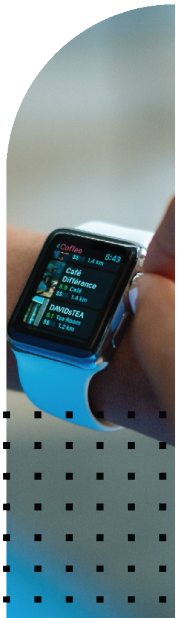
FortiDeceptor Customizaiton Guide

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

Ocotber 7, 2025
FortiDeceptor 6.2.0 FortiDeceptor Customizaiton Guide
50-520-948429-20251007

TABLE OF CONTENTS

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:

<table>
<tr><th>OS</th><th colspan="3">OS version</th></tr>
<tr><td>Windows</td><td>Language</td><td>Supported versions</td><td>Notes</td></tr>
<tr><td></td><td>English</td><td>Windows 10</td><td>Supports custom MSSQL</td></tr>
<tr><td></td><td></td><td>Windows 11 version 23H2</td><td>• Supports custom MSSQL
• FortiDeceptor v6.1.0 does not support Windows 11 version 24H2.</td></tr>
<tr><td></td><td>French</td><td>Windows 10</td><td>Supports custom MSSQL</td></tr>
<tr><td>Windows Server</td><td>Language</td><td>Supported versions</td><td>Notes</td></tr>
<tr><td></td><td>English</td><td>• Windows Server 2016
• Windows Server 2019
• Windows Server 2022</td><td>• Supports custom MSSQL
• Supports custom IIS Service</td></tr>
<tr><td></td><td>French</td><td>French Windows Server 2016</td><td>• Supports custom MSSQL
• Supports custom IIS Service</td></tr>
<tr><td>RedHat Enterprise Linux</td><td colspan="3">• RedHat Enterprise Linux 7.9
• RedHat Enterprise Linux 8.8
• RedHat Enterprise Linux 8.10
• RedHat Enterprise Linux 9.4
• RedHat Enterprise Linux 9.6</td></tr>
</table>

OS	OS version
Ubuntu	• Ubuntu 20.04
Debian	• 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

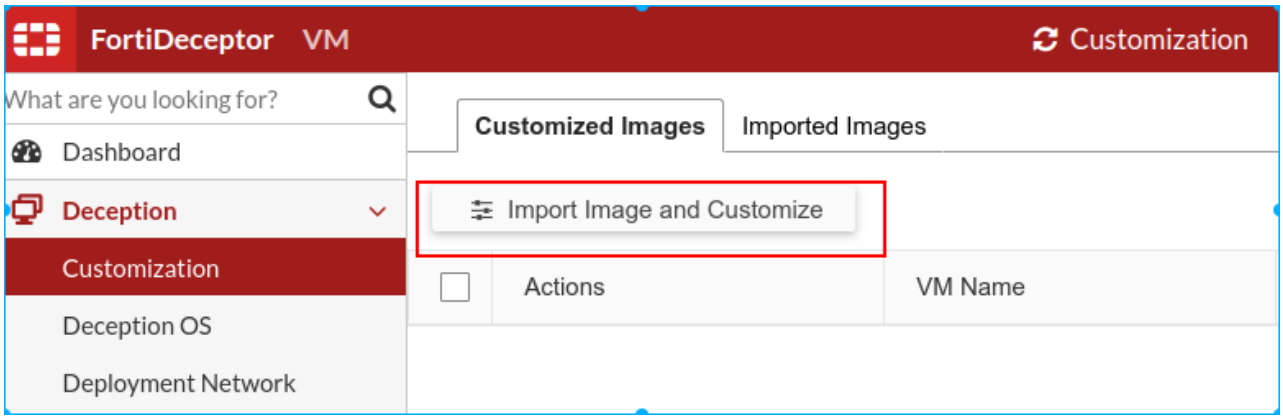
- The FortiDeceptor Custom Decoy Subscription bundle for FDC1000G, FDR100G, FDC-VMS, includes the custom decoy feature and does not require a license.
- The FortiDeceptor Custom Decoy license is required for the old perpetual license for FDC-VM and FDC1000F. This license is no longer being sold but is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

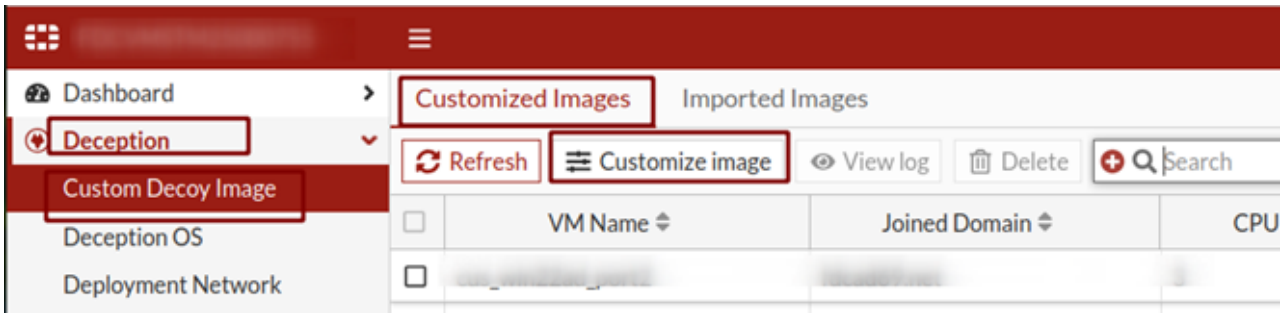
1. Go to *Deception* > *Custom Decoy Image* > *Customized Images*.
2. Click *Customize Image*.



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:

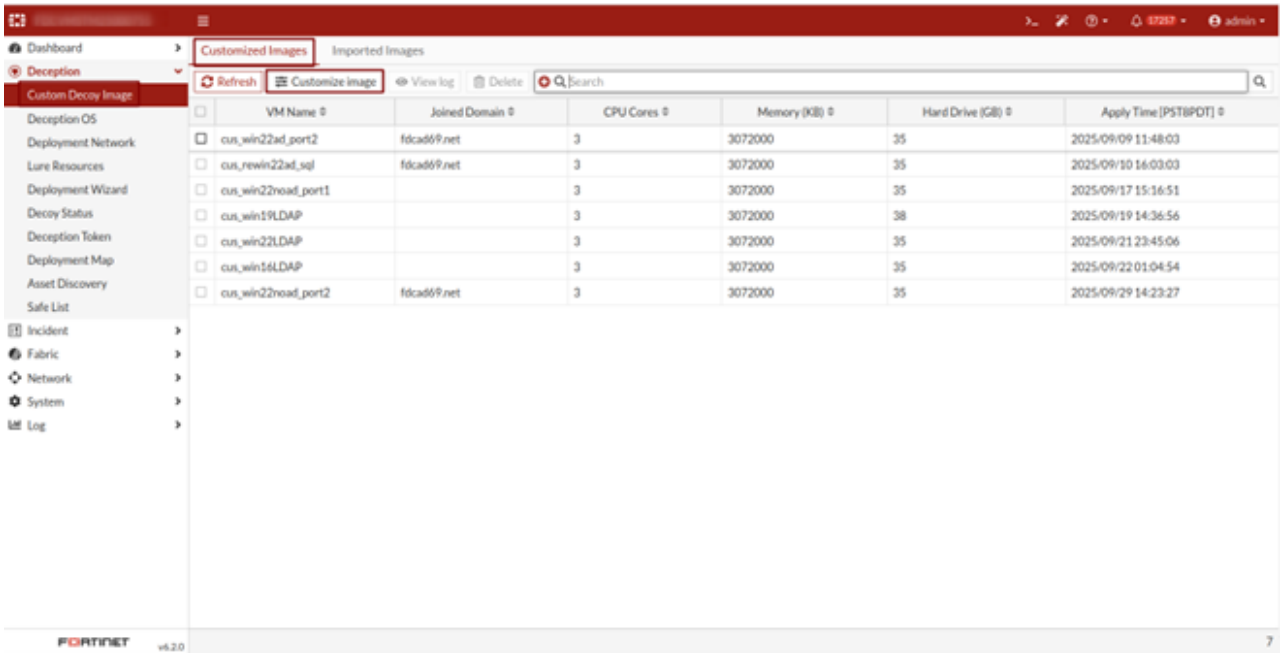
1. Go to *Deception* > *Customization* > *Customized Images*.
2. Click *Import Image and Customize*.
3. Choose an ISO image and click *Delete*.

3. (Optional) Re-customizing existing images

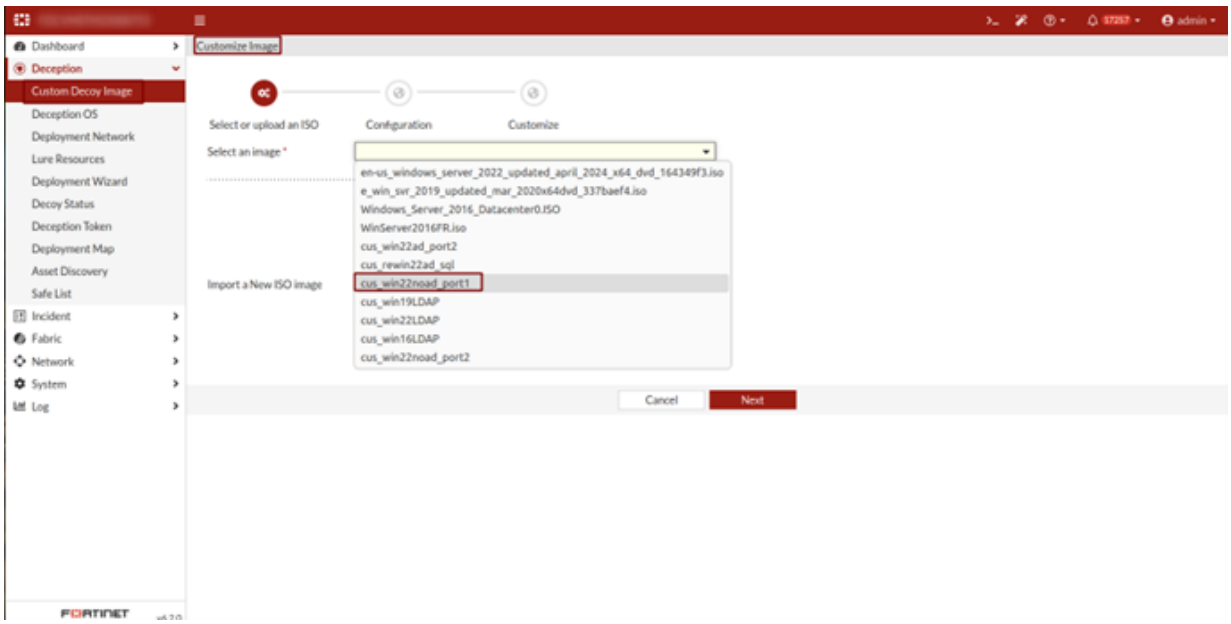
You can update customized images to expand the virtual hard disk (HDD) or apply new configurations.

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.



-

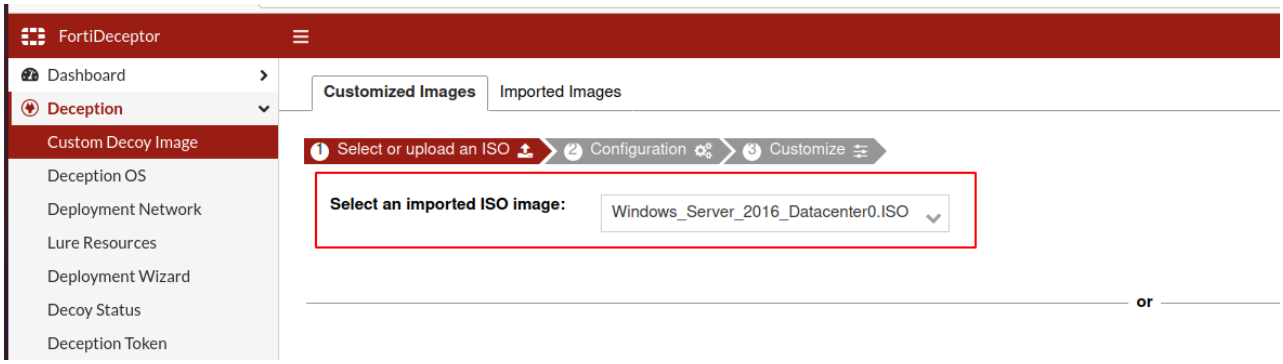
It may take more than 10 minutes for the VNC to load. Please do not customize another image during this process.

Windows OS

1. Initialize the OS instance

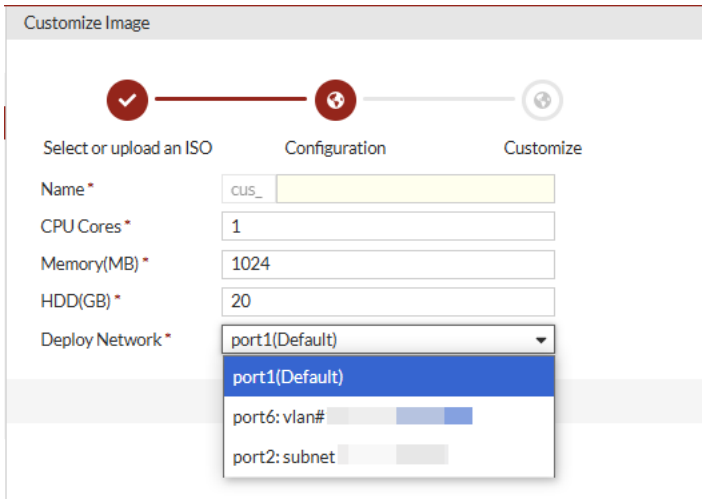
To initialize the OS instance:

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

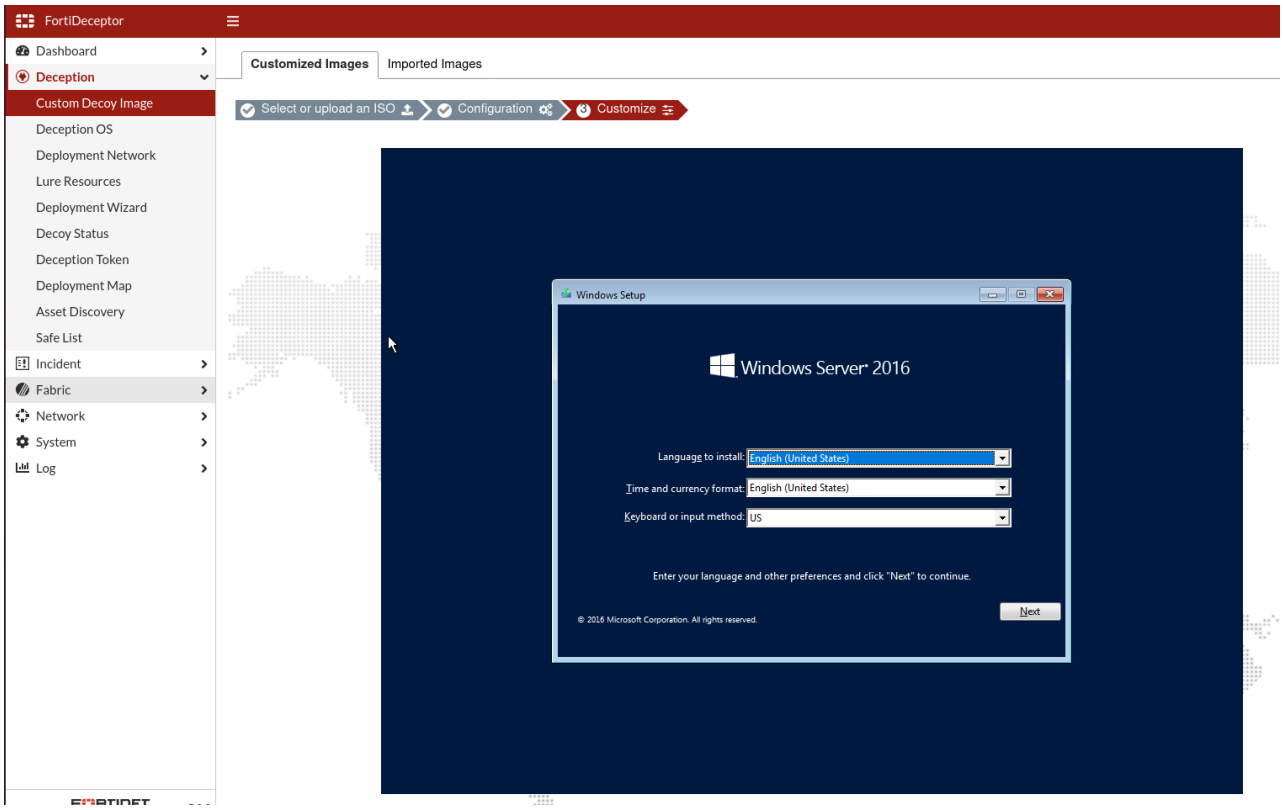


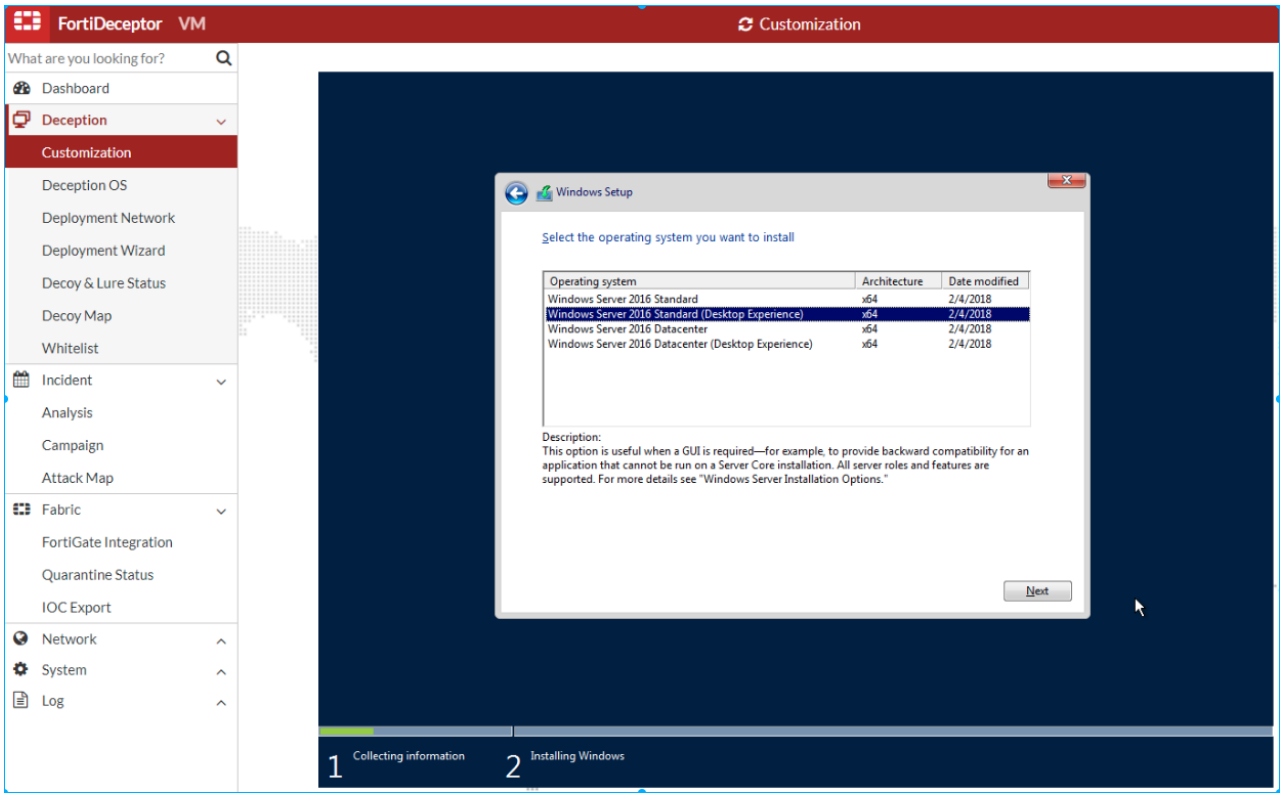
3. Choose an ISO image and click *Next*.
4. Configure the following settings and click *Next*.

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: • IP/Mask • Gateway • DNS



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



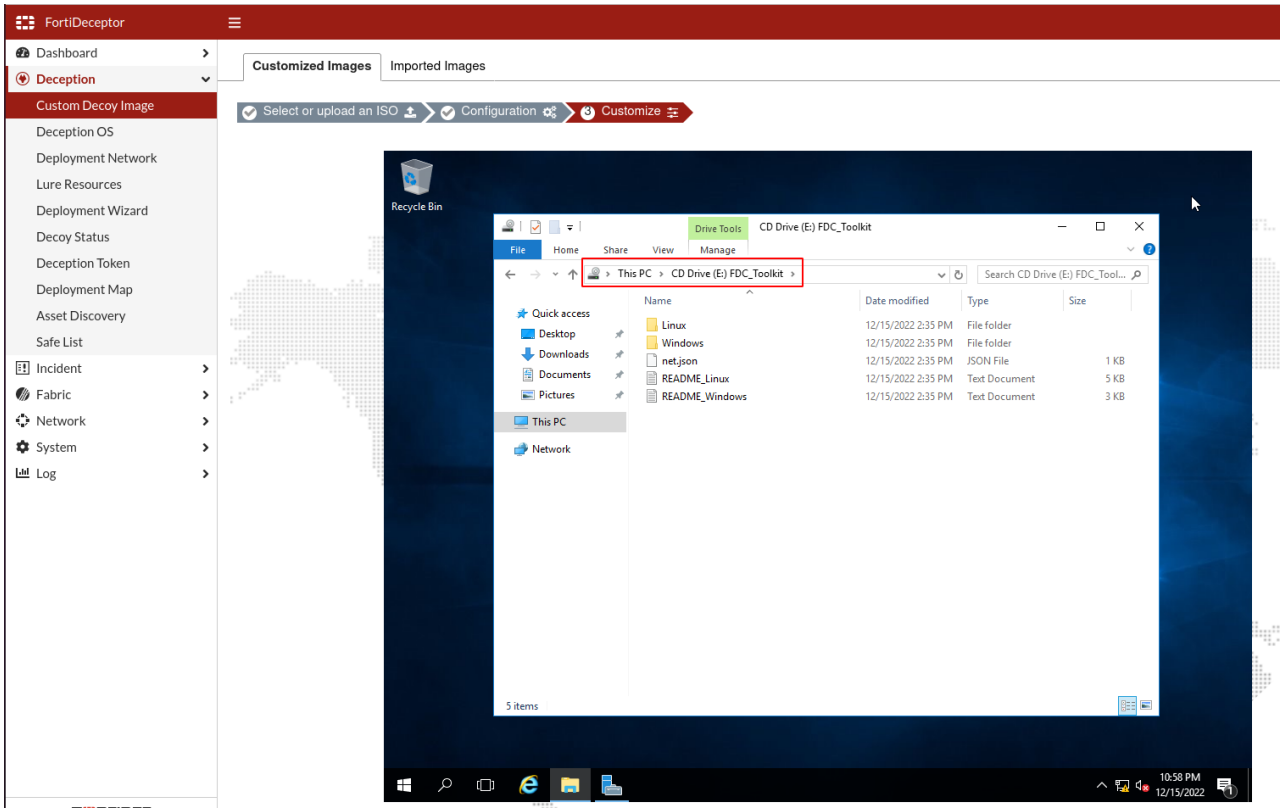


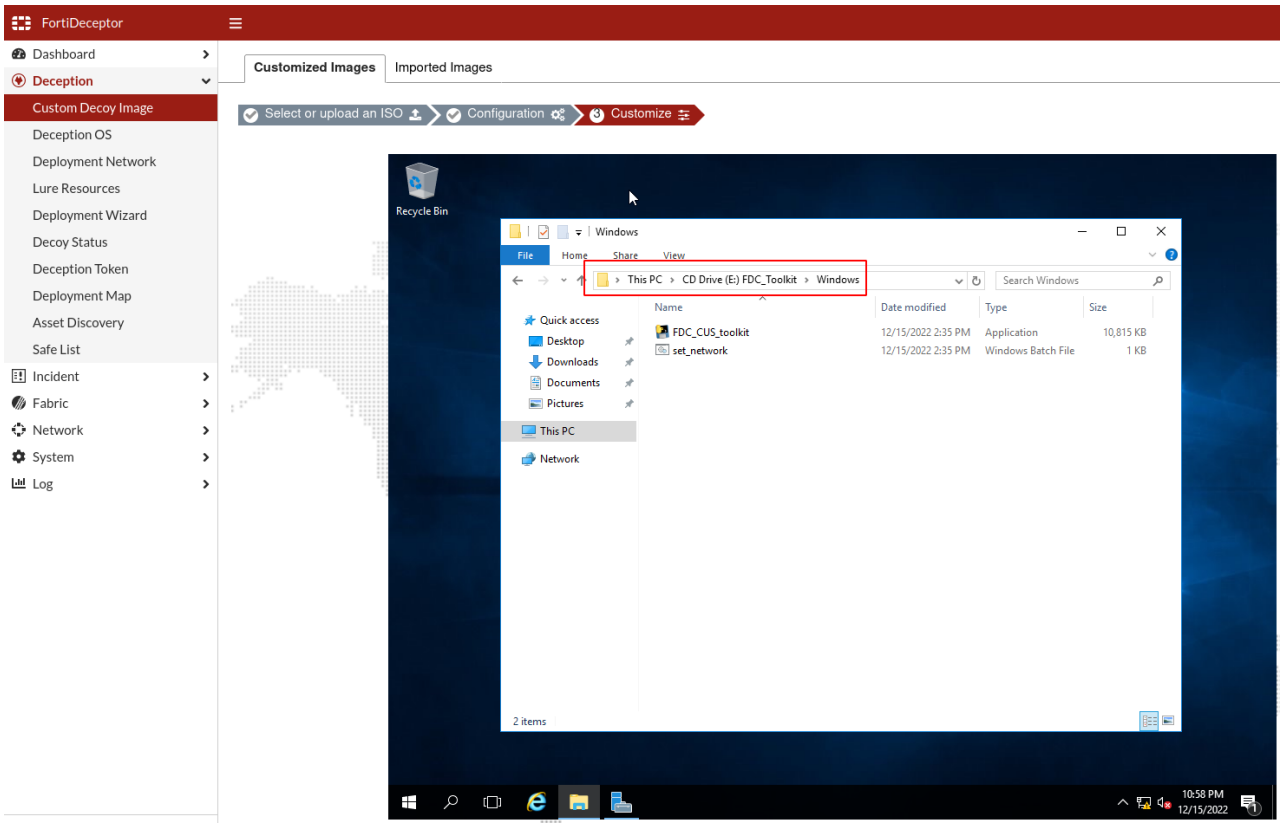
2. Customize the OS

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*.

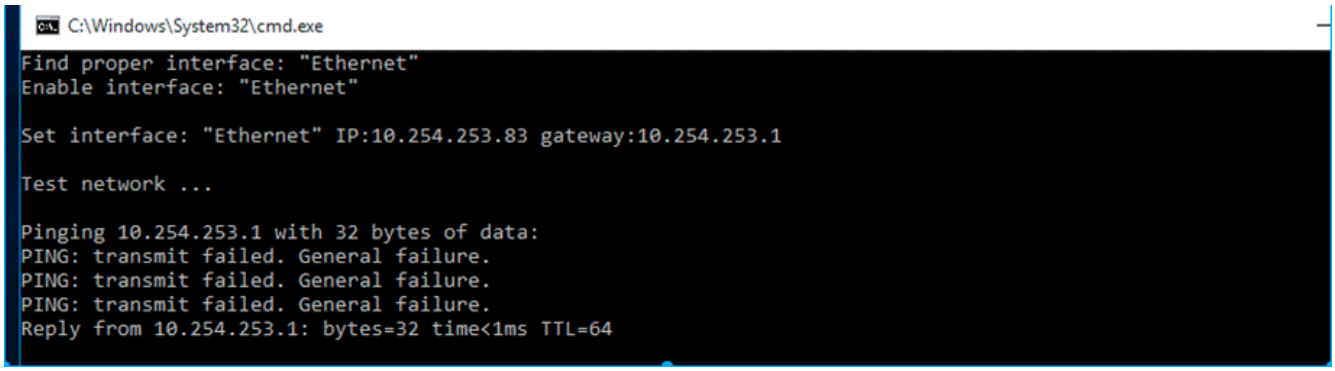




2. Review and follow the guide in file `toolkit_README.txt`.

To configure the network:

To customize/configure	Description
Windows 10/11, French Windows10 OS	Right-click the file named `set_network.bat`, and choose *Run as Administrator*.
Windows server 2016/2019/2022, French Windows server 2016 OS	Double click it to run it directly if you logged on as *Administrator*.
IP, gateway and DNS	In Windows, go to *Control Panel* > *Network and Internet* > *Network Connections*. Follow the settings in file named `net.json` to configure the IP, gateway, and DNS.



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.

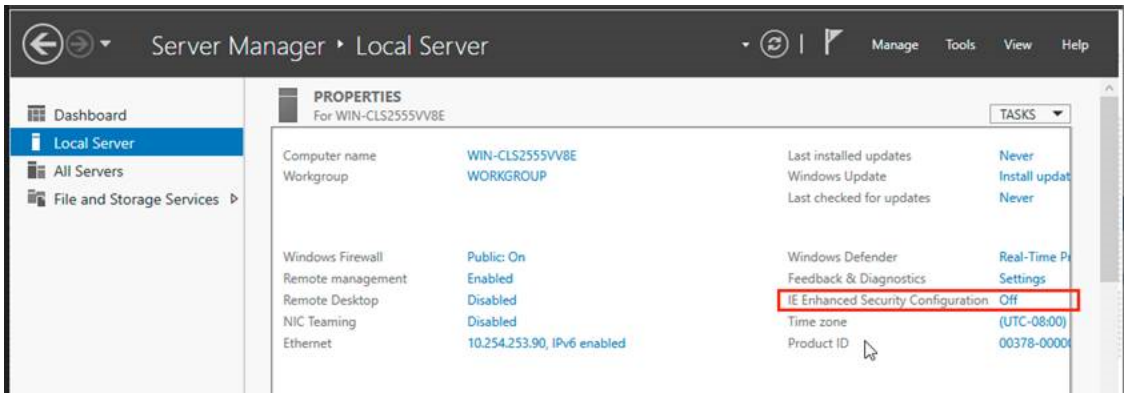
3. (Optional)Install the Microsoft SQL Server

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*.

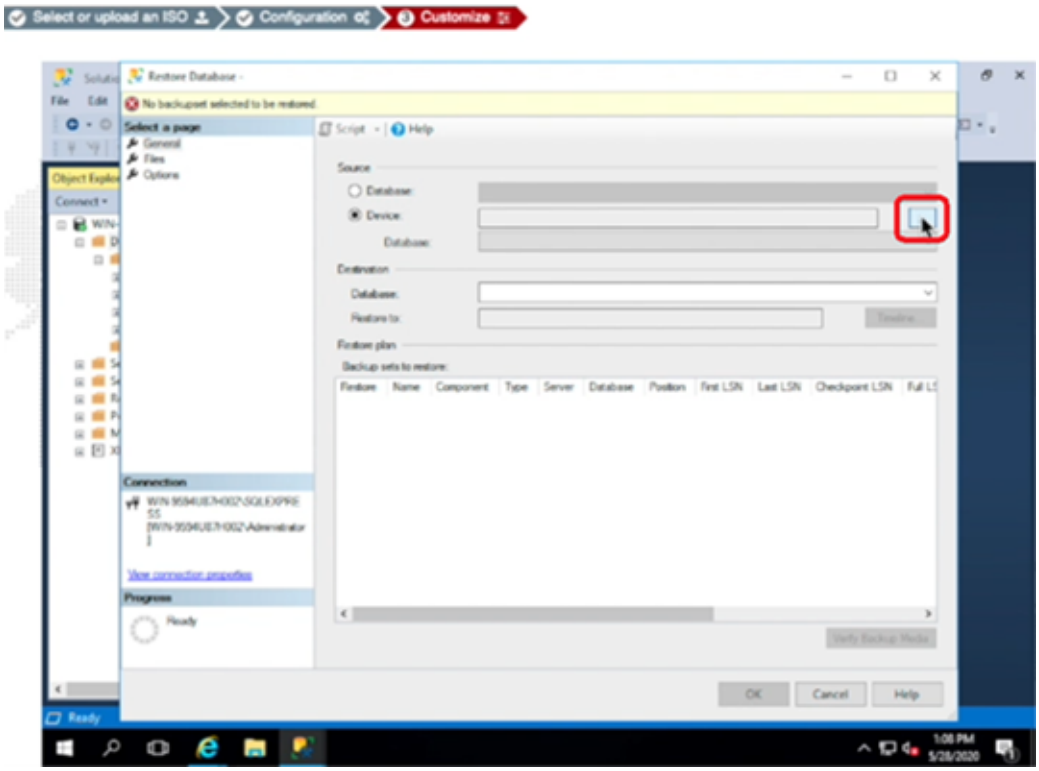


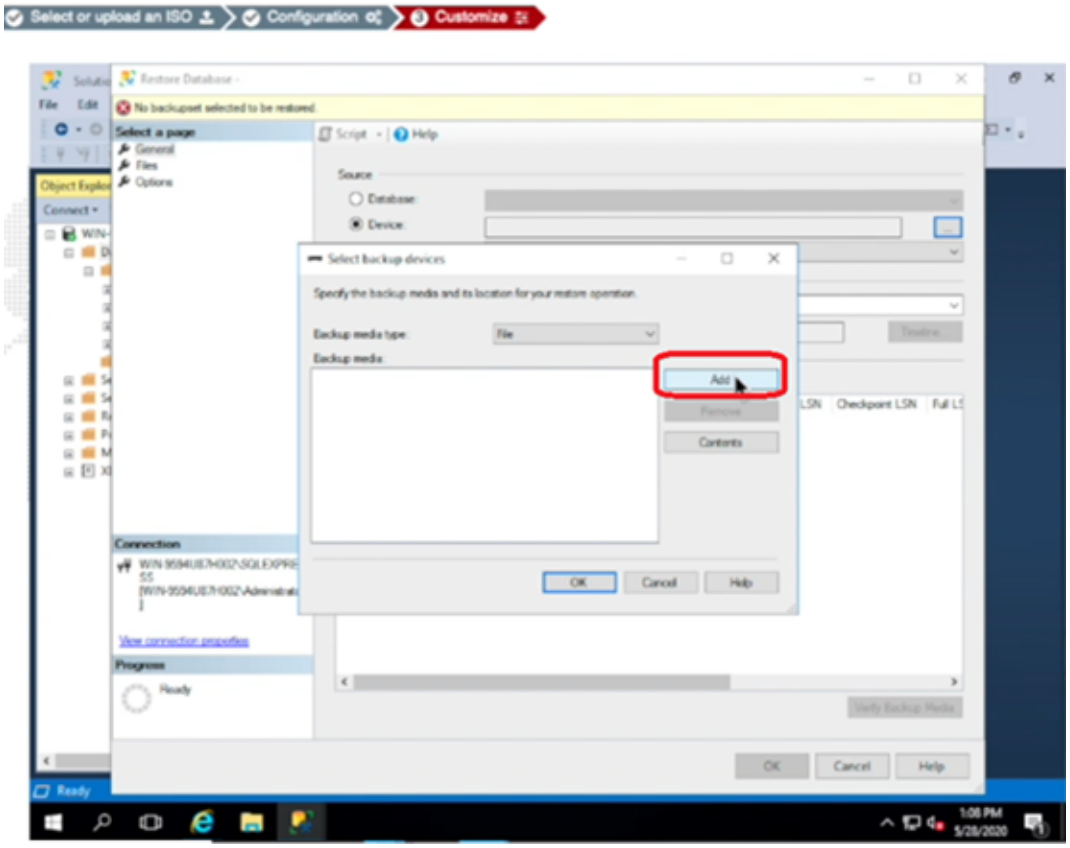
- For Windows Server Core OS, you need to download the installation file onto another computer, and copy the installation file to Server Core OS over SMB service.

To install the Microsoft SQL Server:

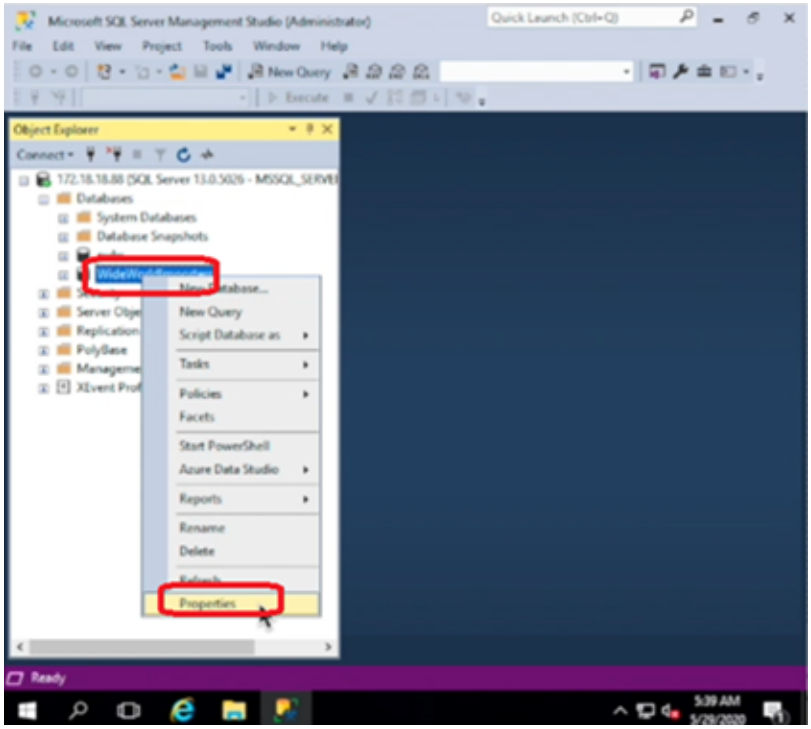
1. Download and install Microsoft SQL Server.
2. When SQL server installation finished, click *Install SSMS* to download and install the SQL server management studio for SQL server management and customization.
3. Download a database sample from this repository: https://github.com/Microsoft/sql-server-samples/releases/download/wide-world-importers-v1.0/WideWorldImporters-Full.bak
4. Open the SQL management studio software on your windows server from the FortiDeceptor "*decoy customization*" console.
5. 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*.

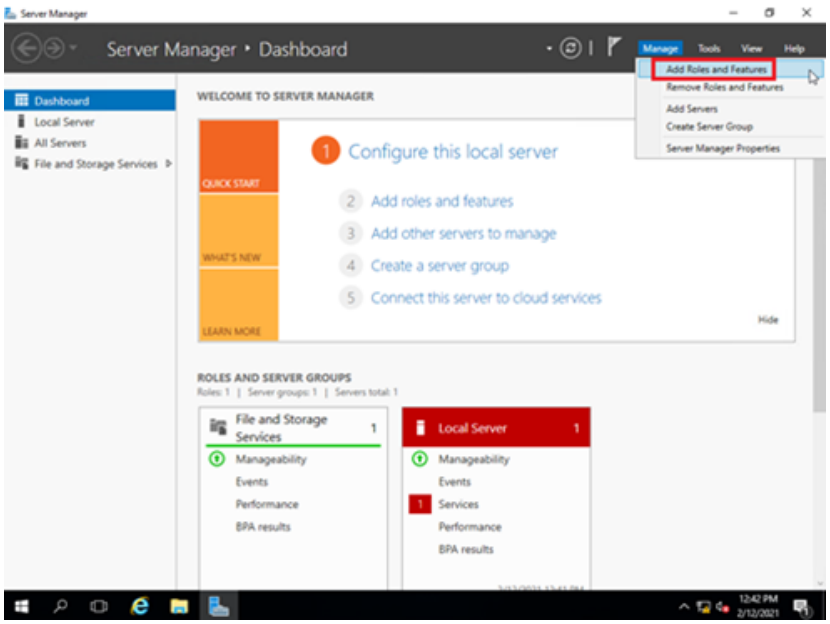
4. (Optional) Install the Internet Information Service (IIS)

The following versions are supported:

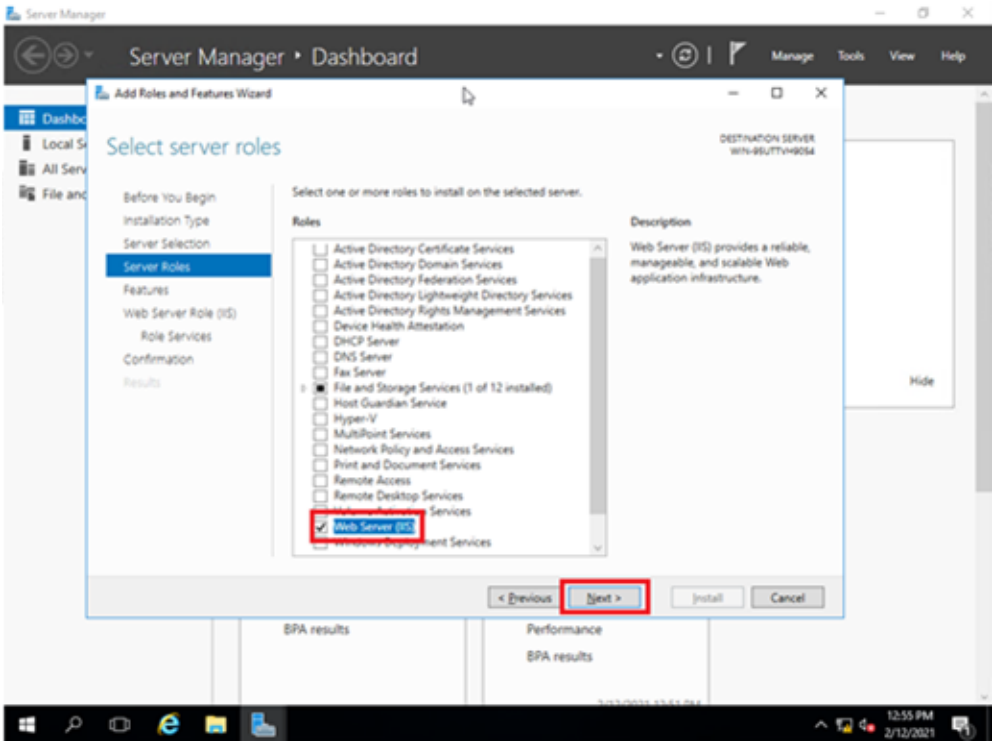
- IIS 10 on Server 2016
- IIS 10 on Server 2019
- IIS 10 on Server 2022
- IIS 10 on French Windows Server 2016

To add IIS role and service:

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

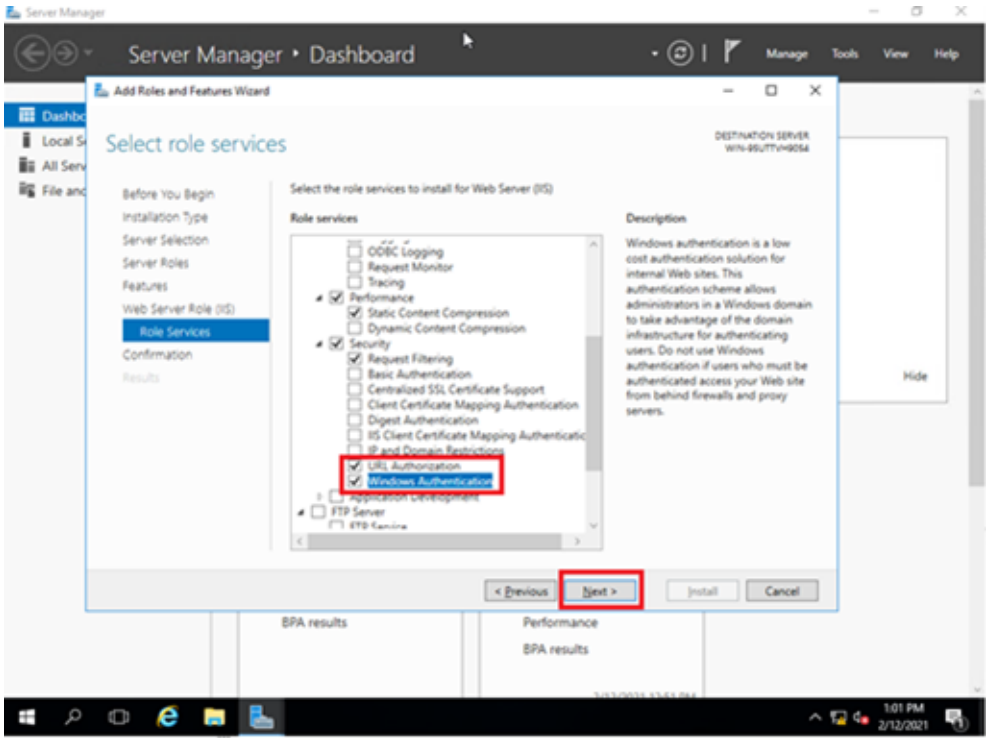


3. On the *Before you begin* page, click *Next*.
4. On the *Installation Type* page, click *Next*.
5. On the *Server Selection* page, click *Next*".
6. In the *Select server roles* diaglog, select *Web Server (IIS) > Add Features*, and click *Next*.

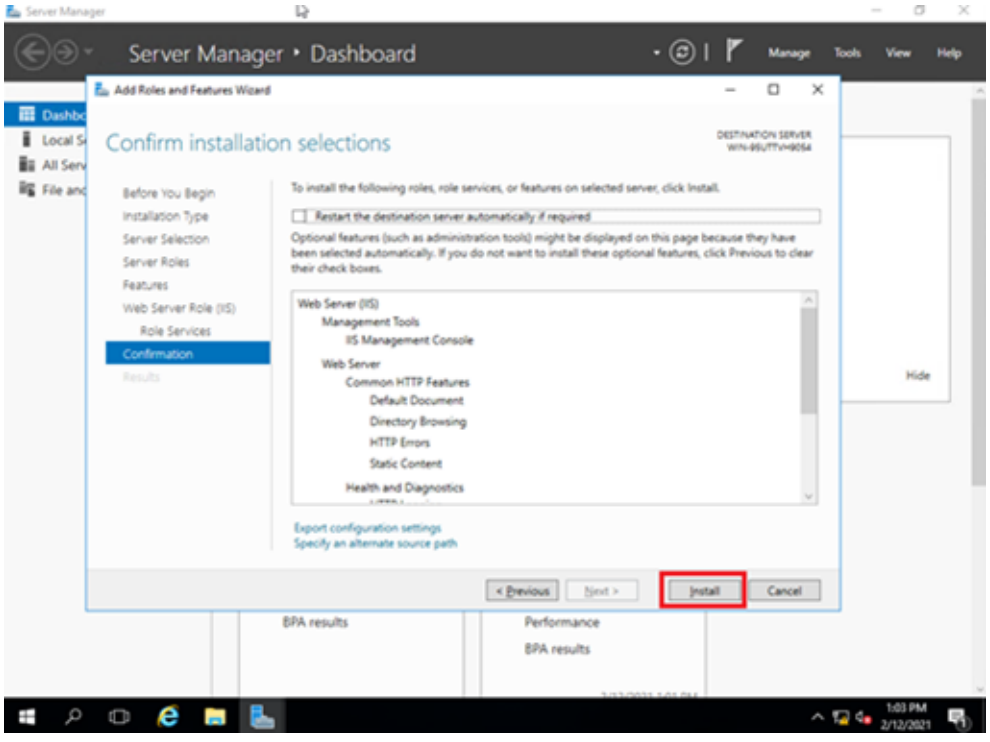


7. On the *Select Features* page, click *Next*.
8. On the *Web Server Role (IIS)* page, click *Next*.

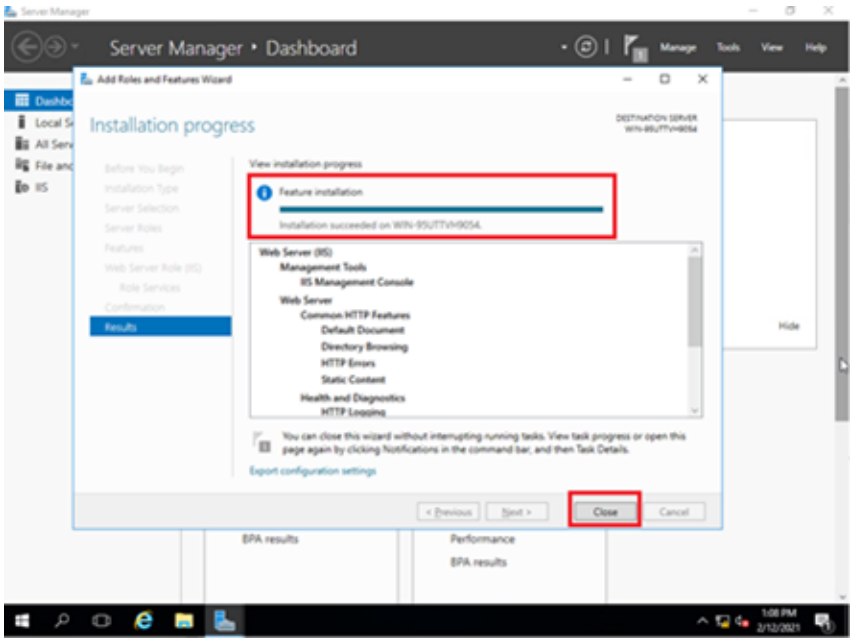
9. On the *Role Services* page, select *URL Authorization* and *Windows Authentication* then click *Next*.



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



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

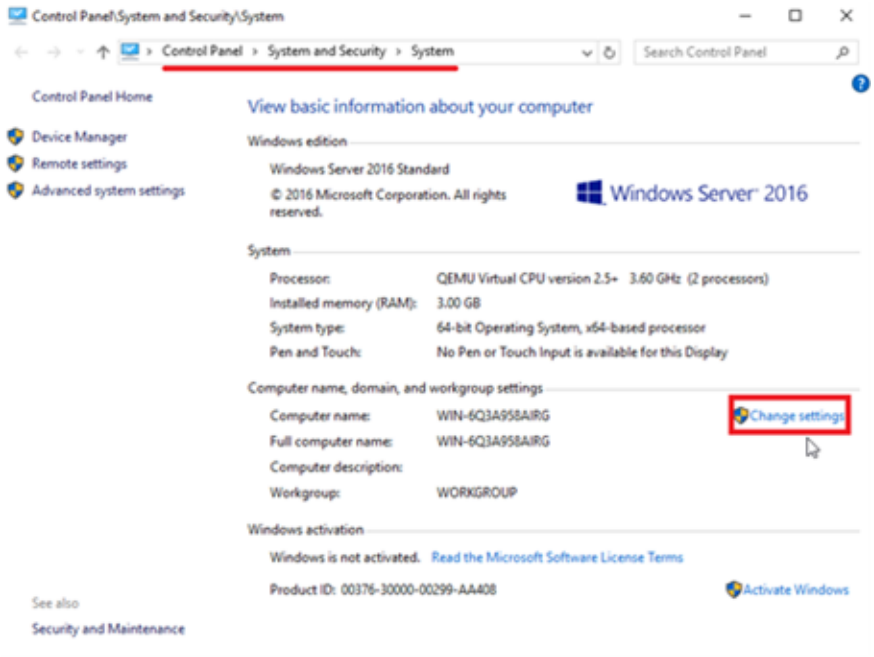


5. (Optional) Join a domain

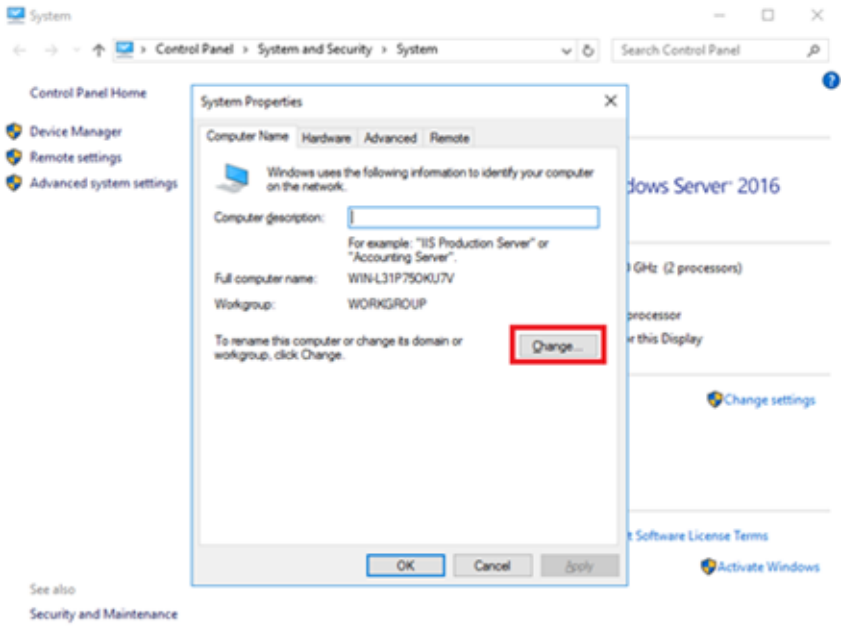
Before you join the customized windows OS to a domain, its DNS server should be changed to the DNS server of the domain. Otherwise, it will fail.

To join a domain:

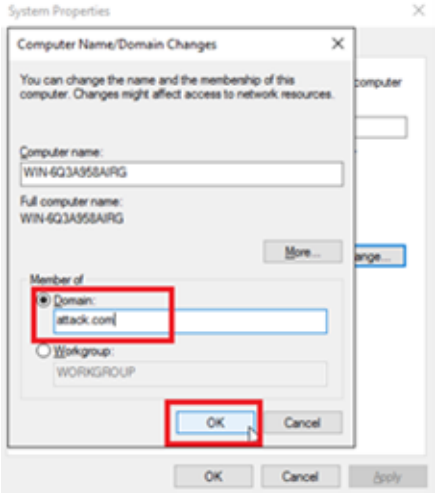
1. Go to *Control Panel > System*, and click *Change settings*.



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



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

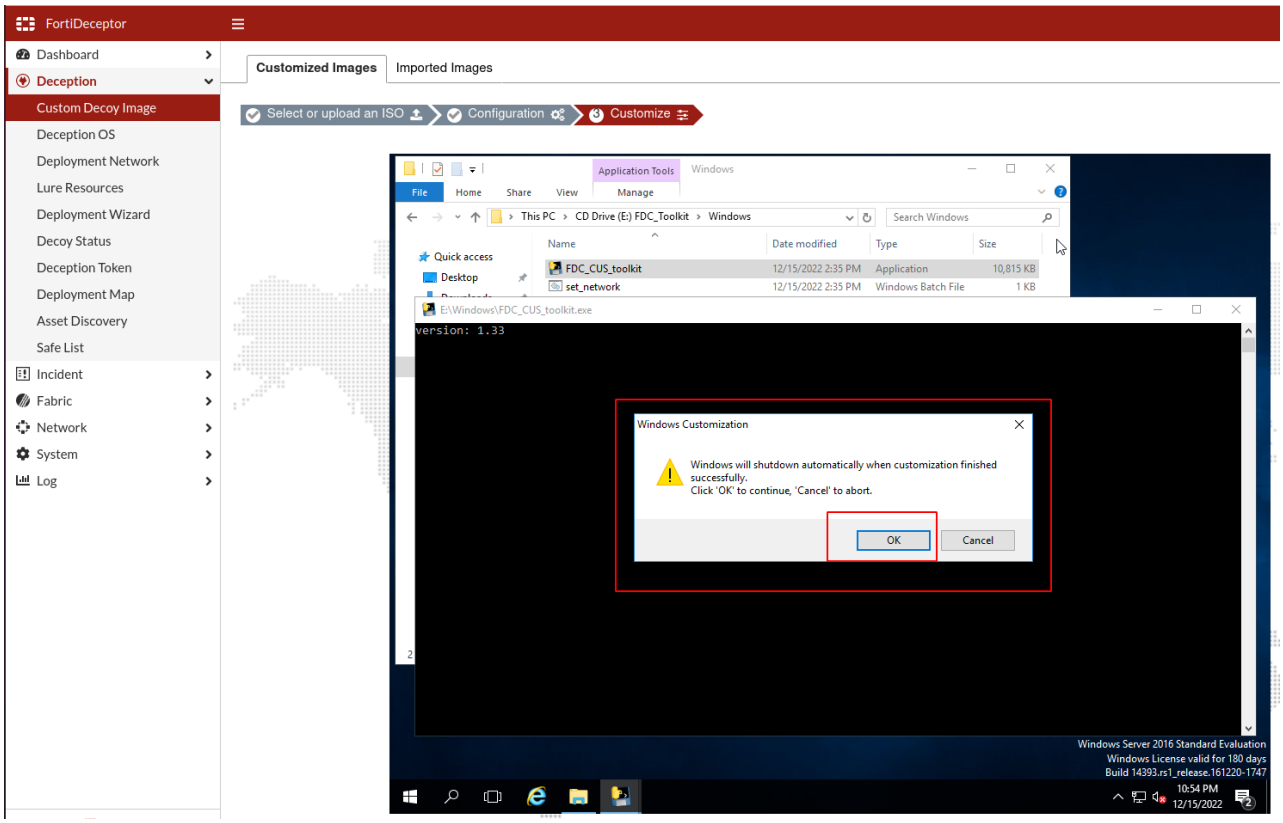


4. Input the domain account, click *OK*.
5. After joining the domain, a restart is required, click *Close*.
6. Click *Restart now*.
7. After Windows restarts, sign on as a local Administrator.

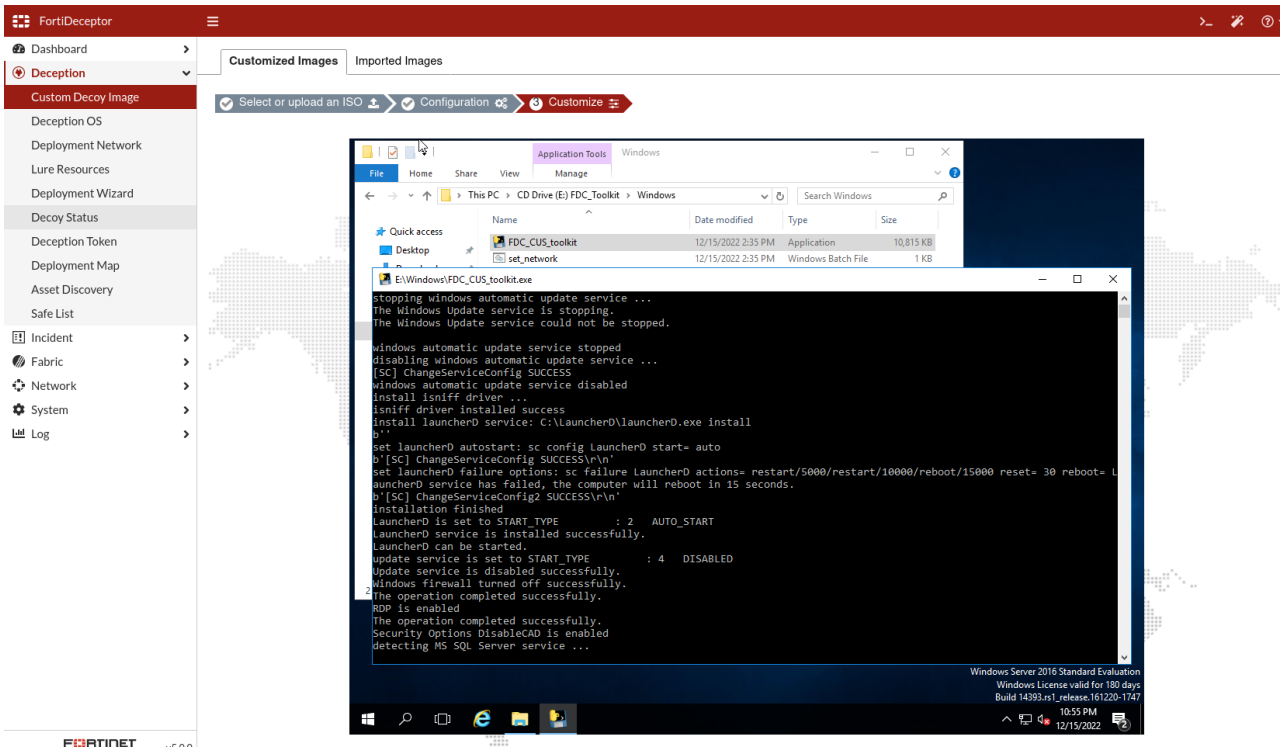
6. Install the FortiDeceptor customization toolkit

To install the customization toolkit:

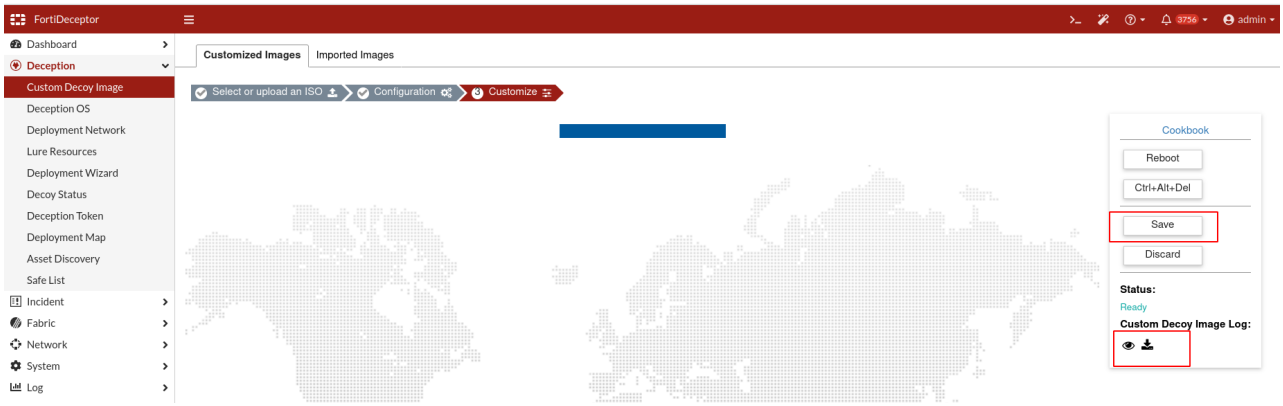
1. After you are finished customizing the image, right-click the file `FDC_CUS_toolkit.exe`, and select *Run as Administrator*. The warning message *Windows will shut down automatically when customization finished successfully*, appears.



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



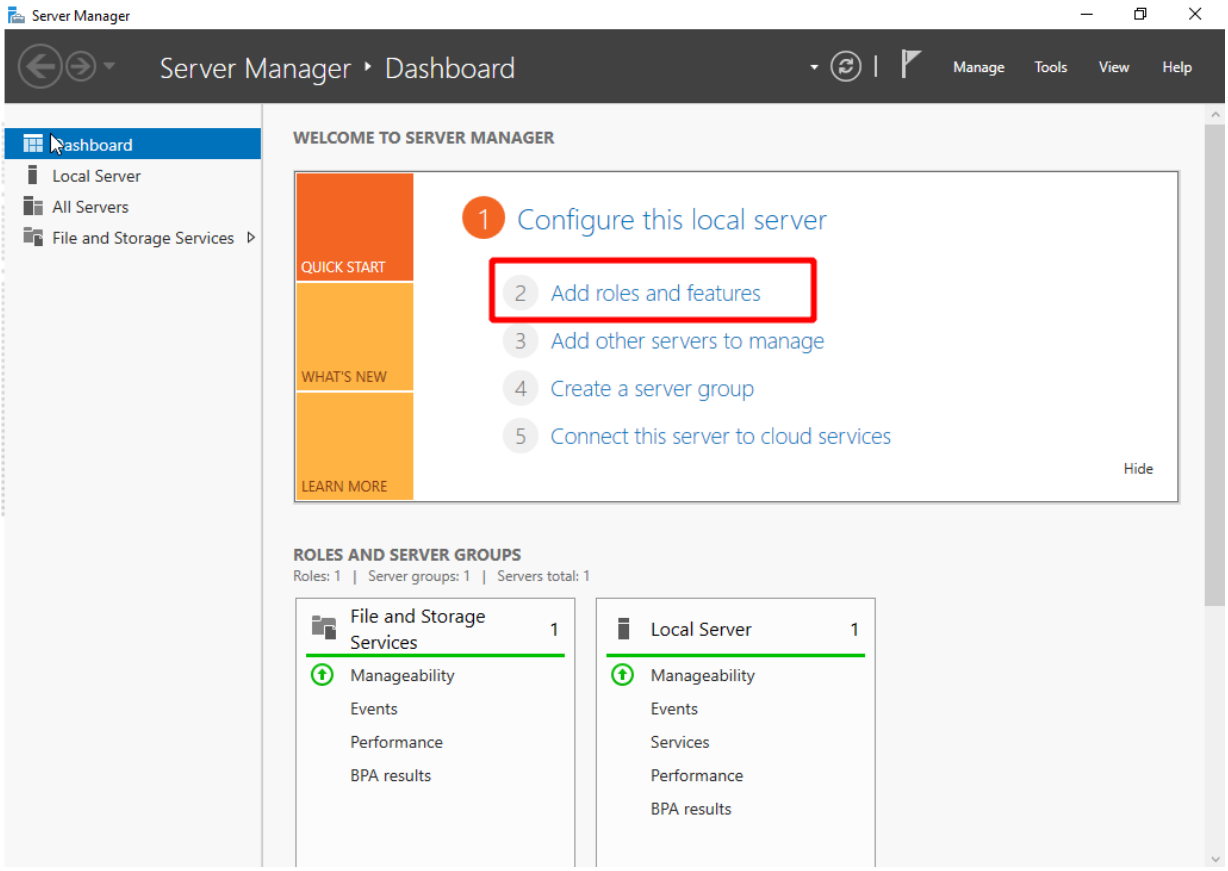
3. After the toolkit is installed, click *Save*. You can also *View* or *Download* the *Custom Decoy Image Log*.



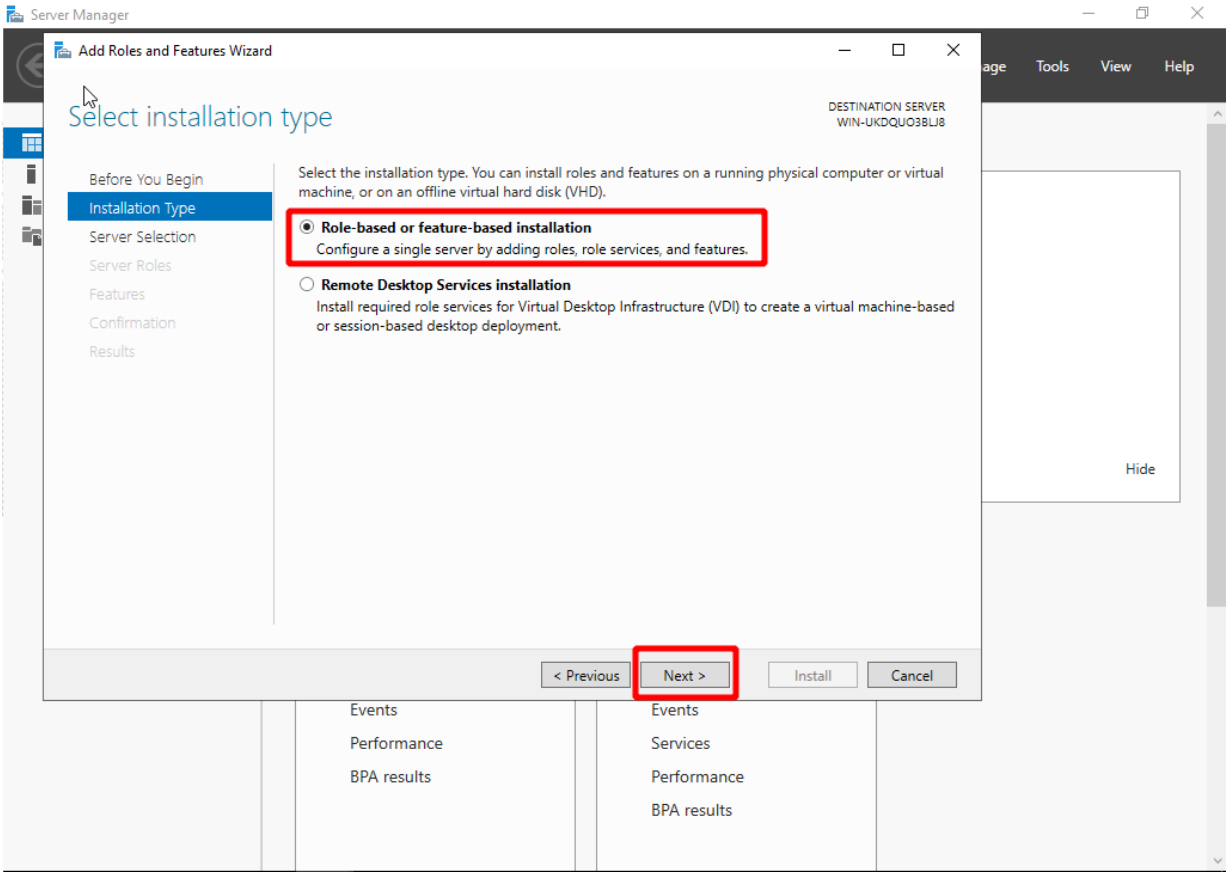
7. (Optional) Turn on Active Directory (AD) controller

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*.

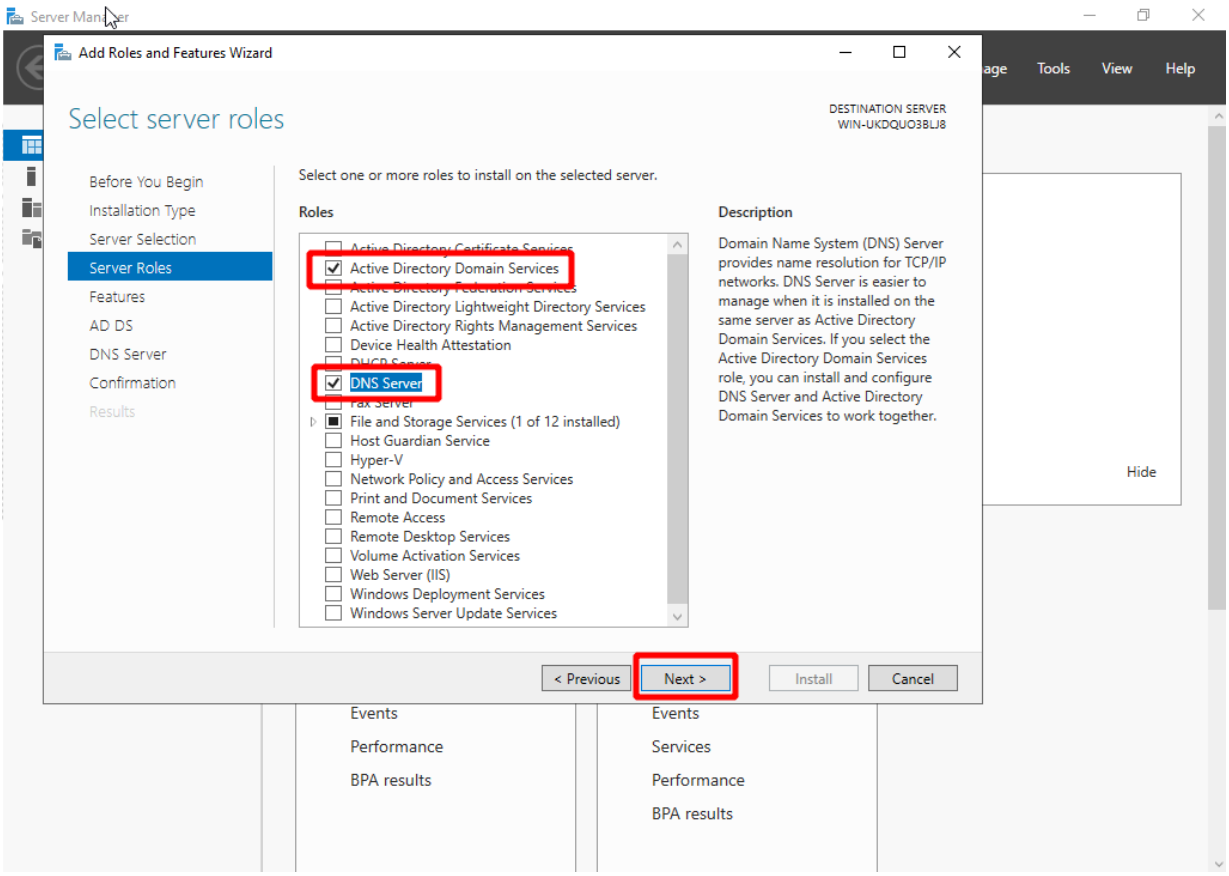


b. Select *Role-bases or Feature-based installation*.

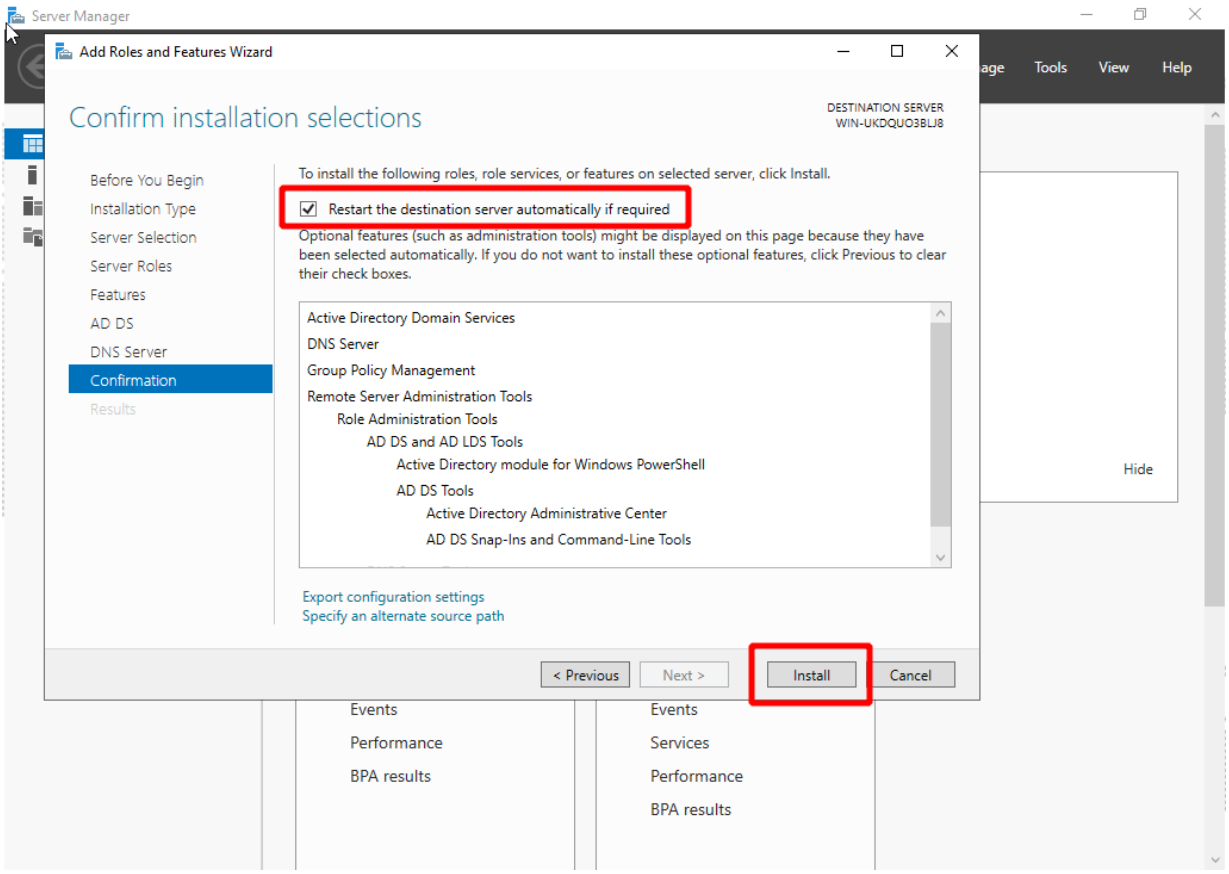


c. Click *Server Role* and select *Active Directory Domain Services* and click *Next*.

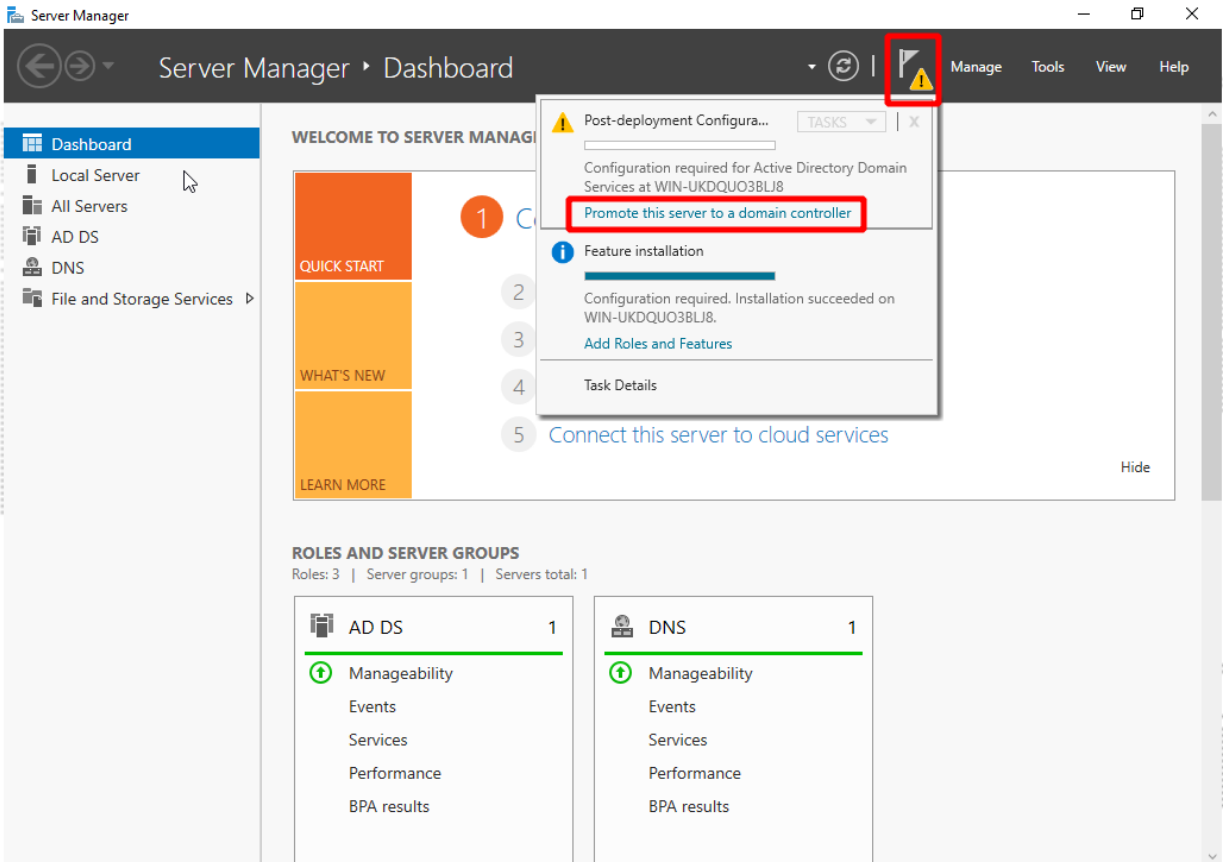
The DNS Server role is no longer supported in the version 6.2 GA. For domain name resolution, use a standalone third-party DNS server, such as a Linux-based dnsmasq server or a Windows DNS server hosted on a separate machine.



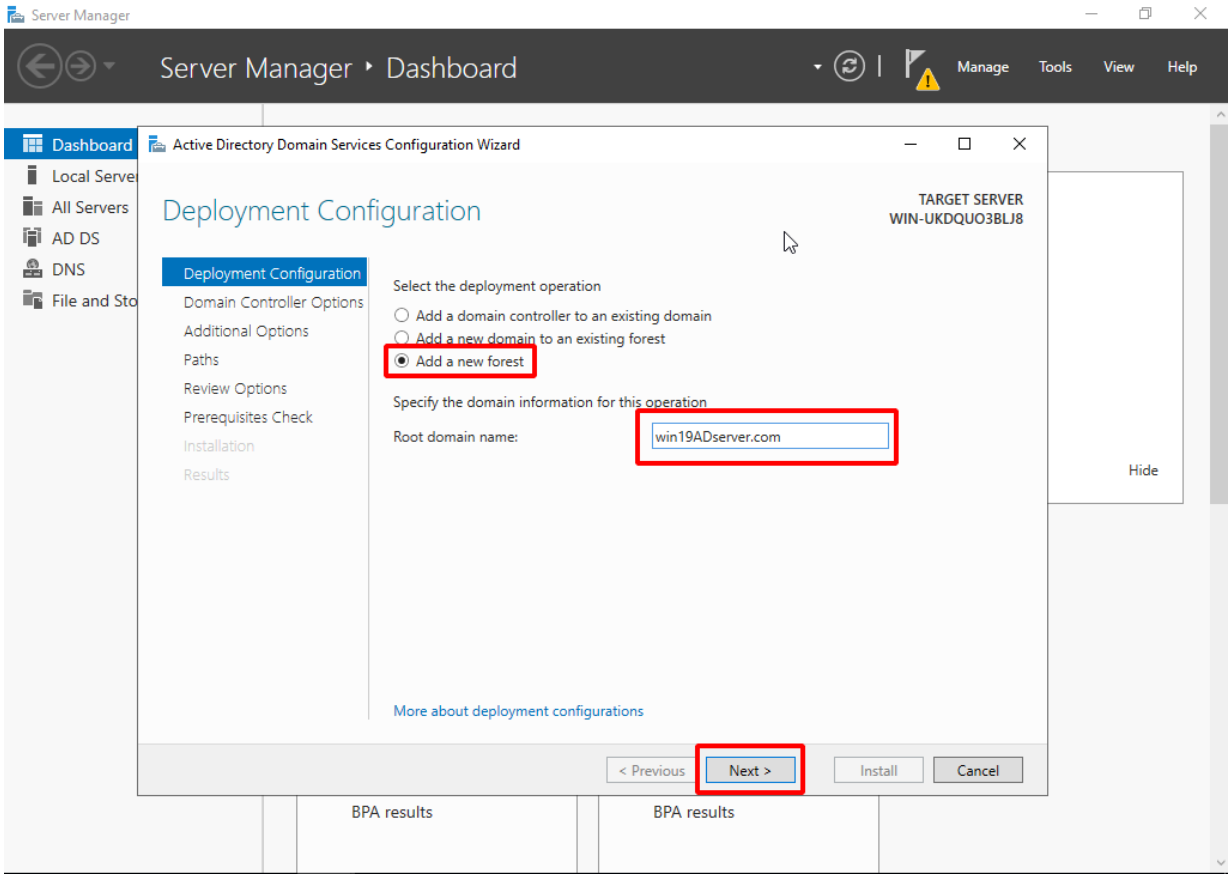
d. Keep clicking *Next* until you reach the *Confirmation* page. Select *Restart the destination server automatically if required*, and click *Install*.



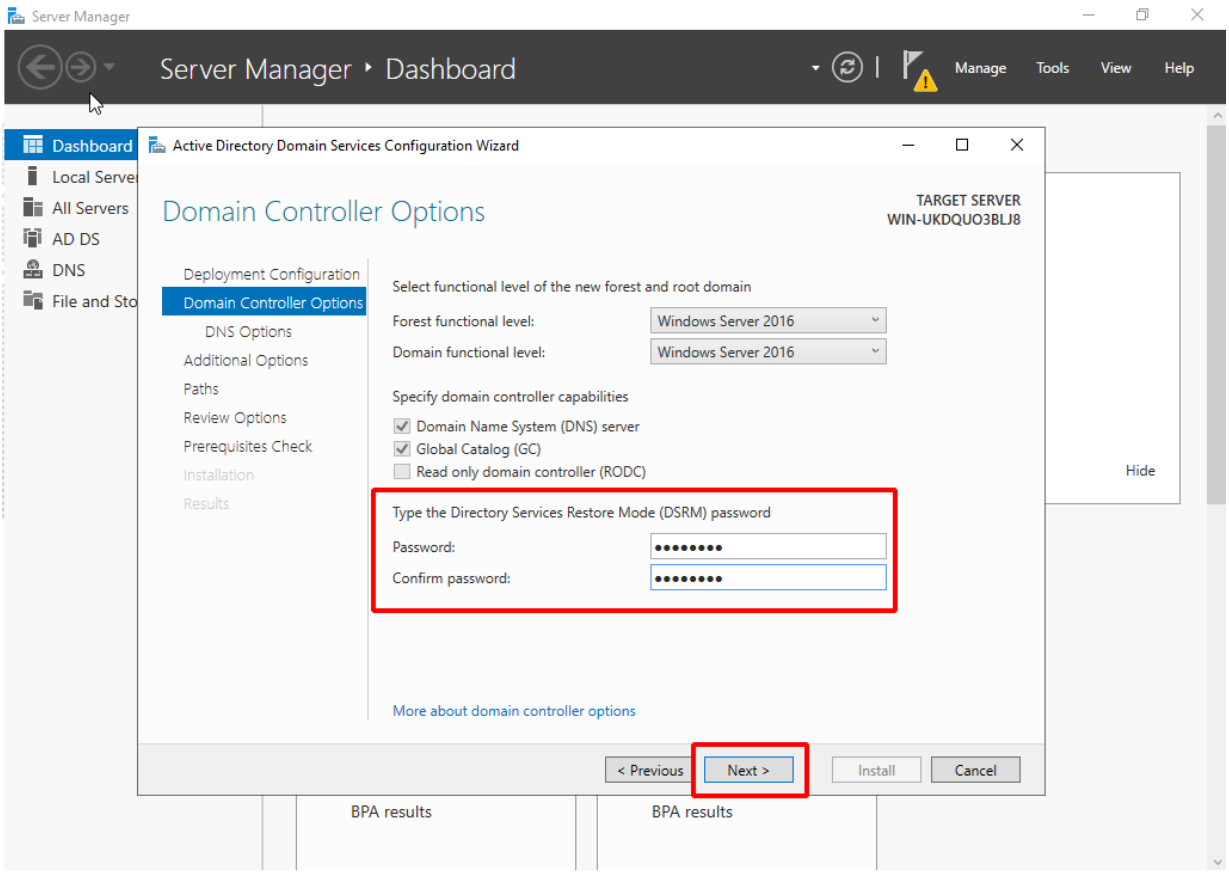
2. Promote the server into a domain controller.
   a. Click the notification flag next to the *Manage* menu and click *Promote this server to a domain controller*. The configuration wizard opens.


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGE
QUICK START
WHAT'S NEW
LEARN MORE
1
2
3
4
5
Connect this server to cloud services
Hide
Post-deployment Configura...
TASKS
Configuration required for Active Directory Domain Services at WIN-UKDQUO3BLJ8
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on WIN-UKDQUO3BLJ8.
Add Roles and Features
Task Details
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS 1
Manageability
Events
Services
Performance
BPA results

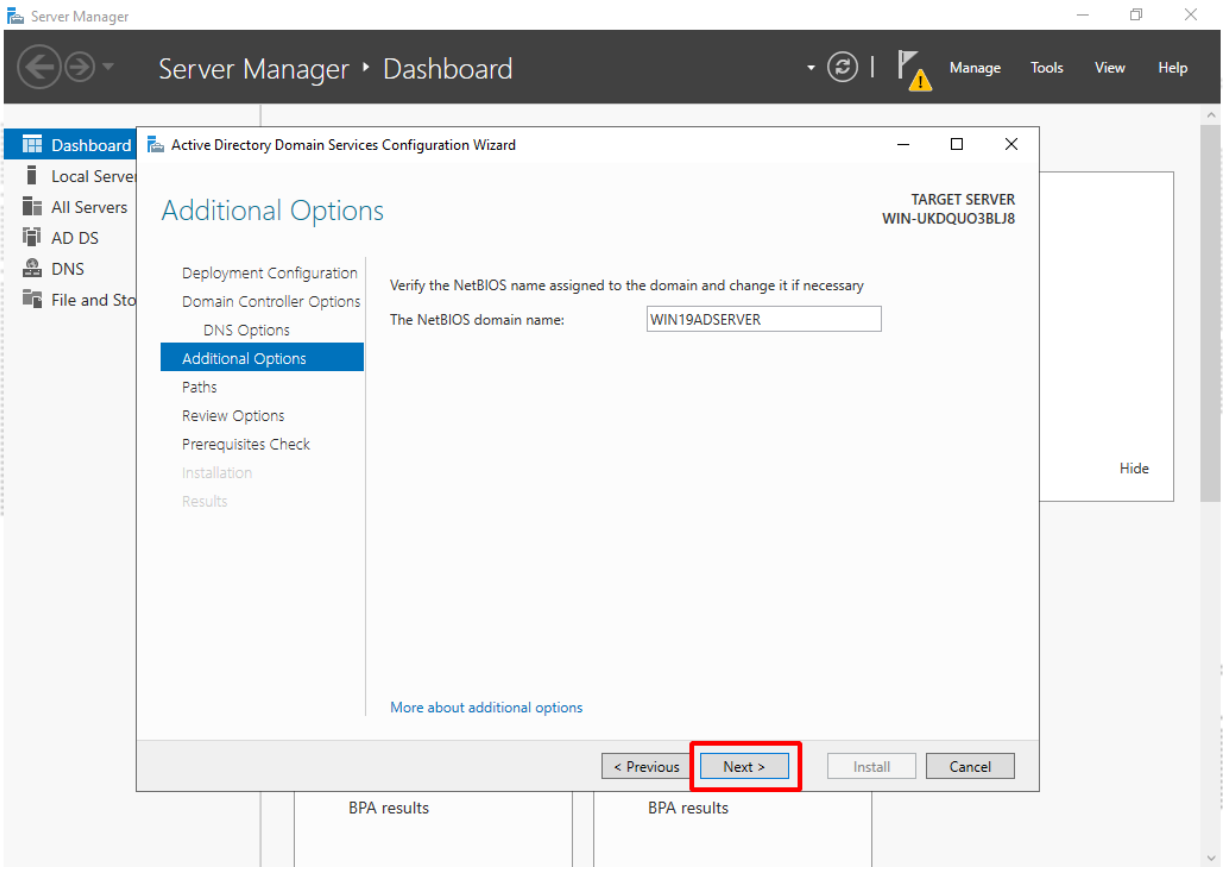
b. In *Deployment Configuration*, select *Add a new forest* and enter the *Root domain name*.



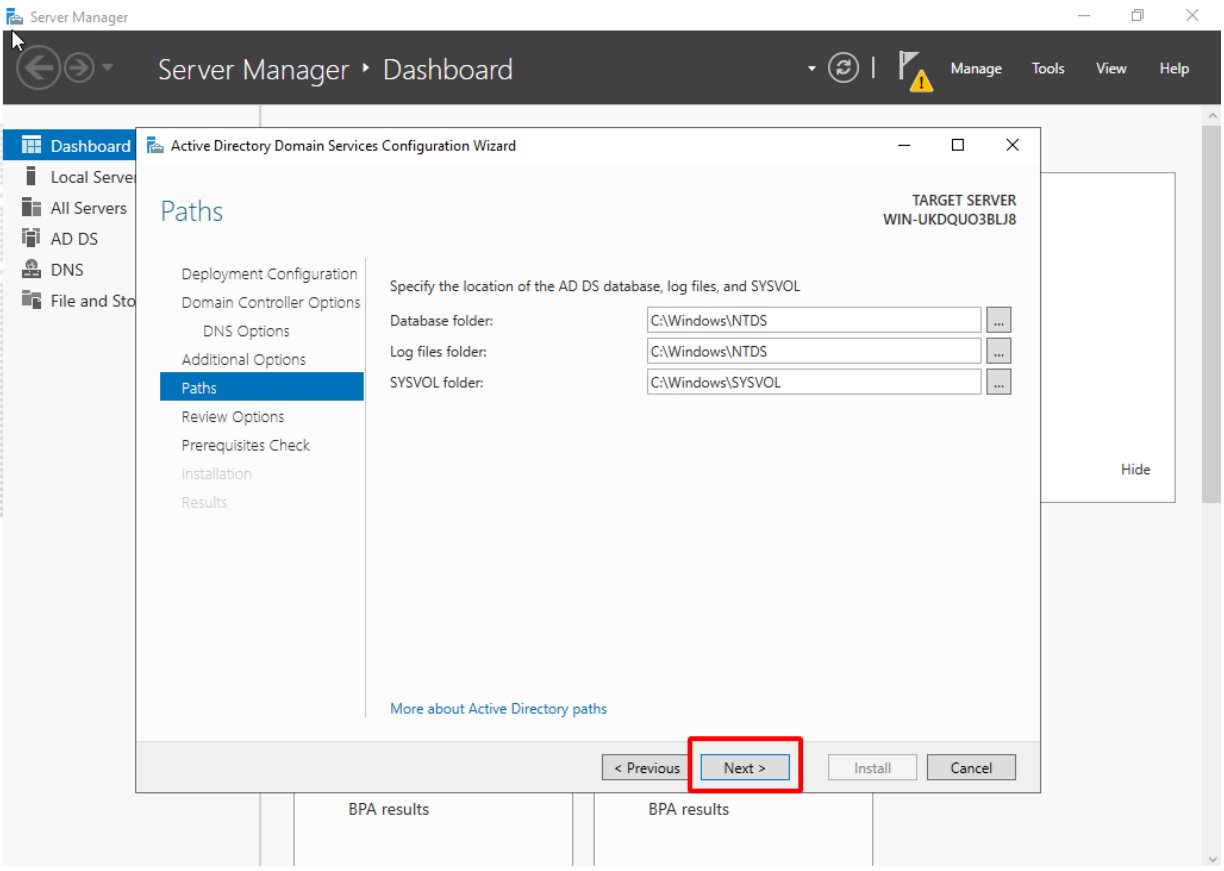
c. In *Domain Controller Options*, enter a password for the domain.



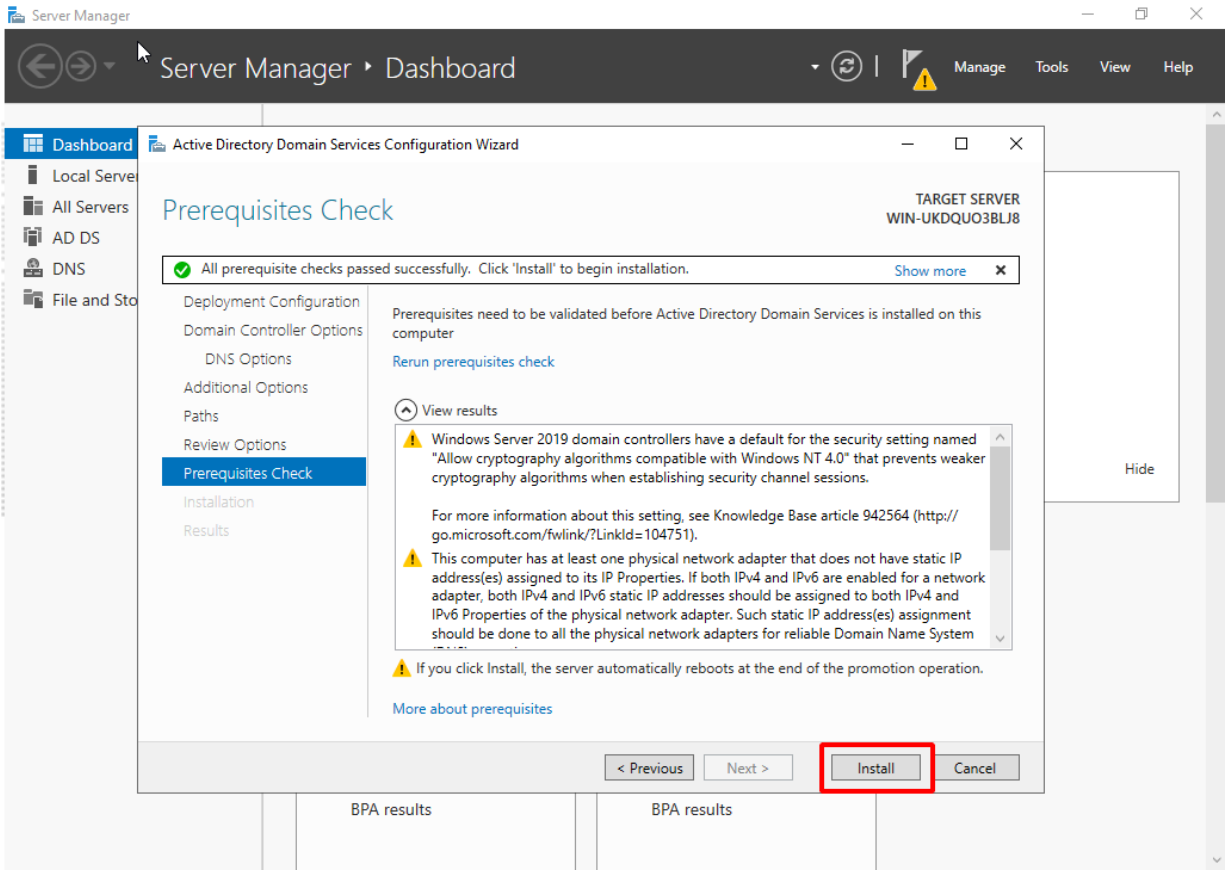
d. In *Additional Options*, enter a NetBIOS name for your domain (the default name is recommended).



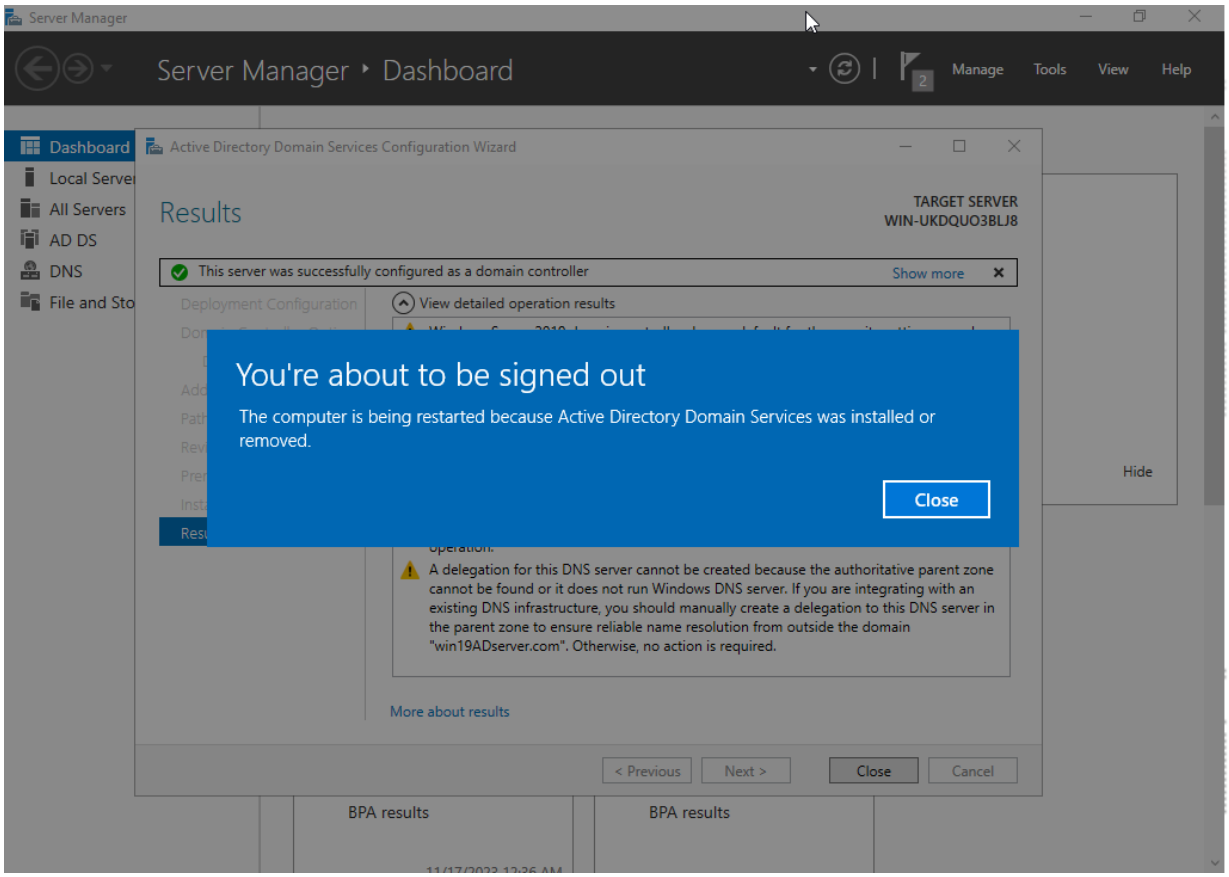
e. In *Paths*, select the folder where your database, log files, and SYSVOL will be stored (the default folder is recommended), then click *Next*.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Sto
Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
WIN-UKDQUO3BLJ8
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel
Hide
BPA results
BPA results

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



g. The PC will restart.



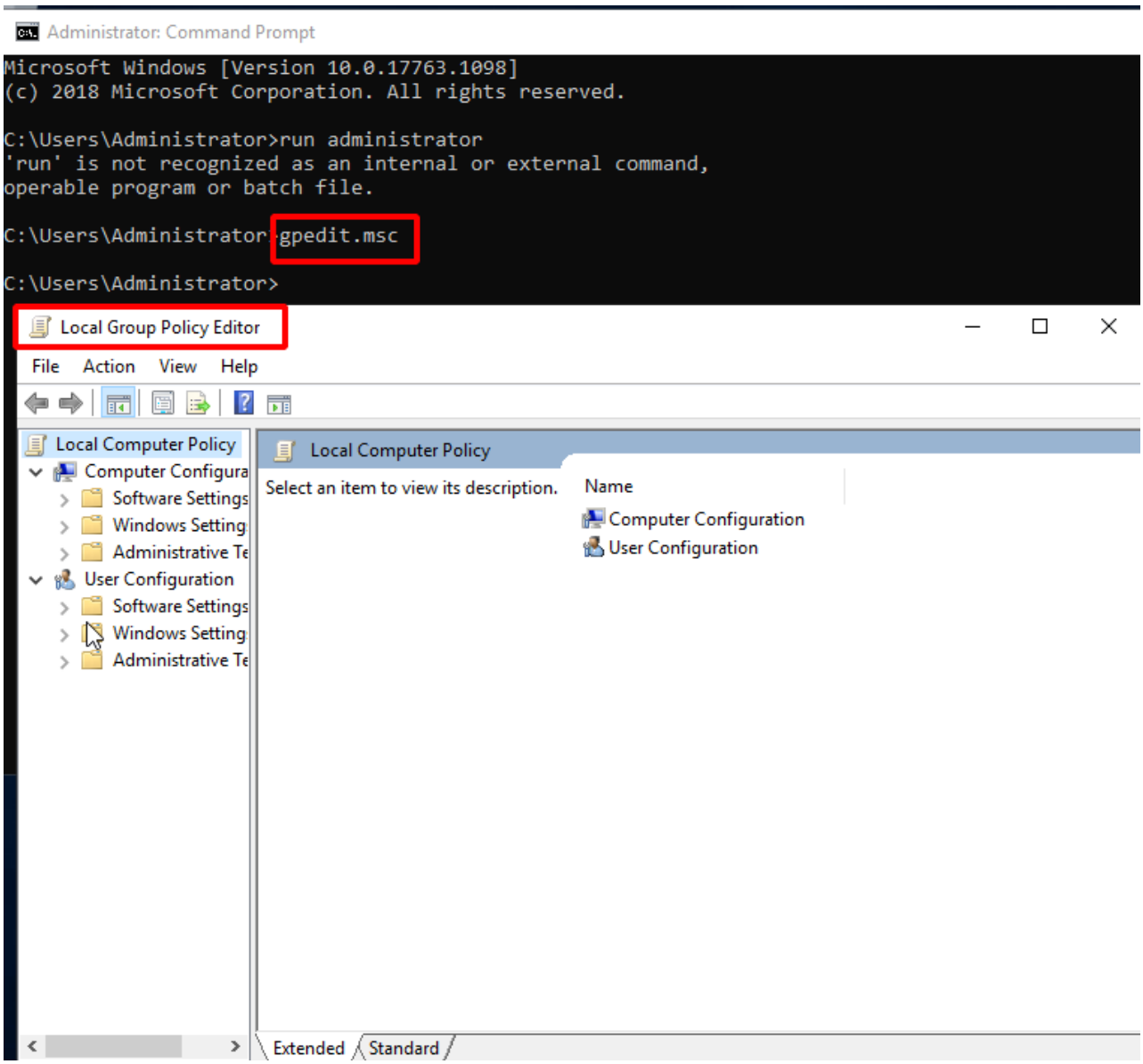
2. (Required) Set up the DNS server

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).

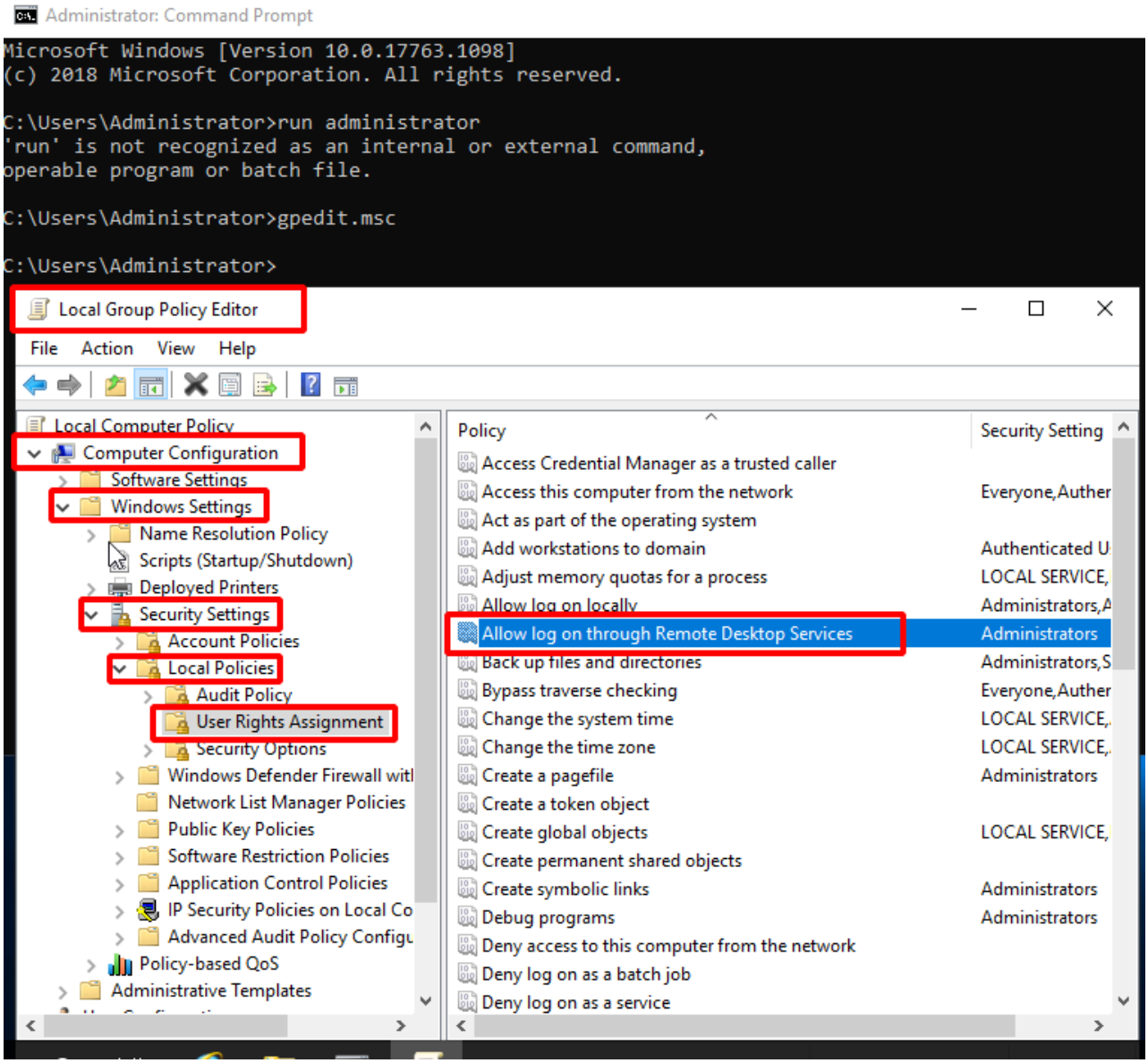
- To add more endpoints to this domain, you may want to configure the DNS forward rule to allow these endpoints to resolve public domains.
- To use a standalone DNS server, *DNS server* should not be installed in Step 1.
- The endpoint may use two DNS servers, one for the local domain, and another for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

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

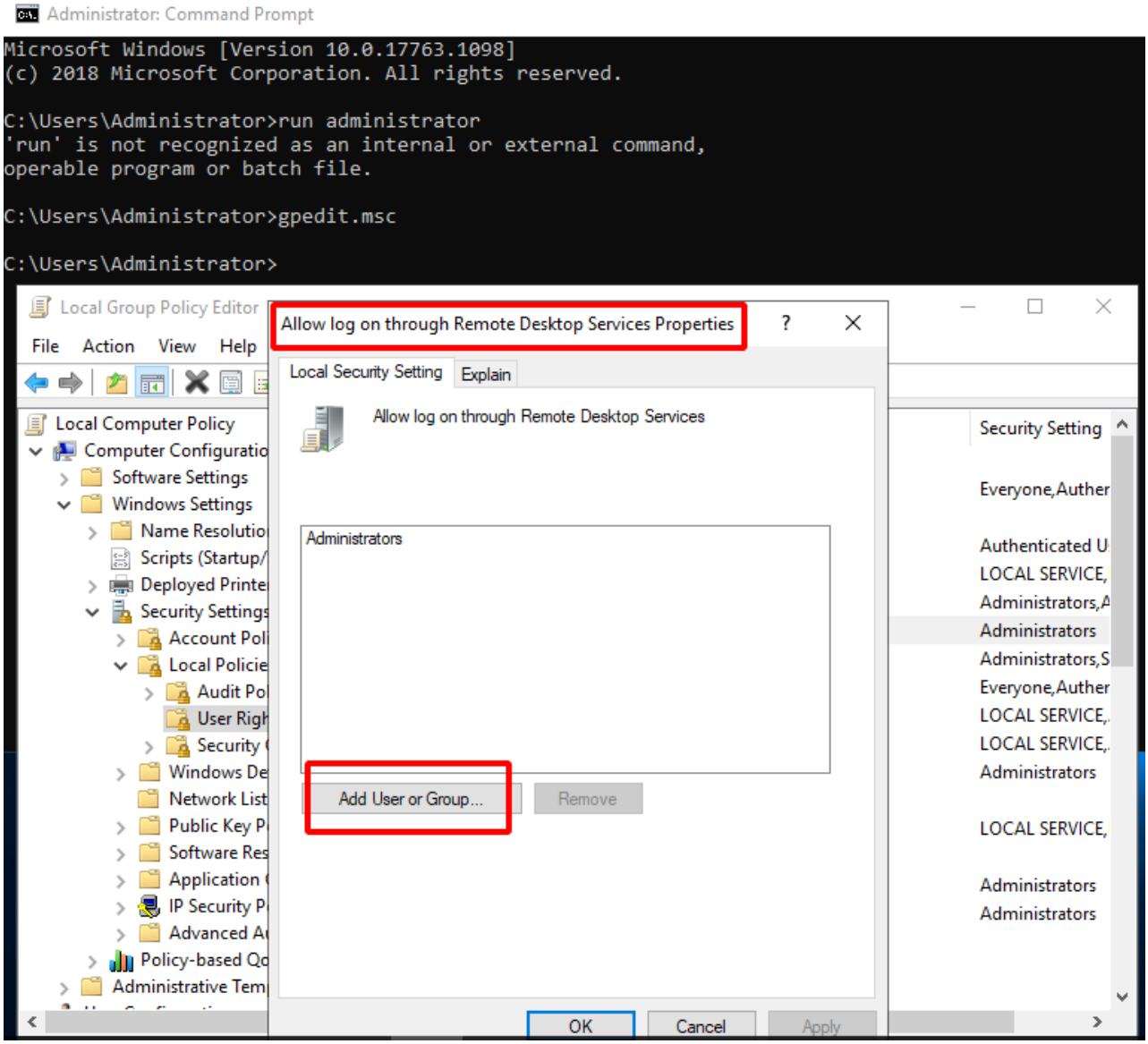
1. Open a command window as an administrator, then enter `gpedit.msc` to open the local group policy.



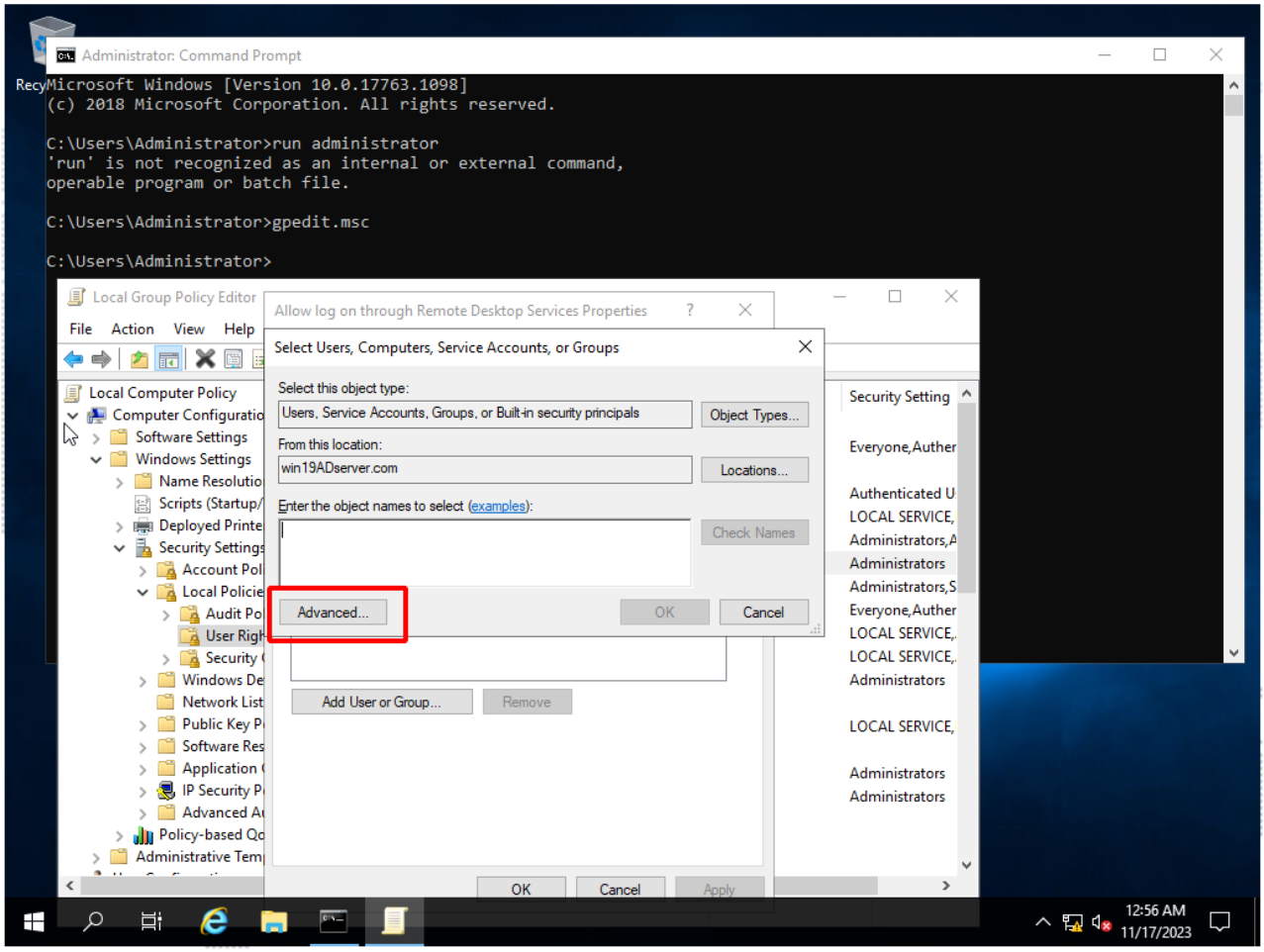
2. Go to *Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Policy Name: Allow log on through Remote Desktop Services*.


Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>run administrator
'run' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>gpedit.msc
C:\Users\Administrator>
Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall witl
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Co
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates
Policy
Security Setting
Access Credential Manager as a trusted caller
Access this computer from the network
Everyone,Auther
Act as part of the operating system
Add workstations to domain
Authenticated U
Adjust memory quotas for a process
LOCAL SERVICE,
Allow log on locally
Administrators,A
Allow log on through Remote Desktop Services
Administrators
Back up files and directories
Administrators,S
Bypass traverse checking
Everyone,Auther
Change the system time
LOCAL SERVICE,
Change the time zone
LOCAL SERVICE,
Create a pagefile
Administrators
Create a token object
Create global objects
LOCAL SERVICE,
Create permanent shared objects
Create symbolic links
Administrators
Debug programs
Administrators
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service

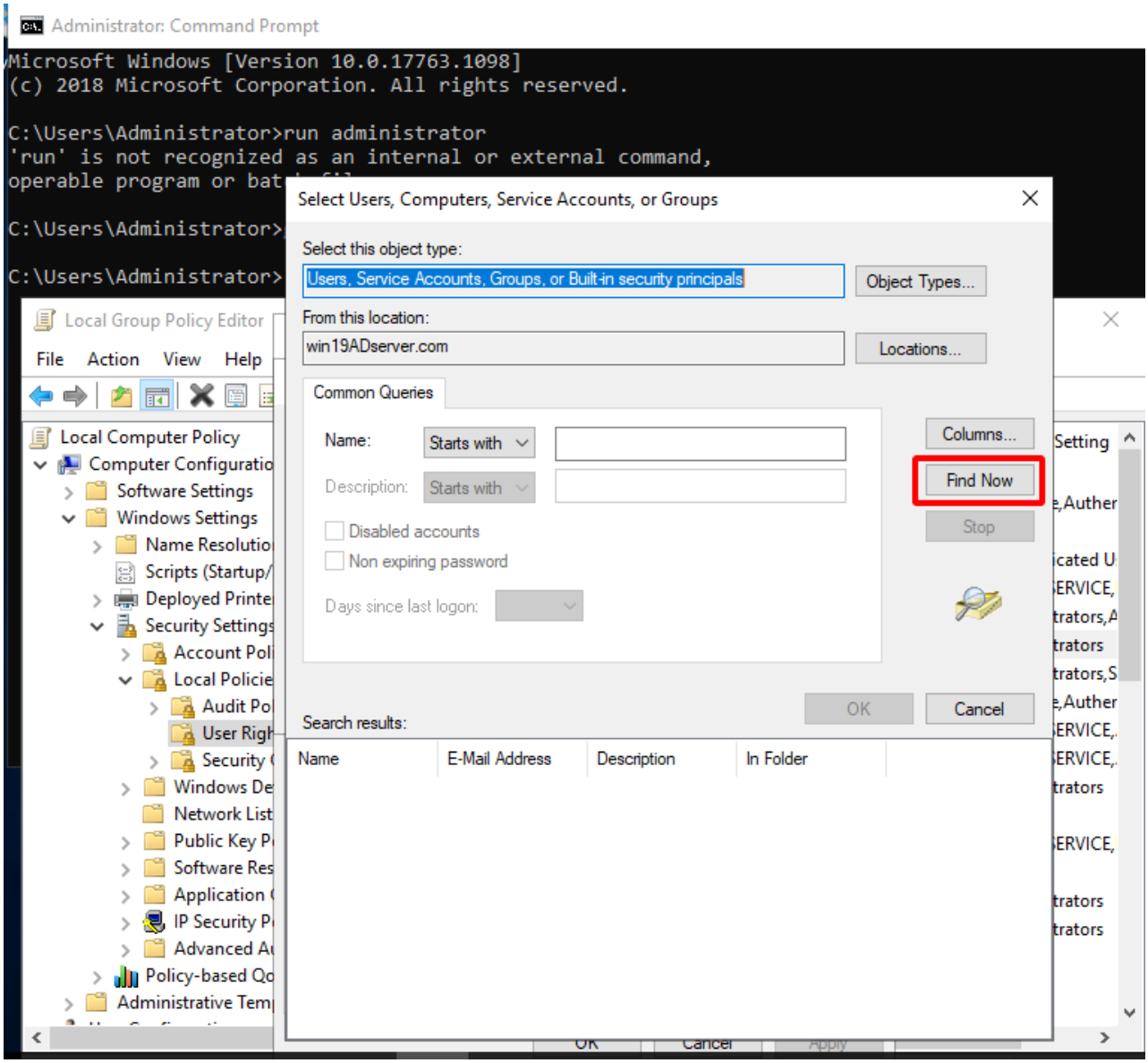
3. Select *Add User or Group of Allow log on through Remote Desktop Services policy*.



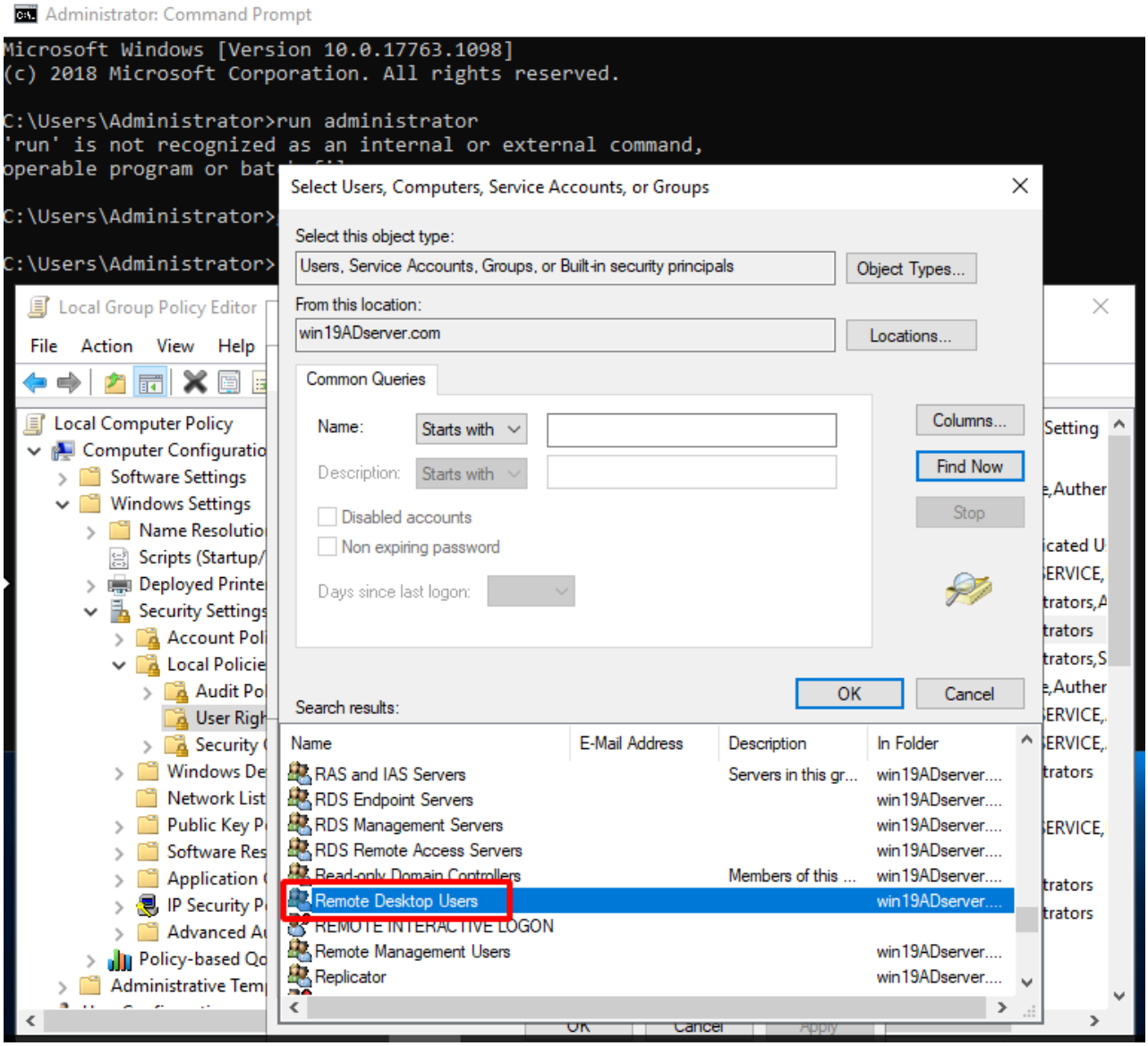
4. Click *Advanced*.



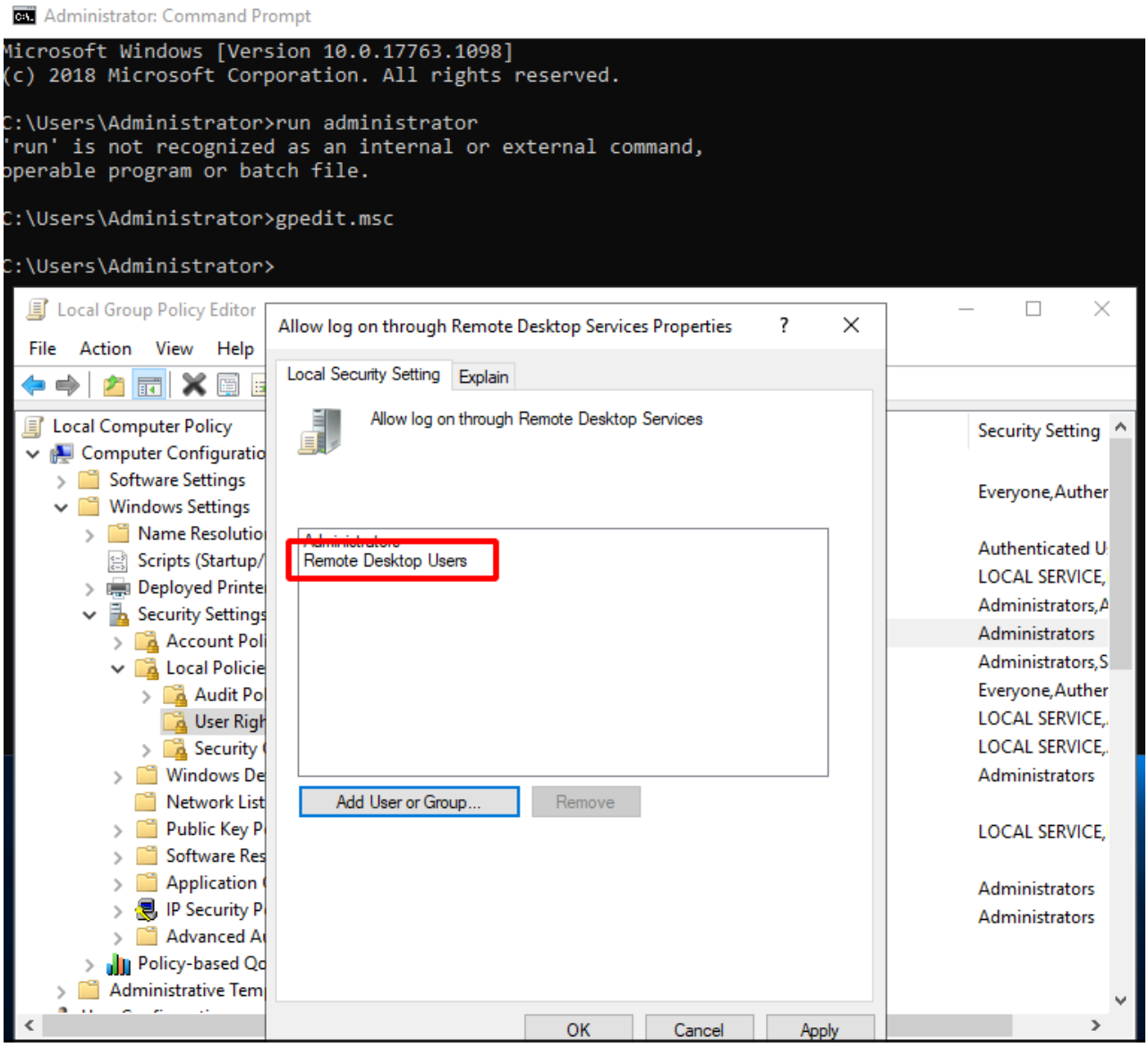
5. Click *Find Now*.



6. Add *Remote Desk User group*.

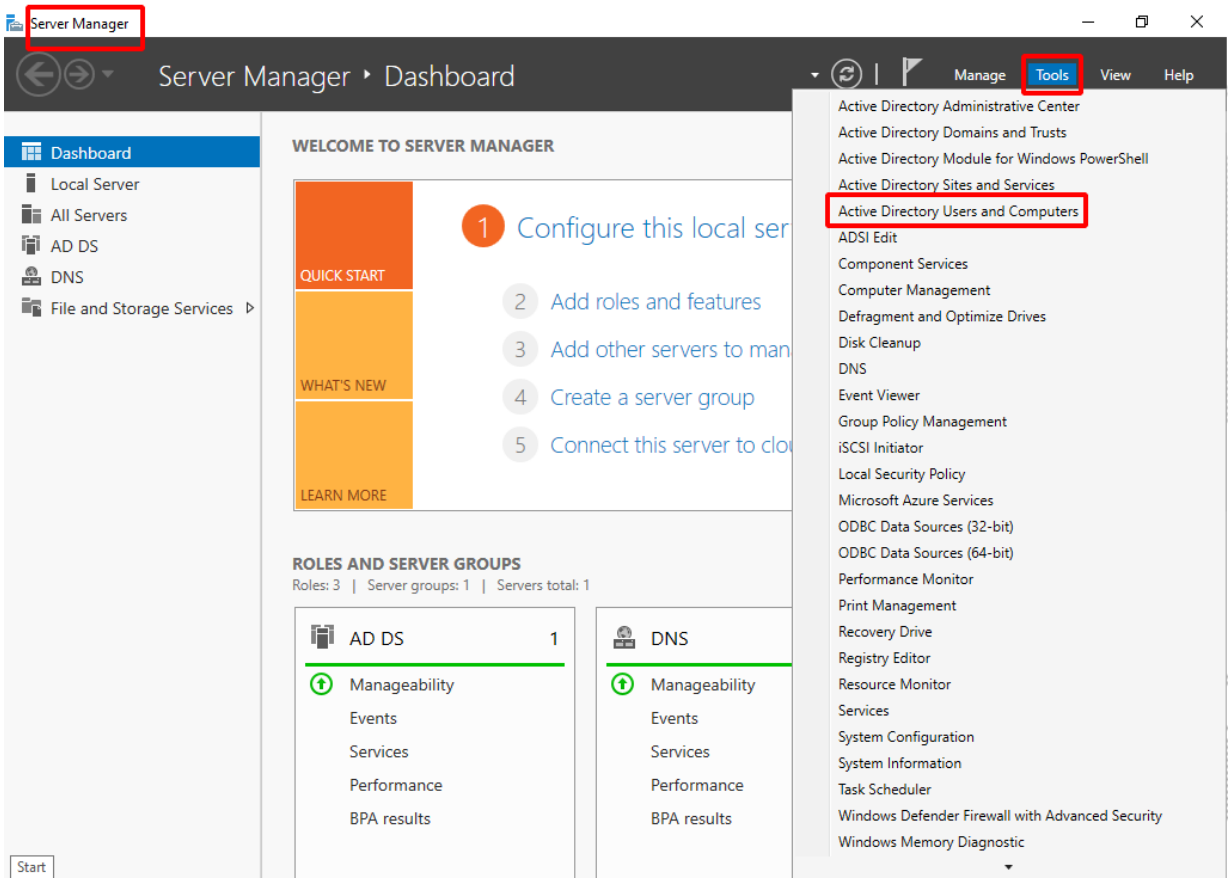


7. *Remote Desktop Users* is added.

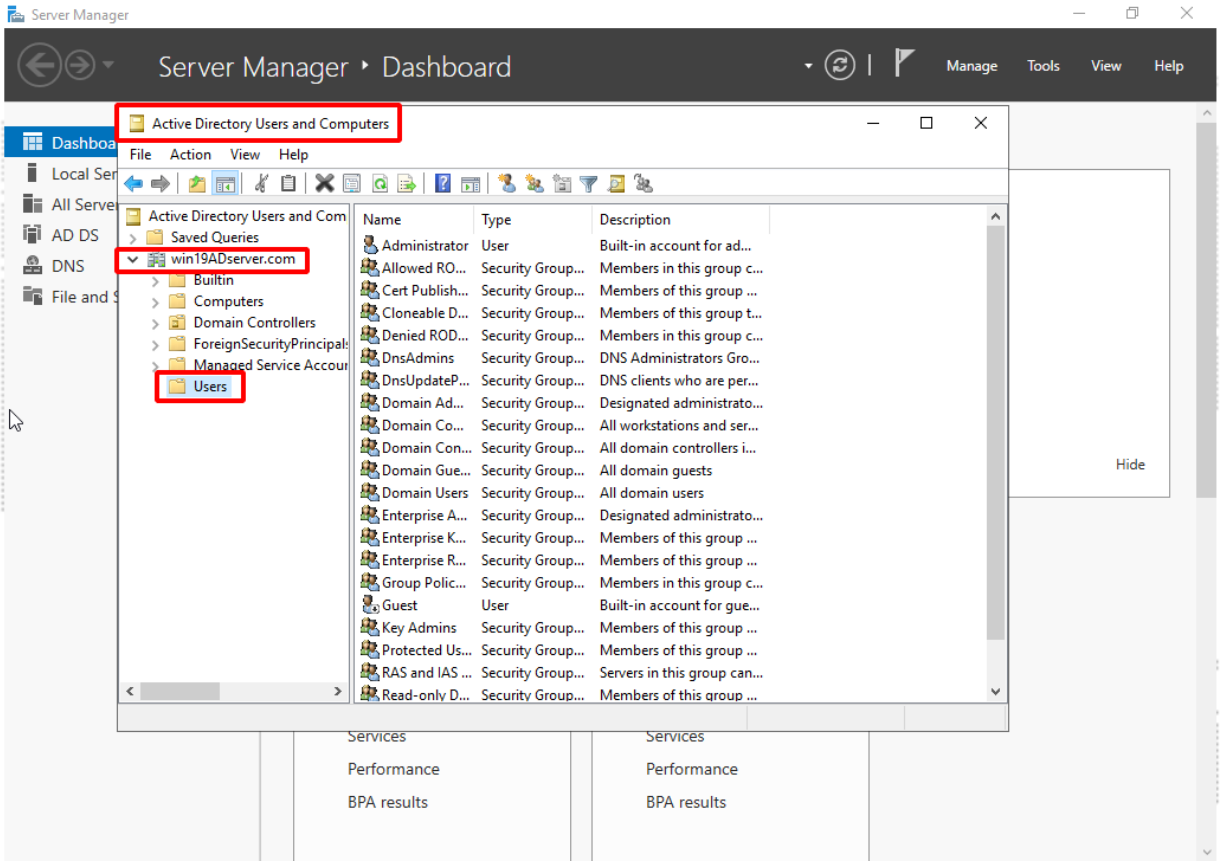


4. (Optional) Add AD Users to the Remote Desk User group

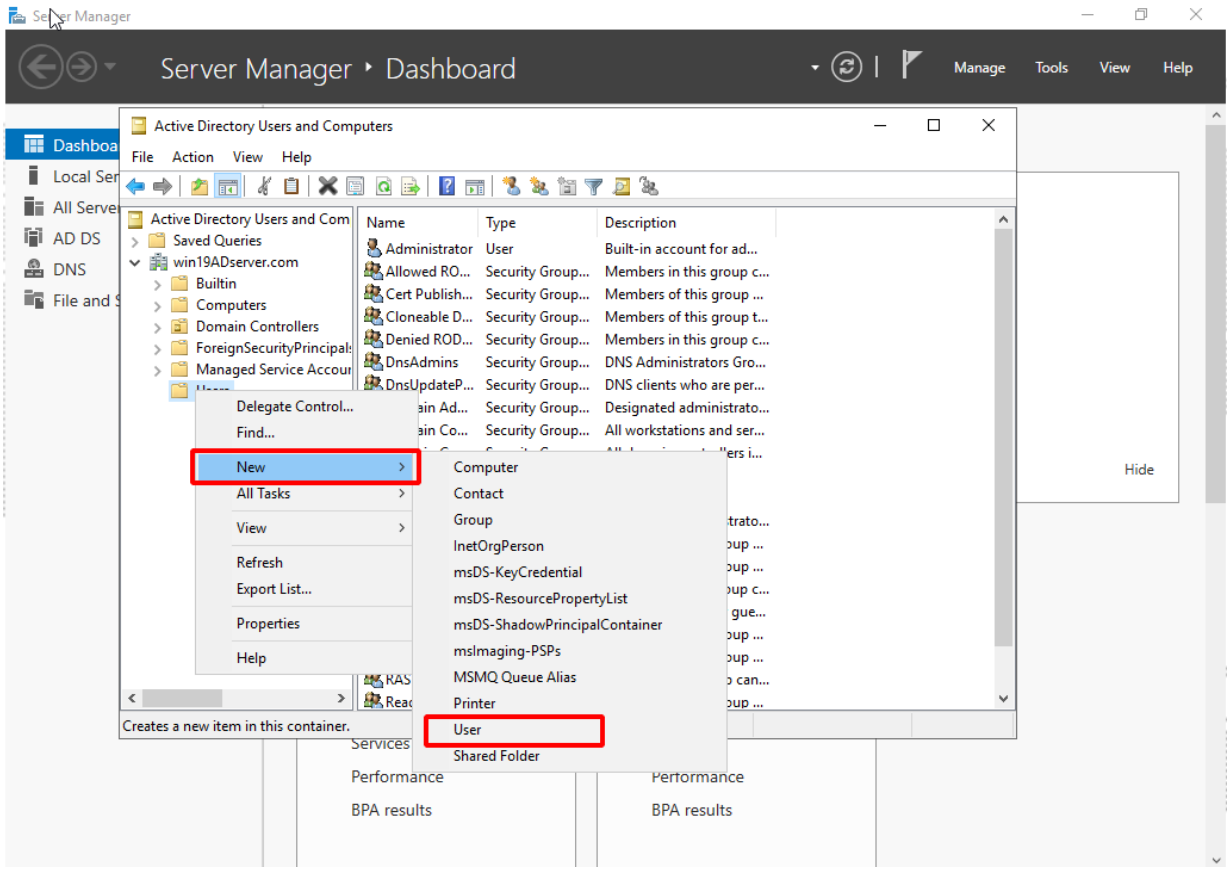
1. Add Active Directory Users
   a. In the Server Manager, click *Tools > Active Directory Users and Computers*.



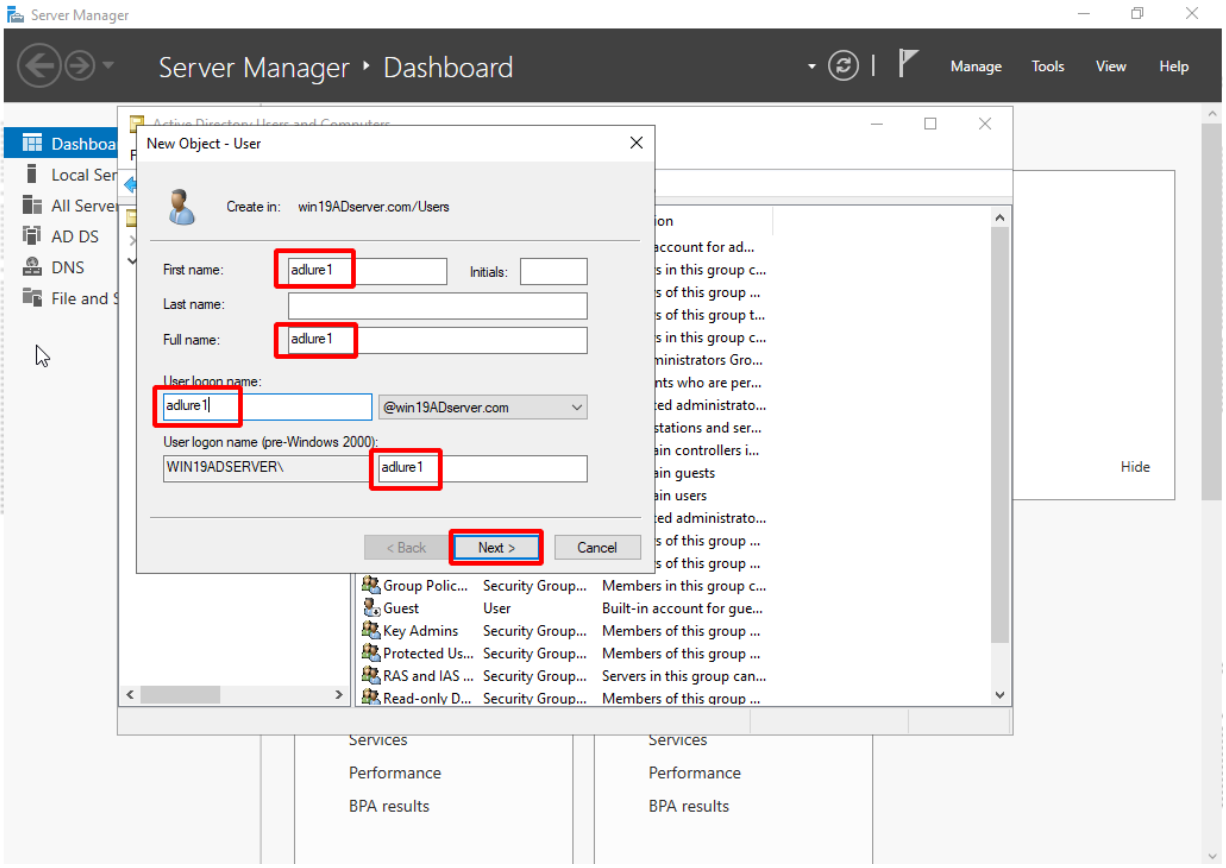
b. Right-click the domain name and open the *Users* folder.



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

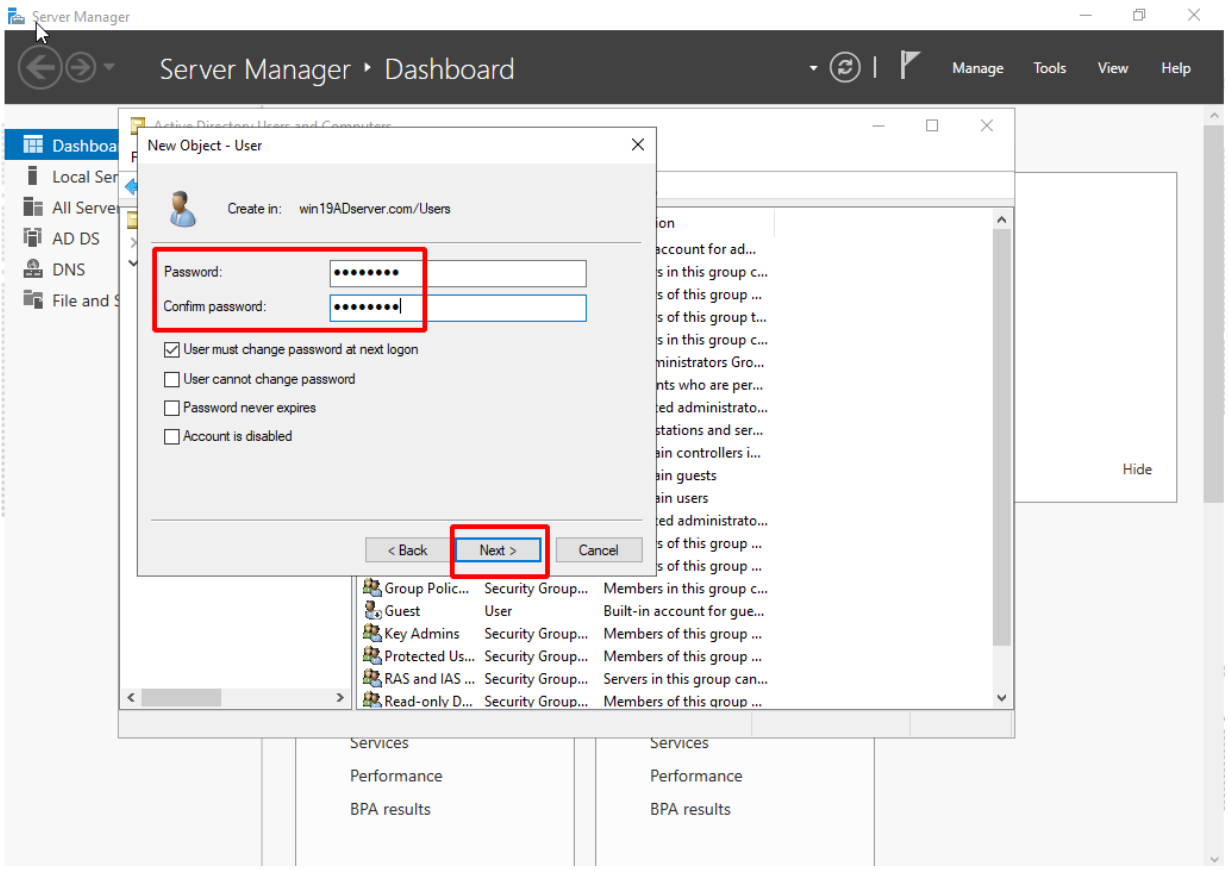


d. Enter the AD user name and click *Next*.

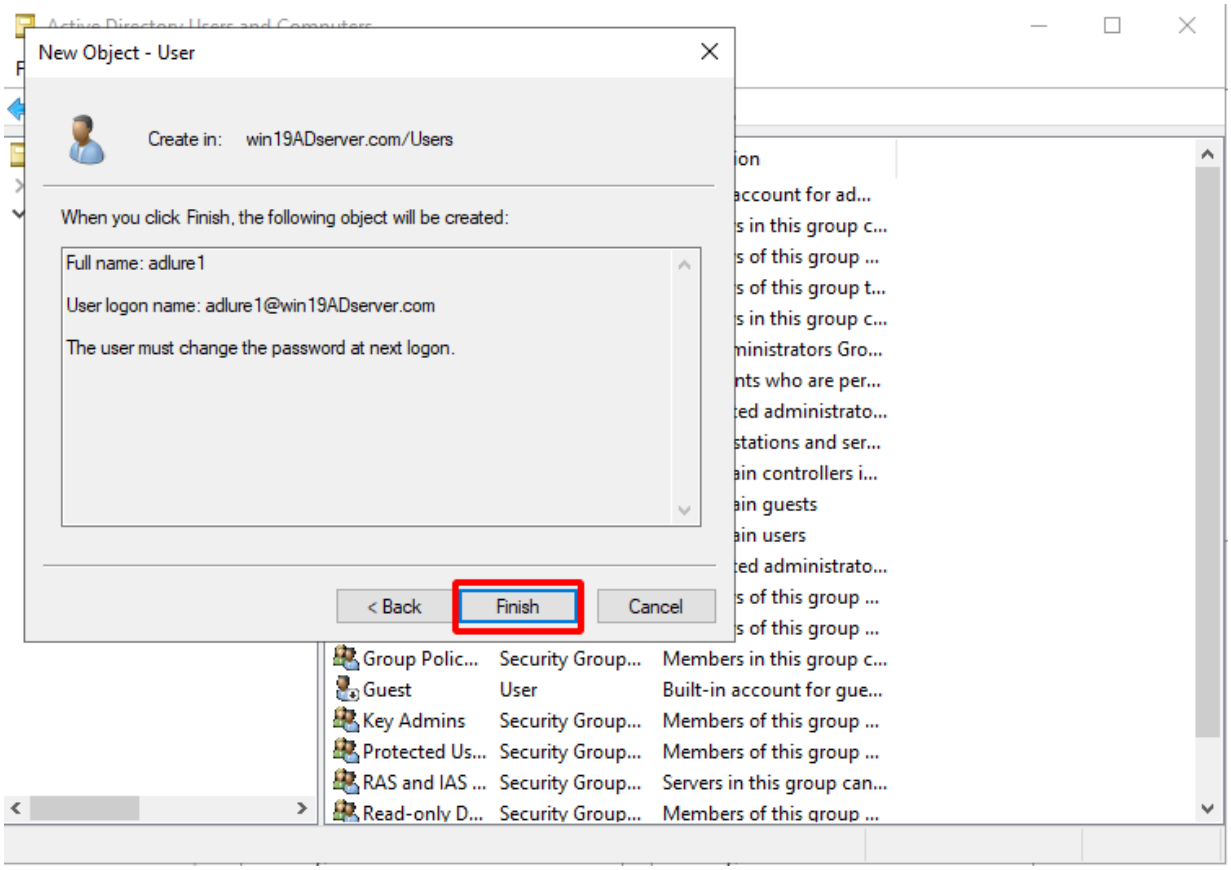


e. Enter the AD user password and click *Next*.

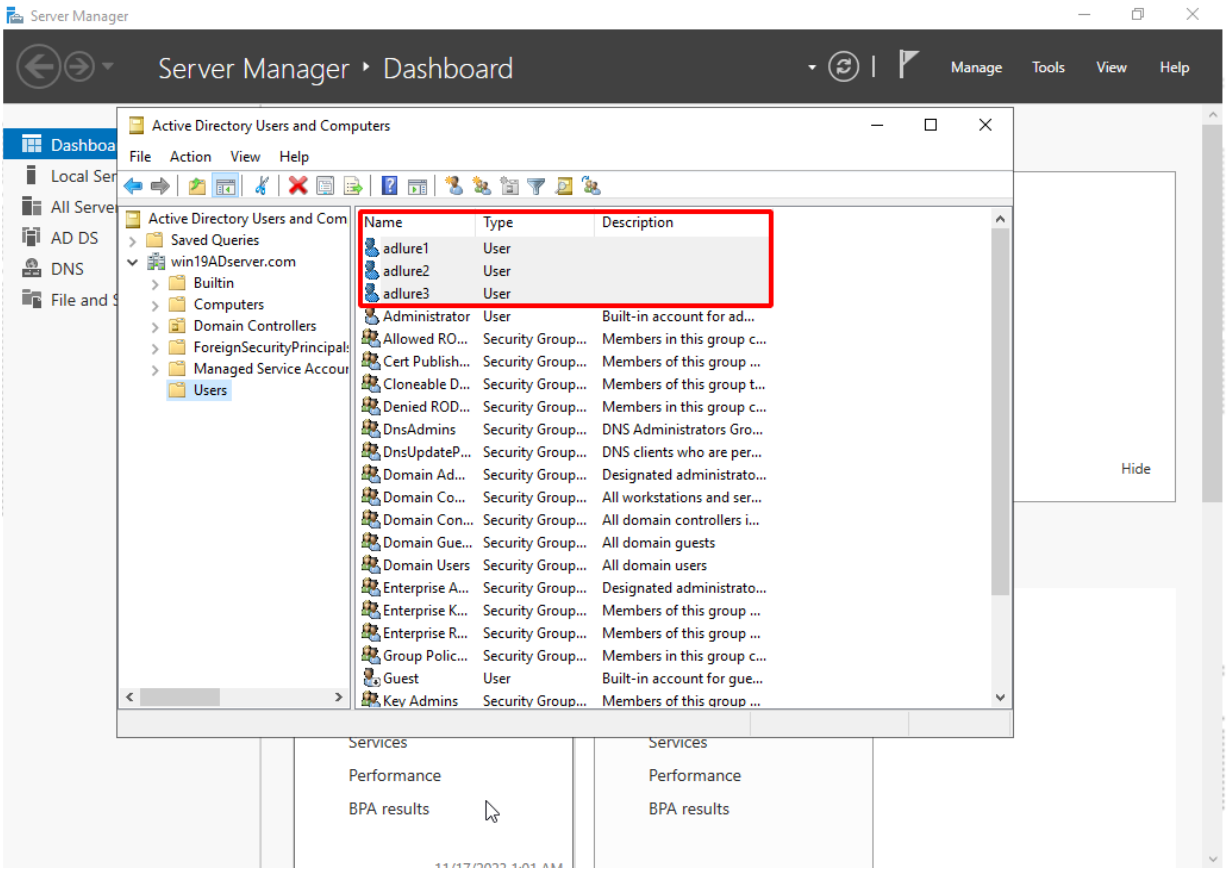
- Disable *User must change password at next logon*.
- Enable *User cannot change password* and *Password never expires*.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
New Object - User
Create in: win19ADserver.com/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
Hide
Services
Performance
BPA results

f. Click *Finish*.

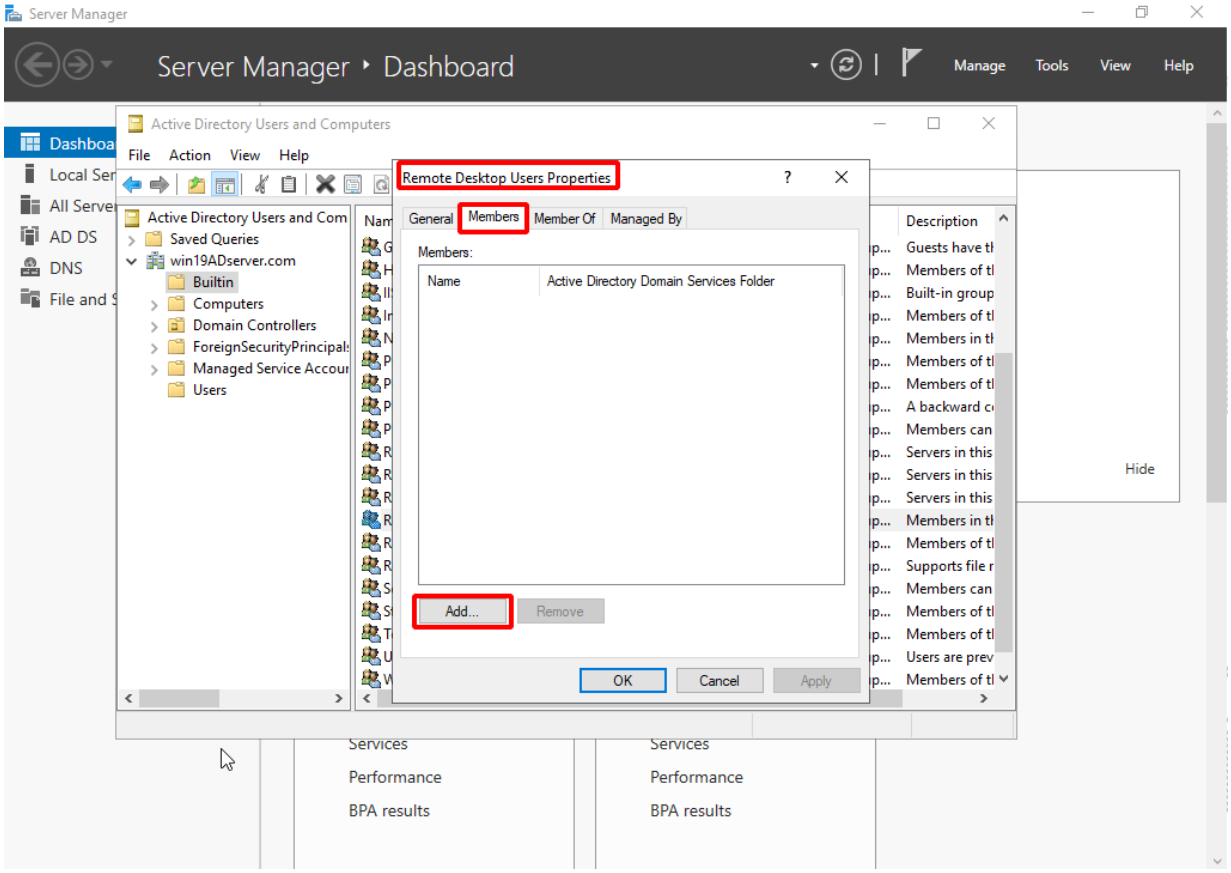


g. The AD Users are added.

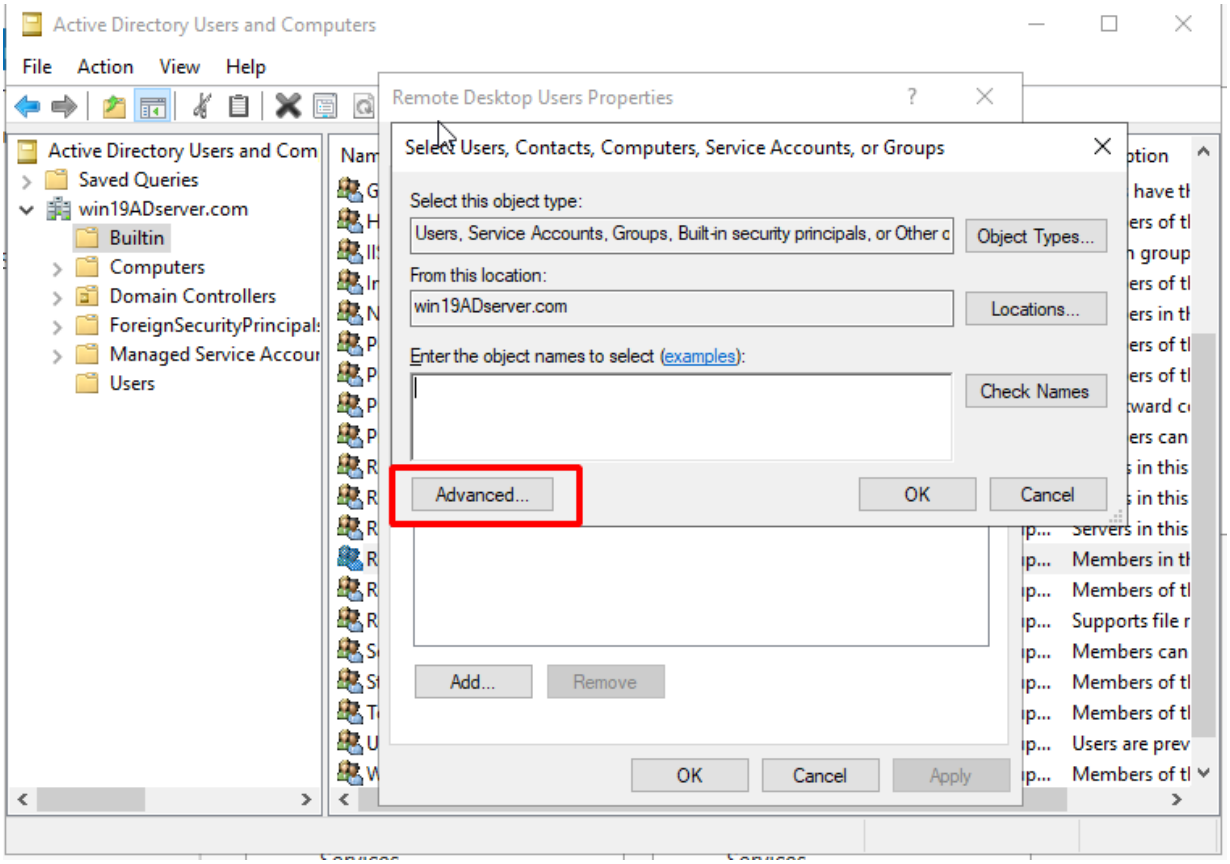


2. Add the new AD users to the Remote Desk User group.
   a. In the Server Manager, go to *Tools > Active Directory Users and Computers >{domain name} > Builtin > Remote Desk User group*.

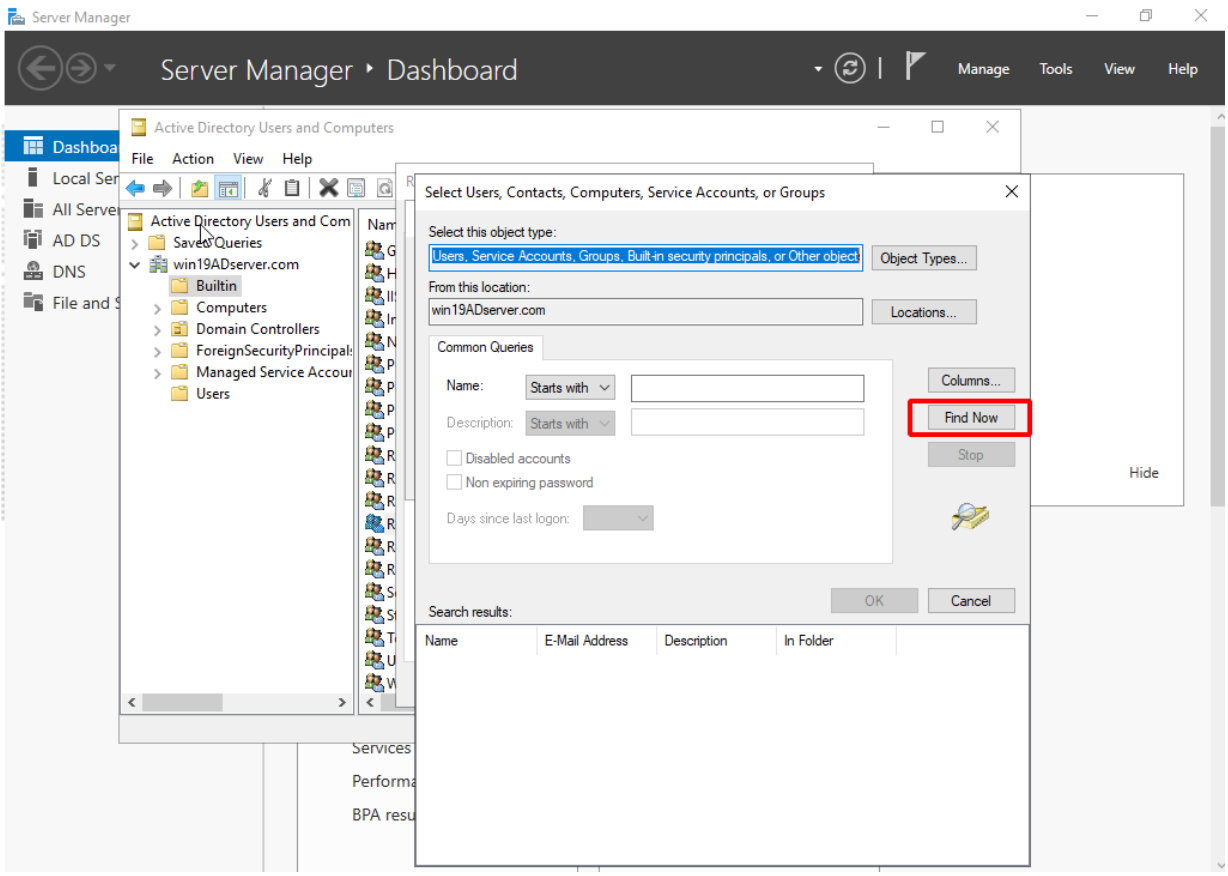
b. Double-click *Remote Desk User group*, click the *Members* tab and click *Add*.



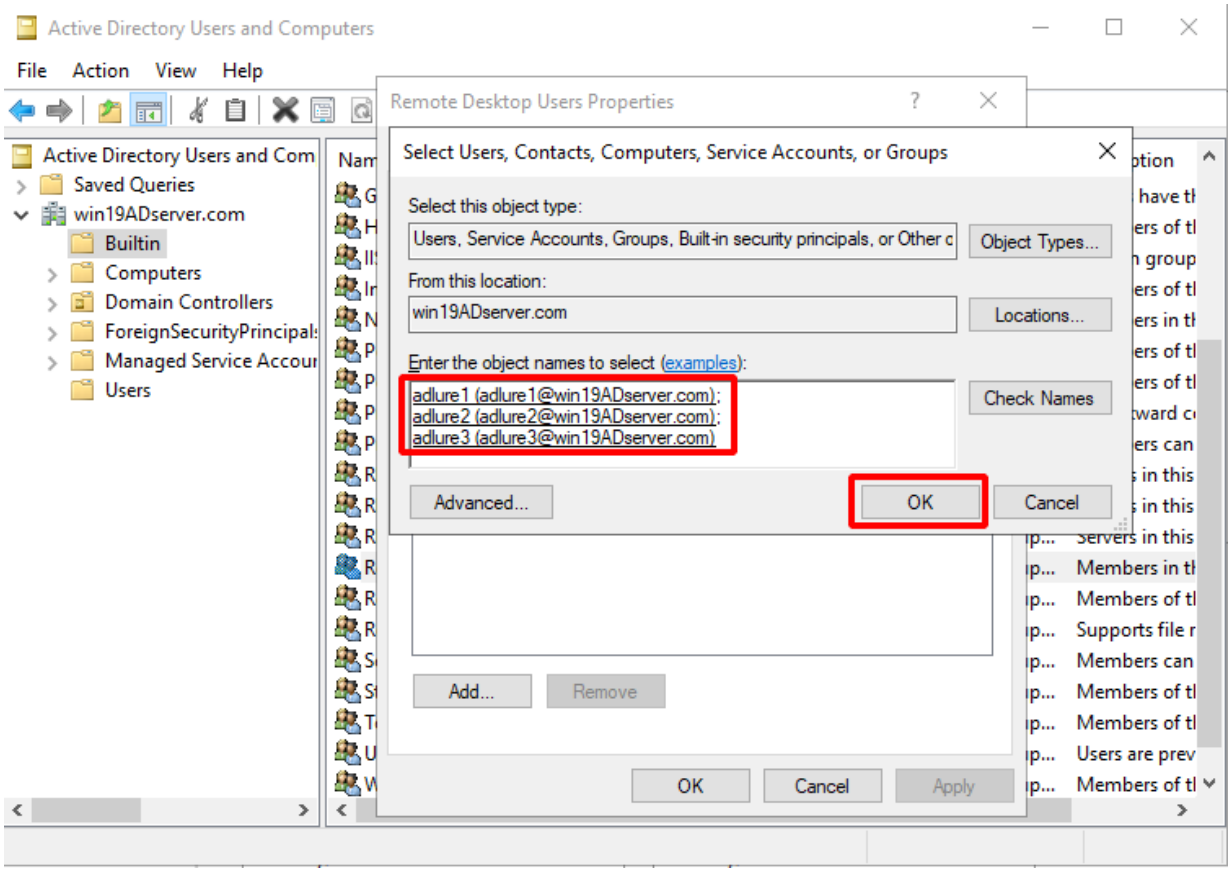
c. Click *Advanced*.



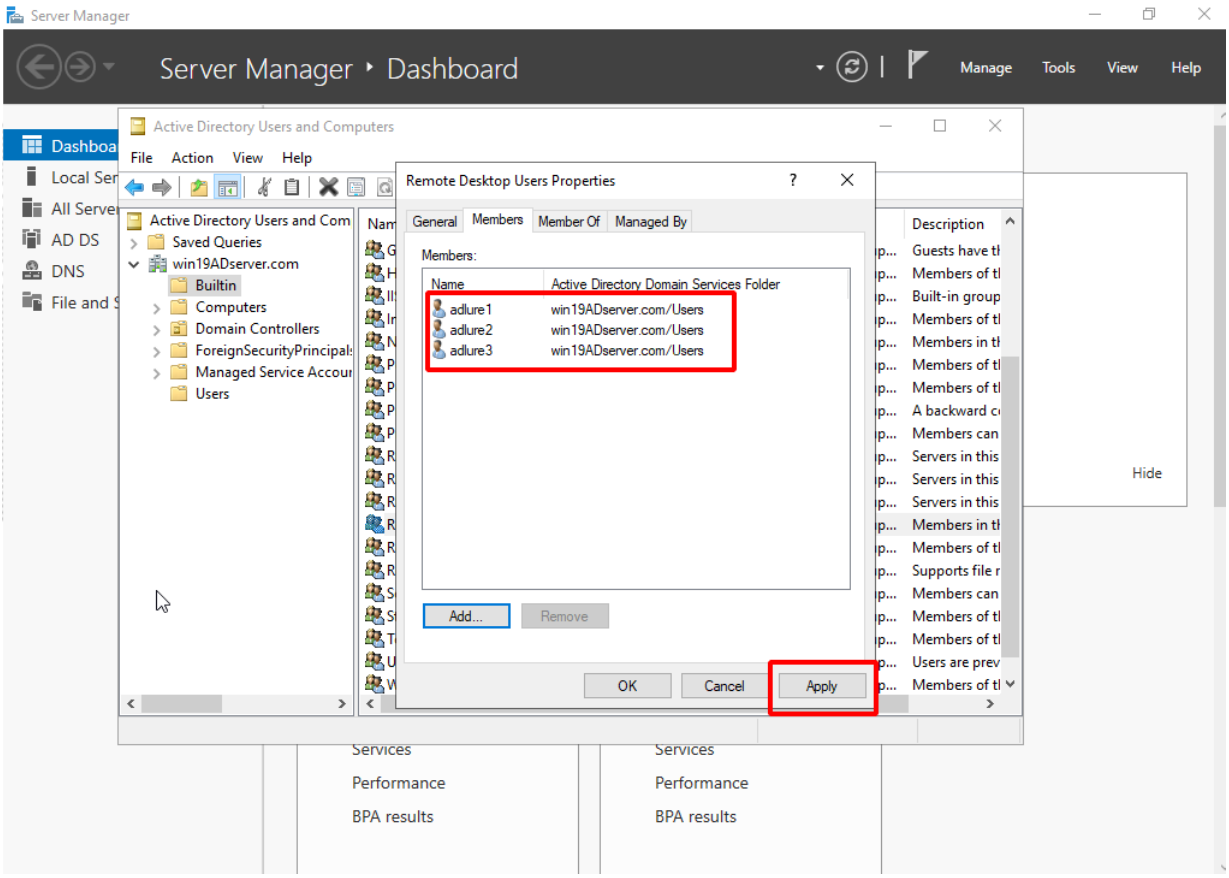
d. Click *Find Now* and choose the AD users you would like to add to the Remote Desk User group.



e. Click *OK*.

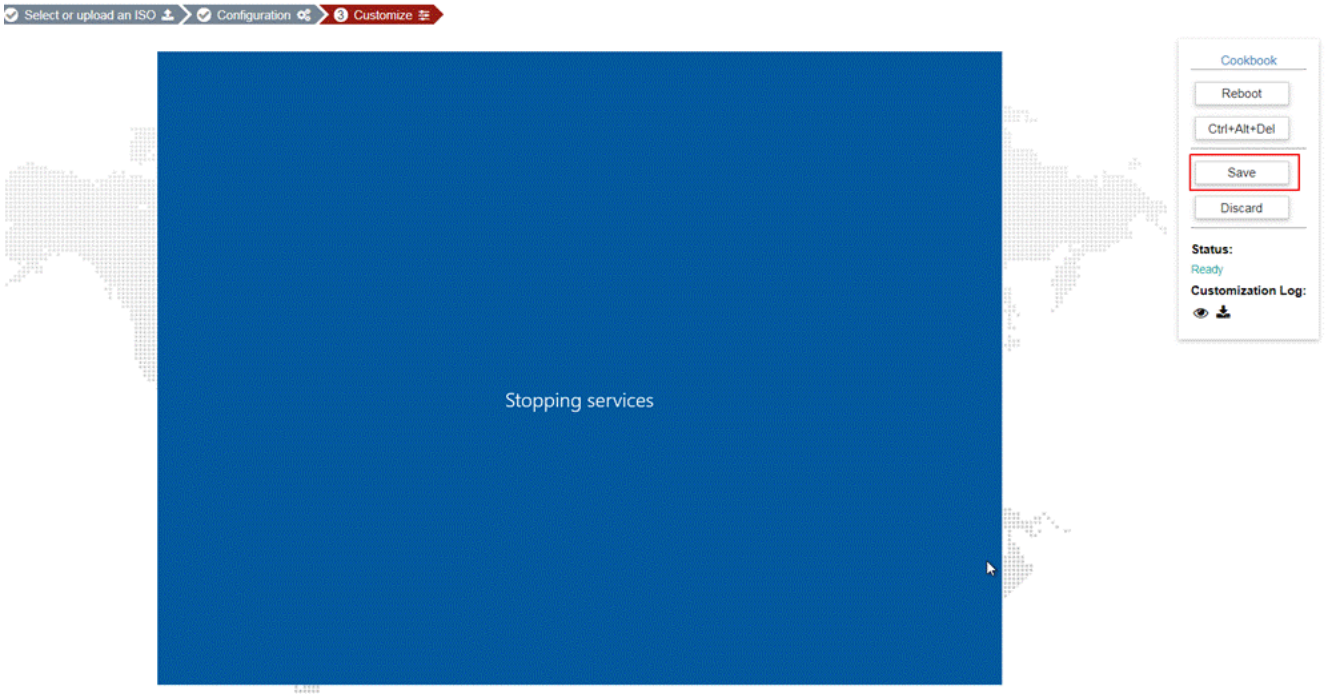

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
win19ADserver.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Remote Desktop Users Properties
Select Users, Contacts, Computers, Service Accounts, or Groups
Select this object type:
Users, Service Accounts, Groups, Built-in security principals, or Other c
Object Types...
From this location:
win19ADserver.com
Locations...
Enter the object names to select (examples):
adlure1 (adlure1@win19ADserver.com);
adlure2 (adlure2@win19ADserver.com);
adlure3 (adlure3@win19ADserver.com)
Check Names
Advanced...
OK
Cancel
Add...
Remove
OK
Cancel
Apply

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



8. Save the customized image

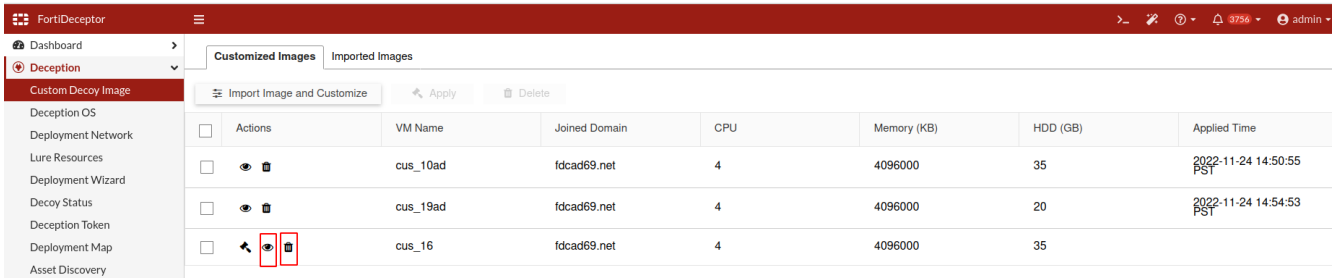
After Windows shuts down successfully, click *Save* to save this image. It may take several minutes to save the entire image. After it's finished, the page will display the *Customized Images* table with a new entry.



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 and Administrator In this case, 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.



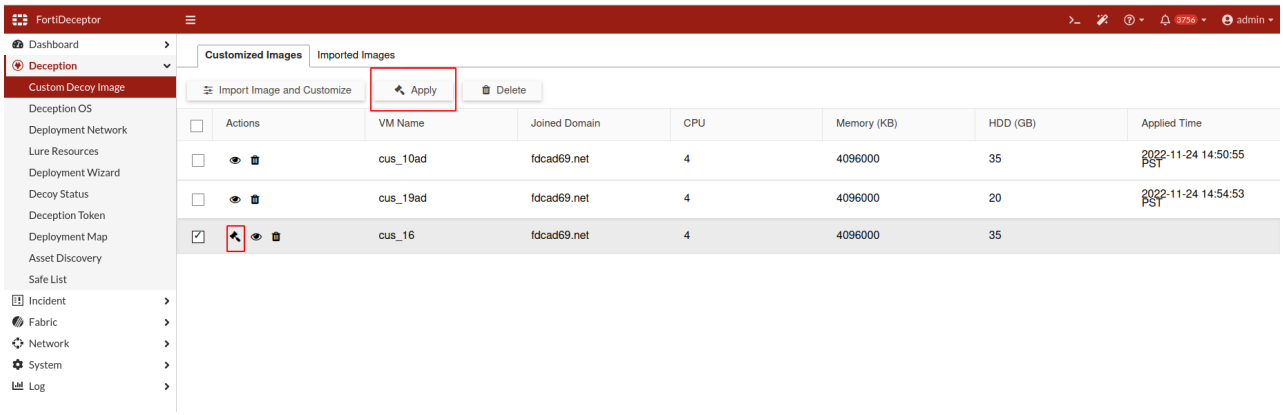
Use the custom Windows image

10. Use the custom Windows image

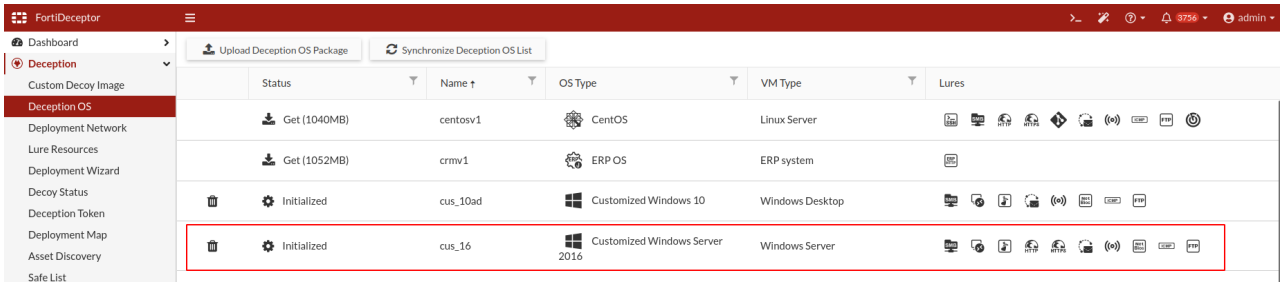
Apply the custom images

To apply a custom image:

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



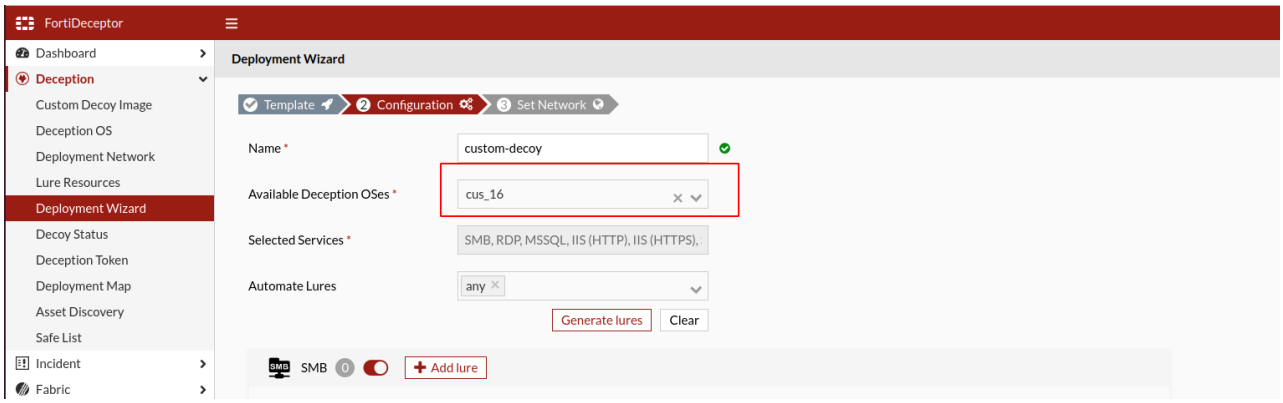
2. Choose a custom image and click *Apply*". The applied image is displayed in the *Deception OS* table. It may take several minutes for the image to appear in the table.



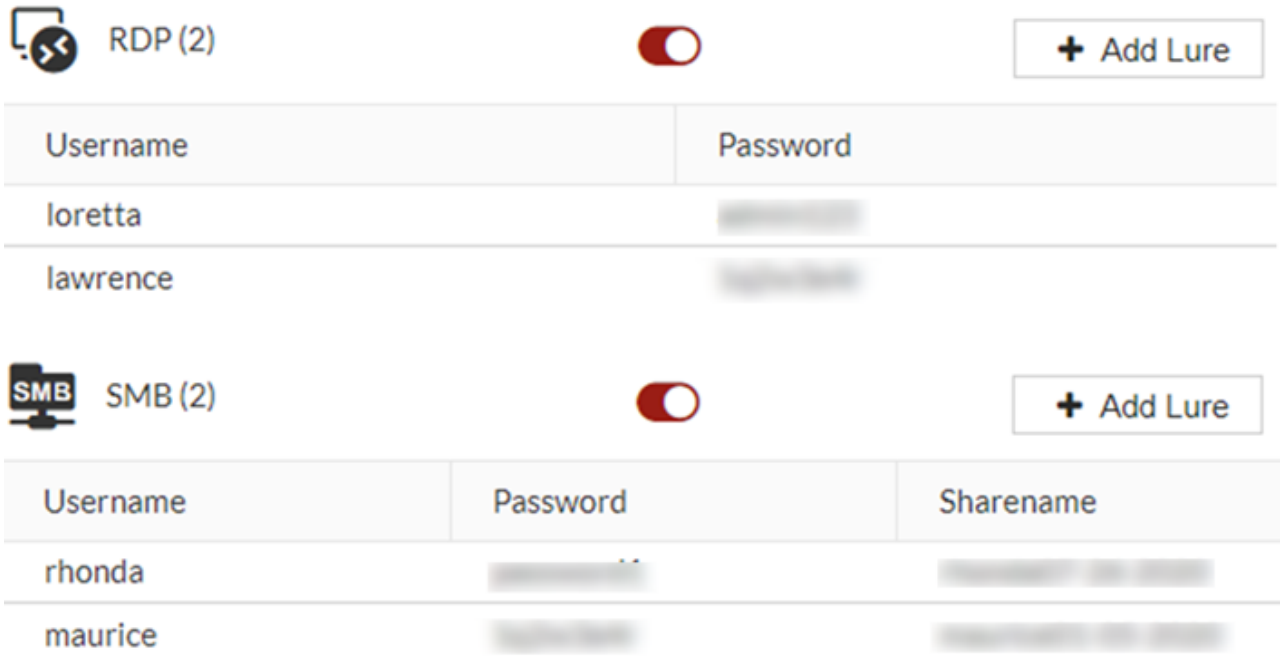
Deploy decoys with custom generic Image

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.

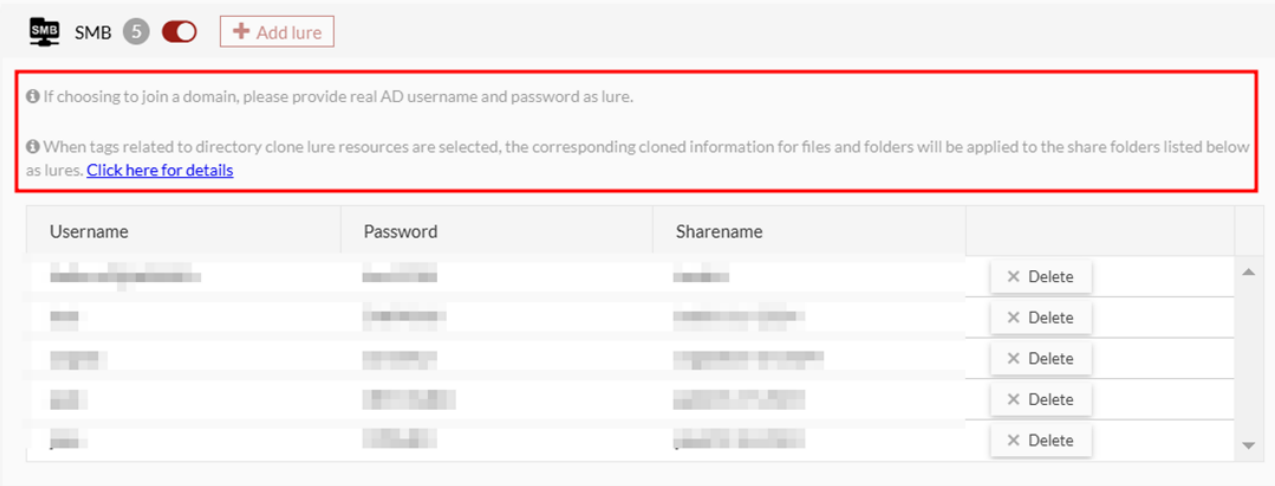


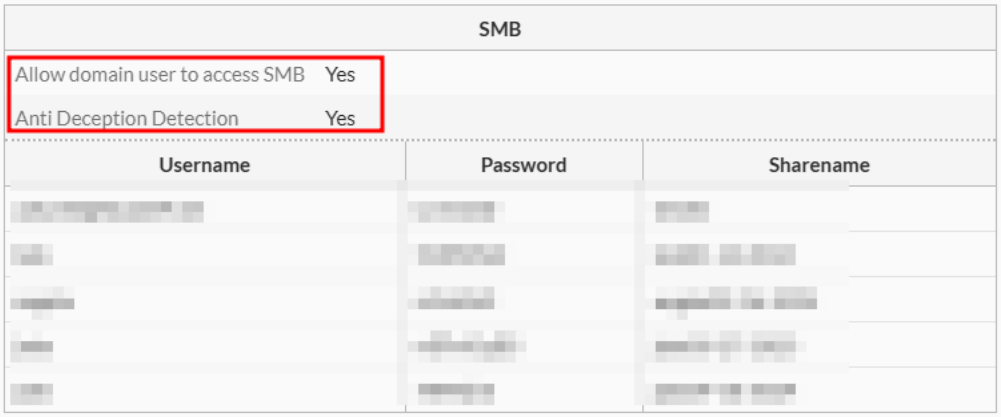
3. Select the RDP and SMB domain users will access.
For normal users:



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`.

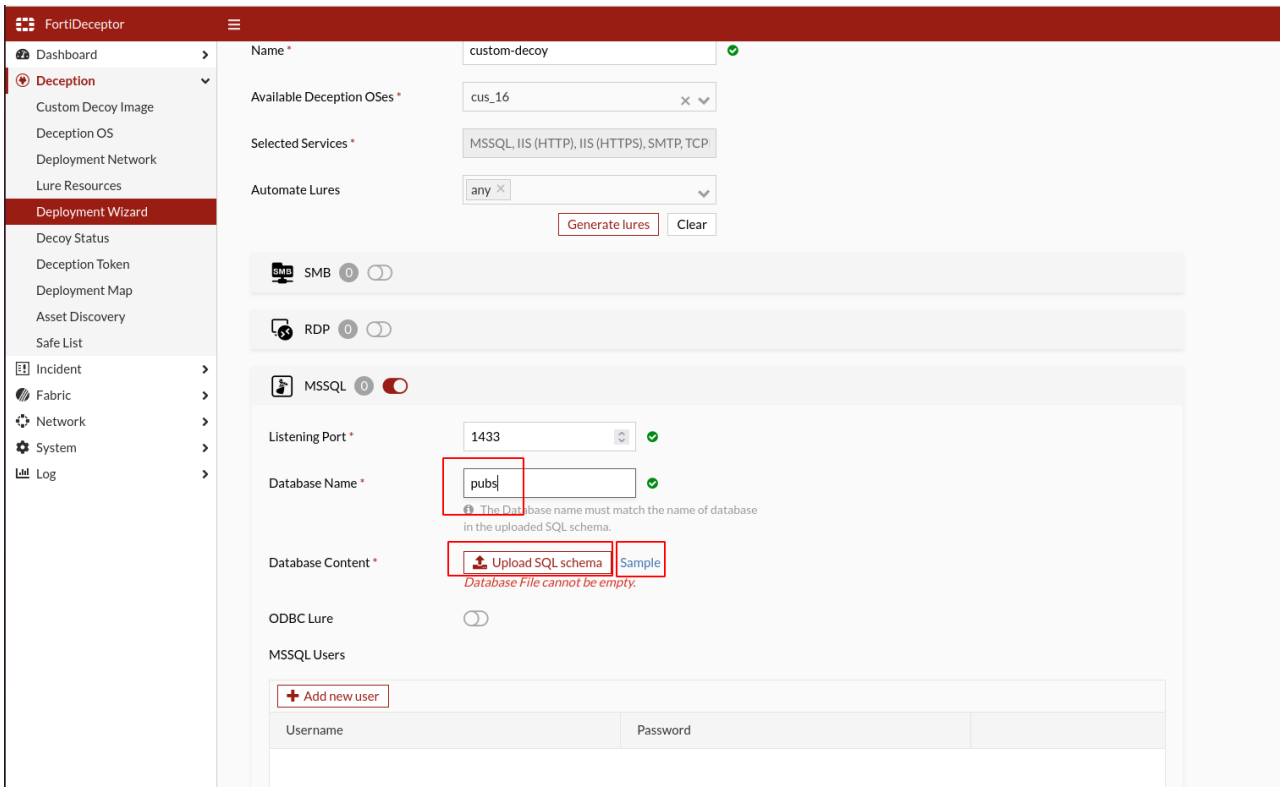




Deploy decoys with a customized SQL Server image

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.

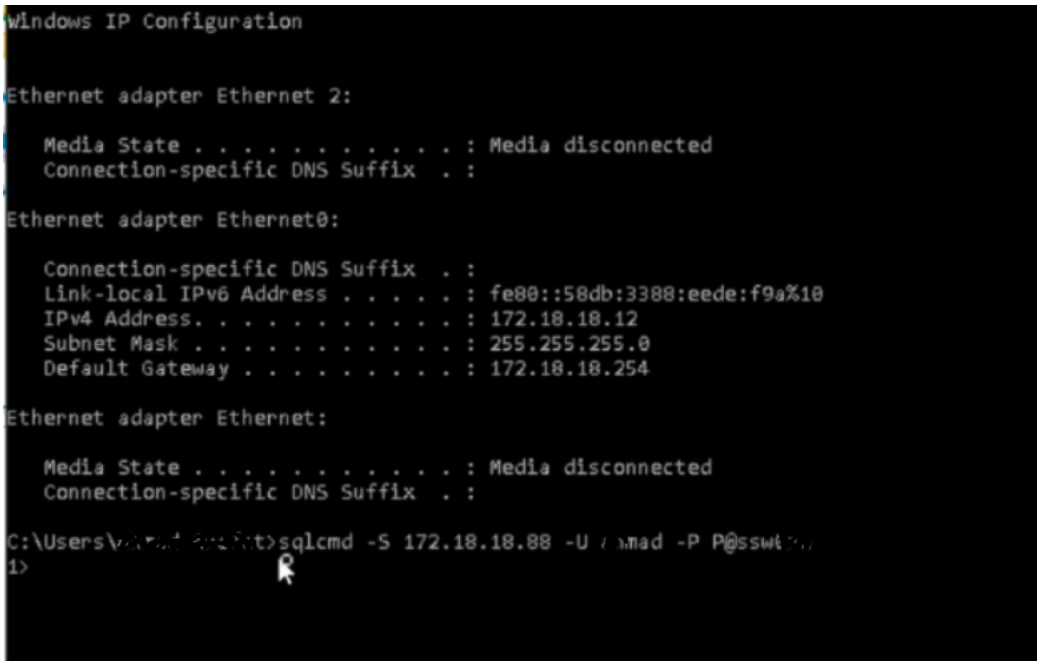


4. To generate SQL alerts using the *SQLCMD* tool run the following command inside the command line:

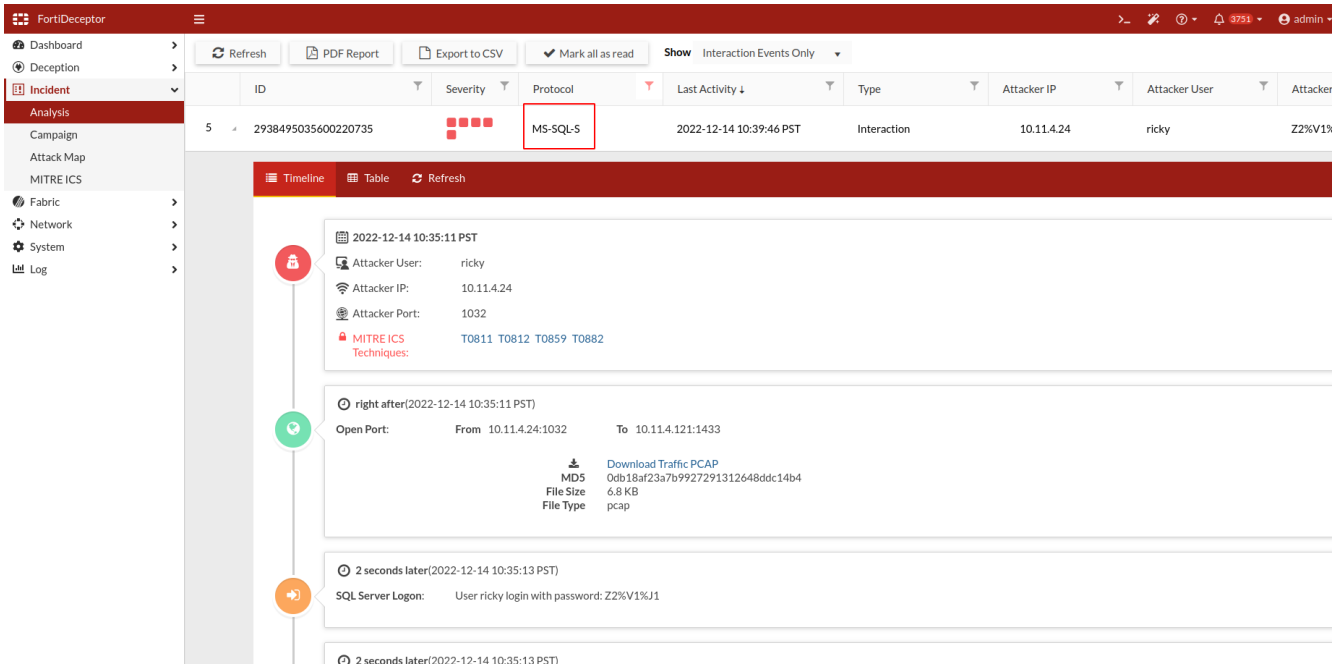
```
sqlcmd -S "IP Address" -U "username" -P "password"
Use WideWorldImporters;
SELECT name
from SYSOBJECTS
WHERE
xtype = 'U'
ogo
```

Or

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



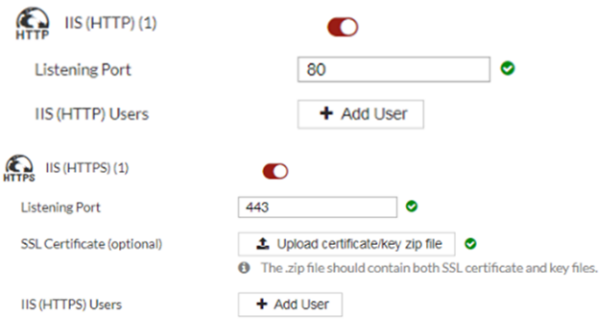
In the image below, you can see the FortiDeceptor create an alerts for the SQL server attack.



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

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

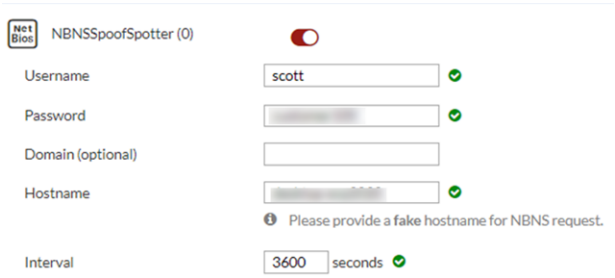
1. Go to *Deception* > *Deployment Wizard*.
2. Click a custom IIS image.



Deploy decoys with a custom NBNSSpoofSpotter image

To deploy decoys with a custom NBNSSpoofSpotter image:

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



NBNSSpoofSpotter 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*.

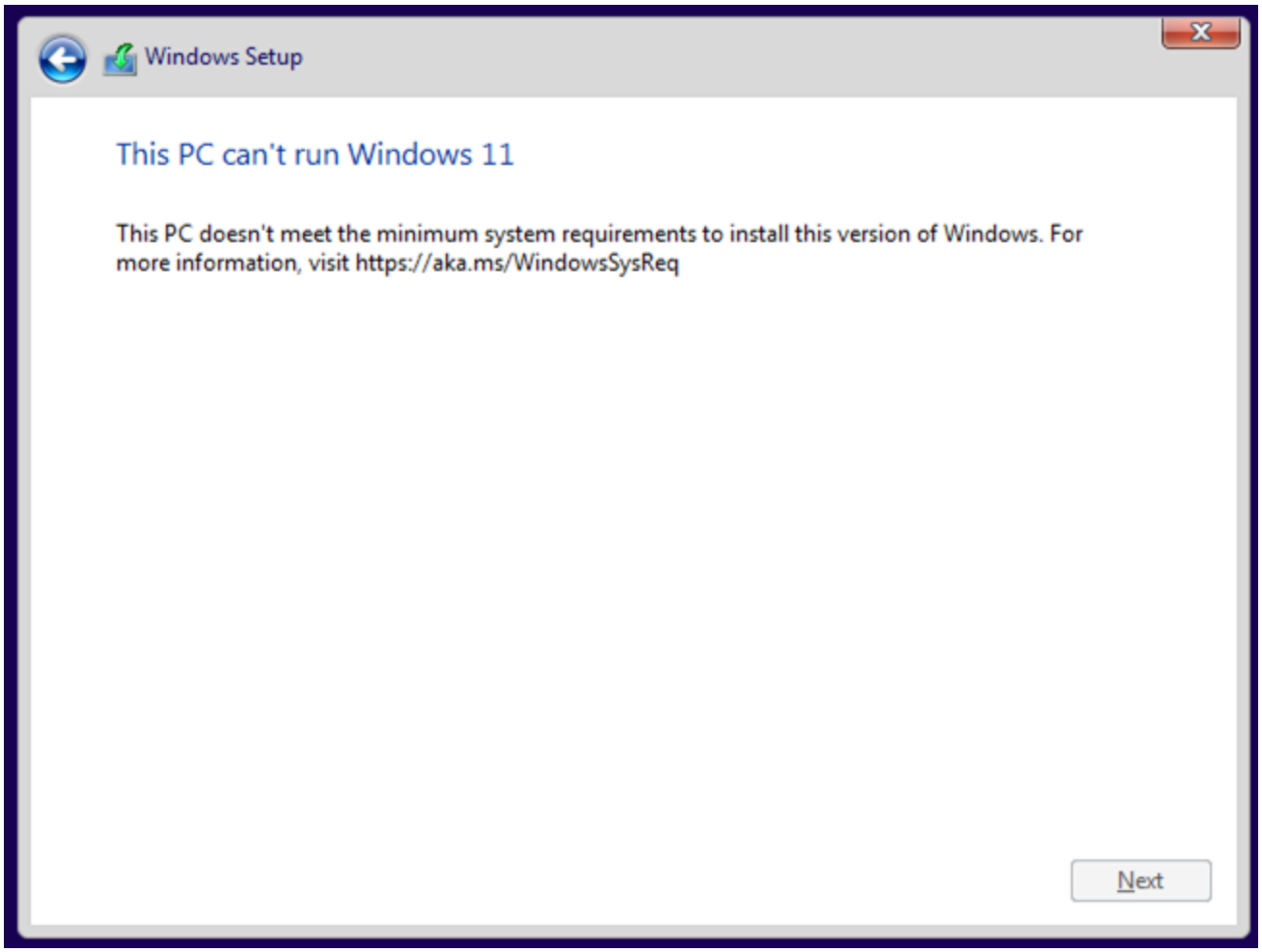
Troubleshooting

The PC does not meet the Windows 11 minimum system requirements

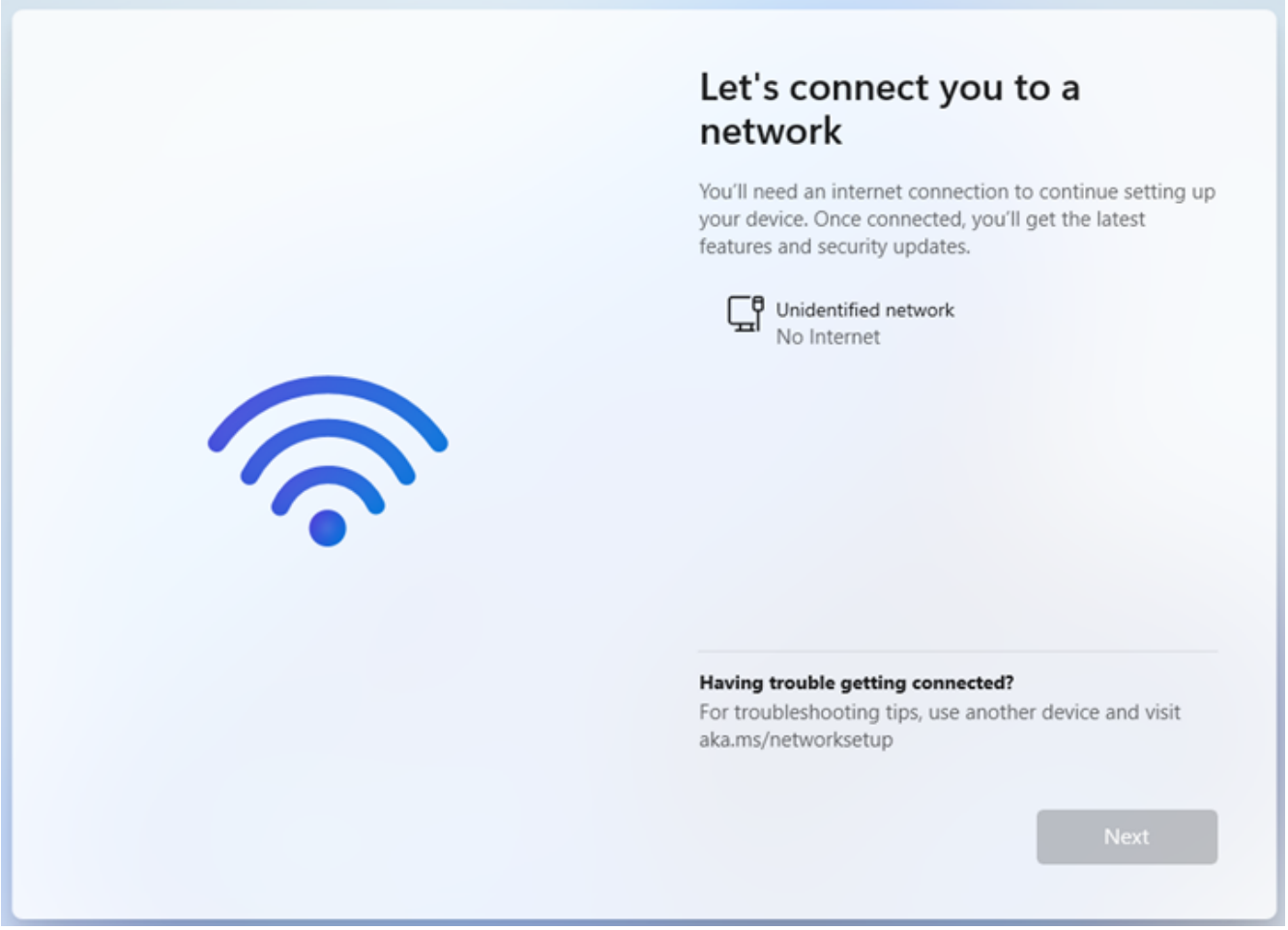
Supported Windows OS versions:

- 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:

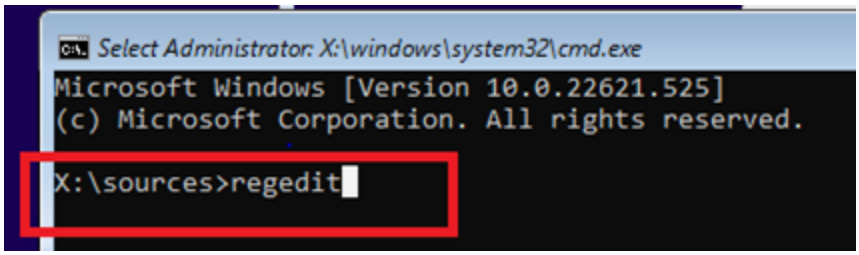


You may also be blocked on the following OOBE page.

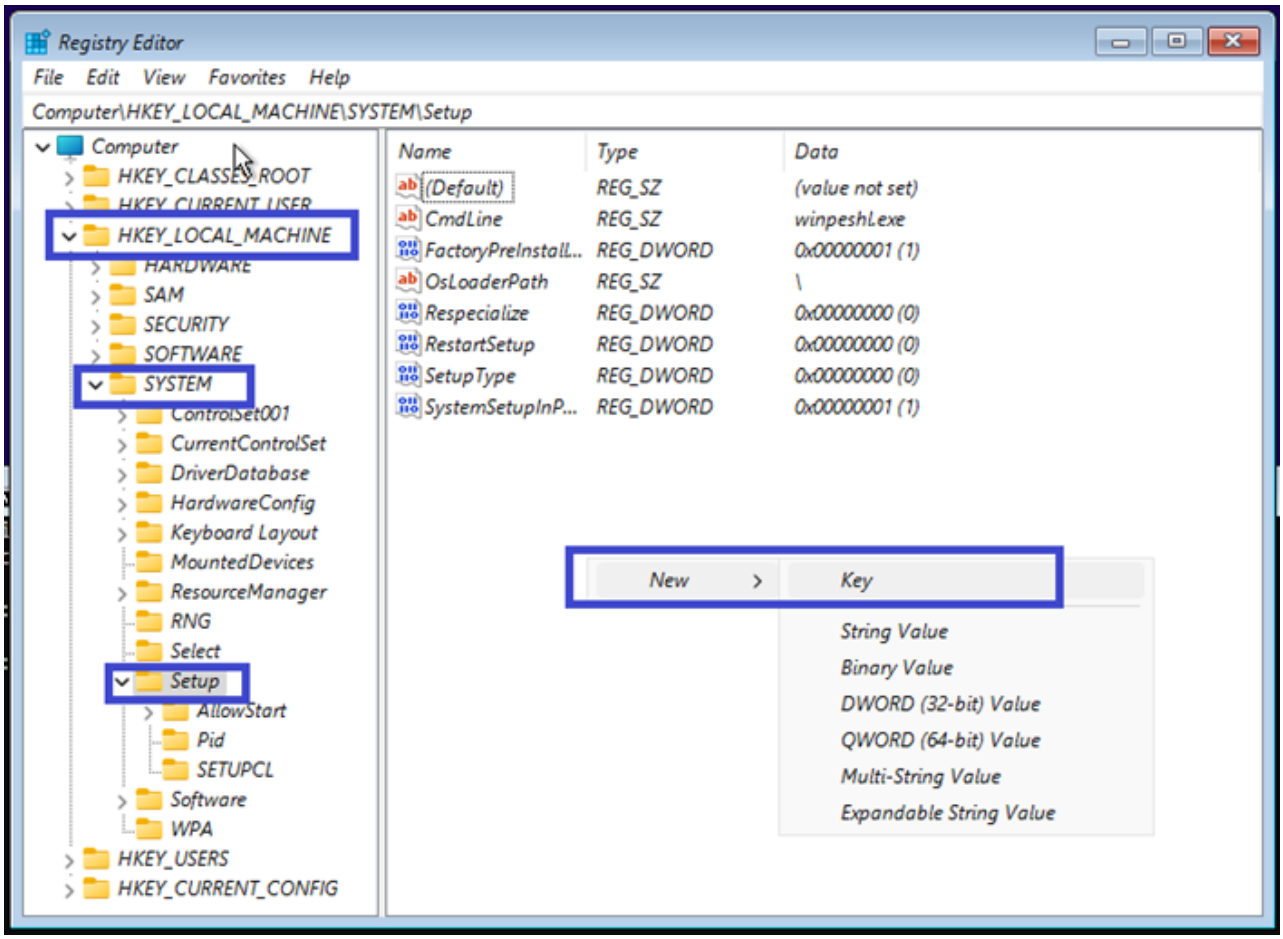


To run Set Bypass TPM and SecureBoot check:

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*.

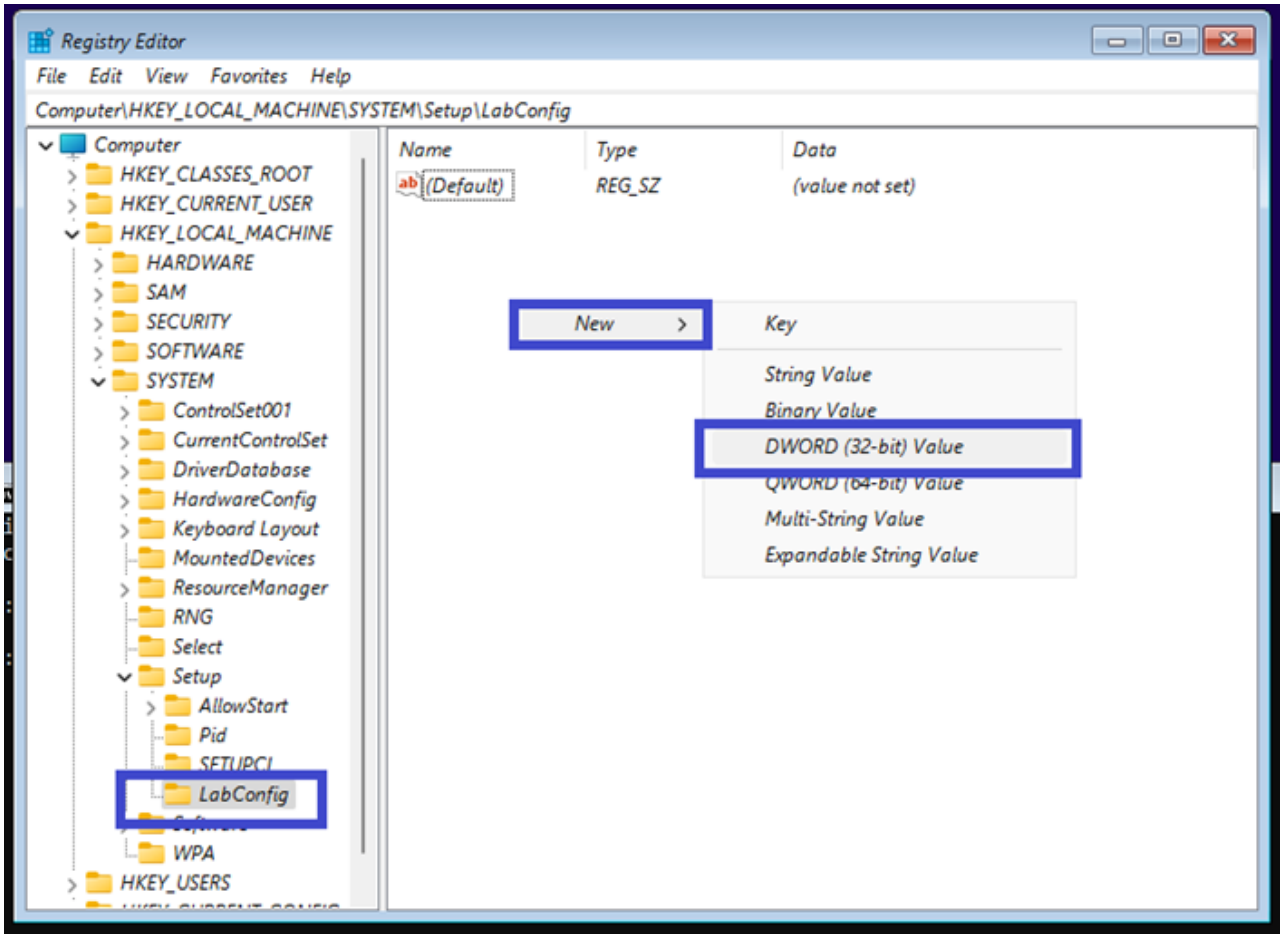


4. Go to *HKEY_LOCAL_MACHINE > SYSTEM> Setup*. Right-click the folder to add a new key folder called `LabConfig`.

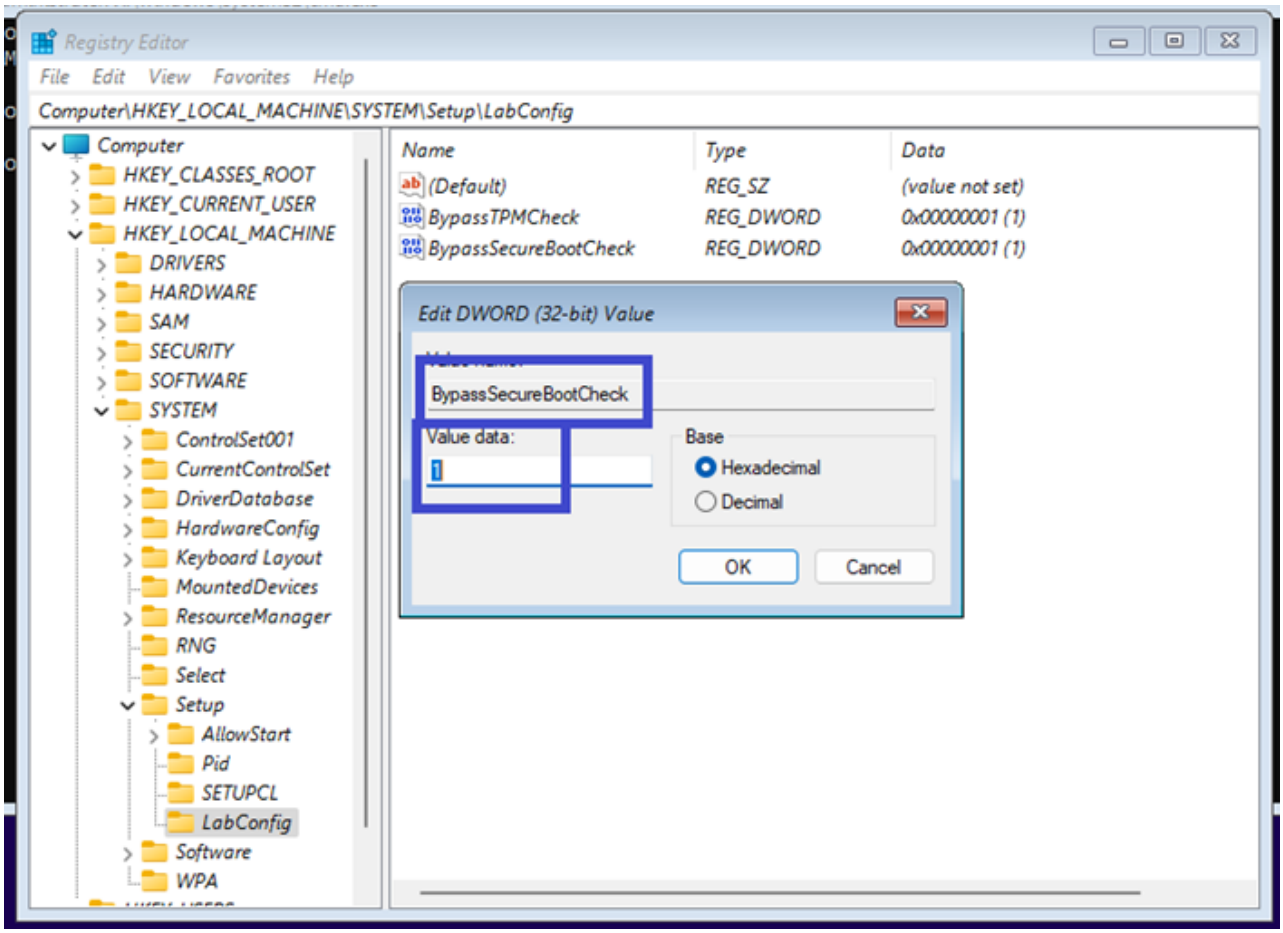


5. Add new value named `BypassTPMCheck`.

6. In the *LabConfig* folder, type REG_DWORD", set it to 1.



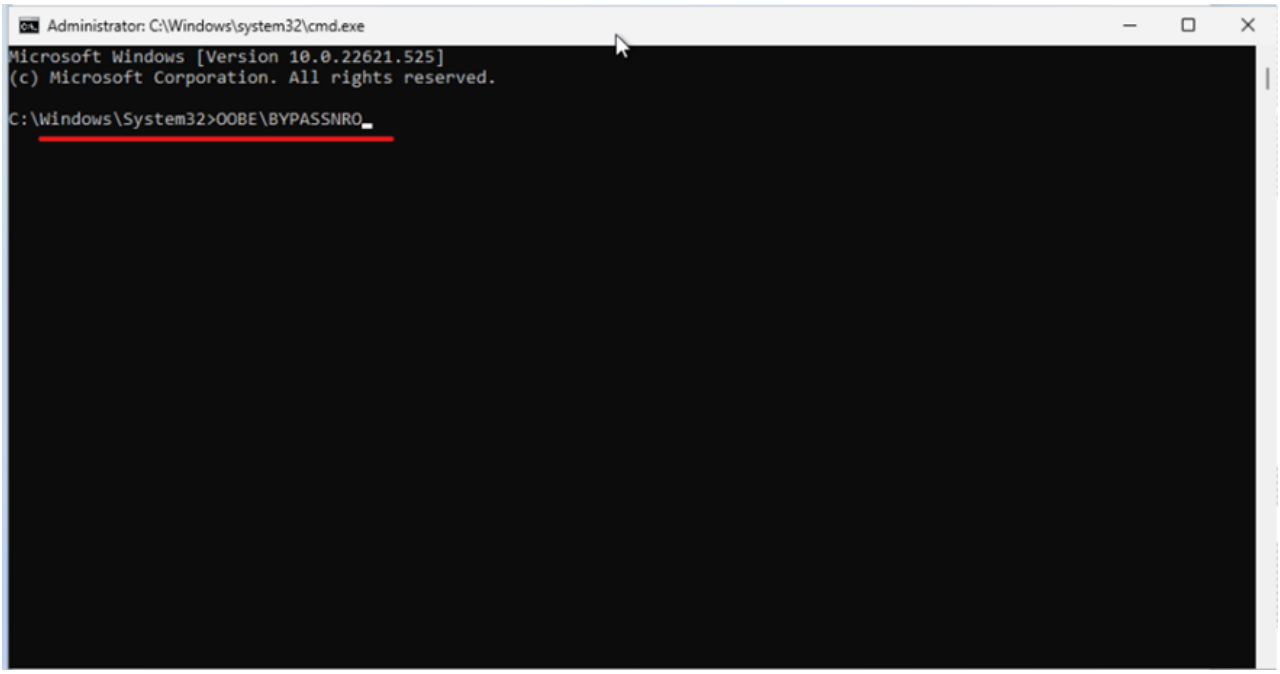
7. In the *LabConfig* folder, add a new value called `BypassSecureBootCheck` then type *REG_DWORD*, and set it to *1*.



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 OOBE:

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*.



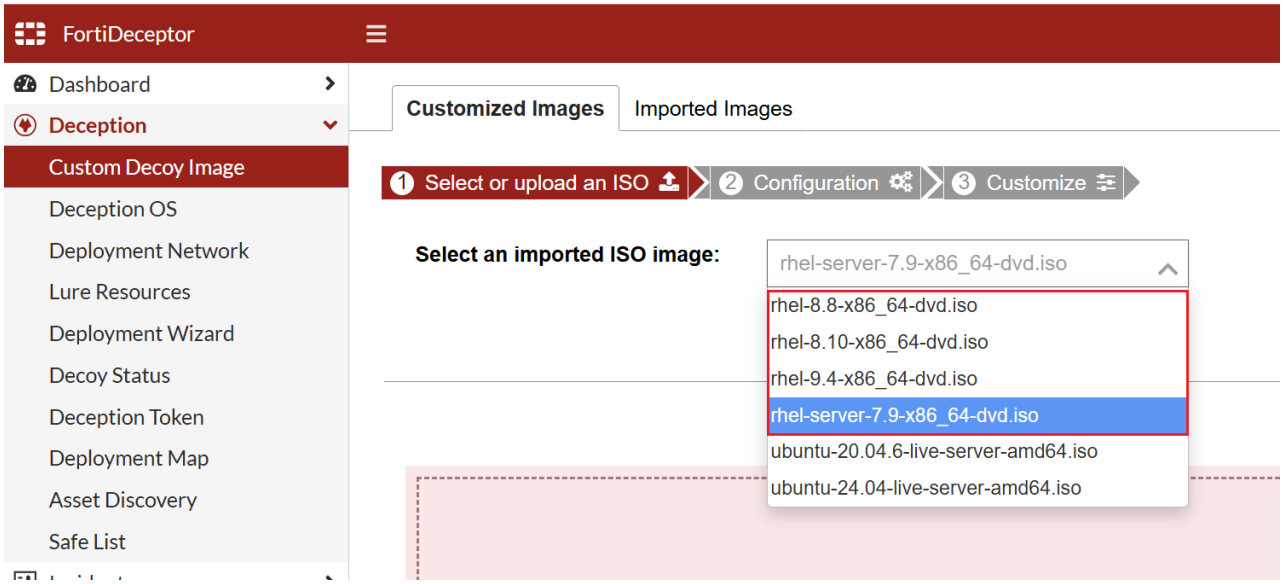
3. Click the *View* icon to review the customization log for the customized image. Click the *Delete* icon to remove the customized image.

Redhat OS

1. Initialize the OS instance

To initialize the OS instance:

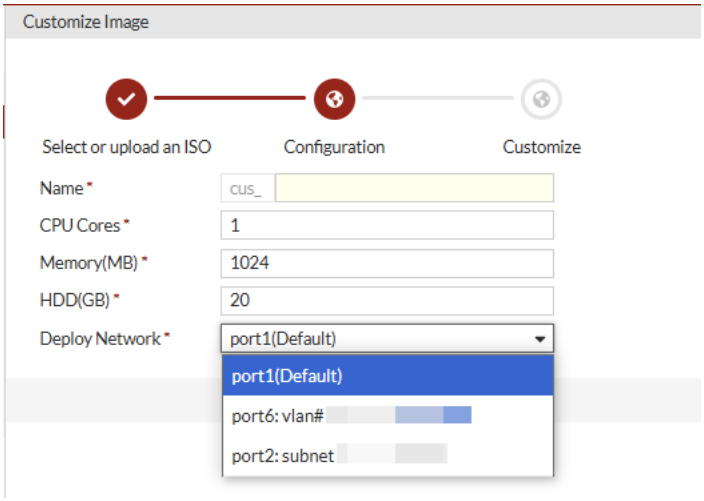
1. Go to *Deception* > *Customization* > *Customized Images*.
2. Click *Import Image and Customize*.



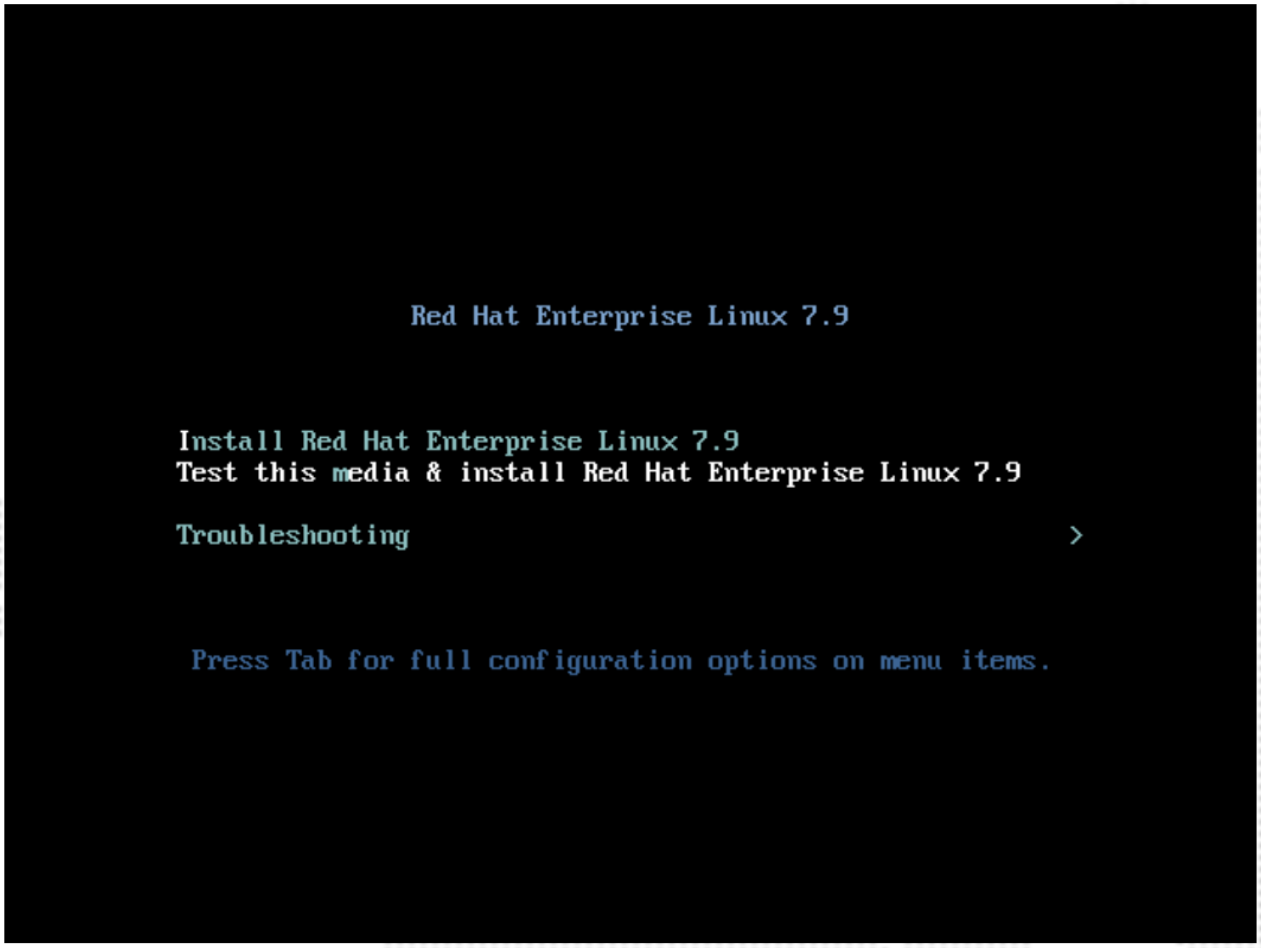
3. Choose an ISO image and click *Next*.
4. Configure the following settings and click *Next*.

Name	Characters in range “A-Za-z0-9-_” , less than 48 characters.	
CPU Cores	1-4	
Memory	1024– 8192 MB.	
Storage	• Minimum: 20 GB • Maximum: Up to the supported hard drive size	
Deploy Network	**Port1**	Default
	PortX	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

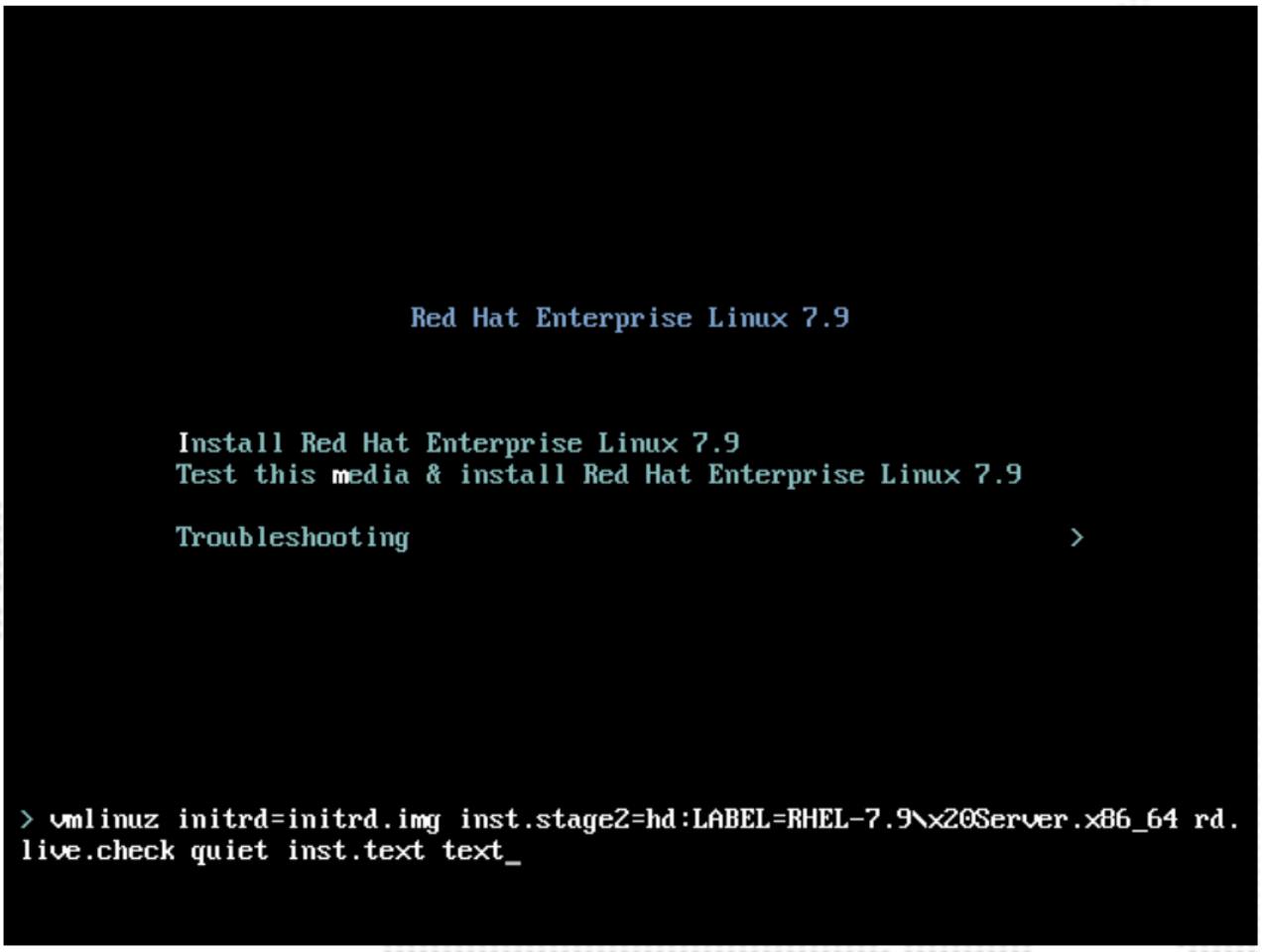


5. In the VNC window, press Tab for full configuration options on menu items.

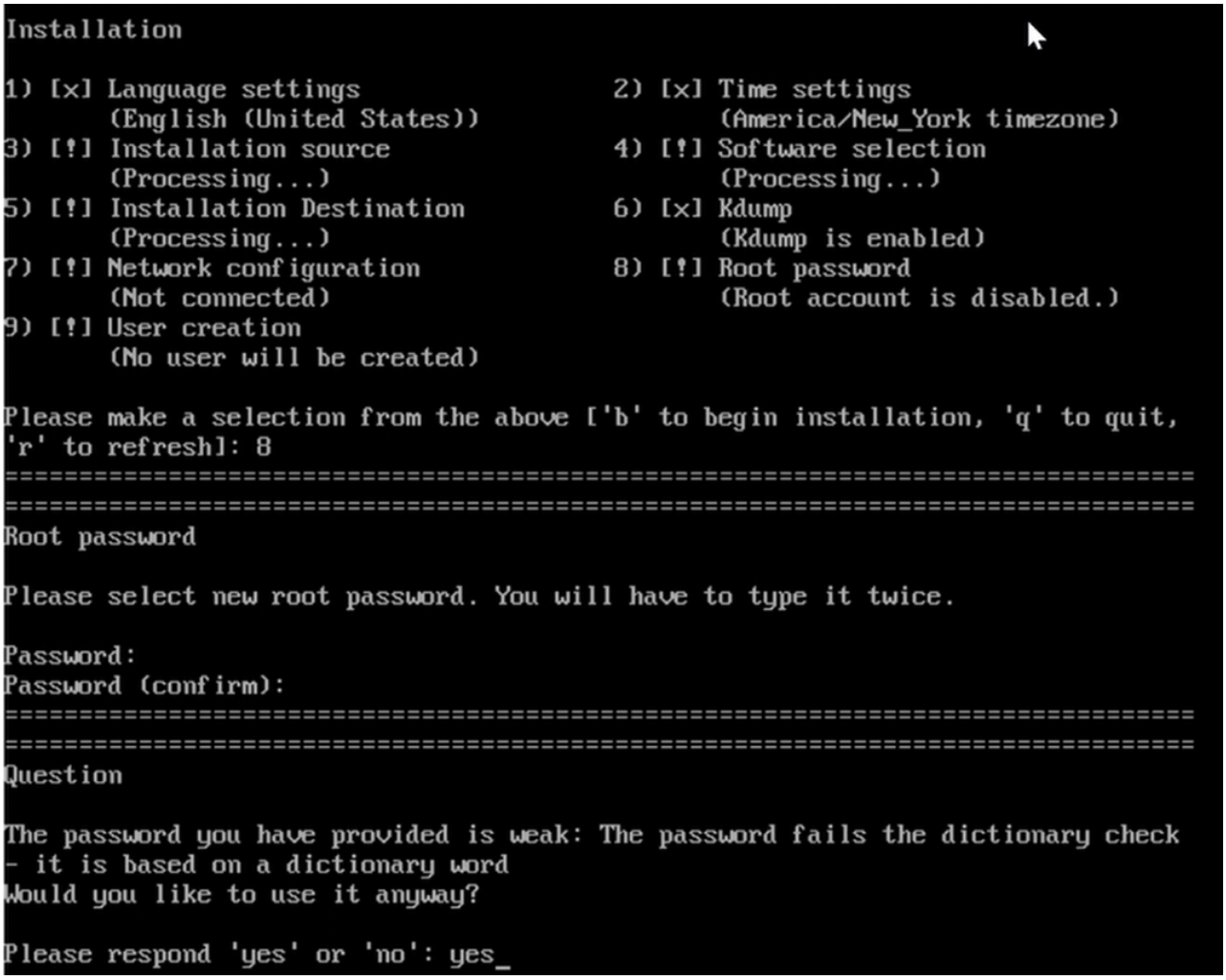


6. Enable the test-based installer mode by adding `inst.text text` at the end of the `vmlinuz` command.

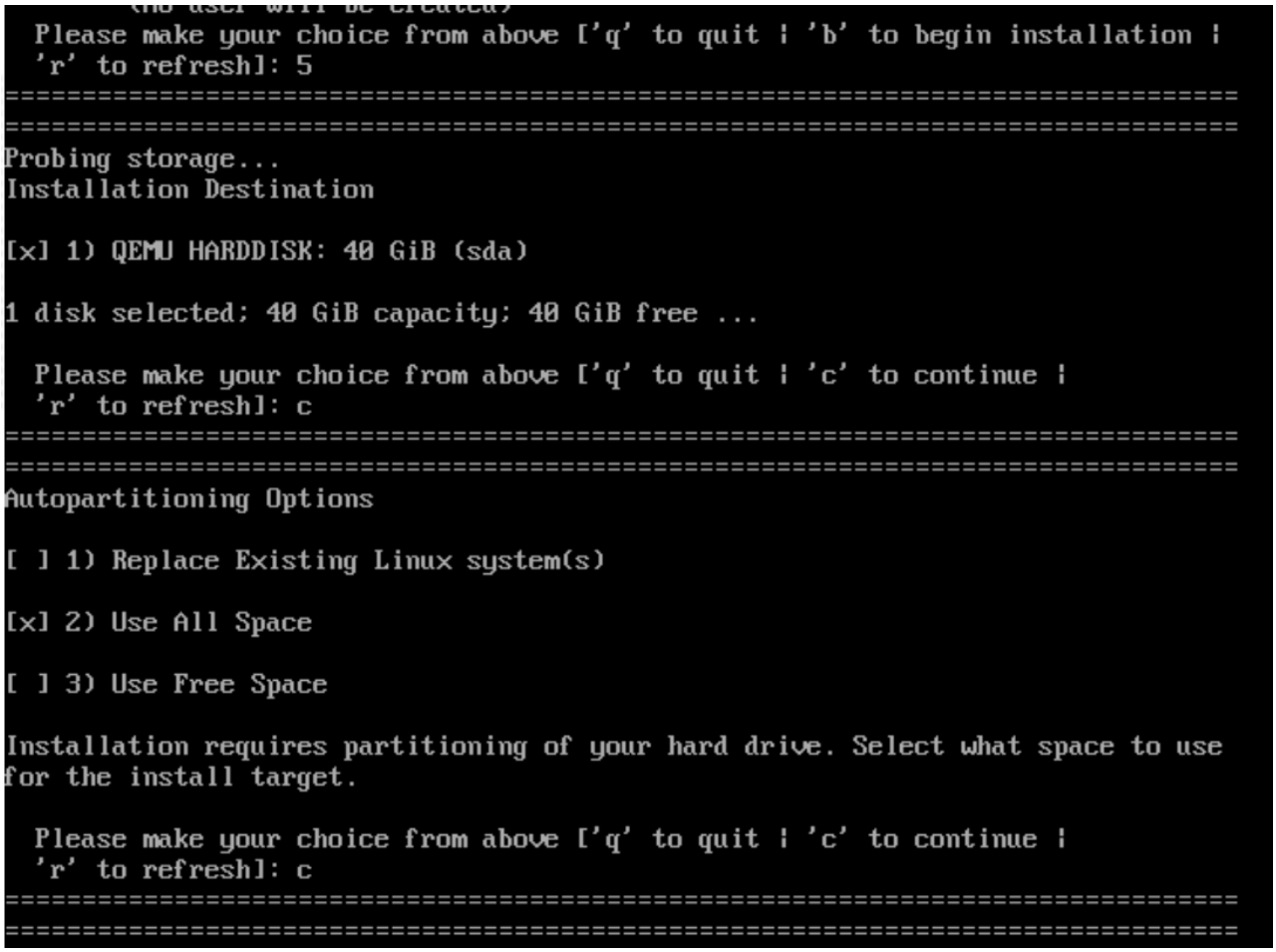
While VNC windows supports the default graphical mode of Red Hat Enterprise Linux (RHEL) installations, the test-based installer mode is recommended for faster and minimal setup.



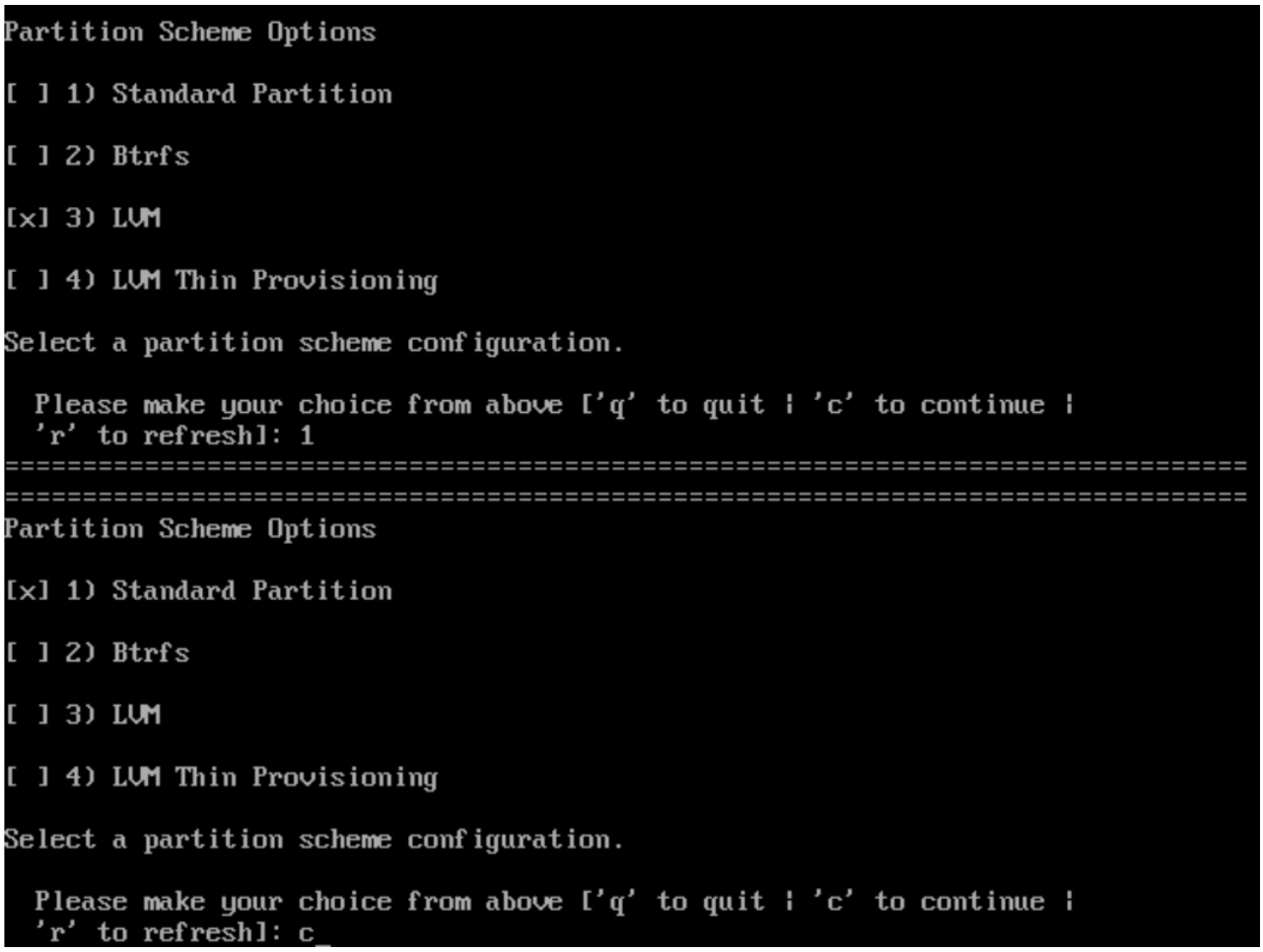
7. Set the root password.



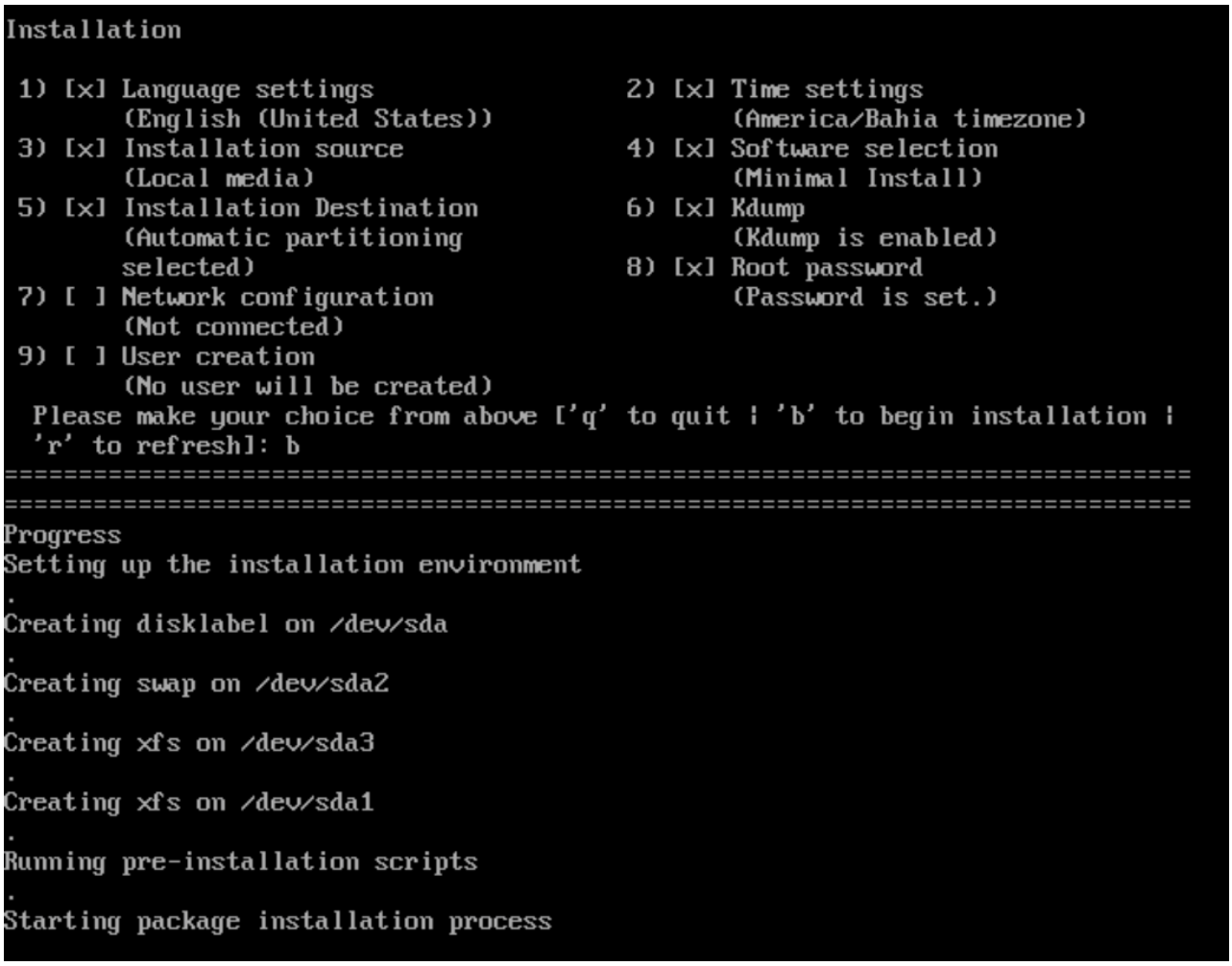
8. Select the installation destination.



Standard Partition is recommended.

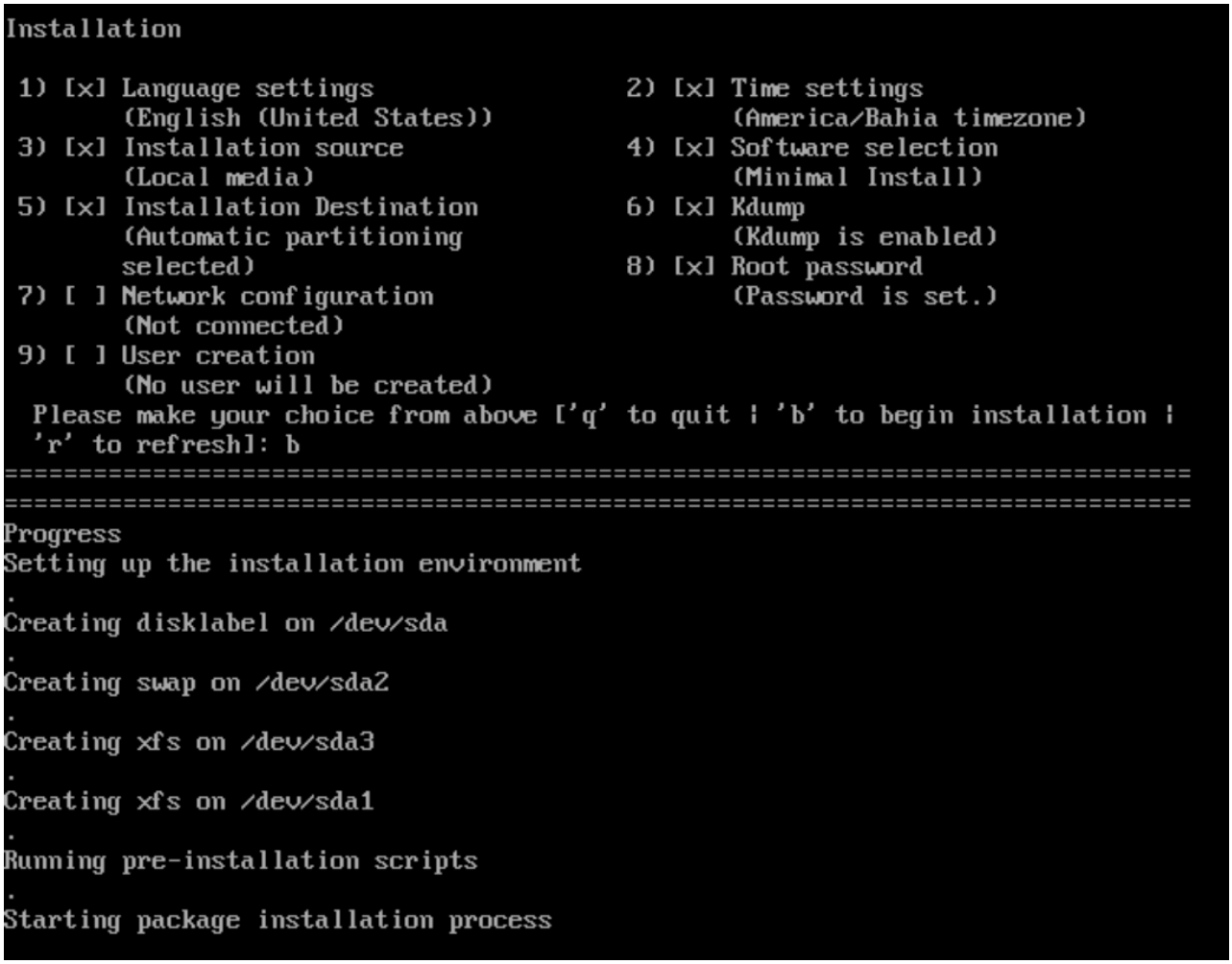

Partition Scheme Options
[ ] 1) Standard Partition
[ ] 2) Btrfs
[x] 3) LVM
[ ] 4) LVM Thin Provisioning
Select a partition scheme configuration.
Please make your choice from above ['q' to quit | 'c' to continue |
'r' to refresh]: 1
Partition Scheme Options
[x] 1) Standard Partition
[ ] 2) Btrfs
[ ] 3)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



```
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.



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.

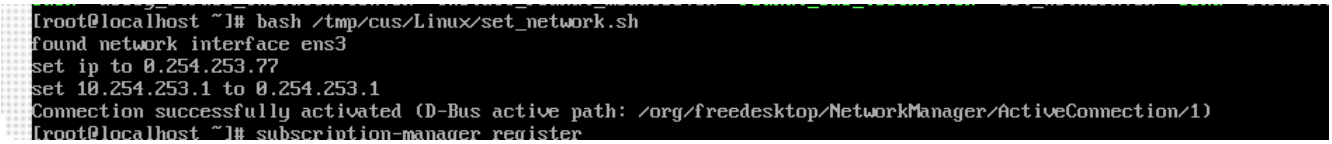
3. Check the file list in this mounted directory.

3. Configure network

You can configure the network automatically or manually.

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

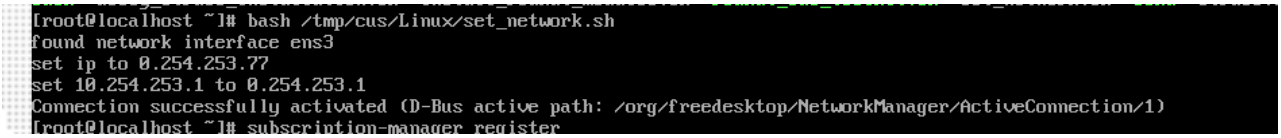
```
bash set_network.sh
```



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. Register the server

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

To register the server:

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

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

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

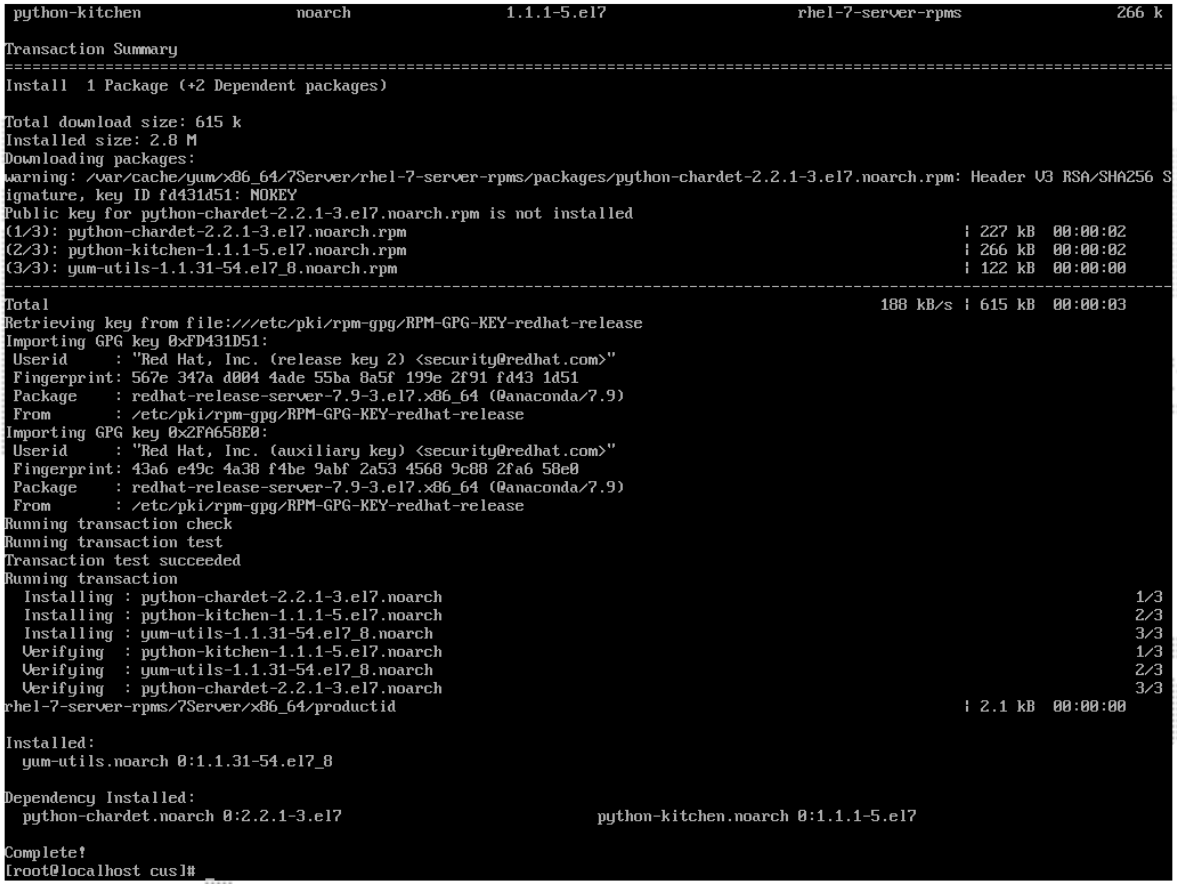
This script will take up to about one hour to run.

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
   ```

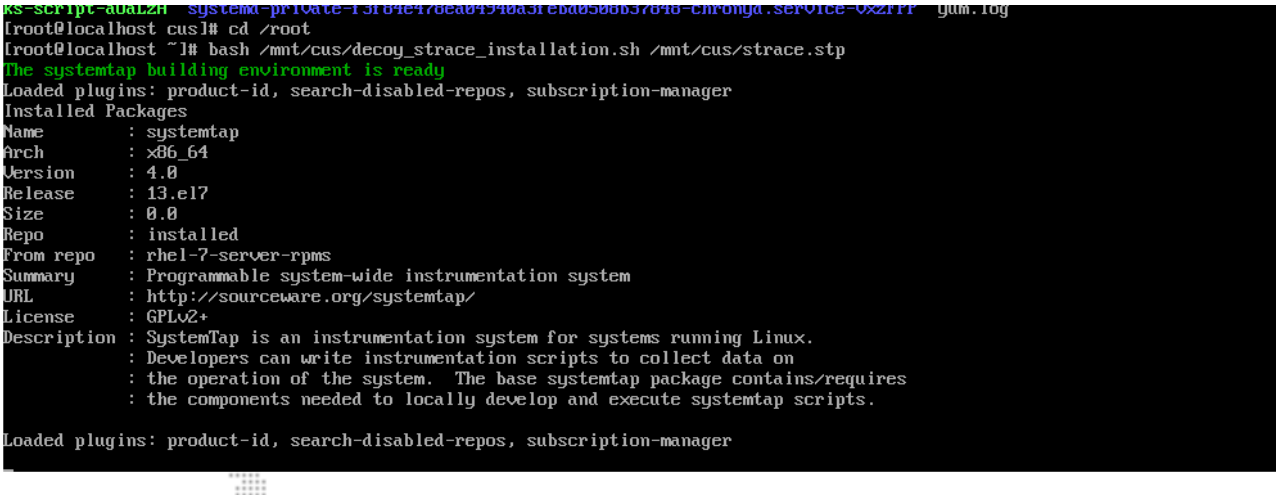


6. Build the custom Linux tracer

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

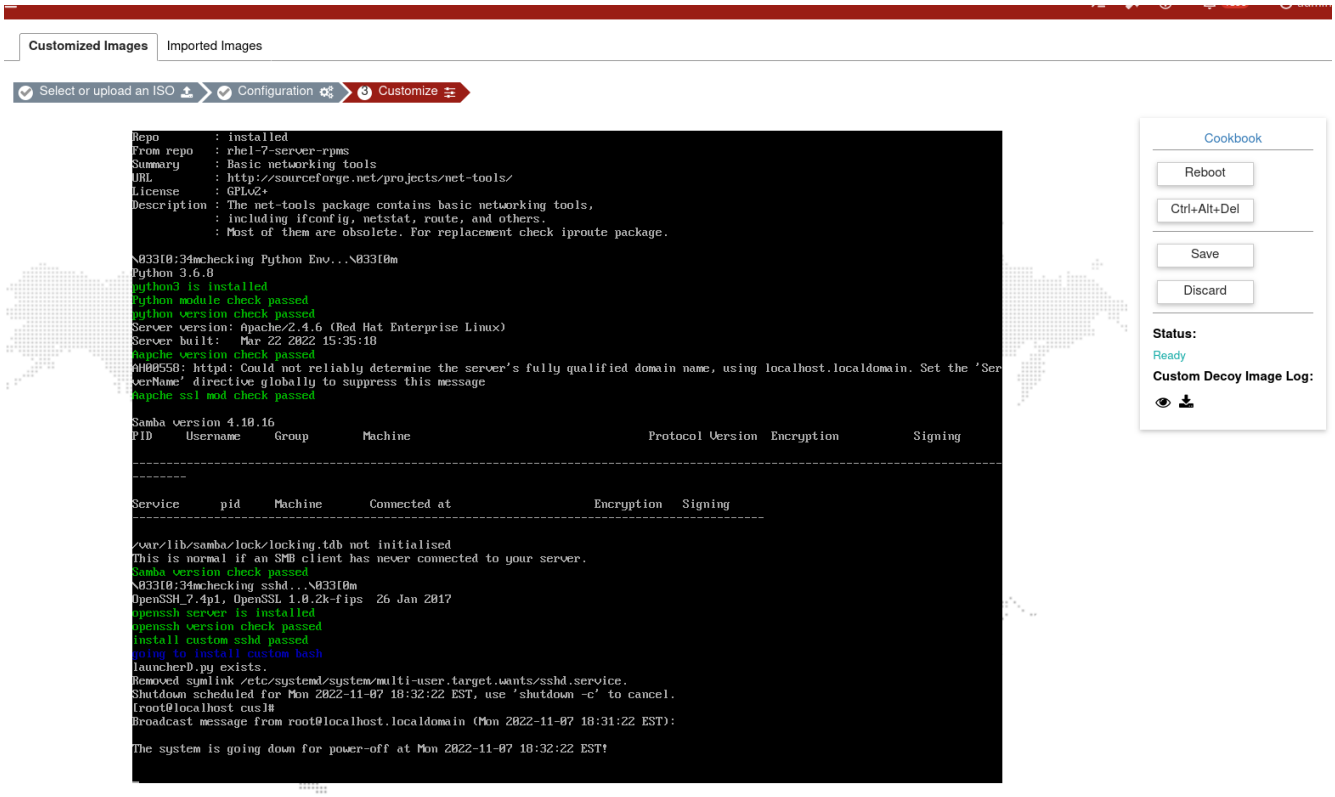


If the build is successful, the output will look like this:

7. Install the FDC toolkit

To install the FDC toolkit:

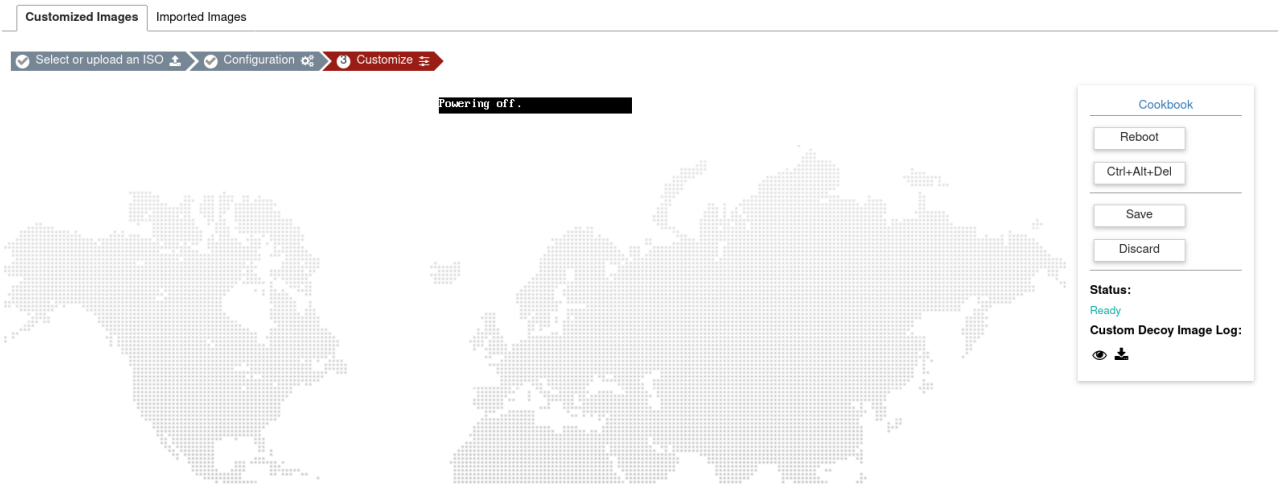
1. Ensure the system customization is completed as expected.
2. Run the following command prompt you for missing packages: `bash redhat_cus_toolkit.sh`
3. Wait for the installation to finish. The system will:
   - Unregister from redhat.com
   - Shut down automatically if there are no errors



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*.

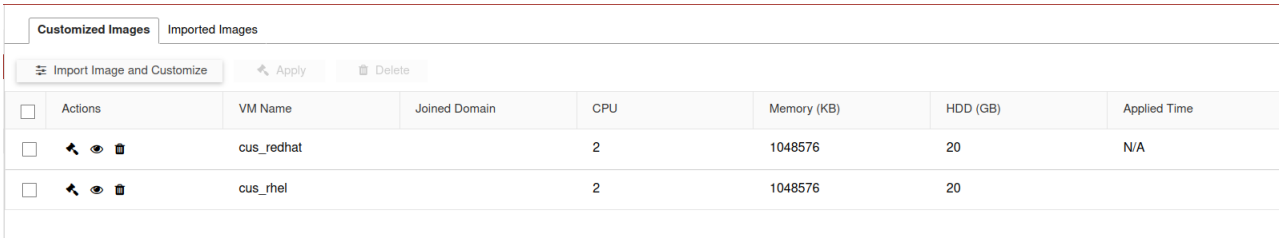


2. Click *Save* when the system is powered off.

9. Review the result

To review the result:

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



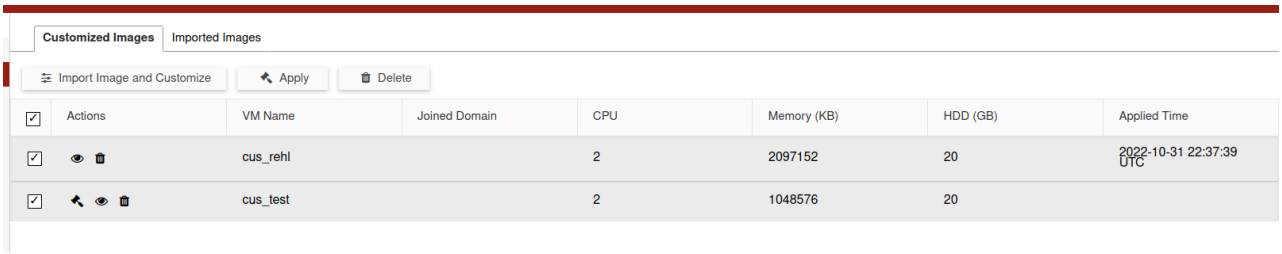
2. (Optional) Click the *Delete* button to remove the custom image.

10. Use the custom Redhat image

Apply the custom images

To apply a custom image:

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

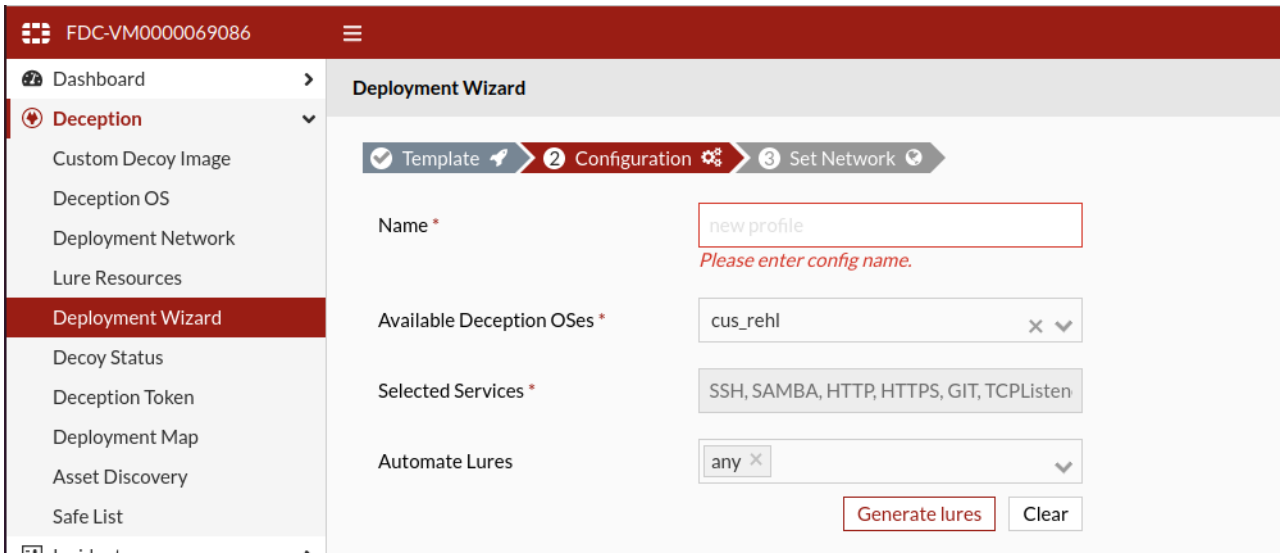


2. Select a customized image and click *Apply*. he applied image is displayed in the *Deception OS* table. It may take several minutes for the image to appear in the table.

Deploy decoys with custom 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.

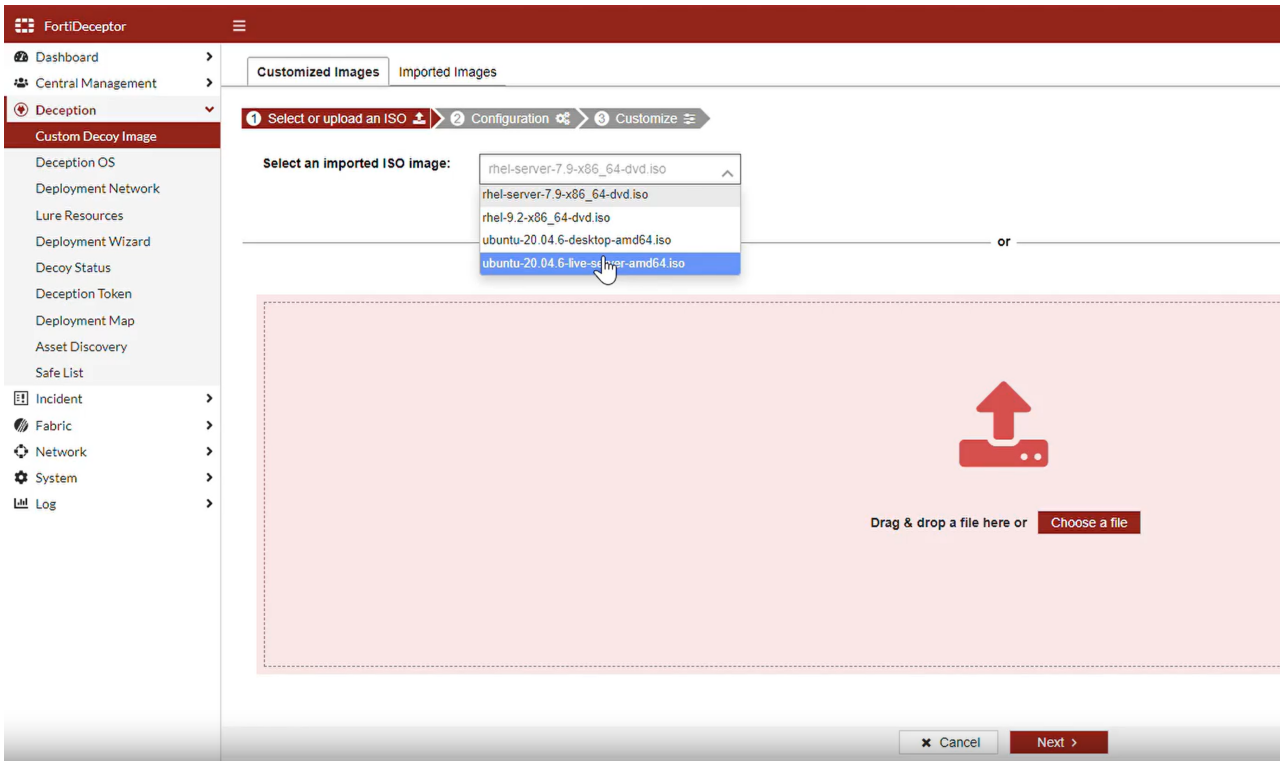


Ubuntu OS

1. Initialize the OS instance

To initialize the OS instance:

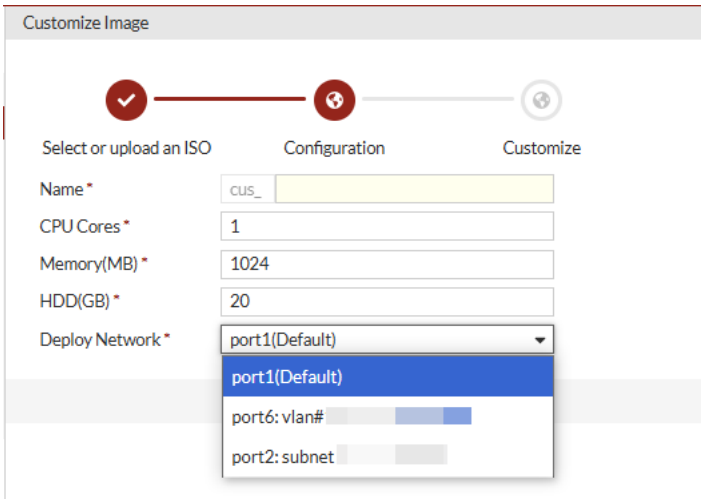
1. Go to *Deception* > *Customization* > *Customized Images*.
2. Click *Import Image and Customize*.
3. Choose an ISO image and click *Next*.



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

Name	Characters in range “A-Za-z0-9-_” , less than 64 characters.
CPU Cores	1 - 4
Memory	1024 – 8192 MB.
Storage	• Minimum: 20 GB • Maximum: Up to the supported hard drive size

Deploy Network	**Port1**	Default
	PortX	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



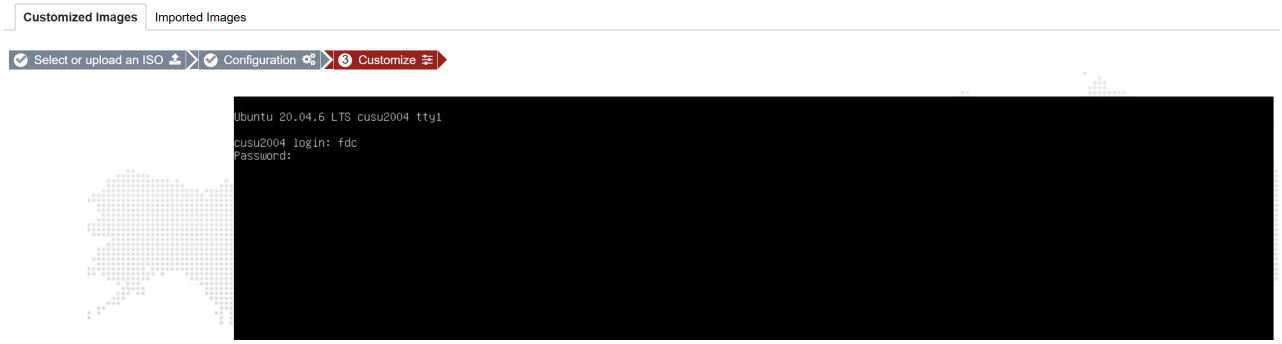
To configure the system setting in the VNC Windows

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 Ubunto 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,



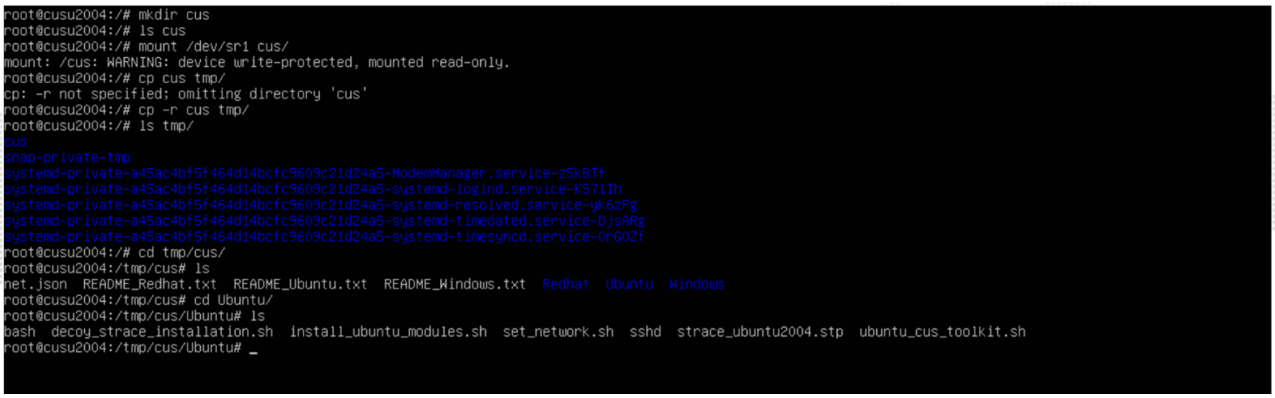
2. Access the `root` directory.
3. Create a new directory and give it a name (for example, `/cus`) using the terminal command: `mkdir <directory_name>`
   Example: `mkdir cus`
4. Mount the `/dev/sr1` directory to the directory you just created with terminal command: `mount /dev/sr1 <directory_name>/`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

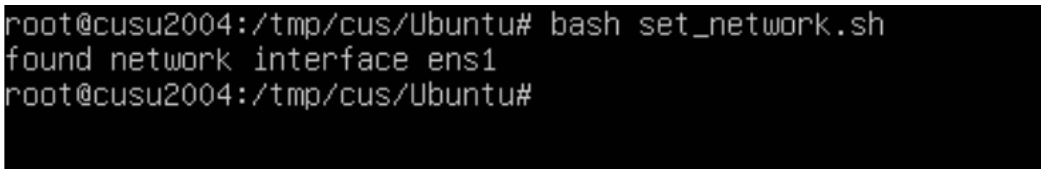


3. Configure network

You can configure the network automatically or manually.

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

`bash set_network.sh`



Option B: Configure the network manually.

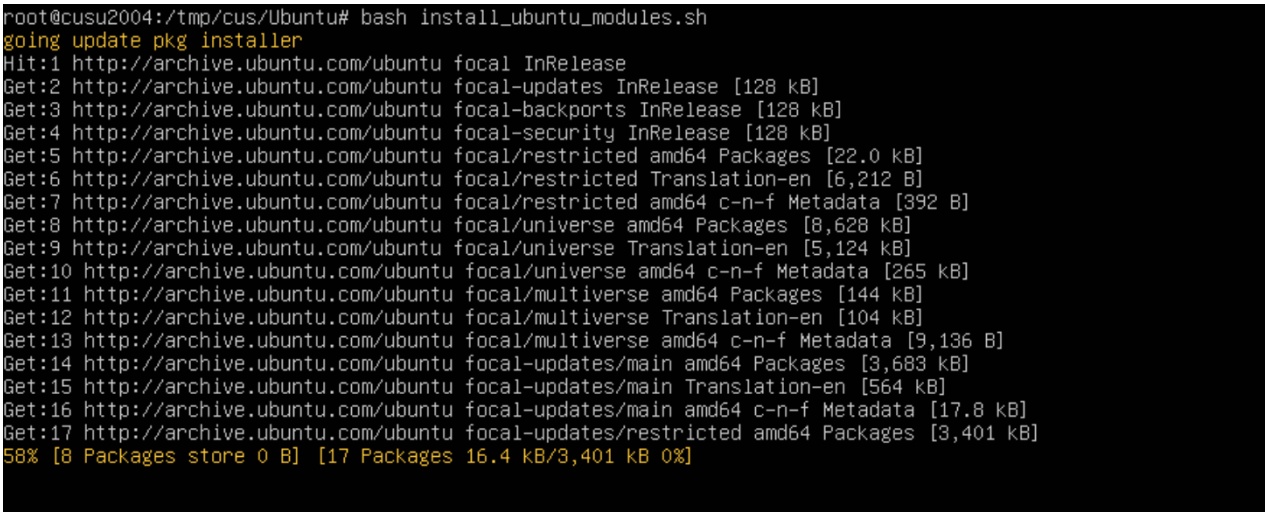
1. Open and read the setting file `net.json`.
2. Follow the settings to configure the IP, gateway, DNS.
3. After you are done, verify your network can access the internet.

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`

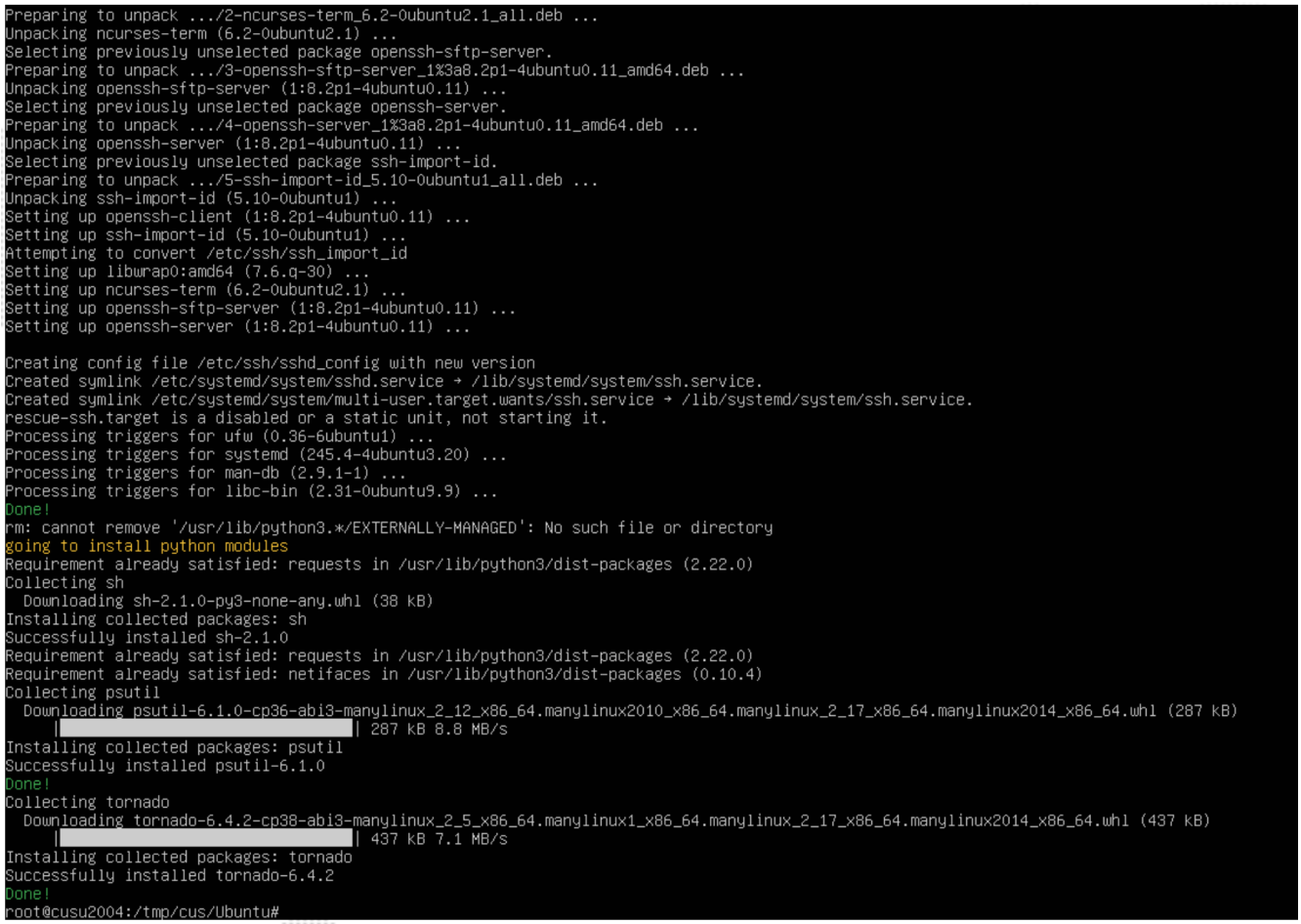


This script will take up to about one hour to run.

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
```



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.Ega2Ch7I14/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-keys C8CAB6595FDFF622
gpg: key C8CAB6595FDFF622: 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 'vwmgfx'
Pass 1: parsed user script and 476 library scripts using 102984virt/91088res/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: identif
ier '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/stapLxXAGN/vwmgfx_src.c" using 178700virt/168496res/8992shr/159456data kb, in 40usr/10sys/57real ms.
vwmgfx.ko
Pass 4: compiled C into "vwmgfx.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-dbgsym
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
  linux-image-5.4.0-144-generic-dbgsym
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-dbgsym (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-dbgsym
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-dbgsym (5.4.0-144.161) ...
root@cusu2004:/tmp/cus/Ubuntu# _
```

6. Install the FDC toolkit

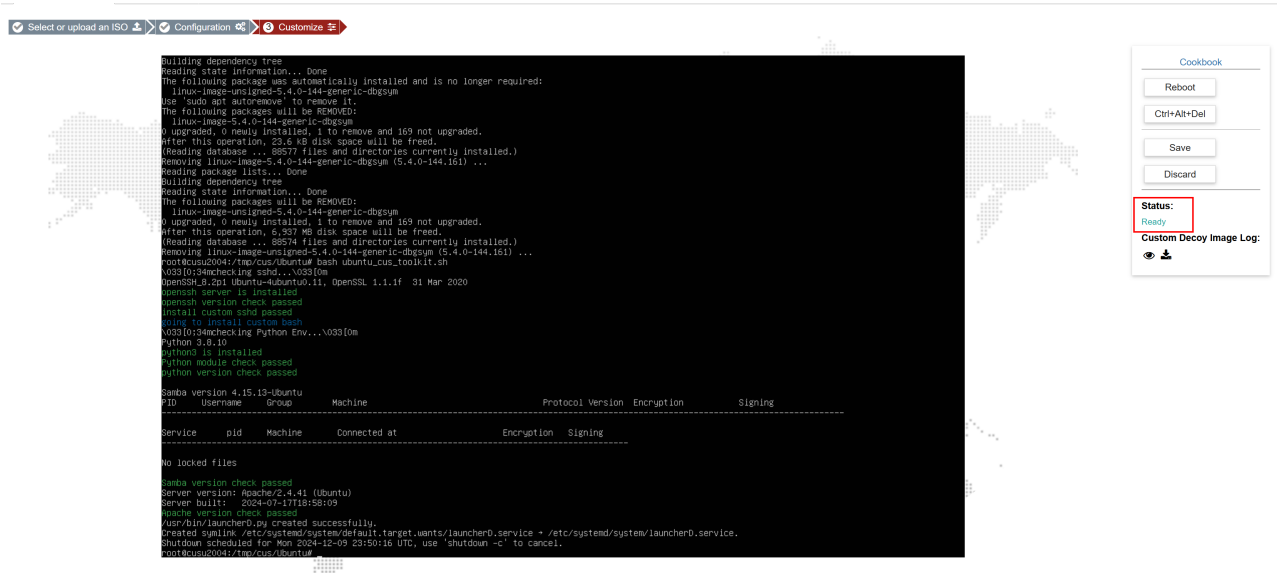
To install the FDC toolkit:

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

7. Save the custom Image

To save the custom image:

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

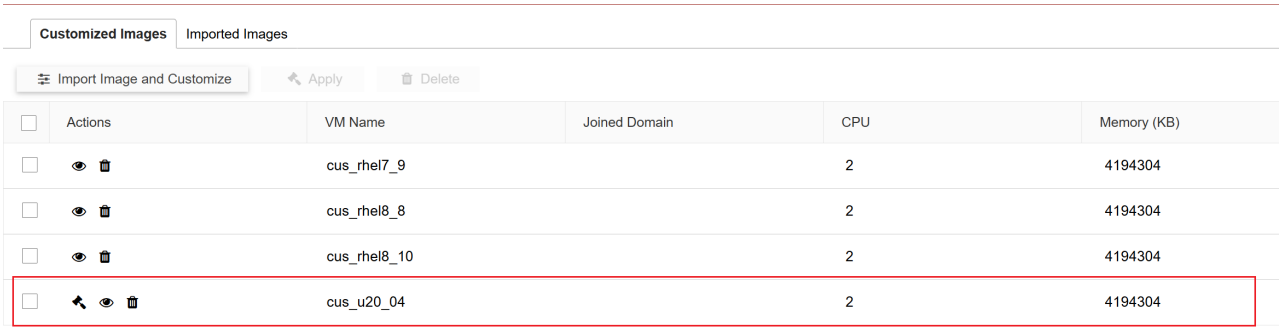


2. Click *Save* when the system is powered off.

8. Review the result

To review the result:

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



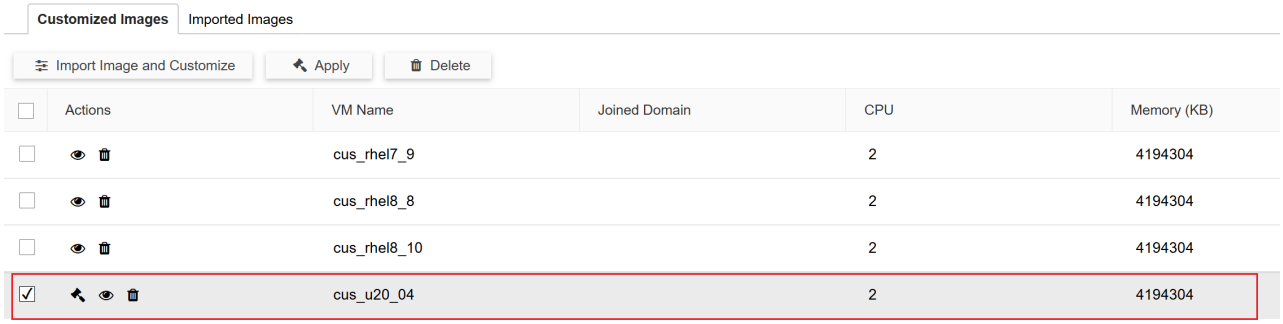
2. (Optional) Click the *Delete* button to remove the custom image.

9. Use the custom Ubuntu image

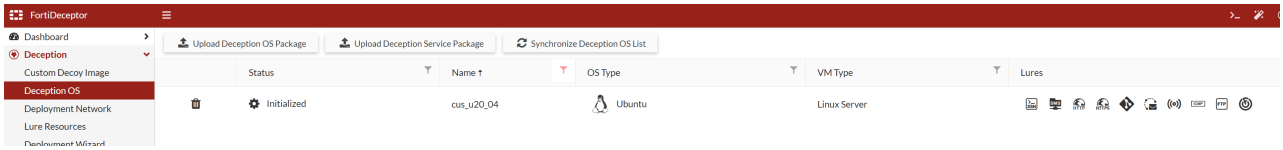
Apply the custom images

To apply a custom image:

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



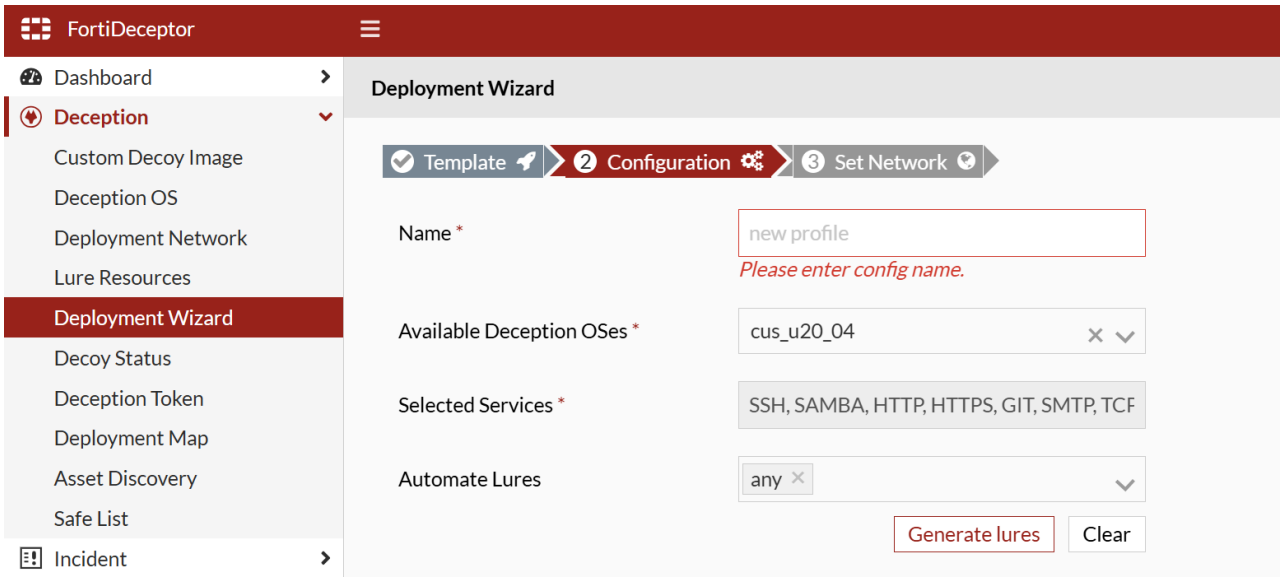
2. Select a customized image and click *Apply*. The applied image is displayed in the *Deception OS* page. It may take several minutes for the image to appear in the table.



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.

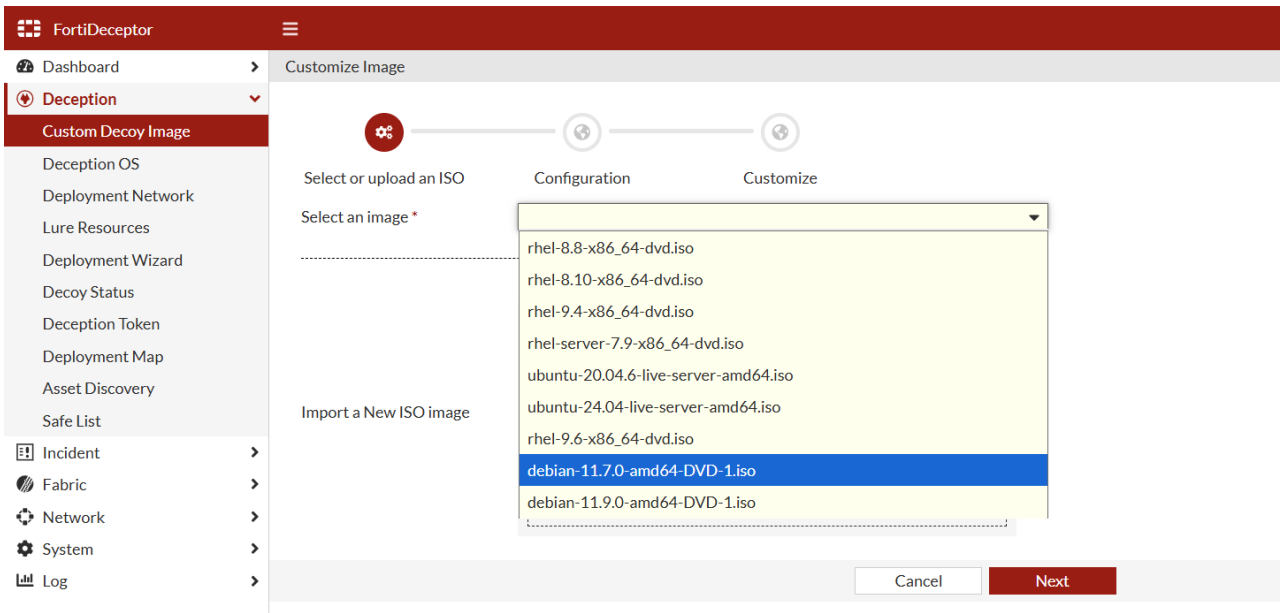

FortiDeceptor
Dashboard
Deception
Custom Decoy Image
Deception OS
Deployment Network
Lure Resources
Deployment Wizard
Decoy Status
Deception Token
Deployment Map
Asset Discovery
Safe List
Incident
Deployment Wizard
Template
2 Configuration
3 Set Network
Name *
new profile
Please enter config name.
Available Deception OSes *
cus_u20_04
Selected Services *
SSH, SAMBA, HTTP, HTTPS, GIT, SMTP, TCF
Automate Lures
any
Generate lures
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*.

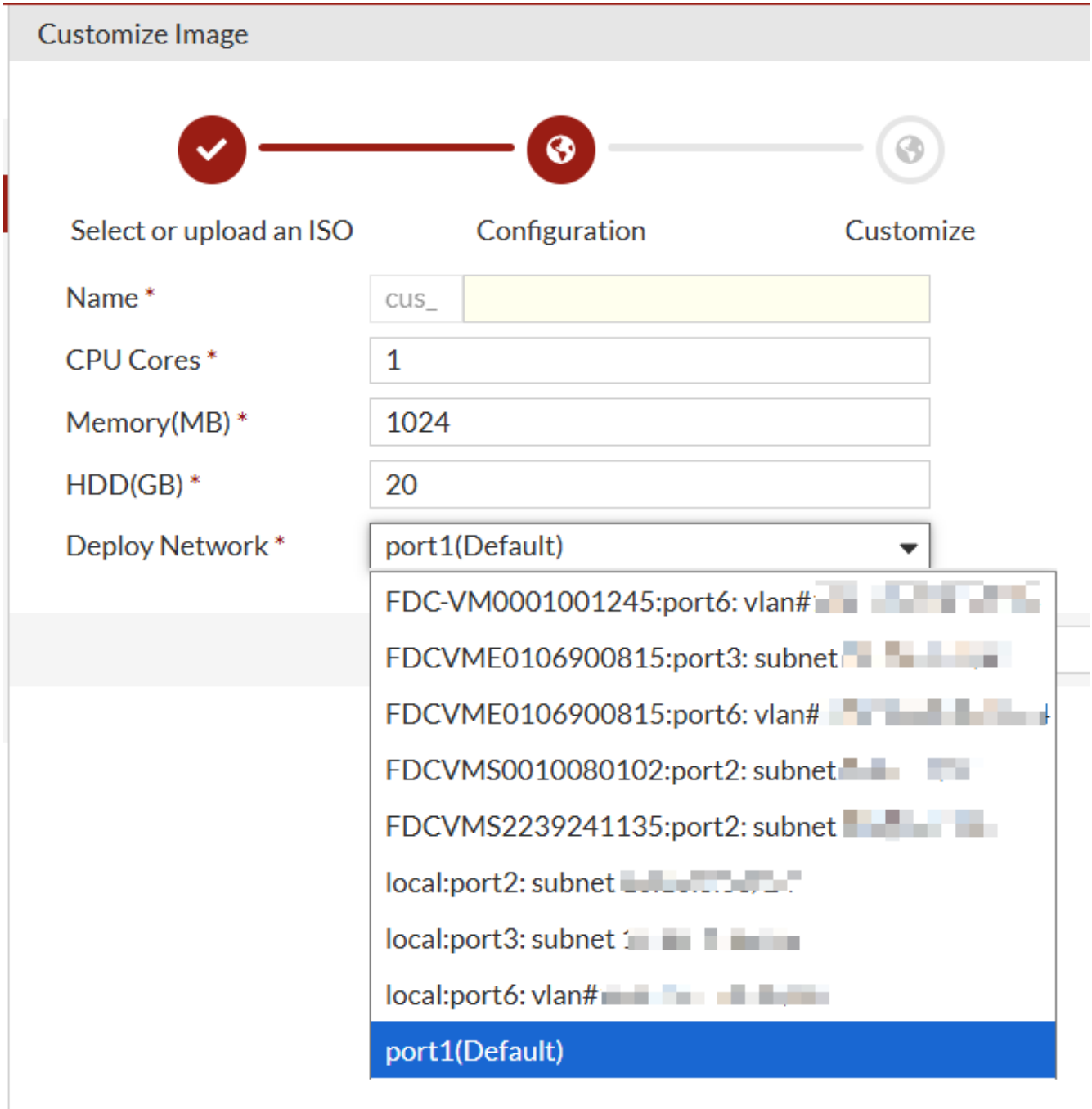


4. Configure the following settings and click *Next*.

Name	Characters in range “A-Za-z0-9-_” , less than 64 characters.	
CPU Cores	1 – 4	
Memory	1024 – 8129 MB 2048 MB recommended for graphical system	
Storage	• Minimum: 20 GB • Maximum: Up to the supported hard drive size	
Deploy Network	**Port1**	Default
	PortX	Select the deployment network.

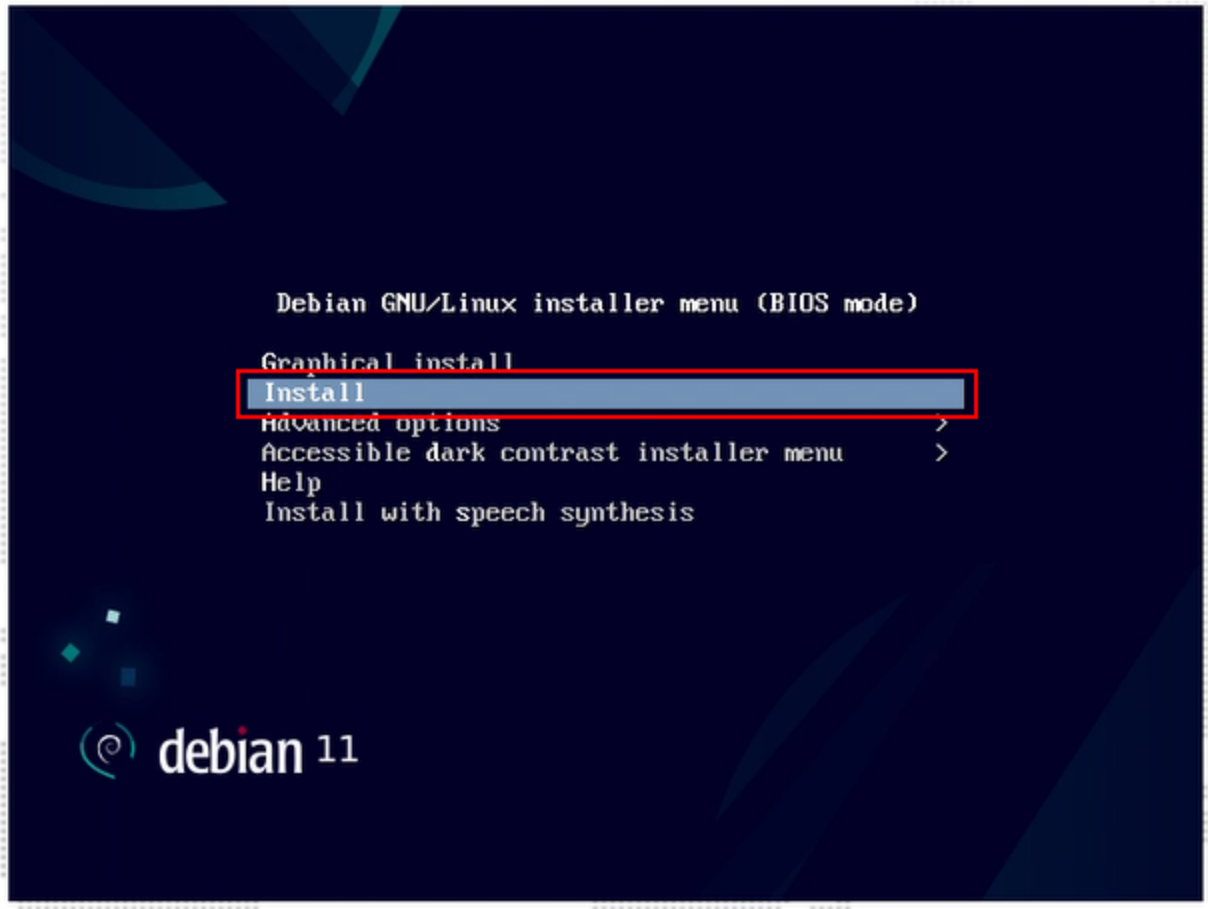
Ensure specified IP is not already in use and the following settings align with the PortX configuration:

- IP/Mask
- Gateway
- DNS

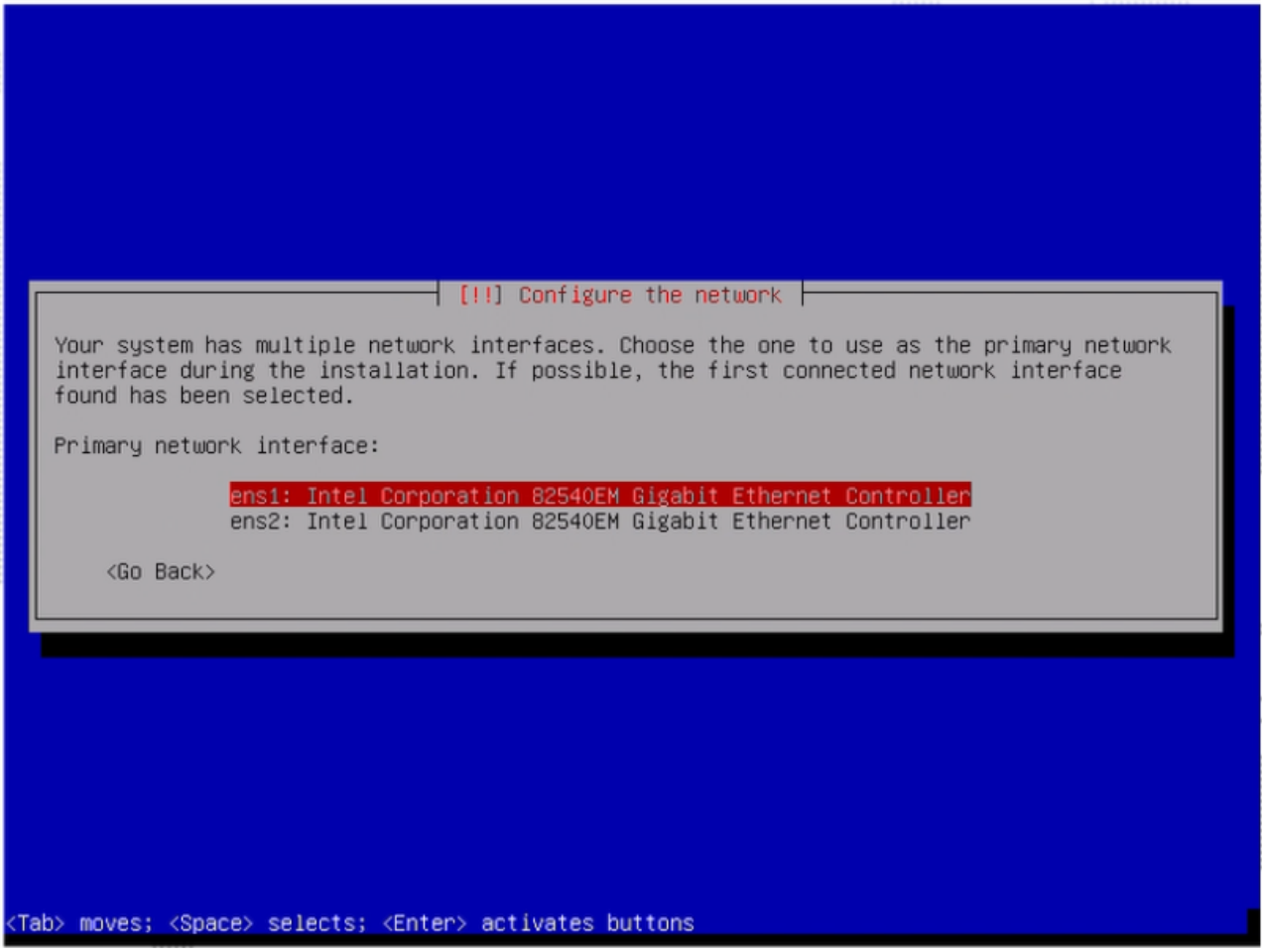


To configure the system setting in the VNC window

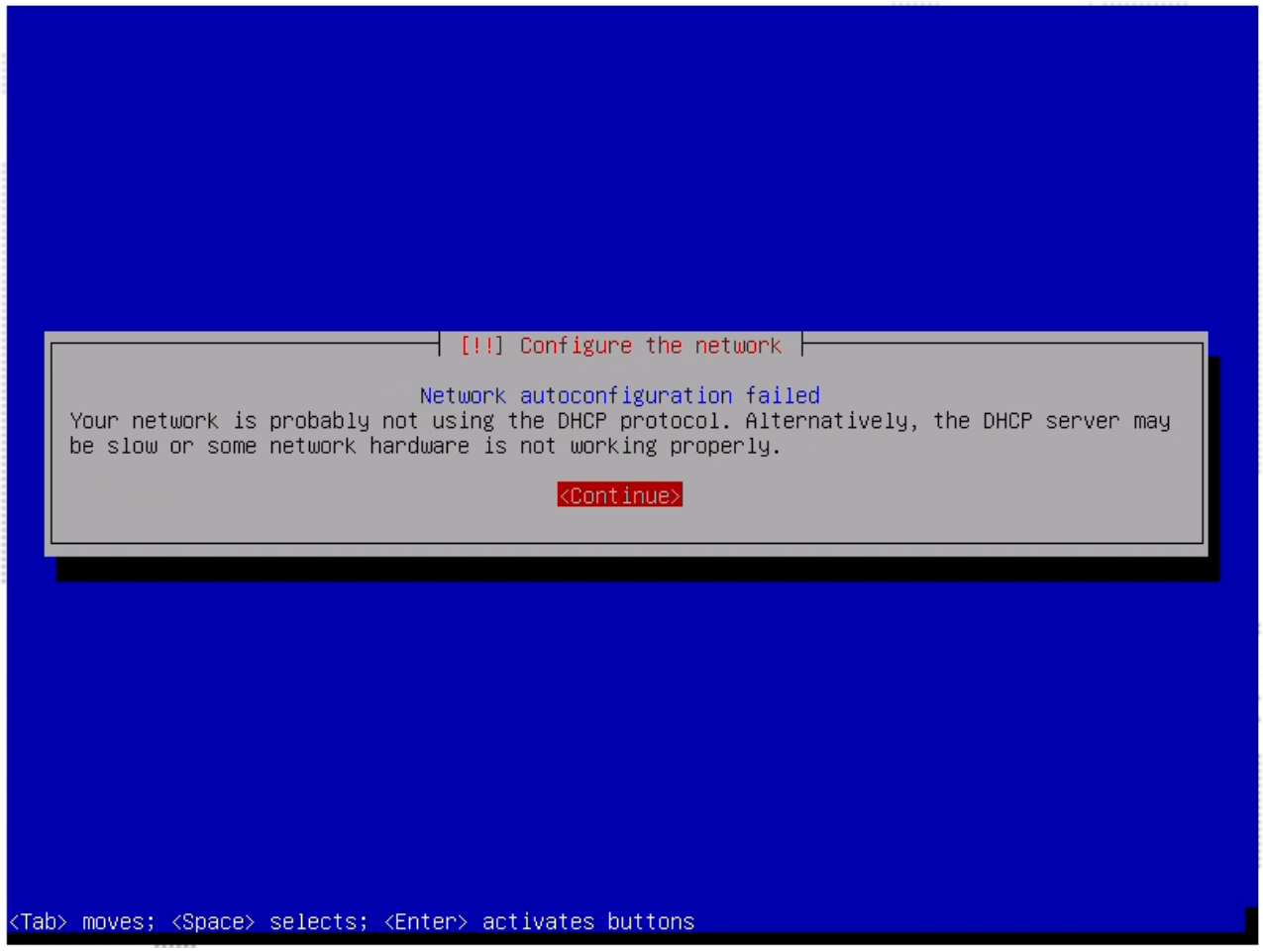
1. In the *Welcome* window, select the text-based *Install* option



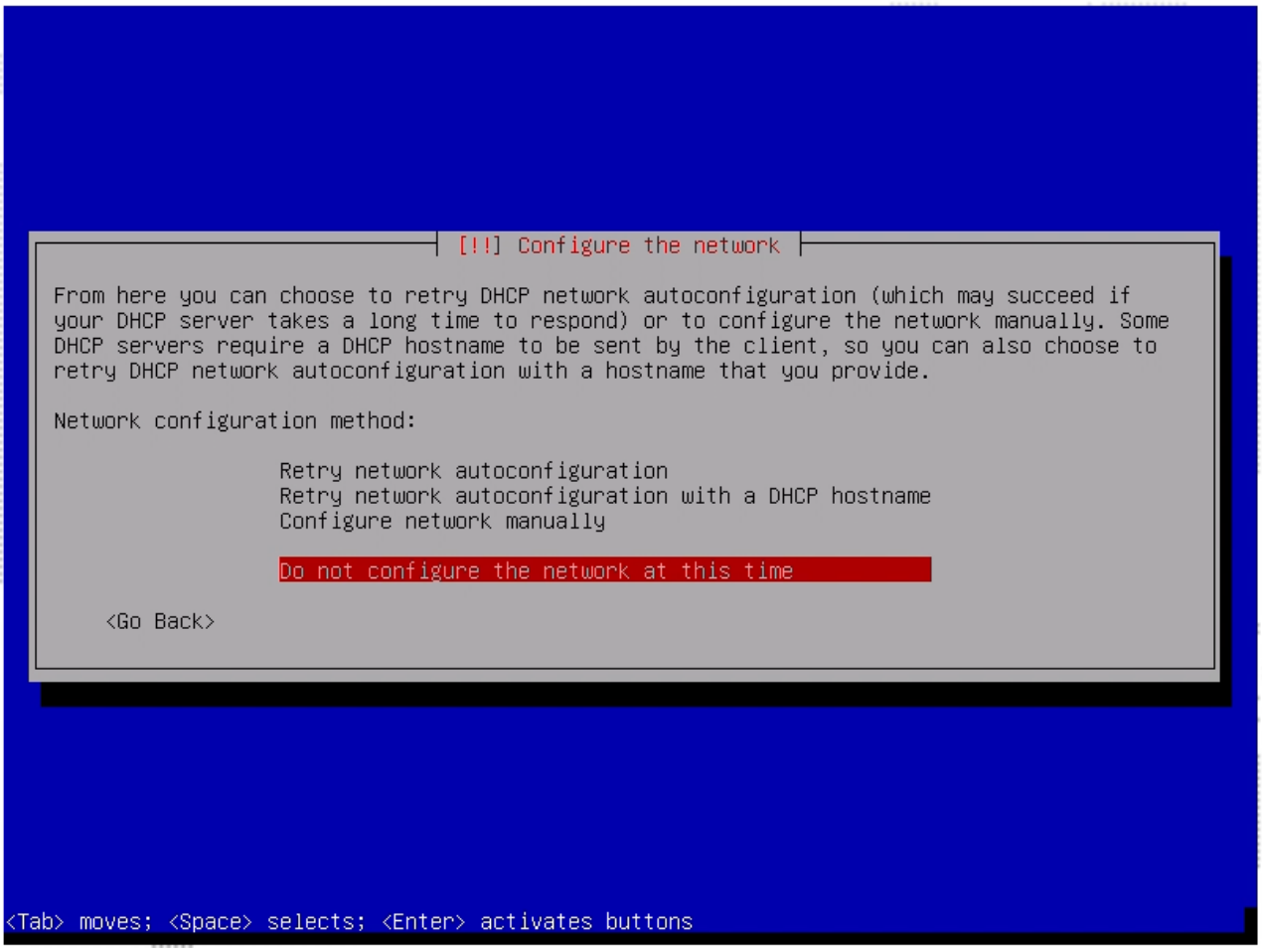
2. In the *Language* configuration window, follow the prompts to select your preferred language.
3. In the *Keyboard configuration* window, select your preferred keyboard layout.
4. In the *Network configuration* window, select your preferred interface. Continue without network configuration.



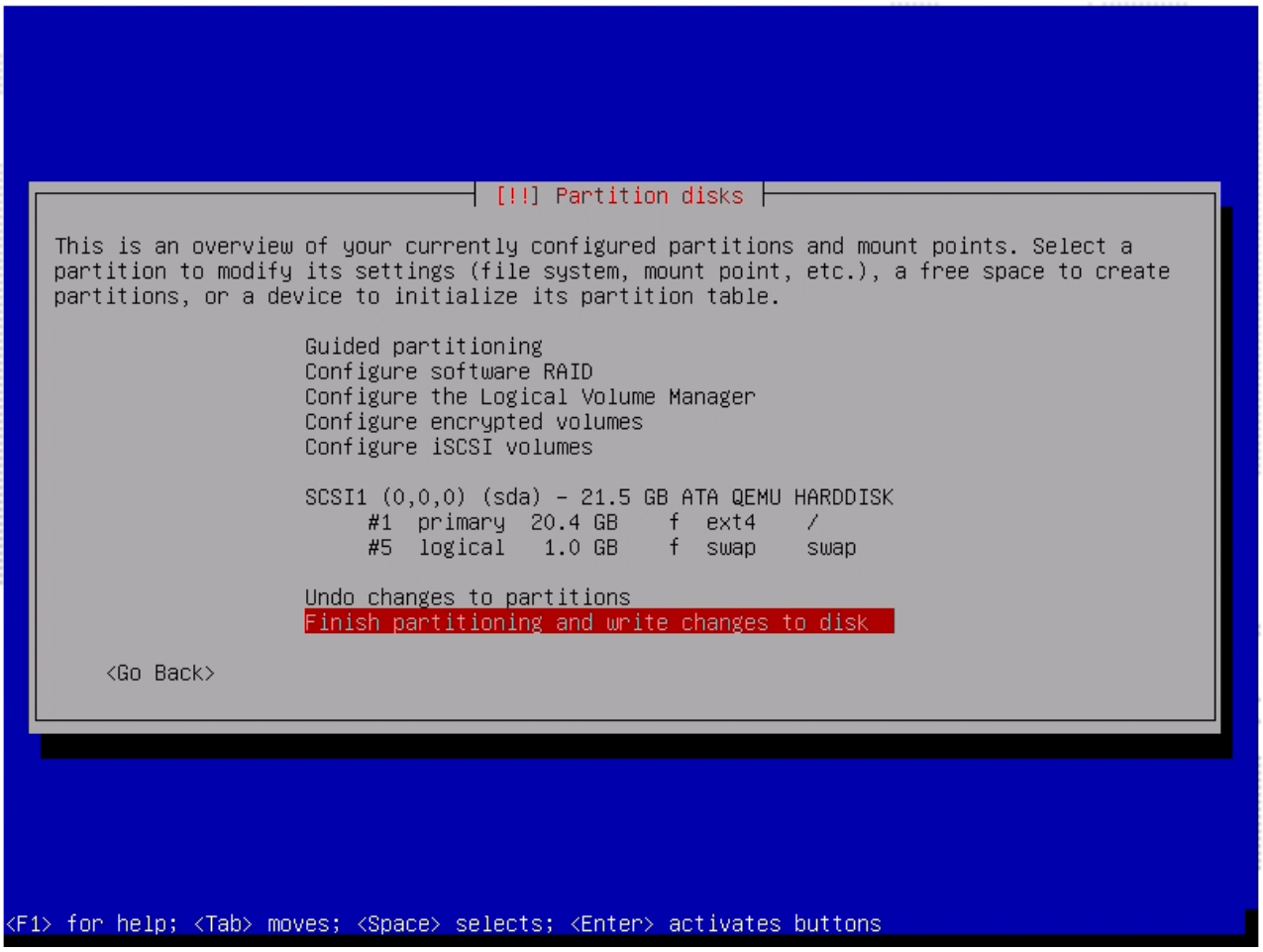
5. Select *Continue* when network autoconfiguration fails.

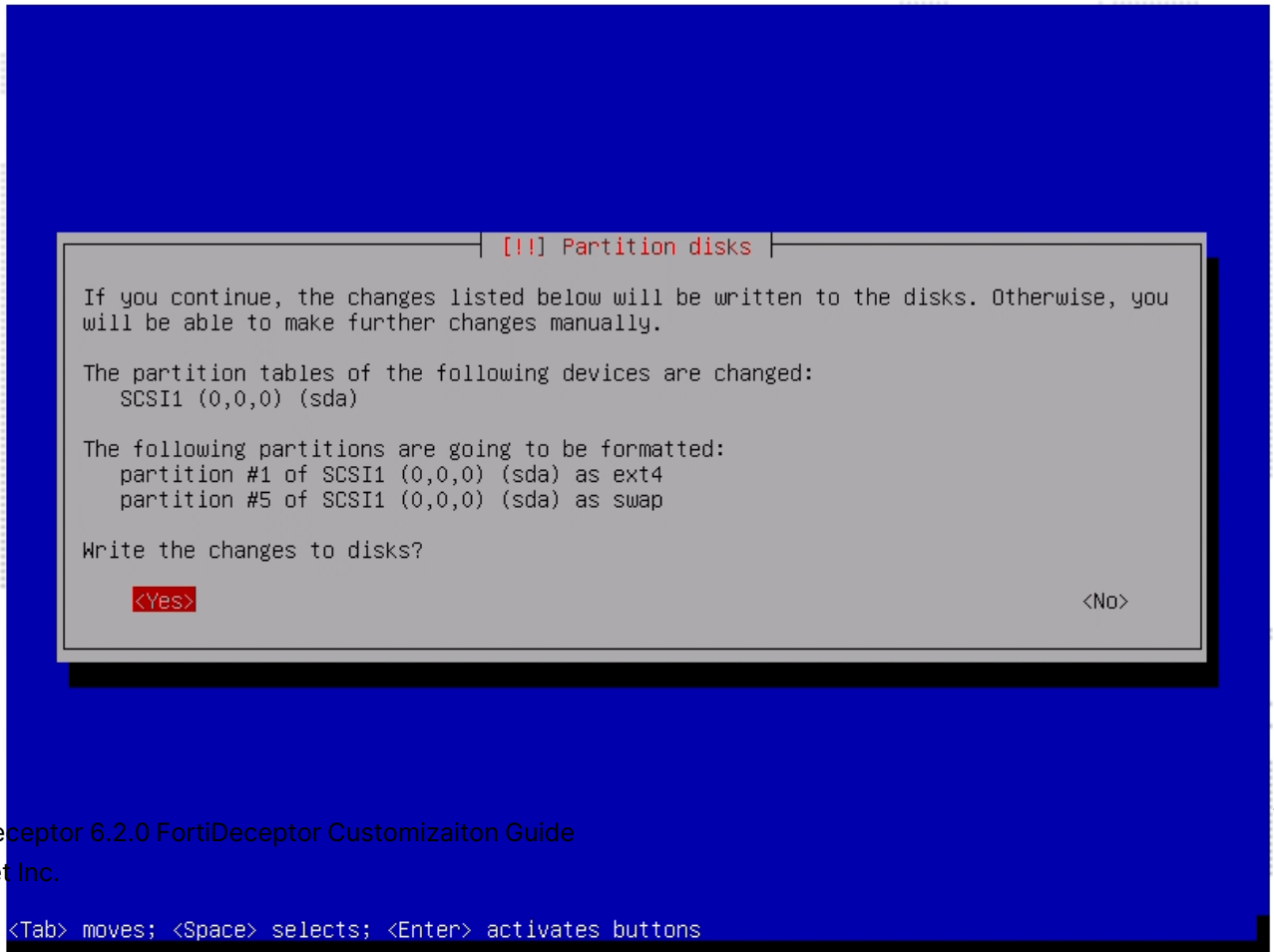


6. In the returned *Network configuration* window, select *Do not configure the network at this time*.



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.

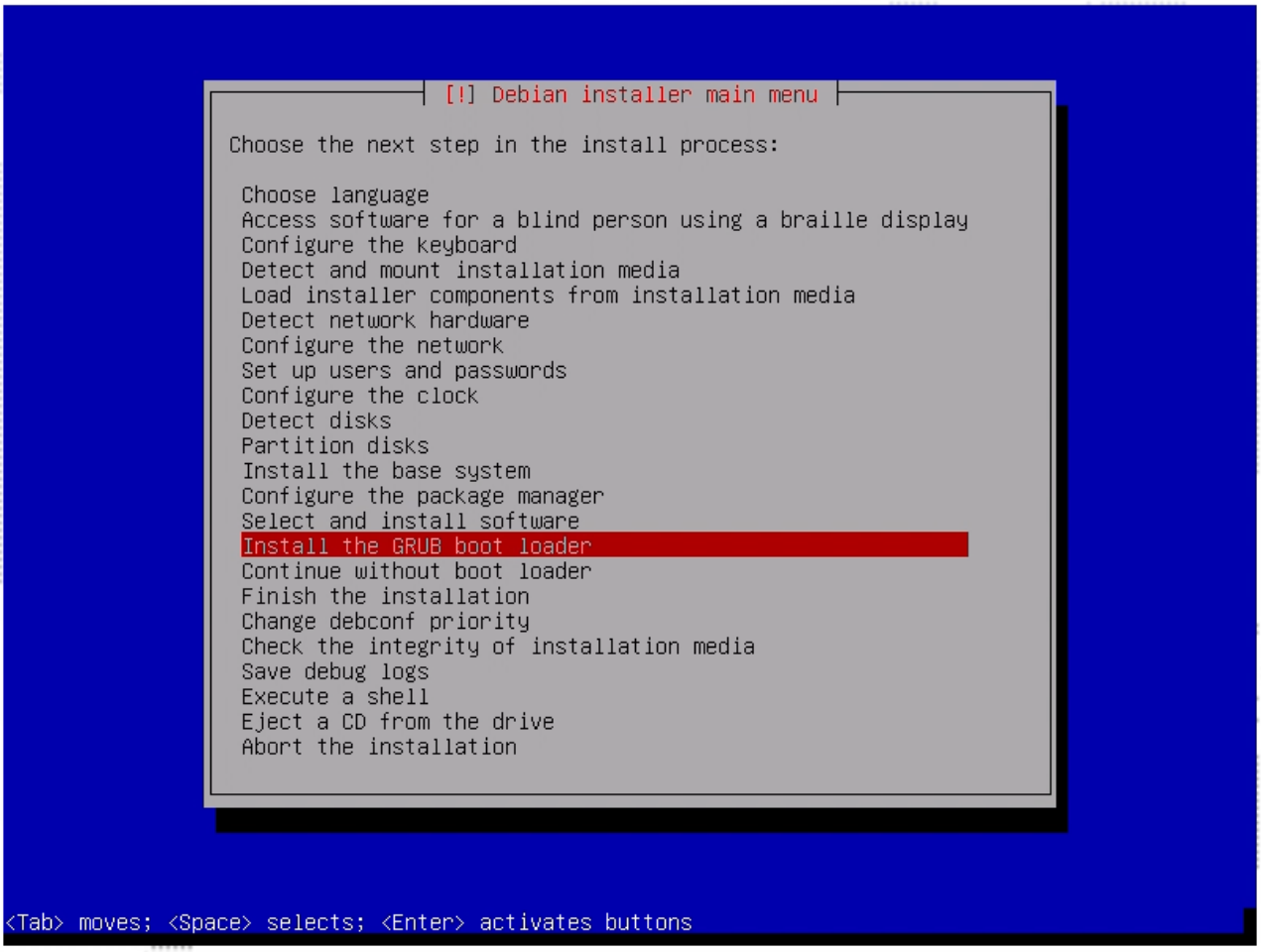

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI1 (0,0,0) (sda) - 21.5 GB ATA QEMU HARDDISK
#1 primary 20.4 GB f ext4 /
#5 logical 1.0 GB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI1 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI1 (0,0,0) (sda) as ext4
partition #5 of SCSI1 (0,0,0) (sda) as swap
Write the changes to disks?
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons

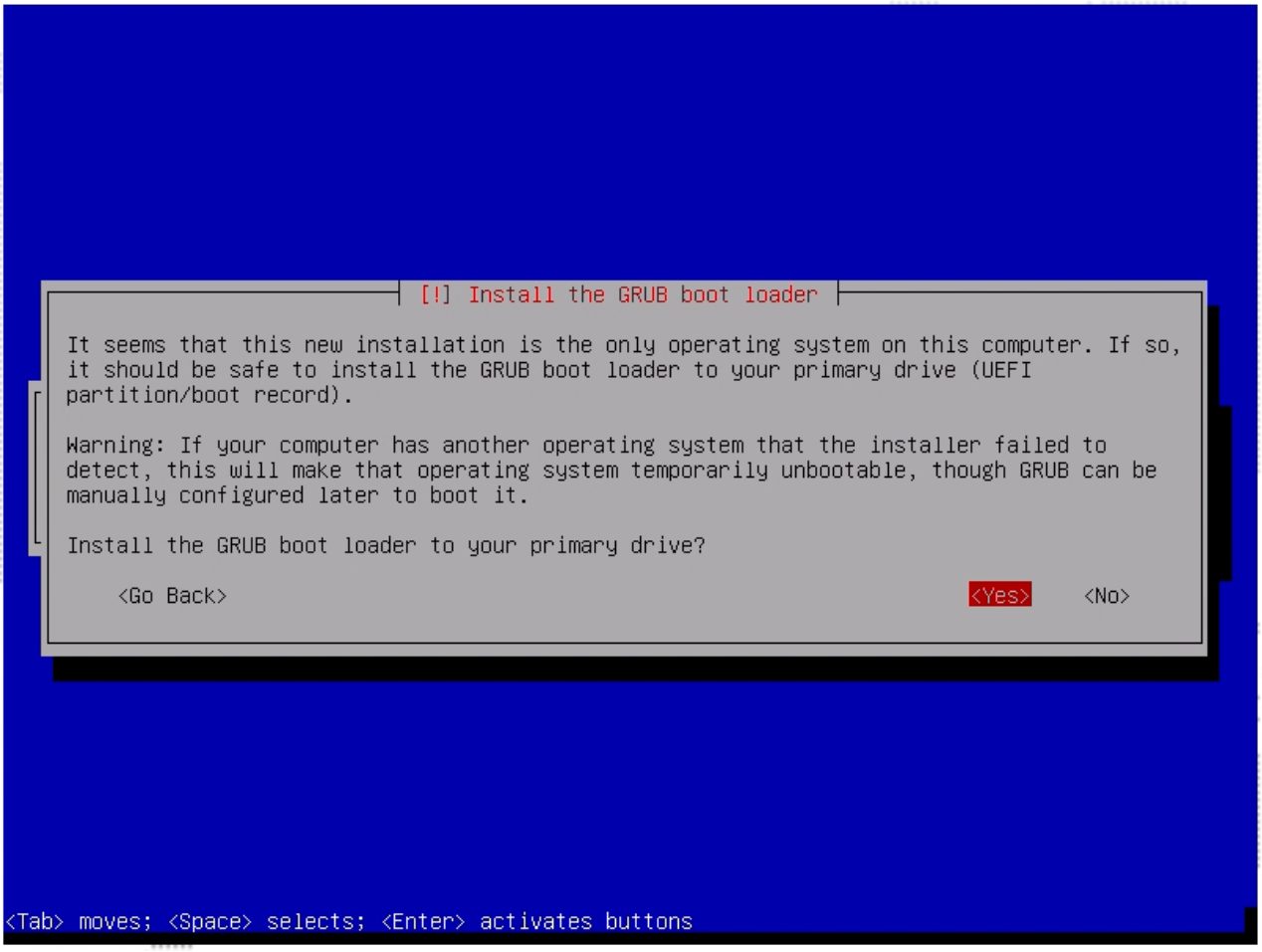
10. The installer will install the base system and configure the package manager automatically.
11. Select *Go Back* to return to the installer main menu while any apt configuration problem.

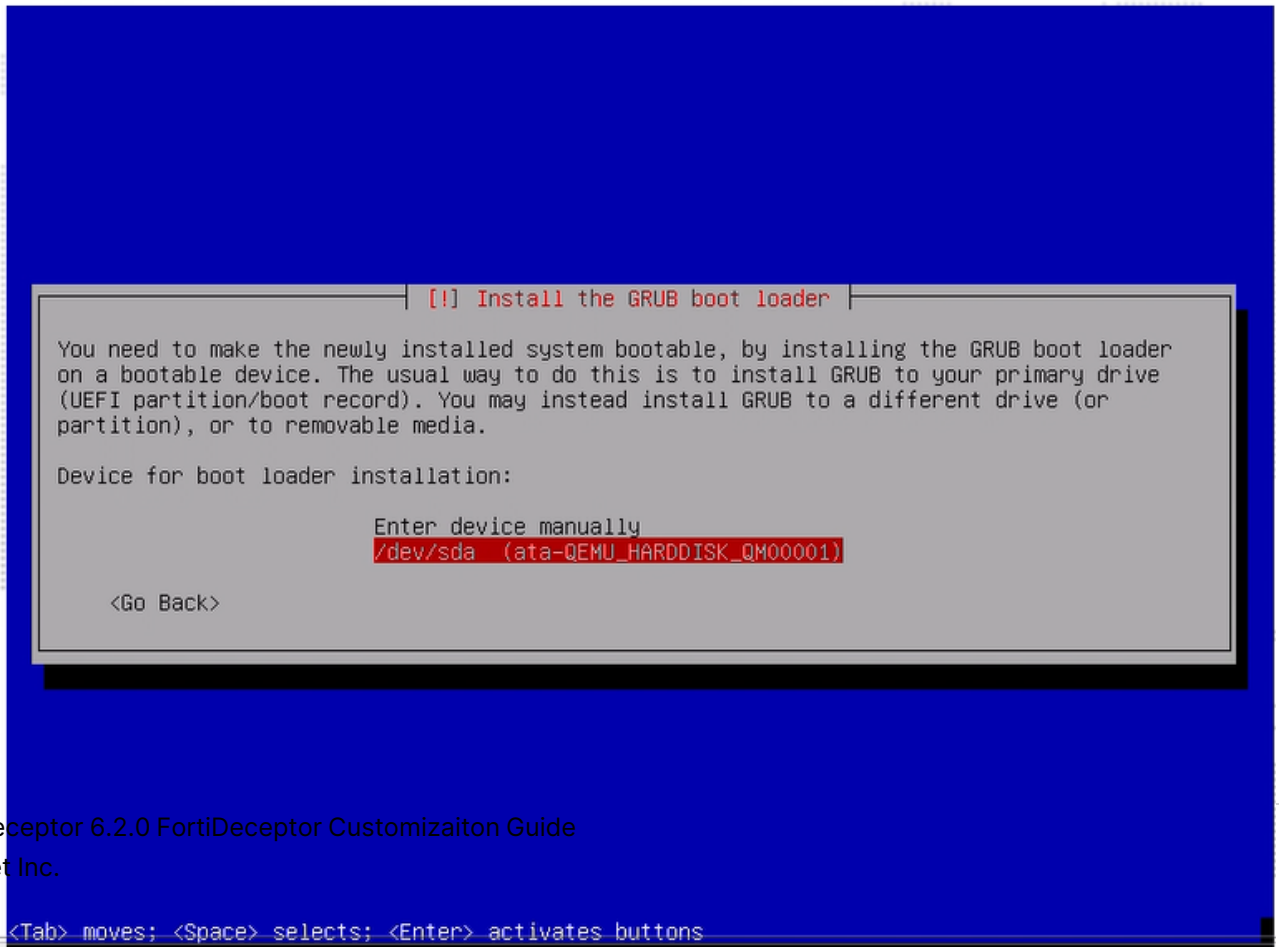
Do not click *Continue* to start the software installation. This will cause the GRUB boot loader installation to fail. If this occurs, you must discard the customization and start over.

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.


[!] Install the GRUB boot loader
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to your primary drive?
<Go Back>
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!] Install the GRUB boot loader
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.
Device for boot loader installation:
Enter device manually
/dev/sda (ata-QEMU_HARDDISK_QM00001)
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

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:

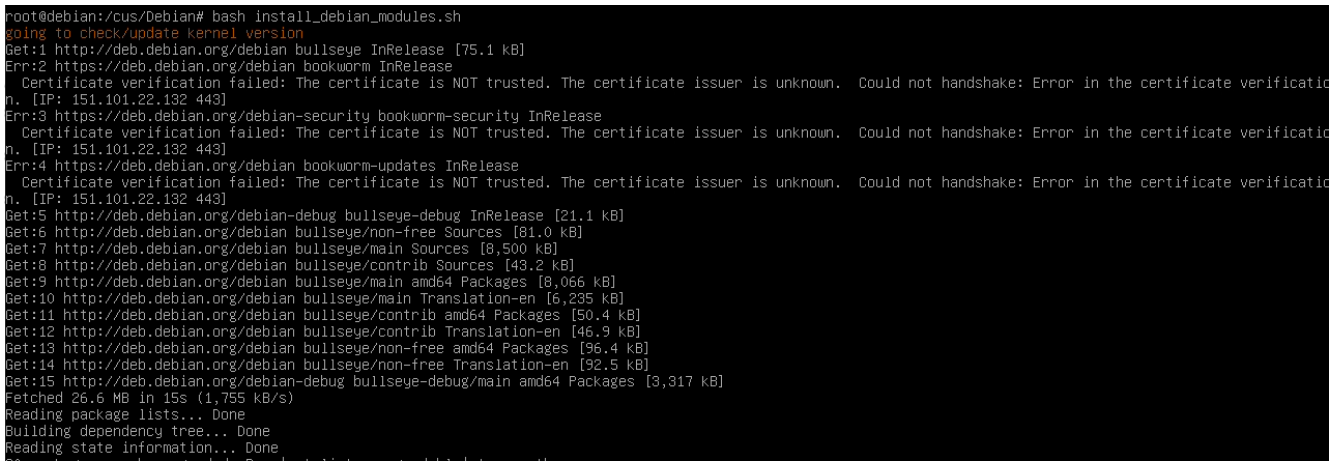
1. Open and read the setting file `net.json`.
2. Follow the settings to configure the IP, gateway, DNS.
3. After you are done, verify that your network can access the internet.

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`



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 requests
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'
```

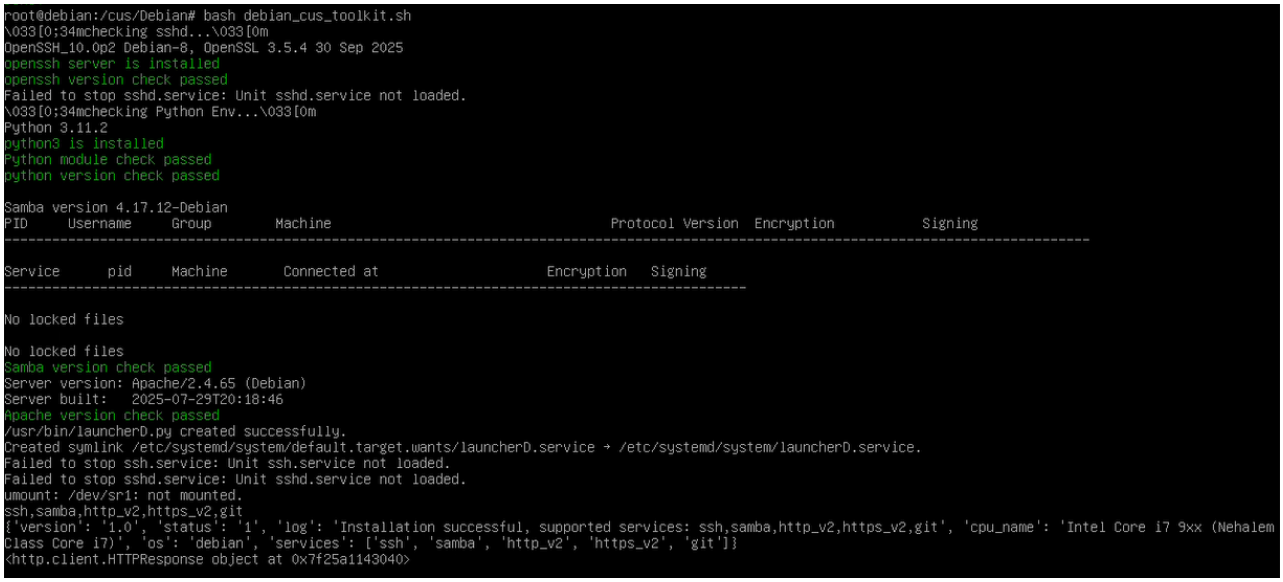
If the build is successful, the output will look like this:

```
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:

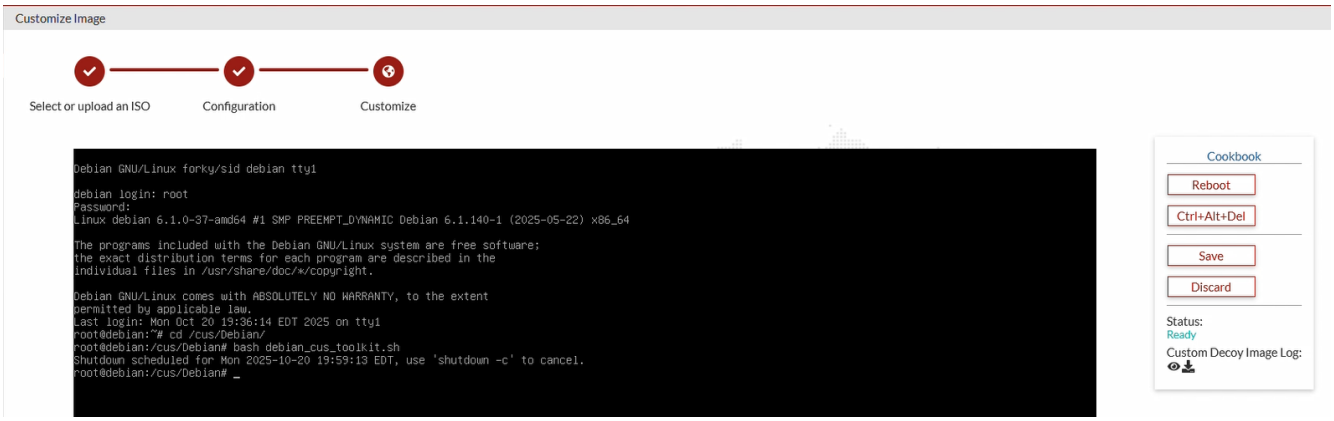
1. Ensure the system customization is completed as expected.
2. Run the following command to check and install missing packages:
   `bash debian_cus_toolkit.sh`
3. Wait for the installation to finish. The system will reboot if there are no errors.



7. Save the custom Image

To save the custom image:

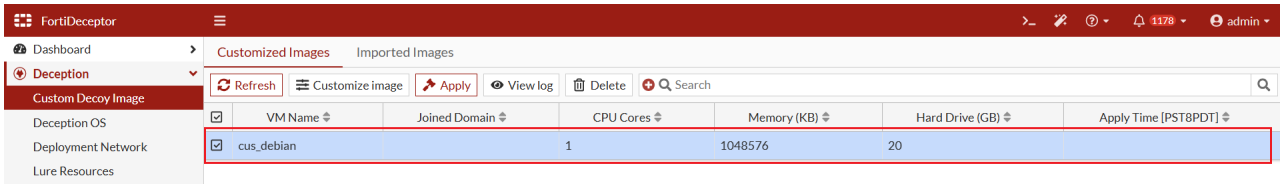
1. In the FortiDeceptor GUI, verify the image *Status* is *Ready*.
2. Install the FDC toolkit again with command: `bash debian_cus_toolkit.sh`
3. Click *Save* when the system is powered off.



8. Review the result

To review the result:

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

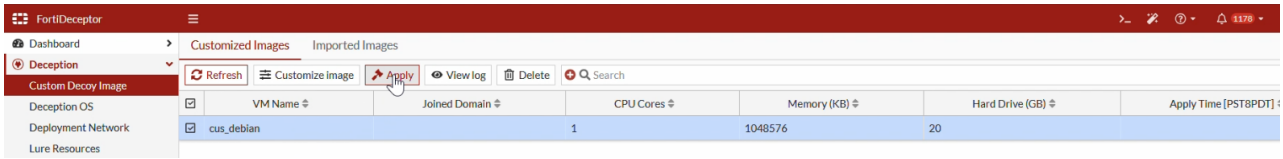


2. (Optional) Click the *Delete* button to remove the custom image.

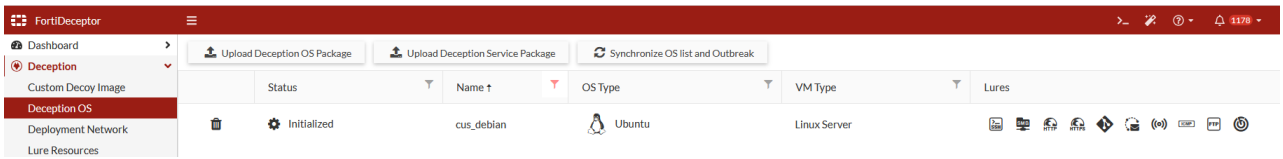
9. Apply the custom images

To apply a custom image:

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



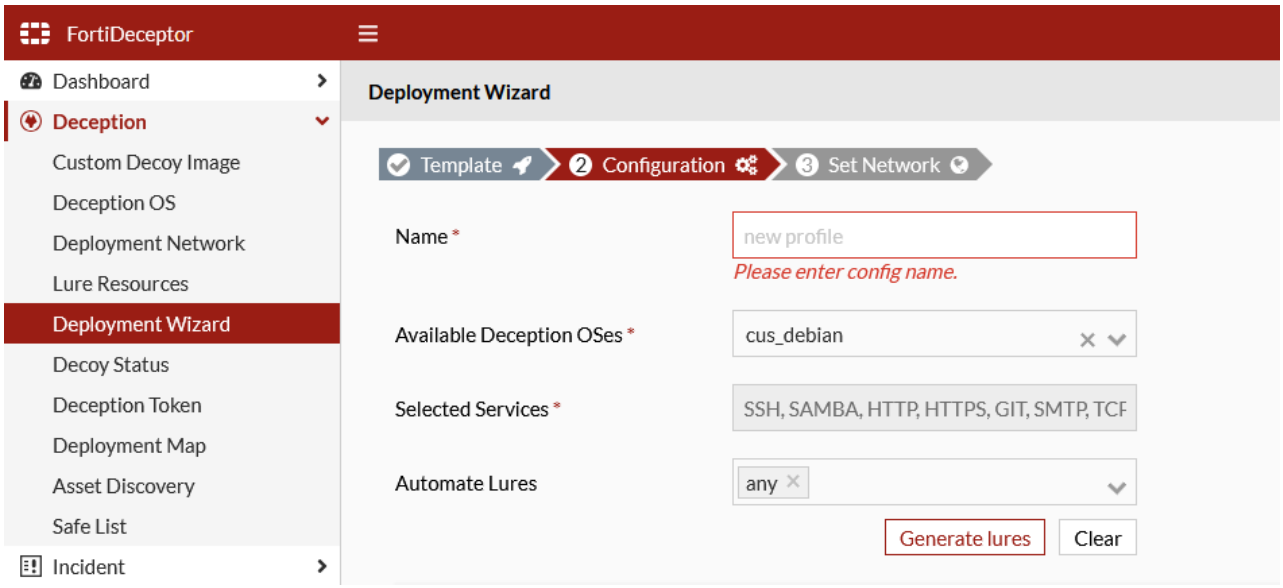
The applied image is displayed in the *Deception OS* page. It may take several minutes for the image to appear in the table.



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