

Windows Server 2019 Training – Final Project

By Alaa' Omar

(alaa.omer2009@gmail.com)

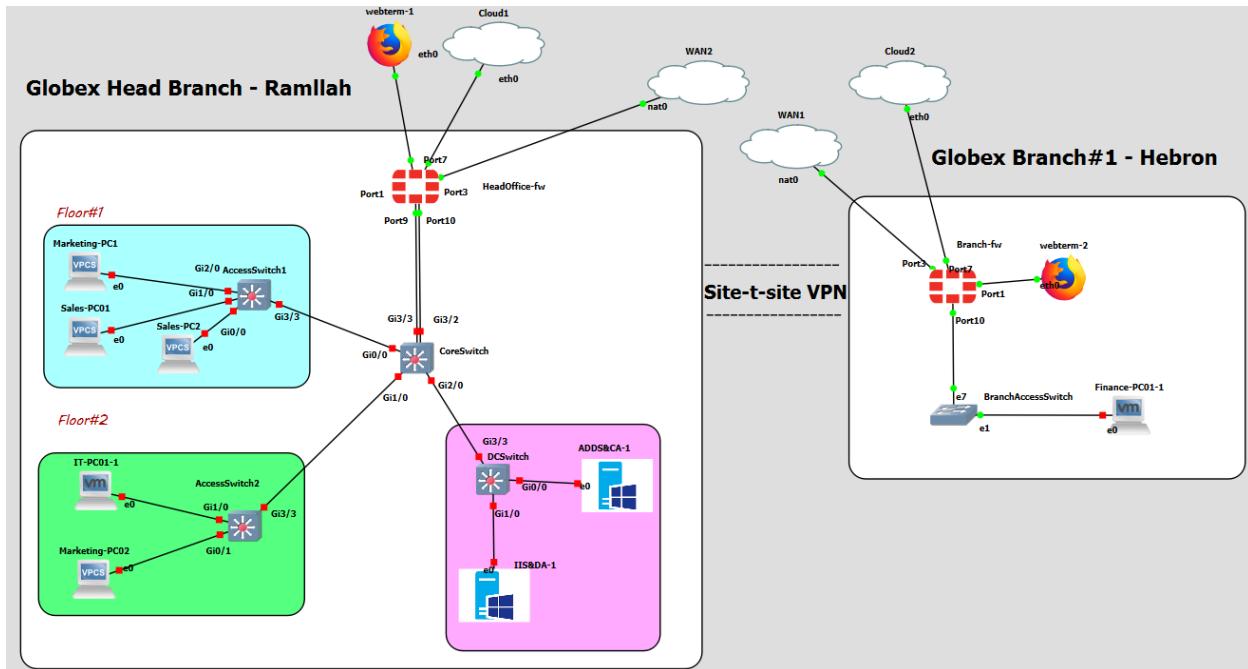


Figure 1 Globex Network Diagram

Table of Contents

Windows Server 2019 Training – Final Project	1
Network Construction, and Hardware Configuration	4
Head Office Firewall	4
Core Switch Configurations	6
Switch Access 2 Configurations.....	8
Switch Access 1 Configurations.....	8
DC-Switch Configurations.....	9
PCS	9
Internet Settings.	11
Hebron Office :	13
Firewall settings:.....	13
Hebron Branch – Internet Settings	18
Security, Permissions and Operational Requirements:.....	20
Configure Security policies	20
IT-PC01 Configuration	32
Finance-PC01	34
Read only admin (Head Firewall).....	36
Servers VLAN.....	38
IPSEC Site to Site VPN	39
ADDS – Users and groups.	43
Organizational Units.....	43
Created Users:.....	44
User Properties	45
Group Policy:.....	46
Standardize Wallpaper	46
Disable removable Storage.....	47
Folder Redirection Group Policy.....	48
Password Policy	52
Map Drive Policy :	52
Join Domain IT PC	53
Configuring IIS&DA.....	56
DA Configuration.....	57

Certificate Authority Configuration:	60
https://staff.globex.it.....	74
https://www.globex.it.....	75
Workstation Communication CA	77
Add Group Policy to distribute certificate.	82
Shared folders	83

Network Construction, and Hardware Configuration

Head Office Firewall

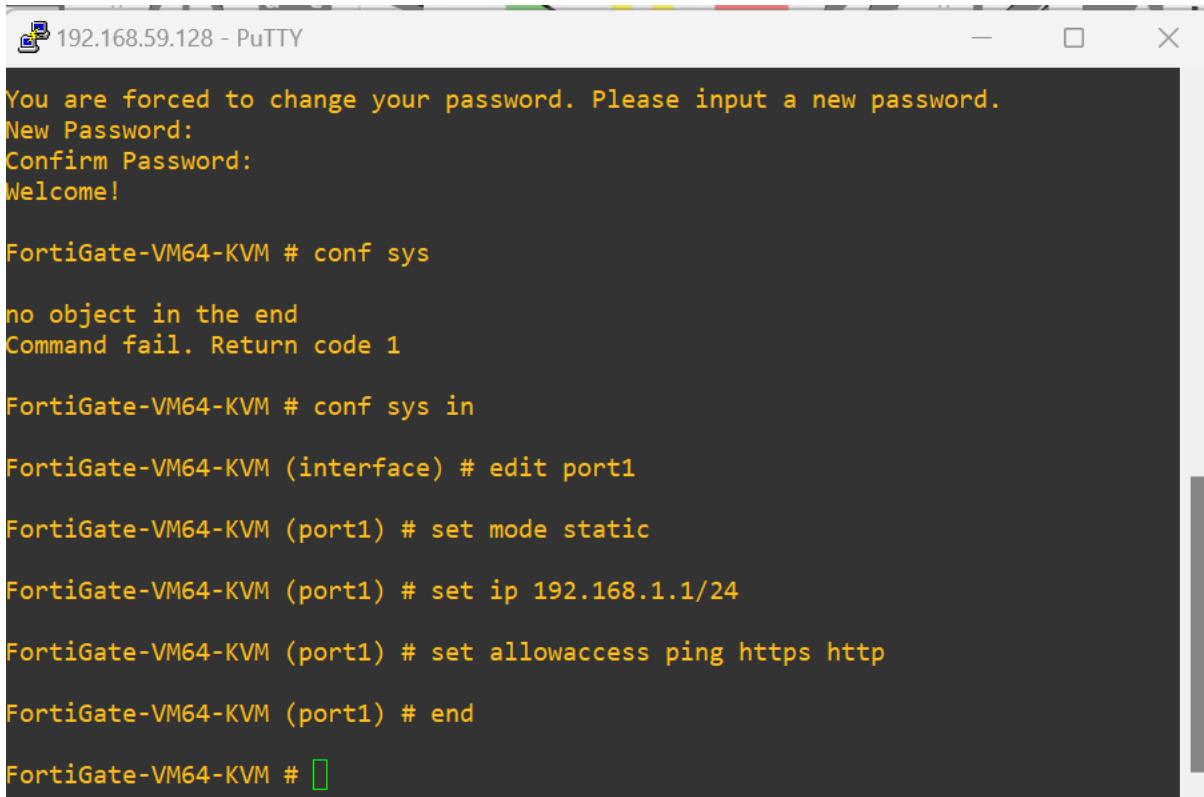
Firewall settings:

Ip address: 192.168.10.10

Username: admin

Password: admin

Firewall Configuration



```
You are forced to change your password. Please input a new password.  
New Password:  
Confirm Password:  
Welcome!  
  
FortiGate-VM64-KVM # conf sys  
  
no object in the end  
Command fail. Return code 1  
  
FortiGate-VM64-KVM # conf sys in  
  
FortiGate-VM64-KVM (interface) # edit port1  
  
FortiGate-VM64-KVM (port1) # set mode static  
  
FortiGate-VM64-KVM (port1) # set ip 192.168.1.1/24  
  
FortiGate-VM64-KVM (port1) # set allowaccess ping https http  
  
FortiGate-VM64-KVM (port1) # end  
  
FortiGate-VM64-KVM #
```

```

# This is a sample network config, please uncomment lines to configure the network
#
# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*
#
# Static config for eth0
auto eth0
iface eth0 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    gateway 192.168.1.1
    #
    up echo nameserver 192.168.0.1 > /etc/resolv.conf
#
# DHCP config for eth0
#auto eth0

```

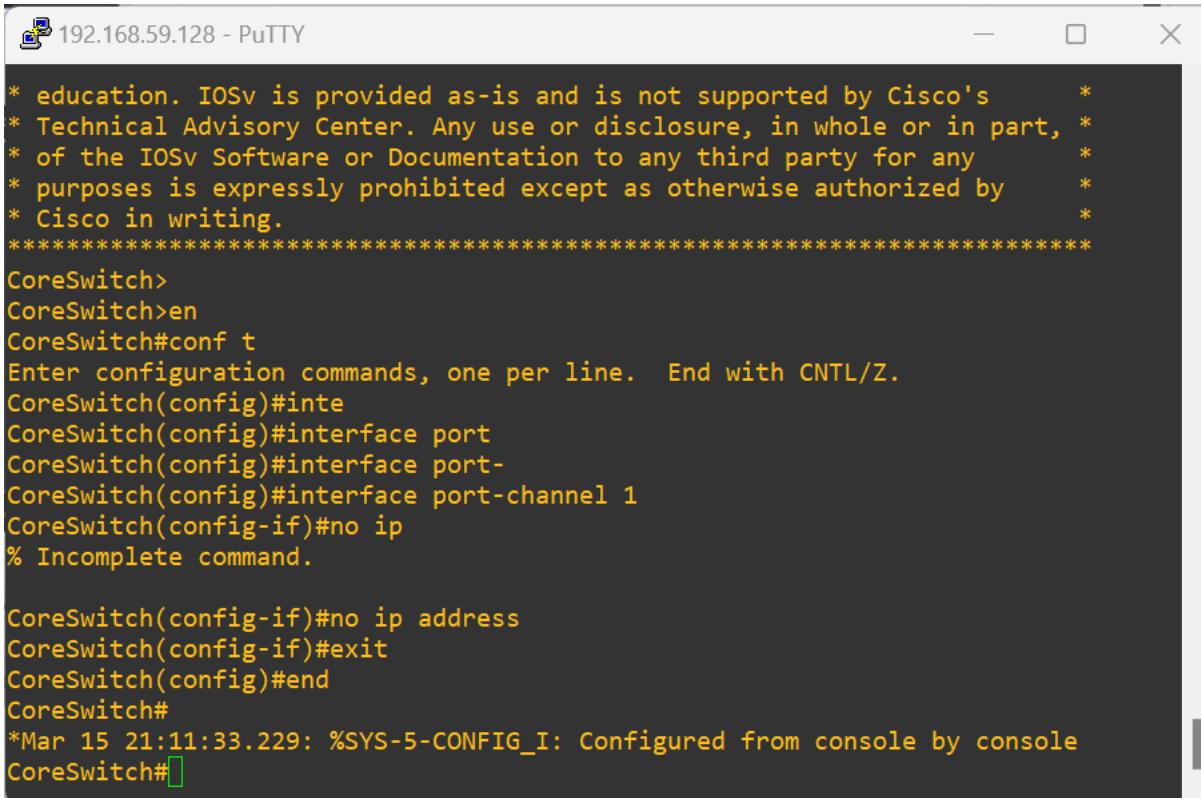
Refresh Save Cancel

Figure 2 Webterm Configurations

Name	Type	Members	IP/Netmask	Administrative Access
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connecti
To-Core	802.3ad Aggregate	port9 port10	0.0.0.0/0.0.0.0	
port1	Physical Interface		192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP +2
port2	Physical Interface		0.0.0.0/0.0.0.0	
port3	Physical Interface		0.0.0.0/0.0.0.0	
port4	Physical Interface		0.0.0.0/0.0.0.0	

Figure 3 Firewall Configurations

Core Switch Configurations



The screenshot shows a PuTTY terminal window titled "192.168.59.128 - PuTTY". The window displays the configuration of a Cisco Core Switch. The configuration includes enabling global configuration mode, defining a port-channel interface, and configuring it without an IP address. A timestamp message at the end indicates the configuration was done via the console.

```
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part,   *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                       *
*****  
CoreSwitch>  
CoreSwitch>en  
CoreSwitch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
CoreSwitch(config)#inte  
CoreSwitch(config)#interface port  
CoreSwitch(config)#interface port-  
CoreSwitch(config)#interface port-channel 1  
CoreSwitch(config-if)#no ip  
% Incomplete command.  
  
CoreSwitch(config-if)#no ip address  
CoreSwitch(config-if)#exit  
CoreSwitch(config)#end  
CoreSwitch#  
*Mar 15 21:11:33.229: %SYS-5-CONFIG_I: Configured from console by console  
CoreSwitch#
```

 192.168.59.128 - PuTTY
CoreSwitch(config-if)#switchport mode trunk
CoreSwitch(config-if)#
*Mar 15 21:27:35.959: %LINK-3-UPDOWN: Interface Port-channel1, changed state to down
*Mar 15 21:27:36.961: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down
*Mar 15 21:27:41.124: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Mar 15 21:27:42.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
CoreSwitch(config-if)#
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport a
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk a
CoreSwitch(config-if)#switchport trunk allowed v1
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#interface gigabitEthernet 2/0
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk all
CoreSwitch(config-if)#switchport trunk allowed v1
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#interface gigabitEthernet 0/0
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk all
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#interface gigabitEthernet 1/0
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk all
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#[

Figure 4 CoreSwitch Configurations

Switch Access 2 Configurations

```
192.168.59.128 - PuTTY

SwitchAccess2#
SwitchAccess2#
SwitchAccess2#en
SwitchAccess2#show v
SwitchAccess2#show vl
SwitchAccess2#show vlan br
SwitchAccess2#show vlan brief

VLAN Name          Status    Ports
-----  -----
1   default        active    Gi0/0, Gi0/2, Gi0/3, Gi1/1
                           Gi1/2, Gi1/3, Gi2/0, Gi2/1
                           Gi2/2, Gi2/3, Gi3/0, Gi3/1
                           Gi3/2
100  sales         active    Gi0/1
110  marketing     active    Gi1/1
120  IT            active    Gi1/0
130  servers       active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
SwitchAccess2#
```

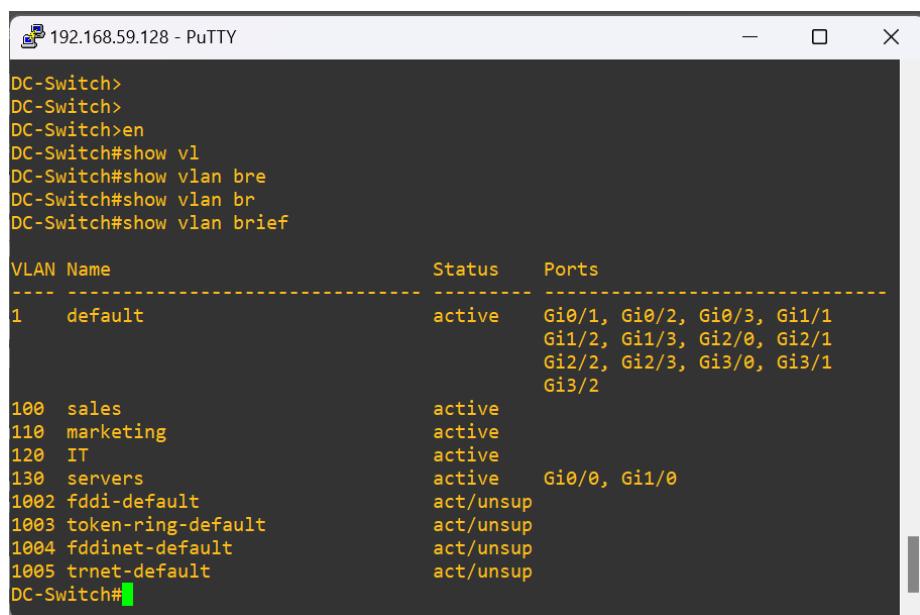
Switch Access 1 Configurations

```
192.168.59.128 - PuTTY

AccessSwitch1>
AccessSwitch1>
AccessSwitch1>
AccessSwitch1>en
AccessSwitch1#show v1
AccessSwitch1#show vlan be=r
AccessSwitch1#show vlan br
AccessSwitch1#show vlan brief

VLAN Name          Status    Ports
-----  -----
1   default        active    Gi0/1, Gi0/2, Gi0/3, Gi1/1
                           Gi1/2, Gi1/3, Gi2/1, Gi2/2
                           Gi2/3, Gi3/0, Gi3/1, Gi3/2
100  sales         active    Gi0/0, Gi1/0
110  marketing     active    Gi2/0
120  IT            active
130  servers       active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
AccessSwitch1#
```

DC-Switch Configurations

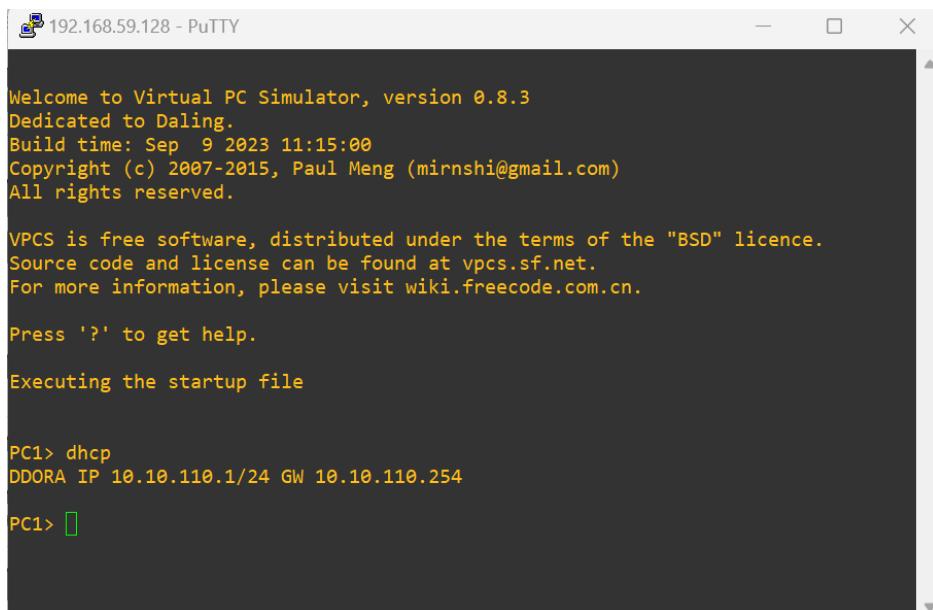


```
192.168.59.128 - PuTTY

DC-Switch>
DC-Switch>
DC-Switch>en
DC-Switch#show vl
DC-Switch#show vlan bre
DC-Switch#show vlan br
DC-Switch#show vlan brief

VLAN Name          Status    Ports
-----  -----
1     default      active    Gi0/1, Gi0/2, Gi0/3, Gi1/1
                           Gi1/2, Gi1/3, Gi2/0, Gi2/1
                           Gi2/2, Gi2/3, Gi3/0, Gi3/1
                           Gi3/2
100   sales        active
110   marketing    active
120   IT           active
130   servers      active    Gi0/0, Gi1/0
1002  fddi-default act/unsup
1003  token-ring-default act/unsup
1004  fddinet-default act/unsup
1005  trnet-default act/unsup
DC-Switch#
```

PCS



```
192.168.59.128 - PuTTY

Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> dhcp
DDORA IP 10.10.110.1/24 GW 10.10.110.254

PC1> 
```

Figure 5 Marketing VLAN DHCP

```
192.168.59.128 - PuTTY

Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC3> dhcp
DDORA IP 10.10.100.1/24 GW 10.10.100.254

PC3> 
```

Figure 6 Sales VLAN DHCP

```
192.168.59.128 - PuTTY

Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> dhcp
DDORA IP 10.10.100.2/24 GW 10.10.100.254

PC2> 
```

Figure 7 Sales PC2

```

192.168.59.128 - PuTTY

Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Hostname is too long. (Maximum 12 characters)

VPCS> dhcp
DDORA IP 10.10.110.2/24 GW 10.10.110.254

VPCS>

```

Figure 8 Marketing PC2

Internet Settings.

- Static route was added.
- A policy from vlans to WAN was added.

Destination	Gateway IP	Interface	Status
0.0.0.0/0	0.0.0.0	WAN (port3)	Enabled

Figure 9 Firewall Static Route

But before adding the policy, from Feature visibility, I activate multiple interface policy.

The screenshot shows the FortiGate management interface in Mozilla Firefox, connected to the URL `192.168.1.1/ng/system/features`. The left sidebar has a 'System' section selected, which includes 'Feature Visibility'. The 'Feature Visibility' page lists several features with toggle switches:

- DoS Policy (On)
- Email Collection (Off)
- Advanced Endpoint Control (Off)
- FortiExtender (Off)
- ICAP (Off)
- Implicit Firewall Policies (On)
- Load Balance (Off)
- Local In Policy (Off)
- Local Reports (Off)
- Multicast Policy (Off)
- Multiple Interface Policies (On)
- Policy Advanced Options (Off)

A green 'Apply' button is located at the bottom right of the feature list. A 'Changes' box on the right indicates 'No changes'.

The screenshot shows the FortiGate management interface. The left sidebar is collapsed, and the main area displays the 'Firewall Policy' list. A single policy, 'VLANS-2-WAN', is selected and highlighted in orange. The policy details are shown in a table:

Name	From	To	Source	Destination	Schedule
VLANS-2-WAN	IT marketing sales servers	WAN (port3)	IT address marketing address sales address servers address	all	always
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input type="checkbox"/> all	<input type="checkbox"/> all	<input type="checkbox"/> always

Figure 10 VLANS -to- WAN Policy

Hebron Office :

Firewall settings:

Ip address: 192.168.10.10

Username: admin

Password: admin

```
FortiGate-VM64-KVM # config system interface  
  
FortiGate-VM64-KVM (interface) # edit port1  
  
FortiGate-VM64-KVM (port1) # set mode static  
  
FortiGate-VM64-KVM (port1) # set ip 192.168.10.10/24  
  
FortiGate-VM64-KVM (port1) # set allowaccess ping https http telnet ssh  
  
FortiGate-VM64-KVM (port1) # end
```

Figure 11 Branch Firewall Console Settings

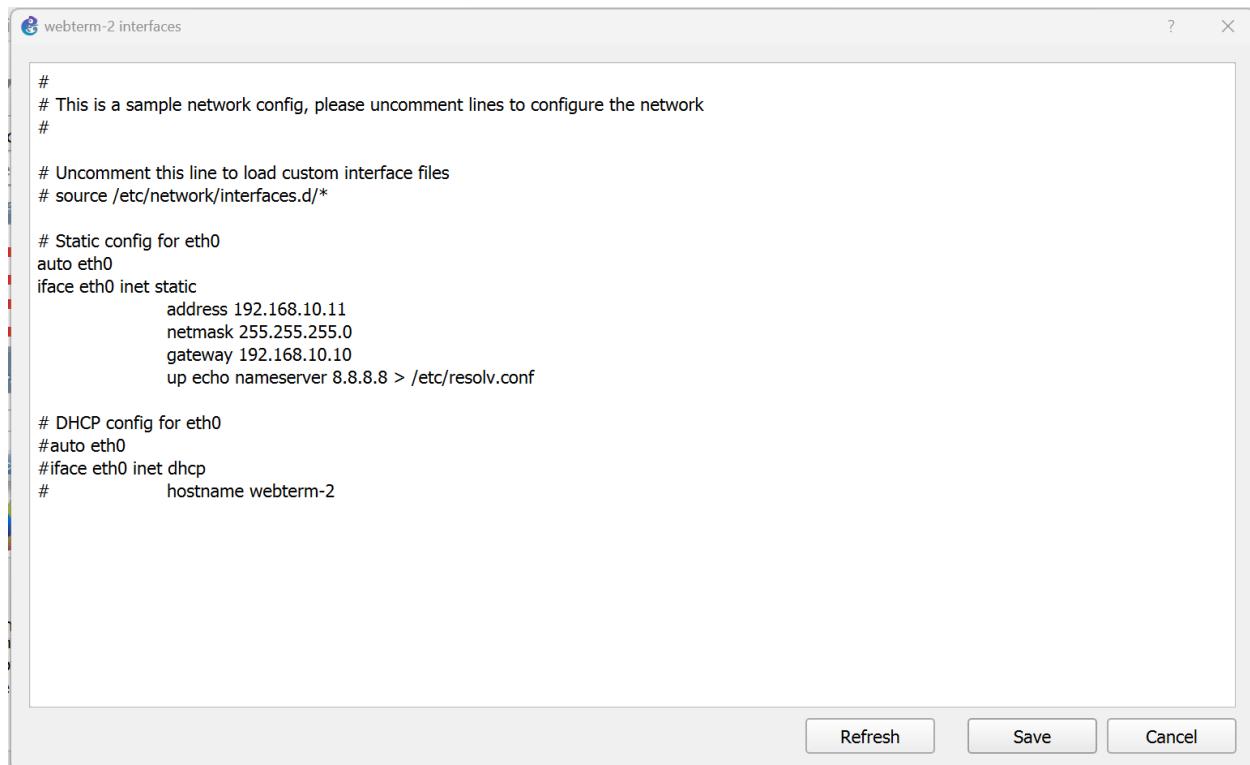


Figure 12 Webterm Settings

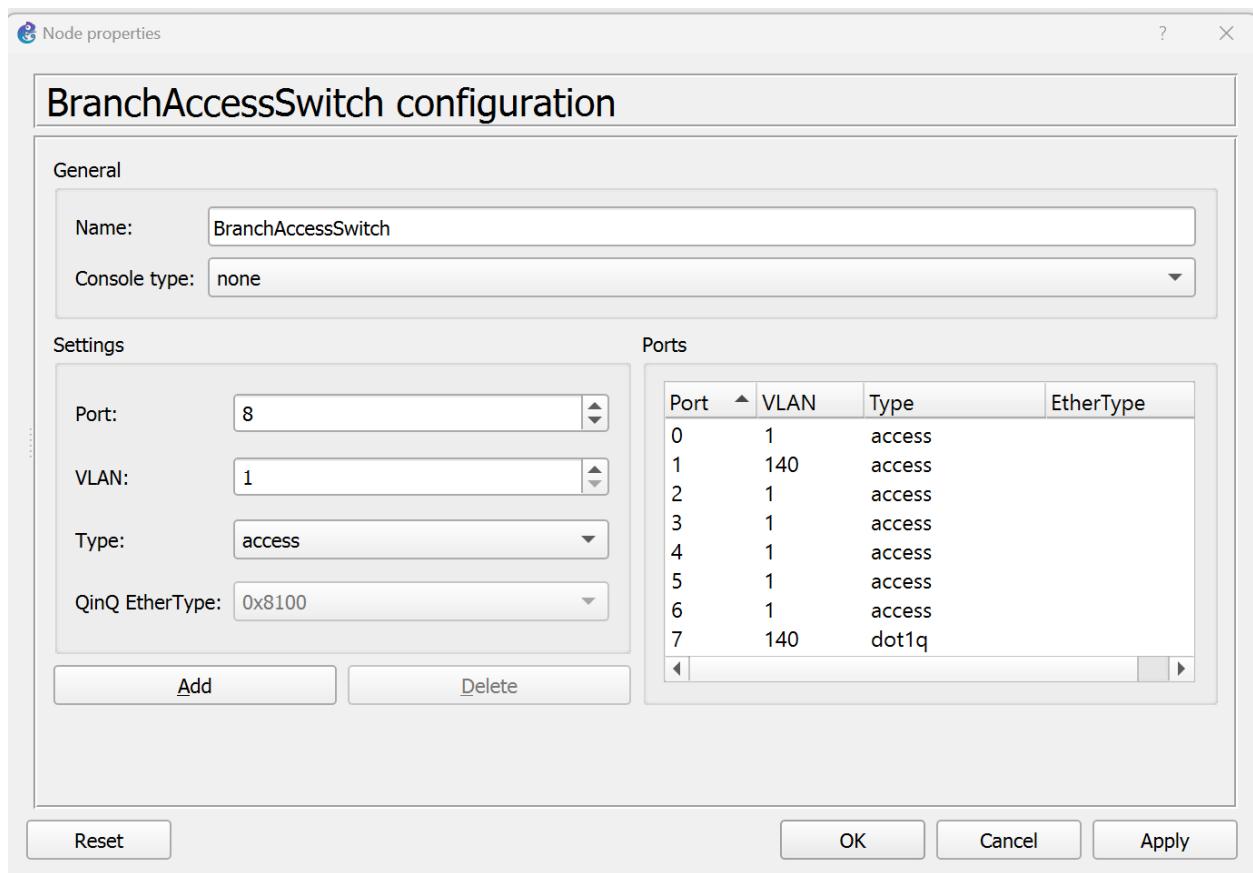


Figure 13 Branch Switch Configuration

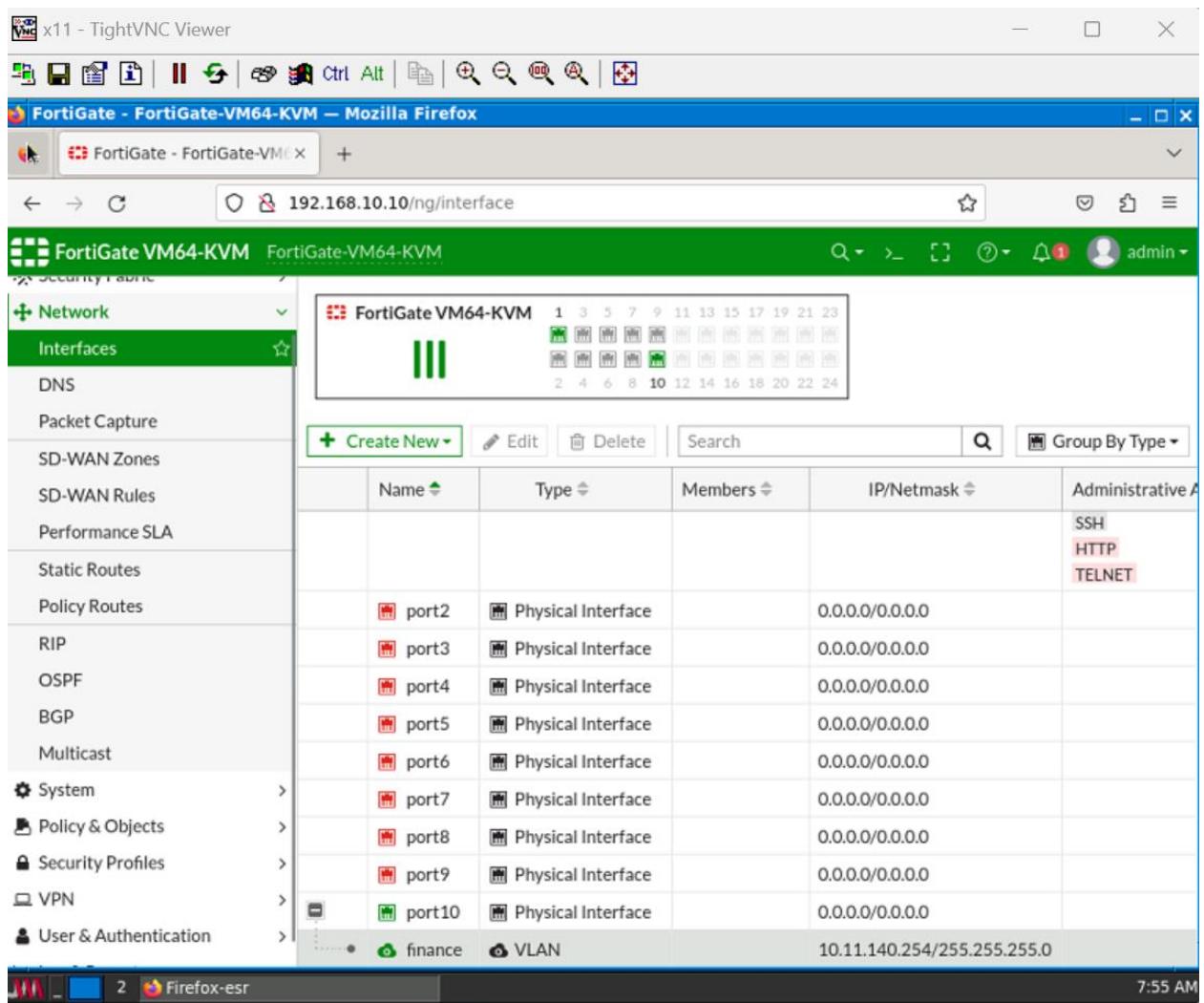
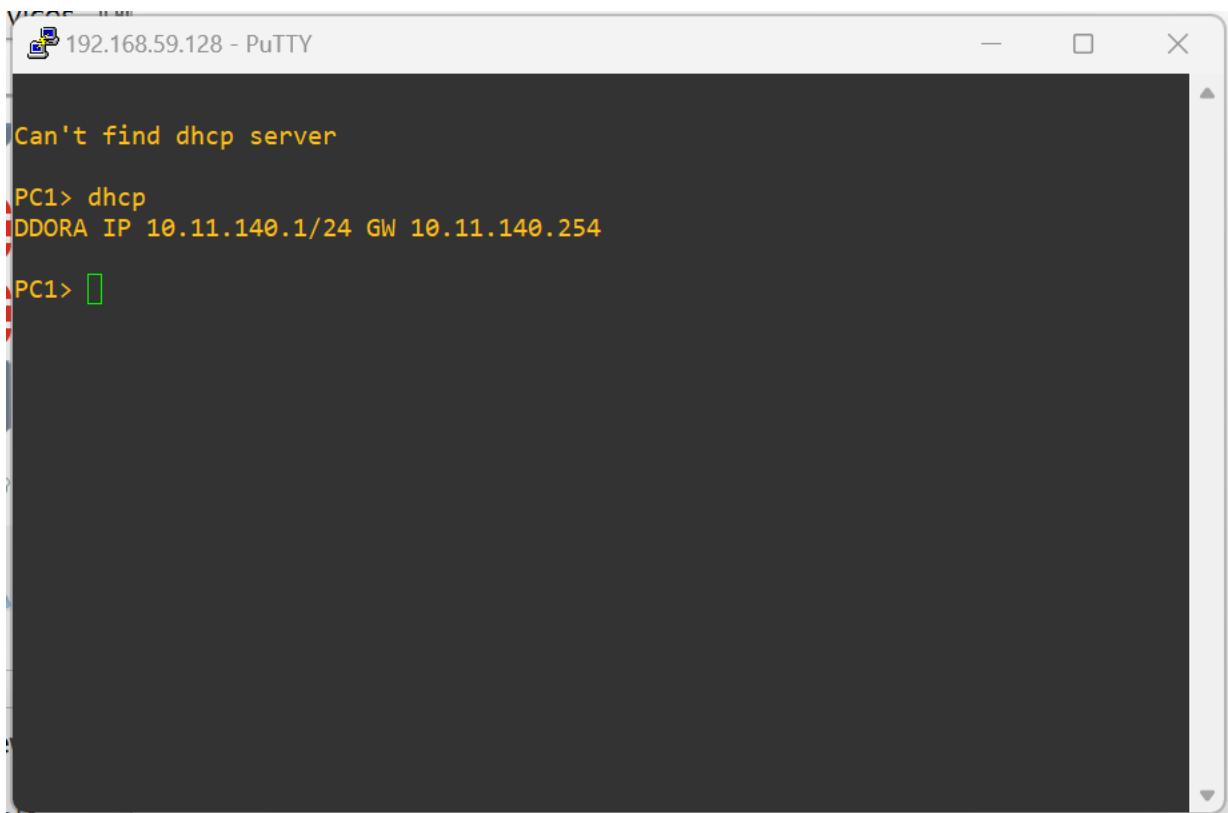


Figure 14 Firewall interfaces.



A screenshot of a PuTTY terminal window titled "192.168.59.128 - PuTTY". The window shows a command-line interface with the following text:
Can't find dhcp server
PC1> dhcp
DDORA IP 10.11.140.1/24 GW 10.11.140.254
PC1> █

Figure 15 Activate DHCP Marketing VLAN

Hebron Branch – Internet Settings

The screenshot shows the FortiGate VM64-KVM interface in Mozilla Firefox. The URL is 192.168.10.10/ng/firewall/policy/standard?showInList={"q_origin_key":1}. The left sidebar under 'Policy & Objects' is expanded to show 'Firewall Policy'. A table lists policies, with one row selected: 'finance → port3'. The selected row details the policy: Source is 'LAN-2-WAN', Destination is 'finance address', Action is 'ACCEPT', and Status is 'Enabled'. Other columns include 'Name', 'Source', 'Destination', 'Schedule', 'Service', 'Action', 'NAT', and 'Sequence'.

Figure 16 LAN To WAN Policy

The screenshot shows a Windows Command Prompt window titled 'Windows IP Configuration'. It displays the IP configuration for the 'Ethernet adapter Ethernet0 2'. The configuration includes:

- Connection-specific DNS Suffix . :
- Link-local IPv6 Address : fe80::1425:f765:e972:190b%20
- IPv4 Address : 10.11.140.10
- Subnet Mask : 255.255.255.0
- Default Gateway : 10.11.140.254

Below this, it shows the configuration for the 'Ethernet adapter Bluetooth Network Connection':

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

At the bottom, a 'ping' command is run:

```
C:\Users\alaa>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=70ms TTL=126
Reply from 8.8.8.8: bytes=32 time=66ms TTL=126
Reply from 8.8.8.8: bytes=32 time=69ms TTL=126
Reply from 8.8.8.8: bytes=32 time=66ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 66ms, Maximum = 70ms, Average = 67ms

C:\Users\alaa>
```

Figure 17 Finance PC02 (IP Configuration)

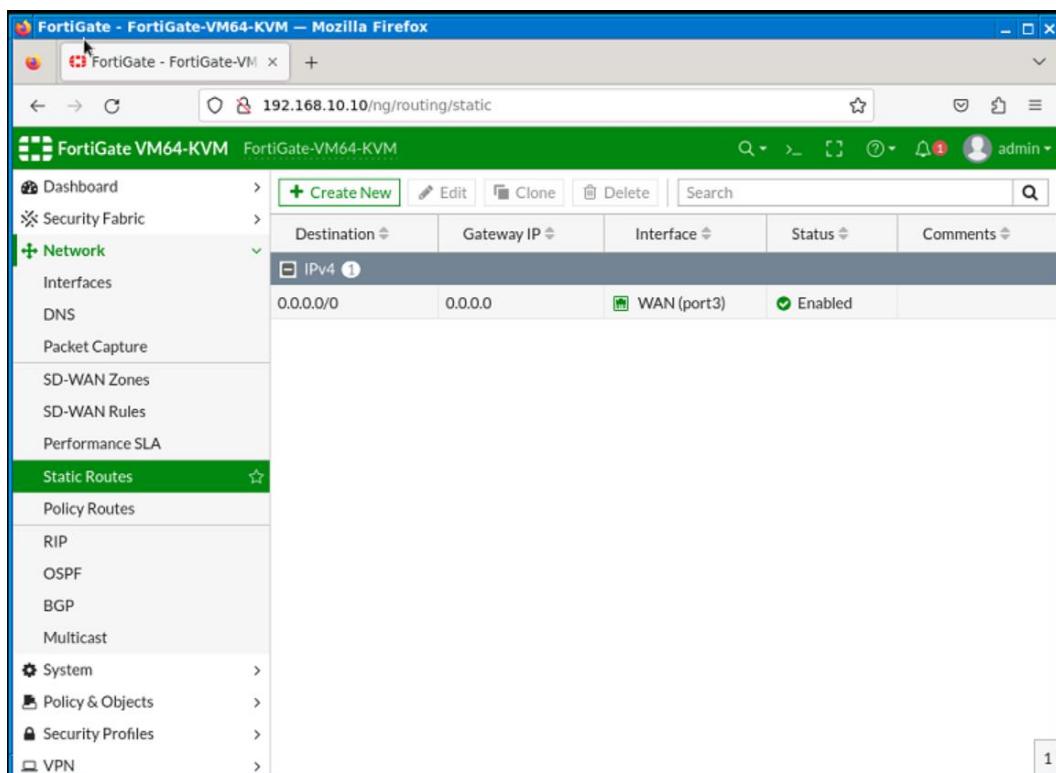


Figure 18 Branch Static Route

```
8.8.8.8 icmp_seq=5 timeout
PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=66.298 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=65.233 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=65.438 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=65.092 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=167.488 ms

PC1>
```

Figure 19 Testing Internet

Security, Permissions and Operational Requirements:

Configure Security policies.

Security Profile	App/Web	Action	VLAN	Time
Web Filter	facebook	Warning	Sales, Marketing	All Time
Web Filter	youtube	Limit	Marketing	All Time
Web Filter	hacking	Allow 3 Website	IT	08:00 - 09:00 All day
Web Filter	phishing	Warning 3 Website	IT	15:00-16:00 Saturday
Web Filter	Word "destroy"	Block	Sales, Marketing	All day
App Control	Azureus	Allow	marketing	1/4/2024- 1/7/2024
App Control	Winmx	Allow	IT	All day
App Control	WorldOfTanks	Allow	Sales, Marketing	All day
App Control	https	Enable	Sales, Marketing, IT	All day
Antivirus	ftp	Enable	Sales, Marketing, IT	Saturday, Sunday
Intrusion Prevention	Sev 3 Sev 5	block	Sales, Marketing, IT	All Day

1. Antivirus, ftp allows

The screenshot shows the FortiGate VM64-KVM web interface. The left sidebar navigation menu is visible, with 'Security Profiles' and 'AntiVirus' selected. The main content area is titled 'New AntiVirus Profile' and shows the configuration for a profile named 'ftp'. The 'Name' field is set to 'ftp'. Under 'Comments', there is a placeholder 'Write a comment...' with a character count of '0/255'. The 'Detect Viruses' section has two options: 'Block' (selected) and 'Monitor'. Below that, the 'Feature set' is set to 'Flow-based'. The 'Inspected Protocols' section lists several protocols with their inspection status: HTTP (off), SMTP (off), POP3 (off), IMAP (off), FTP (on), and CIFS (off). In the 'APT Protection Options' section, two options are enabled: 'Treat Windows Executables in Email Attachments as Viruses' and 'Include Mobile Malware Protection'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Figure 20 Antivirus Enable FTP

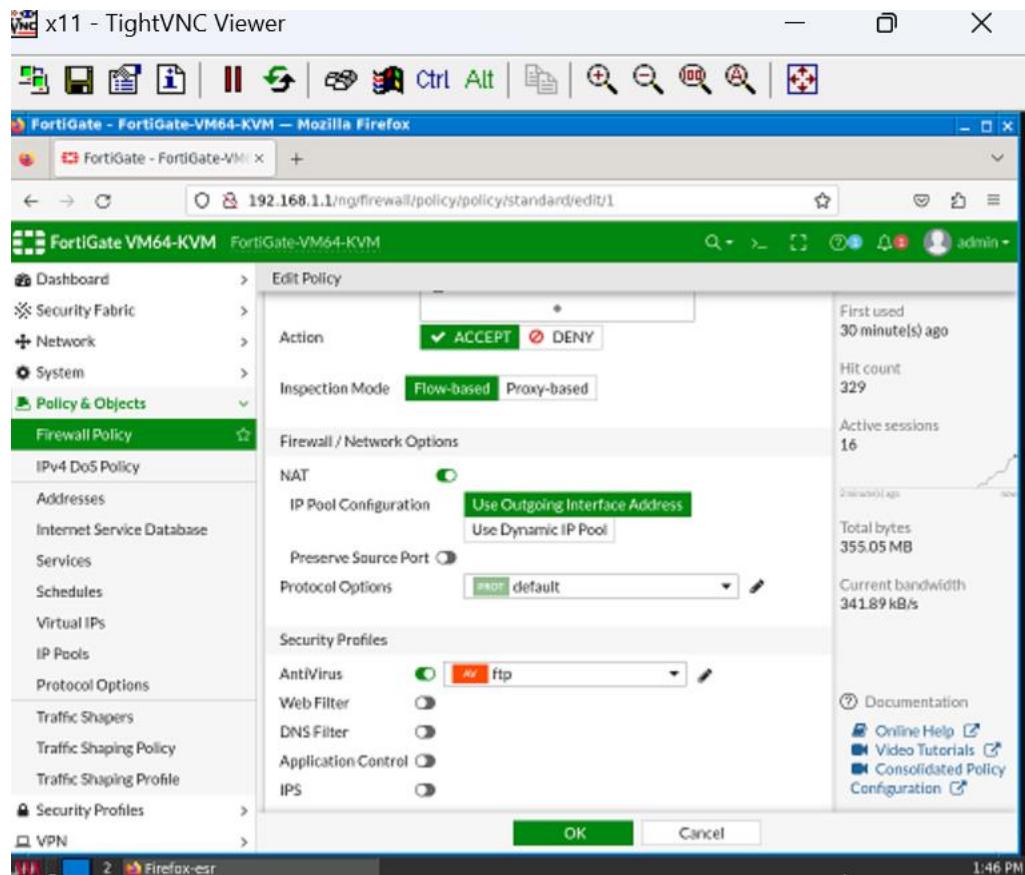


Figure 21 Link Antivirus to Firewall Policy

Marketing Firewall Policy

Web Filter profile (youtube) and block destroy as in the picture

URL	Type	Action	Status
*youtube.com	Wildcard	Exempt	Enable

Pattern Type	Pattern	Language	Action	Status
Regular Expression	^destroy^	Western	Block	Disable

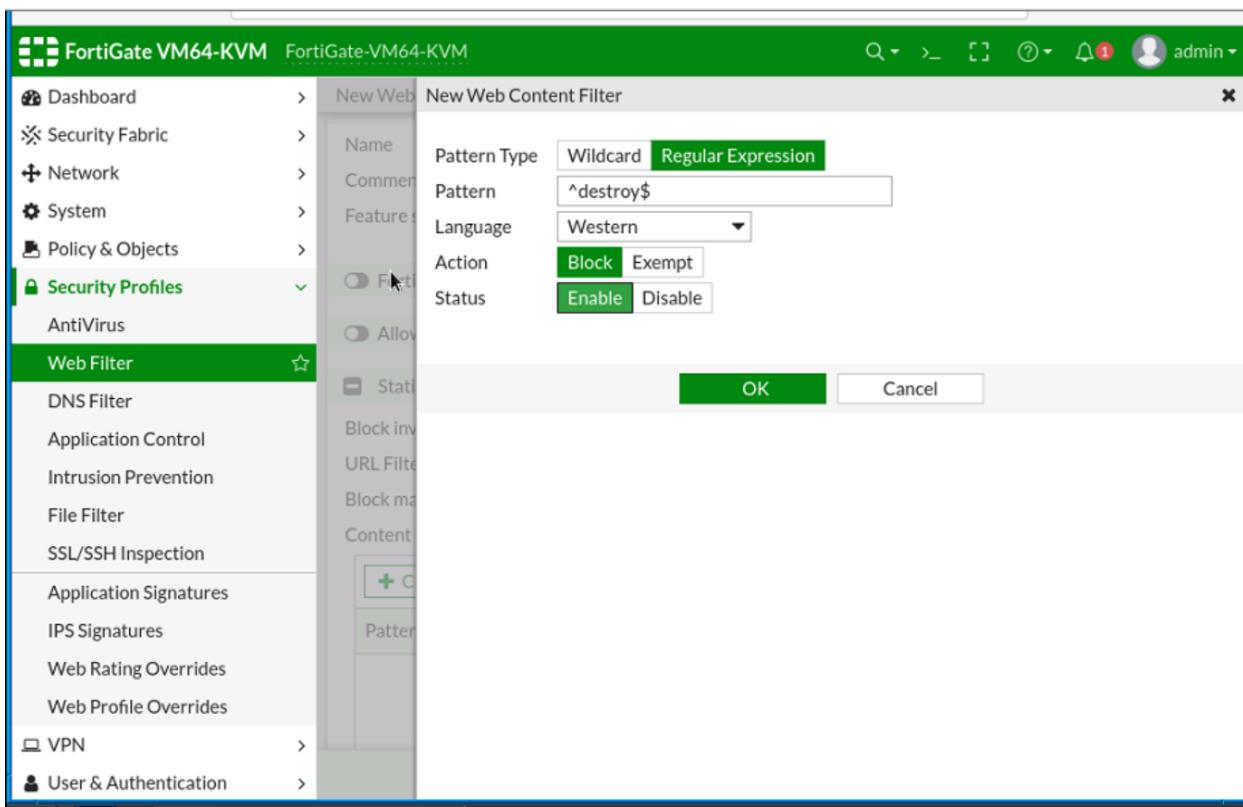


Figure 22 Web Filter destroy word block

Marketing_Sales_IT Policy

New Policy

Use Dynamic IP Pool

Preserve Source Port

Protocol Options PROT default

Security Profiles

AntiVirus	<input checked="" type="checkbox"/> AV <input checked="" type="checkbox"/> ftp <input type="button" value=""/>
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input checked="" type="checkbox"/> IPS <input checked="" type="checkbox"/> block_sev3_sev5 <input type="button" value=""/>
File Filter	<input type="checkbox"/>
SSL Inspection	<input checked="" type="checkbox"/> SSL certificate-inspection <input type="button" value=""/>

Logging Options

Log Allowed Traffic Security Events All Sessions

Generate Logs when Session Starts

Policies Summary

Name	From	To	Source	Destination	Schedule
VLANS-2-WAN	IT marketing sales servers-130 (s...)	WAN (port3)	IT address marketing address sales address servers address	all	always
IT-2-Servers	IT	servers-130 (servers)	IT address	servers address	always
Servers-2-IT	servers-130 (s...)	IT	servers address	IT address	always
vpn_Hebron-Branch_local_...	servers-130 (s...)	Hebron-Branch	Hebron-Branch_local	Hebron-Branch_...	always
vpn_Hebron-Branch_remo...	Hebron-Branch	servers-130 (servers)	Hebron-Branch_re...	Hebron-Branch_...	always
IT-PC01-2-VLANS	IT marketing sales servers-130 (servers)	IT-PC01	marketing address sales address servers address		always
VLANS-2-Servers	IT marketing sales	servers-130 (servers)	IT address marketing address sales address	servers address	always

0% 11 | Updated: 11:09:08

PortGate-VM64-KVM

Policy Lookup

Interface Pair View By Sequence

Name	From	To	Source	Destination	Schedule
VLANS-2-Servers	IT marketing sales Hebron-Branch	servers-130 (servers)	IT address marketing address sales address Hebron-Branch_local	servers address	always
marketing_2_wan	marketing	WAN (port3)	marketing address	all	always
IT-2-WAN	IT	WAN (port3)	IT address	all	always
sales_marketing_it_2_wan	IT marketing sales	WAN (port3)	IT address marketing address sales address	all	always

Edit IPS Sensor

Name: block_sev3_sev5

Comments: Write a comment... / 0/255

Block malicious URLs:

IPS Signatures and Filters

Create New Edit Delete

Details	Exempt IPs	Action	Packet Logging
SEV SEV		🚫 Block	✗ Disabled

1

Botnet C&C

Scan Outgoing Connections to Botnet Sites **Disable** **Block** **Monitor**

OK **Cancel**

Figure 23 Block SEV3 and SEV5

App Control, Azureus, Allow (marketing firewall policy)

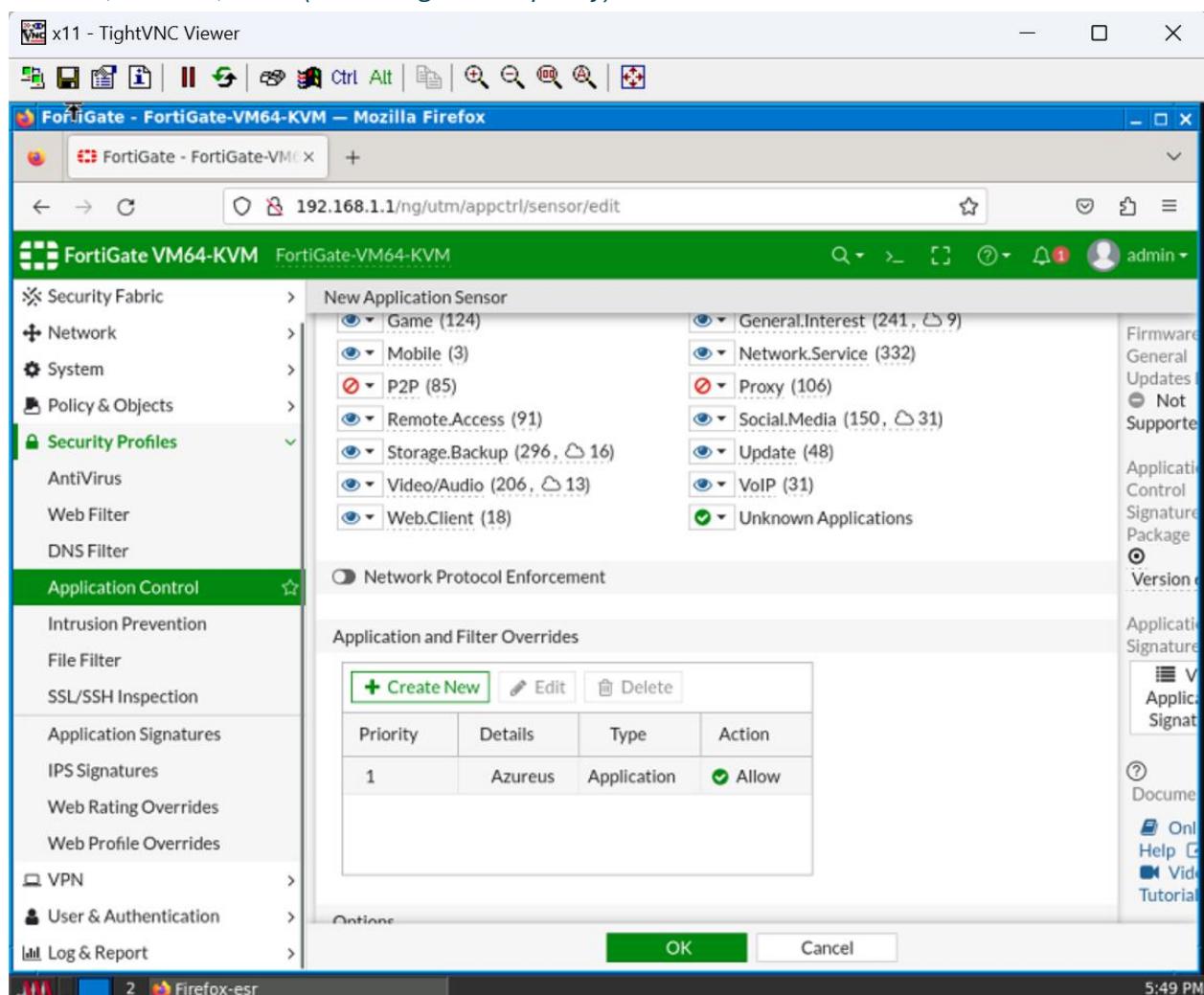


Figure 24 App Control, Azureus, Allow

New Policy

IP Pool Configuration

Use Outgoing Interface Address
 Use Dynamic IP Pool

Preserve Source Port

Protocol Options

Security Profiles

AntiVirus

Web Filter WEB marketing

DNS Filter

Application Control APP Allow_Azuerus

IPS

File Filter

SSL Inspection

Logging Options

Log Allowed Traffic Security Events All Sessions

Figure 25 Marketing Policy

App control, Allow Winmx

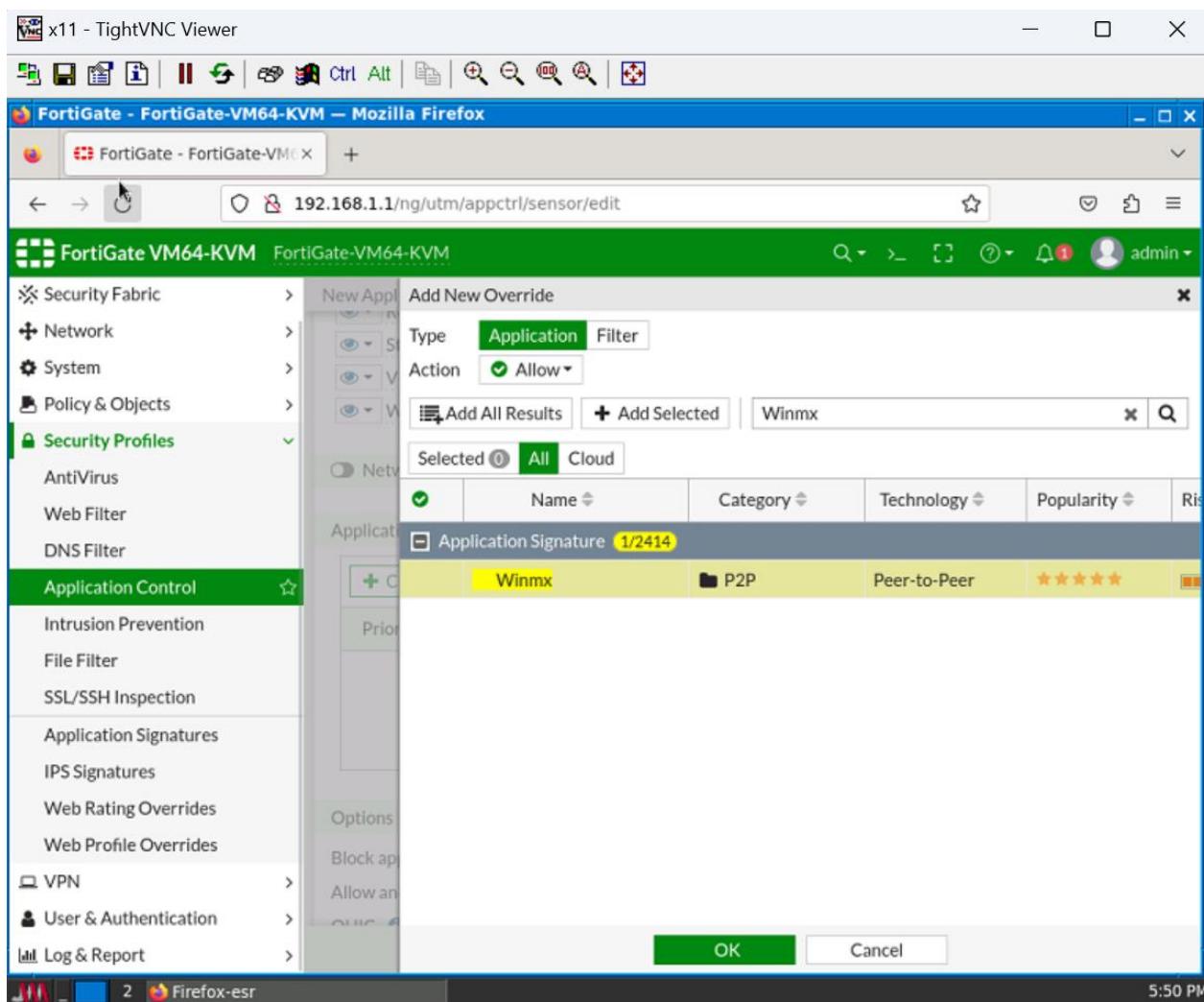


Figure 26 App control, Allow Winmx

App Control, WorldOfTanks, Allow

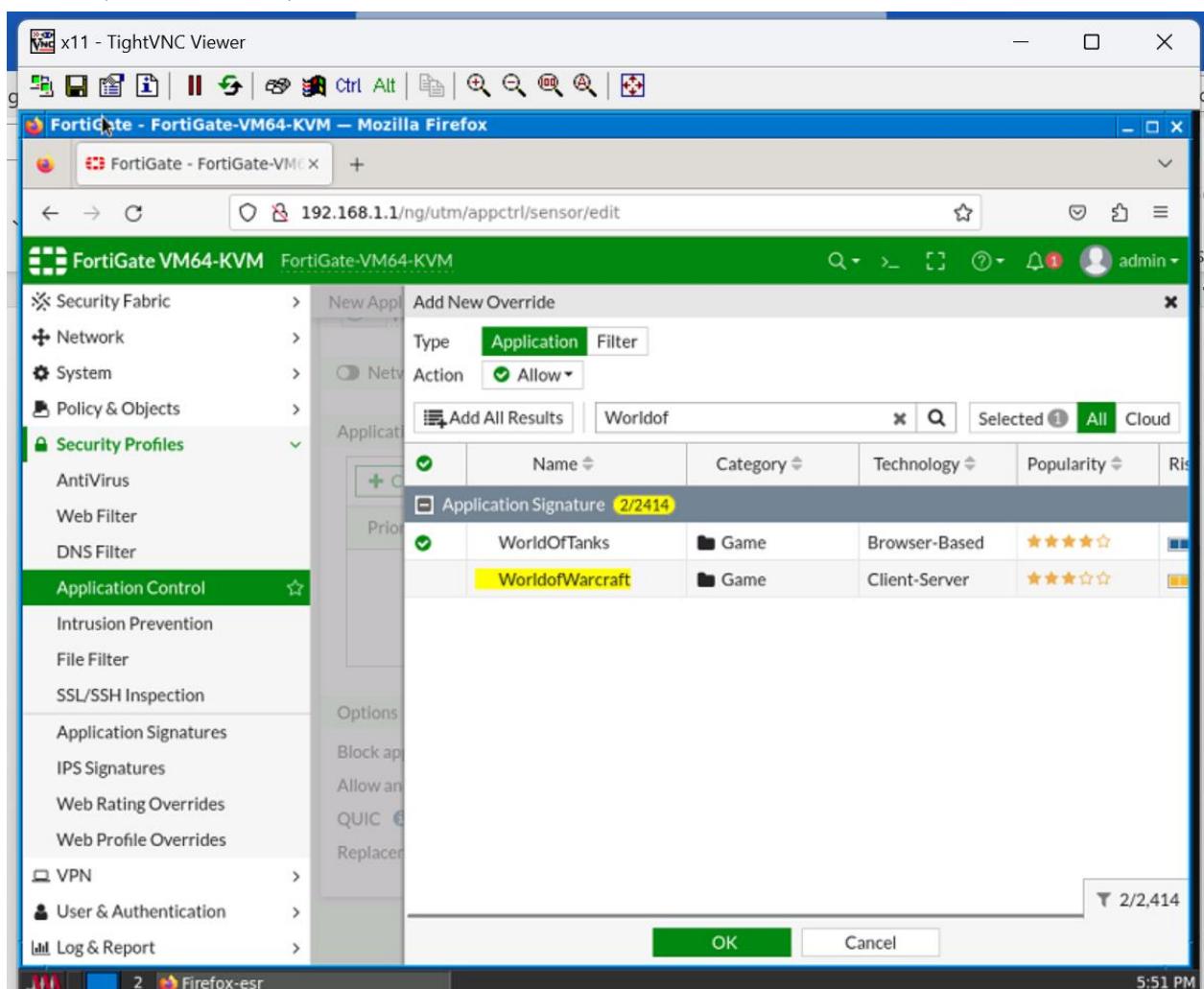


Figure 27 App Control, WorldOfTanks, Allow

App Control, https, Enable

The screenshot shows the configuration of the App Control feature. At the top, there is a list of application sensors:

- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, 16)
- Video/Audio (206, 13)
- Web.Client (18)
- General.Interest (241, 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)
- VoIP (31)
- Unknown Applications

Below this is a section titled "Network Protocol Enforcement" with a toggle switch that is turned on. Underneath are buttons for "Create New", "Edit", "Delete", and "Search". A search bar contains the text "PROT HTTPS".

Port	Enforce Protocols	Violation Action
Port undefined	PROT HTTPS	Monitor

A small number "1" is displayed in the bottom right corner of the table.

Application and Filter Overrides

Figure 28 App Control, https, Enable

The above profiles are connected to the Marketing_sales_it firewall policy

IT-2-WAN Policy

New Policy

Action ACCEPT DENY

Inspection Mode Flow-based Proxy-based

Firewall / Network Options

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options PROT default

Security Profiles

AntiVirus

Web Filter WEB it-web-filter

DNS Filter

Application Control APP Allow_Azuerus

IPS

Figure 29 it-2-wan

The screenshot shows a web application interface for managing URLs. At the top, there are four buttons: '+ Create New', 'Edit', 'Delete', and 'Status'. Below these are two buttons: 'Custom Categories' and a radio button labeled 'Show original categories'.

The main area displays a table with two columns: 'URL' and 'Status'. The 'Status' column contains a dropdown arrow icon. The table is organized into sections by category:

- custom1** (3 items):

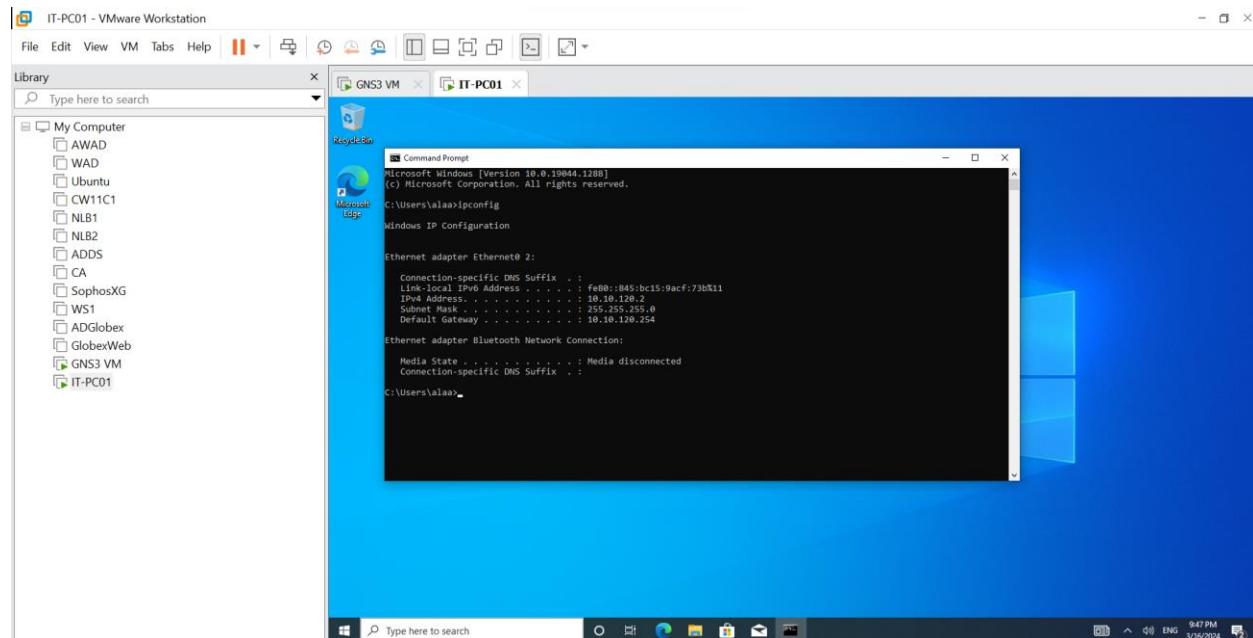
Phishing.org	Enable
phishing3.net	Enable
phisingwebsite.org	Enable
- custom2** (3 items):

hack.com	Enable
hack.net	Enable
haking.org	Enable

Figure 30 it_web_profile

IT-PC01 Configuration

The figure below shows that the PC takes an IP from DHCP, but after that using MAC binding in the firewall, I assign it a static IP mapped to its MAC address (10.10.120.10)



1) Setting Fixed IP with MAC Address ITPC01

IP Address Assignment Rules

Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0c:29:8c:a9:d2	Reserve IP	10.10.120.10
Implicit	Unknown MAC Addresses	Assign IP	

Figure 31 Setting Fixed IP with MAC Address ITPC01

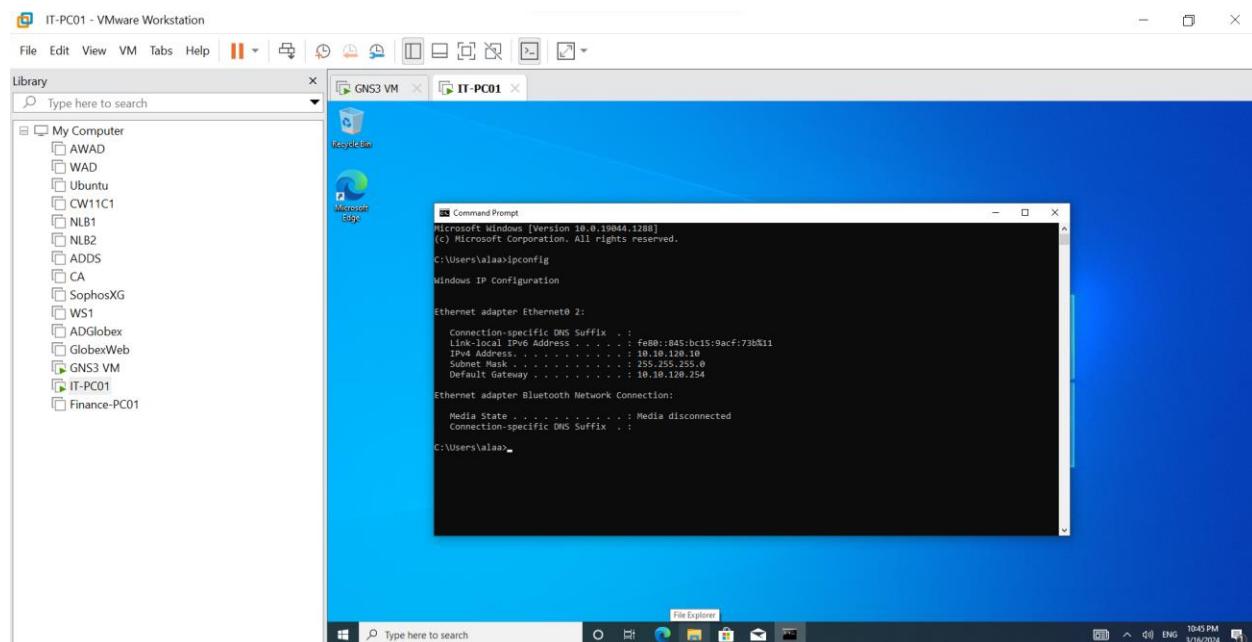


Figure 32 IP Config After MAC Binding

Finance-PC01

2) Bind Finance PC01 wit IP 10.10.140.10

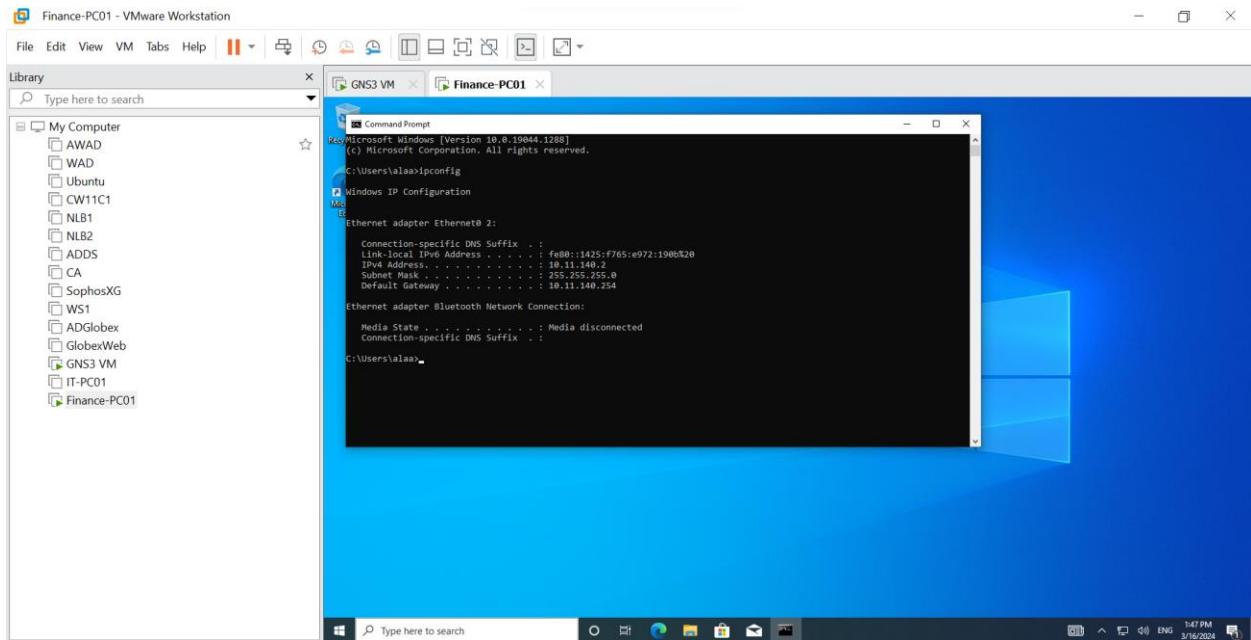
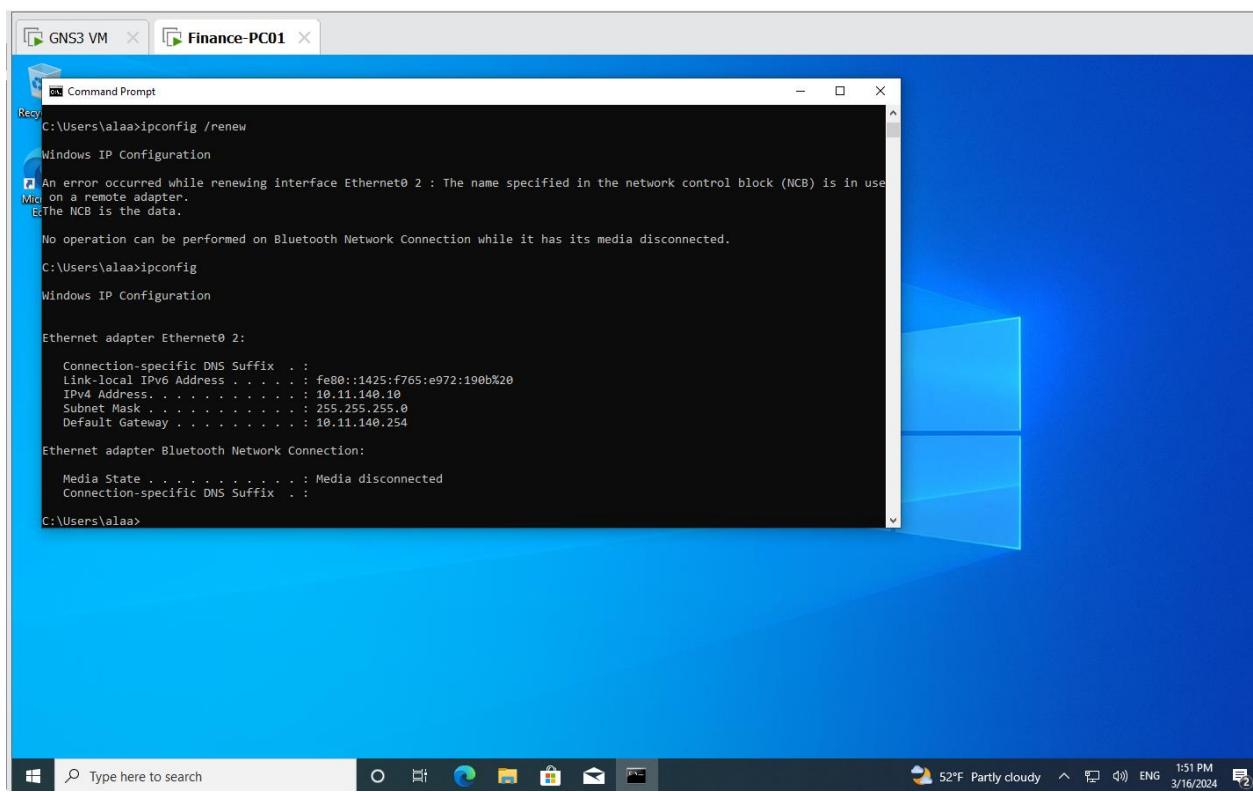


Figure 33 Finance PC After Binding IP

IP Address Assignment Rules			
Create New Edit Delete <input type="text"/> Search			
Add from DHCP Client List			
Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0C:29:28:4E:09	Reserve IP	10.11.140.10
Implicit	Unknown MAC Addresses	Assign IP	

Figure 34 Binding MAC with IP (Firewall)



Read only admin (Head Firewall).

This is done using two steps:

- Add Admin Profile with read only permissions called read_only
- Add a new user called Ali and assign the profile to him.

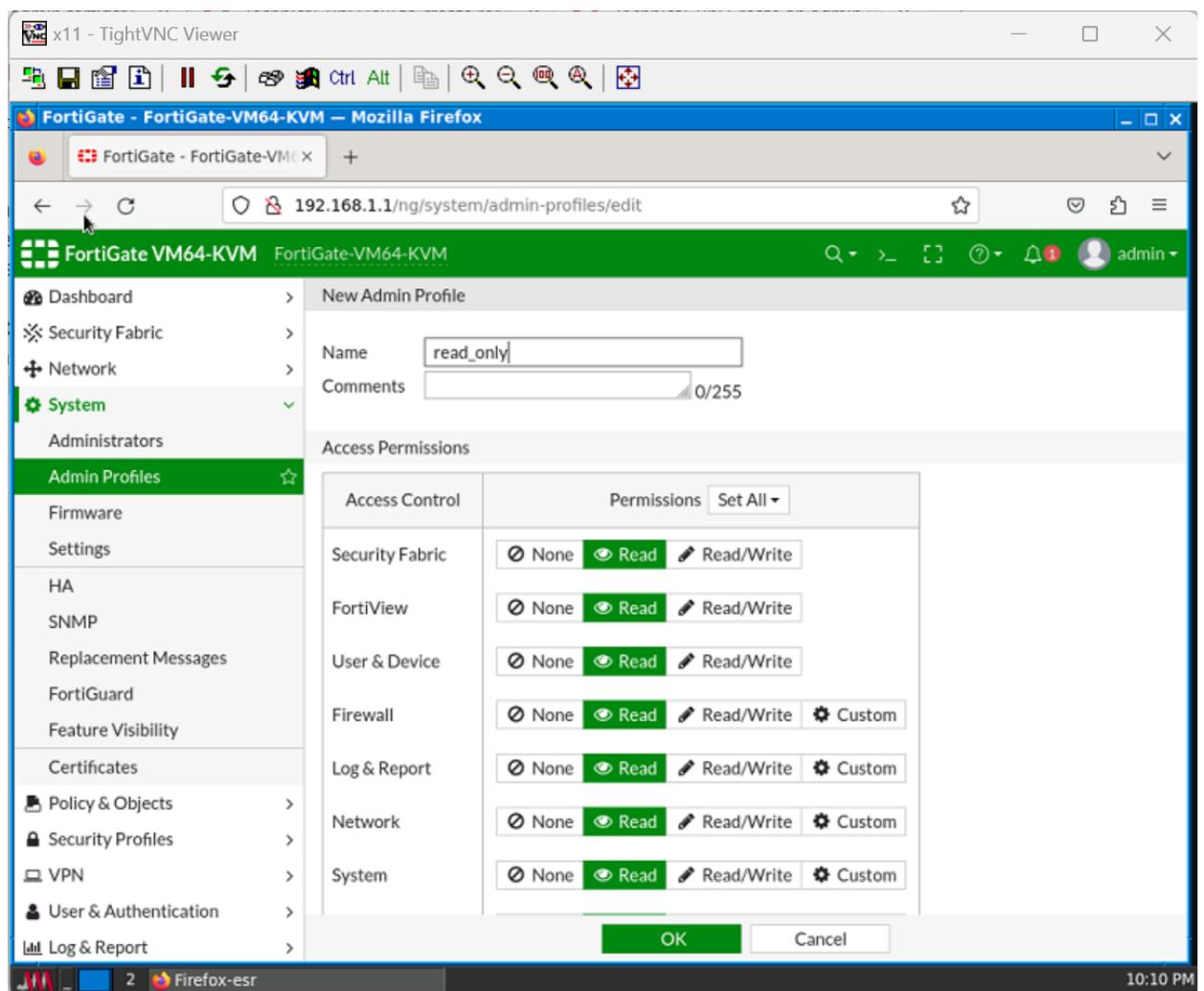


Figure 35 Add New Admin Profile

Step2: Assign the read only profile to the user ali, by creating a new user form system/administrators/create new user.

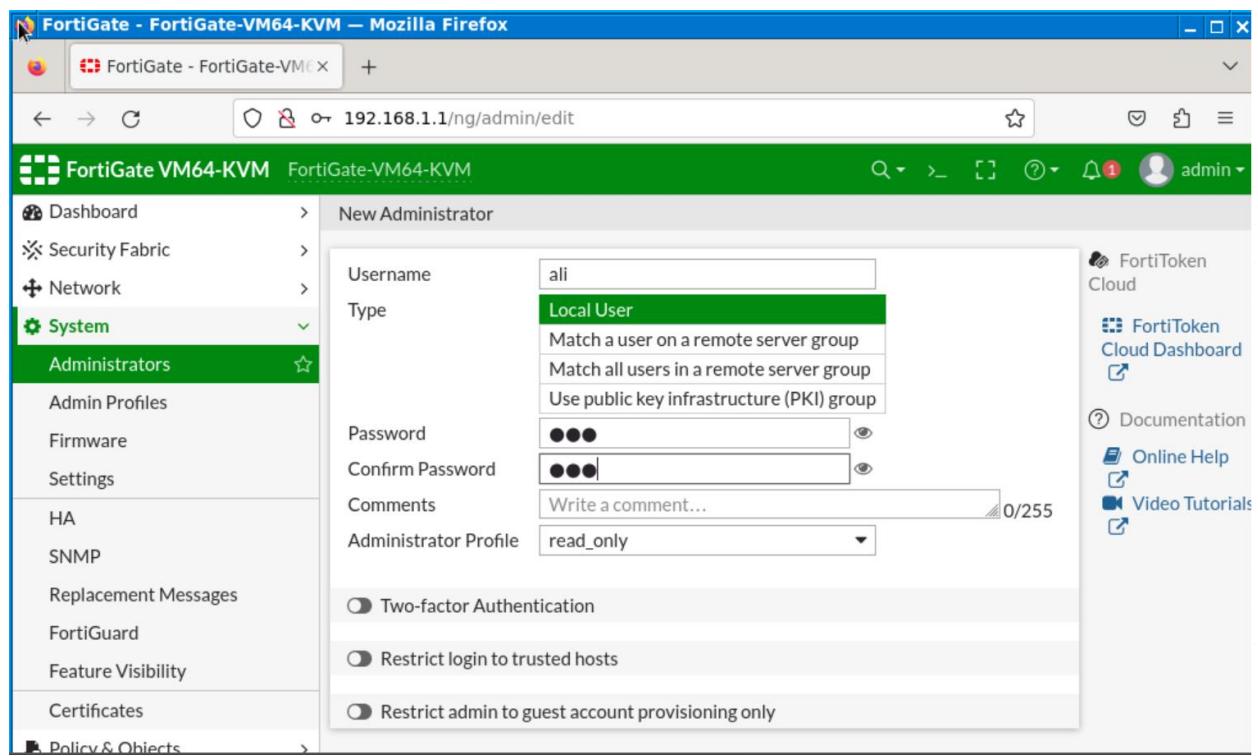
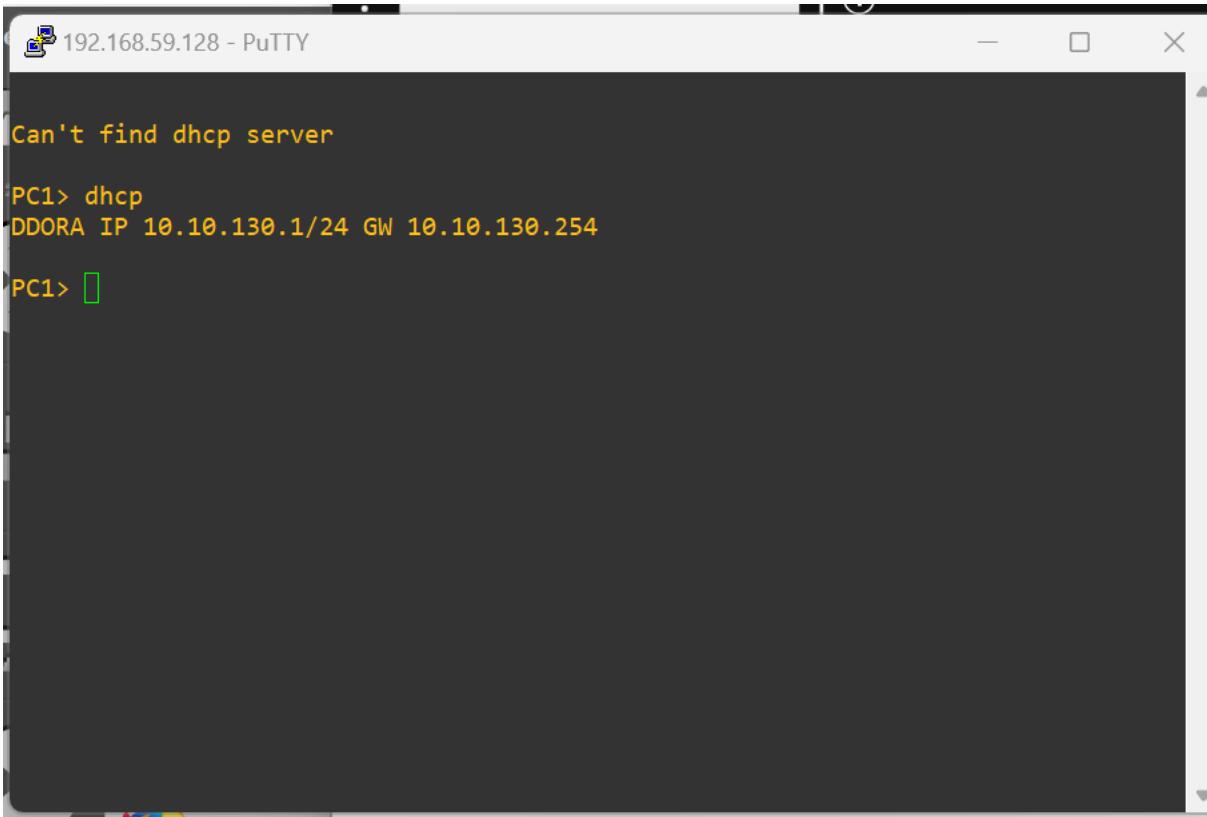


Figure 36 Ali User

Servers VLAN



```
192.168.59.128 - PuTTY

Can't find dhcp server

PC1> dhcp
DDORA IP 10.10.130.1/24 GW 10.10.130.254

PC1>
```

Figure 37 Servers VLANS DHCP

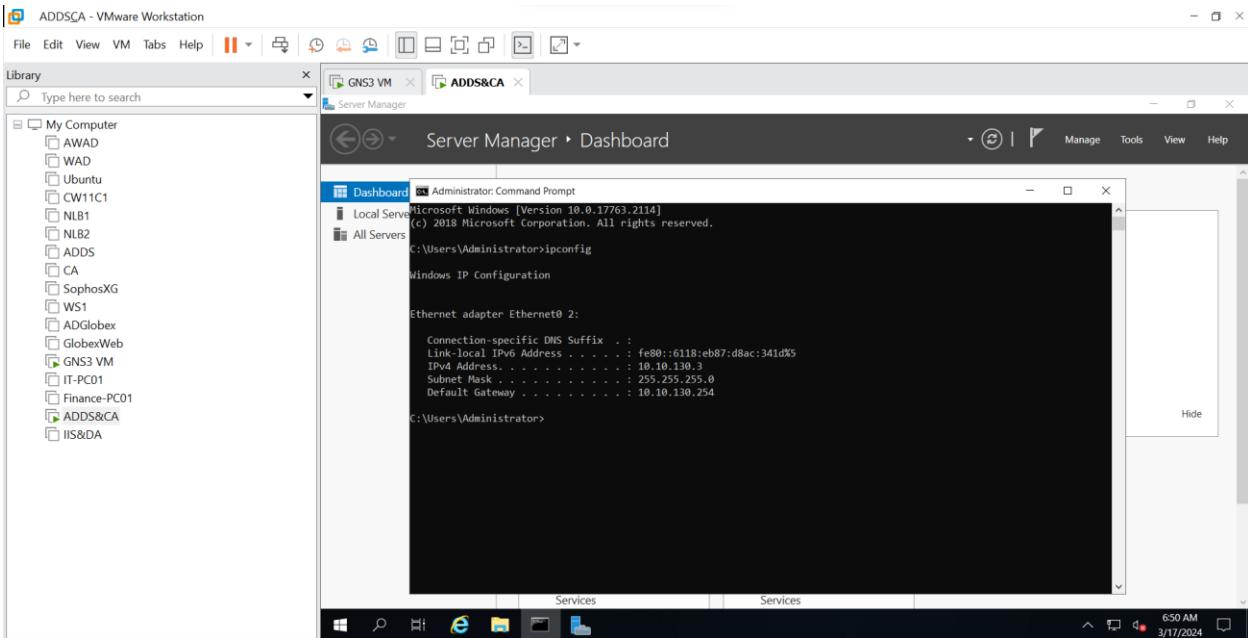


Figure 38 ADDS IP Settings

IPSEC Site to Site VPN

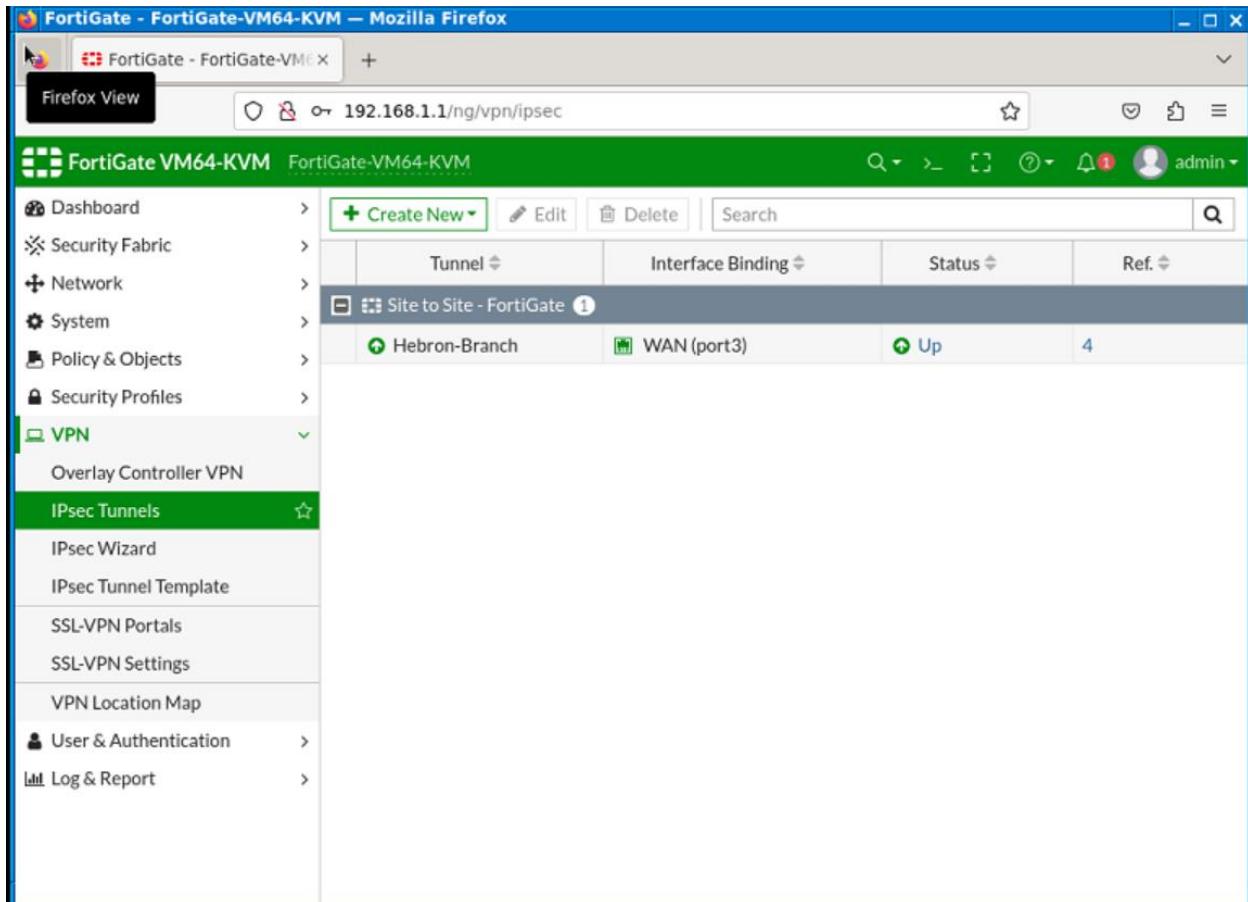


Figure 39 Site to Site VPN (Head Firewall)

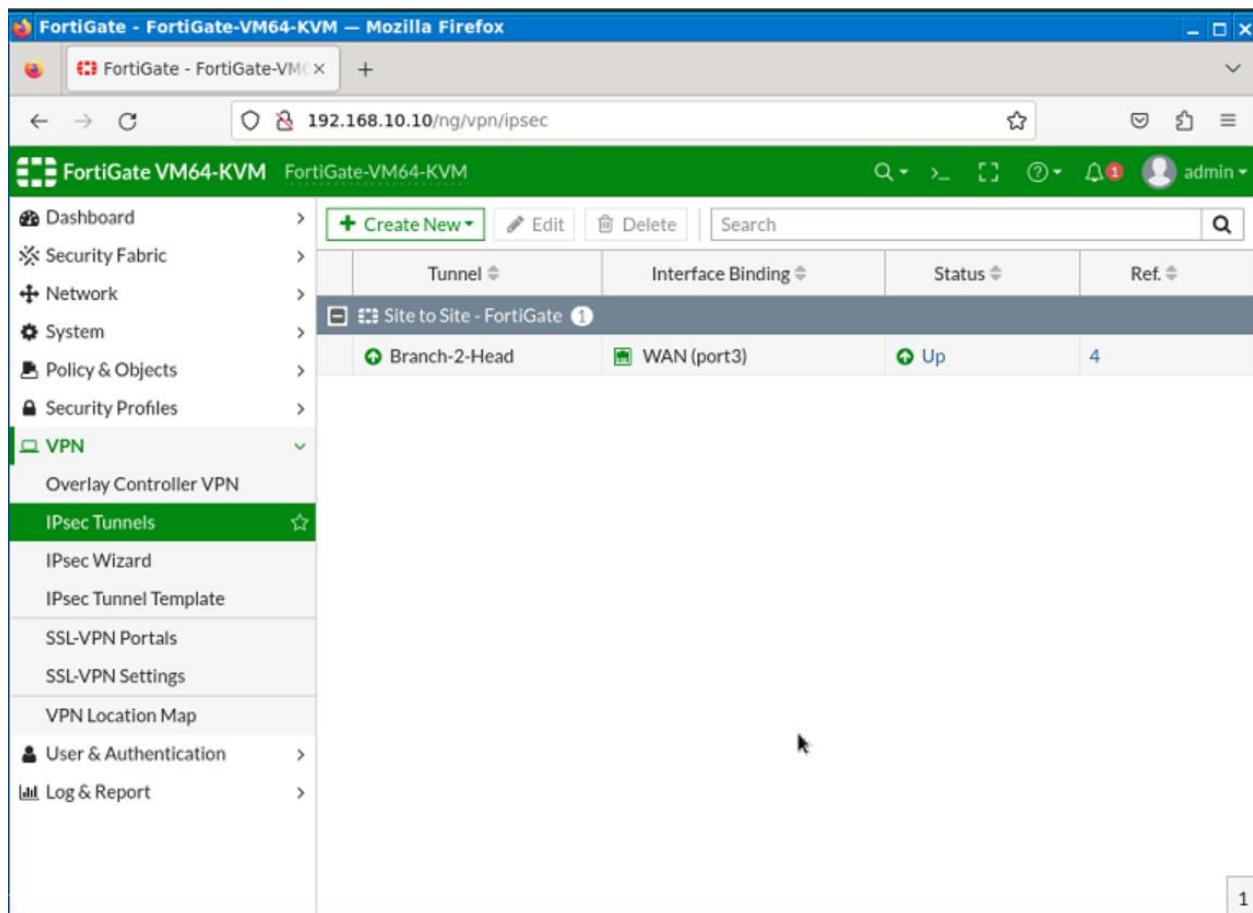


Figure 40 Site to Site VPN Branch Firewall

3) IPC01 and Finance PC02 join to the Domain.

The finance PC joins the domain successfully, However the ITPC01 can ping the ADDS globex.it and when trying to join domain it could not authenticate username and password, this may be because of a limitation in the Virtual machine resources. A policy from VLAN to servers is added so can the VLANS to access ADDS and IIS.

VLANS-2-Servers	<ul style="list-style-type: none"> ● IT ● marketing ● sales ● Hebron-Branch 	● servers-130 (servers)	<input type="checkbox"/> IT address <input type="checkbox"/> marketing address <input type="checkbox"/> sales address <input type="checkbox"/> Hebron-Branch_local	<input type="checkbox"/> servers address <input type="checkbox"/> always
-----------------	---	--	---	---

Figure 41 VLAN to Servers Policy

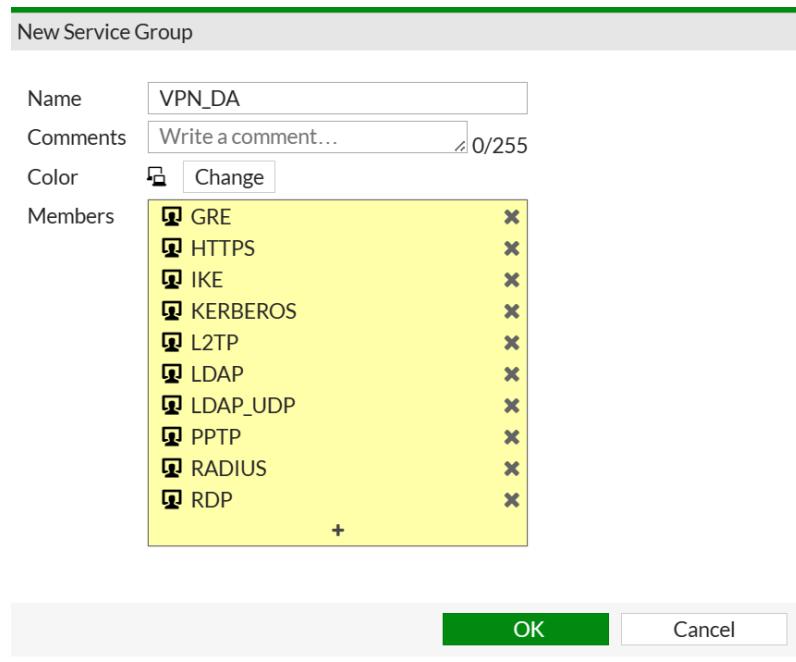


Figure 42 VLAN to SERVERS PORTS

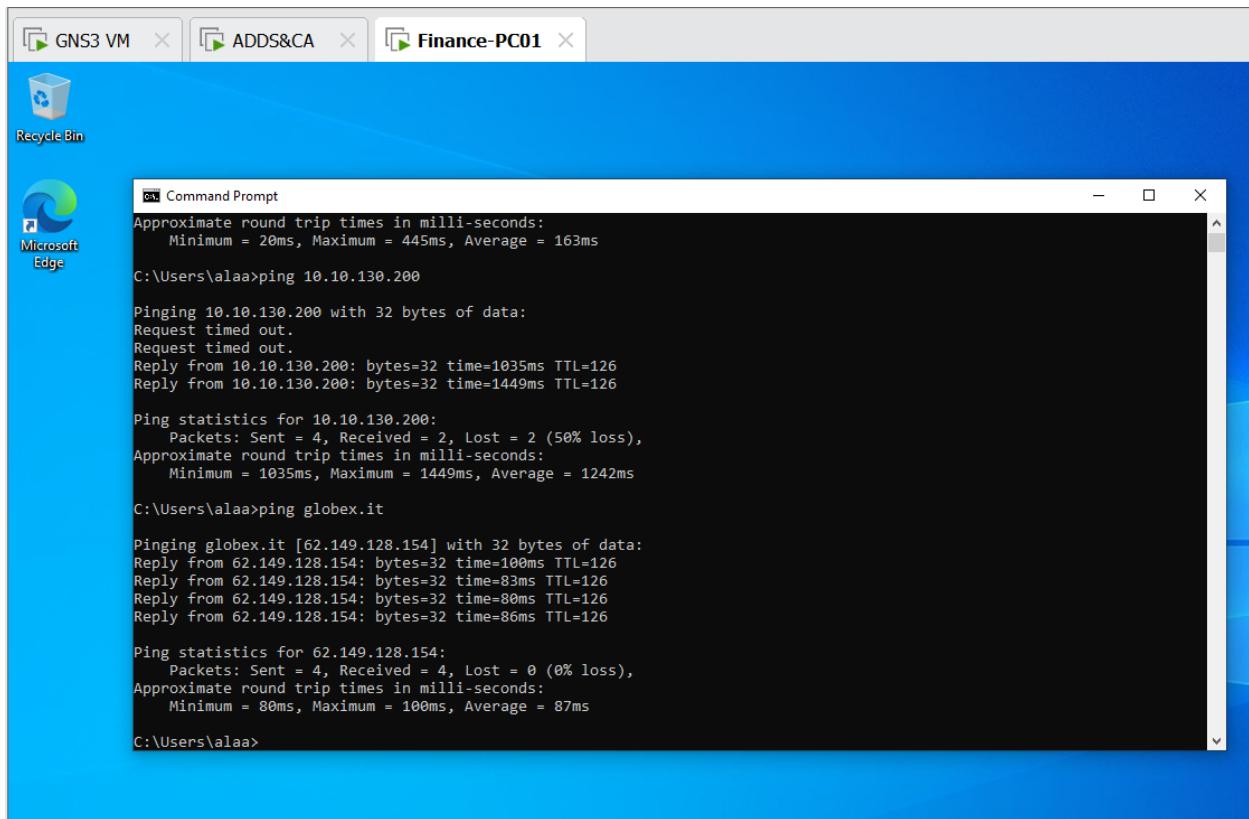


Figure 43 Ping globex.it

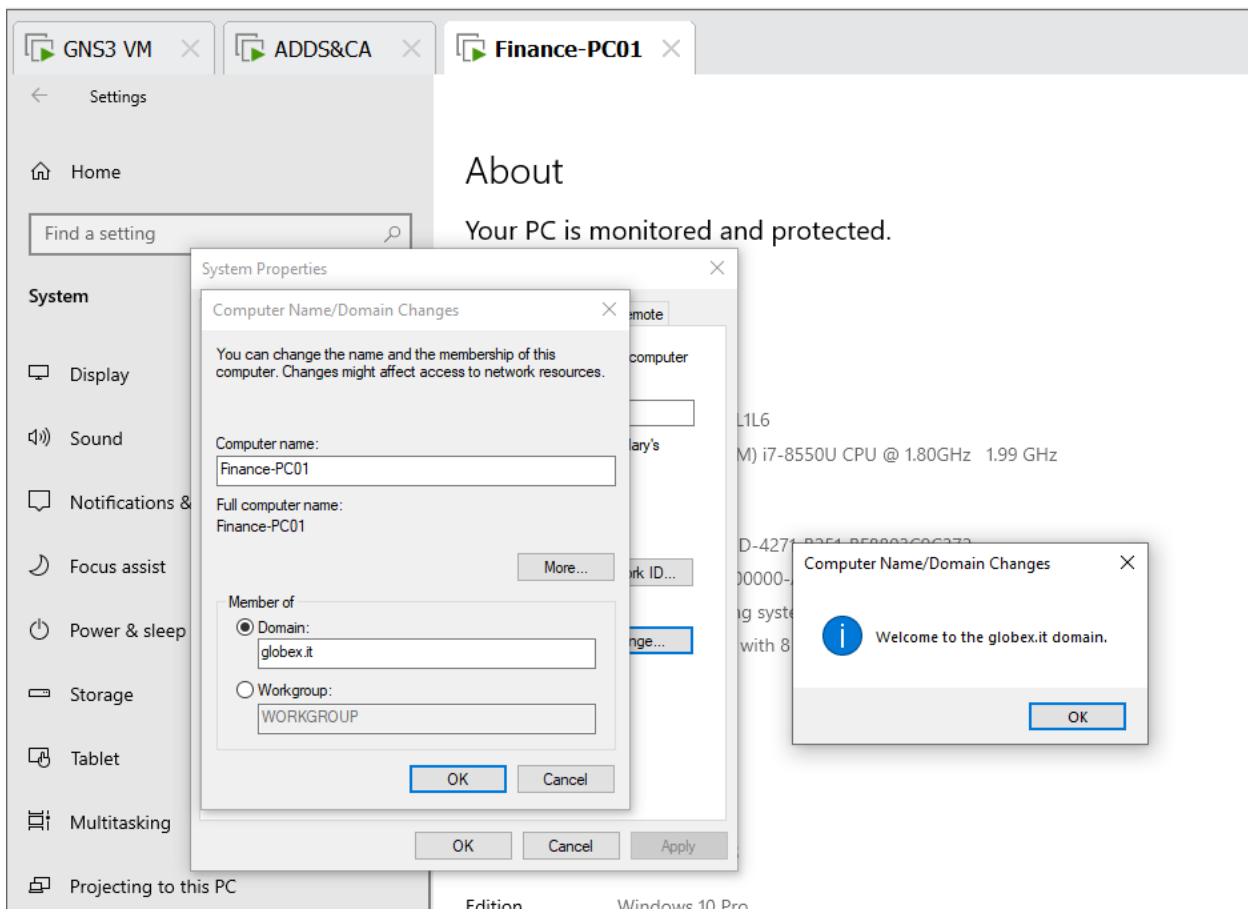


Figure 44 Successful Join of Finance PC02

ADDS – Users and groups.

Organizational Units

OU	Description
Servers	Organizational units for servers
marketing	Organizational units for marketing department users
sales	Organizational units for sales department users
IT	Organizational units for IT department users
Finance	Organizational units for Finance department users
Allowed PCS	Organizational units for Allowed Computers
Denied PCS	Organizational units for denied Computers
Shared Folders	Organizational units for Shared Folders Security groups: <ul style="list-style-type: none">• Marketing• Finance• IT• Sales• administration
Security Groups	Organizational units for the following Security groups (Direct Access): <ul style="list-style-type: none">• DA-Clients

The picture shows the OUs created using the Active directory for each Department.

The screenshot displays the Active Directory Users and Computers (ADUC) interface. On the left, the navigation pane shows the structure of Active Directory, including Saved Queries, globex.it (with subfolders like BuiltIn, Computers, Domain Controllers, ForeignSecurityPrincipals, and globex), and other standard AD components. The main pane lists Organizational Units (OUs) under the globex container. The OUs are:

Name	Type	Description
frp-marketing	Security Group ...	
grp-finance	Security Group ...	
grp-it	Security Group ...	
grp-sales	Security Group ...	
sf-administr...	Security Group ...	

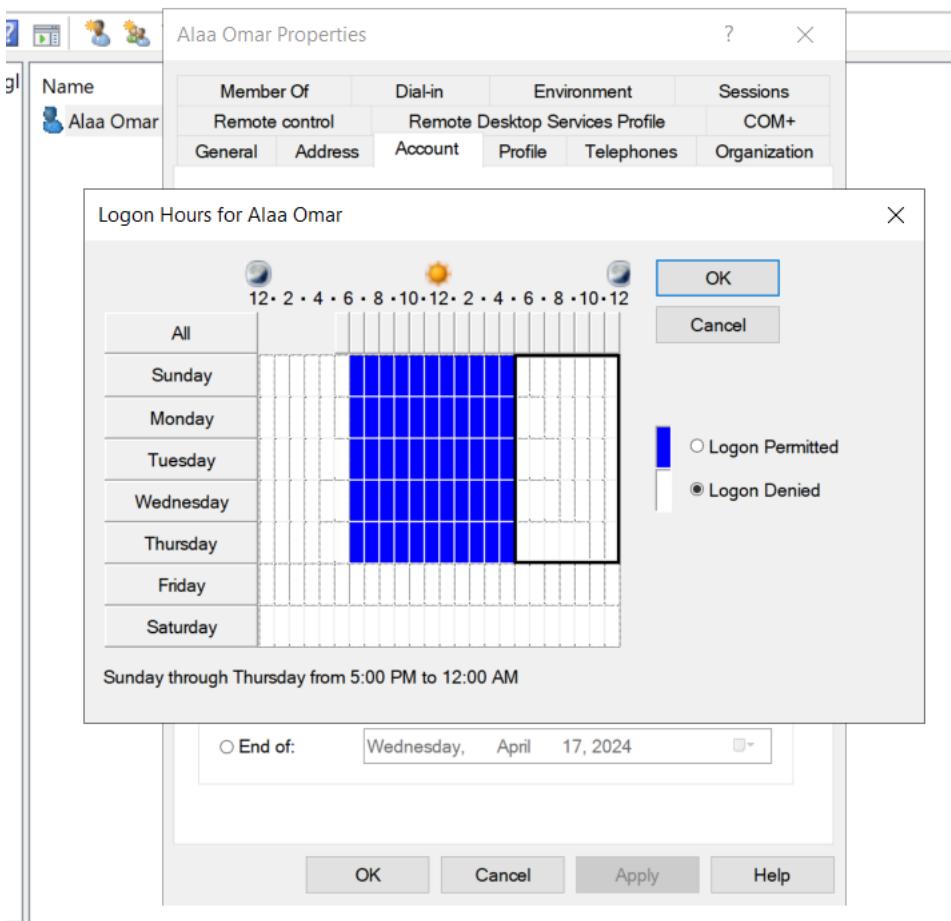
The OU 'SharedFolders' is highlighted with a blue selection bar at the bottom of its list item.

Figure 45 Active Directory OUs

Created Users:

User	Department
somar@globex.it	finance
aissa@glbex.it	IT
aomar@globex.it	marketing
lnairat@globex.it	sales

User Properties



Group Policy:

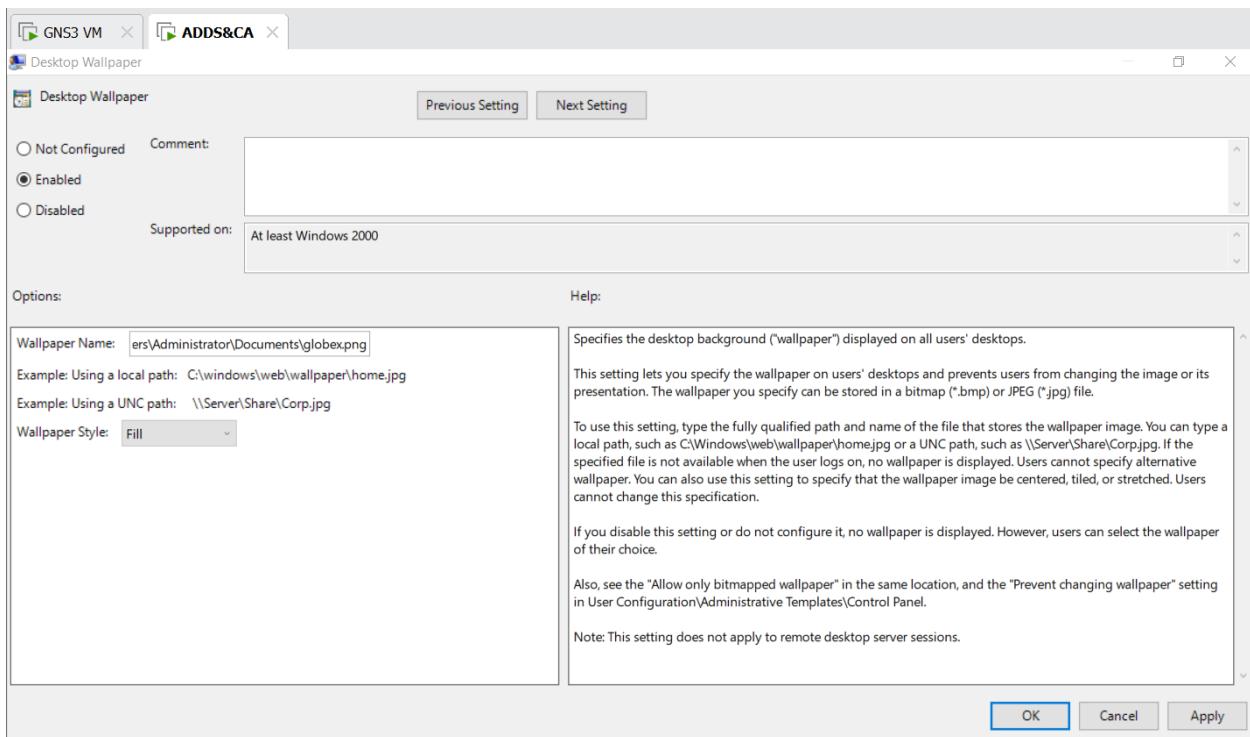
Group Policy Objects in globex.it				
Contents Delegation				
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	3/23/2024 2:49:24 PM	Domain Admins (GLOBEX...)
Default Domain Policy	Enabled	None	3/24/2024 10:12:20 PM	Domain Admins (GLOBEX...)
DirectAccess Client Settings	User configuration settings disabled	None	3/19/2024 5:36:38 PM	Domain Admins (GLOBEX...)
DirectAccess Server Settings	User configuration settings disabled	None	3/19/2024 5:36:30 PM	Domain Admins (GLOBEX...)
Disable removable media GPO	Enabled	None	3/18/2024 11:33:34 PM	Domain Admins (GLOBEX...)
Distribute Certificate GPO	Enabled	None	3/24/2024 11:37:14 PM	Domain Admins (GLOBEX...)
Folder Redirection GPO	Enabled	None	3/24/2024 10:03:00 PM	Domain Admins (GLOBEX...)
MapDrive GPO	Enabled	None	3/23/2024 11:22:12 PM	Domain Admins (GLOBEX...)
Standardize Wallpaper GPO	Enabled	None	3/18/2024 11:28:22 PM	Domain Admins (GLOBEX...)

Figure 46 Group Policy Summary

Standardize Wallpaper

Path: In the Group Policy Management Editor, navigate to User Configuration > Policies > Administrative Templates > Desktop > Desktop > Desktop Wallpaper

Setting	State	Comment
Enable Active Desktop	Not configured	No
Disable Active Desktop	Not configured	No
Prohibit changes	Not configured	No
Desktop Wallpaper	Enabled	No
Prohibit adding items	Not configured	No
Prohibit closing items	Not configured	No
Prohibit deleting items	Not configured	No
Prohibit editing items	Not configured	No
Disable all items	Not configured	No
Add/Delete items	Not configured	No
Allow only bitmapped wallpaper	Not configured	No



Disable removable Storage.

Path: Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access

Removable Storage Access

All Removable Storage classes: Deny all access

Setting

State	Comment
Not configured	No
Enabled	No
Not configured	No

Requirements: At least Windows Vista

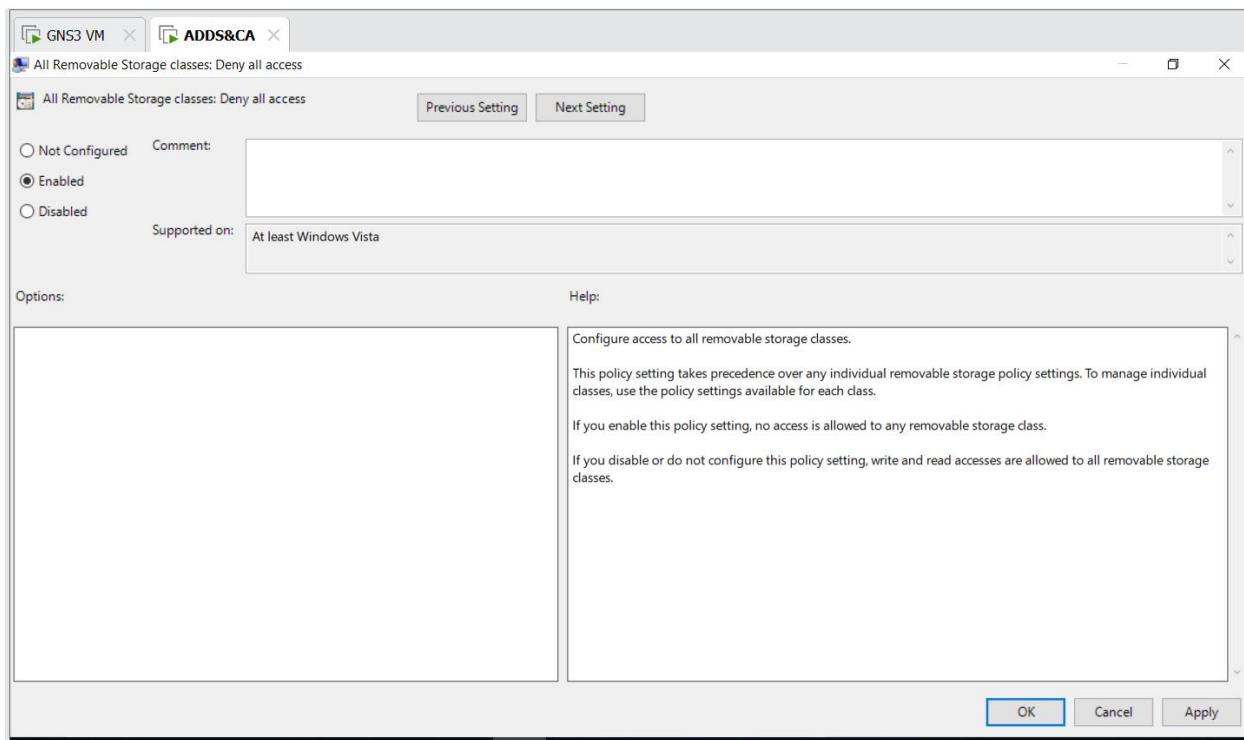
Description: Configure access to all removable storage classes.

This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

If you enable this policy setting, no access is allowed to any removable storage class.

If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.

1.



Prevent removable storage devices for all departments except IT.

Group Policy Management

File Action View Window Help

Forest: globex.it

Domains

globex.it

Default Domain Policy

Domain Controllers

globex

Standardize Wallpaper GPO

AllowedPCs

DeniedPCs

Disable removable media GPO

finance

IT

marketing

sales

servers

SharedFolders

Group Policy Objects

Default Domain Controllers Policy

Default Domain Policy

Disable removable media GPO

Standardize Wallpaper GPO

WMI Filters

Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Links

Display links in this location: globex.it

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

Location	Enforced	Link Enabled	Path
DeniedPCs	No	Yes	globex.it/globex/DeniedPCs

Security Filtering

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

Name

Authenticated Users

Add... Remove Properties

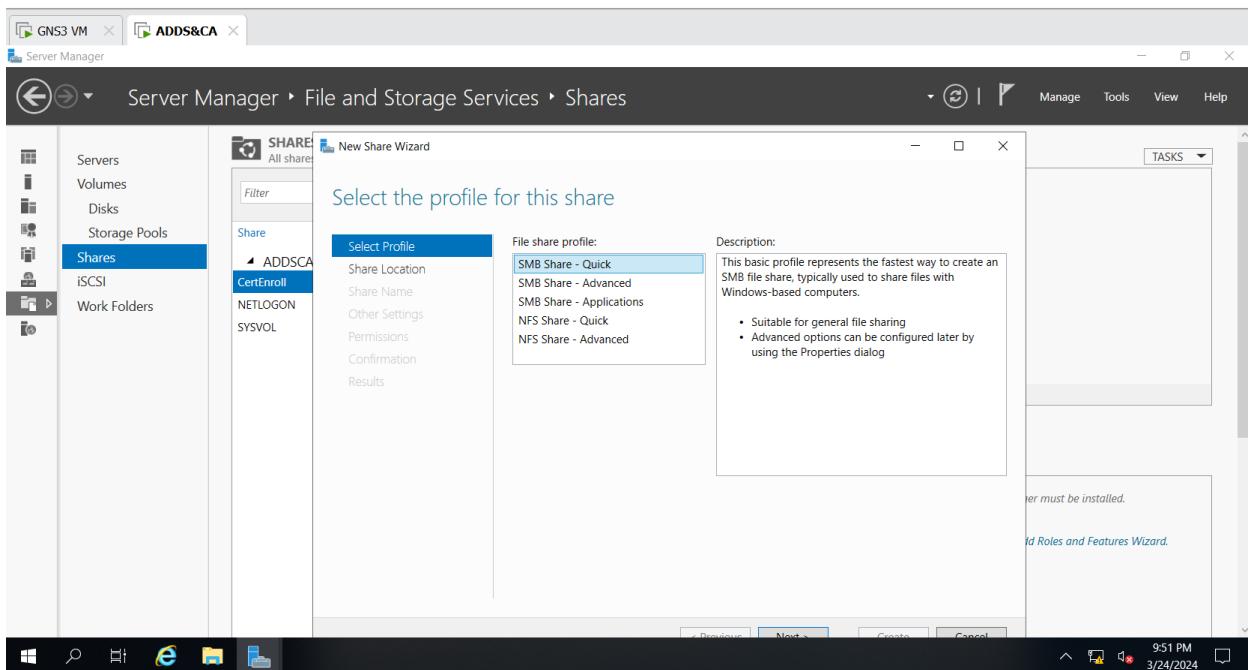
WMI Filtering

This GPO is linked to the following WMI filter:

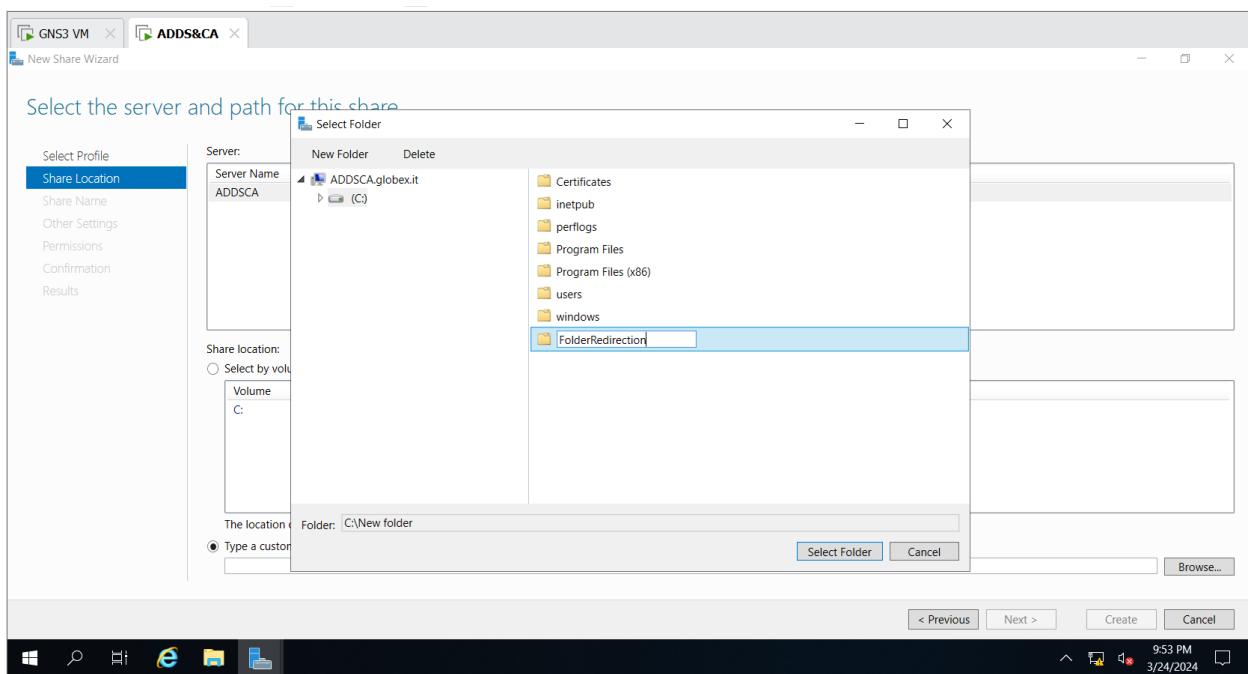
<none>

Folder Redirection Group Policy

Step1: Create a new share.

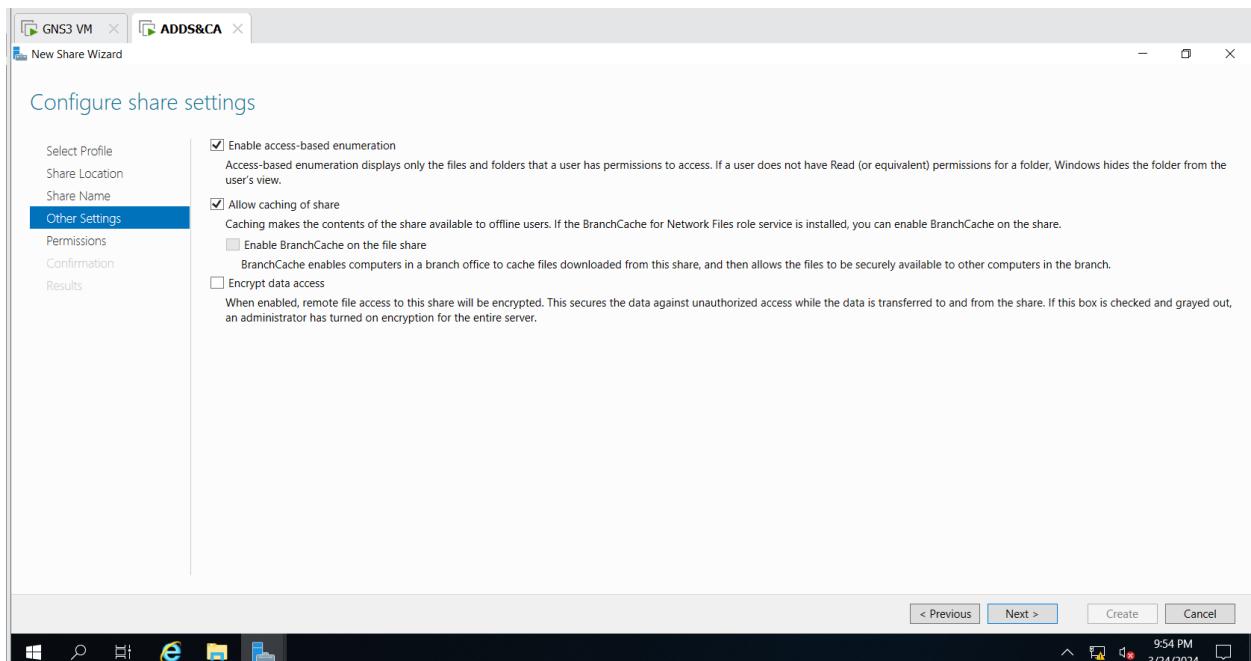


Step2: Create a folder redirection custom path.

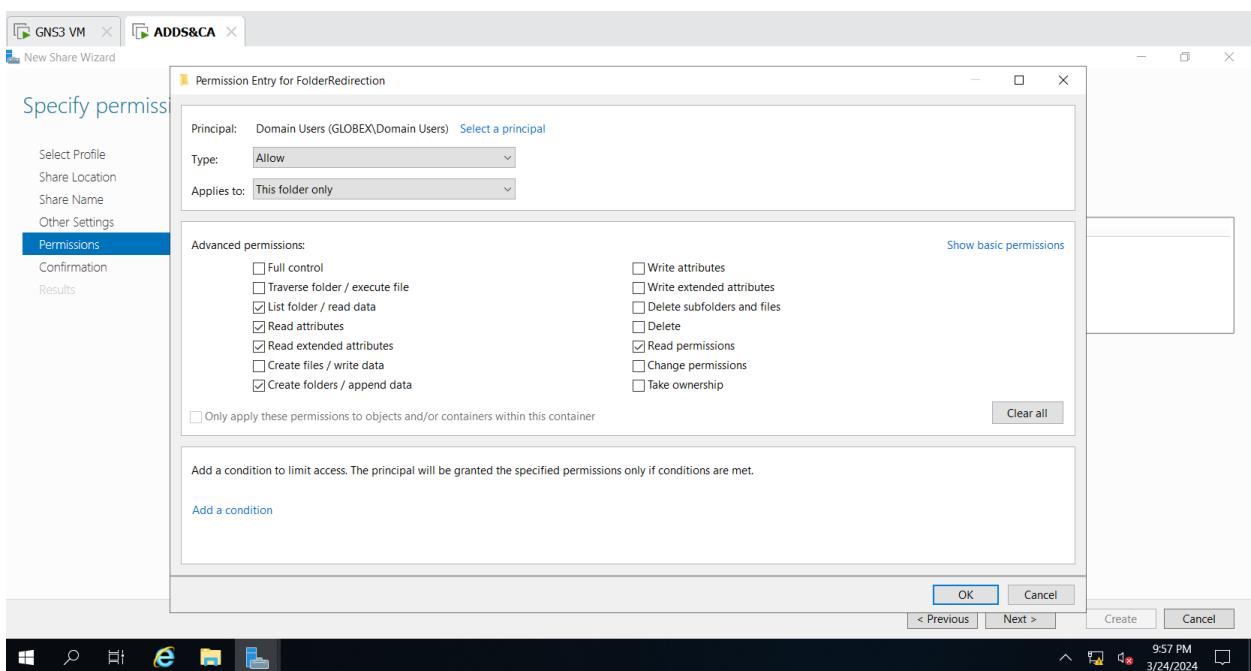


Remote path: [\\ADDSCA\\FolderRedirection\\$](\\ADDSCA\\FolderRedirection$)

Step3: Enable configuration.

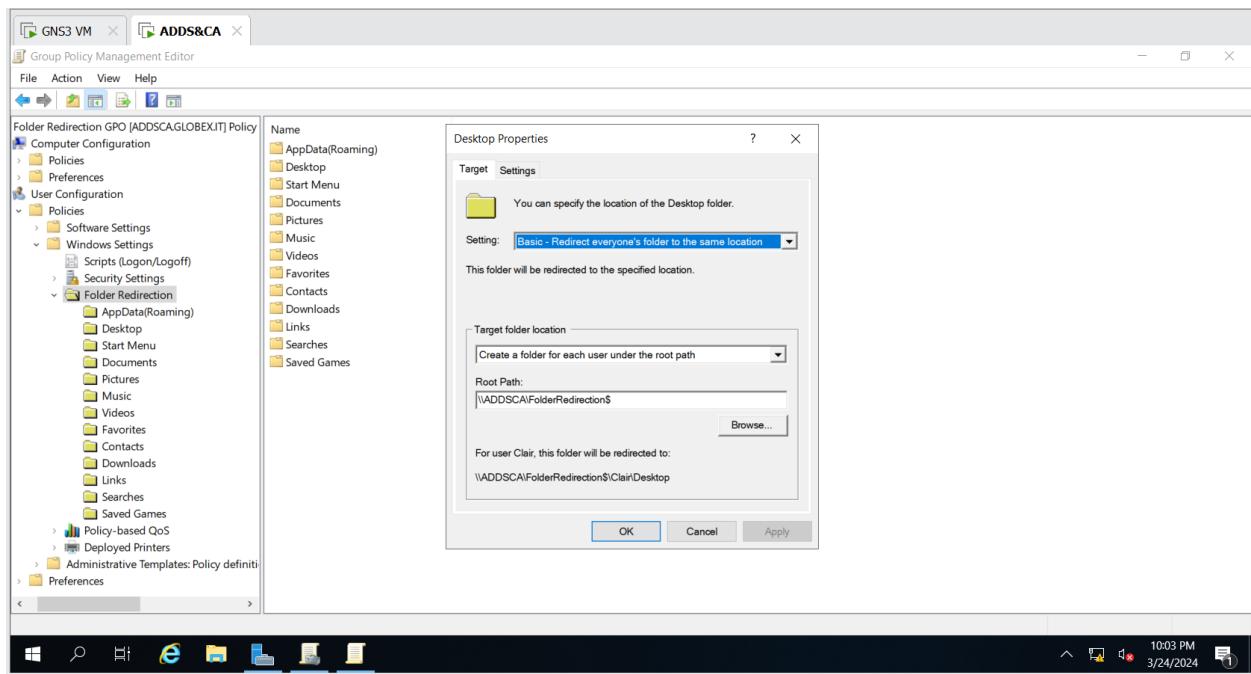


Step4: Specify permissions.

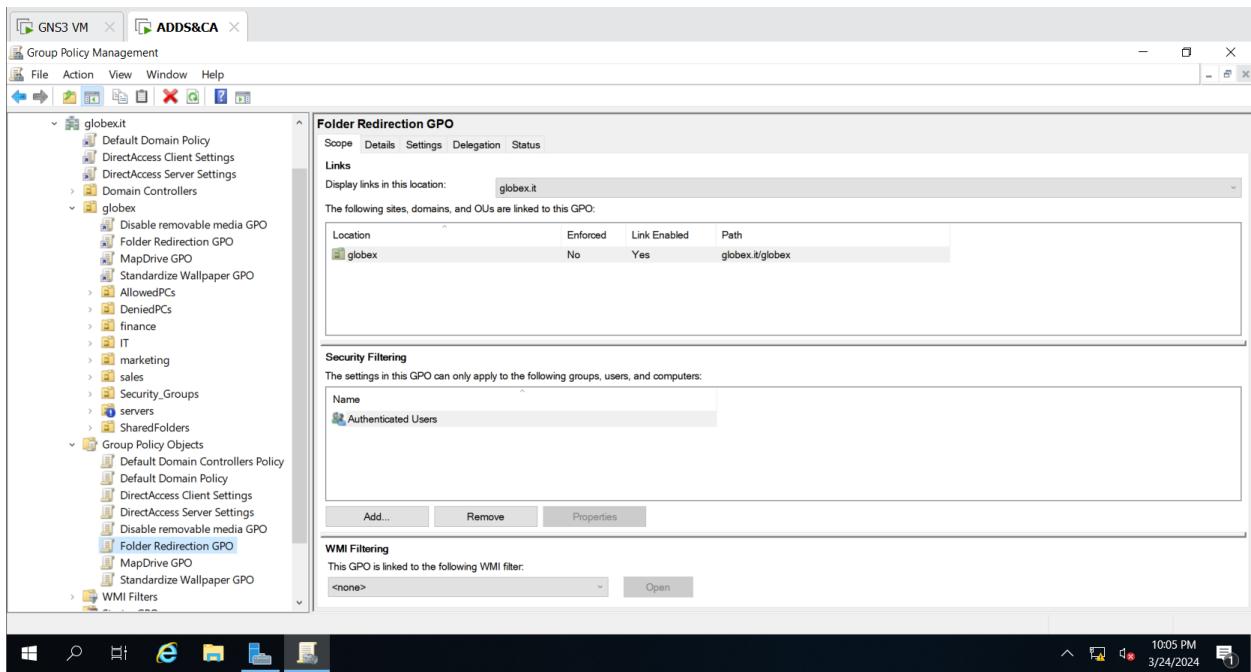


Step5: Add a group policy for Folder redirection.

Open User Configuration > Policies > Windows Settings > Folder Redirection

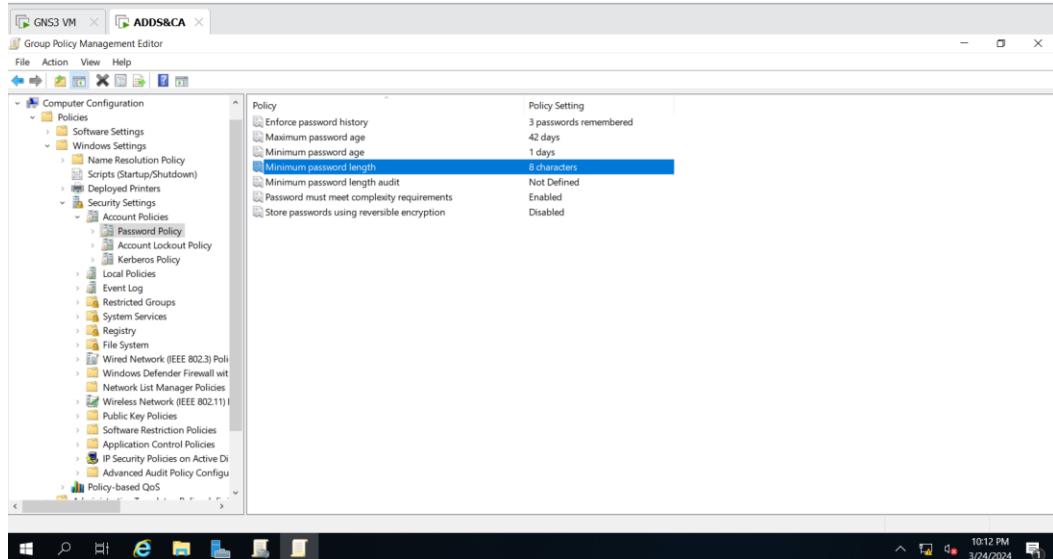


Step6: Link the group policy to Globex OU



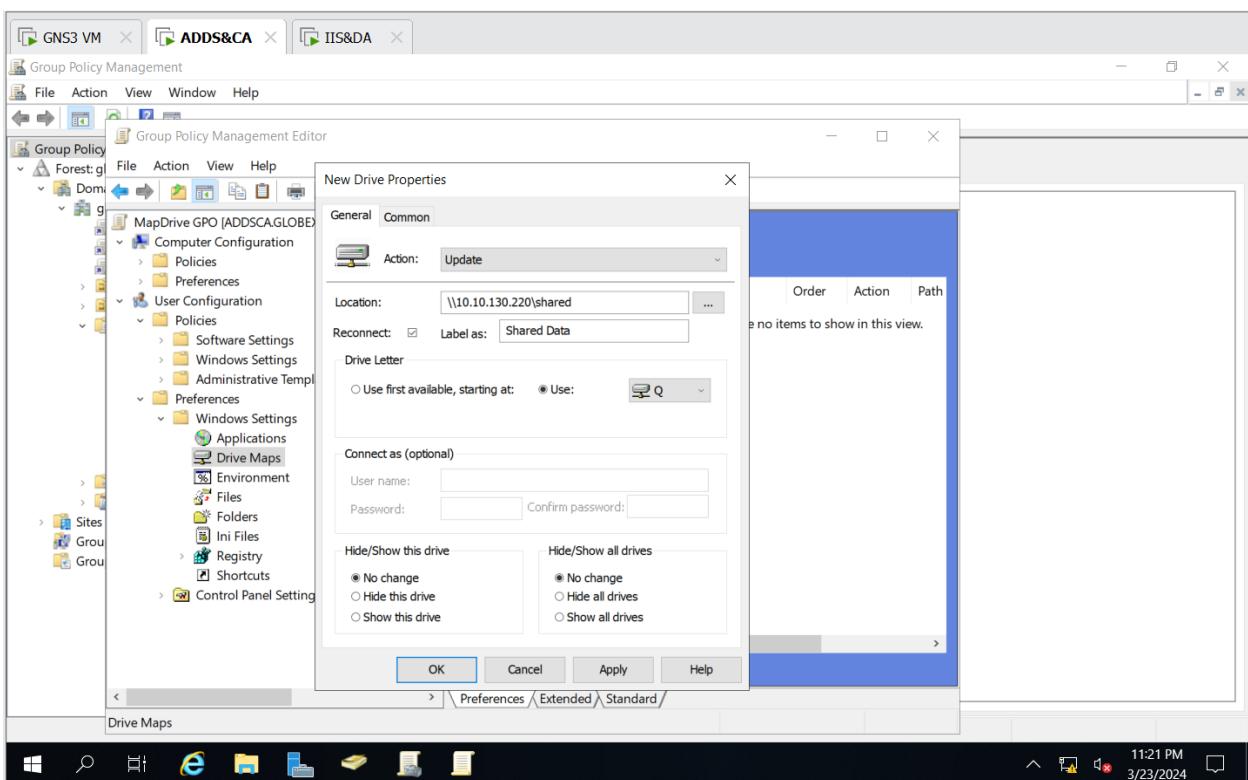
Password Policy

- Right-click the Default Domain Policy folder and click Edit.
- Navigate to Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Account Policies \ Password Policy
- Set Enforce password history for 3 passwords.
- Set minimum length of 8 characters.



Map Drive Policy :

Navigate to User Configuration -> Preferences -> Windows Settings -> Drive Mappings.
Right Click Drive Mappings, Select New – > Mapped Drive. Then Configure Drive Mapping Properties as in the picture.



Join Domain IT PC

Add Policy to access servers VLAN.

		Create New	Edit	Delete	Policy Lookup	<input type="text"/> Search	Export ▾	Interface Pair View	By Sequence
Name		From	To	Source					
VLANS-2-WAN		● IT ● marketing ● sales ● servers-130 (servers)	● WAN (port3)	█ IT address █ marketing address █ sales address █ servers address					
IT-2-Servers		● IT	● servers-130 (servers)	█ IT address					
Servers-2-IT		● servers-130 (servers)	● IT	█ servers address					
vpn_Hebron-Branch_local_0...		● servers-130 (servers)	● Hebron-Branch	█ Hebron-Branch_loca					
vpn_Hebron-Branch_remote...		● Hebron-Branch	● servers-130 (servers)	█ Hebron-Branch_rem					

ITPC to all vlans

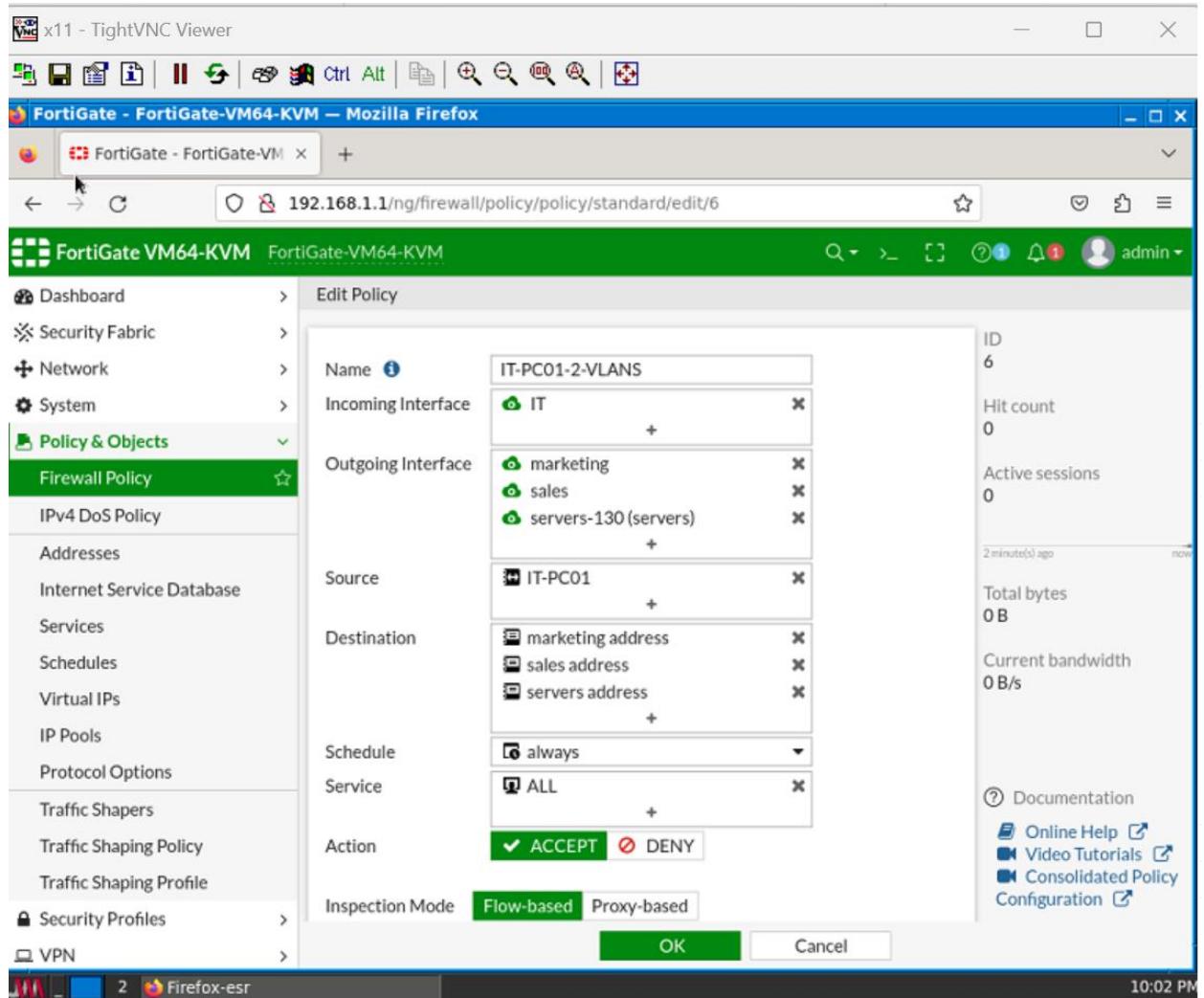


Figure 47 IT- to- VLANS Policy

```
C:\Users\alaa>ping 10.10.120.254 -t
Pinging 10.10.120.254 with 32 bytes of data:
Reply from 10.10.120.254: bytes=32 time=18ms TTL=255
Reply from 10.10.120.254: bytes=32 time=13ms TTL=255
Reply from 10.10.120.254: bytes=32 time=18ms TTL=255
Reply from 10.10.120.254: bytes=32 time=637ms TTL=255
Reply from 10.10.120.254: bytes=32 time=1627ms TTL=255
Reply from 10.10.120.254: bytes=32 time=992ms TTL=255
Request timed out.
```

```

Select Command Prompt - ping globex.it
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\alaa>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::845:bc15:9acf:73b%11
  IPv4 Address . . . . . : 10.10.120.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.10.120.254

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\alaa>ping globex.it

Pinging globex.it [62.149.128.157] with 32 bytes of data:
Reply from 62.149.128.157: bytes=32 time=2476ms TTL=126
Reply from 62.149.128.157: bytes=32 time=3112ms TTL=126

```

Figure 48 ITPC01 Ping globex.it Success

2. All Vlans To servers

The screenshot shows the FortiGate VM64-KVM interface. The left sidebar menu is open, showing various policy and configuration categories under 'Policy & Objects'. The 'Firewall Policy' option is selected. In the main pane, a policy named 'VLANS-2-Servers' is being edited. The policy details are as follows:

- Name:** VLANS-2-Servers
- Incoming Interface:** IT, marketing, sales, Hebron-Branch
- Outgoing Interface:** servers-130 (servers)
- Source:** IT address, marketing address, sales address, Hebron-Branch_local
- Destination:** servers address
- Schedule:** always
- Service:** GRE, HTTPS

On the right side of the screen, there is a summary panel for the policy:

- ID: 7
- Hit count: 0
- Active sessions: 0
- Total bytes: 0 B
- Current bandwidth: 0 B/s

At the bottom of the policy editor, there are 'OK' and 'Cancel' buttons.

Figure 49 VLANS to Servers Policy

Configuring IIS&DA

- Join Domain (the same vlan) no policies are needed.

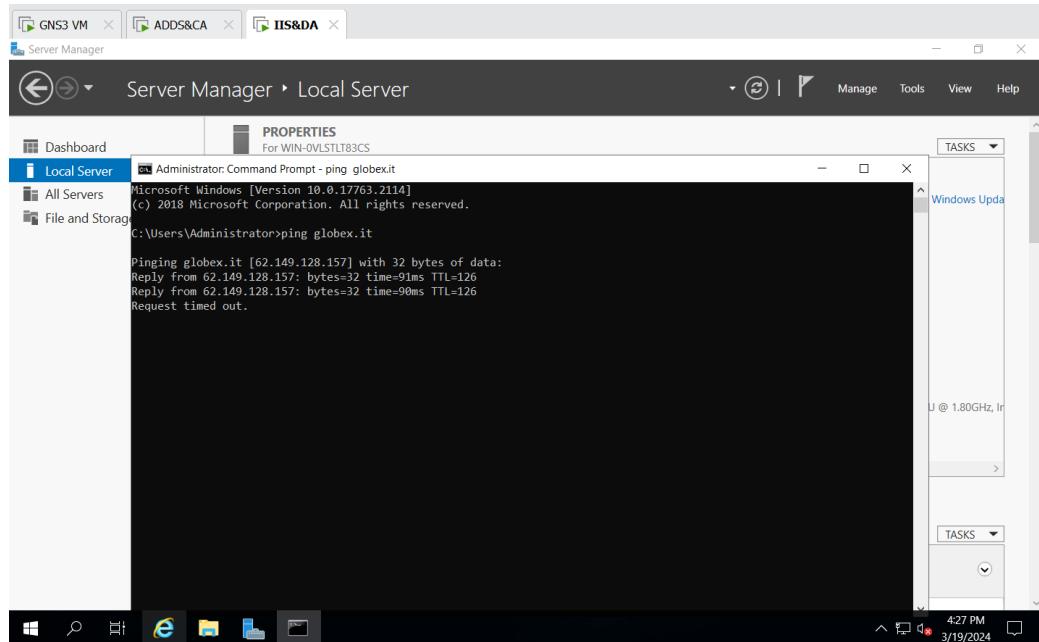


Figure 50 Ping globex.it Success

Join Domain

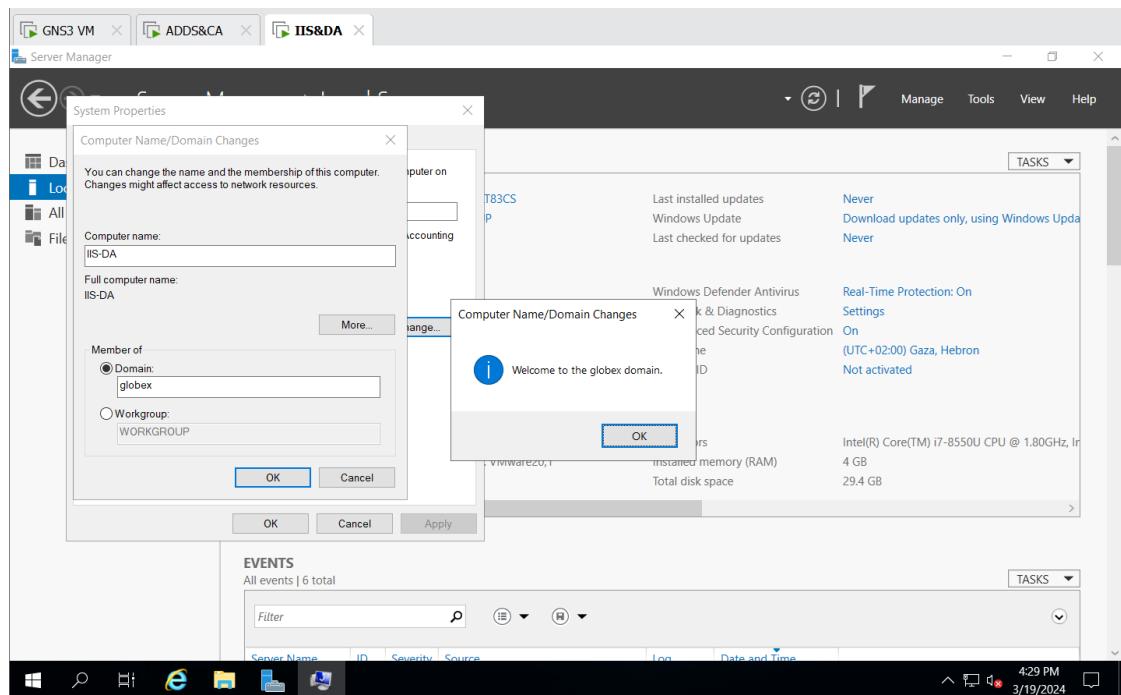


Figure 51 Successful Join to Domain

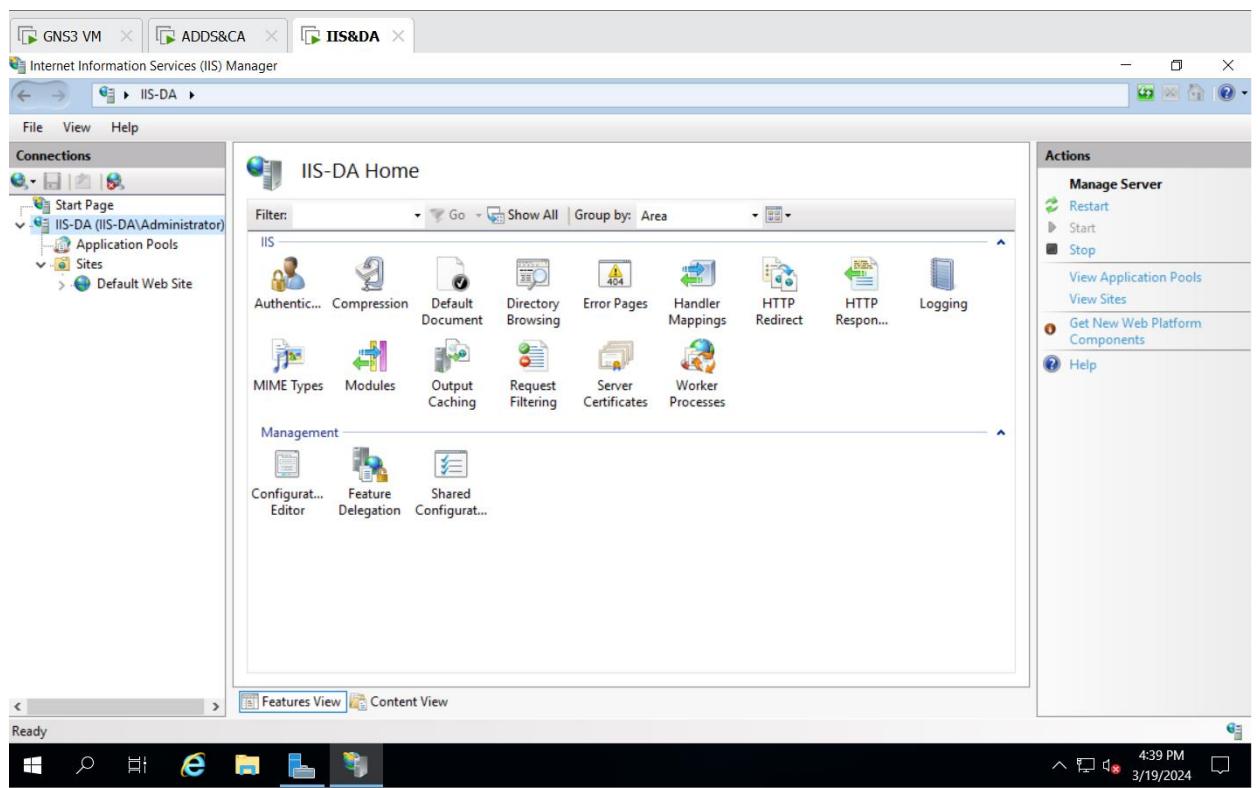


Figure 52 IIS Role

DA Configuration

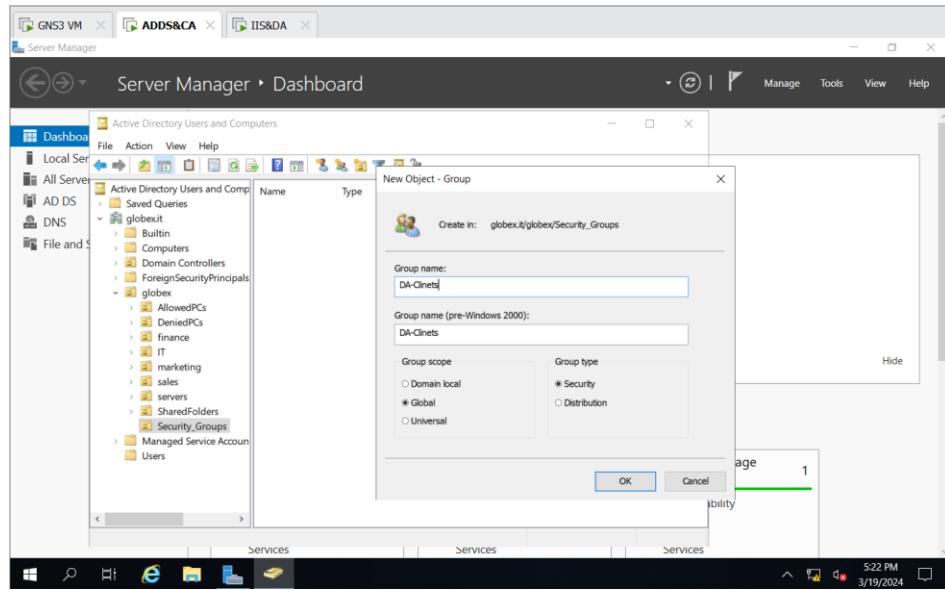


Figure 53 Create a Group for DA Computers

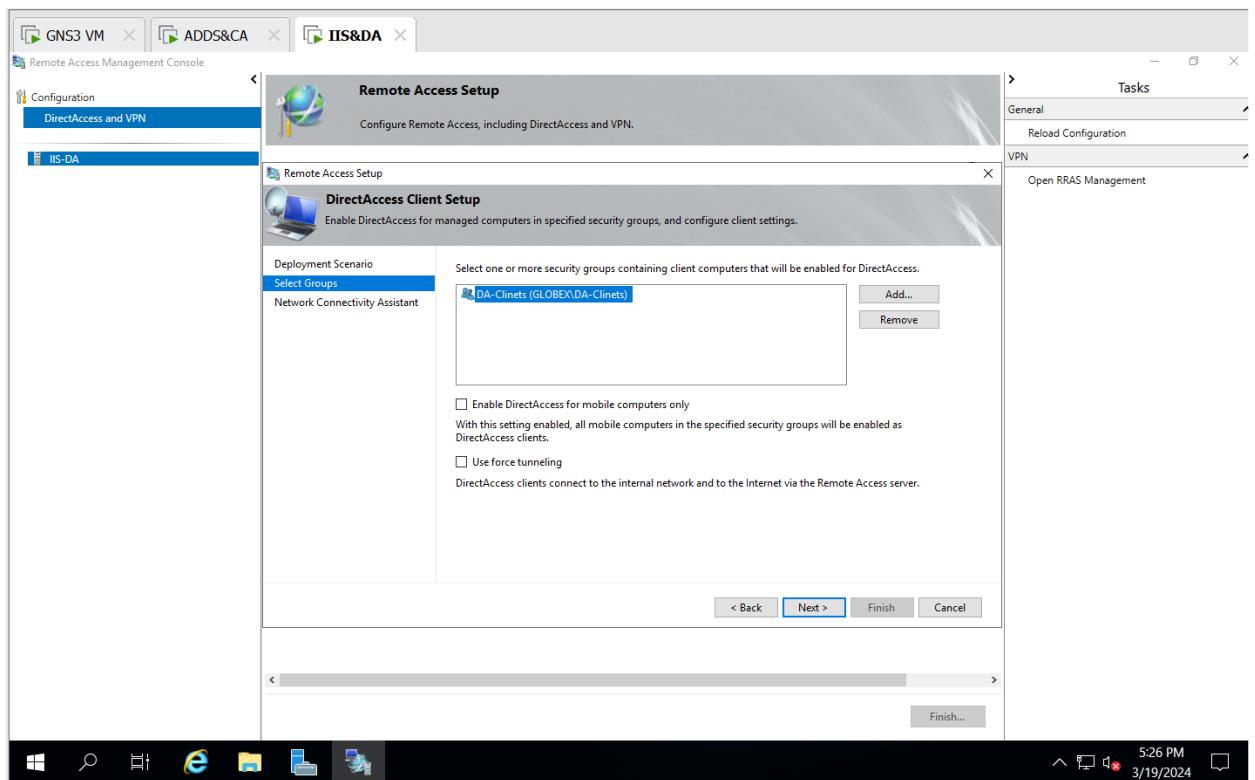


Figure 54 DA Configurations

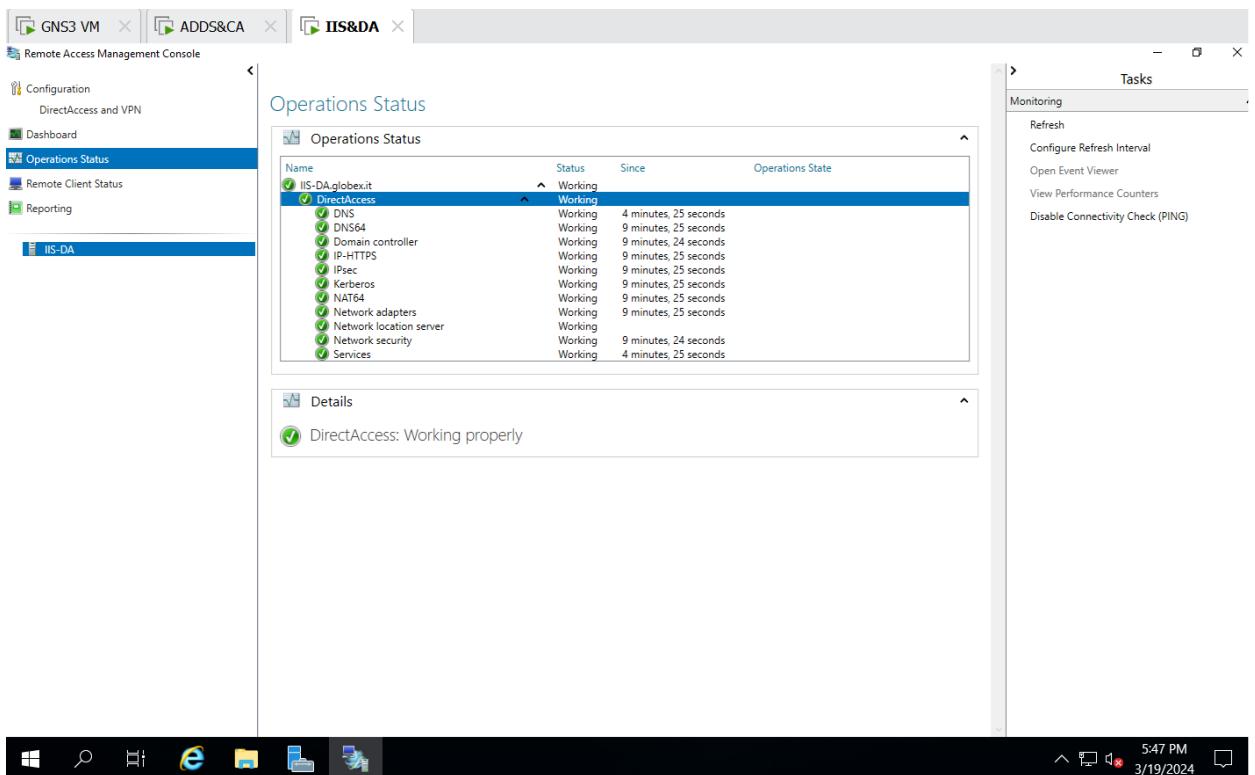


Figure 55 Successful Configurations

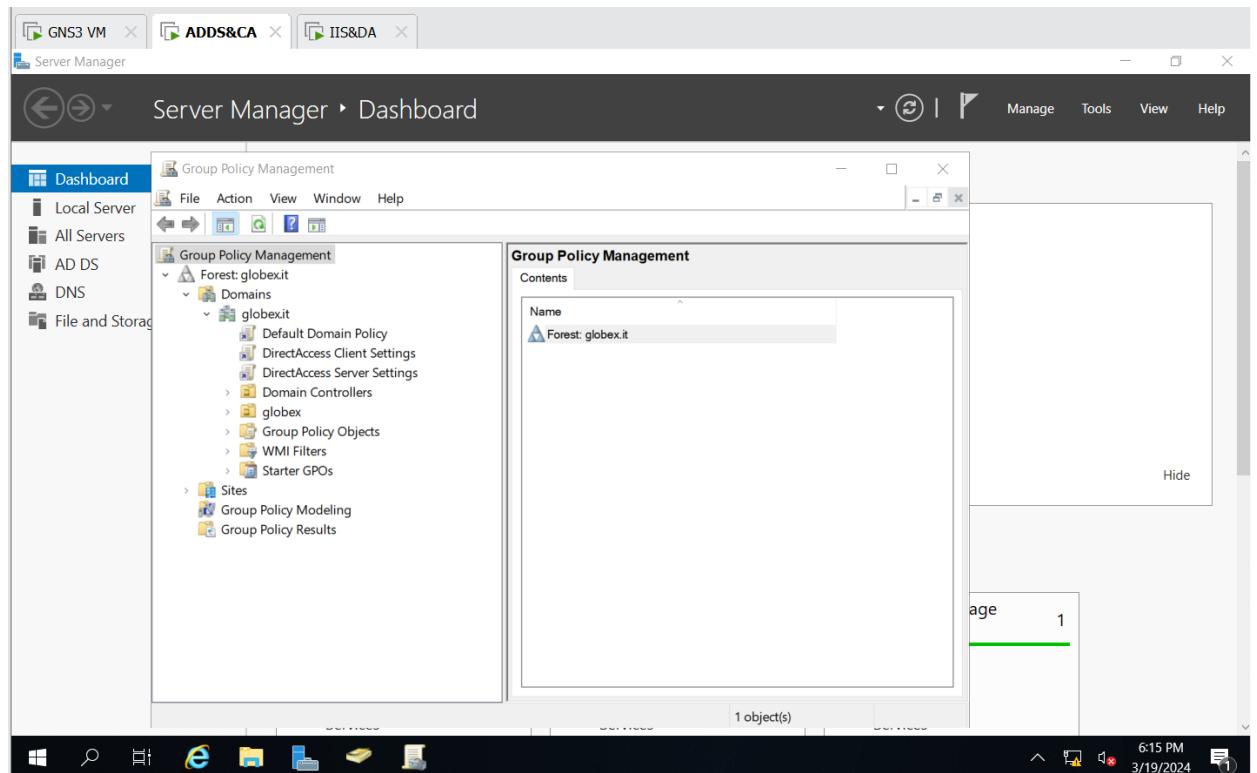


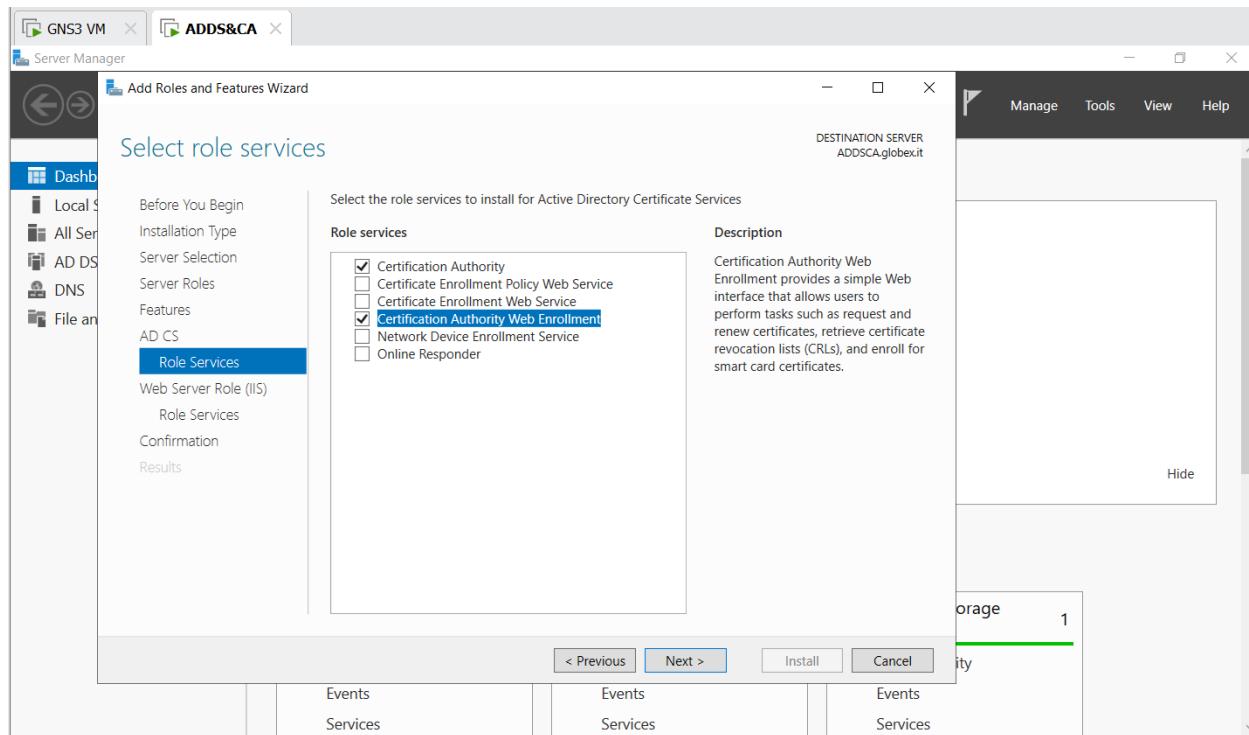
Figure 56 Automatic Created Policies

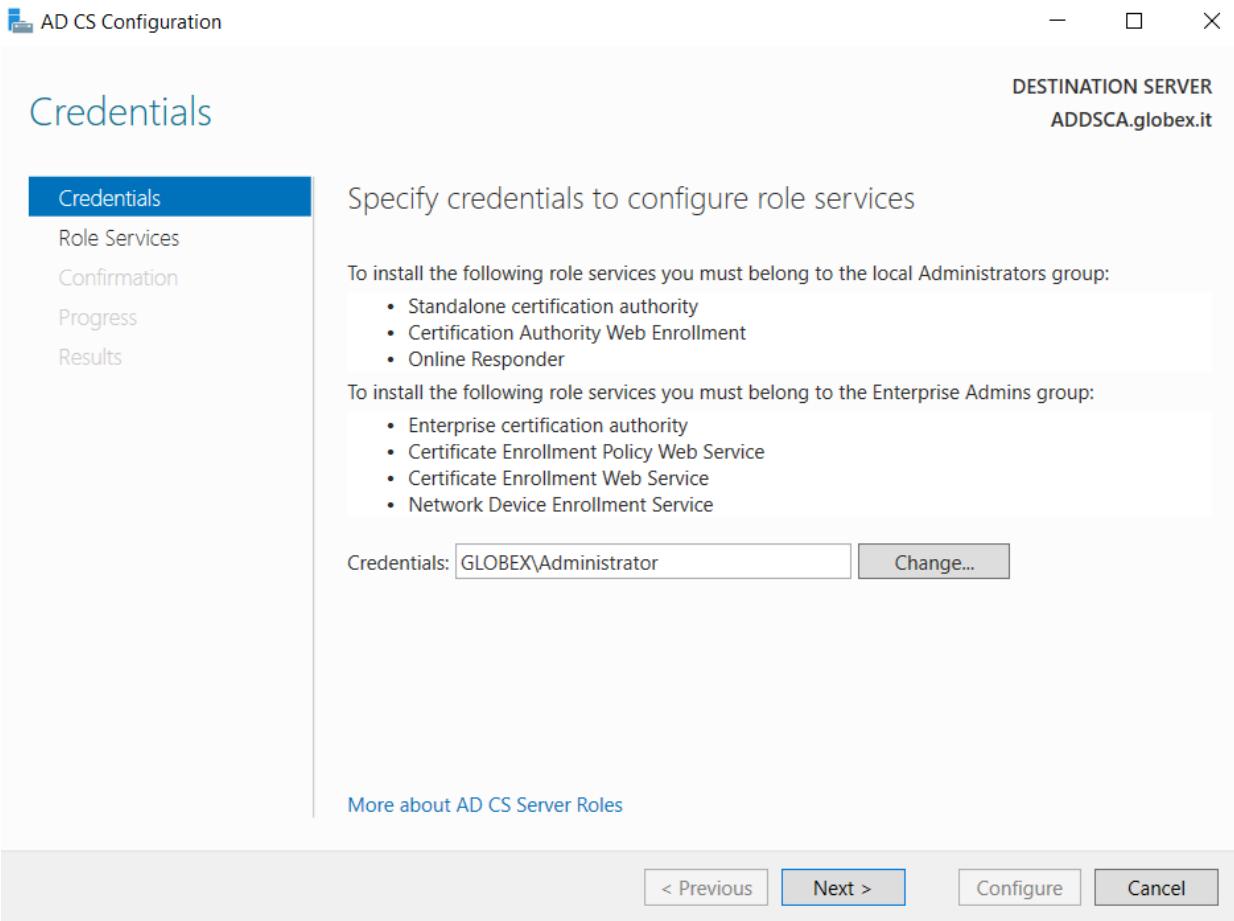
VPN PORTS: GRE, 1701,1723,500,443,47,4500

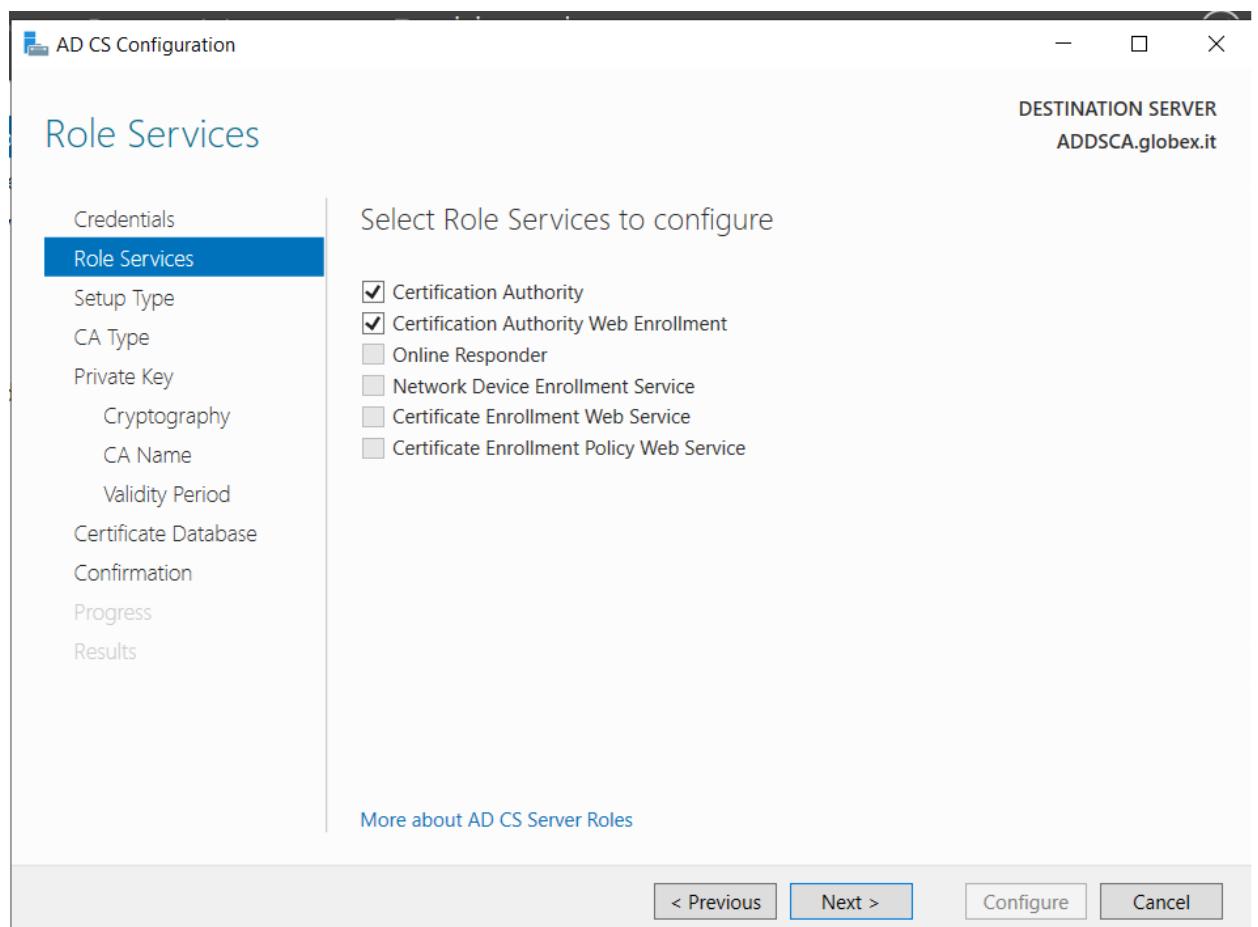
Name	Group	Profile	Enabled	Action
DA_PORTS		All	Yes	Allow
GRE_PORT		All	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
AllJoyn Router (TCP-In)	AllJoyn Router	Domain	Yes	Allow
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retrieval	All	No	Allow
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discover	All	No	Allow
Cast to Device functionality (oWave-TCP-In)	Cast to Device functionality	Private	Yes	Allow
Cast to Device functionality (oWave-UDP-In)	Cast to Device functionality	Private	Yes	Allow
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-Str...)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-Str...)	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTSP-Str...)	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (RTCP-Str...)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (RTSP-Str...)	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTSP-Str...)	Cast to Device functionality	Public	Yes	Allow
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow
COM+ Remote Administration (DCOM-In)	COM+ Remote Administration	All	No	Allow
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow

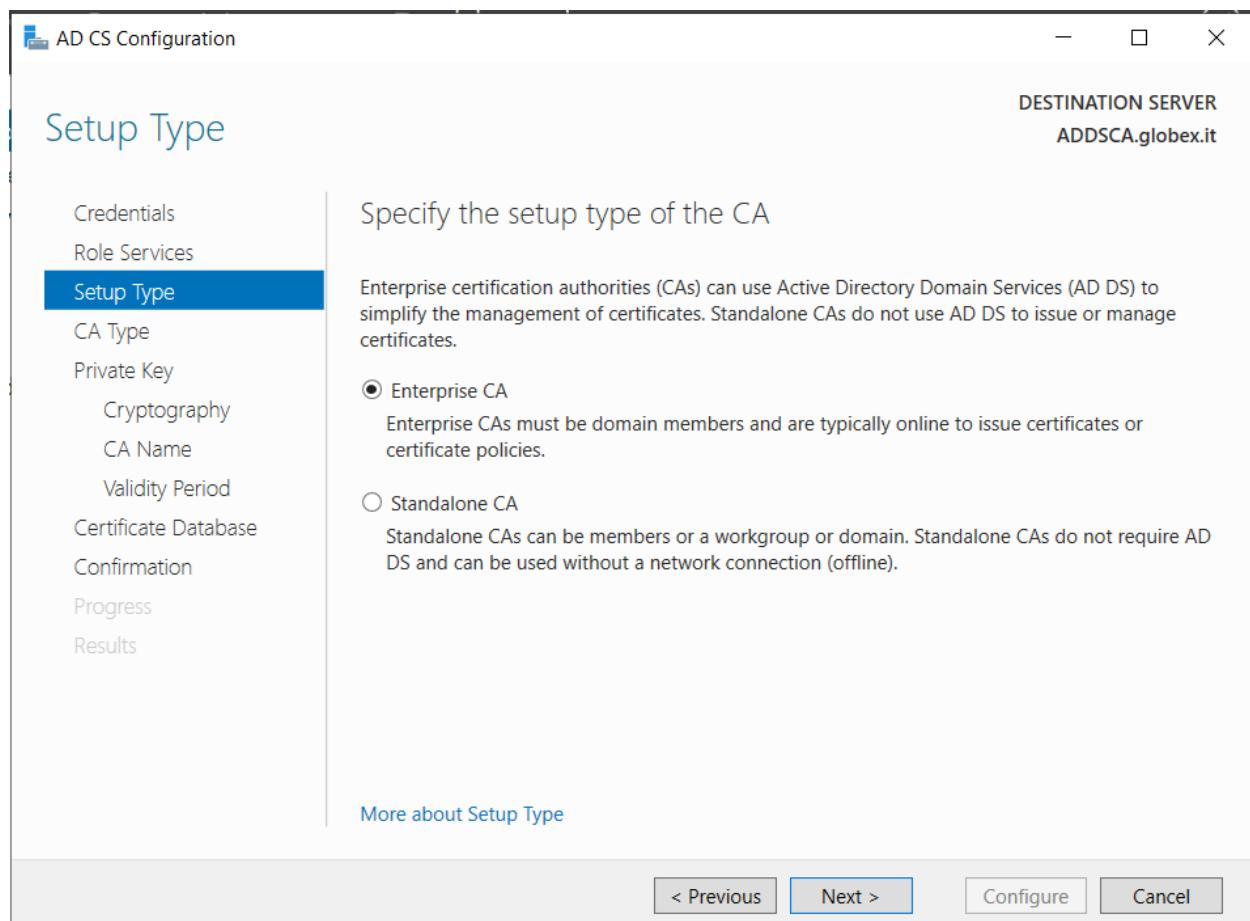
Figure 57 VPN_PORTS

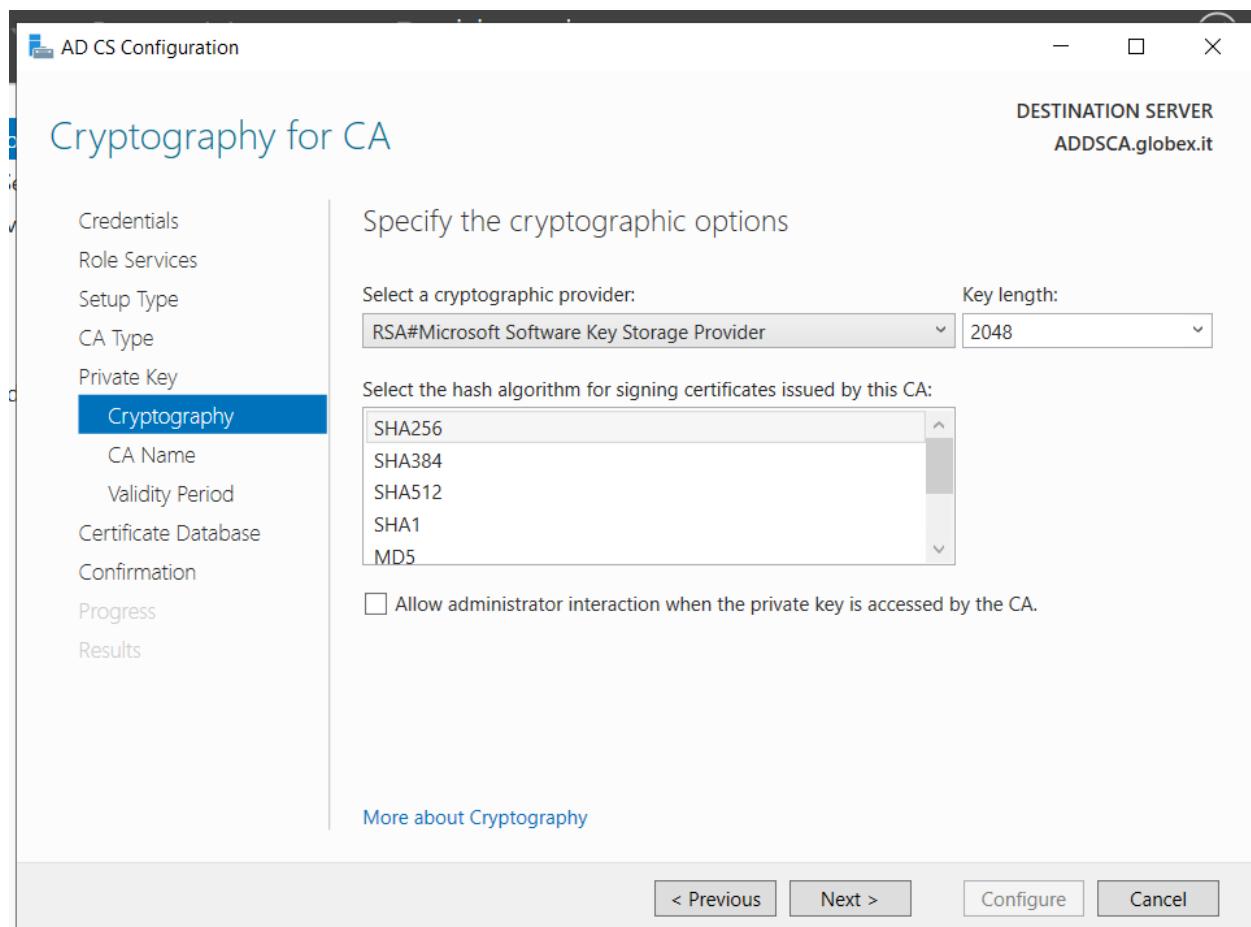
Certificate Authority Configuration:

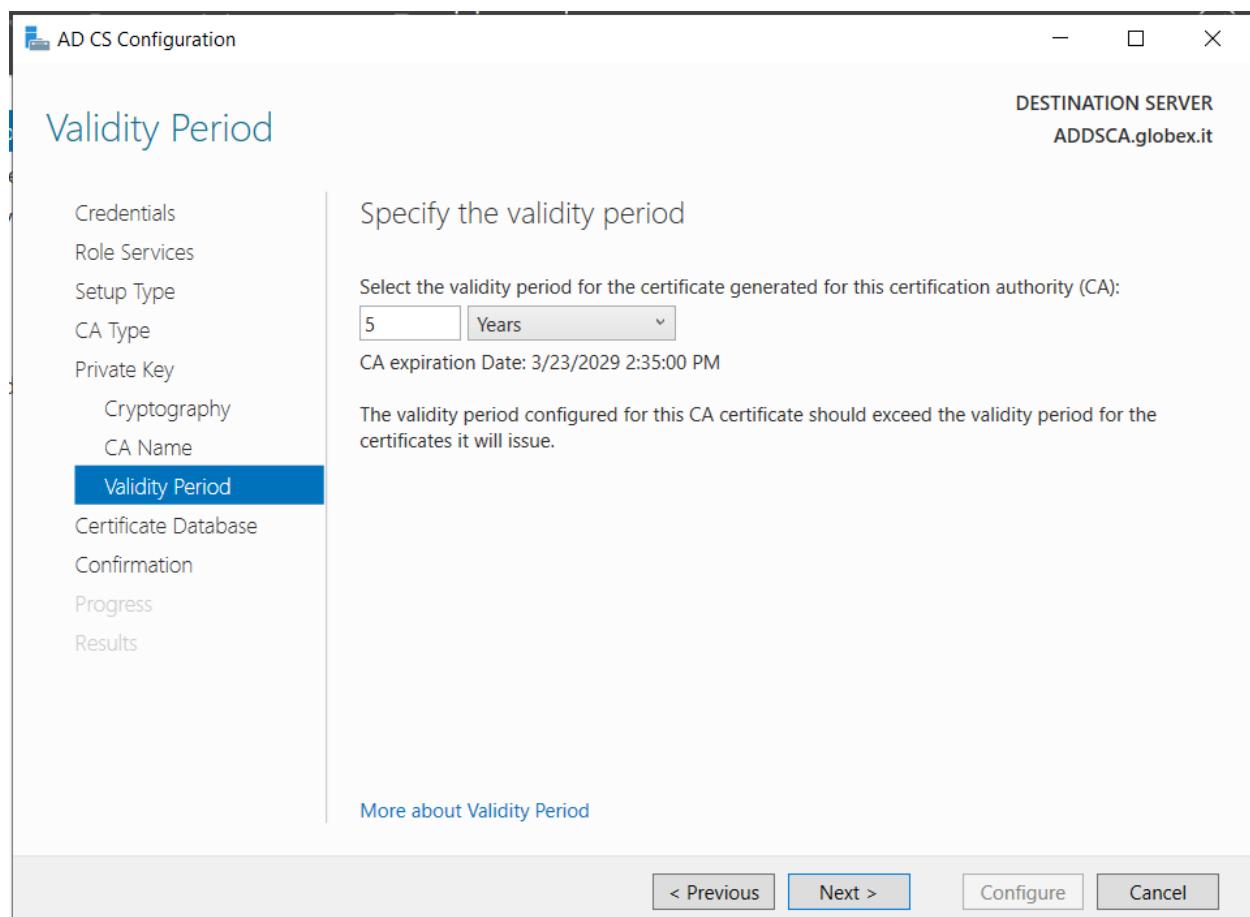


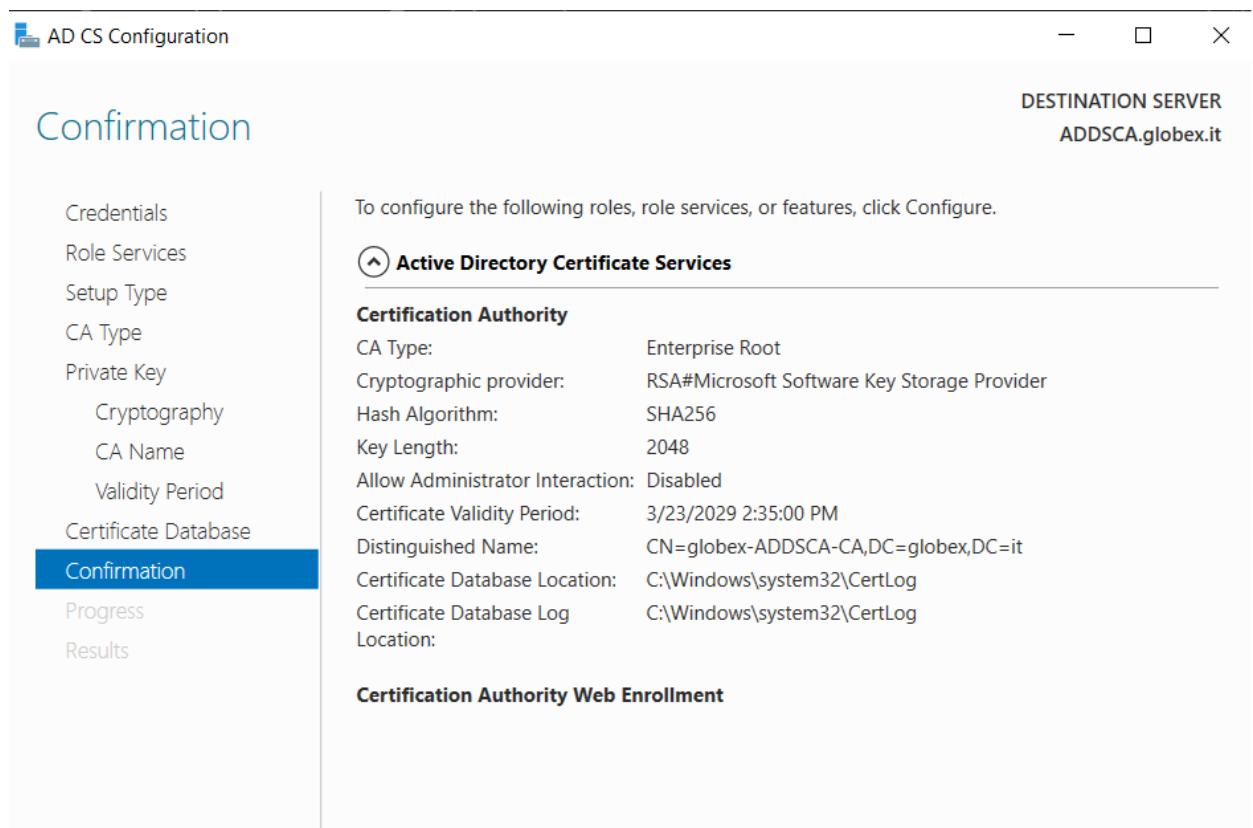












< Previous Next > Configure Cancel

GNS3 VM ADDS&CA

Console3 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Actions
Class 3 Public Primary Certific...	Class 3 Public Primary Certification ...	8/2/2028	Client Authentication...	VeriSign Class 3 Pub...	Normal	Certificates More Actions
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	Microsoft Timestamp...	Normal	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	Client Authentication...	DigiCert	Normal	
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031	Client Authentication...	DigiCert	Normal	
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication...	DigiCert Global Root...	Normal	
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authentication...	DigiCert Global Root...	Normal	
globex-ADDSKA-CA	globex-ADDSKA-CA	3/23/2029	<All>	<None>	Normal	
globex-ADDSKA-CA	globex-ADDSKA-CA	3/23/2029	<All>	<None>	Normal	
Microsoft AuthentICODE(tm) Root...	Microsoft AuthentICODE(tm) Root ...	1/1/2000	Secure Email, Code ...	Microsoft Authenticode...	Normal	
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certif...	2/27/2043	<All>	Microsoft ECC Prod...	Normal	
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS Ro...	Normal	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...	Normal	
Microsoft Root Certificate Author...	Microsoft Root Certificate Authority	5/10/2021	<All>	Microsoft Root Certi...	Normal	
Microsoft Root Certificate Author...	Microsoft Root Certificate Authorit...	6/24/2035	<All>	Microsoft Root Certi...	Normal	
Microsoft Root Certificate Author...	Microsoft Root Certificate Authorit...	3/23/2036	<All>	Microsoft Root Certi...	Normal	
NO LIABILITY ACCEPTED, (c)97 Veri...	NO LIABILITY ACCEPTED, (c)97 VeriS...	1/8/2004	Time Stamping	VeriSign Time Stam...	Normal	
Symantec Enterprise Mobile Root f...	Symantec Enterprise Mobile Root f...	3/15/2032	Code Signing	<None>	Normal	
Thawte Timestamping CA	Thawte Timestamping CA	1/1/2021	Time Stamping	Thawte Timestampi...	Normal	

Trusted Root Certification Authorities store contains 18 certificates.

Steps for creating Custom Certificate:

The screenshot shows two windows of the Microsoft Management Console (MMC) running under the title "GNS3 VM ADDS&CA". Both windows are titled "Console3 - [Console Root]Certificates - Current User\Personal\Certificates".

Top Window (Step 1): Select Certificate Enrollment Policy

This window displays a list of certificate enrollment policies. The "Custom Request" option is selected and highlighted in blue.

- Configured by your administrator: Active Directory Enrollment Policy
- Configured by you: **Custom Request**
- Proceed without enrollment policy

Buttons at the bottom: Next, Cancel, >

Bottom Window (Step 2): Custom request

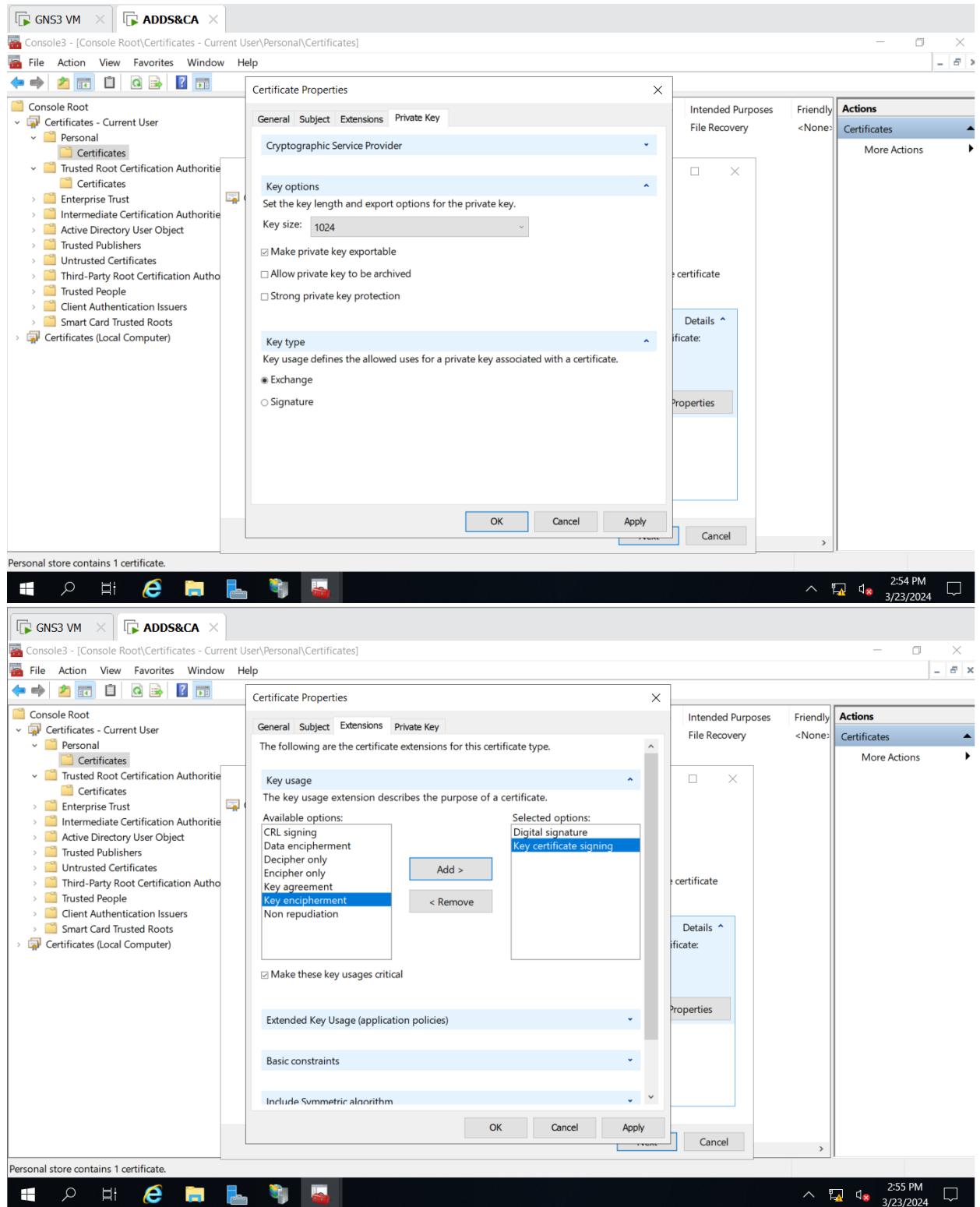
This window shows the configuration for a custom certificate request.

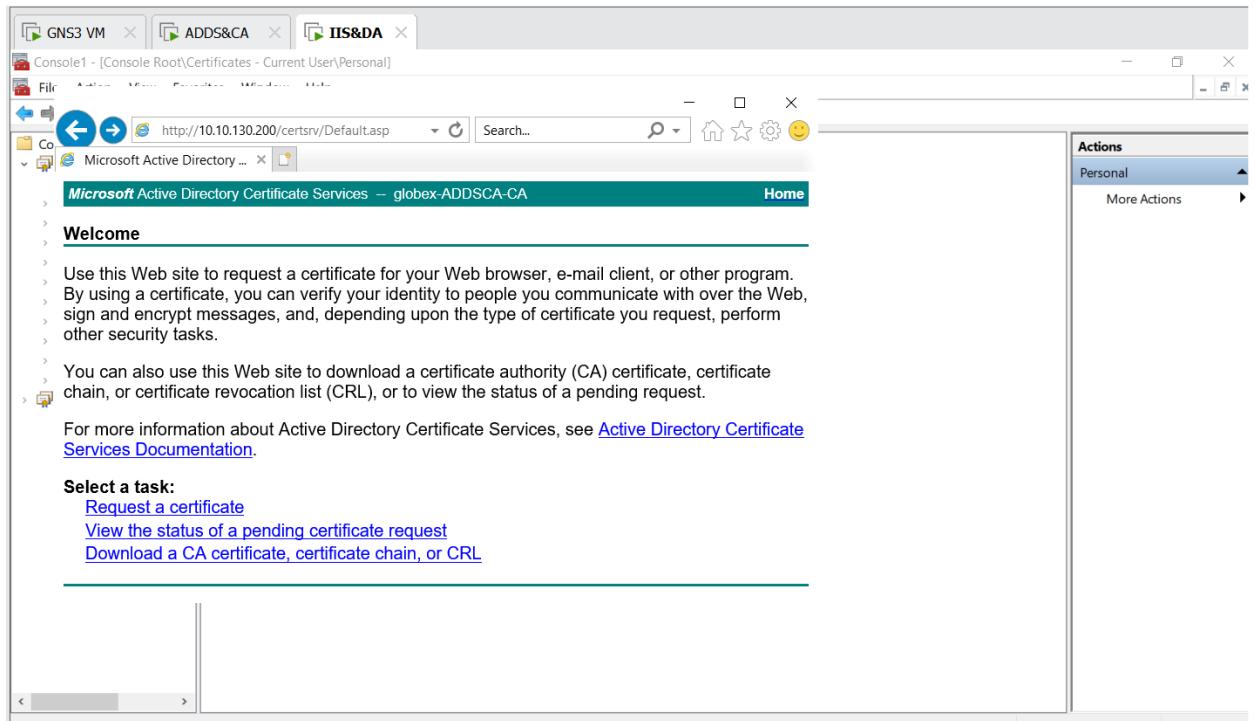
- Template: (No template) Legacy key
- Request format: PKCS #10
 CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

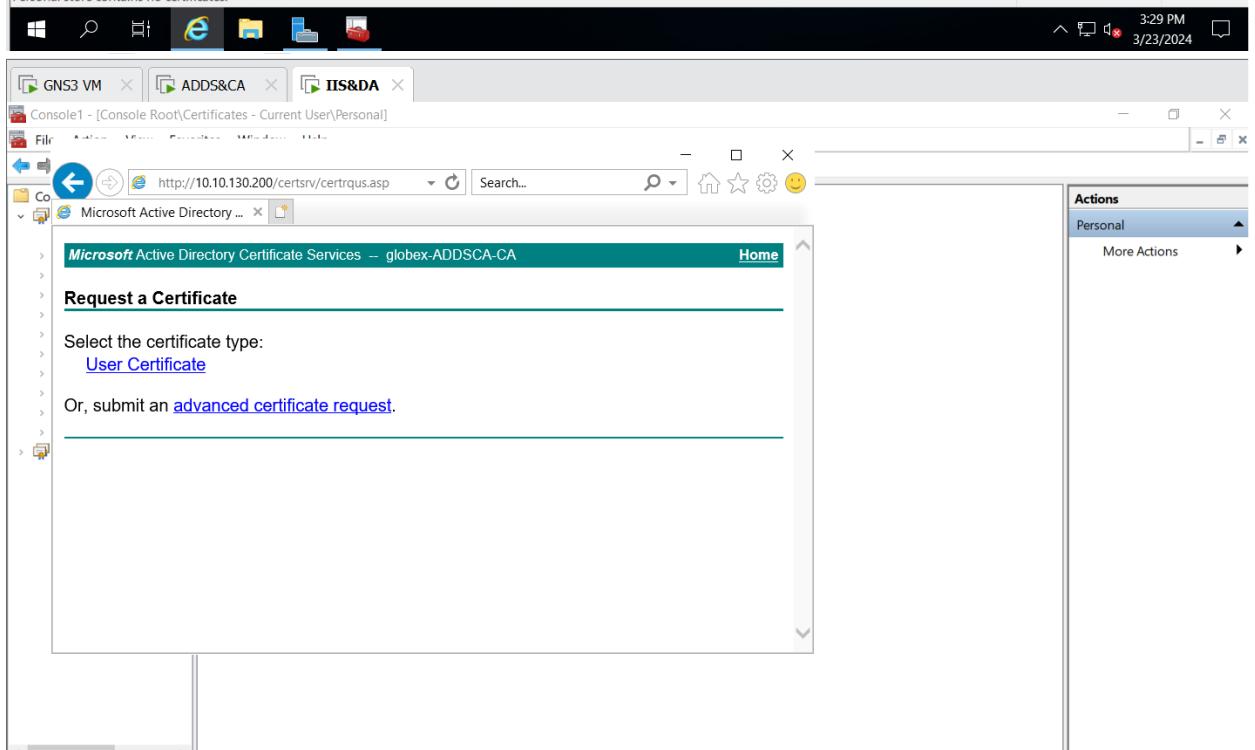
Buttons at the bottom: Next, Cancel, >

At the very bottom of the interface, it says "Personal store contains 1 certificate." and shows the Windows taskbar with the date and time as 2:53 PM 3/23/2024.





The screenshot shows the Microsoft Active Directory Certificate Services Home page. The URL is <http://10.10.130.200/certsrv/Default.asp>. The page title is "Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA". The main content area is titled "Welcome" and contains instructions for requesting certificates. It mentions using the site to request a certificate for a Web browser, e-mail client, or other program, and performing other security tasks. It also notes that you can download a CA certificate, certificate chain, or CRL. A link to "Active Directory Certificate Services Documentation" is provided. Below this, a section titled "Select a task:" lists three options: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL". At the bottom left, it says "Personal store contains no certificates." The system tray at the bottom right shows the date and time as 3/23/2024 3:29 PM.



The screenshot shows the "Request a Certificate" page of Microsoft Active Directory Certificate Services. The URL is <http://10.10.130.200/certsrv/certqus.asp>. The page title is "Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA". The main content area is titled "Request a Certificate" and asks to "Select the certificate type:". It provides a link to "User Certificate". Below this, it says "Or, submit an advanced certificate request." At the bottom left, it says "Personal store contains no certificates." The system tray at the bottom right shows the date and time as 3/23/2024 3:30 PM.

Screenshot of the Microsoft Active Directory Certificate Services interface showing the "Advanced Certificate Request" page.

The title bar shows "Microsoft Active Directory Certificate Services -- globex-ADDS-CA".

The main content area displays the following text:

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

Below this, a message states: "Personal store contains no certificates."

At the bottom right of the window, there is a status bar showing "3:30 PM 3/23/2024".

Screenshot of the Microsoft Active Directory Certificate Services interface showing the "Submit a Certificate Request or Renewal Request" page.

The title bar shows "Microsoft Active Directory Certificate Services -- globex-ADDS-CA".

The main content area displays the following text:

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

```
DgQWBSc67z0E+KPLhkTuz3lQETtvObW4DANBgkqj
gf+43Yb+LmI93II/AS3XbVPRU+fn8aAbZ6G8pd8
aW4BHt4aTC1I4nkKk1DWwlyQZmrB8YAdkIlRMYL
u4ey26/D/DS2ckujV9iv15eiywgrdoelRp6w==
----END NEW CERTIFICATE REQUEST----
```

Certificate Template: Web Server

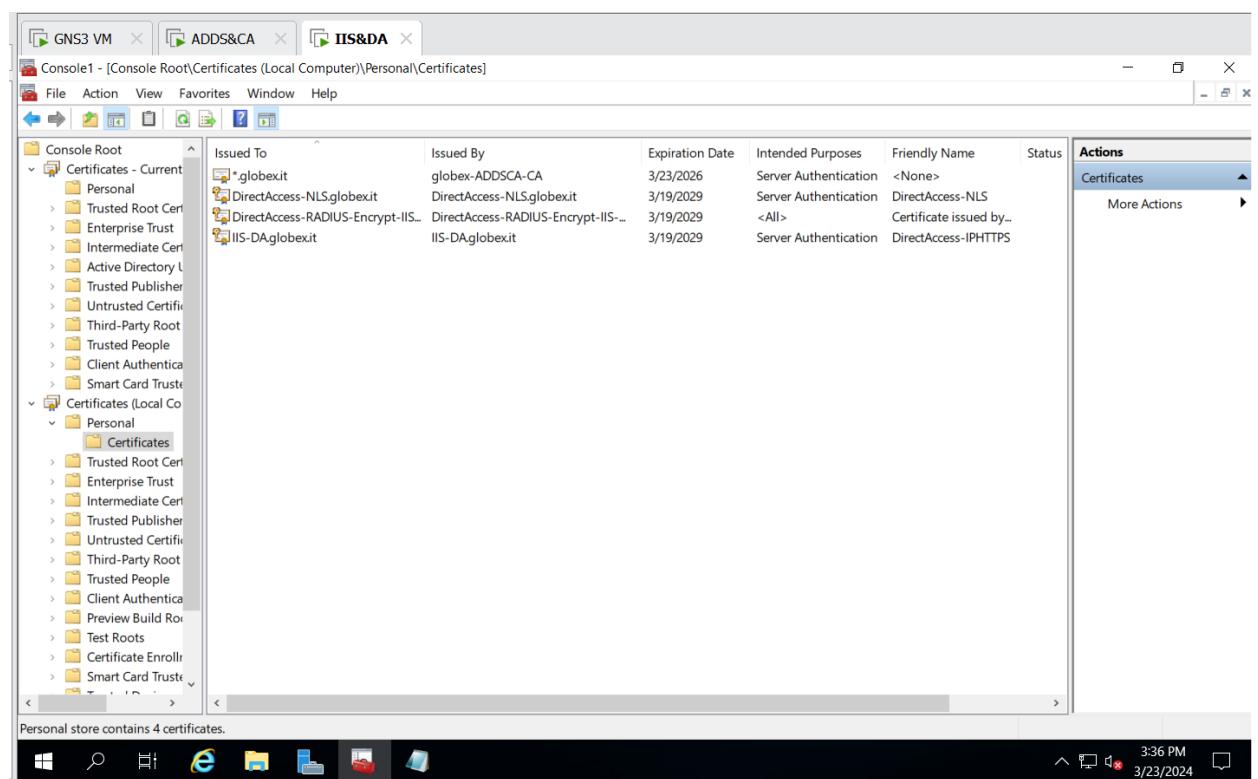
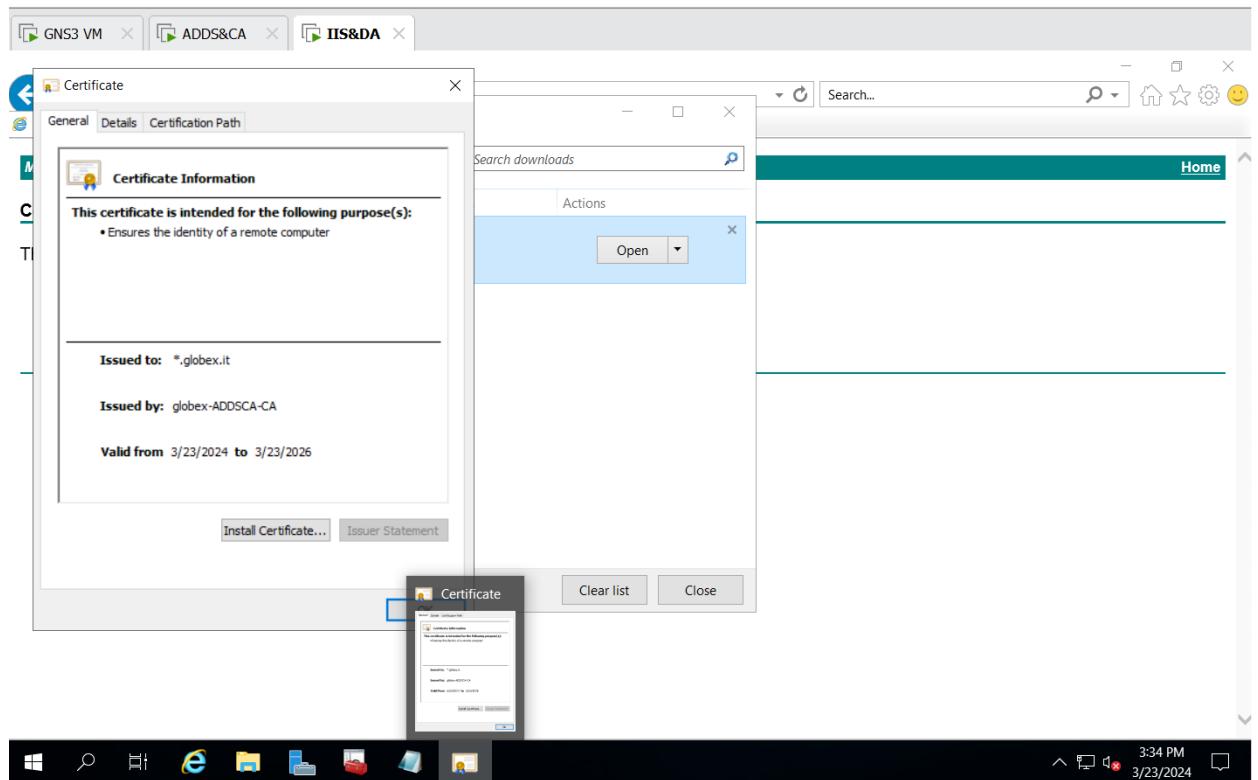
Additional Attributes:

Attributes: (empty dropdown menu)

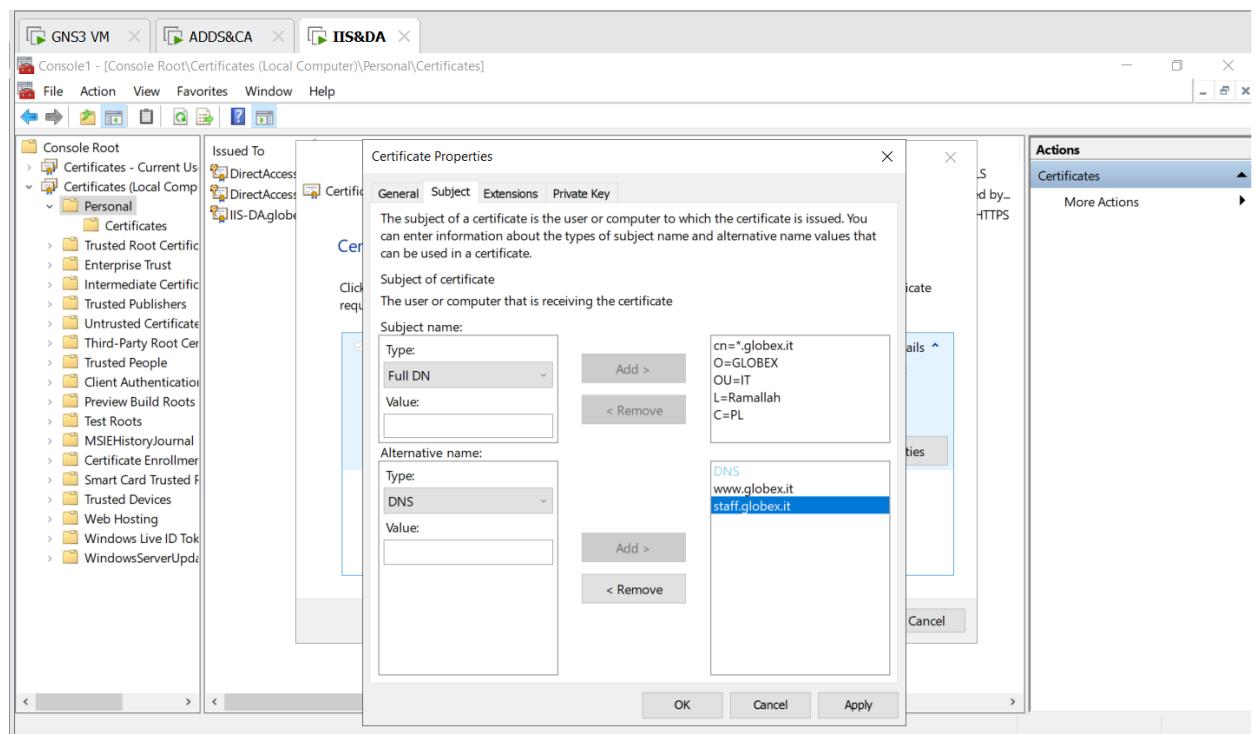
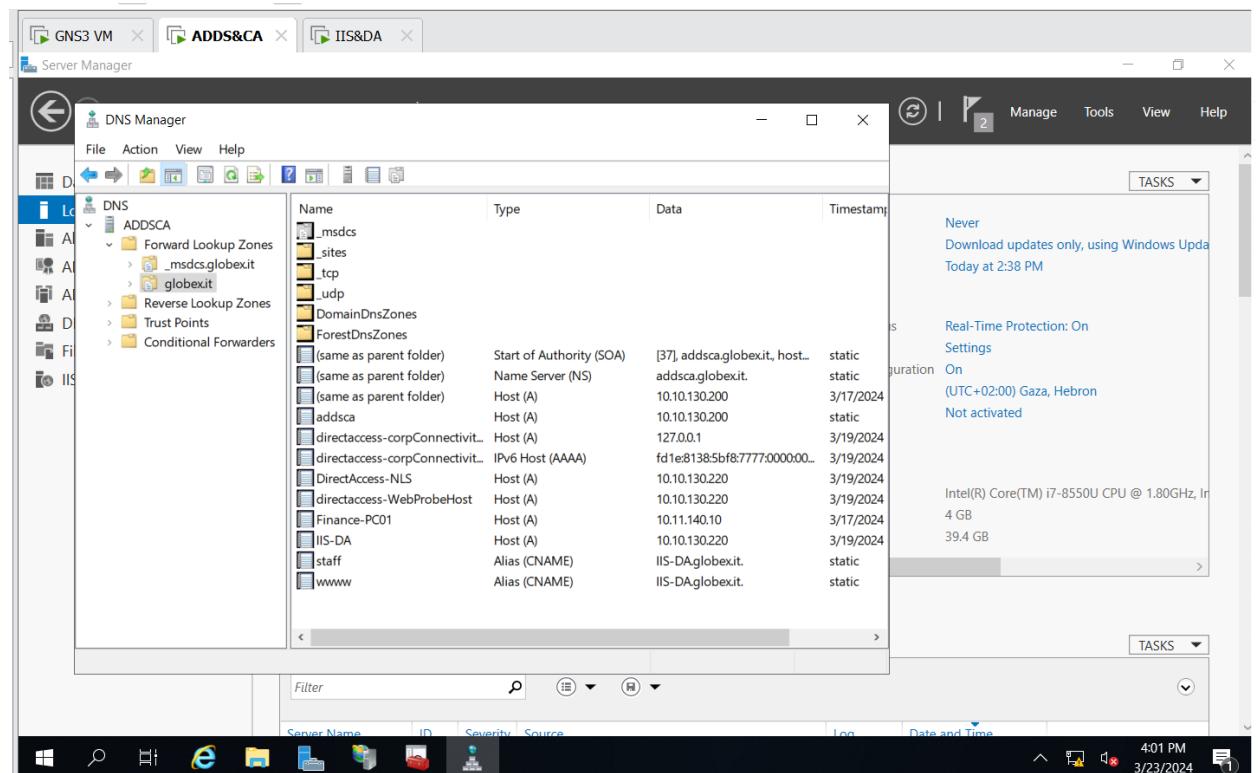
Submit >

At the bottom right of the window, there is a status bar showing "3:31 PM 3/23/2024".

The screenshot shows a Microsoft Edge browser window with three tabs open: GNS3 VM, ADDS&CA, and IIS&DA. The current tab displays the Microsoft Active Directory Certificate Services page at <http://10.10.130.200/certsrv/certfnsh.asp>. The page title is "Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA". A section titled "Certificate Issued" states, "The certificate you requested was issued to you." It includes options for "DER encoded" (selected) or "Base 64 encoded" and links to "Download certificate" and "Download certificate chain". Below this, a download dialog from Internet Explorer is visible, titled "View Downloads - Internet Explorer". The dialog lists a single file: "cer....cer" (1.24 KB) located in "Downloads" with the URL "10.10.130.200". The "Open" button is highlighted.

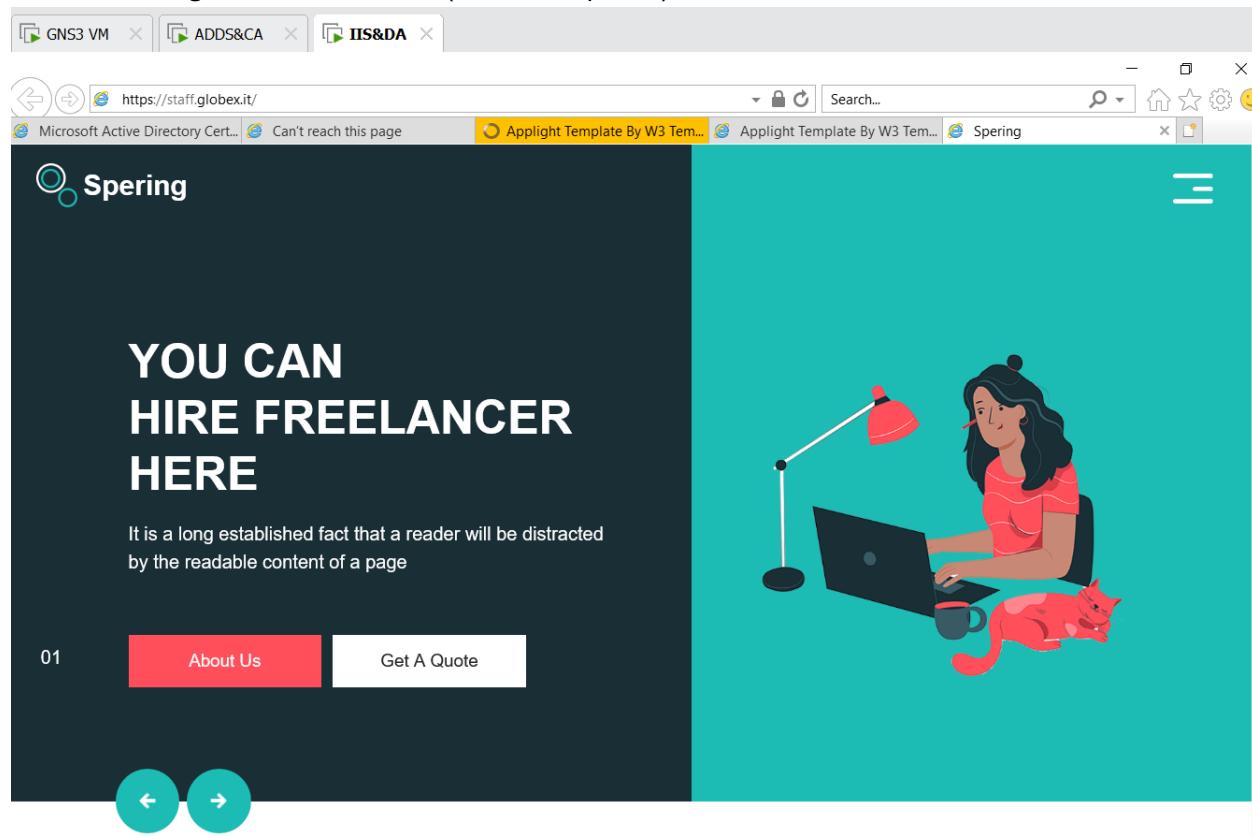


Creating DNS records for the websites

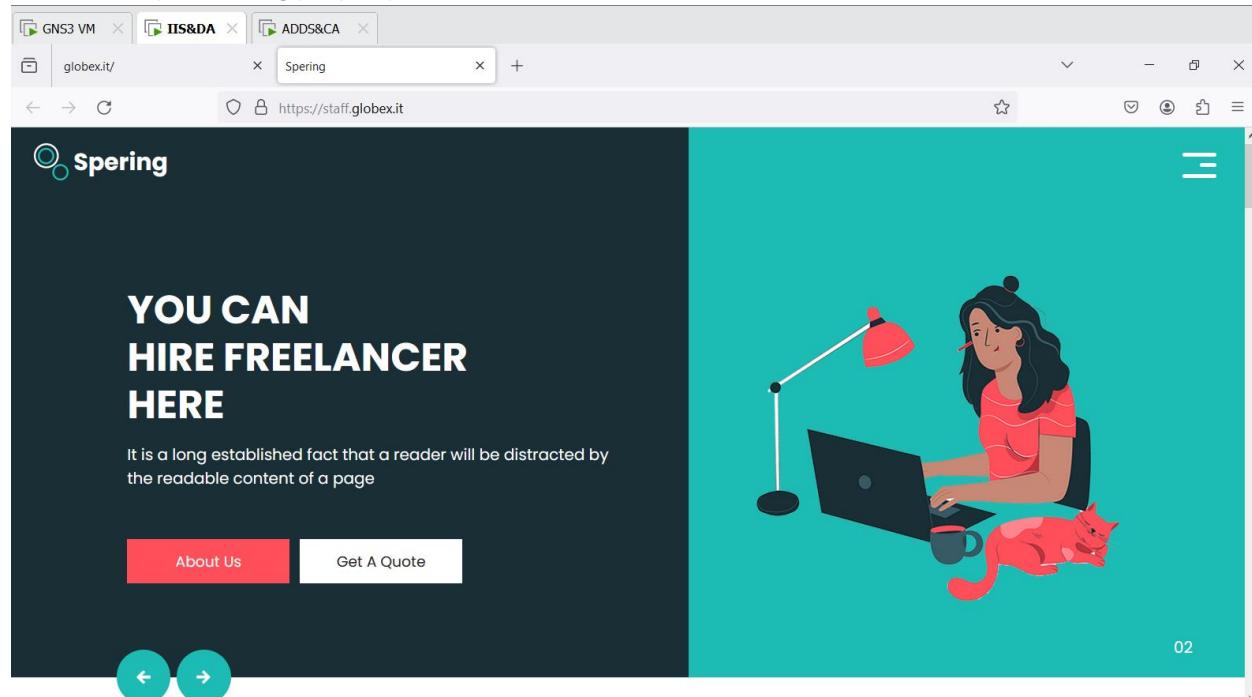


<https://staff.globex.it>

Websites using HTTPS certificates (internet explorer).

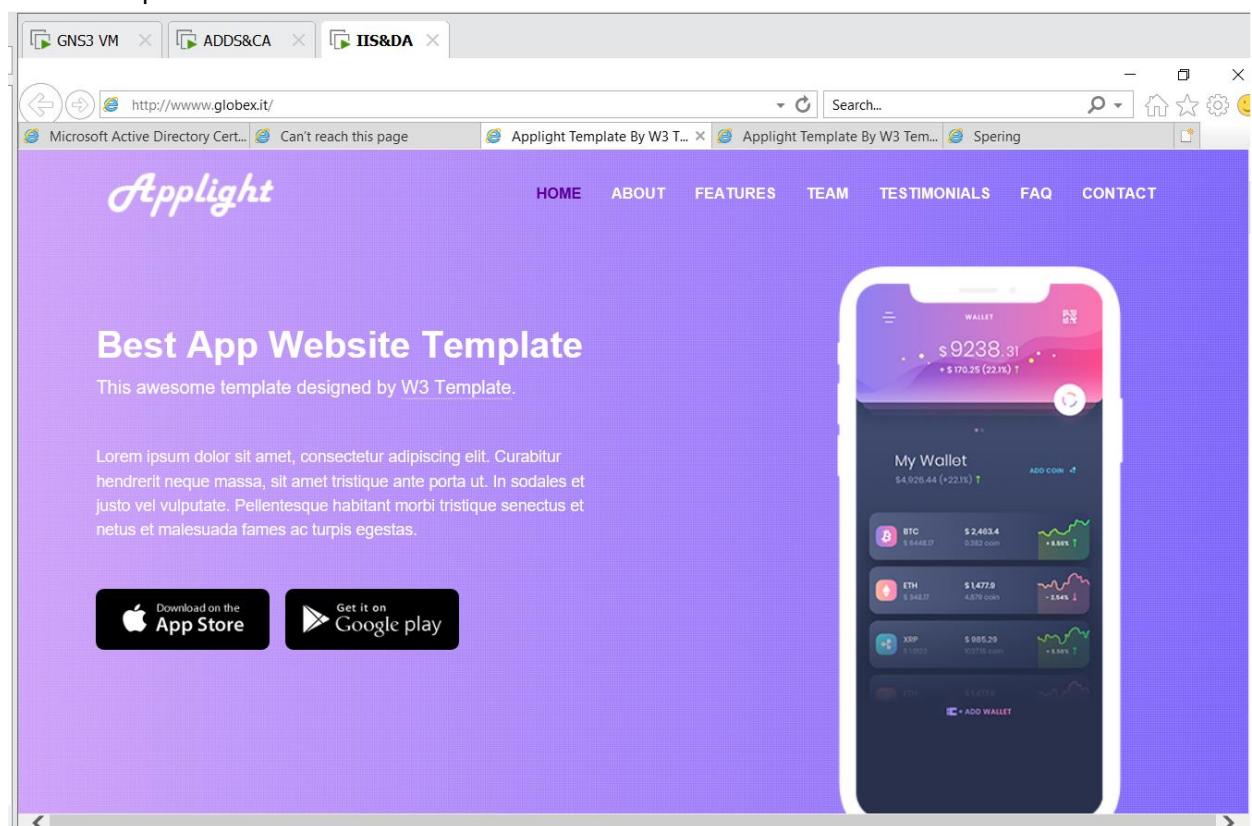


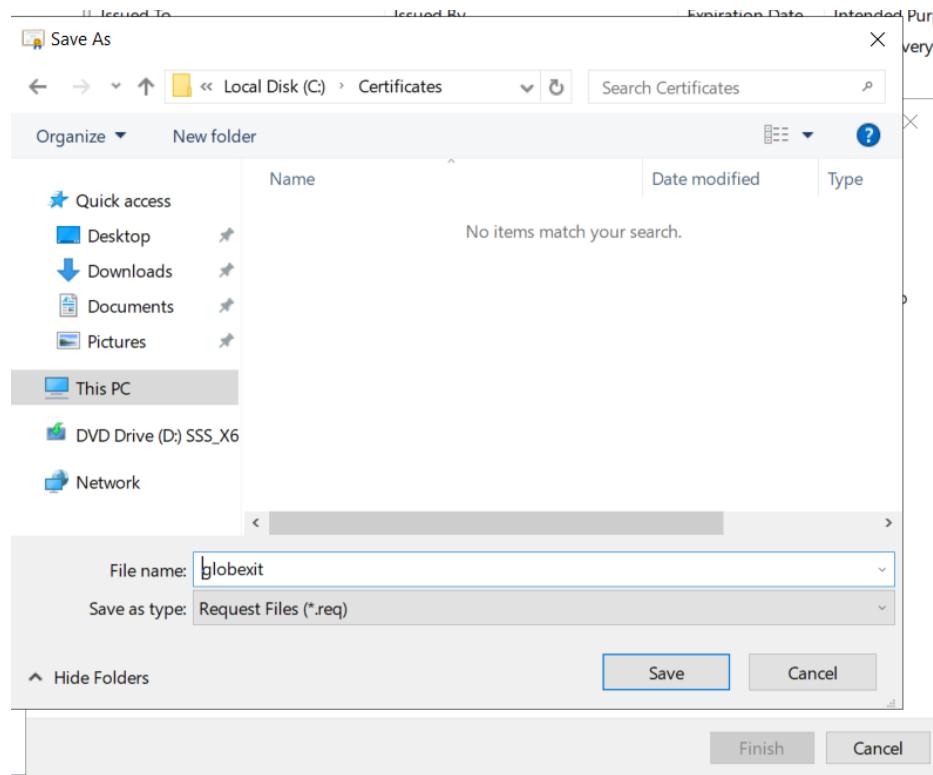
Website https working properly on Firefox.



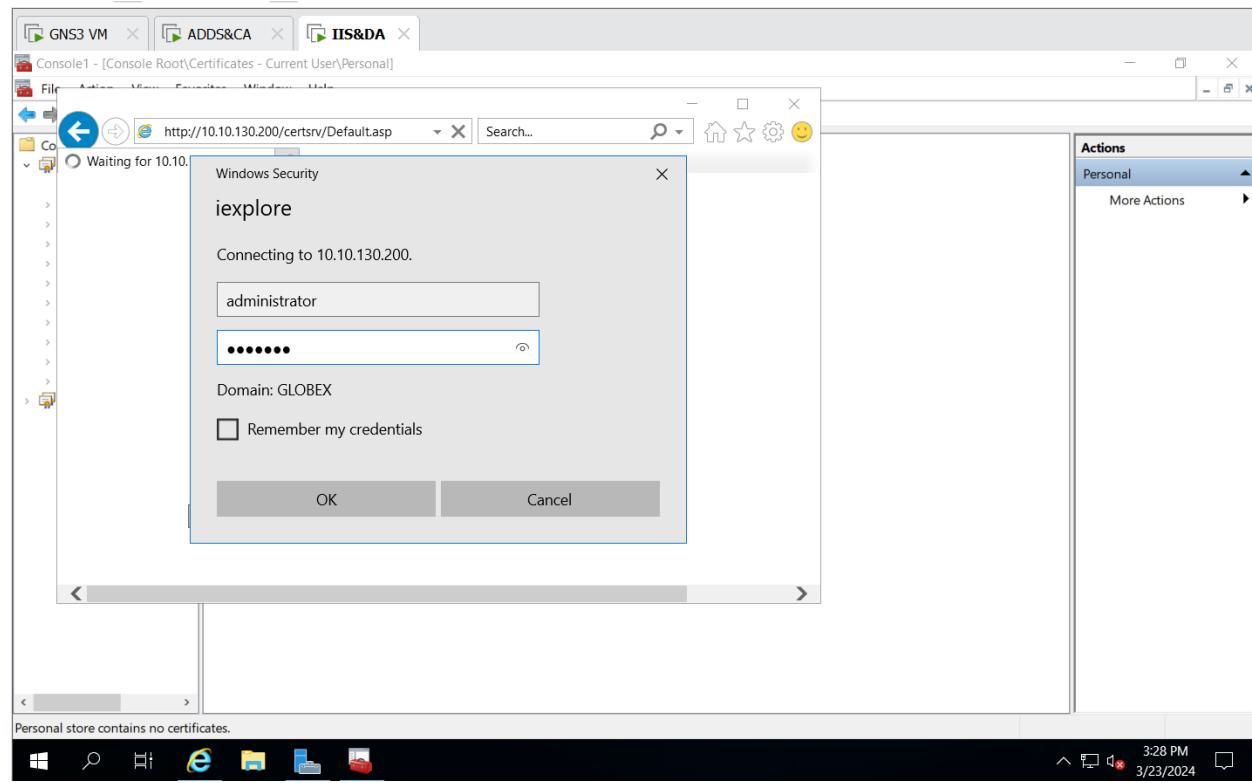
<https://www.globex.it>

1. Internet explorer



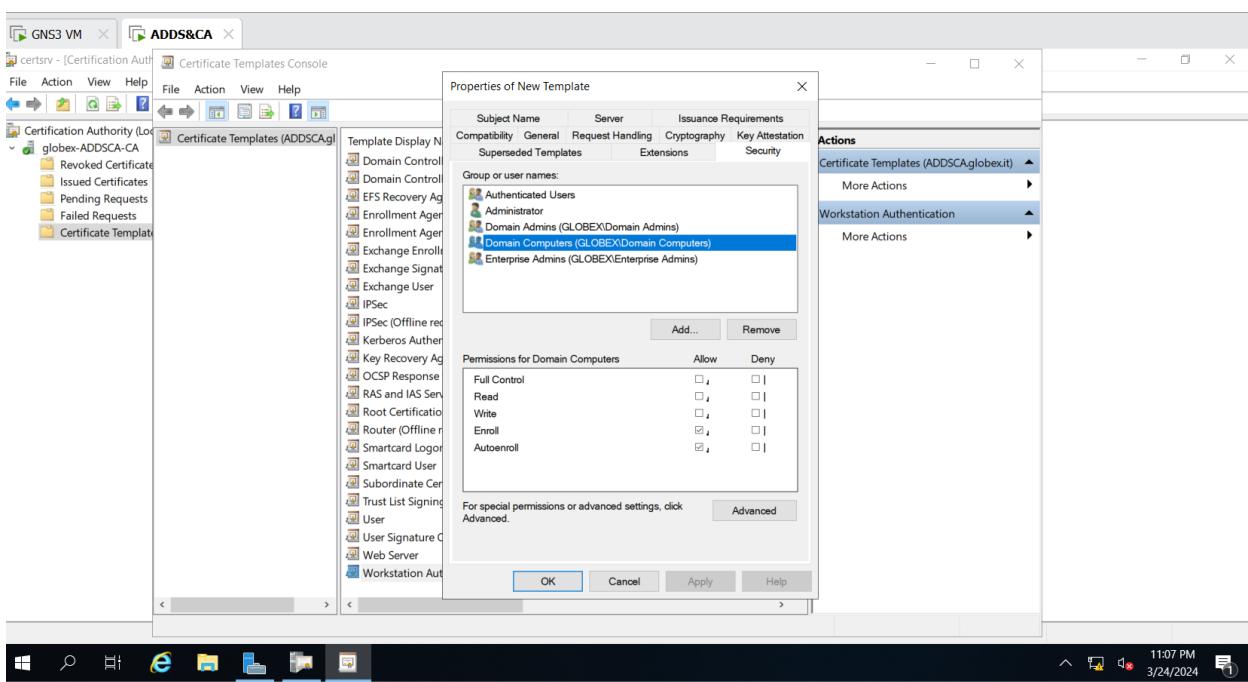
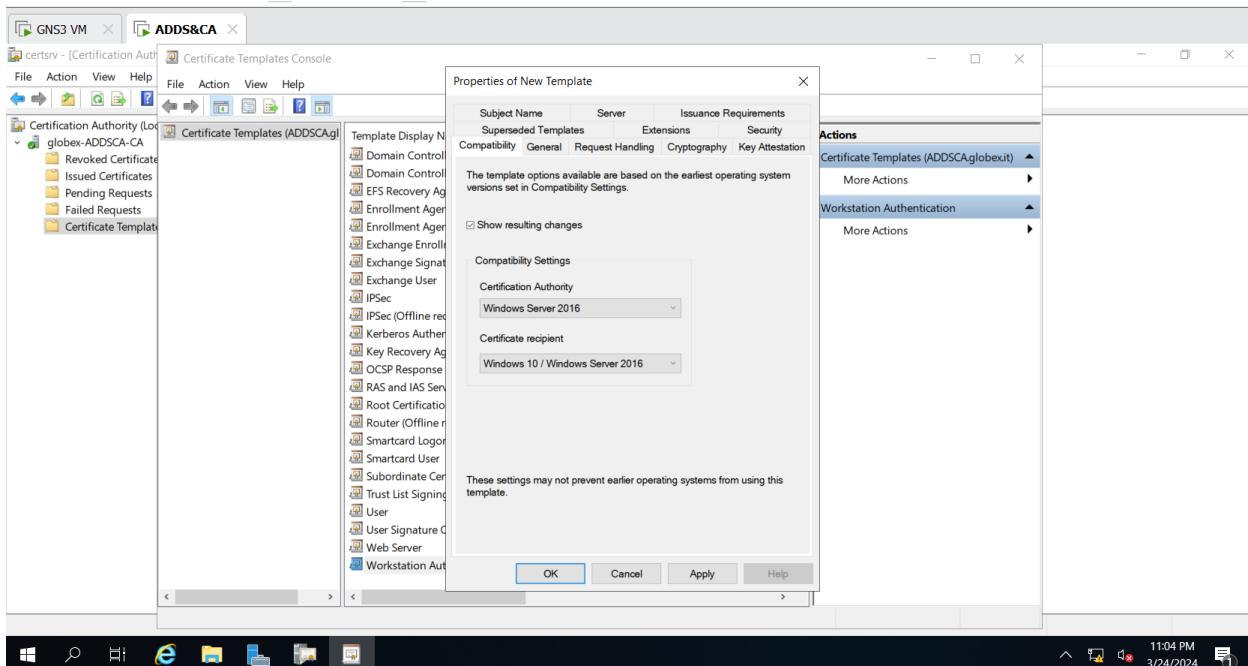


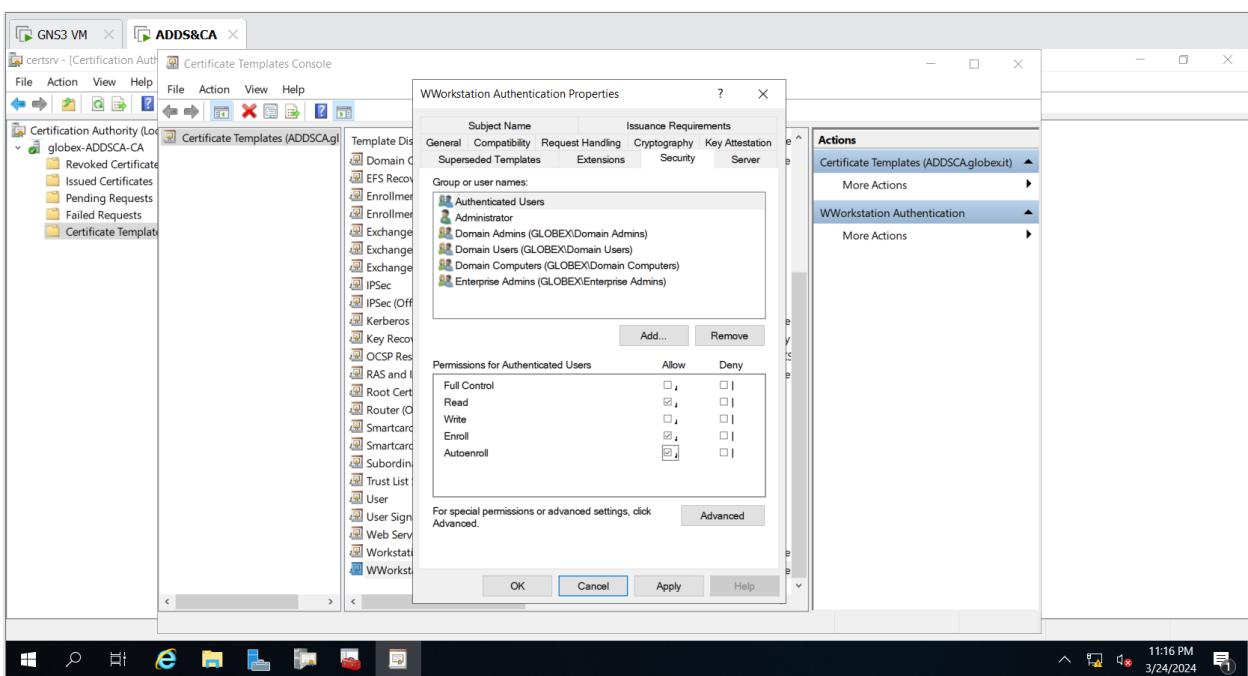
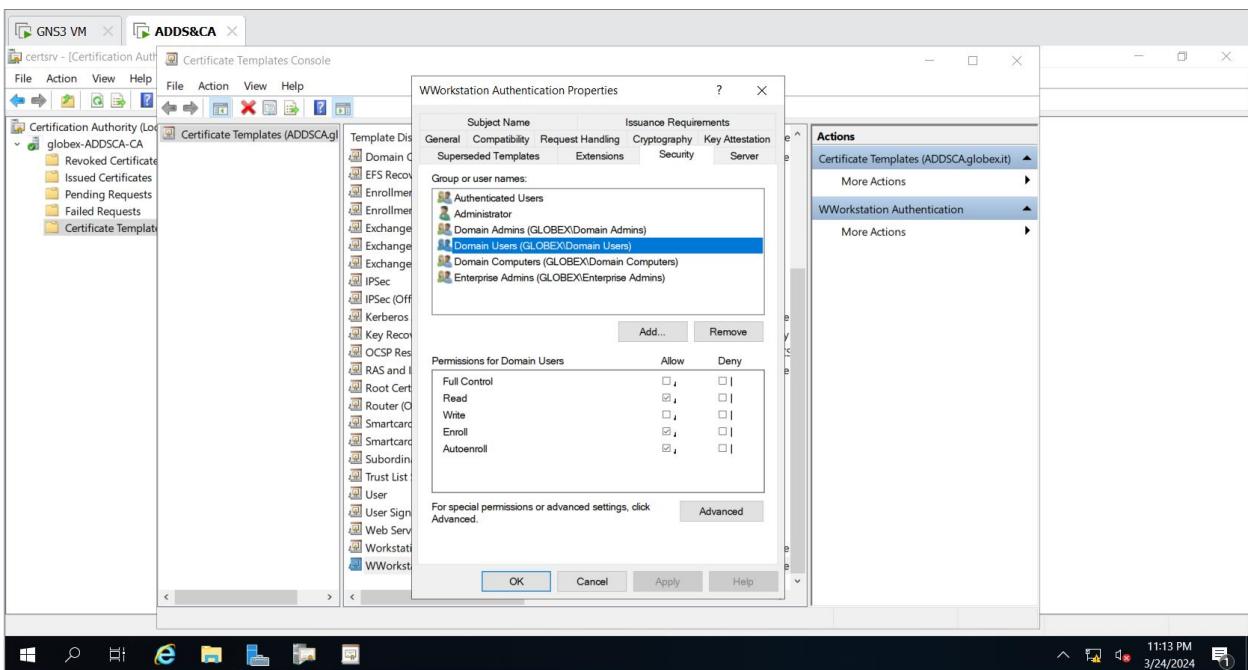
Open certificate Authority from IIS using

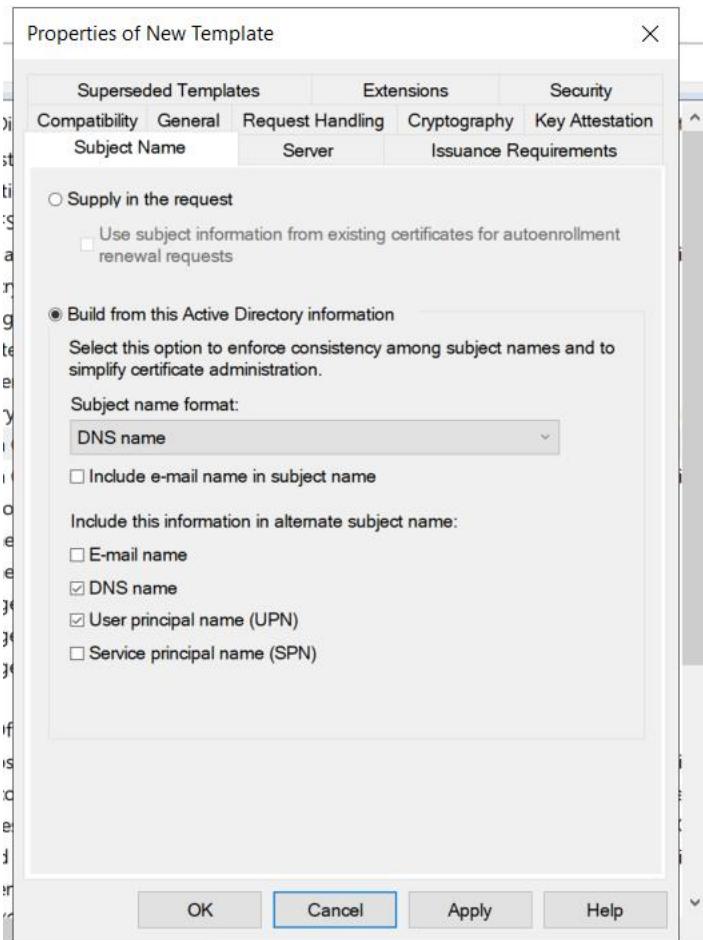


Workstation Communication CA

- We added another certificate from CA by duplicating the Workstation certificate and modifying the settings like in the pictures (compatibility settings, security settings enrolment, and DNS settings) , then we issue a certificate using Microsoft management console MMC. The steps also apply for Domain Controller certificates.





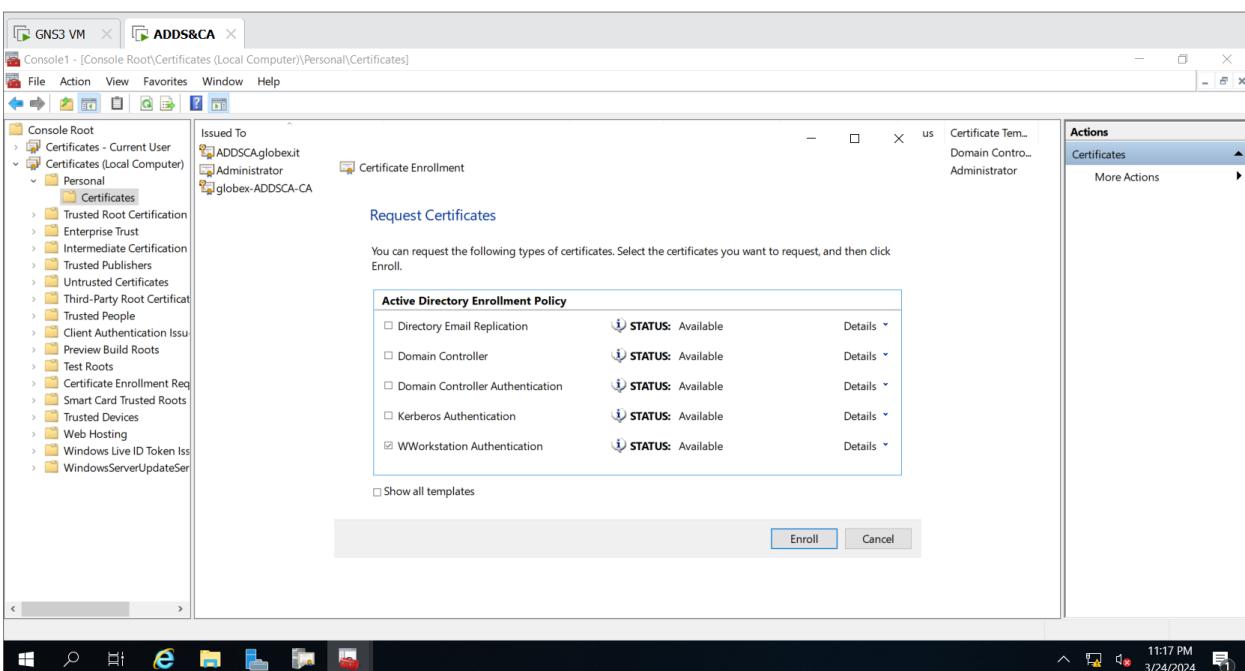
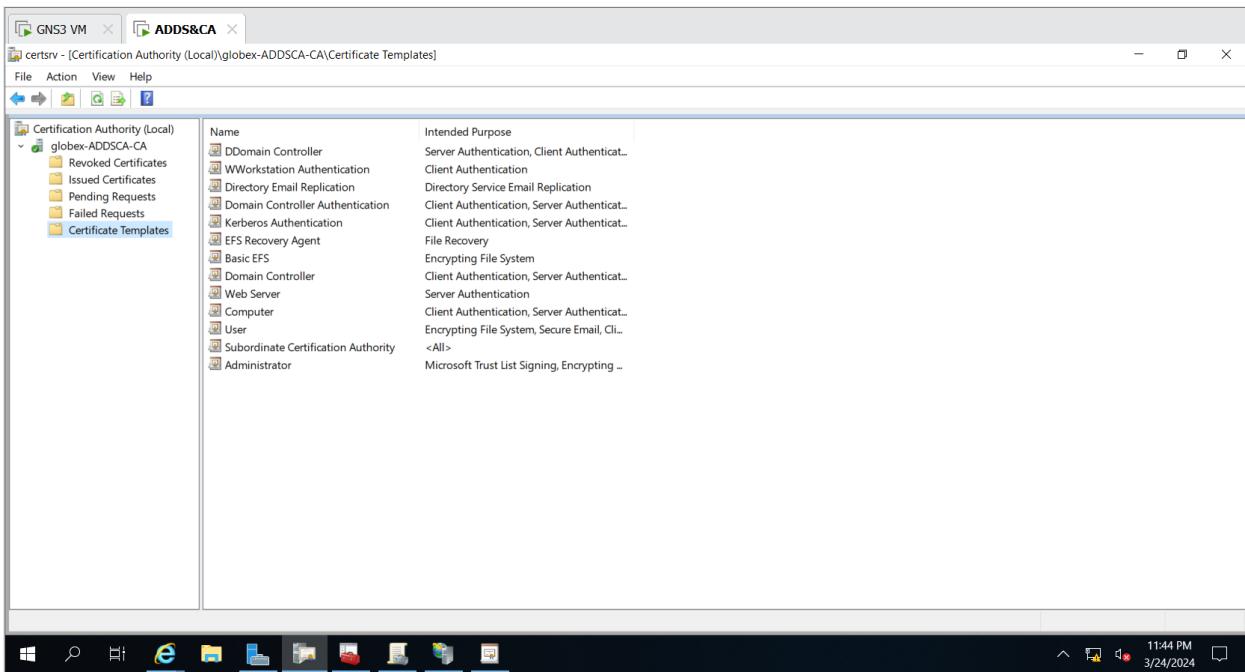


GNS3 VM ADDS&CA

certsrv - [Certification Authority (Local)\globex-ADDS-CA](Certificate Templates)

File Action View Help

Name	Intended Purpose
WWorkstation Authentication	Client Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticat...
Kerberos Authentication	Client Authentication, Server Authenticat...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authenticat...
Web Server	Server Authentication
Computer	Client Authentication, Server Authenticat...
User	Encrypting File System, Secure Email, Cli...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...



GNS3 VM ADDS&CA

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

File Action View Favorites Window Help

Issued To Issued By Expiration Date Intended Purposes Friendly Name Status Certificate Tem... Actions

ADDSCAglobexit	globex-ADDS-CA	3/23/2025	Client Authentication	<None>		Domain Contro...	Certificates
ADDSCAglobexit	globex-ADDS-CA	3/24/2025	Client Authentication	<None>		WWorkstation ...	
Administrator	globex-ADDS-CA	3/23/2025	Microsoft Trust List	<None>		Administrator	
globex-ADDS-CA	globex-ADDS-CA	3/23/2029	<All>	<None>			

More Actions

11:17 PM 3/24/2024

GNS3 VM ADDS&CA

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

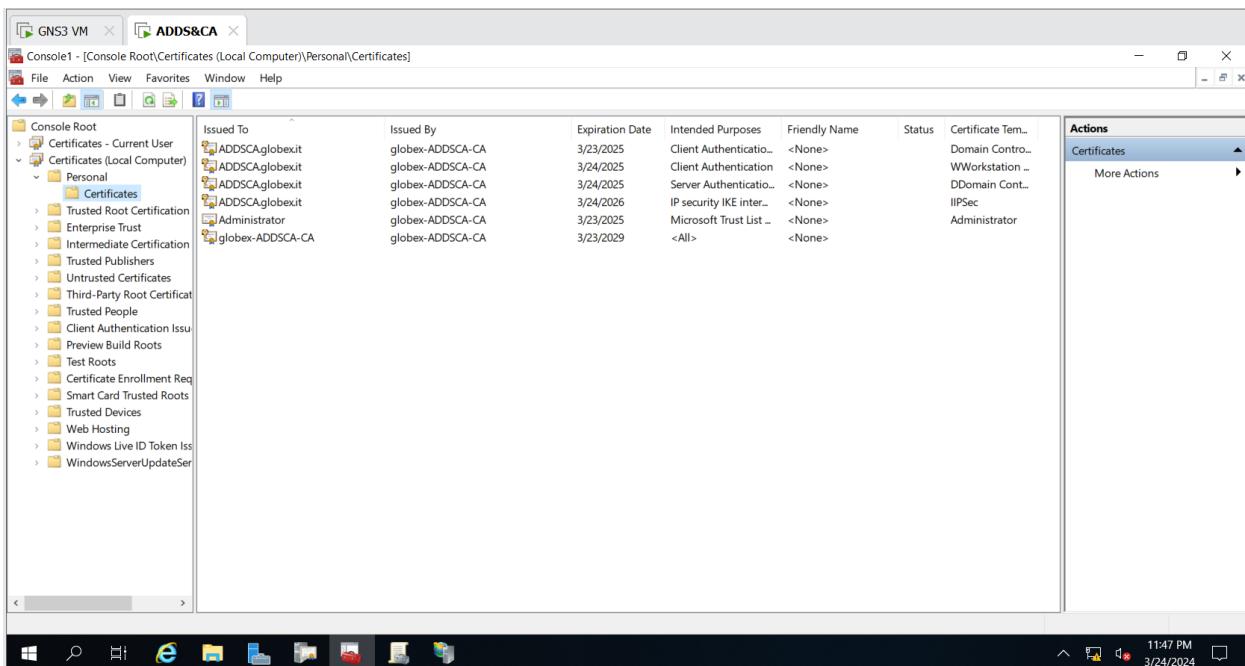
File Action View Favorites Window Help

Issued To Issued By Expiration Date Intended Purposes Friendly Name Status Certificate Tem... Actions

ADDSCAglobexit	globex-ADDS-CA	3/23/2025	Client Authentication	<None>		Domain Contro...	Certificates
ADDSCAglobexit	globex-ADDS-CA	3/24/2025	Client Authentication	<None>		WWorkstation ...	
ADDSCAglobexit	globex-ADDS-CA	3/24/2025	Server Authentication	<None>		DDomain Cont...	
Administrator	globex-ADDS-CA	3/23/2025	Microsoft Trust List	<None>		Administrator	
globex-ADDS-CA	globex-ADDS-CA	3/23/2029	<All>	<None>			

More Actions

11:45 PM 3/24/2024

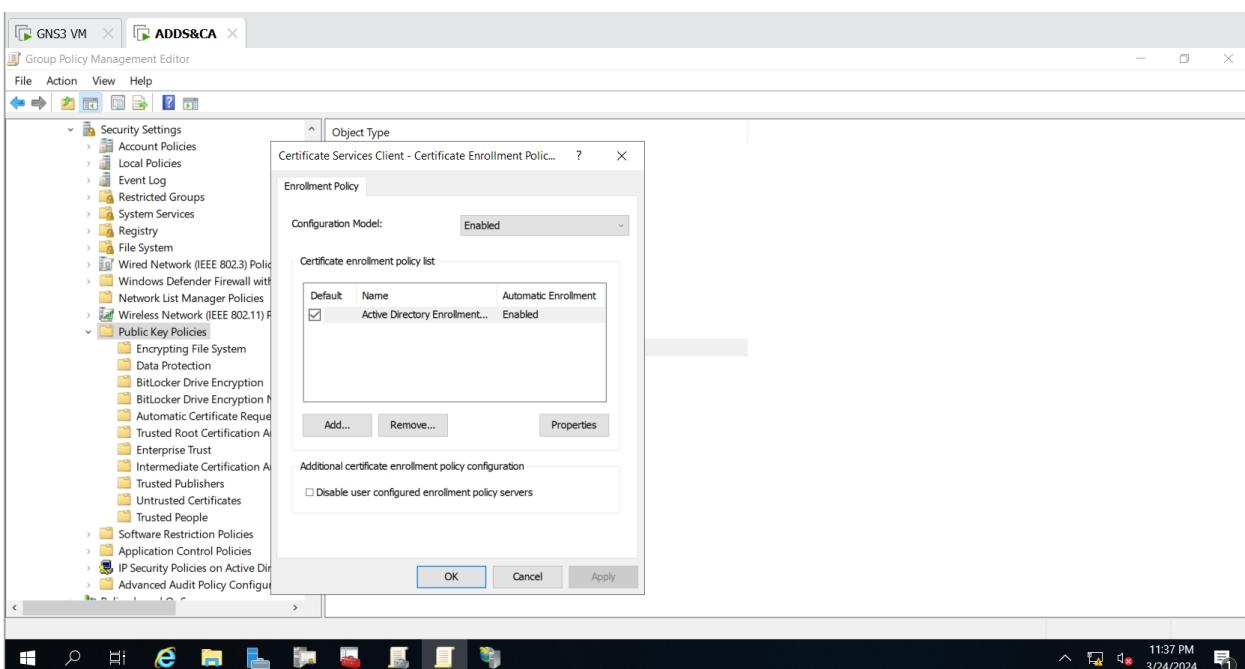
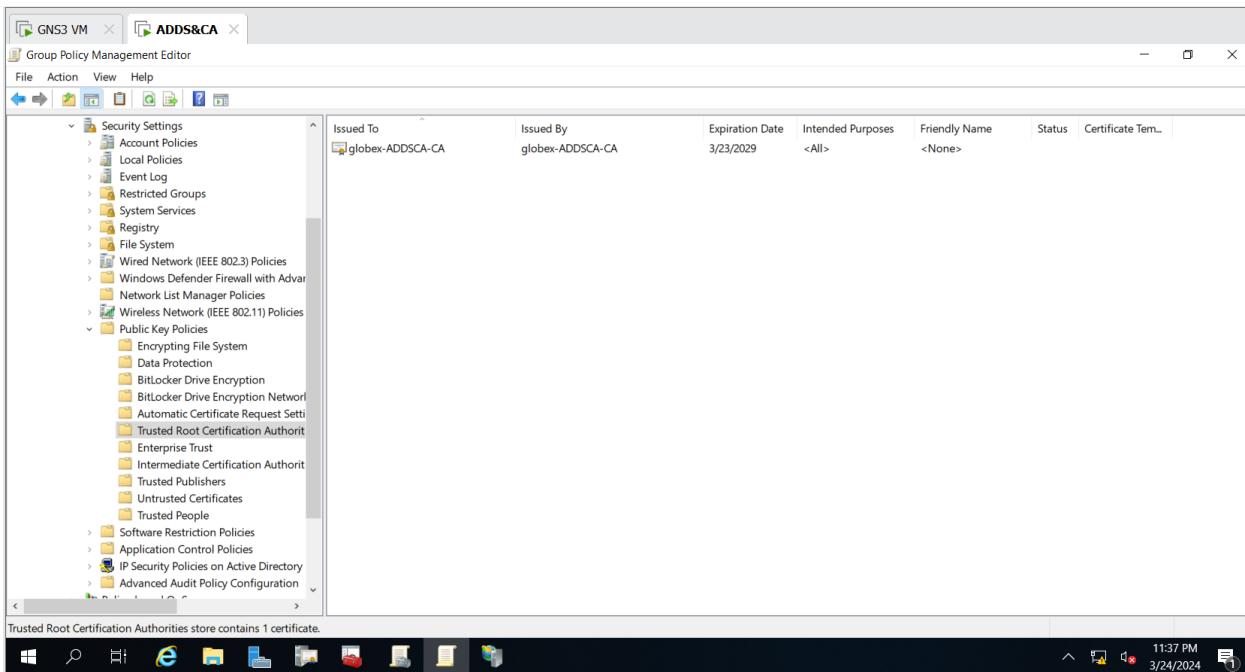


Add Group Policy to distribute certificate.

First I downloaded the main certificate on the ADDS server to be placed in the group policy and distributed to clients.

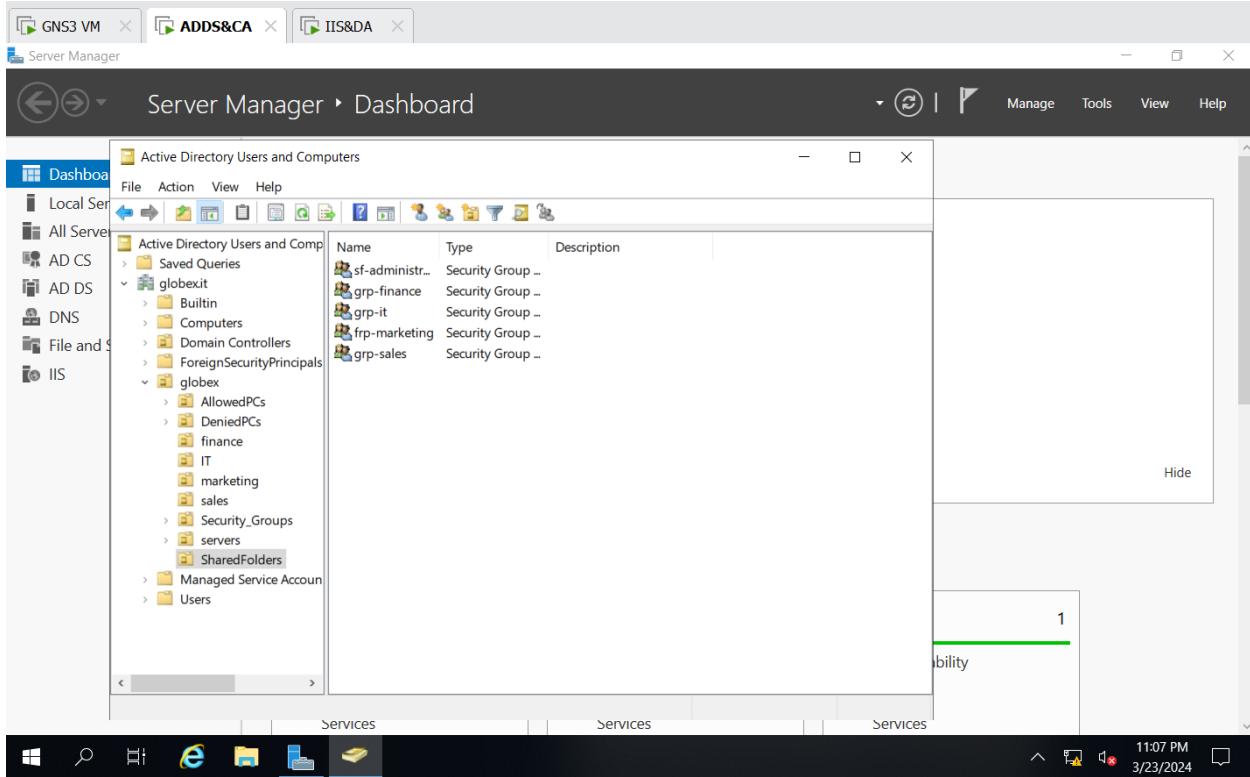
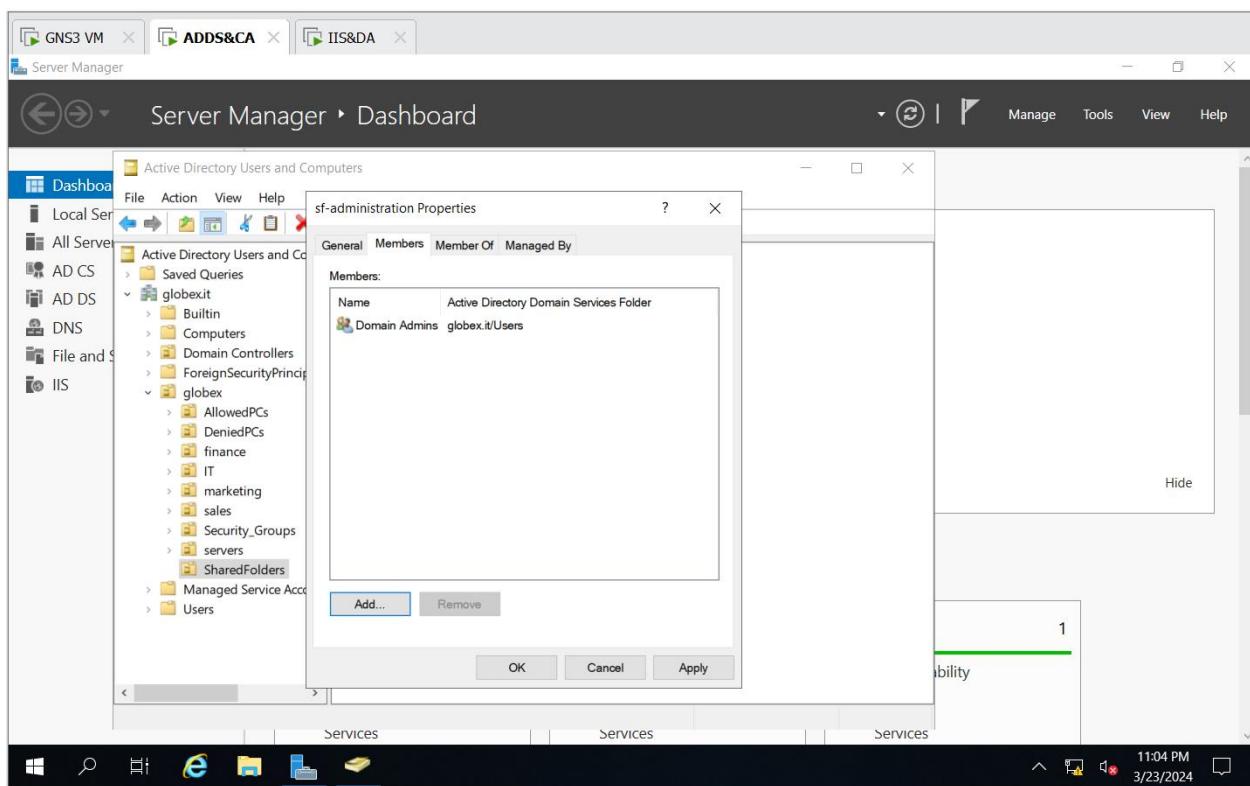
Path: Public Key Policies → trusted root certification authority → Enrollment Policy.

The screenshot shows the Microsoft Active Directory Certificate Services page at <http://localhost/certsrv/certcsrc.asp>. The page title is 'Microsoft Active Directory Certificate Services – globex-ADDS-CA-CA'. It provides instructions for downloading a CA certificate chain or CRL. A dropdown menu shows 'Current [globex-ADDS-CA-CA]'. Under 'Encoding method', 'DER' is selected. Below are links for 'Download CA certificate', 'Download CA certificate chain', 'Download latest base CRL', and 'Download latest delta CRL'.



Shared folders

First, I created a OU for shared folders, and added a group for each department, and one for the administration.



Step two: for each created folder, I updated the owner to sf_administration group, disable inheritance, and add a certain group that matches the folder with the proper permissions.

