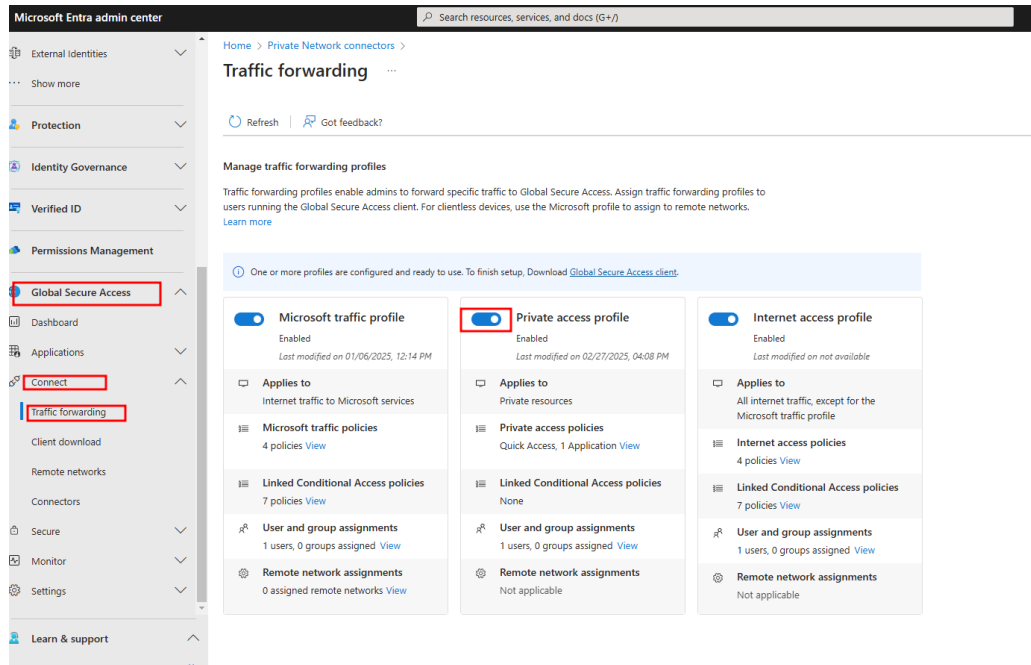
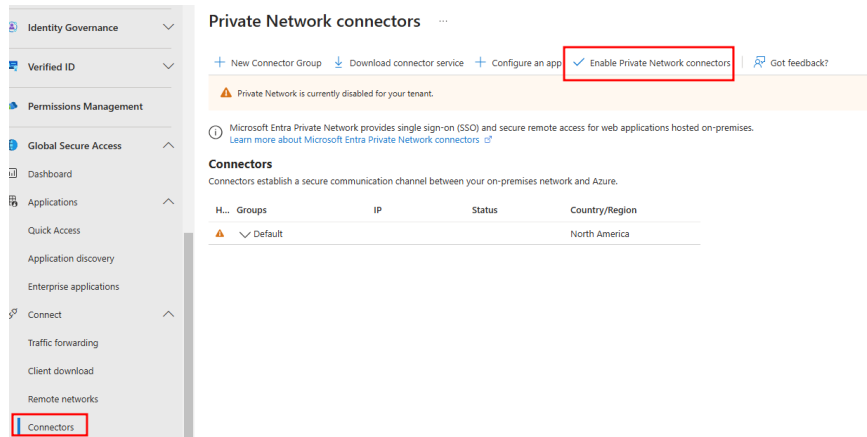


1. Microsoft Entra Private access

1. Log in to Microsoft Entra Admin center , go to “Global Security Access”
2. “Connect > Traffic forwarding ” , turn On private access. Also add user group to User and group assignments.



3. Then go to “Connector” and “Enable Private Network”



4. Now Create a VM on azure on same targeted network where all the services is.

Microsoft Azure

Home > Virtual machines >

Create a virtual machine

Validation passed

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Subscription	ZTR Subscription
Resource group	ServersRG
Virtual machine name	GSA-Connect
Region	East US
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard D51 v2 (1 vcpu, 3.5 GiB memory)
Enable Hibernation	No
Username	
Already have a Windows license?	No
Azure Spot	No

Disks

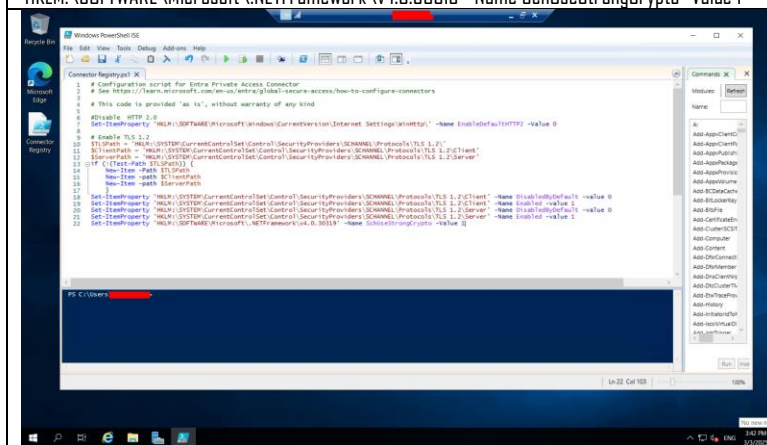
OS disk size	Image default
OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled

< Previous | Next > | Create

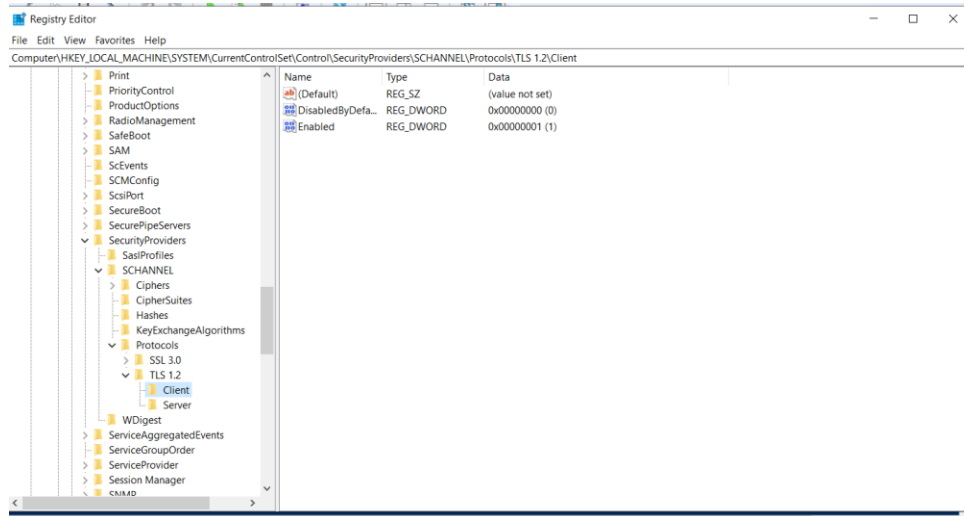
5. Add the sever to domain

6. Now run the following Power shell script for recommended registry update.

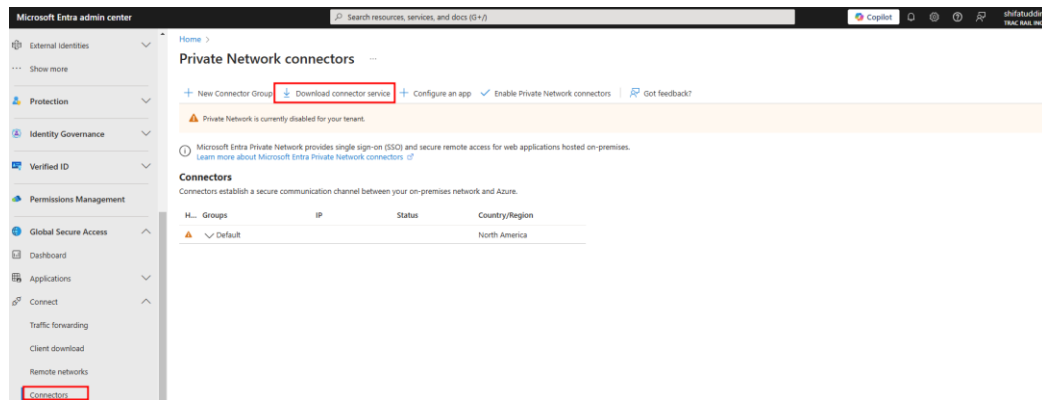
```
# Configuration script for Entra Private Access Connector # See https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-connectors # This code is provided 'as is', without warranty of any kind #Disable HTTP 2.0 Set-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp' -Name EnableDefaultHTTP2 -Value 0 # Enable TLS 1.2 $TLSPath = 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\' $ClientPath = 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' $ServerPath = 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' if (!(Test-Path $TLSPath)) { New-Item -Path $TLSPath New-Item -path $ClientPath New-Item -path $ServerPath } Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -Name DisabledByDefault -value 0 Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -Name Enabled -value 1 Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Name DisabledByDefault -value 0 Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Name Enabled -value 1 Set-ItemProperty 'HKLM:\SOFTWARE\Microsoft\NETFramework\v4.0.30319' -Name SchUseStrongCrypto -Value 1
```



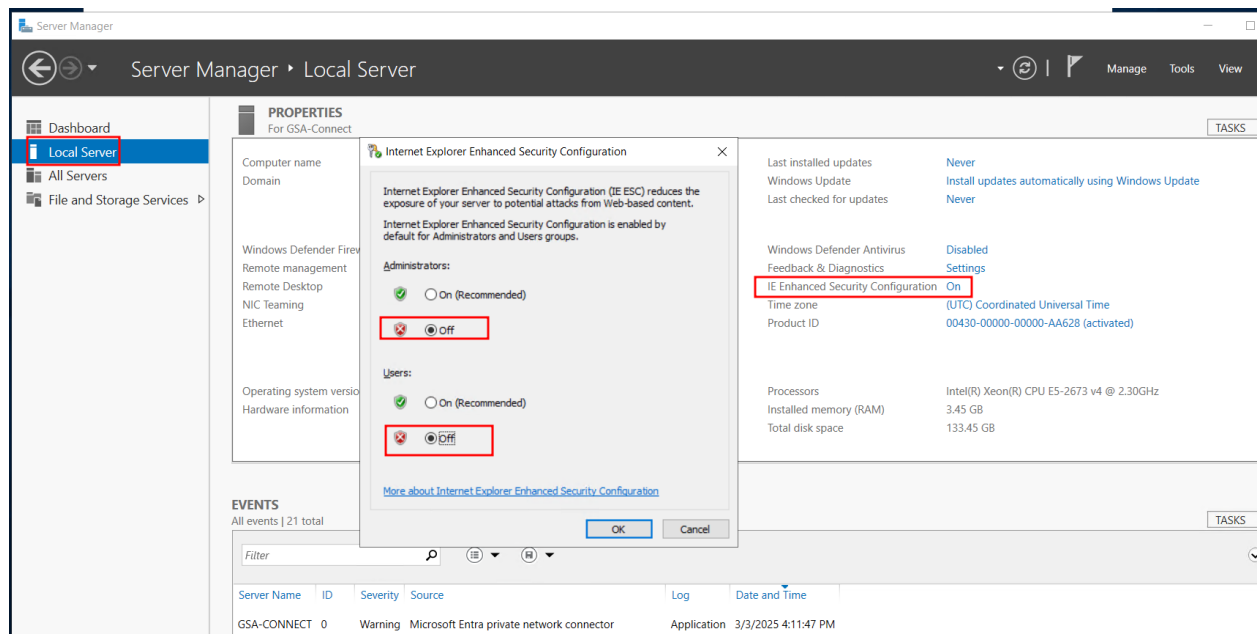
7. Now check the Registry if the changes applied correctly. Then reboot the server.



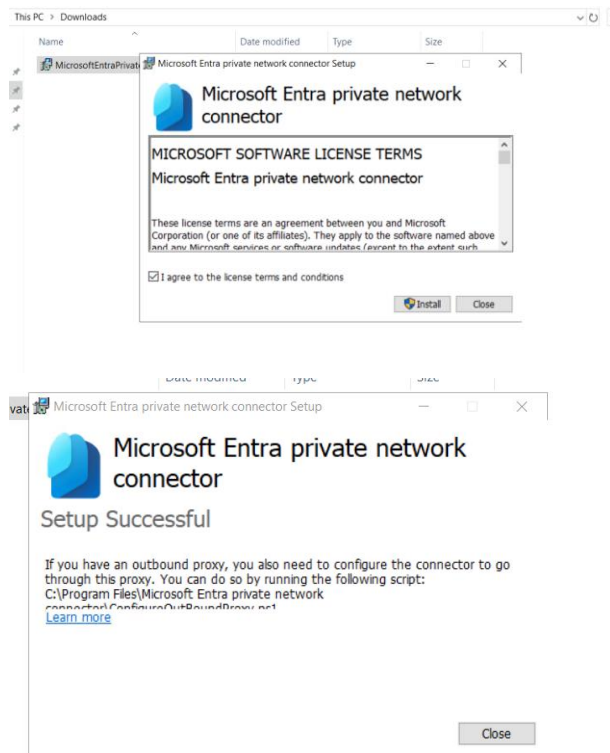
8. Now from Entra admin Center download connector



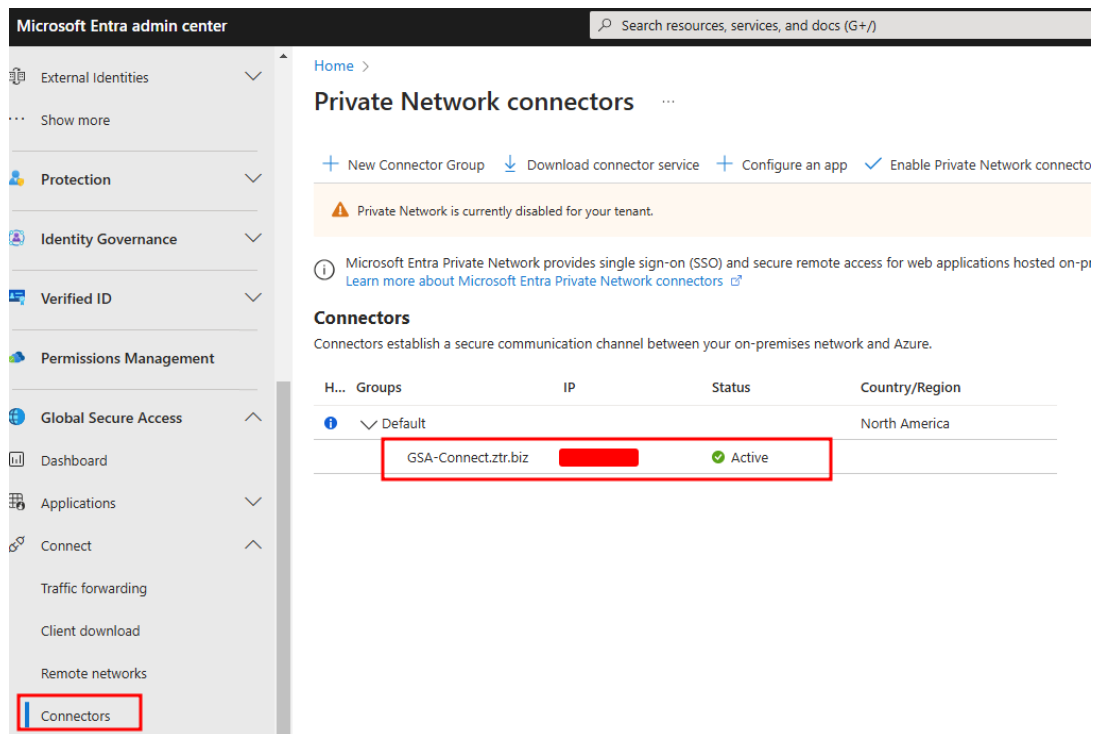
9. Now log in to the Server(Azure VM), Open server manager. Click on “Local server” . turn off IE Enhanced Security Configuration. Turn back on after installation on connector.



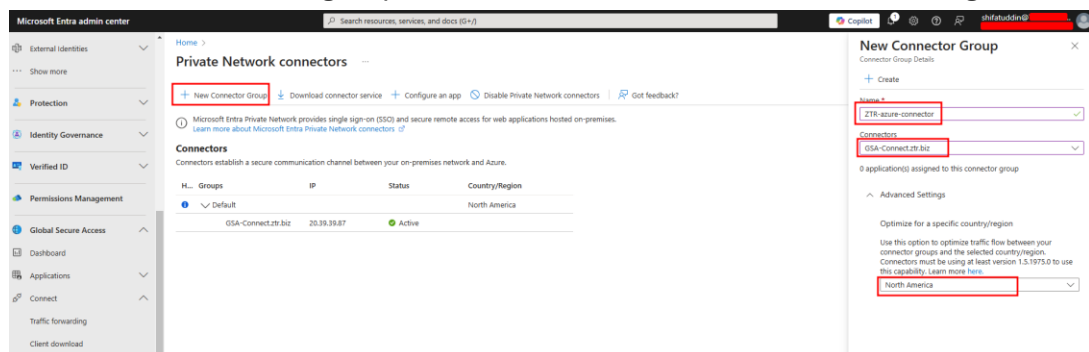
10. Install the connector and signin



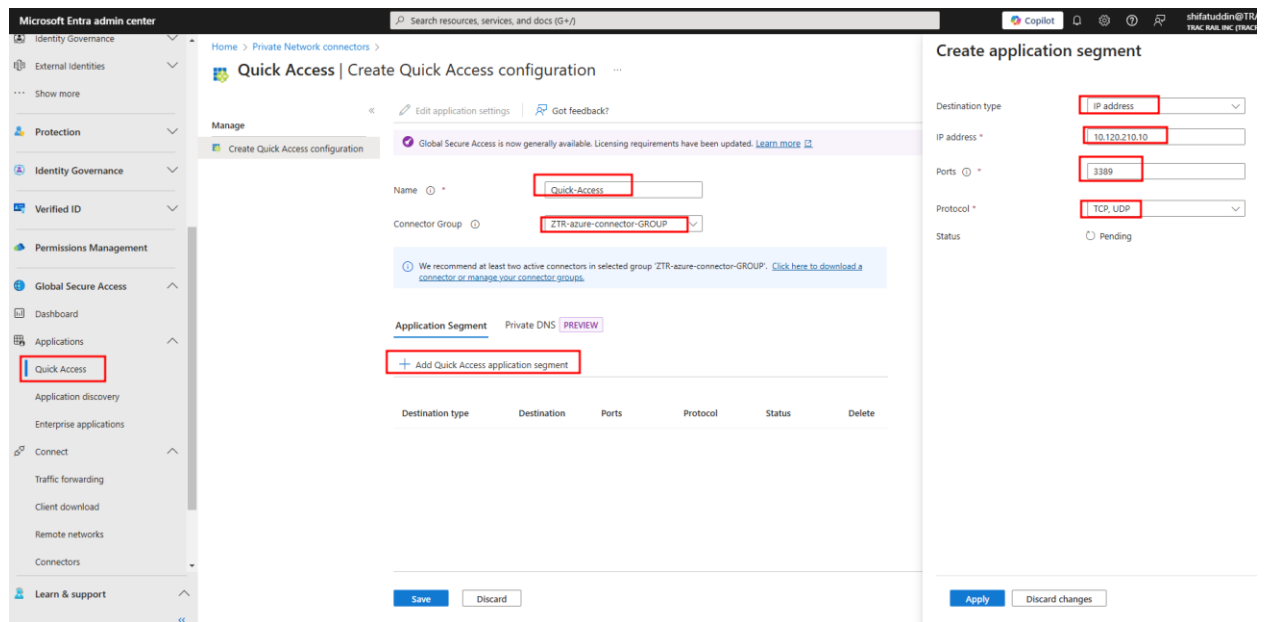
11 . On the Entra Connector section we can see the connector is active



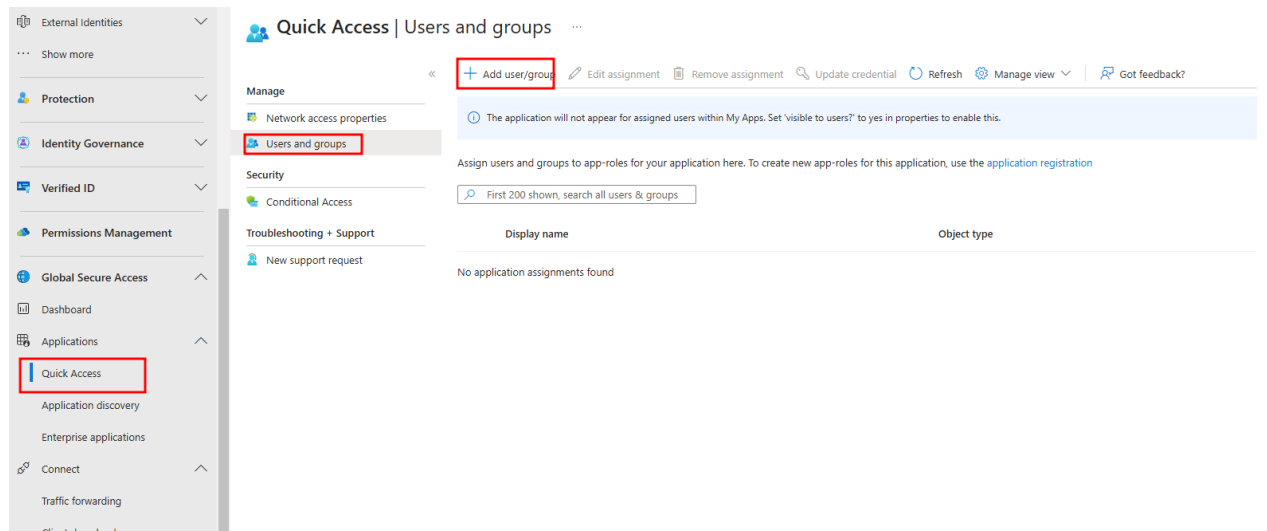
11. Create new connector group and add the Connector also select the region.



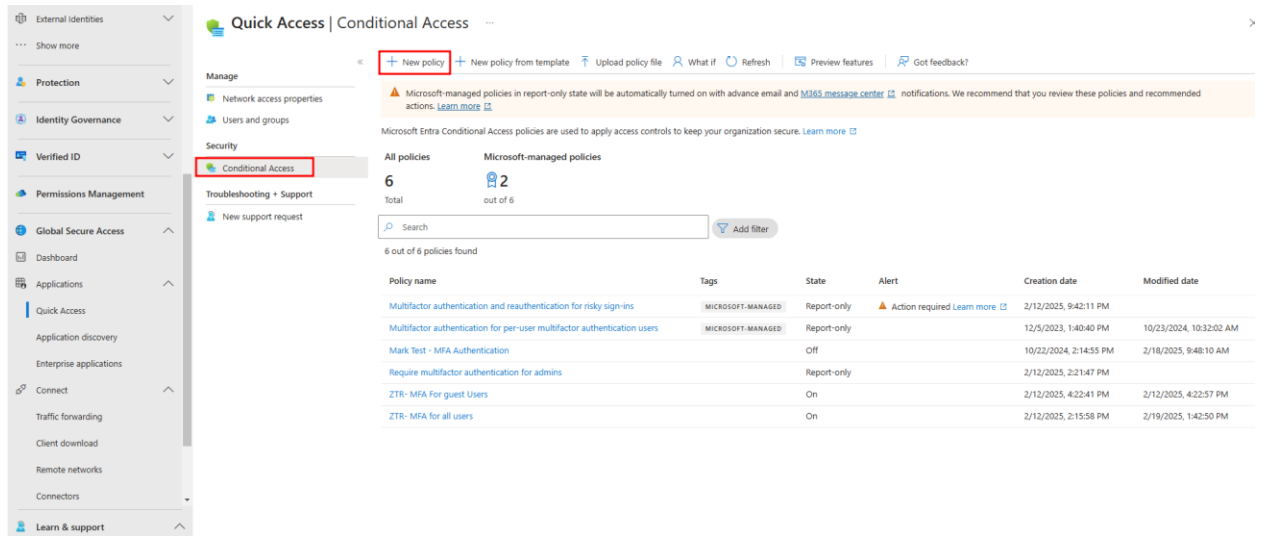
12. Now From the Entra admin center click on Global Secure Access > Applications > Quick Access. Give it a name, Connection group. Also add Endpoint (Vm on same network) to Quick Access Application Segment.



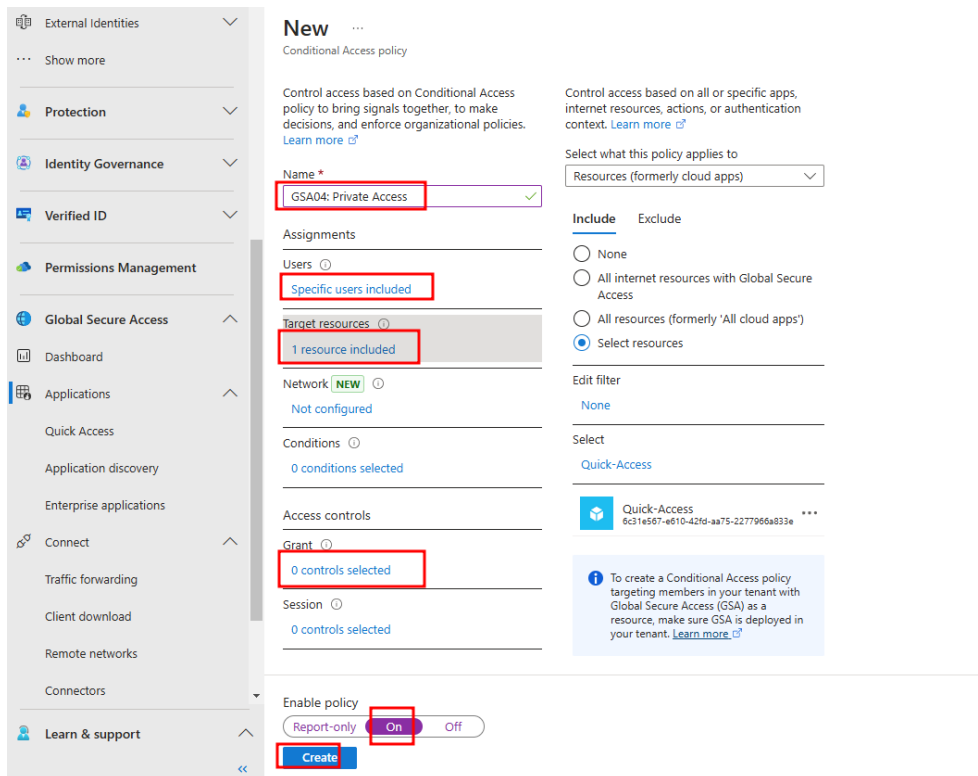
13. Now add users and group



14. Go to Conditional Access and add policy



15. Set user then set Target Resource as Quick-Access



16. Finally you can download GSA client , install and login with a user. The user should avail to access the remote services

Global Secure Access Client - Advanced diagnostics

OverviewHealth checkForwarding profileHostname acquisitionTrafficAdvanced log collection

Network traffic

Collect and analyze this device's network traffic. [Learn more about Traffic page](#)

Start collecting

Export CSV

Clear table

Add filter

Columns

Process name != GlobalSecureAccessClient.exe

Action == Tunnel

Timestamp begin	Conn	Protocol	Destination FQDN	Destination IP	Destination Port
2025-03-03 3:11:45 PM	Active	TCP	192155-ipv4v6.gr.global...	6.6.0.64	443
2025-03-03 3:11:46 PM	Active	TCP	www.bing.com	6.6.0.21	443
2025-03-03 3:11:46 PM	Active	TCP	business.bing.com	6.6.0.32	443
2025-03-03 3:11:47 PM	Active	TCP	substrate.office.com	6.6.0.20	443
2025-03-03 3:11:47 PM	Active	TCP	substrate.office.com	6.6.0.20	443
2025-03-03 3:11:54 PM	Active	TCP	assets.msn.com	6.6.0.34	443
2025-03-03 3:11:54 PM	Active	TCP	fp.msedge.net	6.6.0.96	443
2025-03-03 3:11:56 PM	Active	TCP	searchhighlights.bing.com	6.6.0.33	443
2025-03-03 3:11:57 PM	Active	TCP	agent-us2.us2.ninjarmm....	6.6.0.73	443
2025-03-03 3:12:01 PM	Closed	TCP		10.120.100.10	3389
2025-03-03 3:12:13 PM	Active	TCP		10.120.100.10	3389
2025-03-03 3:12:13 PM	Active	TCP	unitedstates.cp.wd.micro...	6.6.0.121	443
2025-03-03 3:12:14 PM	Active	UDP		10.120.100.10	3389
2025-03-03 3:12:14 PM	Active	UDP		10.120.100.10	3389
2025-03-03 3:11:44 PM	Active	TCP	tracrail-my.sharepoint.co...	6.6.0.52	443

10.120.100.10 - Remote Desktop Connection

S7-PCT - Port Configurati...

TIA admin

TIA Administrator

TIA Portal V18

7jjVv+TS2U+WA81a.0OneDrive.exe14614128