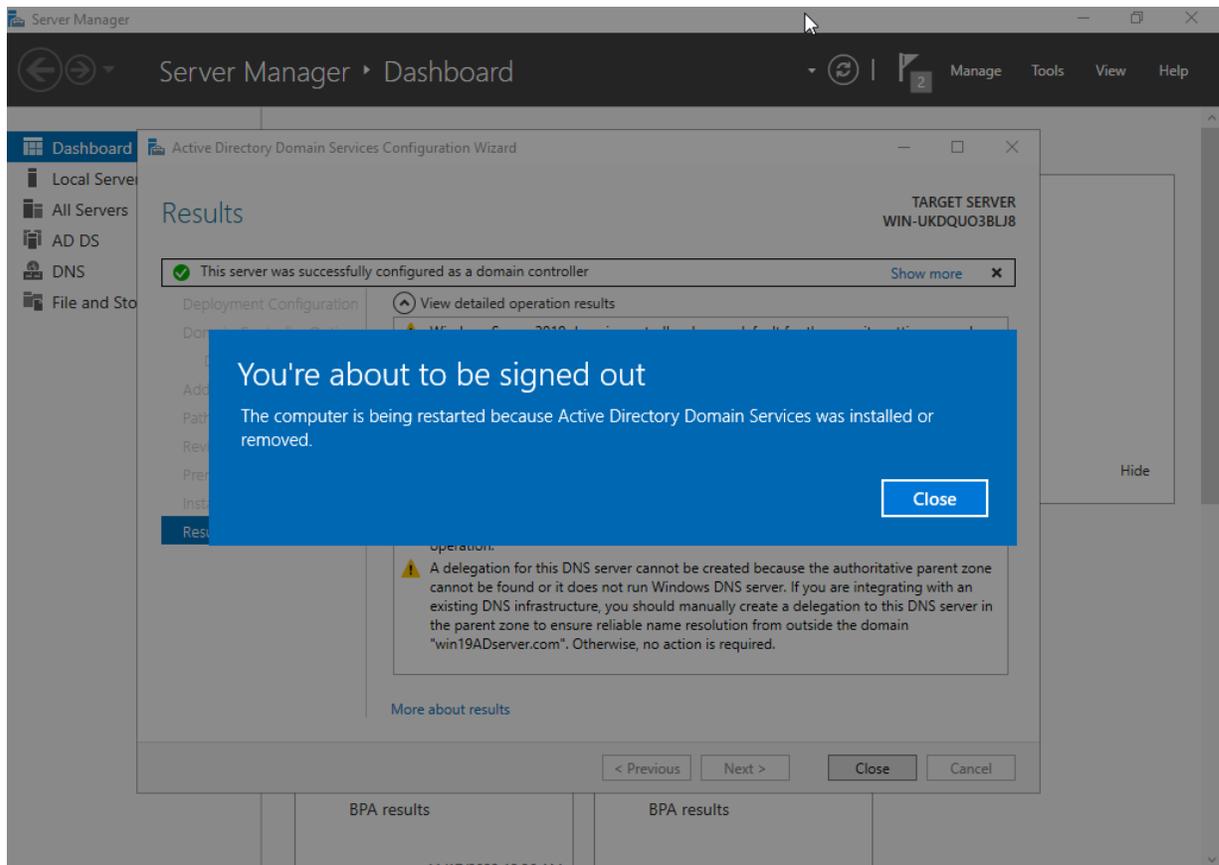
- e. In *Paths*, select the folder where your database, log files, and SYSVOL will be stored (the default folder is recommended), then click *Next*.



- f. Wait for a check-mark to appear and then click *Install*.



- g. The PC will restart.



2. (Required) Set up the DNS server

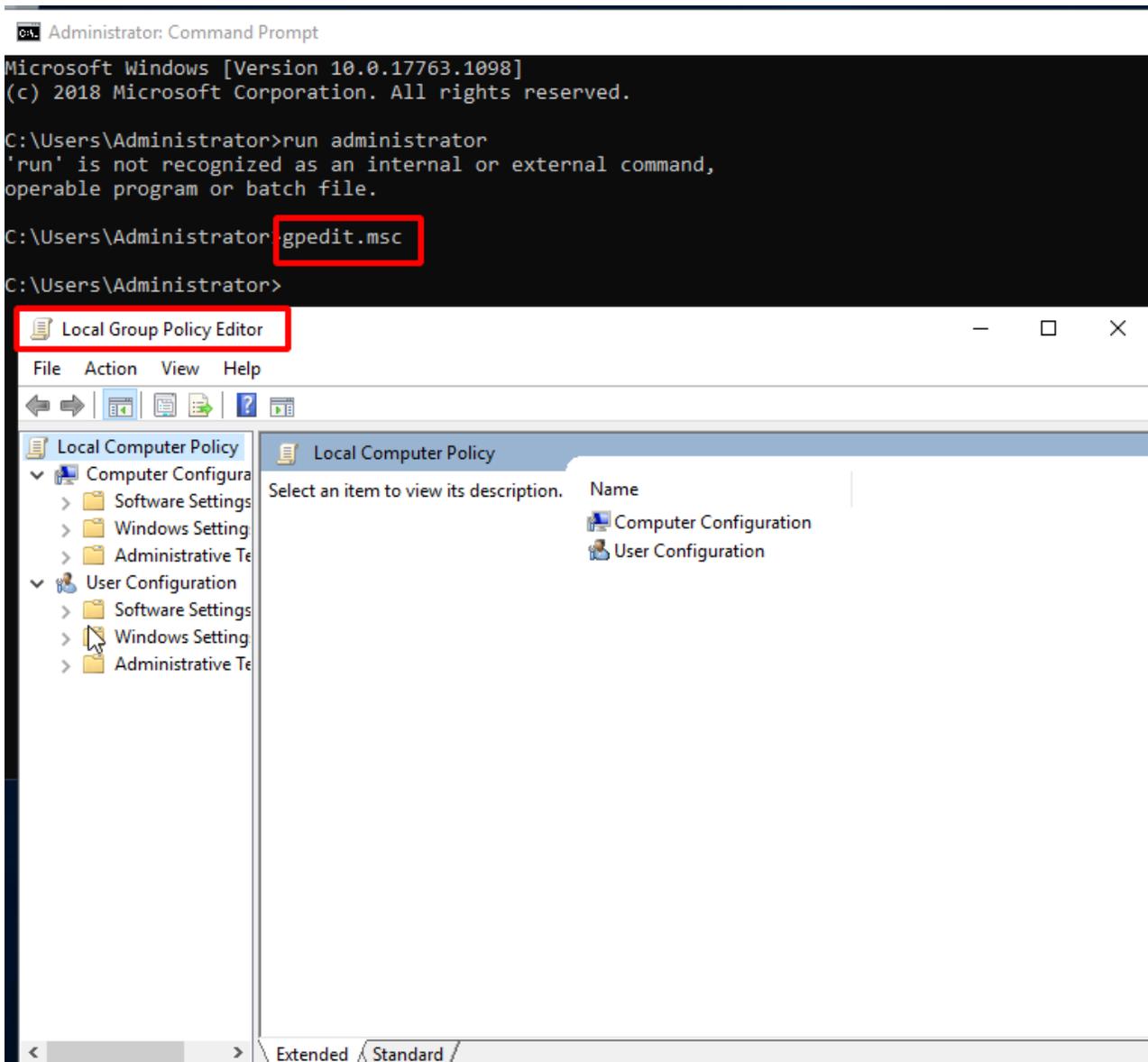


In version 6.2, the default DNS service included with the Windows Server image is no longer supported. You must configure and use an external standalone DNS server to provide domain name resolution for the Active Directory Domain Controller (ADDC).

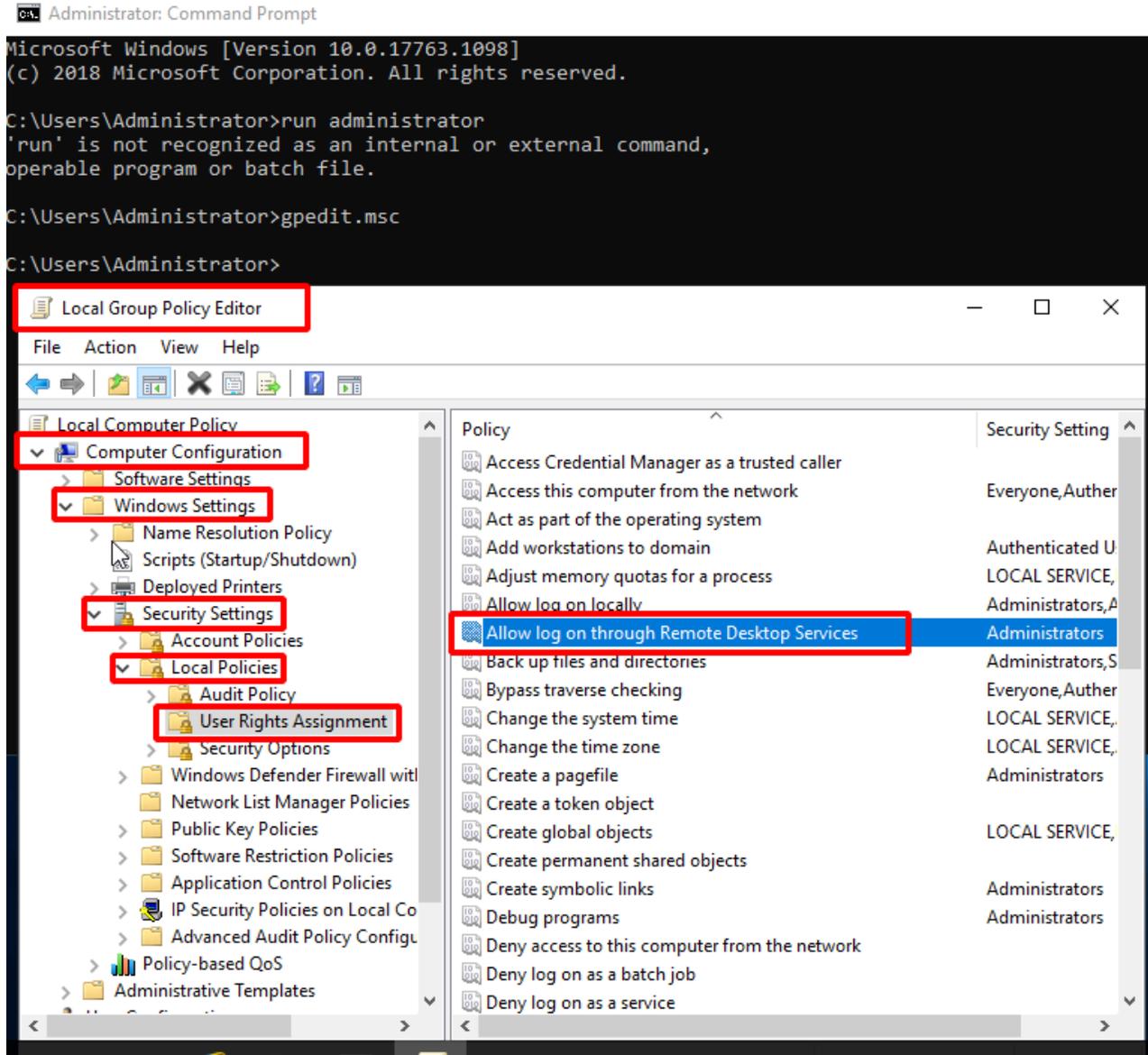
- To add more endpoints to this domain, you may want to configure the DNS forward rule to allow these endpoints to resolve public domains.
- To use a standalone DNS server, *DNS server* should not be installed in [Step 1](#).
- The endpoint may use two DNS servers, one for the local domain, and another for public domains.

3. Add Remote Desktop Users to the Allow log on through Remote Desktop Services Properties policy

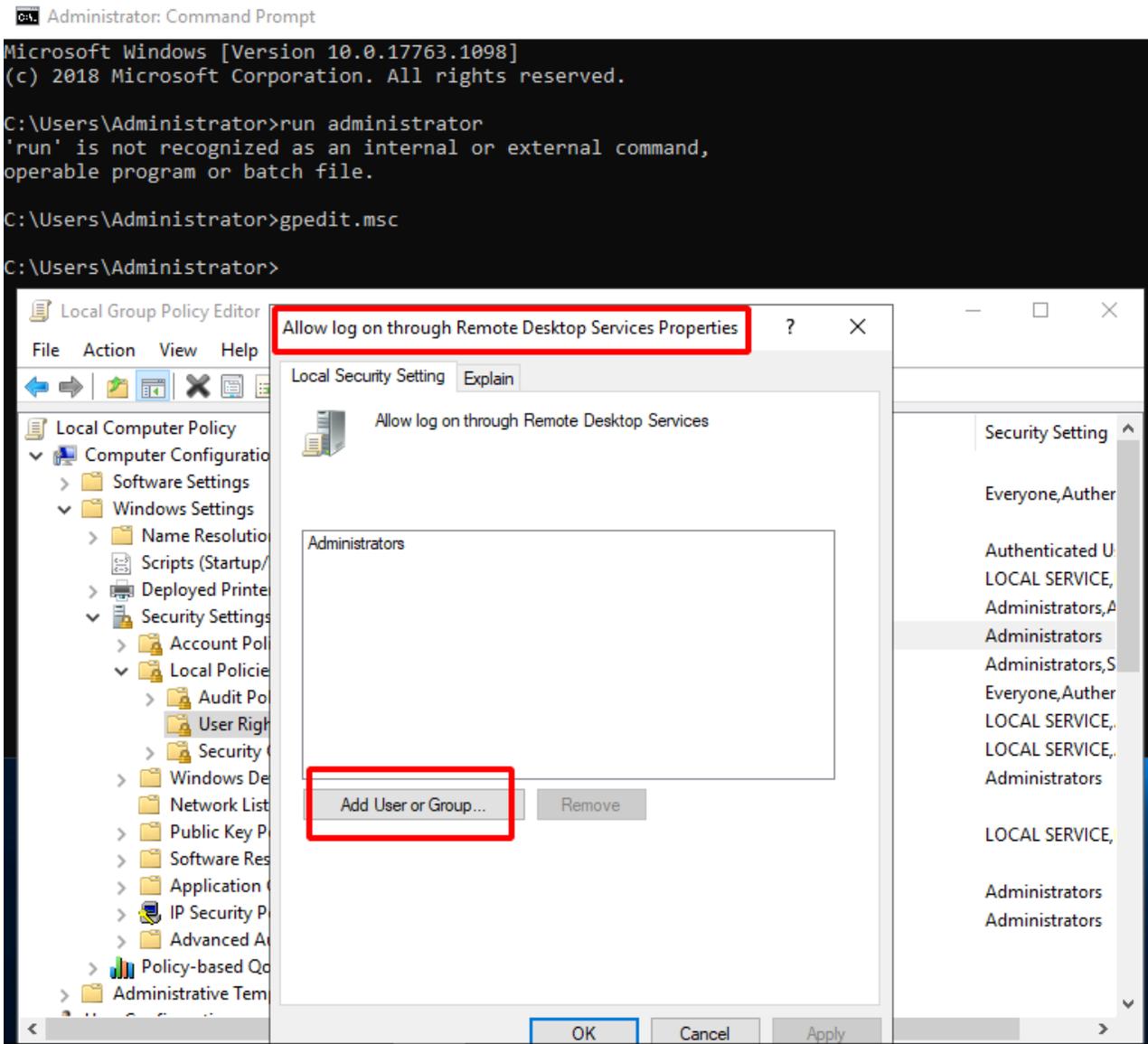
1. Open a command window as an administrator, then enter `gpedit.msc` to open the local group policy.



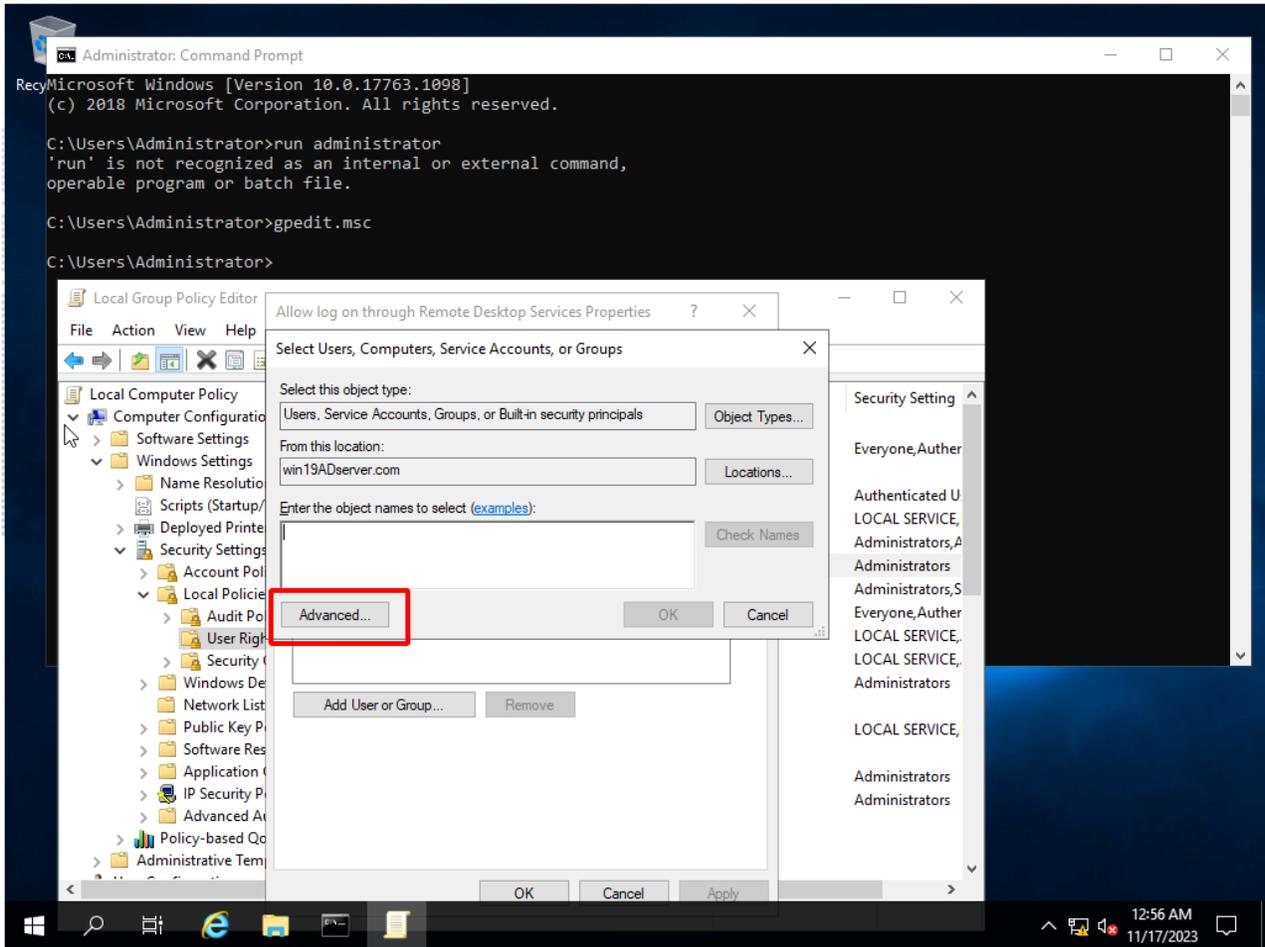
2. Go to *Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Policy Name: Allow log on through Remote Desktop Services*.



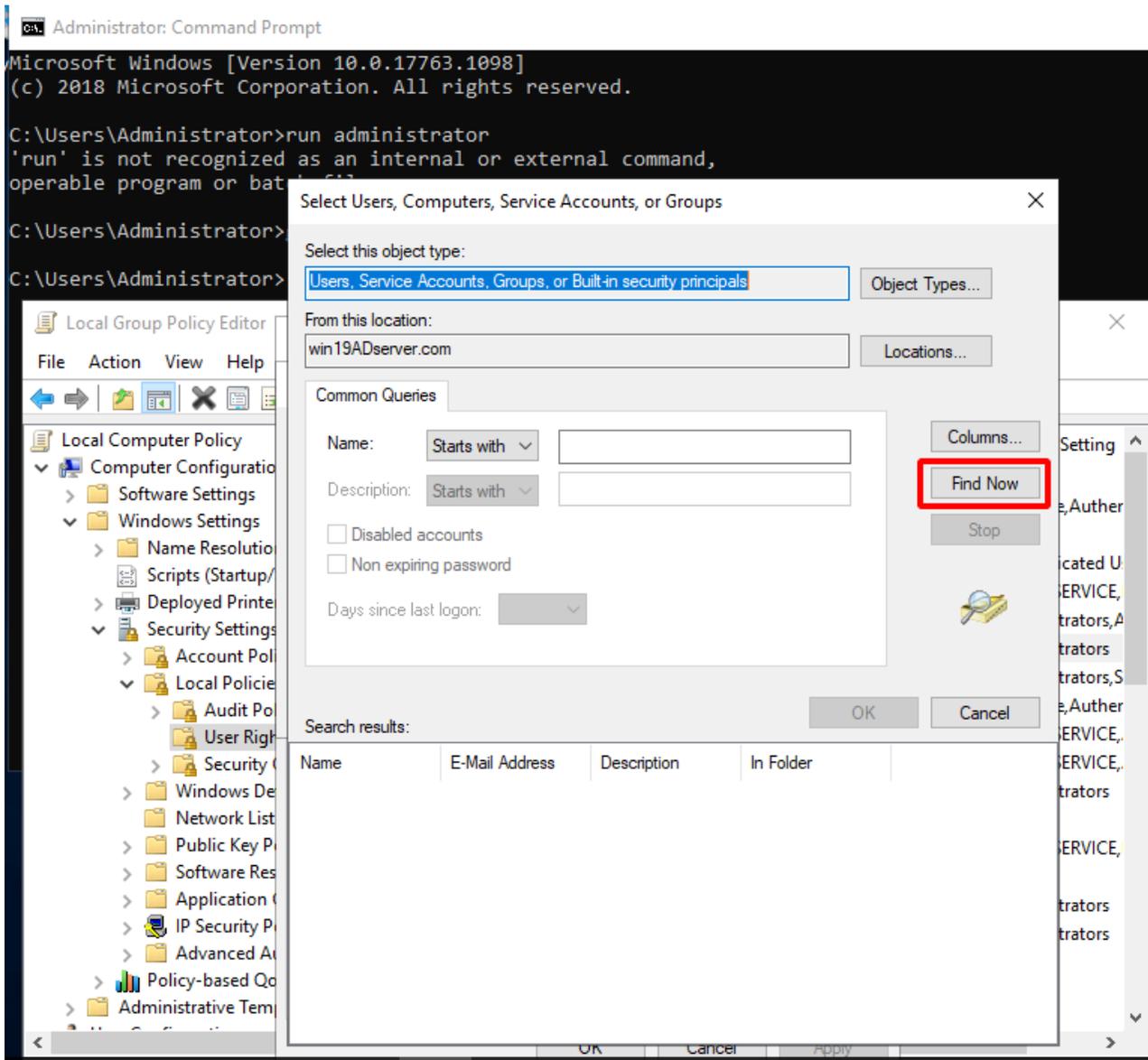
3. Select *Add User or Group* of *Allow log on through Remote Desktop Services* policy.



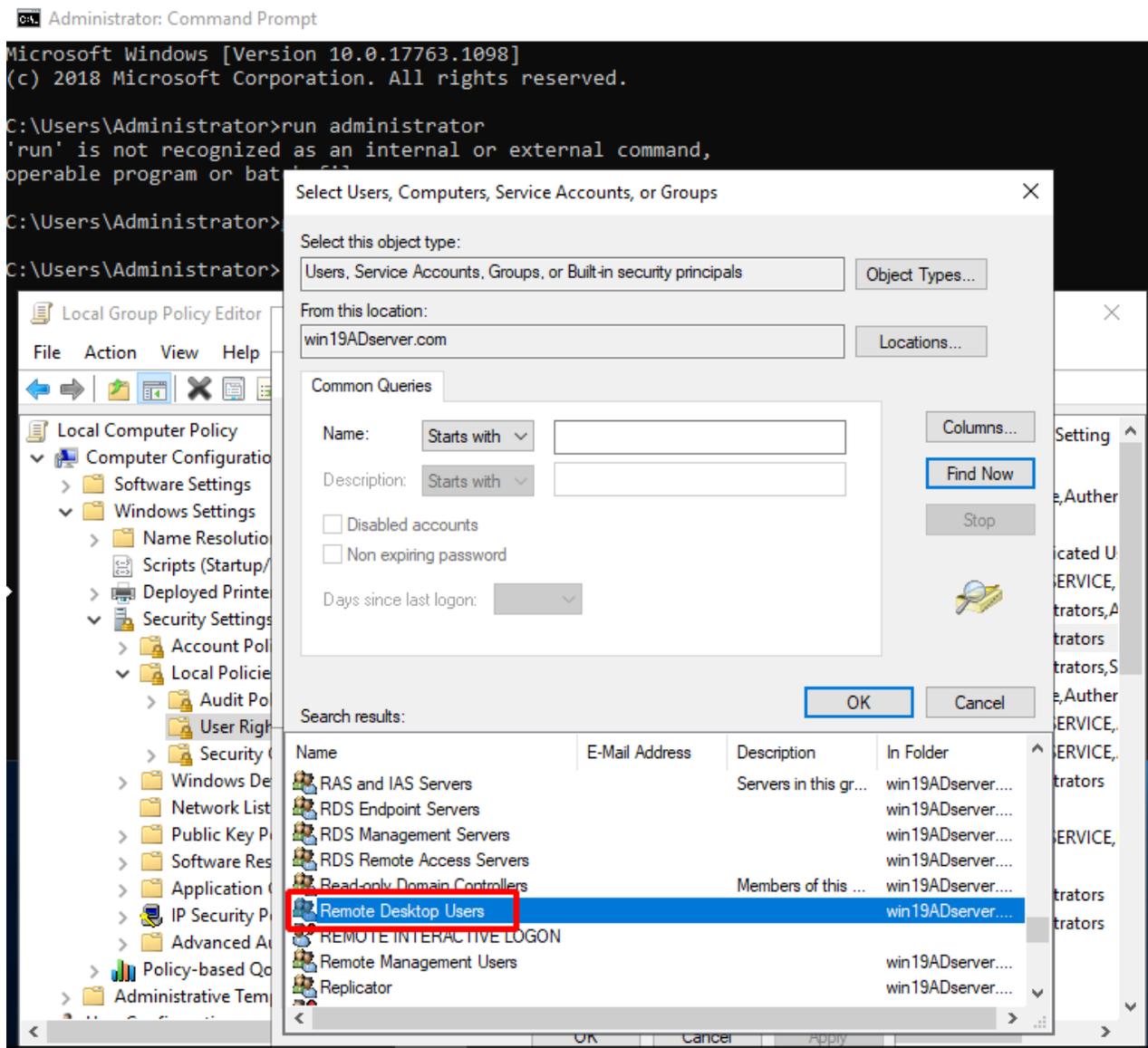
4. Click *Advanced*.



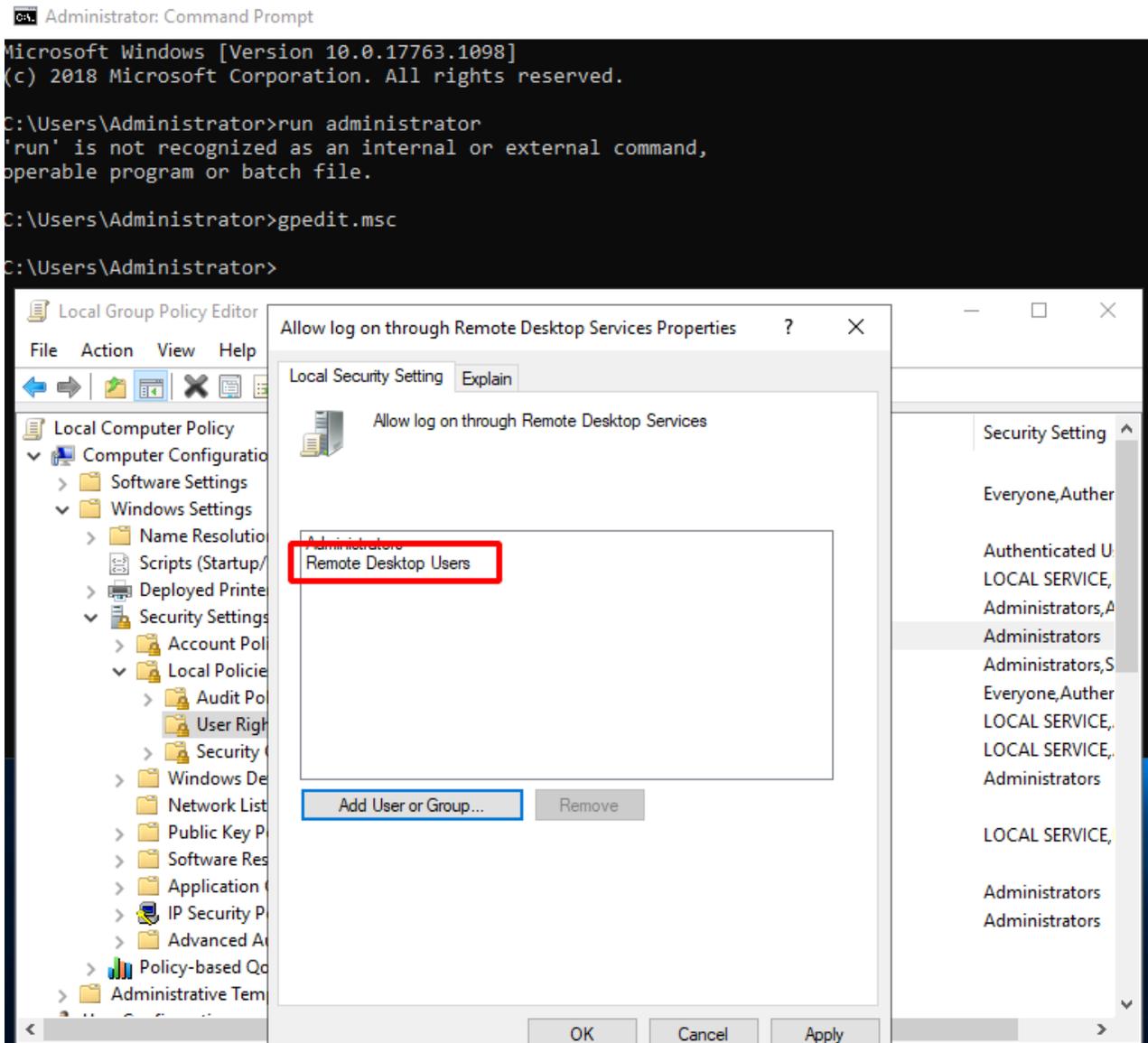
5. Click *Find Now*.



6. Add Remote Desk User group.



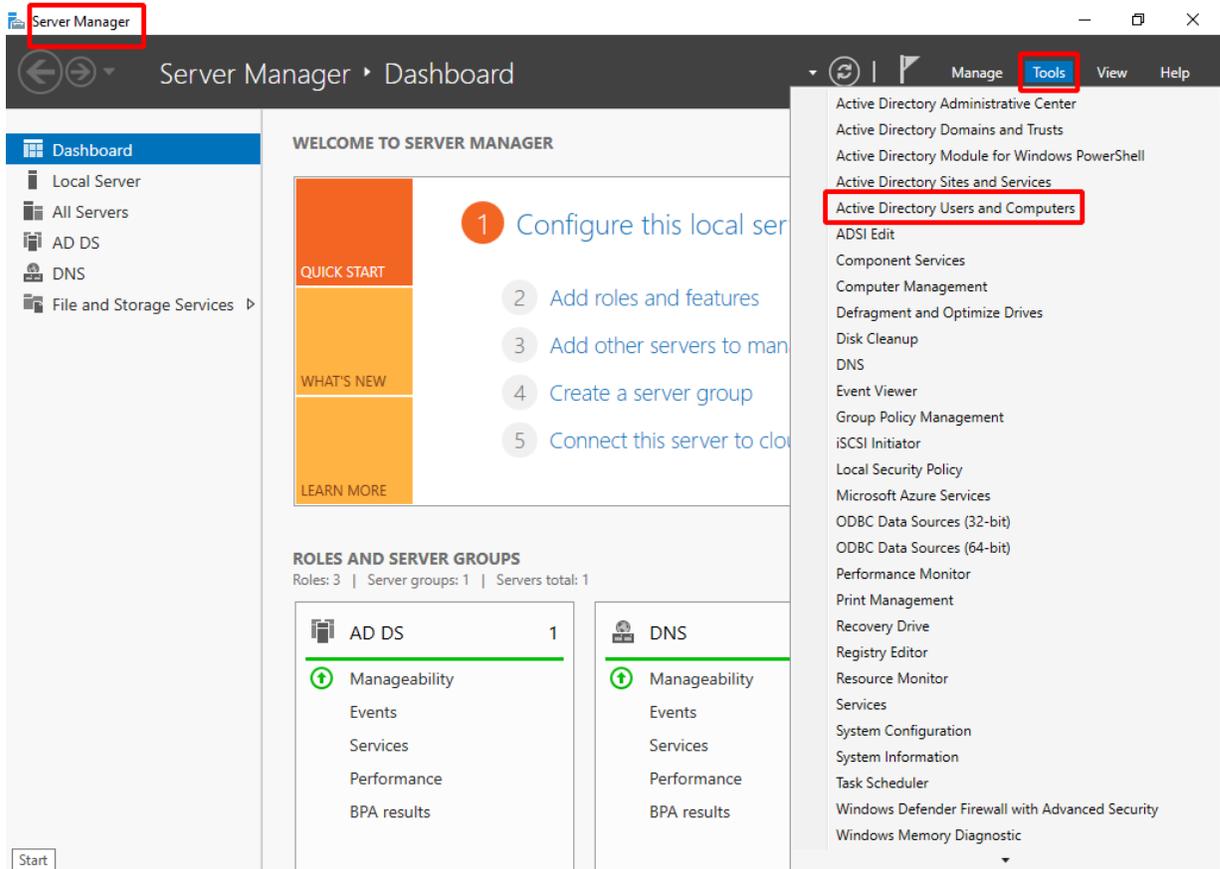
7. Remote Desktop Users is added.



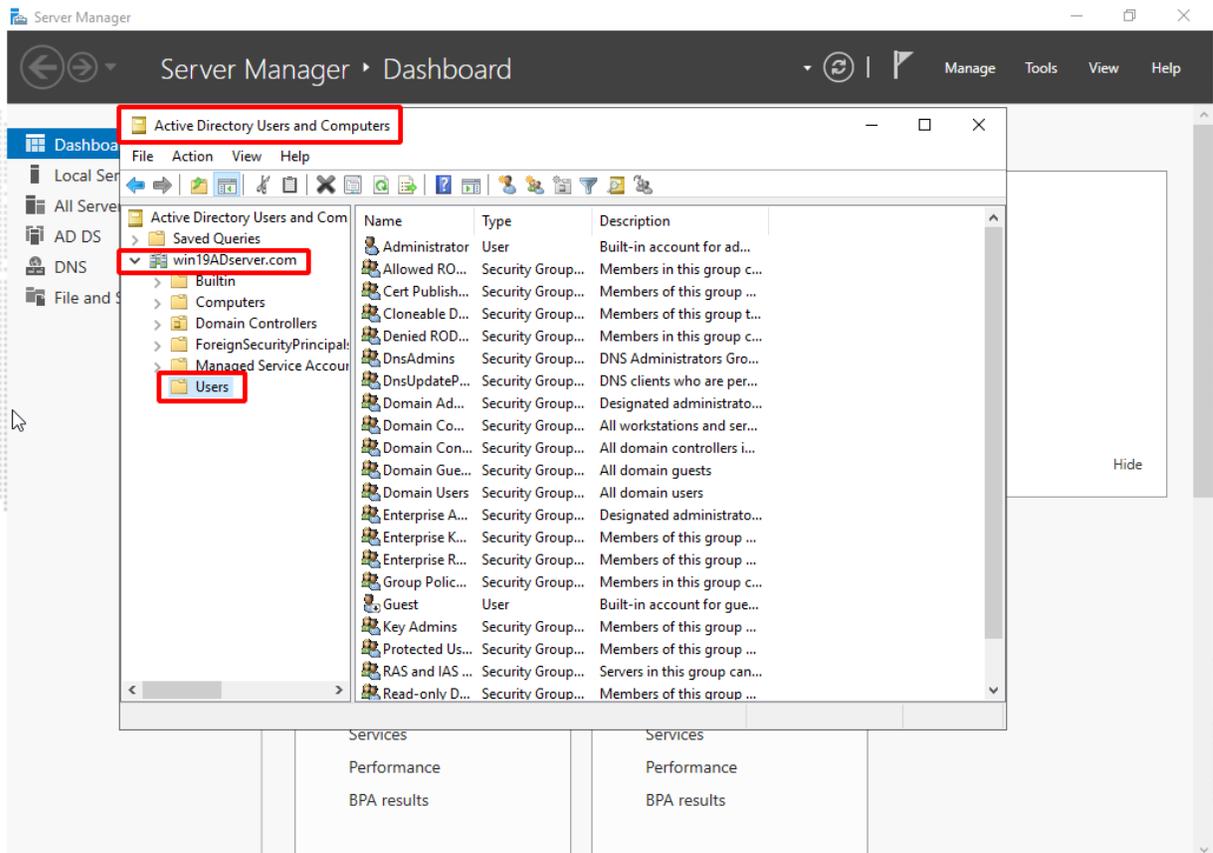
4. (Optional) Add AD Users to the Remote Desk User group

1. Add Active Directory Users

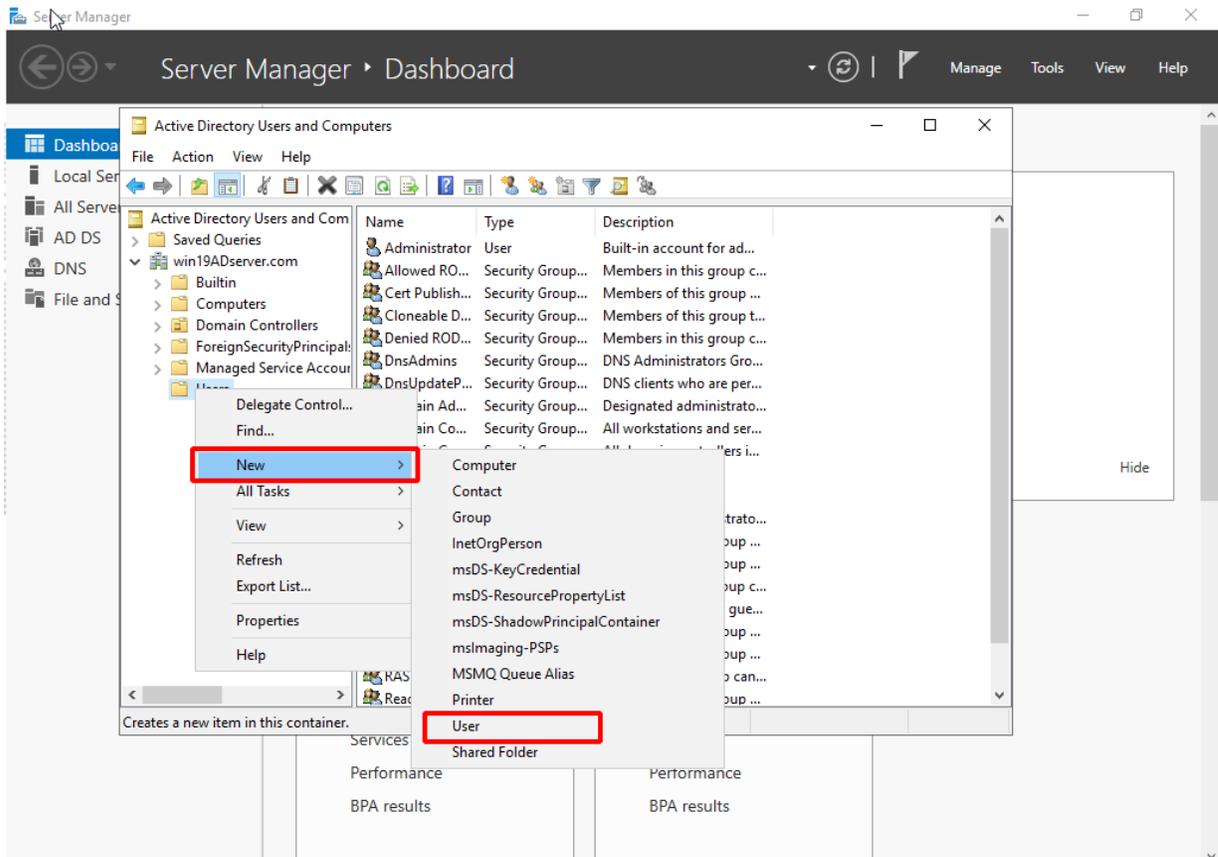
- a. In the Server Manager, click *Tools > Active Directory Users and Computers*.



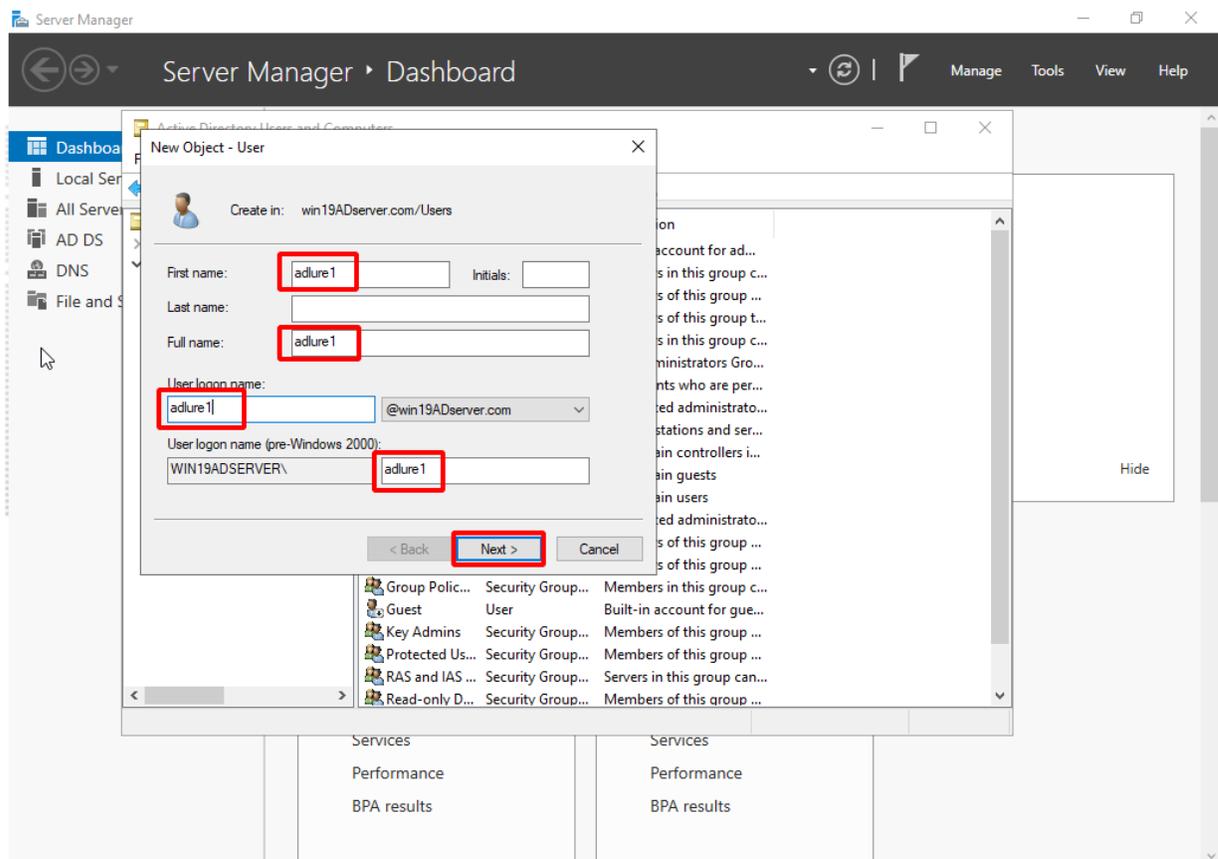
- b. Right-click the domain name and open the *Users* folder.



- c. Right-click the *Users* folder and select *New > User*.

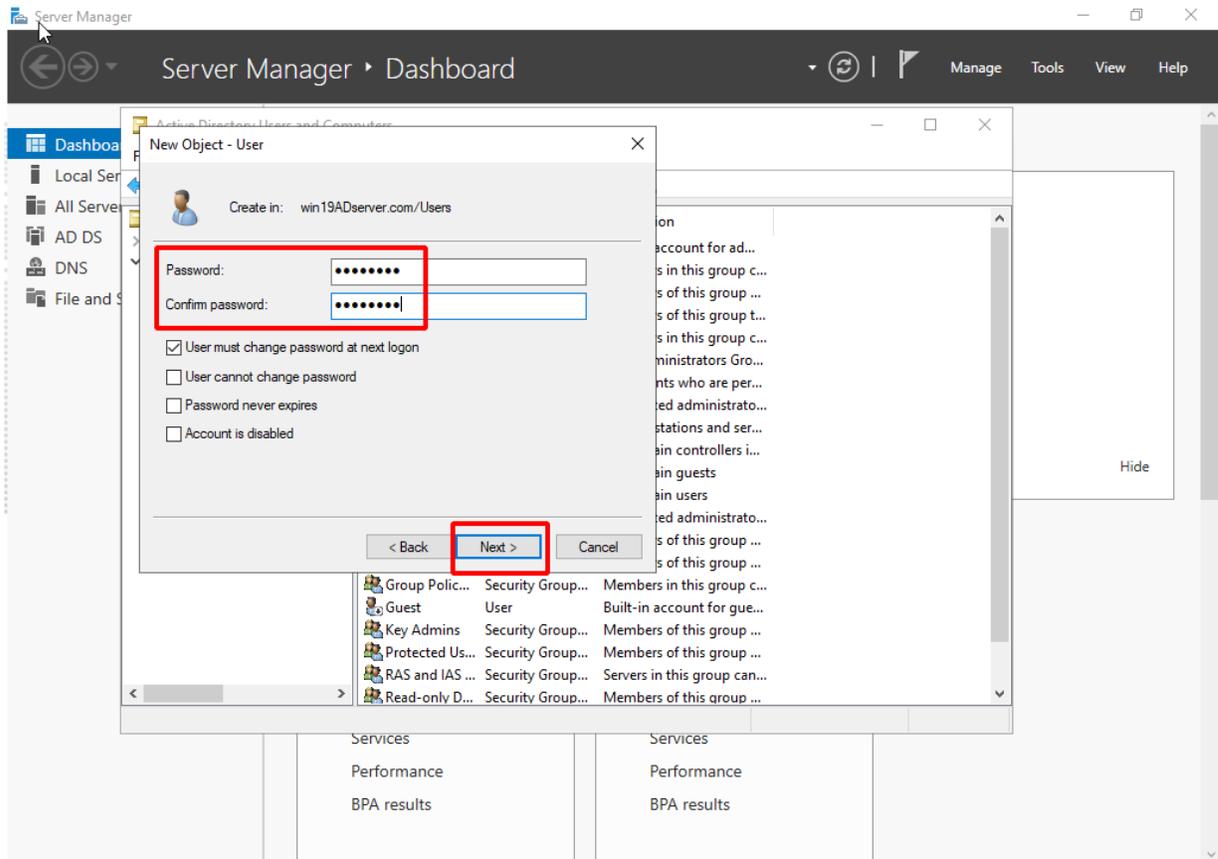


d. Enter the AD user name and click Next.

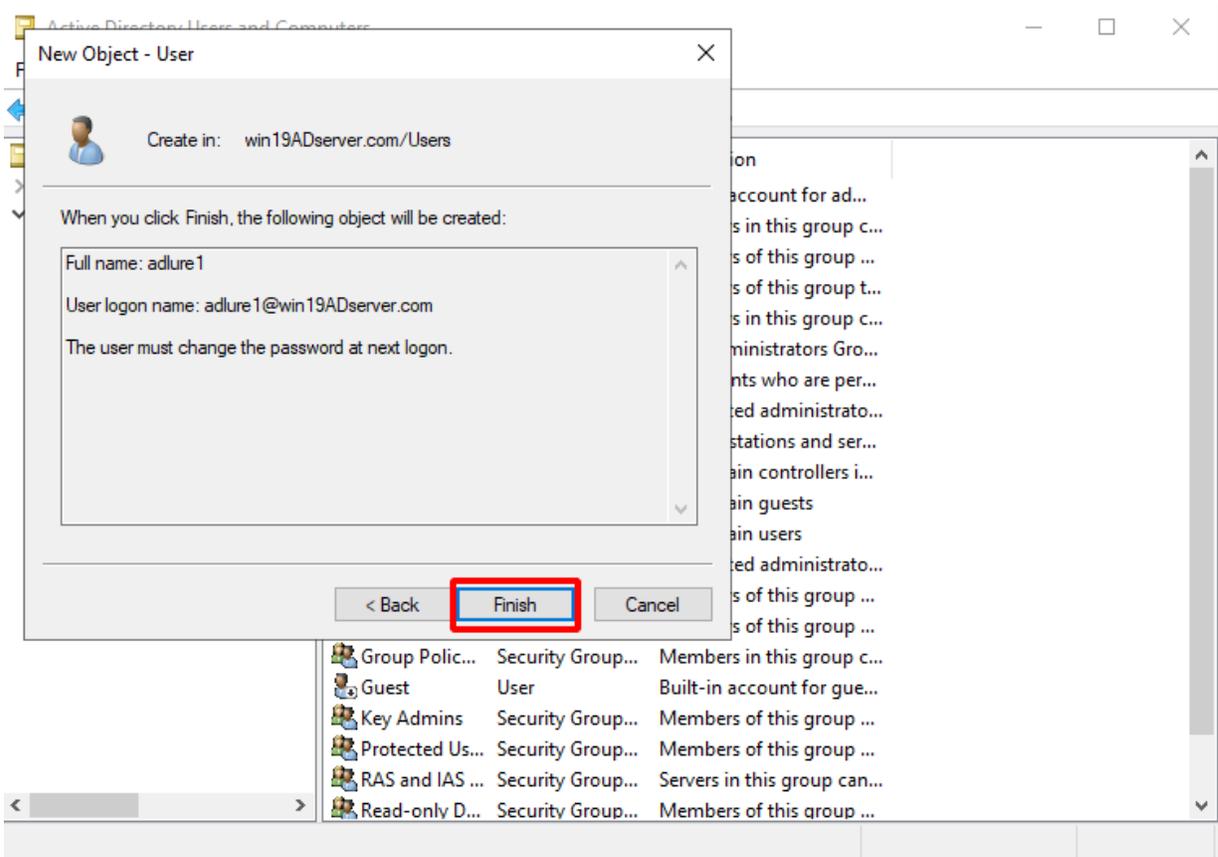


e. Enter the AD user password and click Next.

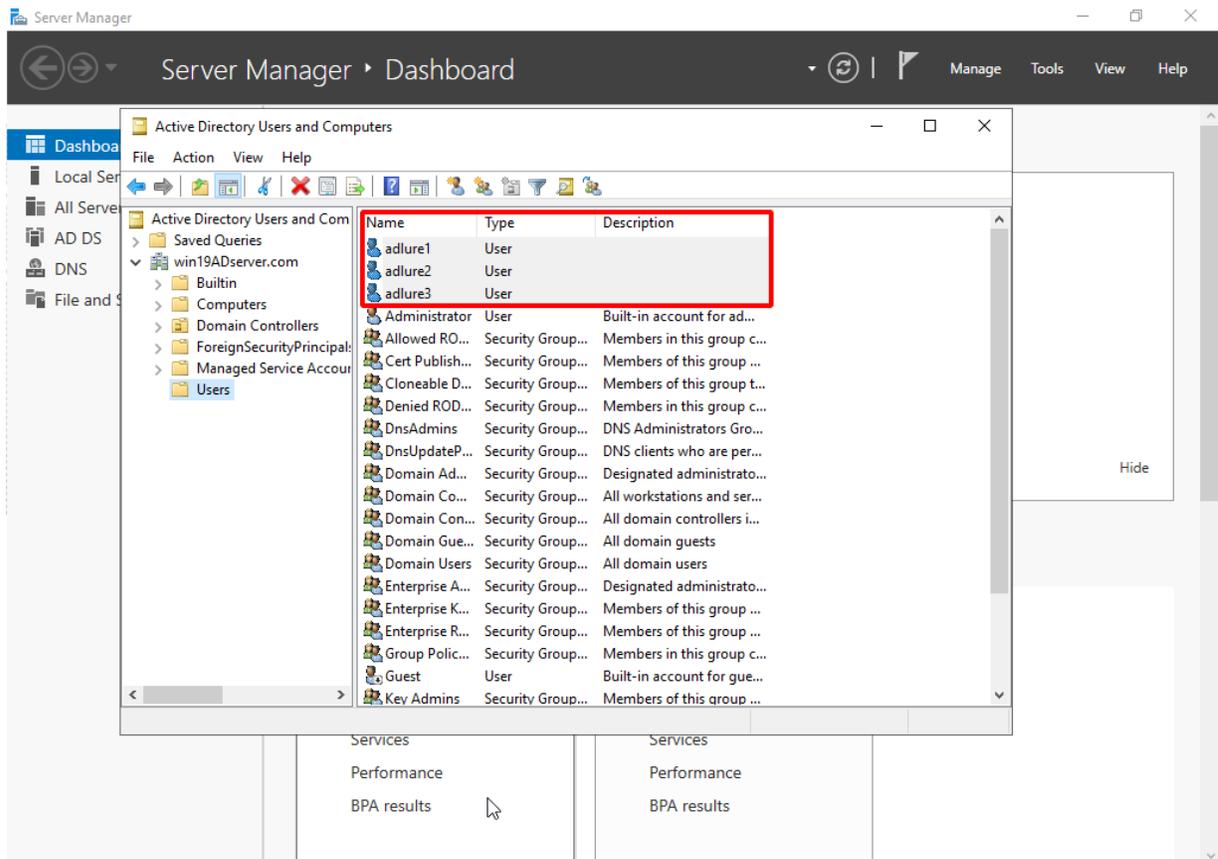
- Disable *User must change password at next logon*.
- Enable *User cannot change password* and *Password never expires*.



f. Click *Finish*.



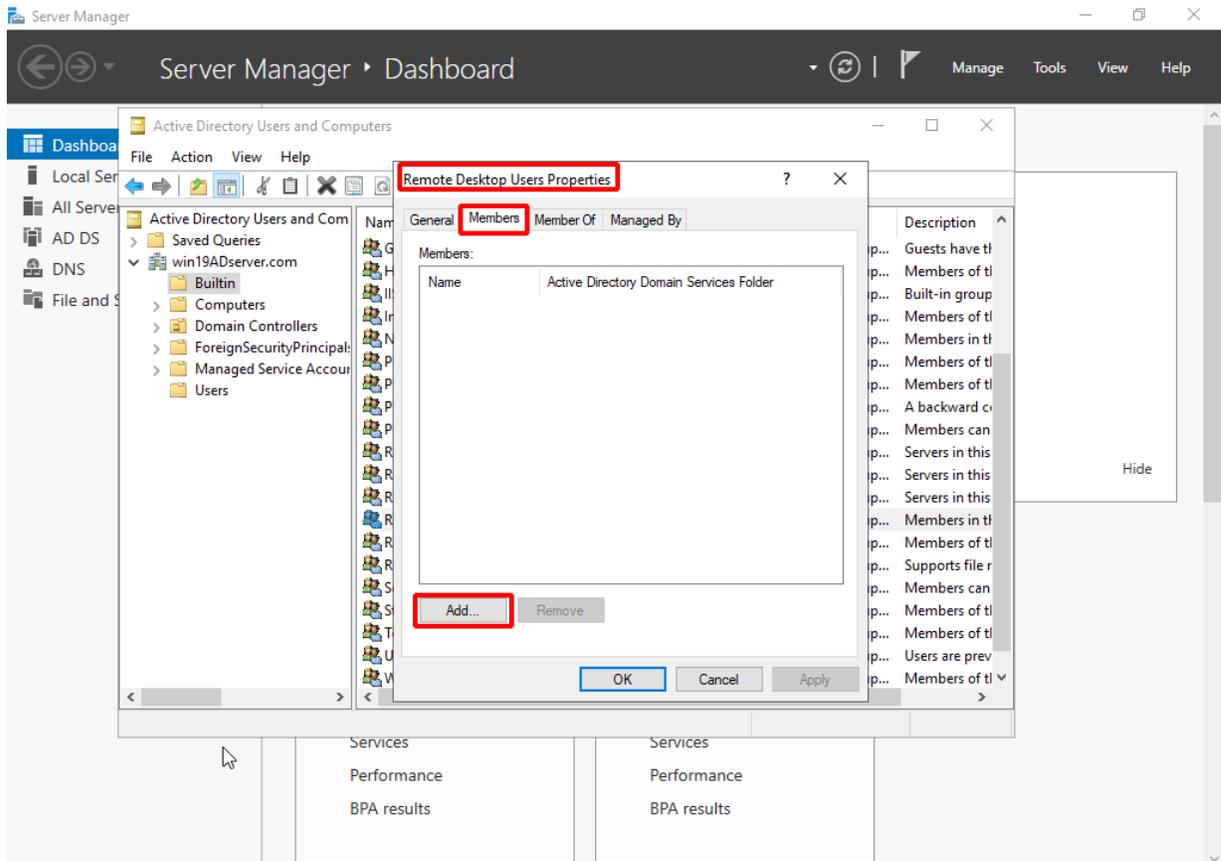
g. The AD Users are added.



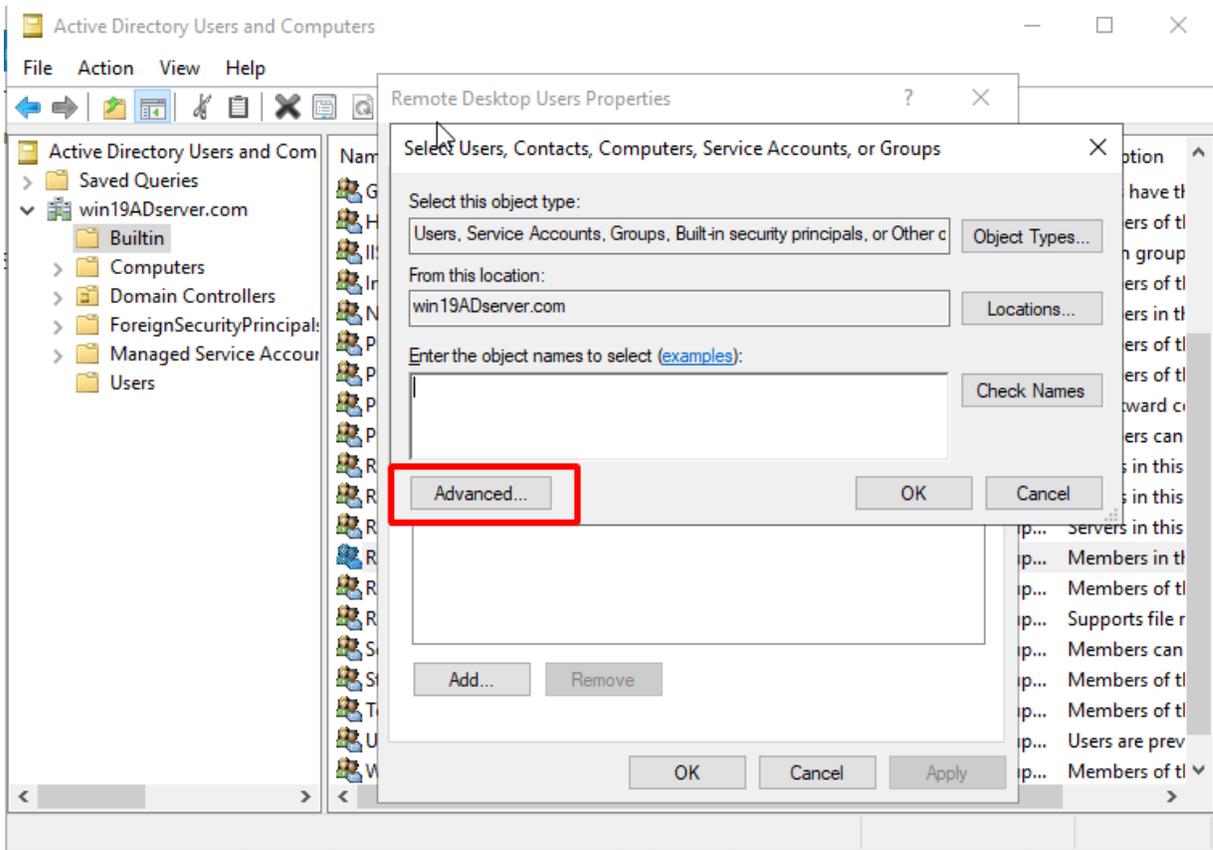
2. Add the new AD users to the Remote Desk User group.

- a. In the Server Manager, go to *Tools > Active Directory Users and Computers > {domain name} > Builtin > Remote Desk User group.*

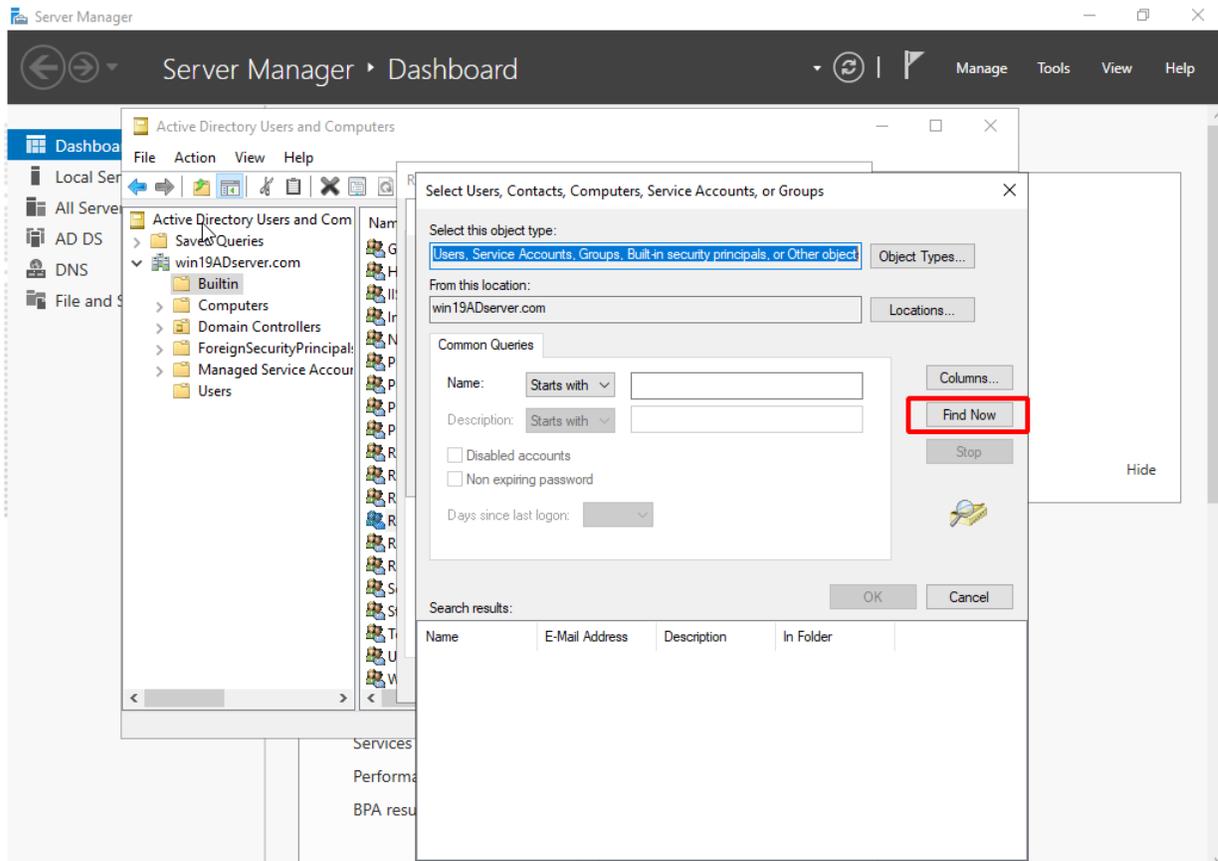
- b. Double-click *Remote Desk User group*, click the *Members* tab and click *Add*.



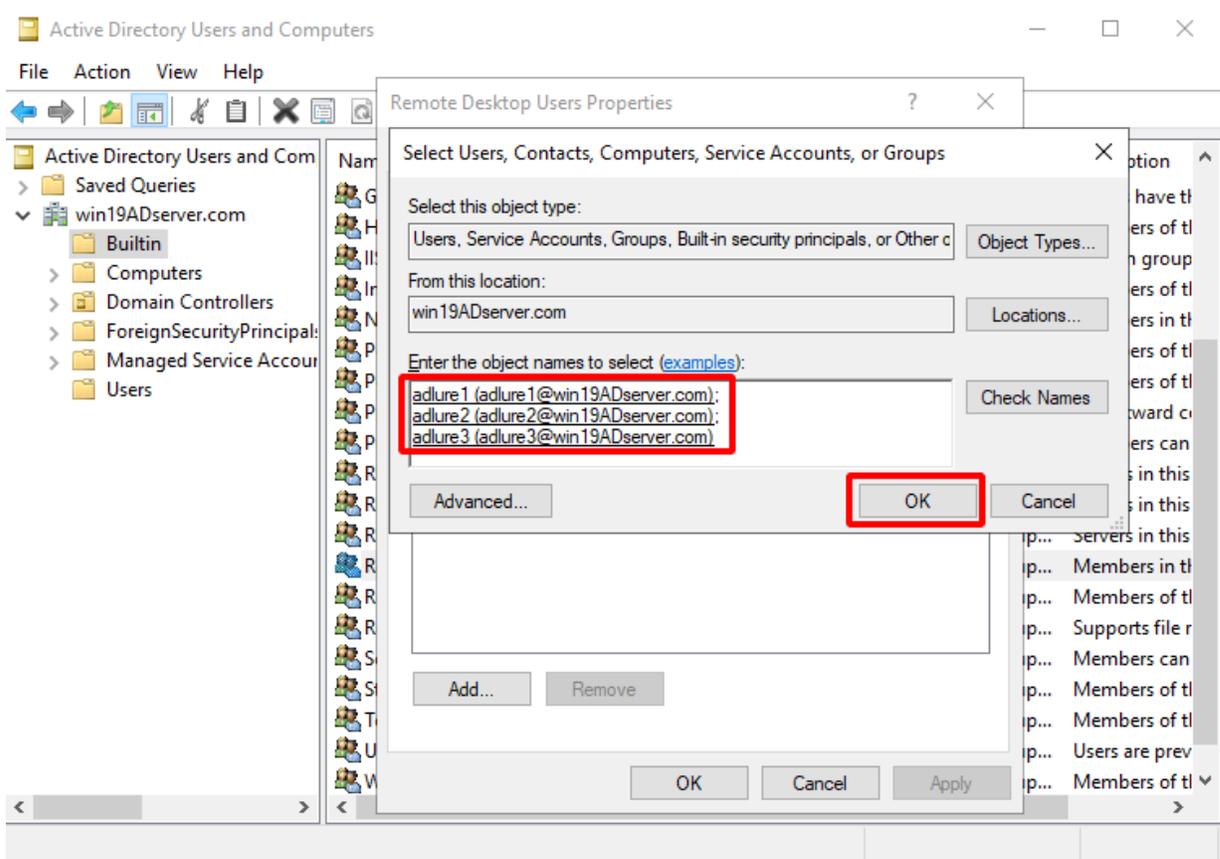
c. Click *Advanced*.



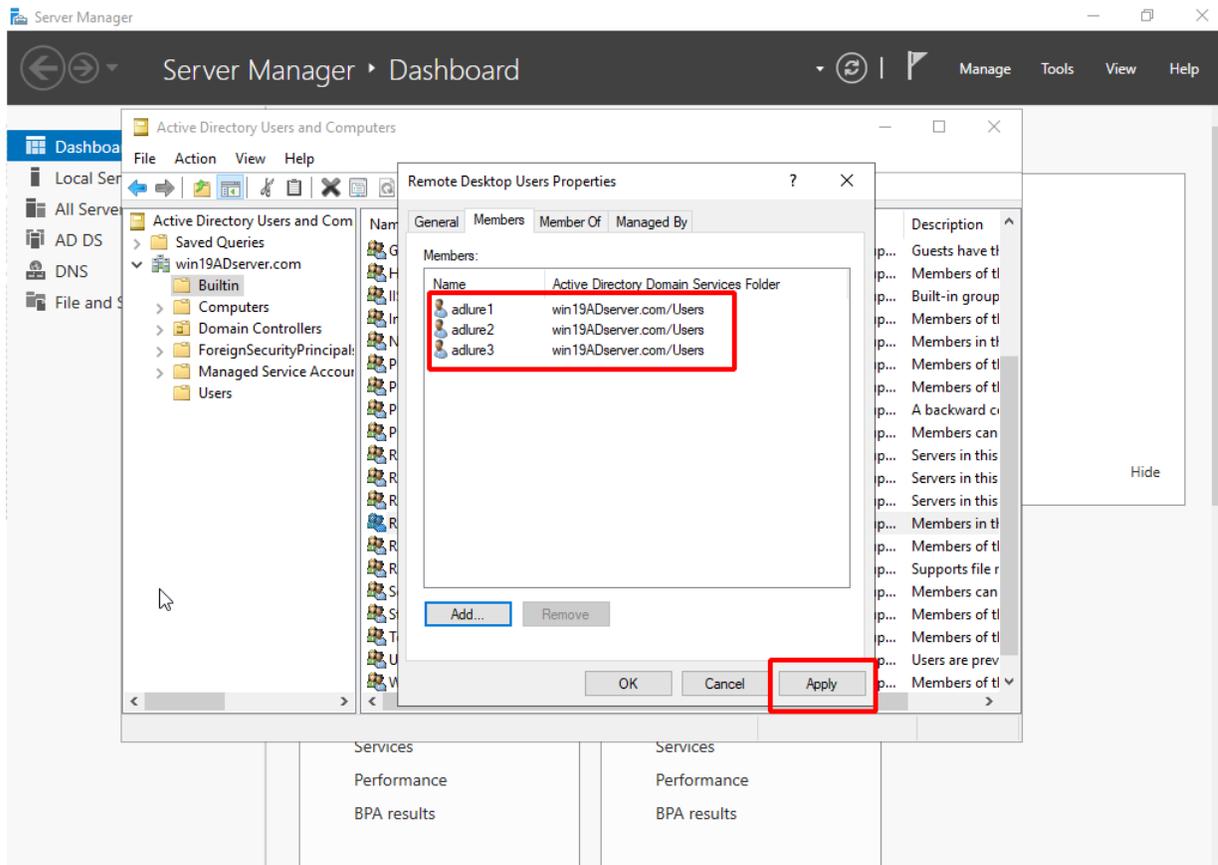
- d. Click *Find Now* and choose the AD users you would like to add to the Remote Desk User group.



e. Click OK.

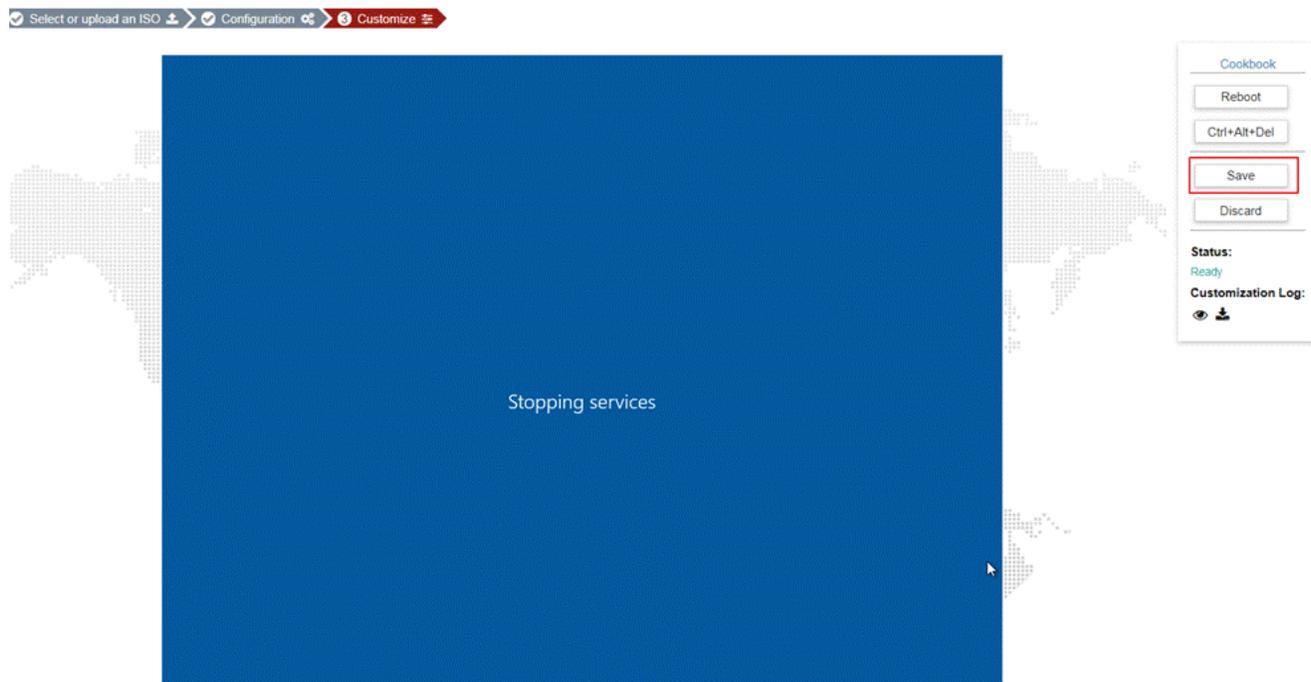


- f. The AD users are added to the Remote Desk User group. Click *Apply*.



8. Save the customized image

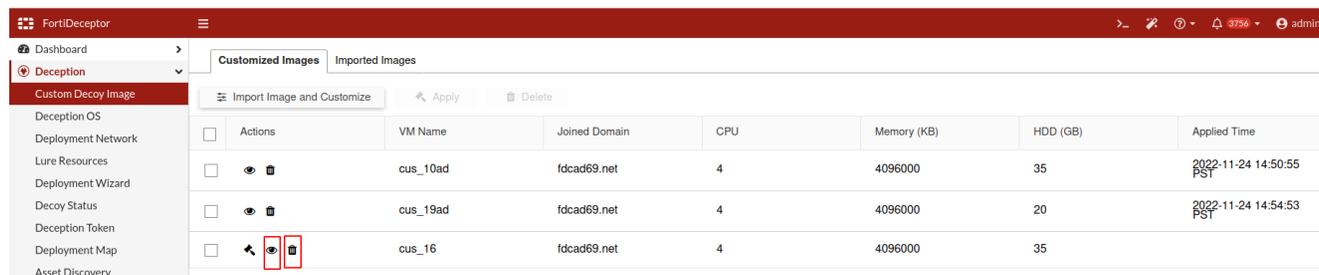
After Windows shuts down successfully, click *Save* to save this image. It may take several minutes to save the entire image. After it's finished, the page will display the *Customized Images* table with a new entry.



The GUI may not display a *Power* option if Windows Server is connected to a domain. To shut down the device, open a Command Prompt as Administrator and run `shutdown /s /t 1 /f`.

9. 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.



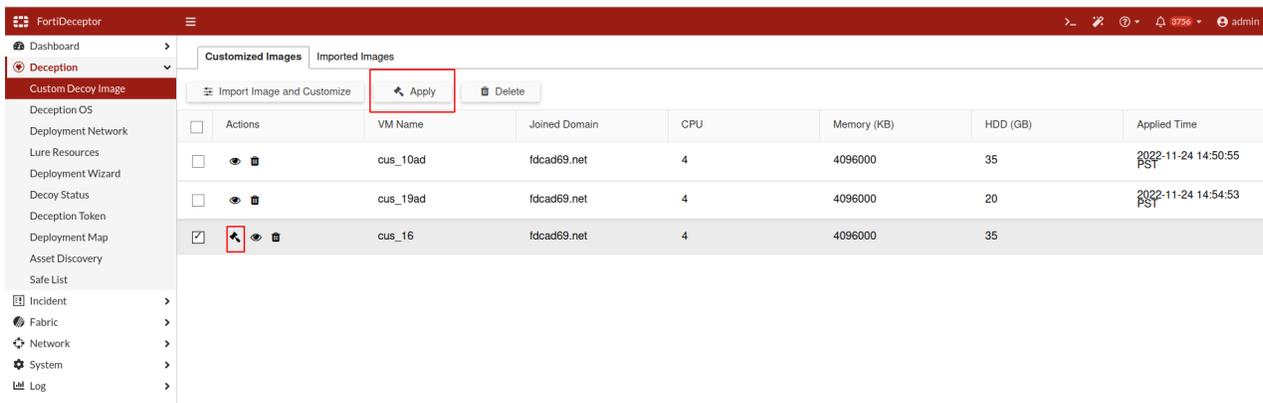
Use the custom Windows image

10. Use the custom Windows image

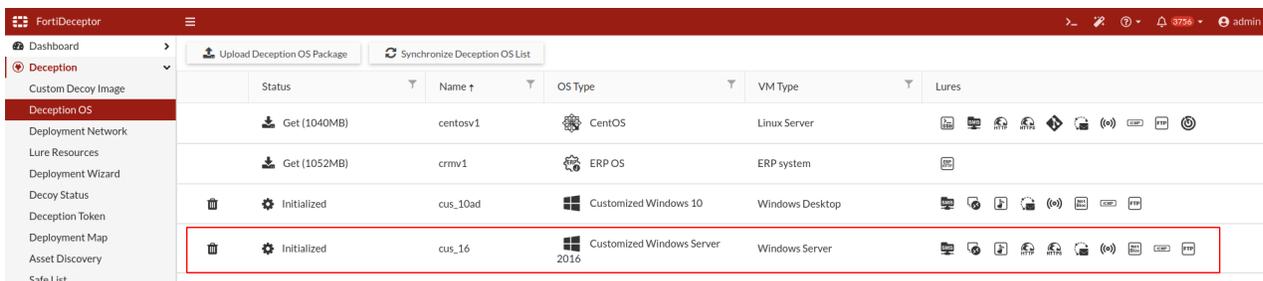
Apply the custom images

To apply a custom image:

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



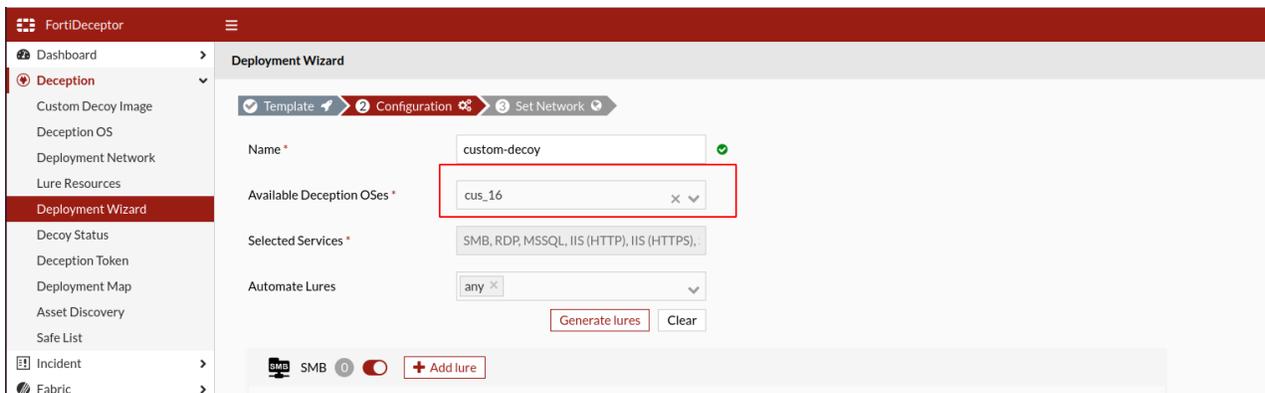
2. Choose a custom image and click *Apply*". The applied image is displayed in the *Deception OS* table. It may take several minutes for the image to appear in the table.



Deploy decoys with custom generic Image

To deploy decoys with a custom generic 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. Select the RDP and SMB domain users will access.

For normal users:

RDP (2)

+ Add Lure

Username	Password
loretta	
lawrence	

SMB (2)

+ Add Lure

Username	Password	Sharename
rhonda		
maurice		

For domain users:



As of version 6.1, the GUI does not include toggles for *Allow domain users to access SMB/RDP* and *Anti-Deception Detection*. Both settings are enabled by default. These settings remain enabled by default even if you enter an AD account in the format `adlure@exampledomain.com`.

SMB 5 + Add lure

ⓘ If choosing to join a domain, please provide real AD username and password as lure.
 ⓘ When tags related to directory clone lure resources are selected, the corresponding cloned information for files and folders will be applied to the share folders listed below as lures. [Click here for details](#)

Username	Password	Sharename	
[REDACTED]	[REDACTED]	[REDACTED]	× Delete
[REDACTED]	[REDACTED]	[REDACTED]	× Delete
[REDACTED]	[REDACTED]	[REDACTED]	× Delete
[REDACTED]	[REDACTED]	[REDACTED]	× Delete
[REDACTED]	[REDACTED]	[REDACTED]	× Delete

SMB

Allow domain user to access SMB Yes
 Anti Deception Detection Yes

Username	Password	Sharename
[REDACTED]	[REDACTED]	[REDACTED]

Deploy decoys with a customized SQL Server image

To deploy decoys with a custom SQL Server 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 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.

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

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
```

```
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\ADMINI~1>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 navigation menu with options like Dashboard, Deception, Incident, Analysis, Campaign, Attack Map, MITRE ICS, Fabric, Network, System, and Log. The main area displays an incident table with columns for ID, Severity, Protocol, Last Activity, Type, Attacker IP, Attacker User, and Attacker. One incident is highlighted with a red box around the 'MS-SQL-S' protocol. Below the table, a 'Timeline' view shows a sequence of events: 1. An alert at 2022-12-14 10:35:11 PST with details for Attacker User (ricky), Attacker IP (10.11.4.24), Attacker Port (1032), and MITRE ICS Techniques (T0811, T0812, T0859, T0882). 2. An 'Open Port' event at the same time, showing traffic from 10.11.4.24:1032 to 10.11.4.121:1433, with a download of a 6.8 KB PCAP file. 3. An 'SQL Server Logon' event 2 seconds later, indicating a successful login for user 'ricky' with password 'Z2%V1%J1'. 4. A final event 2 seconds later.

## Deploy decoys with a custom IIS (HTTP/HTTPS) image

To deploy decoys with a custom IIS (HTTP/HTTPS) image:

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

The screenshot shows two configuration sections for IIS. The top section is for IIS (HTTP) (1), with a listening port of 80 and an 'Add User' button. The bottom section is for IIS (HTTPS) (1), with a listening port of 443, an 'Upload certificate/key zip file' button, and an 'Add User' button. A note below the HTTPS section states: 'The .zip file should contain both SSL certificate and key files.'

## Deploy decoys with a custom NBNSspoofer image

To deploy decoys with a custom NBNSspoofer image:

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

The screenshot shows the configuration for NBNSspoofer (0). It includes fields for Username (scott), Password, Domain (optional), Hostname, and Interval (3600 seconds). A note below the Hostname field states: 'Please provide a fake hostname for NBNS request.'



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

## Deploy decoys with a custom SWIFT Lite2 image

To deploy decoys with a custom SWIFT Lite2 image:

1. Go to *Deception > Deployment Wizard*.
2. Click *SWIFT Lite2 service*.

3. Upload the *MT Files*.



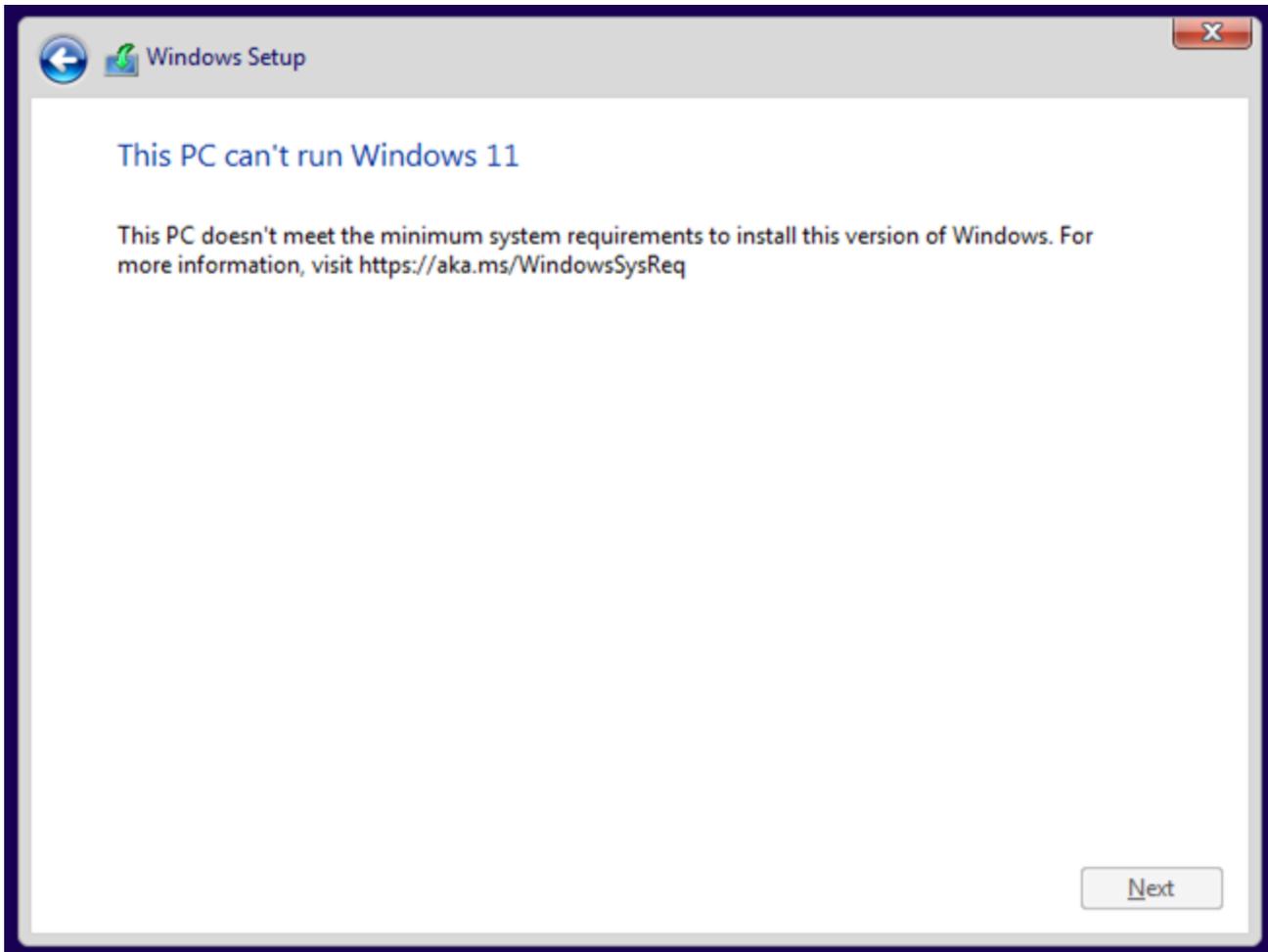
## Troubleshooting

### The PC does not meet the Windows 11 minimum system requirements

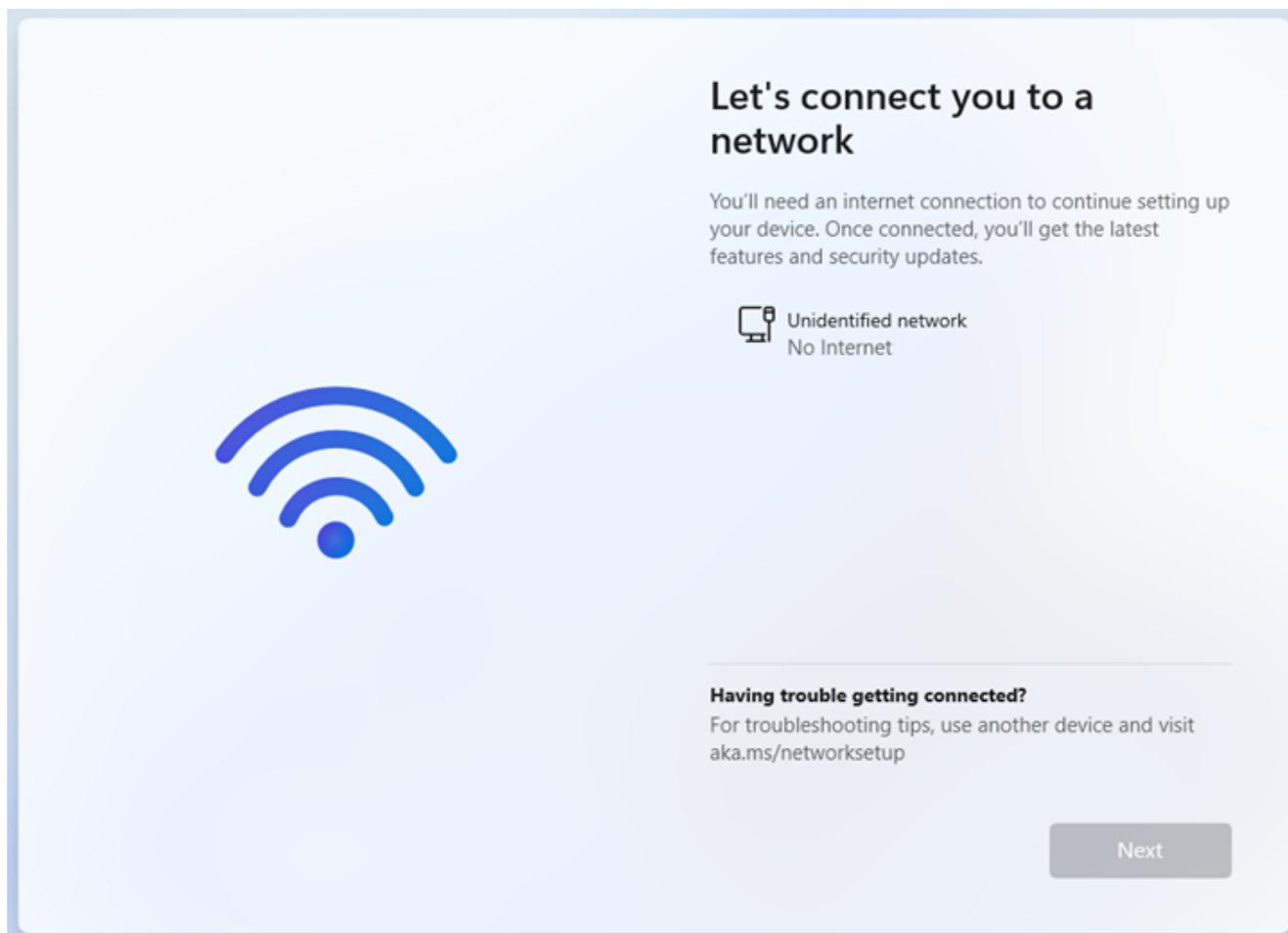
**Supported Windows OS versions:**

- Windows 11(64 bits) version 23H2 is supported
- Windows 11 (64 bits) version 24H2 is not supported

The OS Windows 11(64 bits) version 23H2 deception OS is similar to Windows 10 services. However, the GUI restricts the CPU Cores, Memory and Storage. Since Windows 11 (64 bits) requires more resources, you may see the following messages:

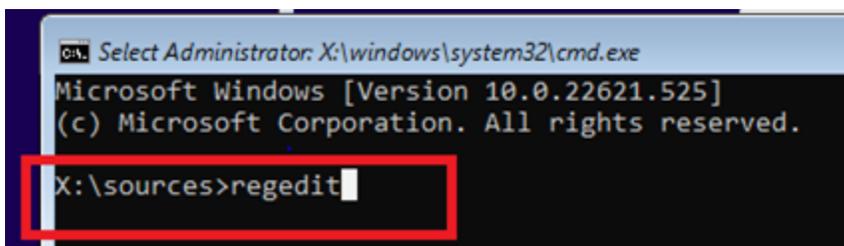


You may also be blocked on the following OOB page.

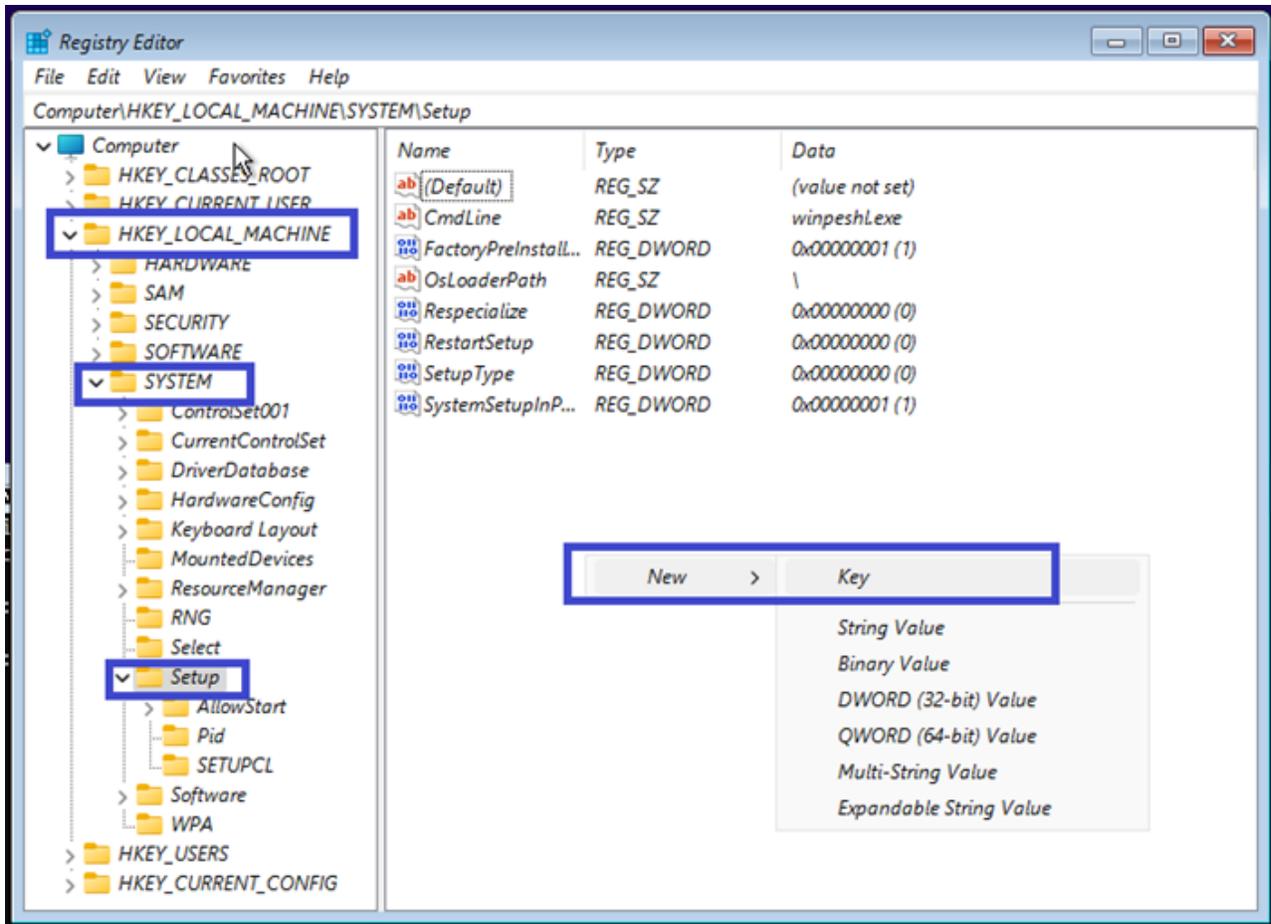


#### To run Set Bypass TPM and SecureBoot check:

1. Boot off of your Windows 11 install disk.
2. Press *SHIFT + F10* to launch the command prompt. If this does not work, try *SHIFT + F10 + FN*.
3. Enter `regedit` and press *Enter*.

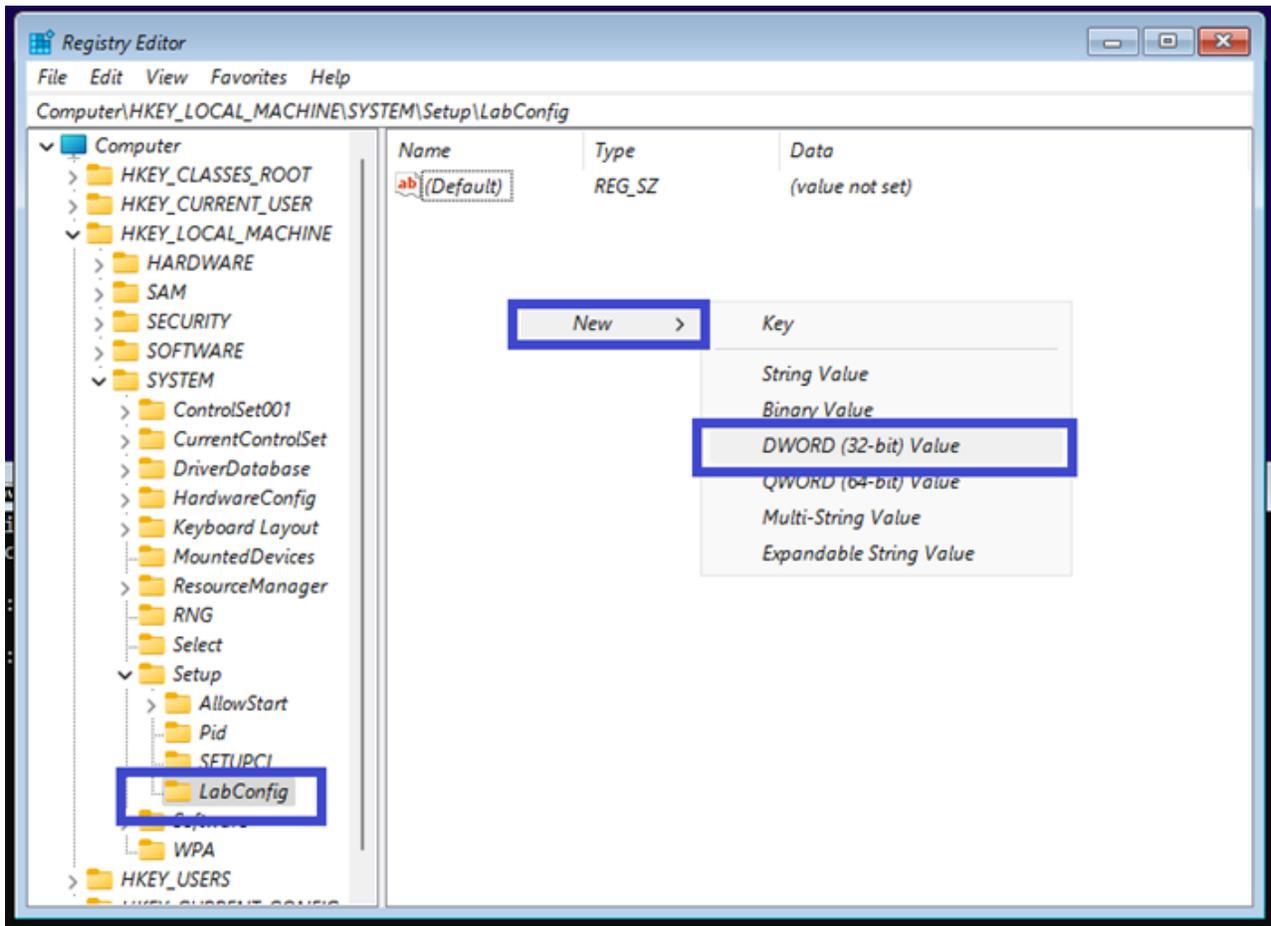


4. Go to `HKEY_LOCAL_MACHINE > SYSTEM > Setup`. Right-click the folder to add a new key folder called LabConfig.

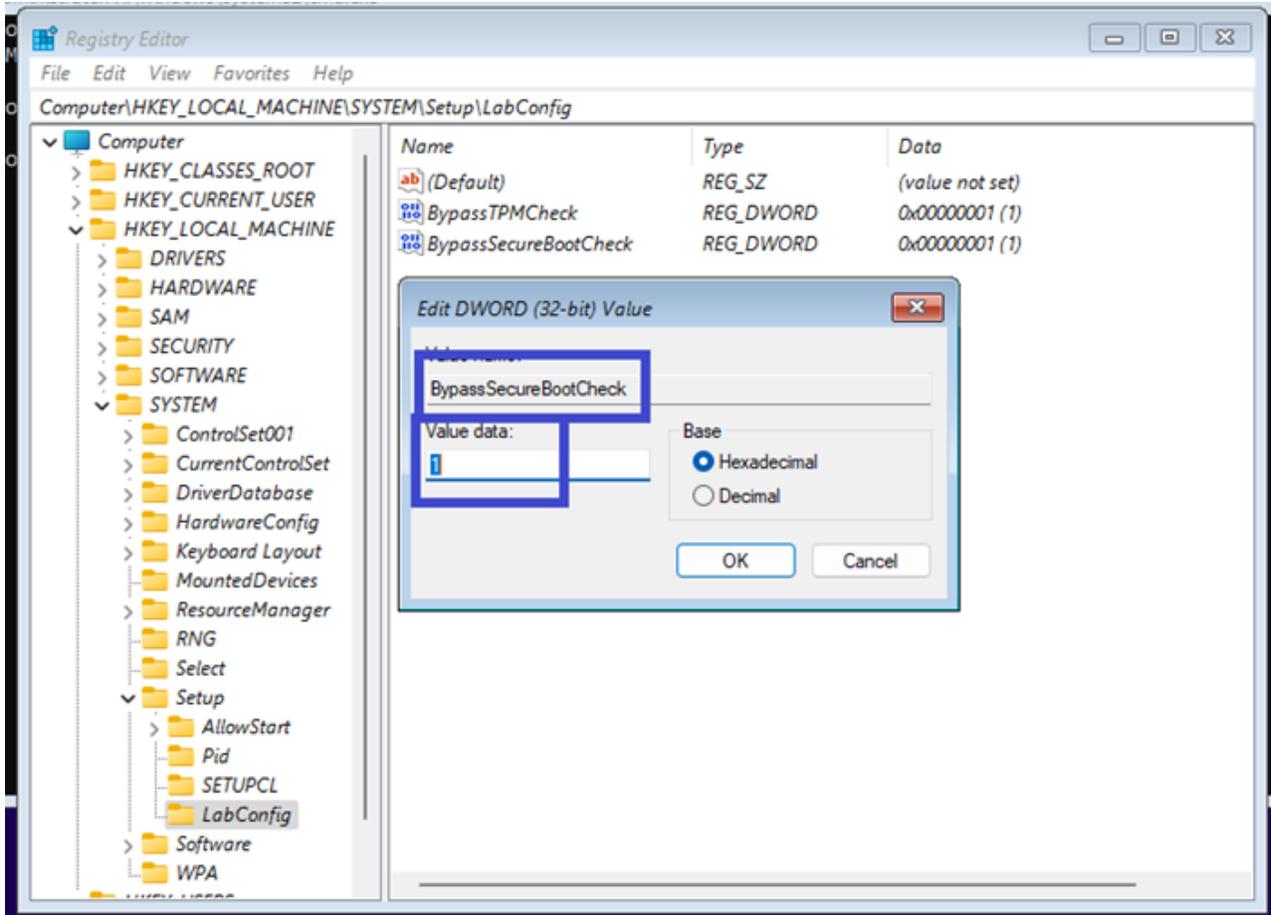


5. Add new value named BypassTPMCheck.

6. In the *LabConfig* folder, type *REG\_DWORD*", set it to 1.



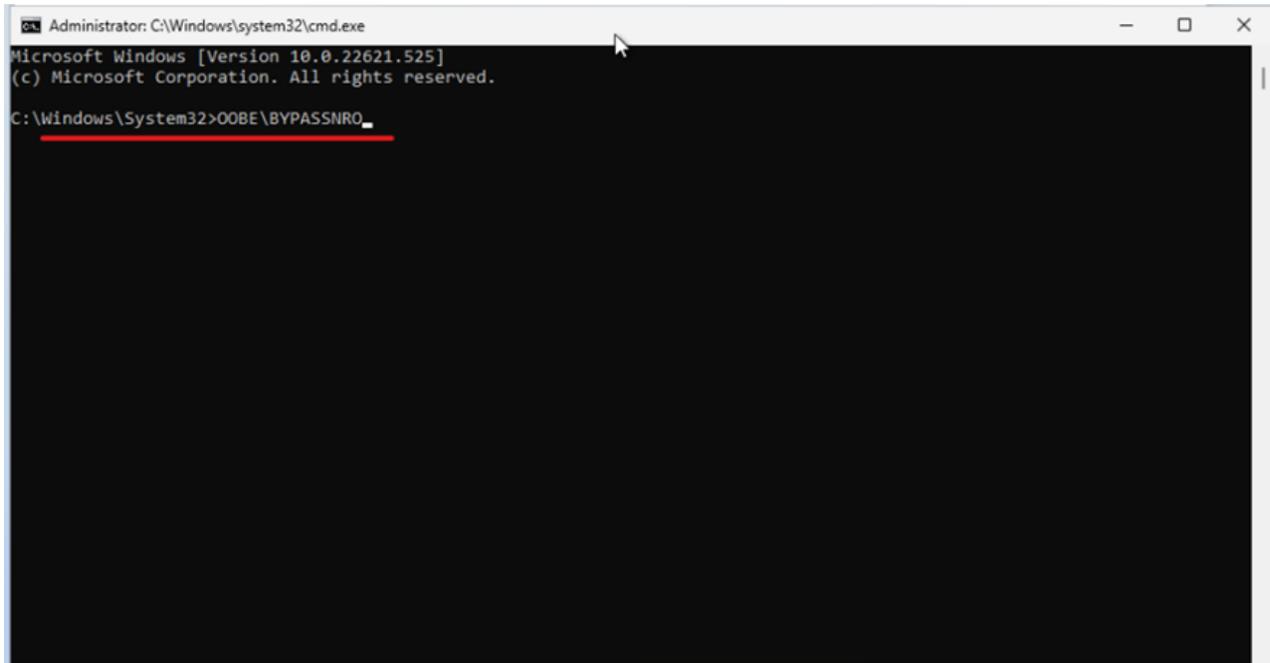
7. In the *LabConfig* folder, add a new value called *BypassSecureBootCheck* then type *REG\_DWORD*, and set it to 1.



You can set the RAM larger than or equal to 4G during configuration. However, if the RAM is less than 4G, you can add another new value called `BypassRAMCheck` to the `LabConfig` folder, and type `REG_DWORD`, and set to 1.

**To set the bypass network setup during OOB:**

1. Press *SHIFT + F10* or *SHIFT +Fn+ F10* to launch the command prompt when asked to setup network
2. Enter `OOBE\BYPASSNRO` and press *Enter*.



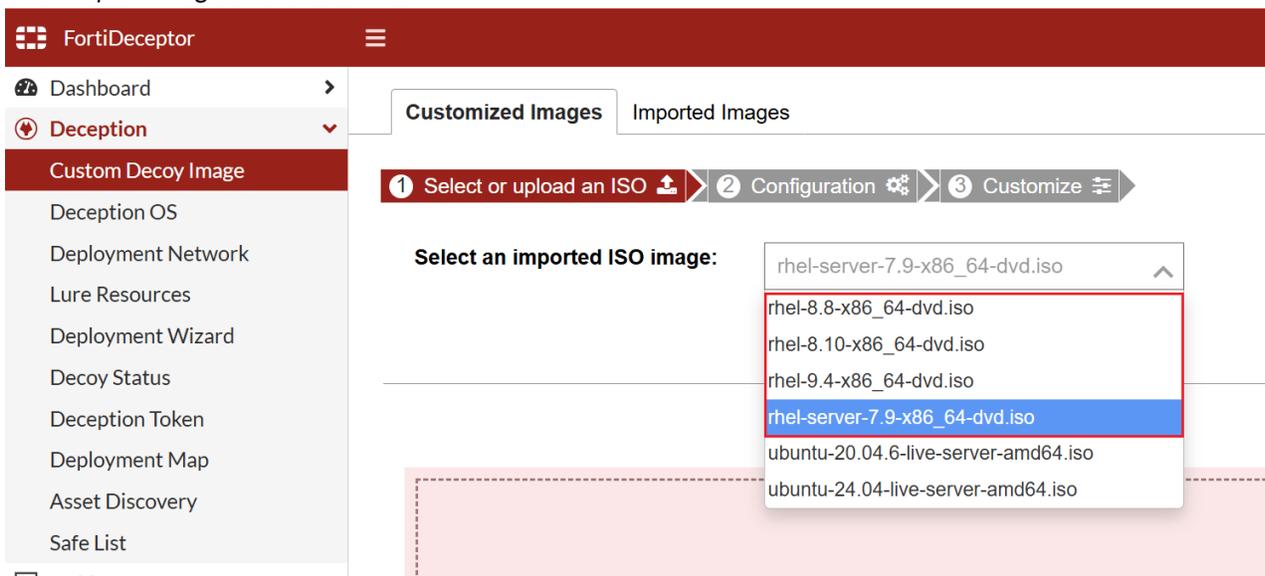
3. Click the *View* icon to review the customization log for the customized image. Click the *Delete* icon to remove the customized image.

# Redhat OS

## 1. Initialize the OS instance

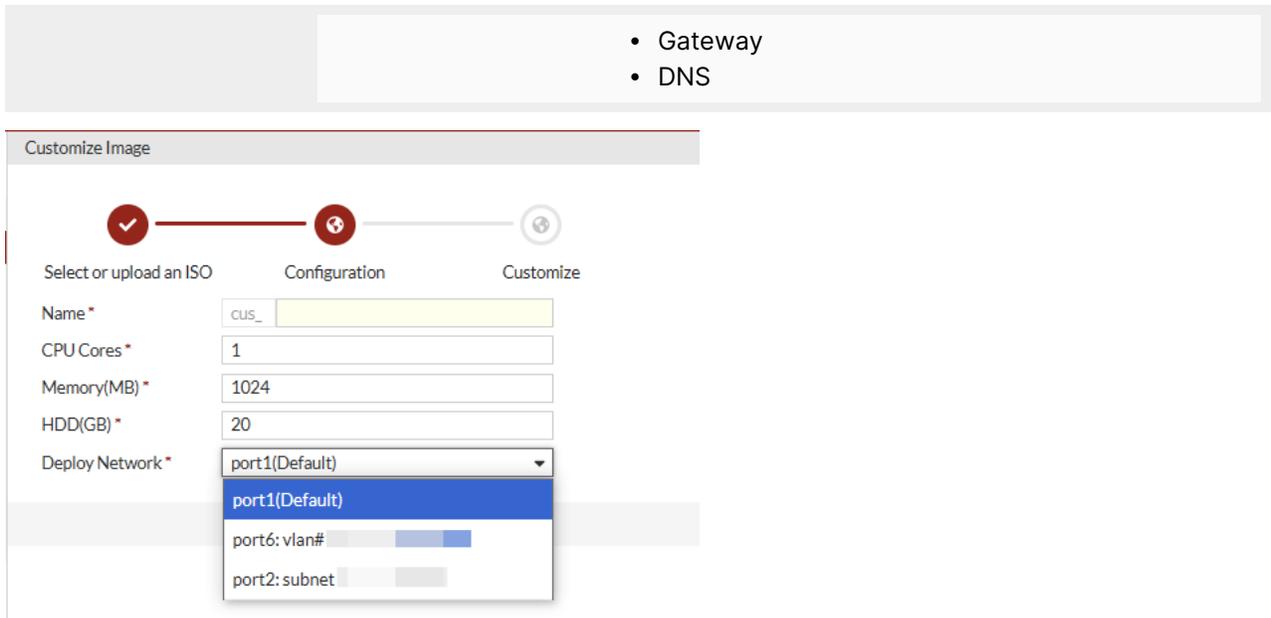
To initialize the OS instance:

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

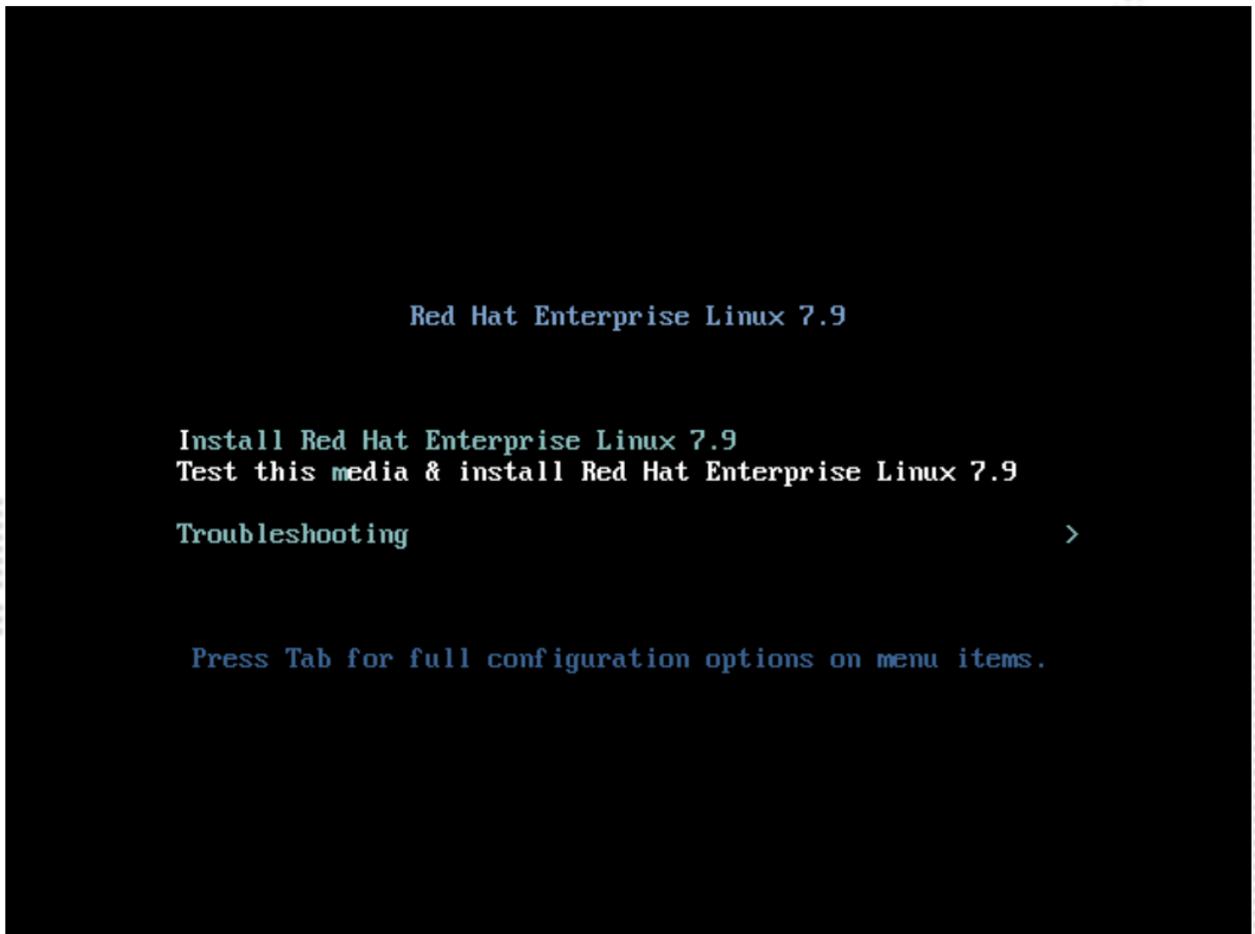


3. Choose an ISO image and click *Next*.
4. Configure the following settings and click *Next*.

|                       |                                                                                                                            |                                                                                                                                                                                                        |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>           | Characters in range "A-Za-z0-9-_", less than 48 characters.                                                                |                                                                                                                                                                                                        |
| <b>CPU Cores</b>      | 1-4                                                                                                                        |                                                                                                                                                                                                        |
| <b>Memory</b>         | 1024- 8192 MB.                                                                                                             |                                                                                                                                                                                                        |
| <b>Storage</b>        | <ul style="list-style-type: none"> <li>• Minimum: 20 GB</li> <li>• Maximum: Up to the supported hard drive size</li> </ul> |                                                                                                                                                                                                        |
| <b>Deploy Network</b> | <b>Port1</b>                                                                                                               | Default                                                                                                                                                                                                |
|                       | <b>PortX</b>                                                                                                               | Select the deployment network.<br>Ensure specified IP is not already in use and the following settings align with the PortX configuration: <ul style="list-style-type: none"> <li>• IP/Mask</li> </ul> |



5. In the VNC window, press Tab for full configuration options on menu items.



6. Enable the test-based installer mode by adding `inst.text text` at the end of the `vmlinux` command.



While VNC windows supports the default graphical mode of Red Hat Enterprise Linux (RHEL) installations, the test-based installer mode is recommended for faster and minimal setup.

```
Red Hat Enterprise Linux 7.9

Install Red Hat Enterprise Linux 7.9
Test this media & install Red Hat Enterprise Linux 7.9

Troubleshooting >

> vmlinux initrd=initrd.img inst.stage2=hd:LABEL=RHEL-7.9\x20Server.x86_64 rd.
live.check quiet inst.text text_
```

## 7. Set the root password.

```
Installation
1) [x] Language settings 2) [x] Time settings
 (English (United States)) (America/New_York timezone)
3) [!] Installation source 4) [!] Software selection
 (Processing...) (Processing...)
5) [!] Installation Destination 6) [x] Kdump
 (Processing...) (Kdump is enabled)
7) [!] Network configuration 8) [!] Root password
 (Not connected) (Root account is disabled.)
9) [!] User creation
 (No user will be created)

Please make a selection from the above ['b' to begin installation, 'q' to quit,
'r' to refresh]: 8
=====
Root password

Please select new root password. You will have to type it twice.

Password:
Password (confirm):
=====
=====
Question

The password you have provided is weak: The password fails the dictionary check
- it is based on a dictionary word
Would you like to use it anyway?

Please respond 'yes' or 'no': yes_
```

8. Select the installation destination.

```
(no user will be created)
Please make your choice from above ['q' to quit | 'b' to begin installation |
'r' to refresh]: 5
=====
=====
Probing storage...
Installation Destination

[] 1) QEMU HARDDISK: 40 GiB (sda)

1 disk selected; 40 GiB capacity; 40 GiB free ...

Please make your choice from above ['q' to quit | 'c' to continue |
'r' to refresh]: c
=====
=====
Autopartitioning Options

[] 1) Replace Existing Linux system(s)

[] 2) Use All Space

[] 3) Use Free Space

Installation requires partitioning of your hard drive. Select what space to use
for the install target.

Please make your choice from above ['q' to quit | 'c' to continue |
'r' to refresh]: c
=====
=====
```



Standard Partition is recommended.

```
Partition Scheme Options
[] 1) Standard Partition
[] 2) Btrfs
[] 3) LVM
[] 4) LVM Thin Provisioning
Select a partition scheme configuration.

Please make your choice from above ['q' to quit ; 'c' to continue ;
'r' to refresh]: 1
=====
Partition Scheme Options
[] 1) Standard Partition
[] 2) Btrfs
[] 3) LVM
[] 4) LVM Thin Provisioning
Select a partition scheme configuration.

Please make your choice from above ['q' to quit ; 'c' to continue ;
'r' to refresh]: c
```

## 9. Set the timezone.

```
Installation

1) [x] Language settings 2) [x] Time settings
 (English (United States)) (America/Bahia timezone)
3) [x] Installation source 4) [x] Software selection
 (Local media) (Minimal Install)
5) [x] Installation Destination 6) [x] Kdump
 (Automatic partitioning (Kdump is enabled)
 selected)
7) [] Network configuration 8) [x] Root password
 (Not connected) (Password is set.)
9) [] User creation
 (No user will be created)

Please make your choice from above ['q' to quit ; 'b' to begin installation ;
'r' to refresh]: b
=====
=====
Progress
Setting up the installation environment
.
Creating disklabel on /dev/sda
.
Creating swap on /dev/sda2
.
Creating xfs on /dev/sda3
.
Creating xfs on /dev/sda1
.
Running pre-installation scripts
.
Starting package installation process
```

```
28) Bogota 79) La_Paz 128) Scoresbysund
29) Boise 80) Lima 129) Sitka
30) Cambridge_Bay 81) Los_Angeles 130) St_Barthelemy
31) Campo_Grande 82) Lower_Princes 131) St_Johns
32) Cancun 83) Maceio 132) St_Kitts
33) Caracas 84) Managua 133) St_Lucia
34) Cayenne 85) Manaus 134) St_Thomas
35) Cayman 86) Marigot 135) St_Vincent
36) Chicago 87) Martinique 136) Swift_Current
37) Chihuahua 88) Matamoros 137) Tegucigalpa
38) Costa_Rica 89) Mazatlan 138) Thule
39) Creston 90) Menominee 139) Thunder_Bay
40) Cuiaba 91) Merida 140) Tijuana
41) Curacao 92) Metlakatla 141) Toronto
42) Danmarkshavn 93) Mexico_City 142) Tortola
Press ENTER to continue
43) Dawson 94) Miquelon 143) Vancouver
44) Dawson_Creek 95) Moncton 144) Whitehorse
45) Denver 96) Monterrey 145) Winnipeg
46) Detroit 97) Montevideo 146) Yakutat
47) Dominica 98) Montserrat 147) Yellowknife
48) Edmonton 99) Nassau
49) Eirunepe
50) El_Salvador
Please select the timezone.
Use numbers or type names directly [b to region list, q to quit]: 21
=====
=====
```

10. Enter 'b' to begin the installation.

```

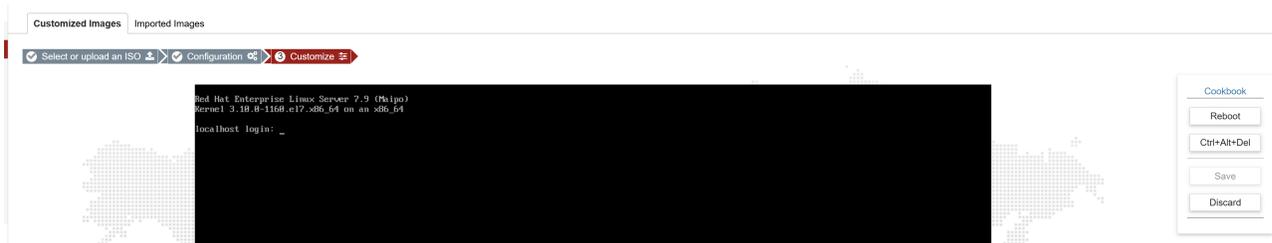
Installation

1) [x] Language settings 2) [x] Time settings
 (English (United States)) (America/Bahia timezone)
3) [x] Installation source 4) [x] Software selection
 (Local media) (Minimal Install)
5) [x] Installation Destination 6) [x] Kdump
 (Automatic partitioning (Kdump is enabled)
 selected)
7) [] Network configuration 8) [x] Root password
 (Not connected) (Password is set.)
9) [] User creation
 (No user will be created)

Please make your choice from above ['q' to quit ; 'b' to begin installation ;
'r' to refresh]: b
=====
=====
Progress
Setting up the installation environment
.
Creating disklabel on /dev/sda
.
Creating swap on /dev/sda2
.
Creating xfs on /dev/sda3
.
Creating xfs on /dev/sda1
.
Running pre-installation scripts
.
Starting package installation process

```

11. The custom system will be reboot and show the login terminal after the installation is complete.



## 2. Mount the device on your system

### To mount a device on the system:

1. Log in with root.
2. Run `mount /dev/sr1` to directory you prefer. (eg, `/tmp/cus` )



To re-customize Linux distributions (e.g., Red Hat, Ubuntu, Debian), the customization scripts are stored on the system drive `/dev/sr0`. Mount `/dev/sr0` to the newly created directory before starting the re-customization process.

3. 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 ~]# _
```

## 3. 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

- 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. Register the server

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

### To register the server:

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

```

[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

```

## 5. 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

- Make sure you have registered your server with [redhat.com](https://redhat.com).
- 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.e17 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.e17.noarch.rpm: Header U3 RSA/SHA256 Signature, key ID fd431d51: NOKEY
Public key for python-chardet-2.2.1-3.e17.noarch.rpm is not installed
(1/3): python-chardet-2.2.1-3.e17.noarch.rpm | 227 kB 00:00:02
(2/3): python-kitchen-1.1.1-5.e17.noarch.rpm | 266 kB 00:00:02
(3/3): yum-utils-1.1.31-54.e17_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.e17.noarch 1/3
 Installing : python-kitchen-1.1.1-5.e17.noarch 2/3
 Installing : yum-utils-1.1.31-54.e17_8.noarch 3/3
 Verifying : python-kitchen-1.1.1-5.e17.noarch 1/3
 Verifying : yum-utils-1.1.31-54.e17_8.noarch 2/3
 Verifying : python-chardet-2.2.1-3.e17.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.e17_8

Dependency Installed:
 python-chardet.noarch 0:2.2.1-3.e17 python-kitchen.noarch 0:1.1.1-5.e17

Complete!
[root@localhost cus]#

```

## 6. 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-aaALZ# systemd-private-13184e178ea04940a31e6a0508b37848-chromiumd.service-0x2f1f1-gdm.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.e17
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:

```

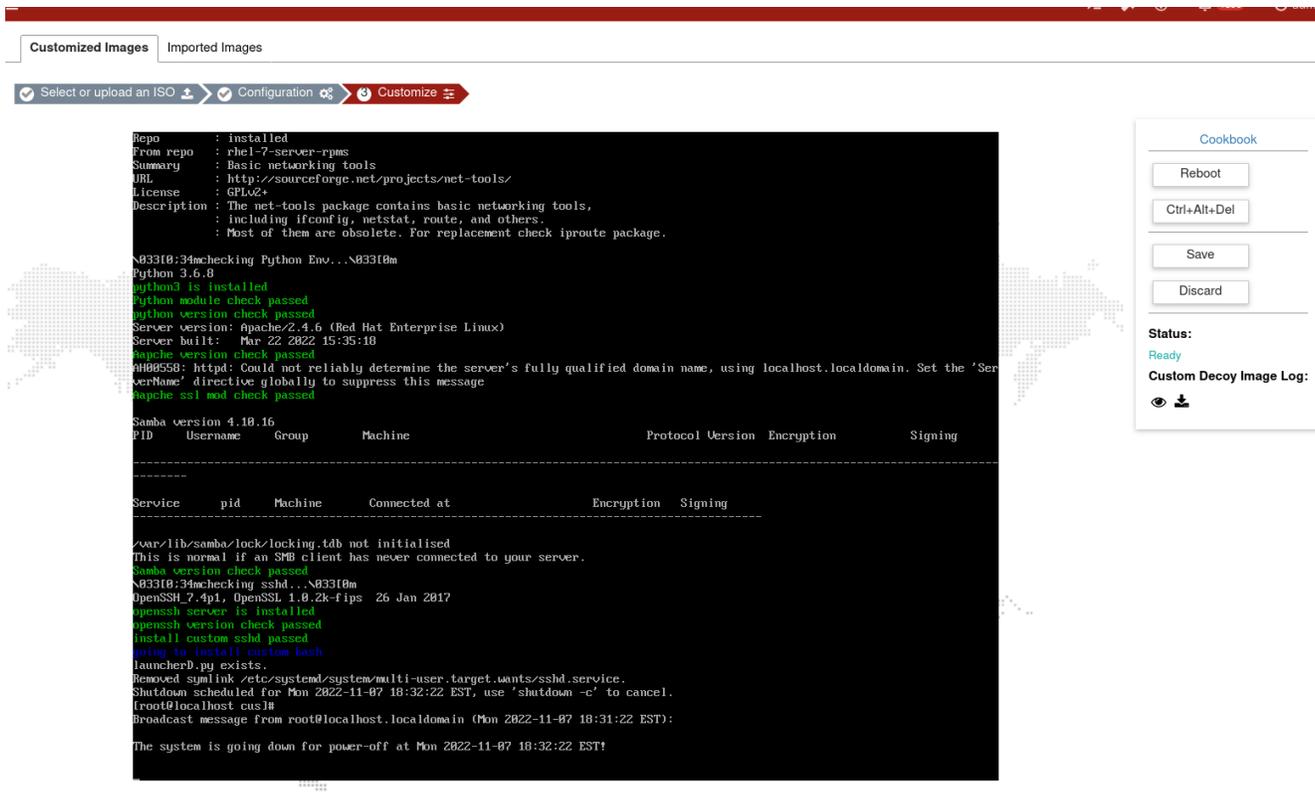
vmmgfx.ko
Number of similar warning messages suppressed: 18.
Rerun with -v to see them.
'vmmgfx.ko' -> '/usr/bin/vmmgfx.ko'
[root@localhost ~]#

```

## 7. 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



## 8. 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.

## 9. Review the result

### To review the result:

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

| 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.

## 10. Use the custom Redhat image

### 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       |                         |

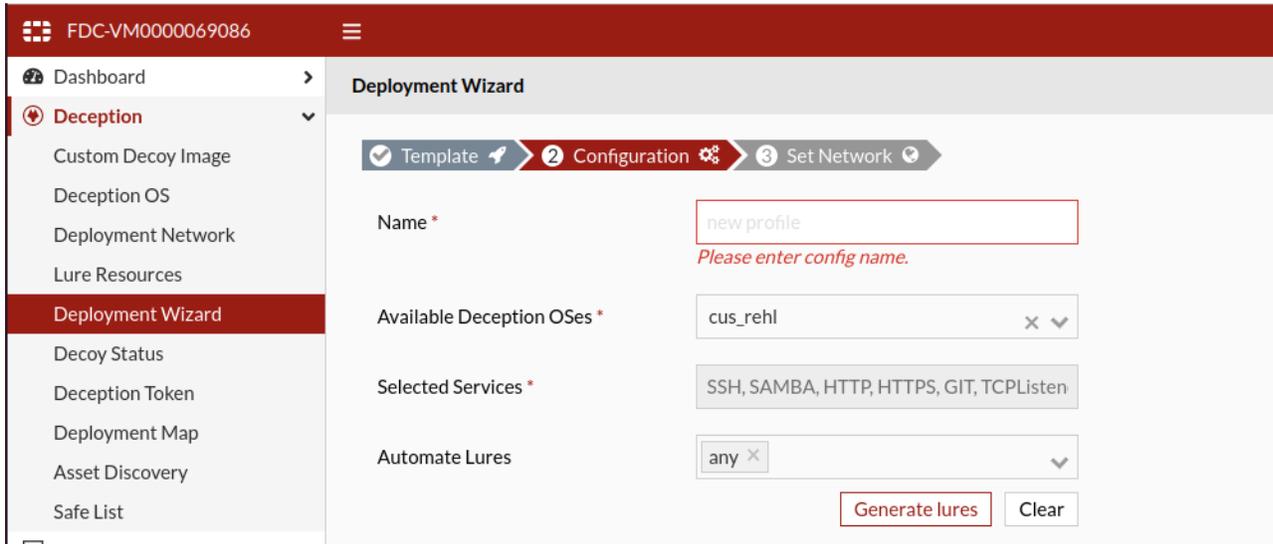
2. Select a customized image and click *Apply*. The applied image is displayed in the *Deception OS* table. It may take several minutes for the image to appear in the table.

| Actions | Status      | VM Name  | OS     | Server       |
|---------|-------------|----------|--------|--------------|
|         | Initialized | cus_rehl | RedHat | Linux Server |
|         | Initialized | cus_test | RedHat | Linux Server |

## 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 into the network.



The screenshot shows the FortiDeceptor interface with the Deployment Wizard open. The wizard is in the 'Configuration' step, which is highlighted in red. The left sidebar shows the navigation menu with 'Deception' expanded and 'Deployment Wizard' selected. The main content area displays the configuration form for a new profile. The form includes the following fields:

- Name \***: A text input field containing 'new profile'. Below it, a red error message reads 'Please enter config name.'
- Available Deception OSes \***: A dropdown menu with 'cus\_rehl' selected.
- Selected Services \***: A text box containing 'SSH, SAMBA, HTTP, HTTPS, GIT, TCPListen'.
- Automate Lures**: A dropdown menu with 'any' selected.

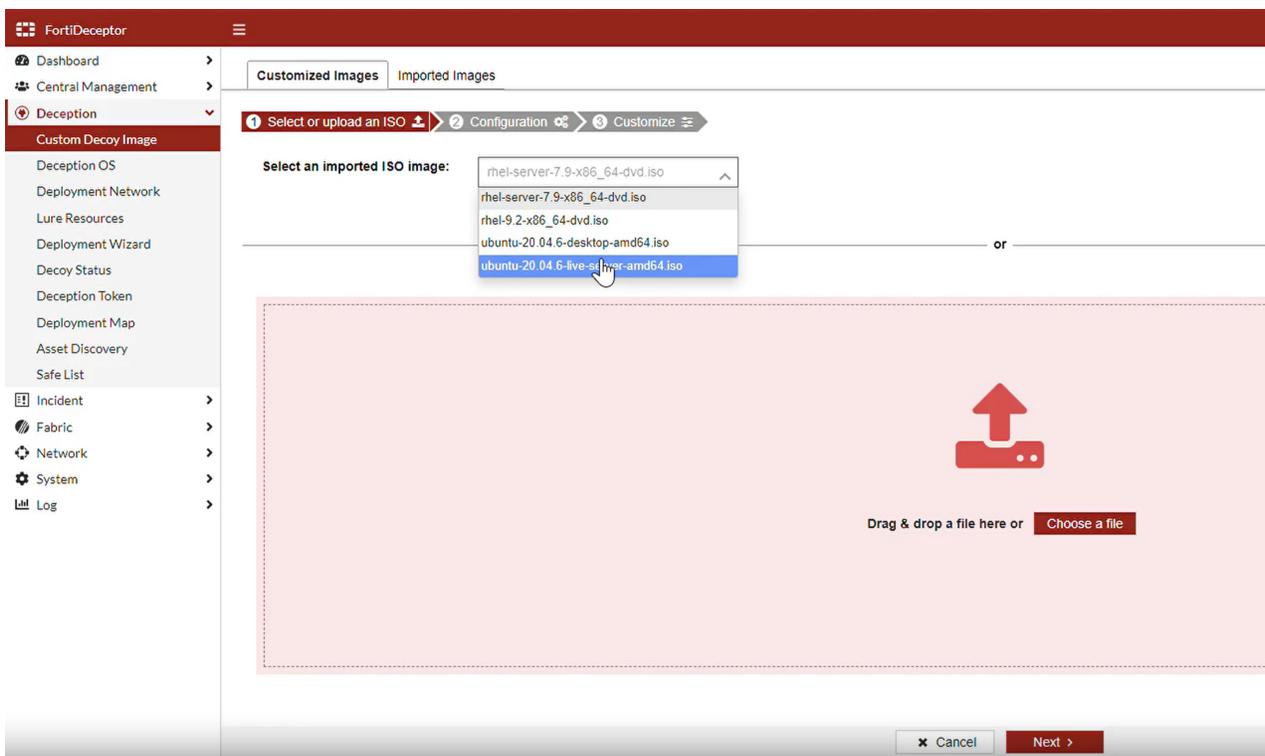
At the bottom right of the form, there are two buttons: 'Generate lures' and 'Clear'.

# Ubuntu OS

## 1. Initialize the OS instance

To initialize the OS instance:

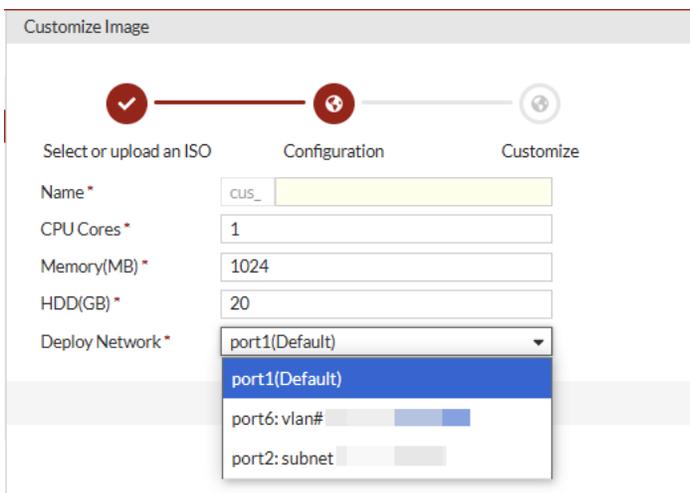
1. Go to *Deception > Customization > Customized Images*.
2. Click *Import Image and Customize*.
3. Choose an ISO image and click *Next*.



4. Configure the following settings and click *Next*.

|                  |                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>      | Characters in range "A-Za-z0-9-_", less than 64 characters.                                                                |
| <b>CPU Cores</b> | 1 - 4                                                                                                                      |
| <b>Memory</b>    | 1024 – 8192 MB.                                                                                                            |
| <b>Storage</b>   | <ul style="list-style-type: none"> <li>• Minimum: 20 GB</li> <li>• Maximum: Up to the supported hard drive size</li> </ul> |

| Deploy Network | Port1        | Default                                                                                                                                                                                                                                  |
|----------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <b>PortX</b> | Select the deployment network.<br>Ensure specified IP is not already in use and the following settings align with the PortX configuration: <ul style="list-style-type: none"> <li>• IP/Mask</li> <li>• Gateway</li> <li>• DNS</li> </ul> |



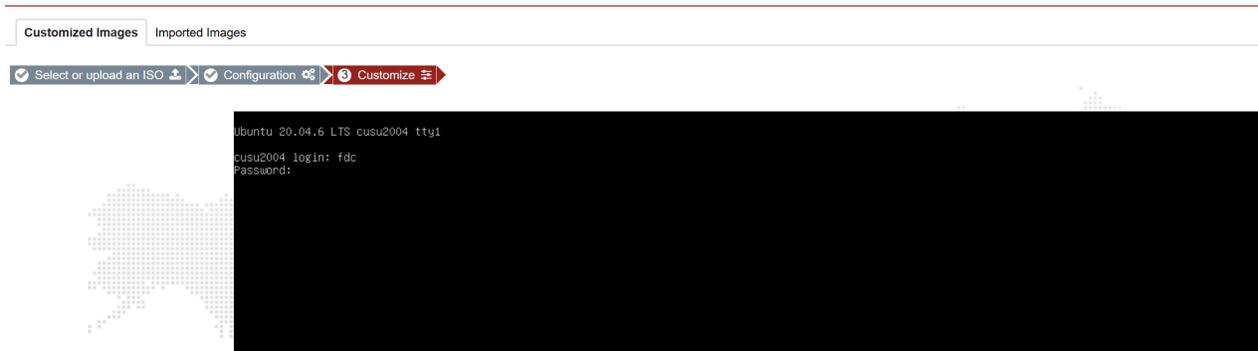
**To configure the system setting in the VNC Windows**

1. In the *Welcome* window, follow the prompts to select your preferred language.
2. In the *Keyboard configuration* window, select you preferred keyboard layout.
3. In the *Network connections* window, click *Continue without network configuration*.
4. In the *Configure proxy* window, do not enter a proxy address and select *Done*
5. In the *Configure Ubuntu archive mirror* window, continue without updating.
6. In the *Guided storage configuration* window, use the space key to deselect *Set up this disk as an LVM group*.
7. In the *Storage configuration* window, continue with the default storage configuration.
8. In the *Storage configuration* window, select *Continue* to confirm the storage configuration.
9. In the *Profile setup* window, follow the prompts set up a profile. Click *Done* when finished.
10. Reboot the Ubuntu server after installation is complete.
11. Press ENTER when the terminal shows *Failed unmounting /cdrom*.

## 2. Mount the device on your system

To mount a device on the system:

1. Log in with the profile you created,



2. Access the root directory.
3. Create a new directory and give it a name (for example, /cus) using the terminal command: `mkdir <directory_name>`  
Example: `mkdir cus`
4. Mount the /dev/sr1 directory to the directory you just created with terminal command: `mount /dev/sr1 <directory_name>/`  
Example: `mount /dev/sr1 cus/`



To re-customize Linux distributions (e.g., Red Hat, Ubuntu, Debian), the customization scripts are stored on the system drive /dev/sr0. Mount /dev/sr0 to the newly created directory before starting the re-customization process.

5. Copy all files from the directory you created to the /tmp director with terminal command: `cp -r <directory_name> tmp/`  
Example: `cp -r <directory_name> tmp/`



Copy the mounted files to a directory where the root user has write permissions (e.g., /tmp/). Otherwise, the customization will fail during the Ubuntu tracer installation step.

6. Check the file list in the destination directory (eg, tmp/cus/).

```

root@cusu2004:~# mkdir cus
root@cusu2004:~# ls cus
root@cusu2004:~# mount /dev/sr1 cus/
mount: /cus: WARNING: device write-protected, mounted read-only.
root@cusu2004:~# cp cus tmp/
cp: -r not specified; omitting directory 'cus'
root@cusu2004:~# cp -r cus tmp/
root@cusu2004:~# ls tmp/
cus
snap-private-tmp
systemd-private-a45ac4bf5f464d14bcfc9609c21d24a5-ModemManager.service-25k8Tf
systemd-private-a45ac4bf5f464d14bcfc9609c21d24a5-systemd-logind.service-K571Ih
systemd-private-a45ac4bf5f464d14bcfc9609c21d24a5-systemd-resolved.service-uk62Pg
systemd-private-a45ac4bf5f464d14bcfc9609c21d24a5-systemd-timedated.service-0J5ARg
systemd-private-a45ac4bf5f464d14bcfc9609c21d24a5-systemd-timesyncd.service-0r60Zf
root@cusu2004:~# cd tmp/cus/
root@cusu2004:~/tmp/cus# ls
net.json README_Redhat.txt README_Ubuntu.txt README_Windows.txt Redhat Ubuntu Windows
root@cusu2004:~/tmp/cus# cd Ubuntu/
root@cusu2004:~/tmp/cus/Ubuntu# ls
bash decoy_strace_installation.sh install_ubuntu_modules.sh set_network.sh sshd strace_ubuntu2004.stp ubuntu_cus_toolkit.sh
root@cusu2004:~/tmp/cus/Ubuntu# _

```

## 3. Configure network

You can configure the network automatically or manually.

### Option A: Configure the network by Ubuntu/set\_network.sh script automatically

```
bash set_network.sh
```

```

root@cusu2004:~/tmp/cus/Ubuntu# bash set_network.sh
found network interface ens1
root@cusu2004:~/tmp/cus/Ubuntu#

```

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

## 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. Ensure the server has internet access.
2. \Run the following command: `bash install_ubuntu_modules.sh`

```
root@cusu2004:/tmp/cus/Ubuntu# bash install_ubuntu_modules.sh
going update pkg installer
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal/restricted amd64 Packages [22.0 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/restricted Translation-en [6,212 B]
Get:7 http://archive.ubuntu.com/ubuntu focal/restricted amd64 c-n-f Metadata [392 B]
Get:8 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8,628 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal/universe Translation-en [5,124 kB]
Get:10 http://archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:11 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:13 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9,136 B]
Get:14 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [3,683 kB]
Get:15 http://archive.ubuntu.com/ubuntu focal-updates/main Translation-en [564 kB]
Get:16 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:17 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [3,401 kB]
58% [8 Packages store 0 B] [17 Packages 16.4 kB/3,401 kB 0%]
```



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

## Option B: Install the modules manually

Install the packages by running:

```
apt -y update
apt -y install acl
apt -y install net-tools
apt -y install python3-dev
apt -y install python3-pip
apt -y install samba samba-client
apt -y install apache2
apt -y install openssh-server
pip3 install requests
pip3 install sh
pip3 install requests
pip3 install netifaces
pip3 install psutil
pip3 install tornado
```

```
Preparing to unpack .../2-ncurses-term_6.2-0ubuntu2.1_all.deb ...
Unpacking ncurses-term (6.2-0ubuntu2.1) ...
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../3-openssh-sftp-server_1%3a8.2p1-4ubuntu0.11_amd64.deb ...
Unpacking openssh-sftp-server (1:8.2p1-4ubuntu0.11) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../4-openssh-server_1%3a8.2p1-4ubuntu0.11_amd64.deb ...
Unpacking openssh-server (1:8.2p1-4ubuntu0.11) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../5-ssh-import-id_5.10-0ubuntu1_all.deb ...
Unpacking ssh-import-id (5.10-0ubuntu1) ...
Setting up openssh-client (1:8.2p1-4ubuntu0.11) ...
Setting up ssh-import-id (5.10-0ubuntu1) ...
Attempting to convert /etc/ssh/ssh_import_id
Setting up libwrap0:amd64 (7.6.q-30) ...
Setting up ncurses-term (6.2-0ubuntu2.1) ...
Setting up openssh-sftp-server (1:8.2p1-4ubuntu0.11) ...
Setting up openssh-server (1:8.2p1-4ubuntu0.11) ...

Creating config file /etc/ssh/sshd_config with new version
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for systemd (245.4-4ubuntu3.20) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
Done!
rm: cannot remove '/usr/lib/python3.*/EXTERNALLY-MANAGED': No such file or directory
going to install python modules
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (2.22.0)
Collecting sh
 Downloading sh-2.1.0-py3-none-any.whl (38 kB)
Installing collected packages: sh
Successfully installed sh-2.1.0
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (2.22.0)
Requirement already satisfied: netifaces in /usr/lib/python3/dist-packages (0.10.4)
Collecting psutil
 Downloading psutil-6.1.0-cp36-abi3-manylinux_2_12_x86_64.manylinux2010_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (287 kB)
|██| 287 kB 8.8 MB/s
Installing collected packages: psutil
Successfully installed psutil-6.1.0
Done!
Collecting tornado
 Downloading tornado-6.4.2-cp38-abi3-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (437 kB)
|██| 437 kB 7.1 MB/s
Installing collected packages: tornado
Successfully installed tornado-6.4.2
Done!
root@cusu2004:/tmp/cus/Ubuntu#
```

## 5. Build the custom Ubuntu tracer

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

```
bash decoy_strace_installation.sh strace_ubuntu2004.stp
```

The script will check your build environment before building the tracer

```

root@cusu2004:/tmp/cus/Ubuntu# bash decoy_strace_installation.sh strace_ubuntu2004.stp
\033[0;34mgoing to install kernel modules...\033[0m
Executing: /tmp/apt-key-gpghome.Ega2Ch7Ii4/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-keys C8CAB6595FDF622
gpg: key C8CAB6595FDF622: public key "Ubuntu Debug Symbol Archive Automatic Signing Key (2016) <ubuntu-archive@lists.ubuntu.com>" imported
gpg: Total number processed: 1
gpg: imported: 1
deb http://ddebs.ubuntu.com/ focal main restricted universe multiverse
deb http://ddebs.ubuntu.com/ focal-updates main restricted universe multiverse
deb http://ddebs.ubuntu.com/ focal-proposed main restricted universe multiverse
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://archive.ubuntu.com/ubuntu focal-security InRelease
Get:5 http://ddebs.ubuntu.com focal InRelease [41.3 kB]
Get:6 http://ddebs.ubuntu.com focal-updates InRelease [41.3 kB]
Get:7 http://ddebs.ubuntu.com focal-proposed InRelease [41.4 kB]
Get:8 http://ddebs.ubuntu.com focal/main amd64 Packages [514 kB]
Get:9 http://ddebs.ubuntu.com focal/universe amd64 Packages [4,376 kB]
Get:10 http://ddebs.ubuntu.com focal/multiverse amd64 Packages [67.6 kB]
Get:11 http://ddebs.ubuntu.com focal-updates/main amd64 Packages [396 kB]
Get:12 http://ddebs.ubuntu.com focal-updates/restricted amd64 Packages [668 B]
Get:13 http://ddebs.ubuntu.com focal-updates/universe amd64 Packages [386 kB]
Get:14 http://ddebs.ubuntu.com focal-updates/multiverse amd64 Packages [2,764 B]
Get:15 http://ddebs.ubuntu.com focal-proposed/main amd64 Packages [56.5 kB]
Get:16 http://ddebs.ubuntu.com focal-proposed/universe amd64 Packages [17.8 kB]
Get:17 http://ddebs.ubuntu.com focal-proposed/multiverse amd64 Packages [668 B]
Fetched 5,942 kB in 4s (1,617 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
170 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
Reading state information... Done
gcc is already the newest version (4:9.3.0-1ubuntu2).
gcc set to manually installed.
The following additional packages will be installed:
 libdw1 libelf1 systemtap-common systemtap-runtime
Suggested packages:
 systemtap-doc vim-addon-manager
The following NEW packages will be installed:
 libdw1 systemtap systemtap-common systemtap-runtime
The following packages will be upgraded:
 libelf1
1 upgraded, 4 newly installed, 0 to remove and 169 not upgraded.
Need to get 2,294 kB of archives.
After this operation, 10.7 MB of additional disk space will be used.
0% [Working]

```

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

```

Truncating module name to 'vumgfix'
Pass 1: parsed user script and 476 library scripts using 102984virt/91068res/7504shr/83740data kb, in 440usr/180sys/792real ms.
WARNING: cross-file global variable reference to identifier 'syscall_string_trunc' at /usr/share/systemtap/tapset/linux/syscalls_cfg_trunc.stp:3:8 from: identifier 'syscall_string_trunc' at /usr/share/systemtap/tapset/linux/sysc_write.stp:23:49
source: buf_str = user_buffer_quoted(buf_uaddr, count, syscall_string_trunc)

 in expansion of macro: operator '@_SYSCALL_WRITE_REGARGS' at /usr/share/systemtap/tapset/linux/sysc_write.stp:100:2
source: @_SYSCALL_WRITE_REGARGS

Pass 2: analyzed script: 55 probes, 64 functions, 102 embeds, 20 globals using 178700virt/168496res/8992shr/159456data kb, in 120200usr/18010sys/79025real ms.
Pass 3: translated to C into "/tmp/stapLXAGN/vumgfix_src.c" using 178700virt/168496res/8992shr/159456data kb, in 40usr/10sys/57real ms.
vumgfix.ko
Pass 4: compiled C into "vumgfix.ko" in 31740usr/4030sys/35334real ms.
kernel module build passed
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
 linux-image-unsigned-5.4.0-144-generic-dbgsum
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
 linux-image-5.4.0-144-generic-dbgsum
0 upgraded, 0 newly installed, 1 to remove and 169 not upgraded.
After this operation, 23.6 kB disk space will be freed.
(Reading database ... 88577 files and directories currently installed.)
Removing linux-image-5.4.0-144-generic-dbgsum (5.4.0-144.161) ...
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
 linux-image-unsigned-5.4.0-144-generic-dbgsum
0 upgraded, 0 newly installed, 1 to remove and 169 not upgraded.
After this operation, 6,937 MB disk space will be freed.
(Reading database ... 88574 files and directories currently installed.)
Removing linux-image-unsigned-5.4.0-144-generic-dbgsum (5.4.0-144.161) ...
root@cusu2004:/tmp/cus/Ubuntu# _

```

## 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 ubuntu_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

```
root@cusu2004:/tmp/cus/Ubuntu# bash ubuntu_cus_toolkit.sh
^O33[0;34mchecking sshd...^O33[0m
OpenSSH_8.2p1 Ubuntu-4ubuntu0.11, OpenSSL 1.1.1f 31 Mar 2020
openssh server is installed
openssh version check passed
install custom sshd passed
going to install custom bash
^O33[0;34mchecking Python Env...^O33[0m
Python 3.8.10
python3 is installed
Python module check passed
python version check passed

Samba version 4.15.13-Ubuntu
PID Username Group Machine Protocol Version Encryption Signing

Service pid Machine Connected at Encryption Signing

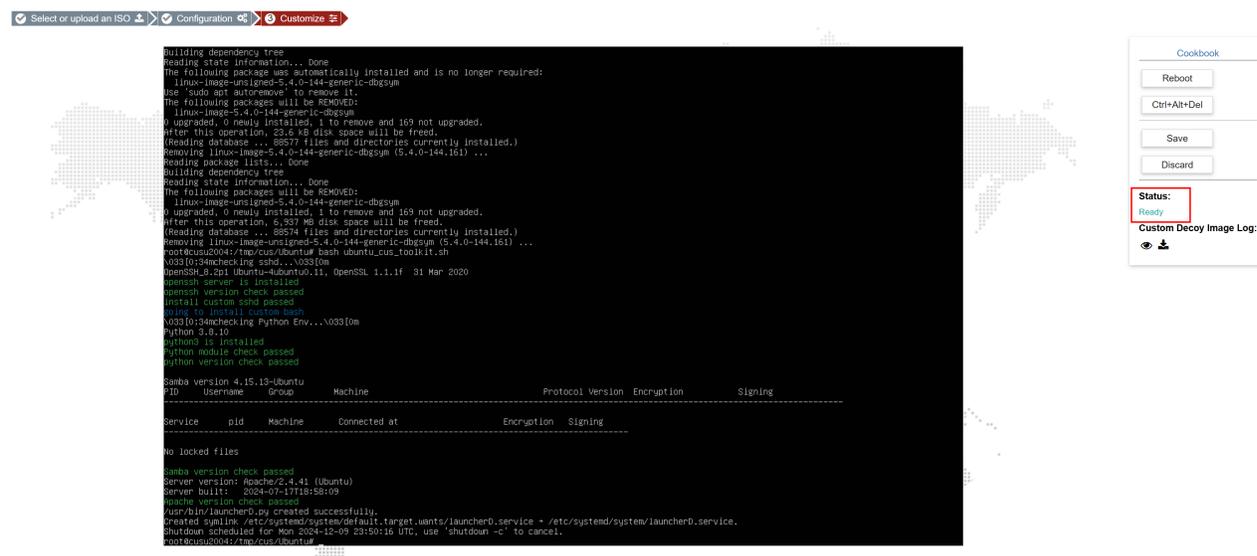
No locked files

Samba version check passed
Server version: Apache/2.4.41 (Ubuntu)
Server built: 2024-07-17T18:58:09
Apache version check passed
/usr/bin/launcherD.py created successfully.
Created symlink /etc/systemd/system/default.target.wants/launcherD.service → /etc/systemd/system/launcherD.service.
```

## 7. Save the custom Image

To save the custom image:

1. In the FortiDeceptor GUI, verify the image *Status* is *Ready*.

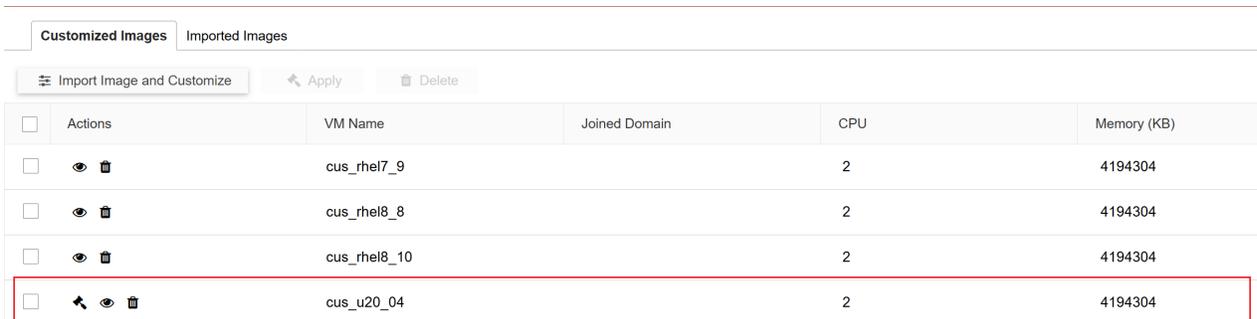


2. Click *Save* when the system is powered off.

## 8. Review the result

To review the result:

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



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

## 9. Use the custom Ubuntu image

### 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) |
|-------------------------------------|--------------|---------------|-----|-------------|
| <input type="checkbox"/>            | cus_rhel7_9  |               | 2   | 4194304     |
| <input type="checkbox"/>            | cus_rhel8_8  |               | 2   | 4194304     |
| <input type="checkbox"/>            | cus_rhel8_10 |               | 2   | 4194304     |
| <input checked="" type="checkbox"/> | cus_u20_04   |               | 2   | 4194304     |

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

| Status      | Name       | OS Type | VM Type      | Lures |
|-------------|------------|---------|--------------|-------|
| Initialized | cus_u20_04 | Ubuntu  | Linux Server |       |

### Deploy decoys with custom Ubuntu images

To deploy decoys with a custom Ubuntu image:

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

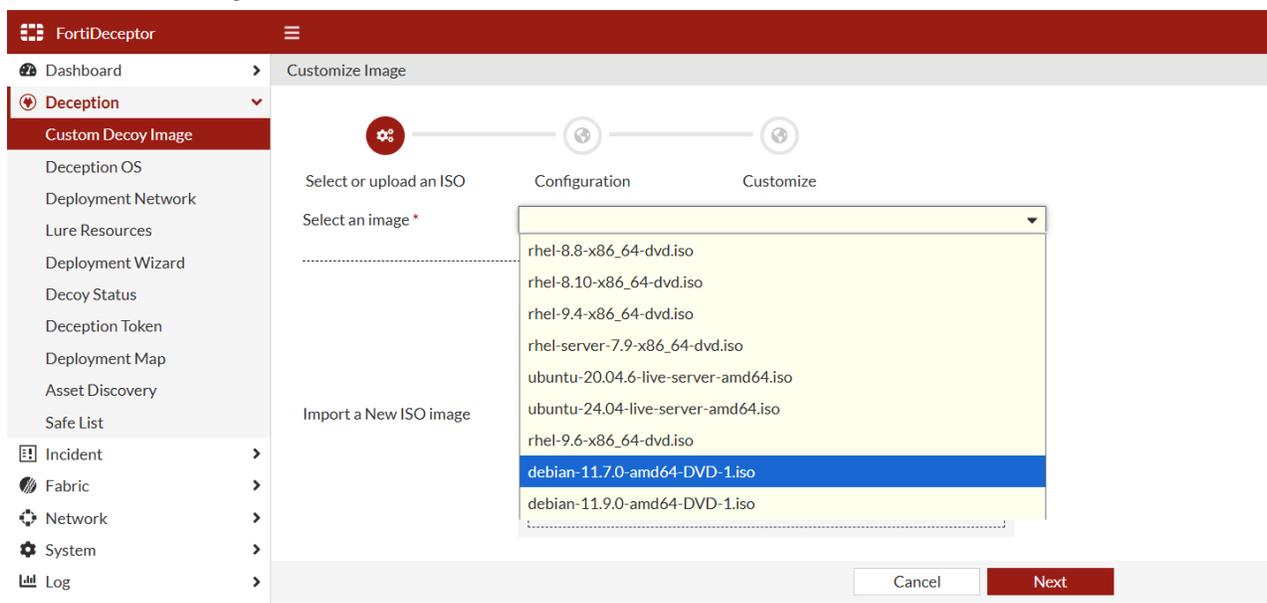
The screenshot shows the FortiDeceptor web interface. The top navigation bar includes the FortiDeceptor logo and a menu icon. The left sidebar contains a navigation menu with the following items: Dashboard, Deception (selected), Custom Decoy Image, Deception OS, Deployment Network, Lure Resources, Deployment Wizard (highlighted), Decoy Status, Deception Token, Deployment Map, Asset Discovery, Safe List, and Incident. The main content area is titled "Deployment Wizard" and features a progress bar with three steps: 1. Template, 2. Configuration (active), and 3. Set Network. Below the progress bar, there 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\_u20\_04"; "Selected Services \*" with a text input containing "SSH, SAMBA, HTTP, HTTPS, GIT, SMTP, TCF"; and "Automate Lures" with a dropdown menu showing "any". At the bottom right of the configuration area, there are two buttons: "Generate lures" and "Clear".

# Debian OS

## 1. Initialize the OS instance

To initialize the OS instance:

1. Go to *Deception > Custom Decoy Image > Customize Images*.
2. Click *Import a New ISO image*.
3. Choose an ISO image and click *Next*.



4. Configure the following settings and click *Next*.

|                       |                                                                                                                            |                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| <b>Name</b>           | Characters in range "A-Za-z0-9-_", less than 64 characters.                                                                |                                |
| <b>CPU Cores</b>      | 1 – 4                                                                                                                      |                                |
| <b>Memory</b>         | 1024 – 8129 MB<br>2048 MB recommended for graphical system                                                                 |                                |
| <b>Storage</b>        | <ul style="list-style-type: none"> <li>• Minimum: 20 GB</li> <li>• Maximum: Up to the supported hard drive size</li> </ul> |                                |
| <b>Deploy Network</b> | <b>Port1</b>                                                                                                               | Default                        |
|                       | <b>PortX</b>                                                                                                               | Select the deployment network. |

Ensure specified IP is not already in use and the following settings align with the PortX configuration:

- IP/Mask
- Gateway
- DNS

### Customize Image



Select or upload an ISO

Configuration

Customize

Name \*

cus\_

CPU Cores \*

Memory(MB) \*

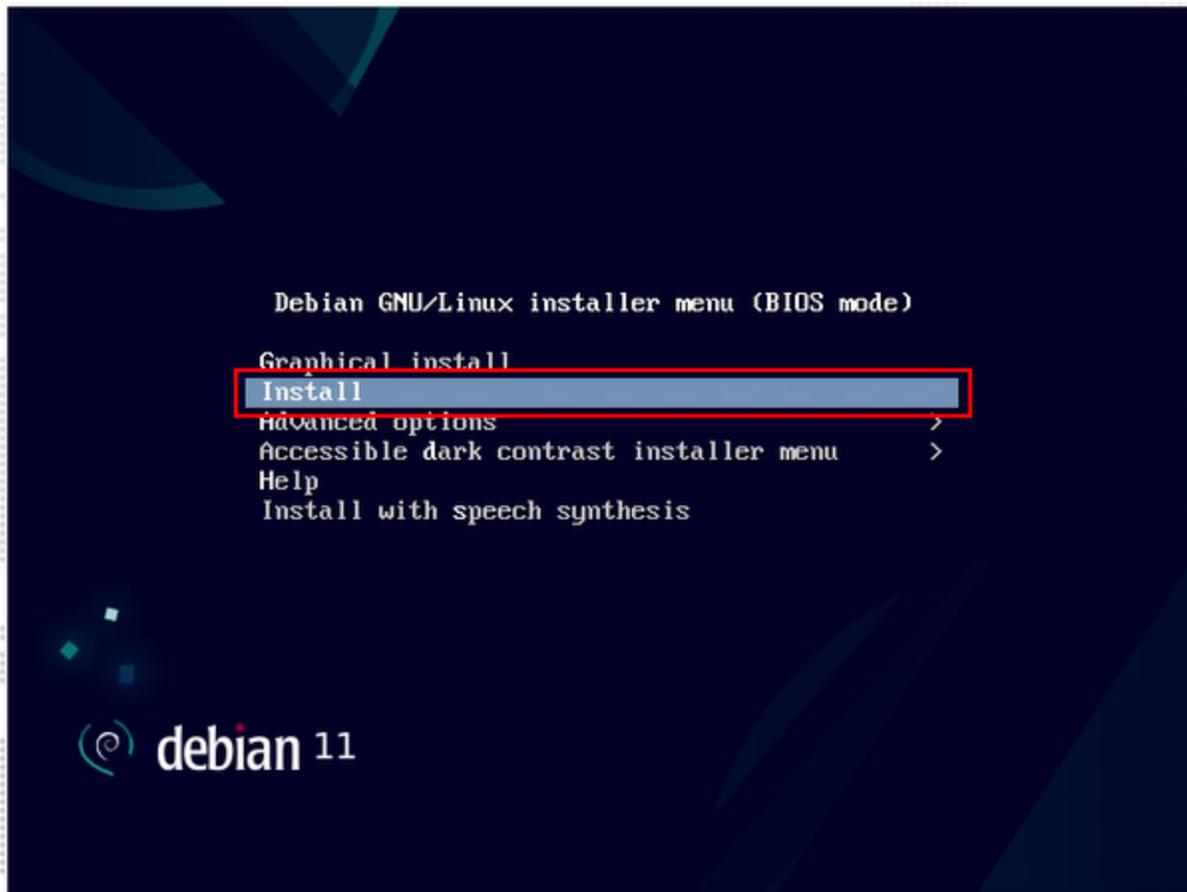
HDD(GB) \*

Deploy Network \*

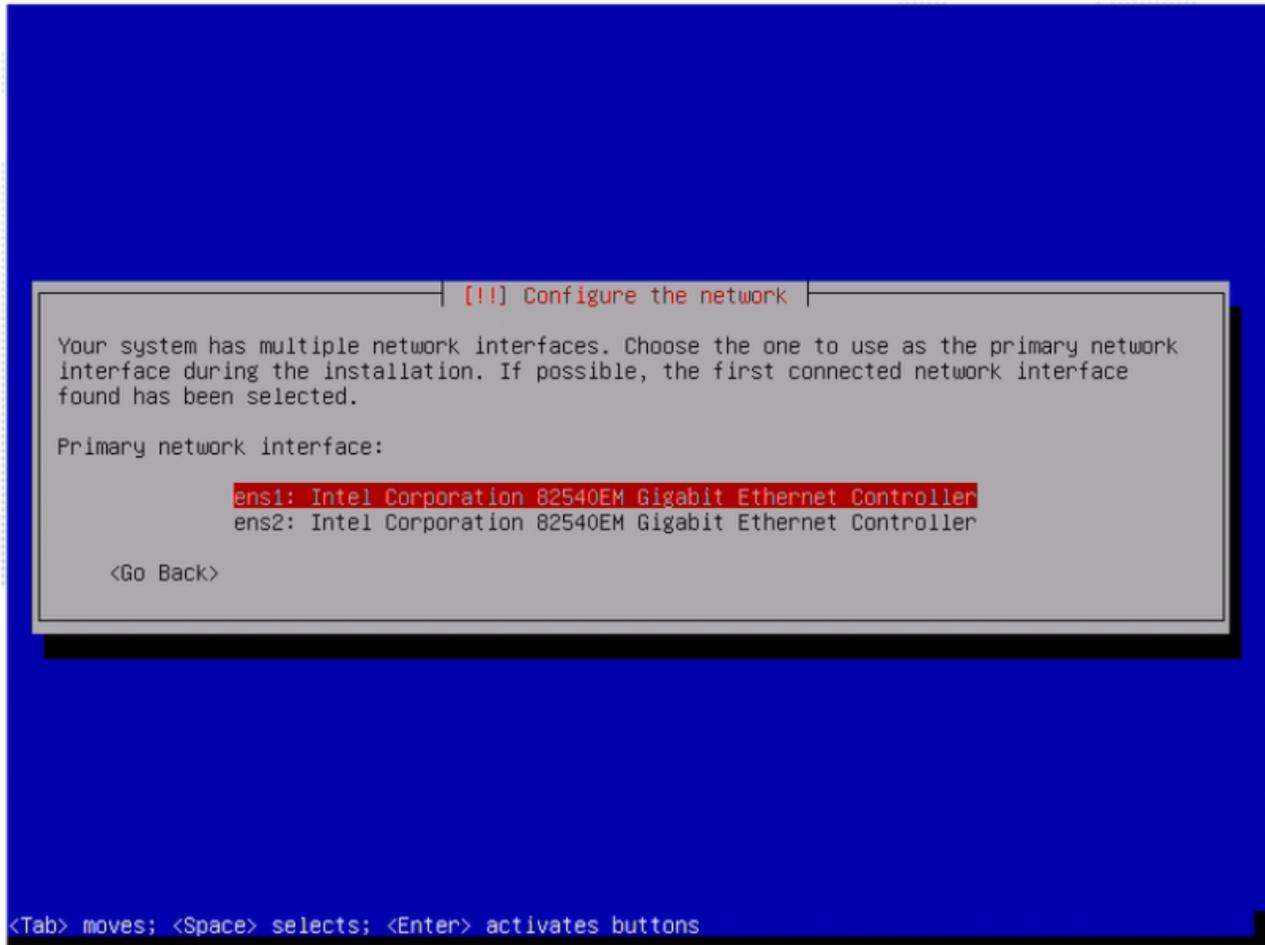
- FDC-VM0001001245:port6: vlan#
- FDCVME0106900815:port3: subnet
- FDCVME0106900815:port6: vlan#
- FDCVMS0010080102:port2: subnet
- FDCVMS2239241135:port2: subnet
- local:port2: subnet
- local:port3: subnet
- local:port6: vlan#
- port1(Default)**

**To configure the system setting in the VNC window**

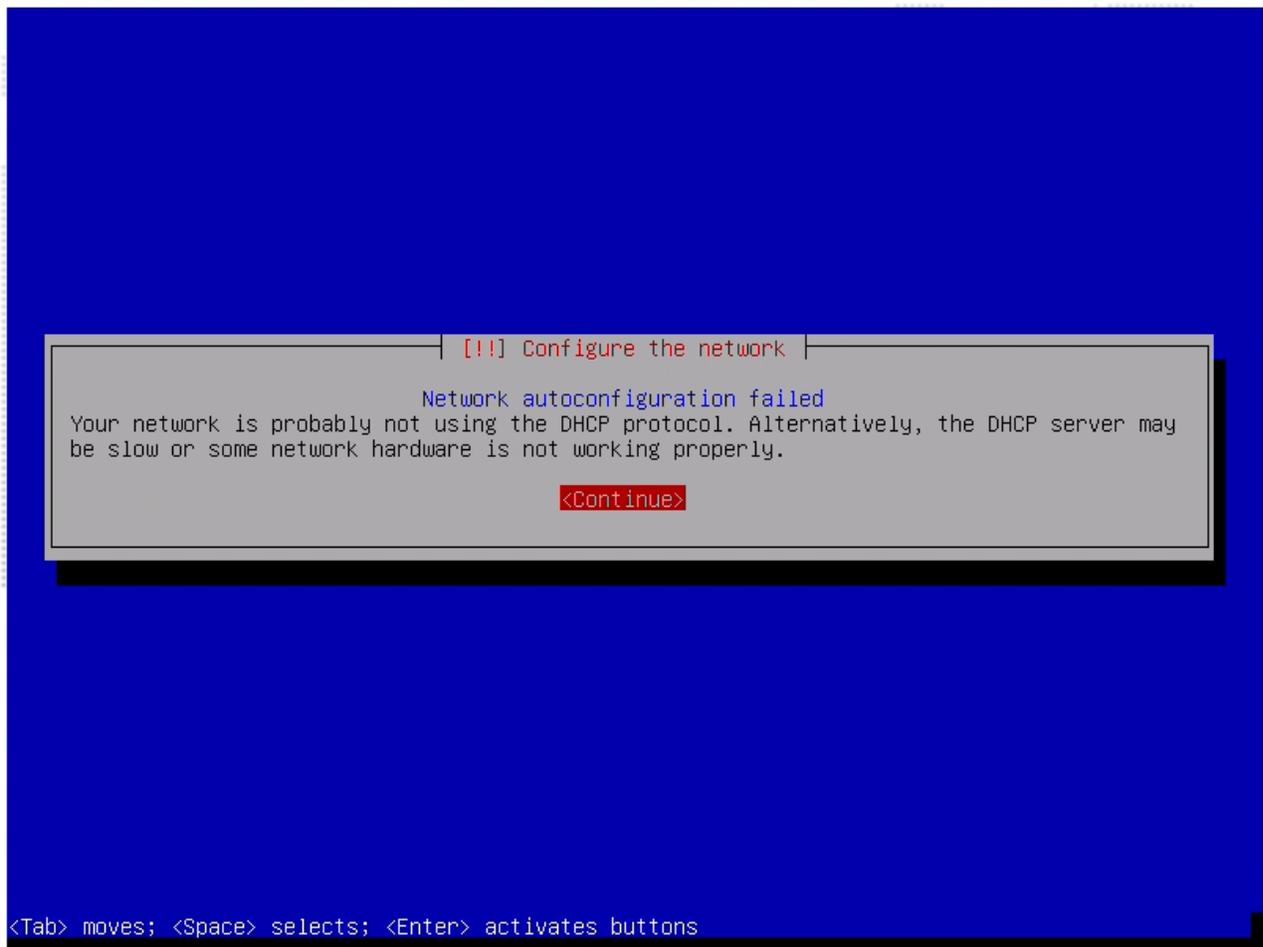
1. In the *Welcome* window, select the text-based *Install* option



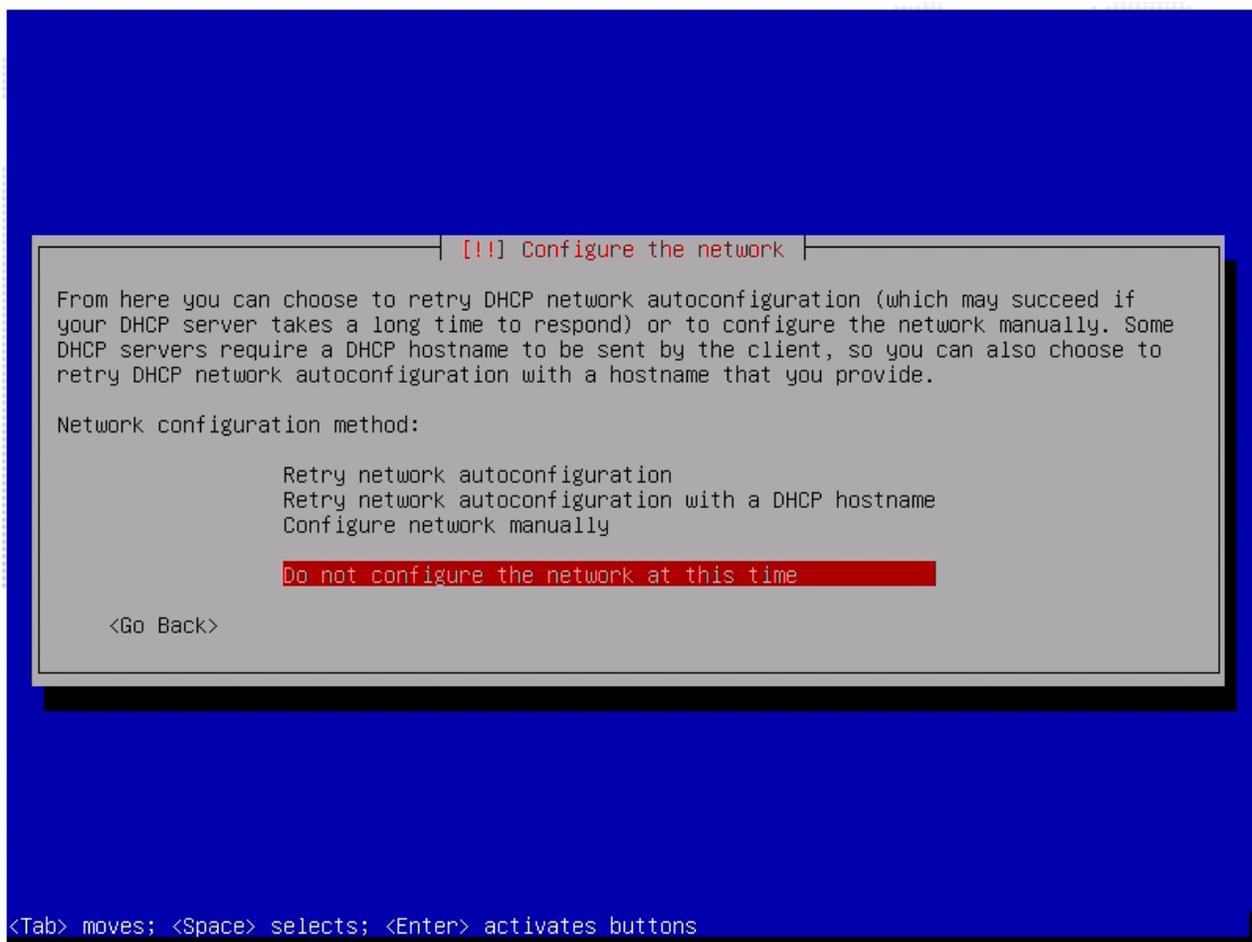
2. In the *Language* configuration window, follow the prompts to select your preferred language.
3. In the *Keyboard configuration* window, select your preferred keyboard layout.
4. In the *Network configuration* window, select your preferred interface. Continue without network configuration.



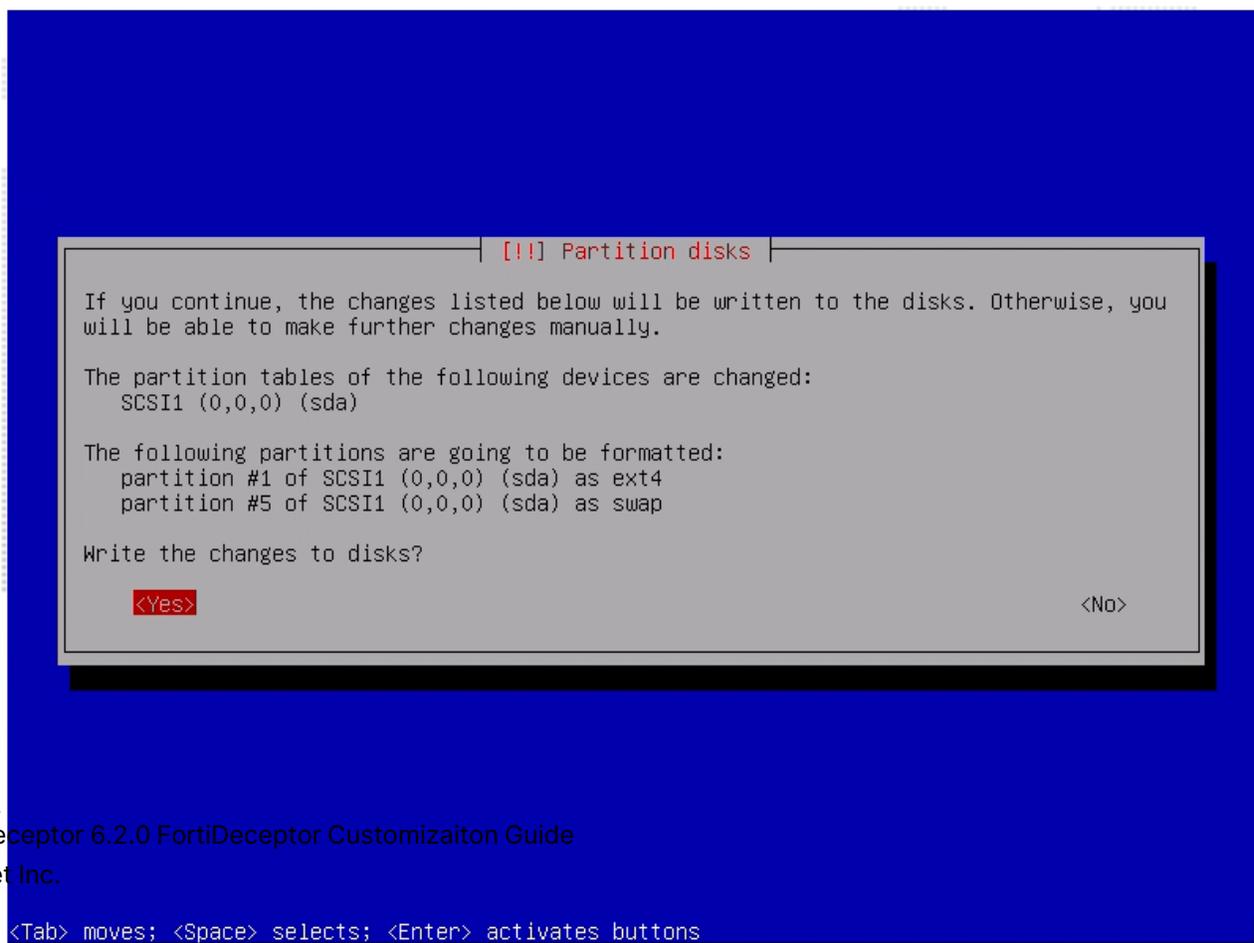
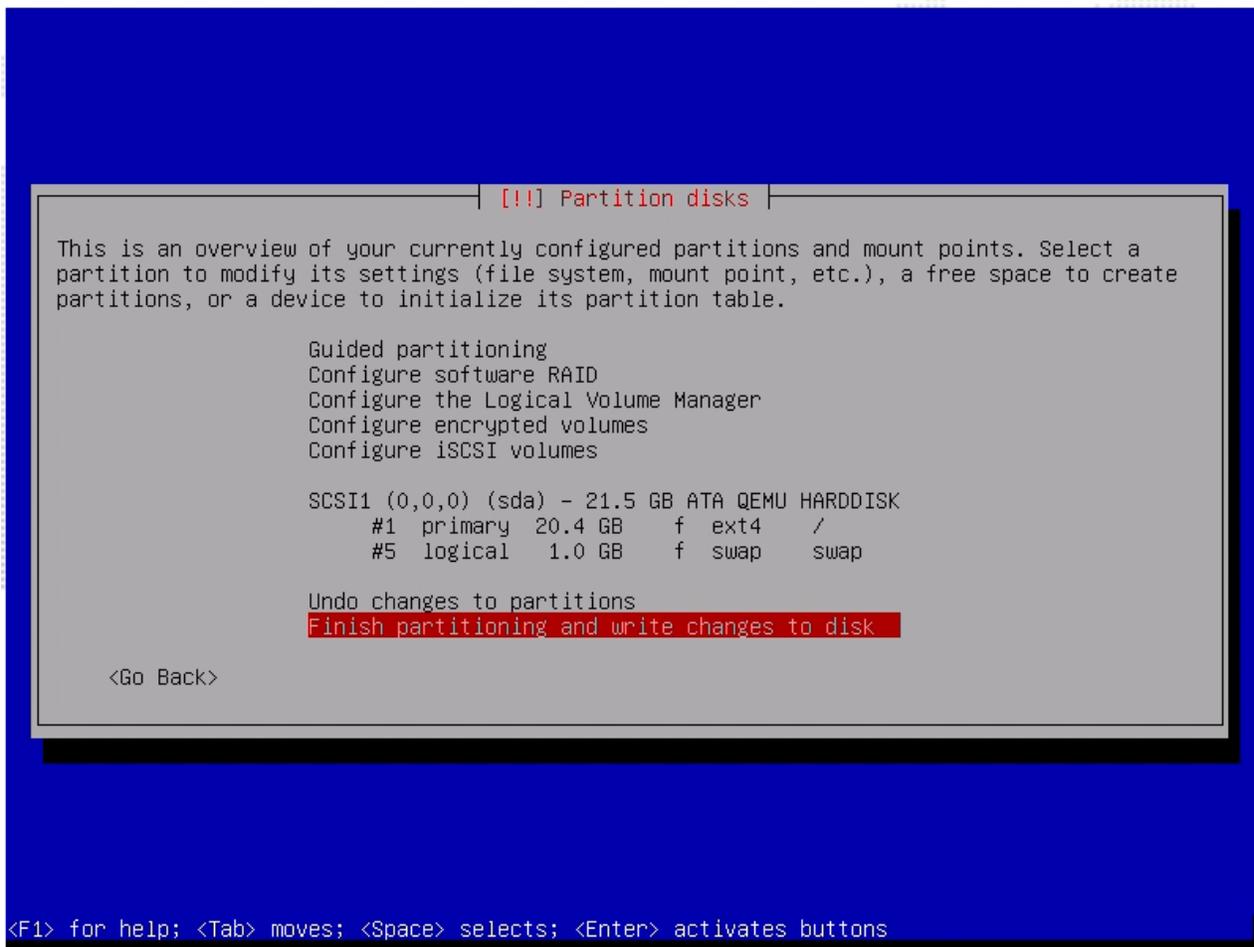
5. Select *Continue* when network autoconfiguration fails.



6. In the returned *Network configuration* window, select *Do not configure the network at this time*.



7. Follow the prompts in the *Users and Passwords Configuration* windows to setup users and passwords.
8. In the *Time zone* configuration window, select your preferred time zone.
9. In the *Guided storage* configuration windows, select and confirm your preferred disk partition.

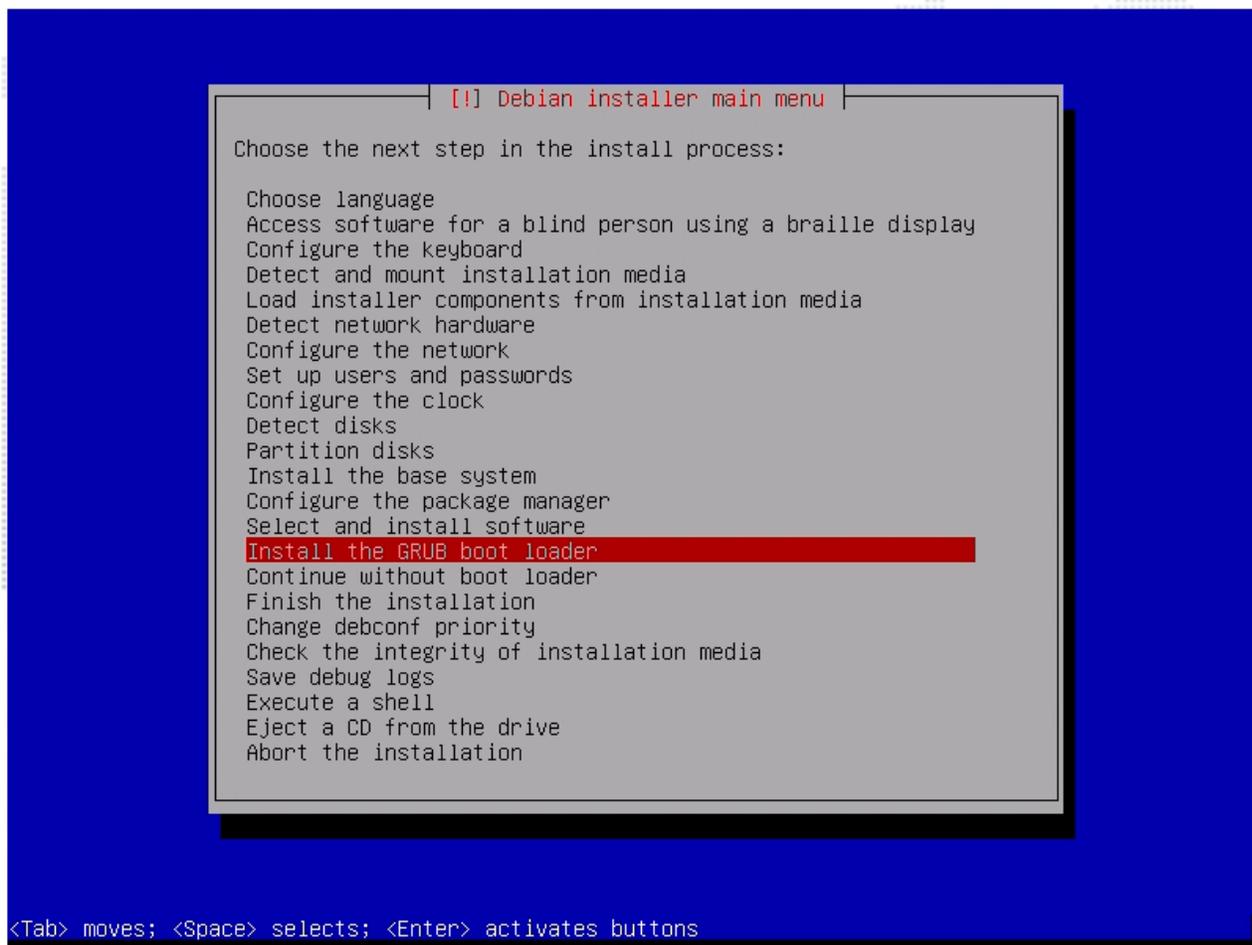


10. The installer will install the base system and configure the package manager automatically.
11. Select *Go Back* to return to the installer main menu while any apt configuration problem.

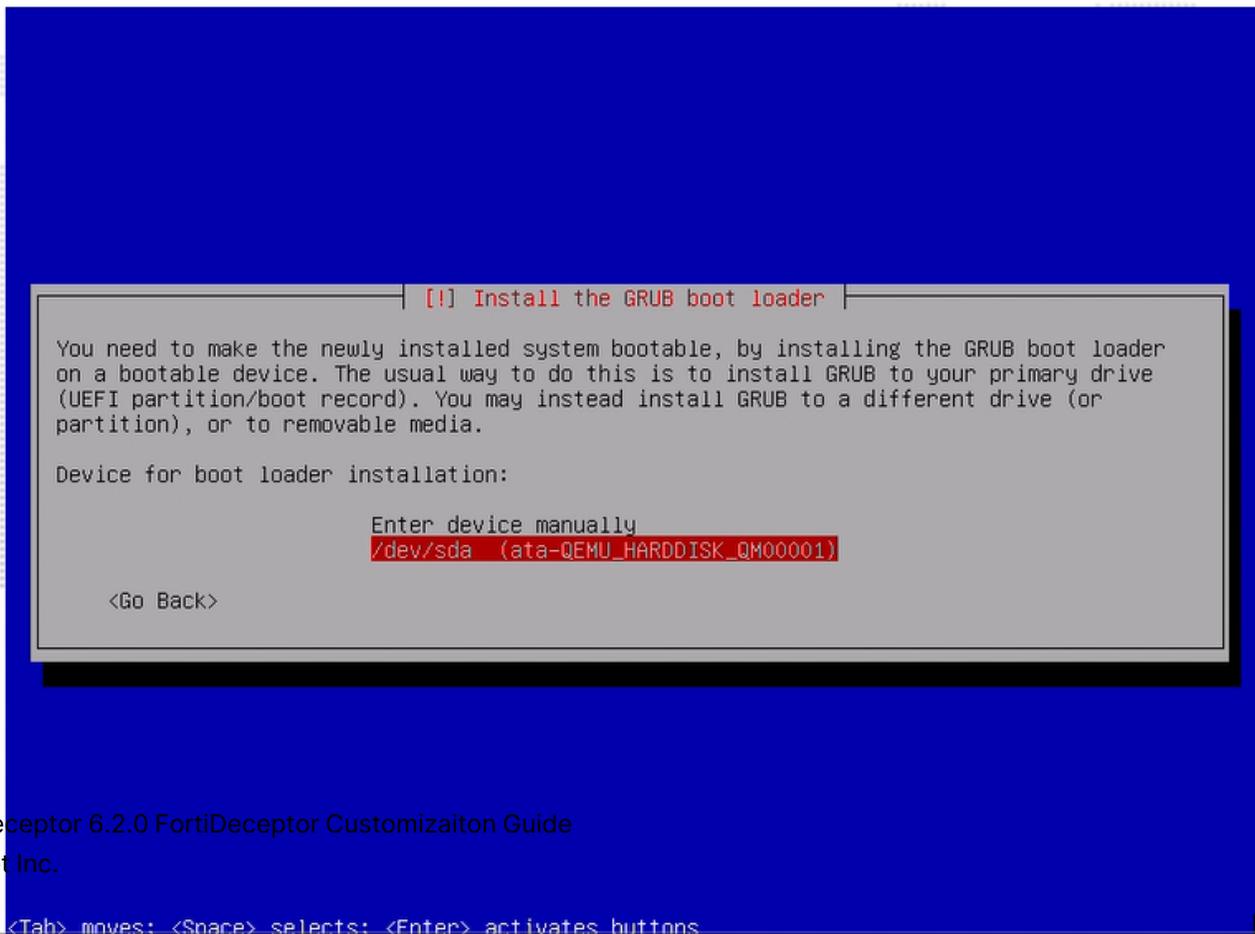
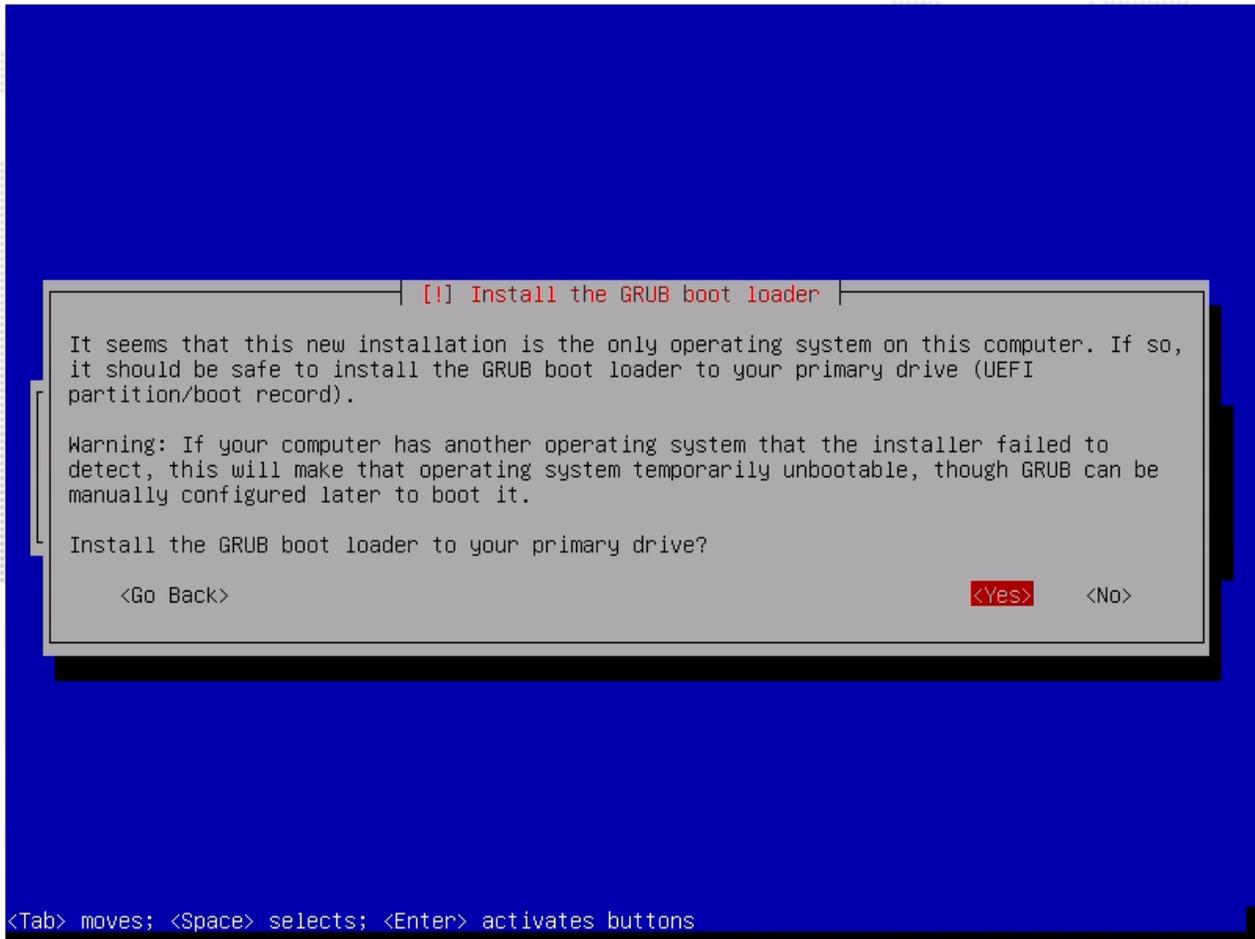


Do not click *Continue* to start the software installation. This will cause the GRUB boot loader installation to fail. If this occurs, you must discard the customization and start over.

12. In the installer main menu window, select *Install the GRUB boot loader* by skipping the package manager configuration and software installation.



13. In the *GRUB boot loader* configuration windows, select yes to install the GRUB boot loader to primary drive. And select the provided device for boot loader installation.



14. Select *Continue* when the installation is completed.
15. The custom system will be rebooted and show the login terminal automatically.

## 2. Mount the device on your system

### To mount a device on the system:

1. Log in with the root user account.
2. Access the root directory.
3. Create a new directory and give it a name (for example, /tmpcus) using the terminal command: `mkdir <directory_name>`.  
Example: `mkdir tmpcus`
4. Mount the /dev/sr1 directory to the directory you just created with terminal command: `mount /dev/sr1 <directory_name1>/`  
Example: `mount /dev/sr1 tmpcus/`



To re-customize Linux distributions (e.g., Red Hat, Ubuntu, Debian), the required customization scripts are located on the system drive /dev/sr0. Before starting the re-customization process, mount /dev/sr0 to the newly created directory.

5. Create another directory and give it a name (for example, /cus) using the terminal command: `mkdir <directory_name2>`  
Example: `mkdir cus`
6. Copy all files from the first directory (for example, /tmpcus) to the second directory (for example, /cus) with terminal command: `cp -r <directory_name1> <directory_name2>`  
Example: `cp -r tmpcus/* cus/`



During module installation, the system may reboot multiple times. To avoid losing customization scripts, copy the mounted files to a newly created directory. Otherwise, you will need to re-mount /dev/sr1 or /dev/sr0 after each reboot.

Check the file list in the destination directory (eg, cus/).

```
Debian GNU/Linux 11 debian tty1
debian login: root
Password:
Linux debian 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~# cd /
root@debian:~# mkdir cus
root@debian:~# mkdir tmpcus
root@debian:~# mount /dev/sr1 tmpcus/
mount: /tmpcus: WARNING: source write-protected, mounted read-only.
root@debian:~# cp -r tmpcus/* cus/
root@debian:~# ls cus/
Debian net.json README_debian.txt README_Redhat.txt README_Ubuntu.txt README_Windows.txt Redhat Ubuntu Windows
root@debian:~# cd cus/Debian/
root@debian:~/cus/Debian# ls
debian_cus_toolkit.sh decoy_strace_installation.sh install_debian_modules.sh set_network.sh strace_debian11.stp
root@debian:~/cus/Debian#
```

## 3. Configure the network

You can configure the network automatically or manually.

**To automatically configure the network using the Debian/set\_network.sh script:**

```
bash set_network.sh
```

```
root@debian:/cus/Debian# bash set_network.sh
found network interface ens1 ens2
root@debian:/cus/Debian# ping google.com
PING google.com (142.250.73.110) 56(84) bytes of data.
64 bytes from 142.250.73.110: icmp_seq=1 ttl=115 time=4.49 ms
^C64 bytes from 142.250.73.110: icmp_seq=2 ttl=115 time=4.57 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 10016ms
rtt min/avg/max/mdev = 4.493/4.529/4.565/0.036 ms
root@debian:/cus/Debian# _
```

**To configure the network manually:**

1. Open and read the setting file net.json.
2. Follow the settings to configure the IP, gateway, DNS.
3. After you are done, verify that your network can access the internet.

## 4. Install the required modules

You can install all modules and packages automatically using the script, or install each package manually with apt and pip3 commands.

**To install all required modules and packages using the script:**

1. Ensure the server has internet access.
2. Run the following command: `bash install_debian_modules.sh`

```

root@debian:/cus/Debian# bash install_debian_modules.sh
going to check/update kernel version
Get:1 http://deb.debian.org/debian bullseye InRelease [75.1 kB]
Err:2 https://deb.debian.org/debian bookworm InRelease
 Certificate verification failed: The certificate is NOT trusted. The certificate issuer is unknown. Could not handshake: Error in the certificate verificati
n. [IP: 151.101.22.132 443]
Err:3 https://deb.debian.org/debian-security bookworm-security InRelease
 Certificate verification failed: The certificate is NOT trusted. The certificate issuer is unknown. Could not handshake: Error in the certificate verificati
n. [IP: 151.101.22.132 443]
Err:4 https://deb.debian.org/debian bookworm-updates InRelease
 Certificate verification failed: The certificate is NOT trusted. The certificate issuer is unknown. Could not handshake: Error in the certificate verificati
n. [IP: 151.101.22.132 443]
Get:5 http://deb.debian.org/debian-debug bullseye-debug InRelease [21.1 kB]
Get:6 http://deb.debian.org/debian bullseye/non-free Sources [81.0 kB]
Get:7 http://deb.debian.org/debian bullseye/main Sources [8,500 kB]
Get:8 http://deb.debian.org/debian bullseye/contrib Sources [43.2 kB]
Get:9 http://deb.debian.org/debian bullseye/main amd64 Packages [8,066 kB]
Get:10 http://deb.debian.org/debian bullseye/main Translation-en [6,235 kB]
Get:11 http://deb.debian.org/debian bullseye/contrib amd64 Packages [50.4 kB]
Get:12 http://deb.debian.org/debian bullseye/contrib Translation-en [46.9 kB]
Get:13 http://deb.debian.org/debian bullseye/non-free amd64 Packages [96.4 kB]
Get:14 http://deb.debian.org/debian bullseye/non-free Translation-en [92.5 kB]
Get:15 http://deb.debian.org/debian-debug bullseye-debug/main amd64 Packages [3,317 kB]
Fetched 26.6 MB in 15s (1,755 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

```



During module installation, the system may reboot multiple times. After each reboot, log in as root and re-run the installation script (`bash install_debian_modules.sh`) located in `/cus/Debian/`. If the customization scripts are removed during a reboot, re-mount `/dev/sr1` or `/dev/sr0` to `/cus/` to reload them.

### To install each package manually:

Install the packages by running:

```

apt -y update
apt -y install acl
apt -y install net-tools
apt -y install python3-dev
apt -y install python3-pip
apt -y install samba samba-client
apt -y install apache2
apt -y install openssh-client
pip3 install requests
pip3 install sh
pip3 install netifaces
pip3 install psutil
pip3 install tornado
pip3 install git

```

## 5. Build the custom Debian tracer

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

```
bash decoy_strace_installation.sh
```

The script will check your build environment before building the tracer.

```
root@debian:/cus/Debian# bash decoy_strace_installation.sh
Configuring for kernel release 6.1.0-37-amd64
Suggestion: consider configuring automatic debuginfo downloading via debuginfod.
The systemtap building environment is ready
The systemtap building environment is ready
\033[0;34mgoing to install update config files...\033[0m
cp: cannot stat '/etc/rsyslog.d/50-default.conf': No such file or directory
sed: can't read /etc/rsyslog.d/50-default.conf: No such file or directory
/cus/Debian
Truncating module name to 'vwmgfx'
```

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

```
Truncating module name to 'vwmgfx'
vwmgfx.ko
Kernel module build passed
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 linux-compiler-gcc-12-x86 linux-headers-6.1.0-37-common linux-kbuild-6.1
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
 linux-headers-6.1.0-37-amd64
0 upgraded, 0 newly installed, 1 to remove and 159 not upgraded.
After this operation, 3,931 kB disk space will be freed.
(Reading database ... 61792 files and directories currently installed.)
Removing linux-headers-6.1.0-37-amd64 (6.1.140-1) ...
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package linux-headers-6.1.0-37-amd64-common
E: Couldn't find any package by glob 'linux-headers-6.1.0-37-amd64-common'
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 linux-compiler-gcc-12-x86 linux-headers-6.1.0-37-common linux-kbuild-6.1
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
 linux-image-6.1.0-37-amd64-dbg
0 upgraded, 0 newly installed, 1 to remove and 159 not upgraded.
After this operation, 5,728 MB disk space will be freed.
(Reading database ... 55275 files and directories currently installed.)
Removing linux-image-6.1.0-37-amd64-dbg (6.1.140-1) ...
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
 linux-compiler-gcc-12-x86 linux-headers-6.1.0-37-common linux-kbuild-6.1
0 upgraded, 0 newly installed, 3 to remove and 159 not upgraded.
After this operation, 61.3 MB disk space will be freed.
(Reading database ... 50345 files and directories currently installed.)
Removing linux-compiler-gcc-12-x86 (6.1.153-1) ...
Removing linux-headers-6.1.0-37-common (6.1.140-1) ...
Removing linux-kbuild-6.1 (6.1.153-1) ...
Done!
root@debian:/cus/Debian#
```

## 6. Install the FDC toolkit

### To install the FDC toolkit:

1. Ensure the system customization is completed as expected.
2. Run the following command to check and install missing packages:  
`bash debian_cus_toolkit.sh`
3. Wait for the installation to finish. The system will reboot if there are no errors.

```

root@debian:/cus/Debian# bash debian_cus_toolkit.sh
\033[0;34mchecking sshd...\033[0m
OpenSSH_10.0p2 Debian-8, OpenSSL 3.5.4 30 Sep 2025
openssh server is installed
openssh version check passed
Failed to stop sshd.service: Unit sshd.service not loaded.
\033[0;34mchecking Python Env...\033[0m
Python 3.11.2
python3 is installed
python module check passed
python version check passed

Samba version 4.17.12-Debian
PID Username Group Machine Protocol Version Encryption Signing

Service pid Machine Connected at Encryption Signing

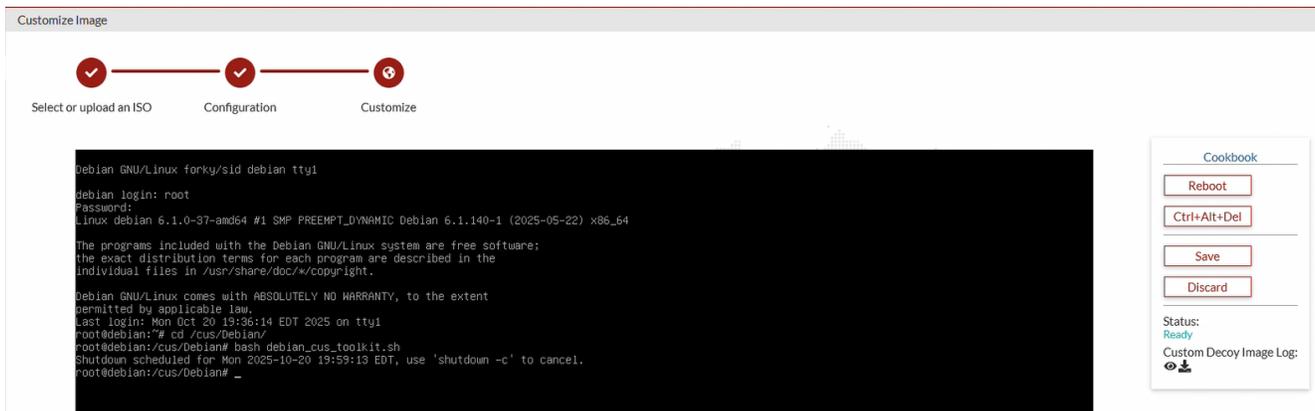
No locked files
No locked files
Samba version check passed
Server version: Apache/2.4.65 (Debian)
Server built: 2025-07-29T20:18:46
apache version check passed
/usr/bin/launcherD.py created successfully.
Created symlink /etc/systemd/system/default.target.wants/launcherD.service + /etc/systemd/system/launcherD.service.
Failed to stop ssh.service: Unit ssh.service not loaded.
Failed to stop sshd.service: Unit sshd.service not loaded.
mount: /dev/sr1: not mounted.
ssh,samba,http_v2,https_v2,git
{ 'version': '1.0', 'status': '1', 'log': 'Installation successful, supported services: ssh,samba,http_v2,https_v2,git', 'cpu_name': 'Intel Core i7 9xx (Nehalem
Class Core i7)', 'os': 'debian', 'services': ['ssh', 'samba', 'http_v2', 'https_v2', 'git']}
<http.client.HTTPResponse object at 0x7f25a1143040>

```

## 7. Save the custom Image

### To save the custom image:

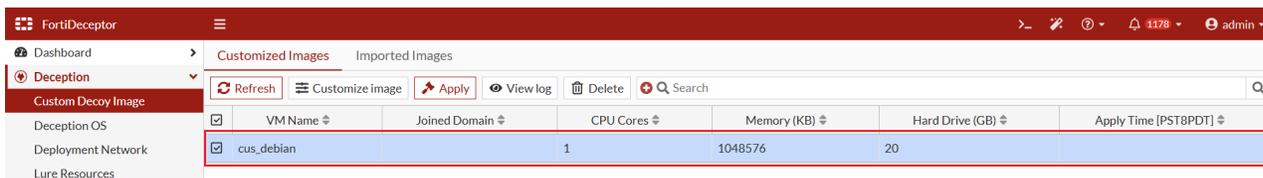
1. In the FortiDeceptor GUI, verify the image *Status* is *Ready*.
2. Install the FDC toolkit again with command: `bash debian_cus_toolkit.sh`
3. Click *Save* when the system is powered off.



## 8. Review the result

To review the result:

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

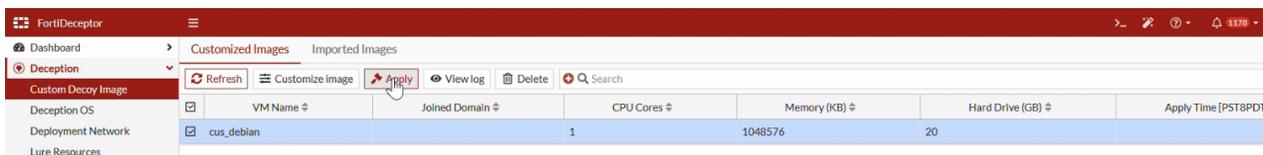


2. (Optional) Click the *Delete* button to remove the custom image.

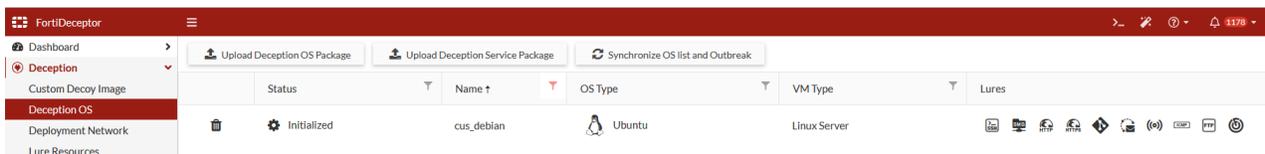
## 9. Apply the custom images

To apply a custom image:

1. In FortiDeceptor, go to *Deception > Customization > Customized Images*.
2. Select a customized image and click *Apply*.



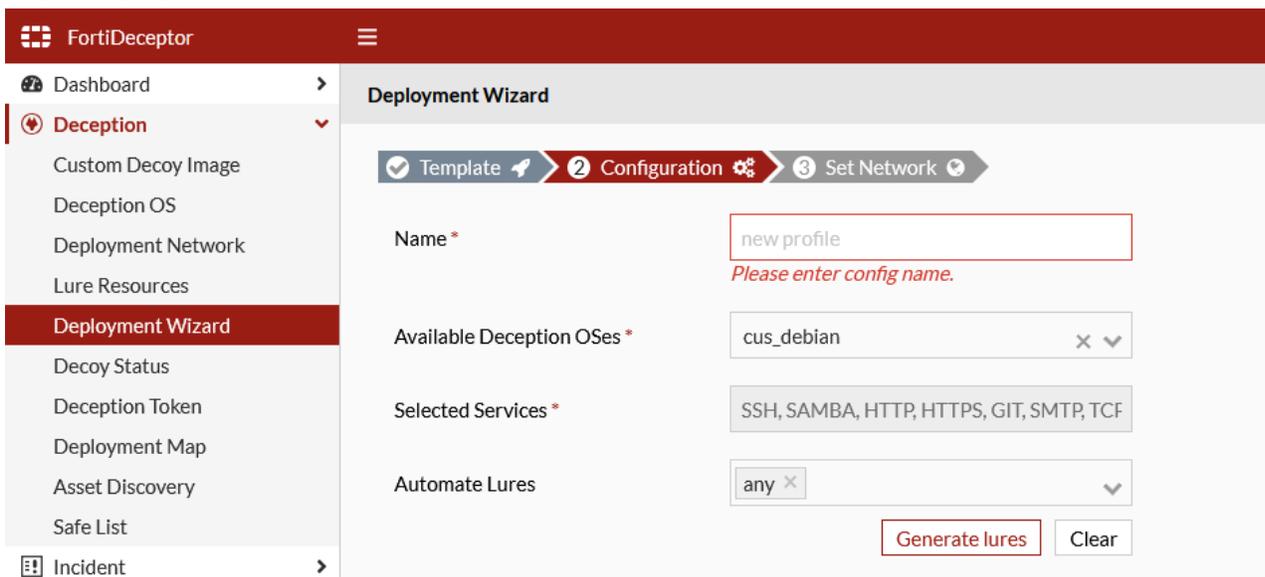
The applied image is displayed in the *Deception OS* page. It may take several minutes for the image to appear in the table.



## 10. Deploy decoys with custom Debian images

To deploy decoys with a custom Debian image:

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





[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 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 Chief Legal Officer, 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.