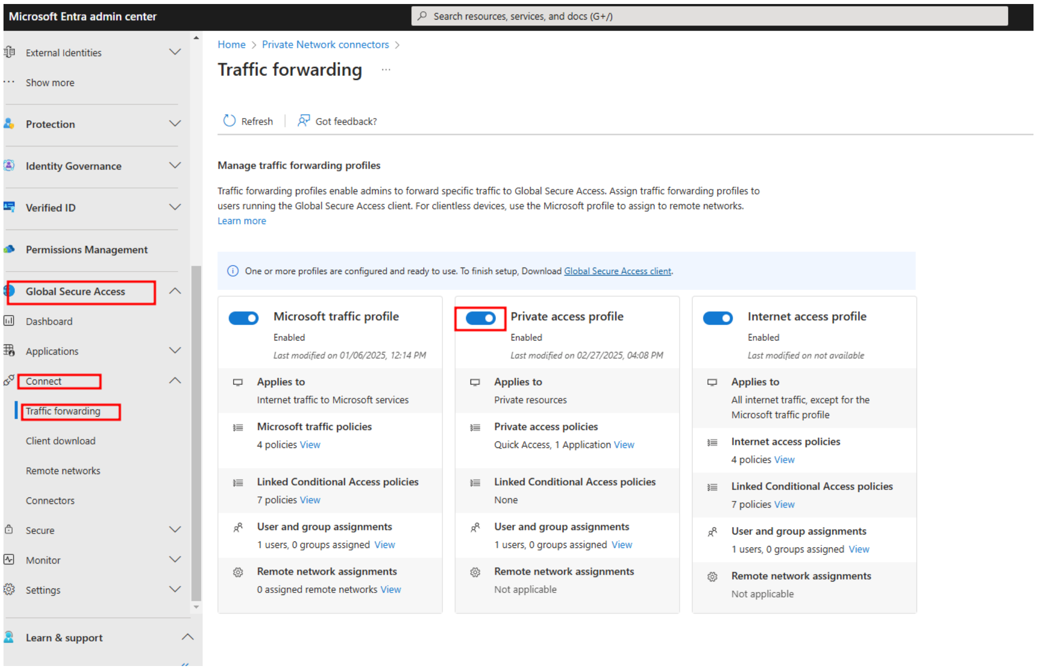
Microsoft Entra Private access

1. Preparing Azure tenant

a. Login to Microsoft Entra Admin center, go to “Global Security Access”

b. “Connect” > “Traffic forwarding” , turn On private access. Also add user group to User and group assignments.



Traffic forwarding

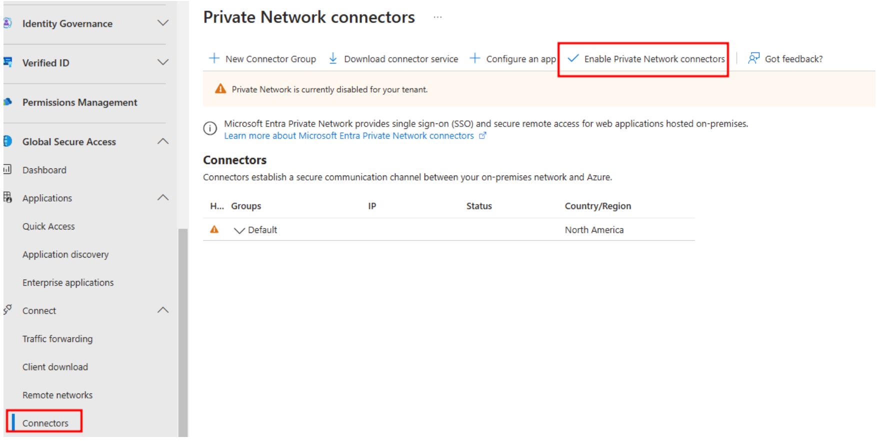
Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks. Learn more

One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.

Microsoft traffic profile	Private access profile	Internet access profile
Enabled *Last modified on 01/06/2025, 12:14 PM*	Enabled *Last modified on 02/27/2025, 04:08 PM*	Enabled *Last modified on not available*
Applies to Internet traffic to Microsoft services	**Applies to** Private resources	**Applies to** All internet traffic, except for the Microsoft traffic profile
Microsoft traffic policies 4 policies View	**Private access policies** Quick Access, 1 Application View	**Internet access policies** 4 policies View
Linked Conditional Access policies 7 policies View	**Linked Conditional Access policies** None	**Linked Conditional Access policies** 7 policies View
User and group assignments 1 users, 0 groups assigned View	**User and group assignments** 1 users, 0 groups assigned View	**User and group assignments** 1 users, 0 groups assigned View
Remote network assignments 0 assigned remote networks View	**Remote network assignments** Not applicable	**Remote network assignments** Not applicable

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



Private Network connectors

Private Network is currently disabled for your tenant.

Microsoft Entra Private Network provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Microsoft Entra Private Network connectors

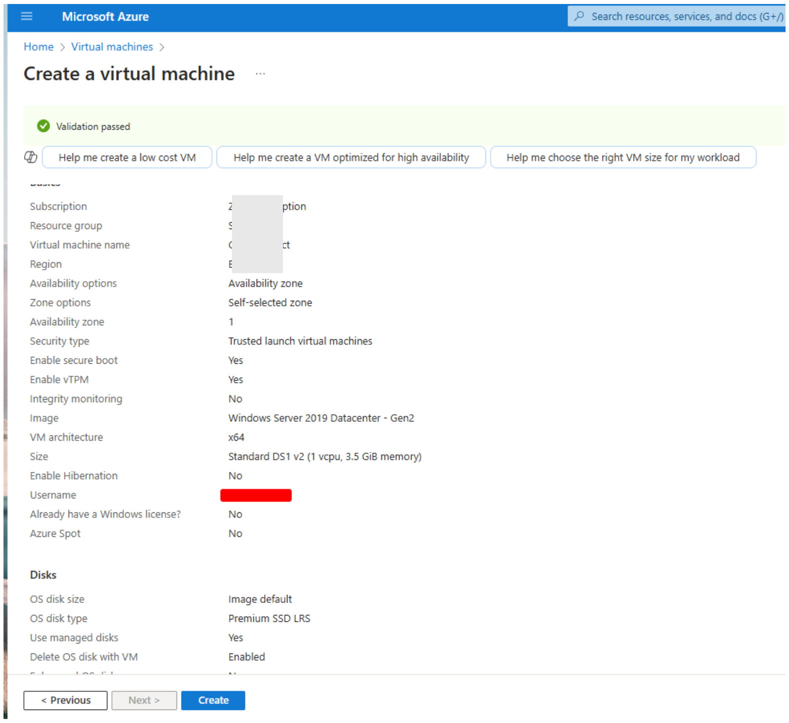
Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

H...	Groups	IP	Status	Country/Region
⚠	Default			North America

2. Installing connector

a. Now Take a Windows server (2012 R2 or later) or Create a VM on azure. Make sure the VM can reach the targeted resources.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual machines >
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
< Previous
Next >
Create

Create a virtual machine

Validation passed

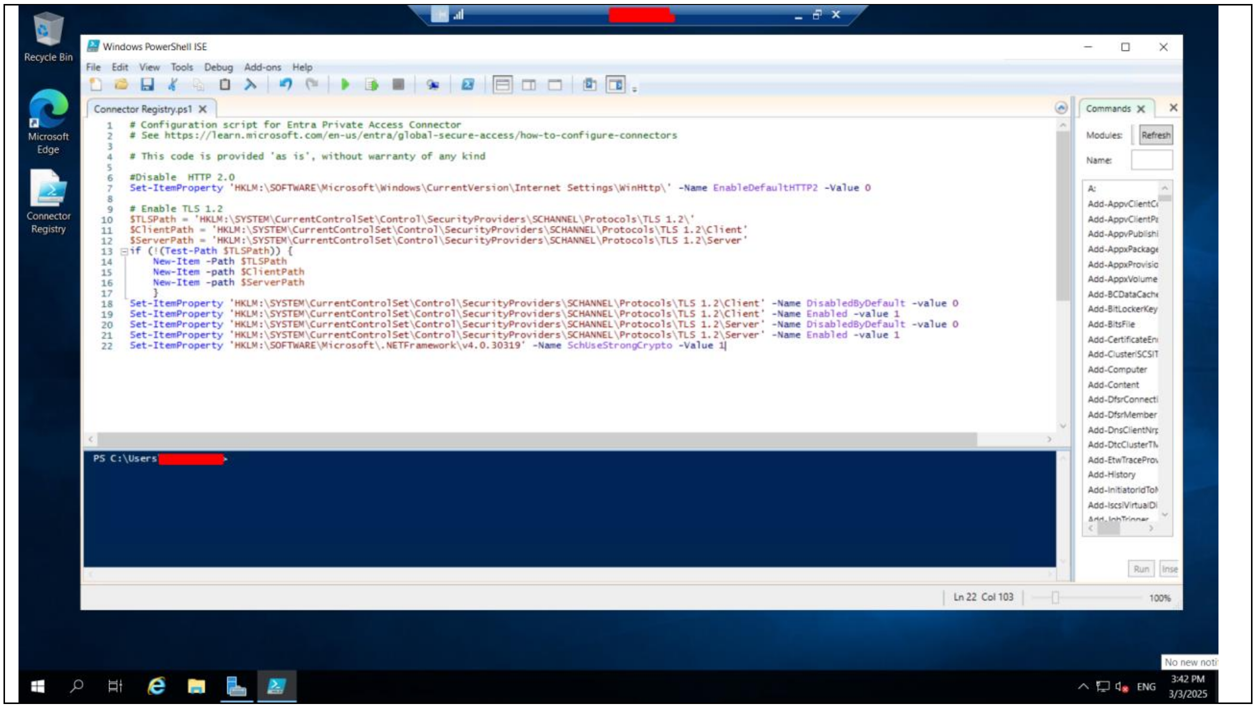
Subscription	[redacted]
Resource group	[redacted]
Virtual machine name	[redacted]
Region	[redacted]
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Enable Hibernation	No
Username	[redacted]
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

3. Add the sever to domain (Optional)
4. Now run the following Power shell script for recommended registry update.

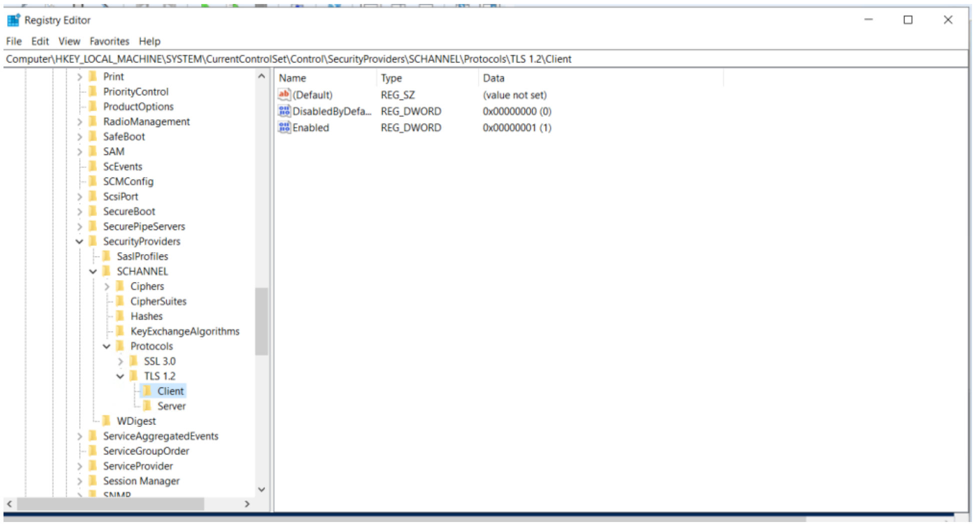
```
# Configuration script for Entra Private Access Connector # See https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-
connectors # This code is provided 'as is', without warranty of any kind #Disable HTTP 2.0 Set-ItemProperty
'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet 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
```



```
# 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
```

```
PS C:\Users[redacted]>
```

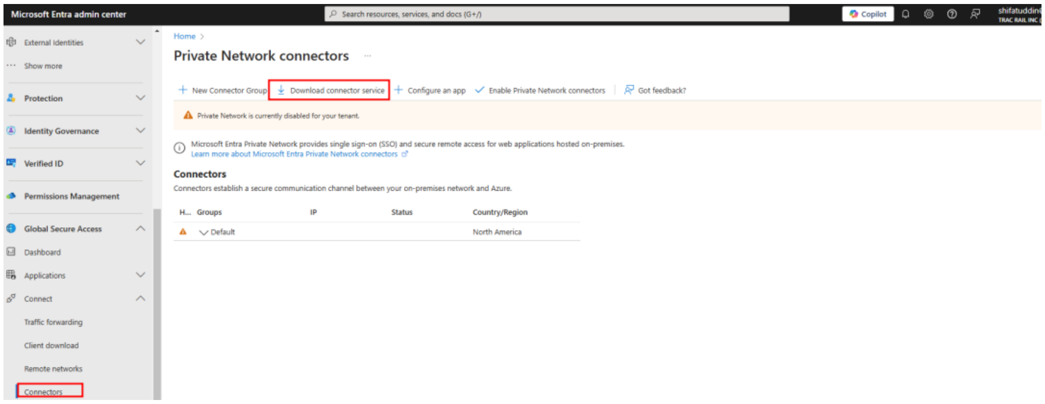
5. Now check the Registry if the changes applied correctly. Then reboot the server.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefa...	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)

6. Now from Entra admin Center download connector



Private Network connectors

Private Network is currently disabled for your tenant.

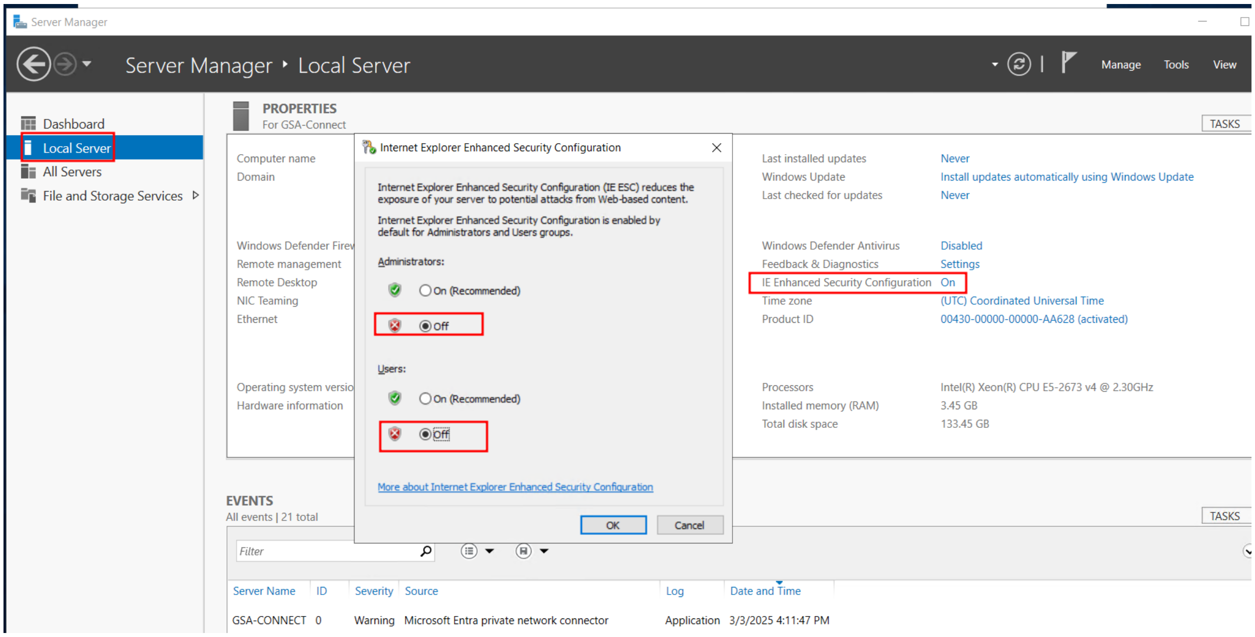
Microsoft Entra Private Network provides single sign-on (SSO) and secure remote access for web applications hosted on-premises.
Learn more about Microsoft Entra Private Network connectors

Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

H...	Groups	IP	Status	Country/Region
⚠	Default			North America

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



PROPERTIES
For GSA-Connect

Computer name
Domain

Windows Defender Firew
Remote management
Remote Desktop
NIC Teaming
Ethernet

Operating system versio
Hardware information

Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:
○ On (Recommended)
● Off

Users:
○ On (Recommended)
● Off

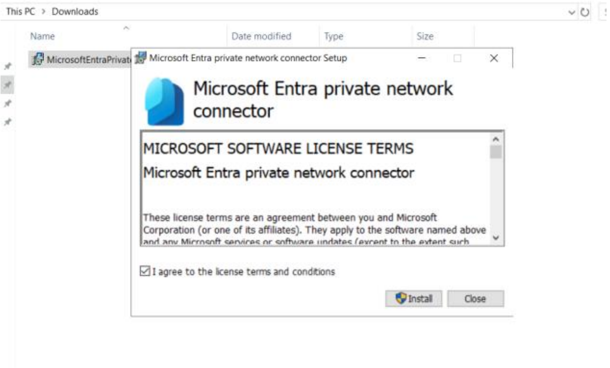
More about Internet Explorer Enhanced Security Configuration

Last installed updates	Never
Windows Update	Install updates automatically using Windows Update
Last checked for updates	Never
Windows Defender Antivirus	Disabled
Feedback & Diagnostics	Settings
IE Enhanced Security Configuration	On
Time zone	(UTC) Coordinated Universal Time
Product ID	00430-00000-00000-AA628 (activated)
Processors	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
Installed memory (RAM)	3.45 GB
Total disk space	133.45 GB

EVENTS
All events | 21 total

Server Name	ID	Severity	Source	Log	Date and Time
GSA-CONNECT	0	Warning	Microsoft Entra private network connector	Application	3/3/2025 4:11:47 PM

8. Install the connector. During installation the agent will ask for Admin signin



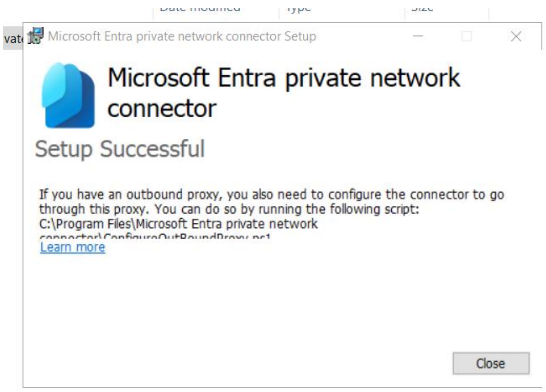
Microsoft Entra private network connector Setup

Microsoft Entra private network connector

MICROSOFT SOFTWARE LICENSE TERMS
Microsoft Entra private network connector

These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to the software named above and any Microsoft services or software updates (except to the extent such

☑ I agree to the license terms and conditions



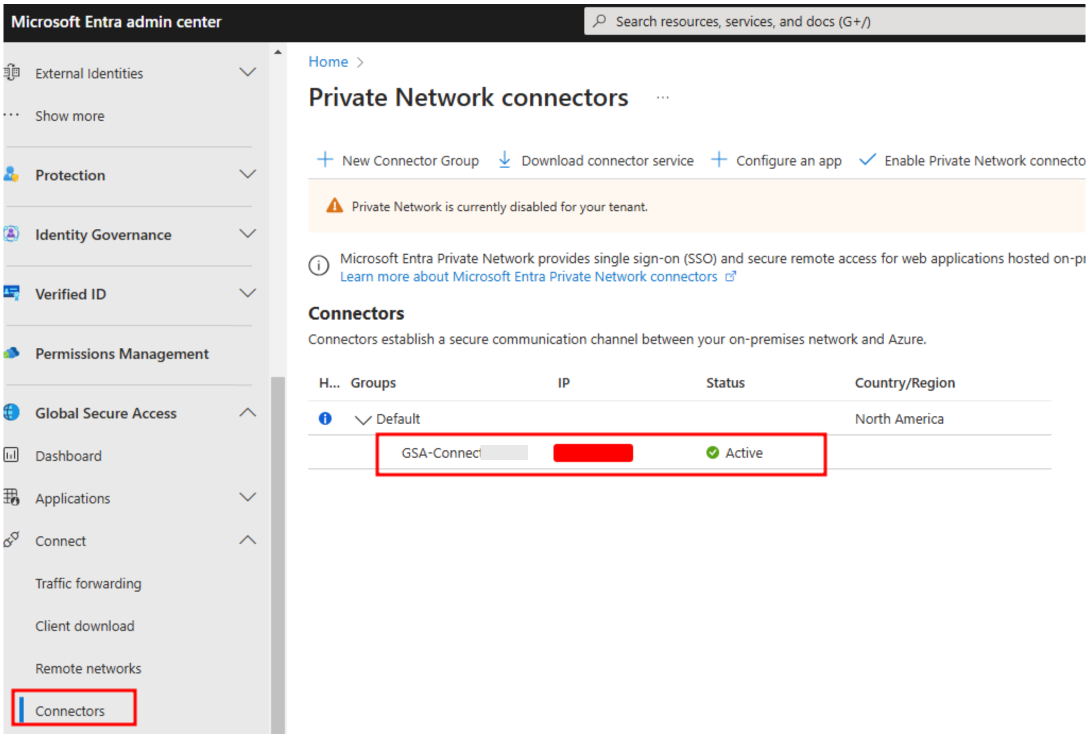
Microsoft Entra private network connector

Setup Successful

If you have an outbound proxy, you also need to configure the connector to go through this proxy. You can do so by running the following script: C:\Program Files\Microsoft Entra private network connector\ConfigureOutBoundProxy.ps1

Learn more

9. On the Entra Connector section we can see the connector is active under default Connector group



Private Network connectors

Private Network is currently disabled for your tenant.

Microsoft Entra Private Network provides single sign-on (SSO) and secure remote access for web applications hosted on-pı

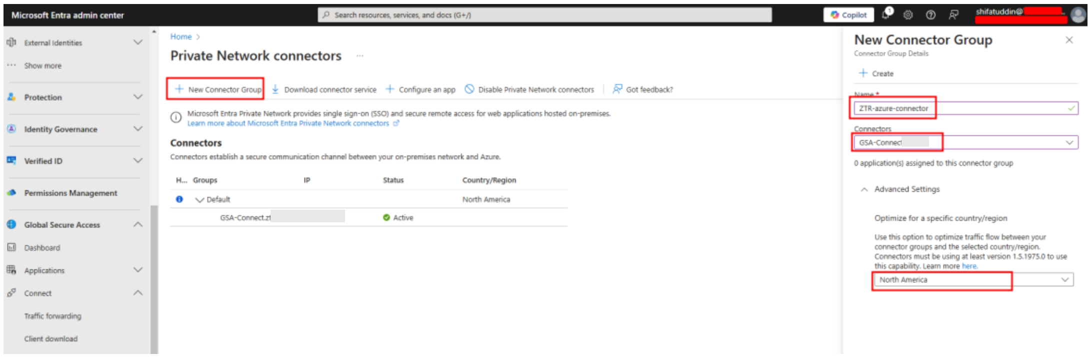
Learn more about Microsoft Entra Private Network connectors

Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

H...	Groups	IP	Status	Country/Region
	Default			North America
	GSA-Connec[redacted]	[redacted]	Active	

10. Now create new connector group and add the Connector also select the region.



[redacted]

Private Network connectors

Microsoft Entra Private Network provides single sign-on (SSO) and secure remote access for web applications hosted on-premises.

Learn more about Microsoft Entra Private Network connectors

Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

H...	Groups	IP	Status	Country/Region
	Default			North America
	GSA-Connect.zt[redacted]		Active	

New Connector Group

Connector Group Details

Name *: ZTR-azure-connector

Connectors: GSA-Connec[redacted]

0 application(s) assigned to this connector group

Advanced Settings

Optimize for a specific country/region

Use this option to optimize traffic flow between your connector groups and the selected country/region. Connectors must be using at least version 1.5.1975.0 to use this capability. Learn more here.

North America

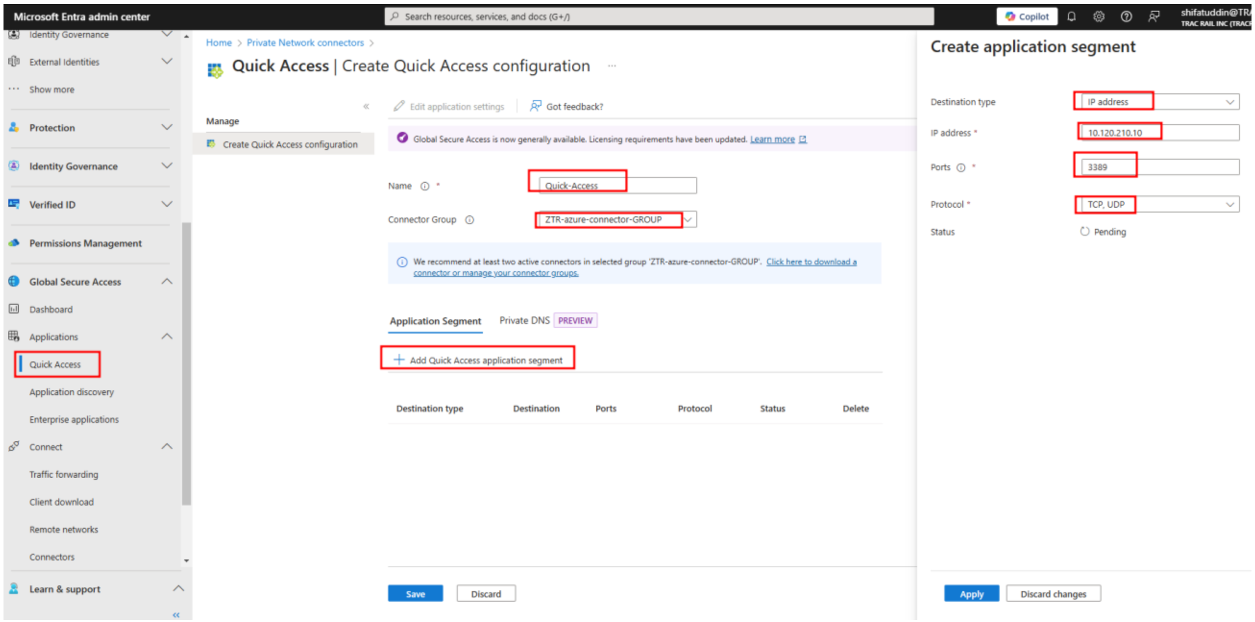
Now each resources needs a corresponding GSA Enterprise Application for permission and protocols. On a smaller scale, built-in Quick Access Application could be used. On the contrary, Individual “Enterprise Application” for each target Resources/ Endpoint is recommended.

3. Quick Access

Now From the Entra admin center click on **Global Secure Access** > Applications > **Quick Access**.

Give it a name, Choose Connection group. Also add Target Endpoint and protocol (tcp/udp & port) to Quick Access Application Segment.

Make sure that Endpoint is reachable from Connector Server .



Quick Access | Create Quick Access configuration

Global Secure Access is now generally available. Licensing requirements have been updated. Learn more

Name * : Quick-Access

Connector Group : ZTR-azure-connector-GROUP

We recommend at least two active connectors in selected group 'ZTR-azure-connector-GROUP'. Click here to download a connector or manage your connector groups.

Destination type	Destination	Ports	Protocol	Status	Delete

Create application segment

Destination type: IP address

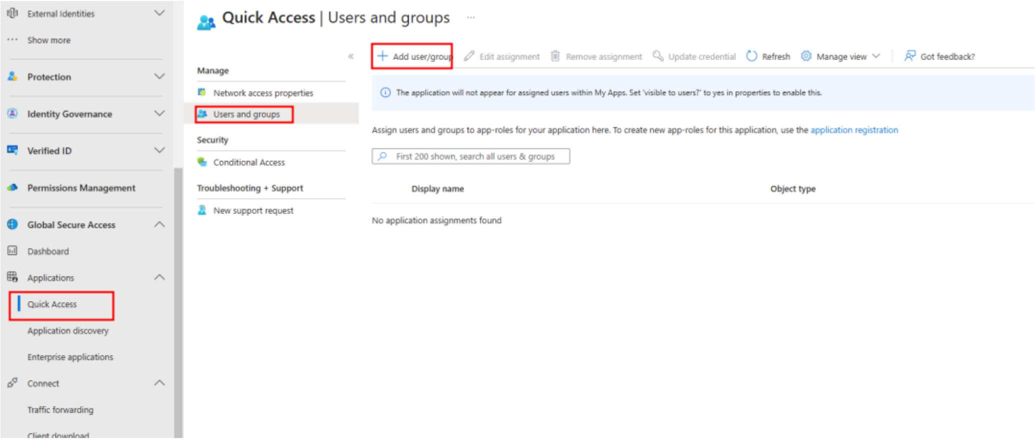
IP address *: 10.120.210.10

Ports *: 3389

Protocol *: TCP, UDP

Status: Pending

1. Now add users and group



The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this.

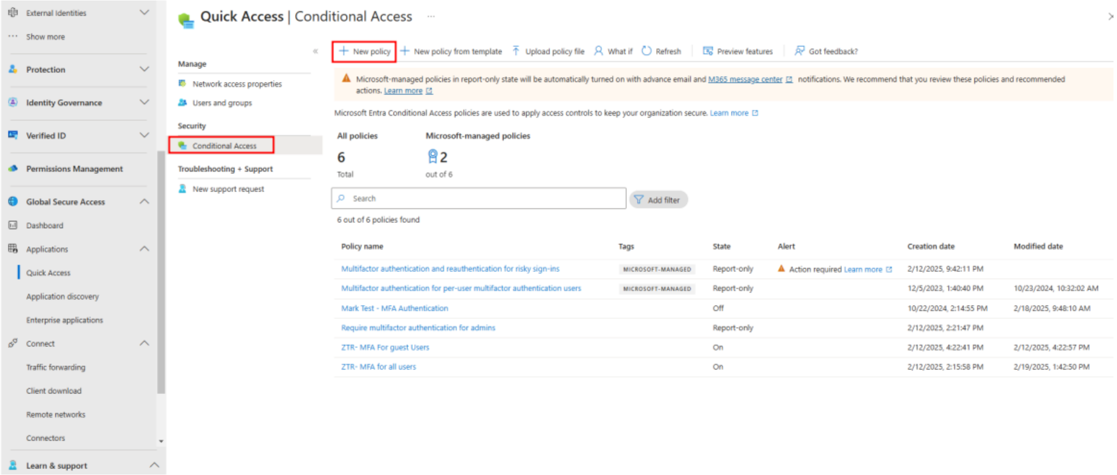
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration

First 200 shown, search all users & groups

Display name	Object type

No application assignments found

2. Go to Conditional Access and add policy



Microsoft-managed policies in report-only state will be automatically turned on with advance email and M365 message center notifications. We recommend that you review these policies and recommended actions. Learn more

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies: 6 Total

Microsoft-managed policies: 2 out of 6

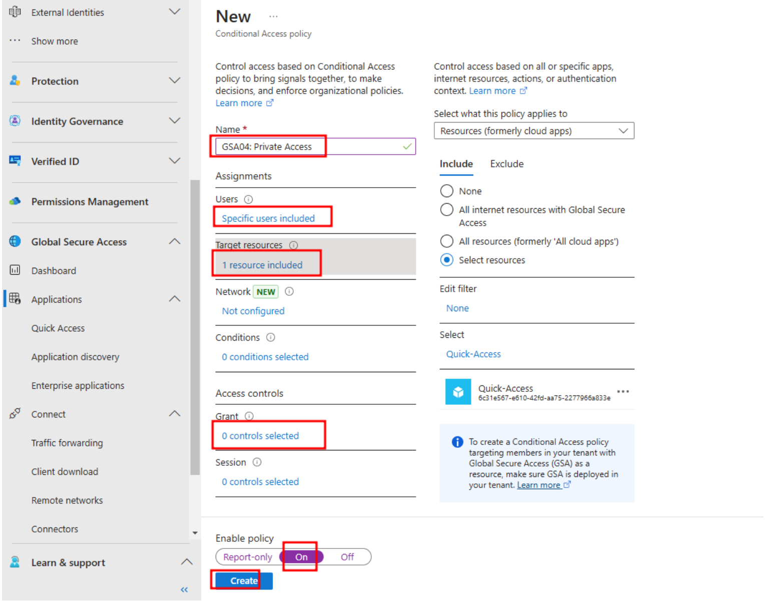
Search

Add filter

6 out of 6 policies found

Policy name	Tags	State	Alert	Creation date	Modified date
Multifactor authentication and reauthentication for risky sign-ins	MICROSOFT-MANAGED	Report-only	Action required Learn more	2/12/2025, 9:42:11 PM	
Multifactor authentication for per-user multifactor authentication users	MICROSOFT-MANAGED	Report-only		12/5/2023, 1:40:40 PM	10/23/2024, 10:32:02 AM
Mark Test - MFA Authentication		Off		10/22/2024, 2:14:55 PM	2/18/2025, 9:48:10 AM
Require multifactor authentication for admins		Report-only		2/12/2025, 2:21:47 PM	
ZTR- MFA For guest Users		On		2/12/2025, 4:22:41 PM	2/12/2025, 4:22:57 PM
ZTR- MFA for all users		On		2/12/2025, 2:15:58 PM	2/19/2025, 1:42:50 PM

3. Set user then set Target Resource as Quick-Access , add User group and grant access



New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *: GSA04: Private Access

Assignments

Users: Specific users included

Target resources: 1 resource included

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Session: 0 controls selected

Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to: Resources (formerly cloud apps)

Include | Exclude

○ None
○ All internet resources with Global Secure Access
○ All resources (formerly 'All cloud apps')
● Select resources

Edit filter: None

Select: Quick-Access

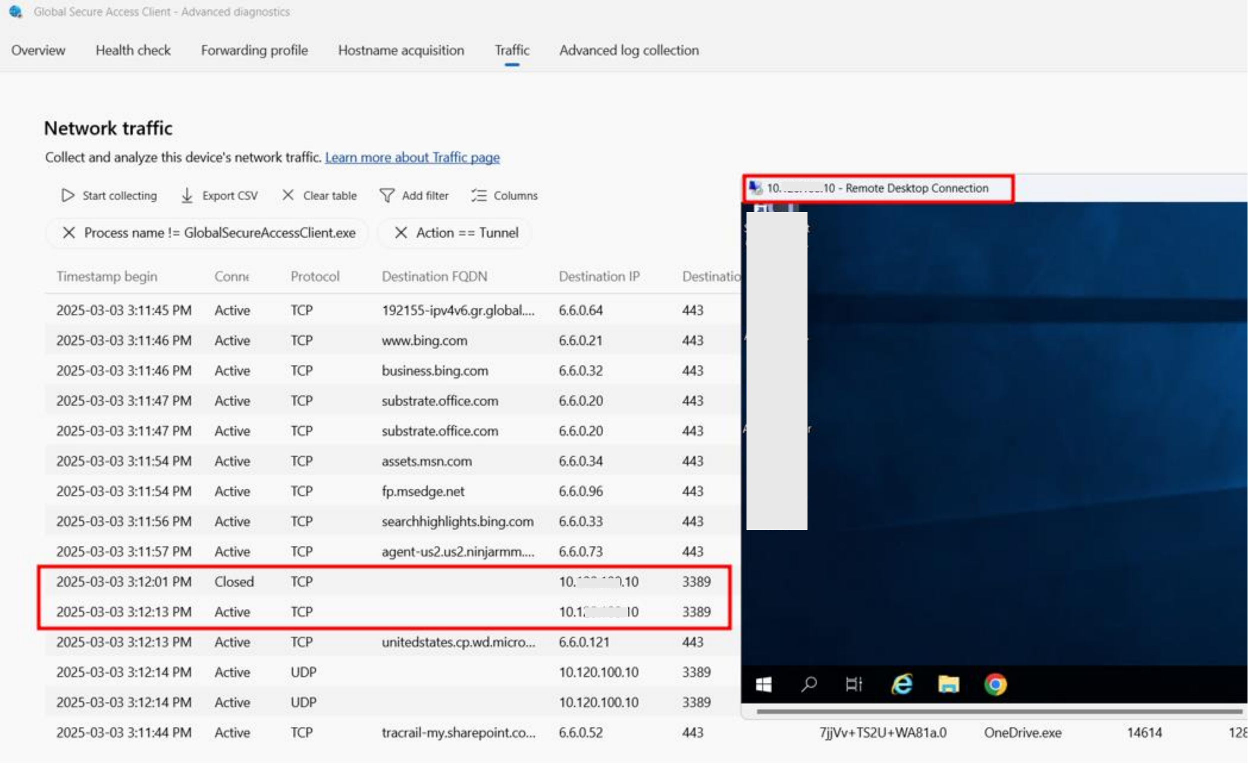
Quick-Access
6c31e567-e610-42fd-aa75-2277966a833e

To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. Learn more

Enable policy: Report-only [✓ On] Off

Create

4. Finally you can download GSA client, install and login with a user (Make sure the user has Microsoft Entra Suite License). The user should avail to access the remote services



Network traffic

Collect and analyze this device's network traffic. Learn more about Traffic page

Process name != GlobalSecureAccessClient.exe

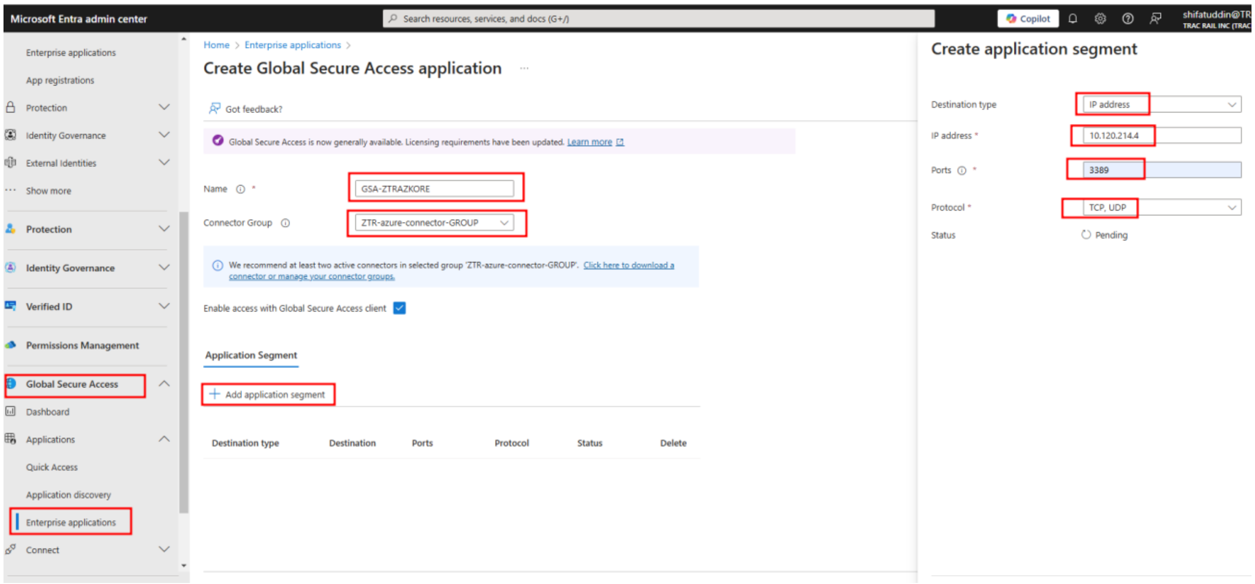
Action == Tunnel

10.[redacted].10 - Remote Desktop Connection

Timestamp begin	Conne	Protocol	Destination FQDN	Destination IP	Destinatio				
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.[redacted].10	3389				
2025-03-03 3:12:13 PM	Active	TCP		10.1[redacted]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	7jjVv+TS2U+WA81a.0	OneDrive.exe	14614	128

4. **Enterprise Application :**

Create Enterprise Application from Entra Admin center, select Connector Group based of the location of Targeted resources. Then click on “Add application segment” and add ip/fdqn , Port and protocols. Make sure the targeted resource is reachable from the Servers on selected Connector Group.



Create Global Secure Access application

Global Secure Access is now generally available. Licensing requirements have been updated.

Name * GSA-ZTRAZKORE

Connector Group ZTR-azure-connector-GROUP

We recommend at least two active connectors in selected group 'ZTR-azure-connector-GROUP'.

Enable access with Global Secure Access client ☑

Destination type	Destination	Ports	Protocol	Status	Delete

Create application segment

Destination type IP address

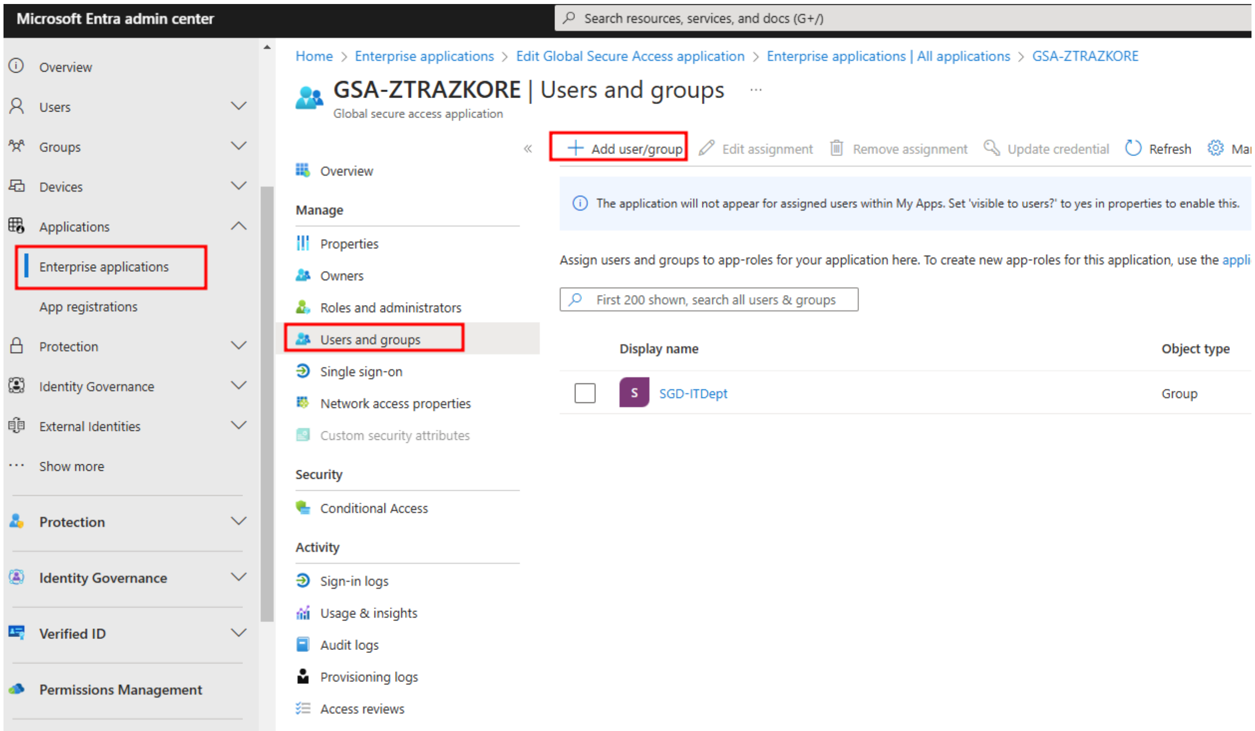
IP address * 10.120.214.4

Ports * 3389

Protocol * TCP, UDP

Status Pending

Now from the Enterprise application add user group.



GSA-ZTRAZKORE | Users and groups

Global secure access application

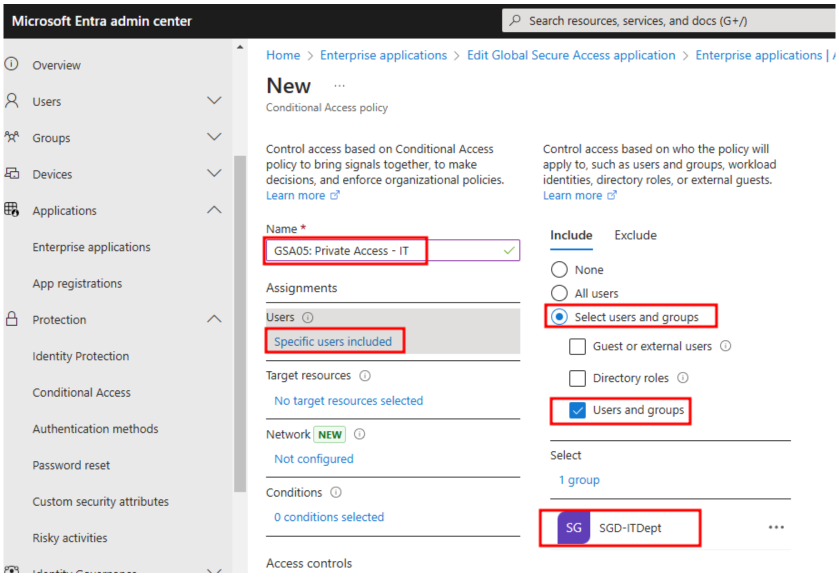
The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the appli

Display name	Object type
☐ SGD-ITDept	Group

On the Entra Admin Center, go to Protection > Conditional Access > policy, and add new policy.

Add targeted group


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Overview
Users
Groups
Devices
Applications
Enterprise applications
App registrations
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Home > Enterprise applications > Edit Global Secure Access application > Enterprise applications | /

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

GSA05: Private Access - IT

Assignments

Users

Specific users included

Target resources

No target resources selected

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Include Exclude

○ None

○ All users

● Select users and groups

□ Guest or external users

□ Directory roles

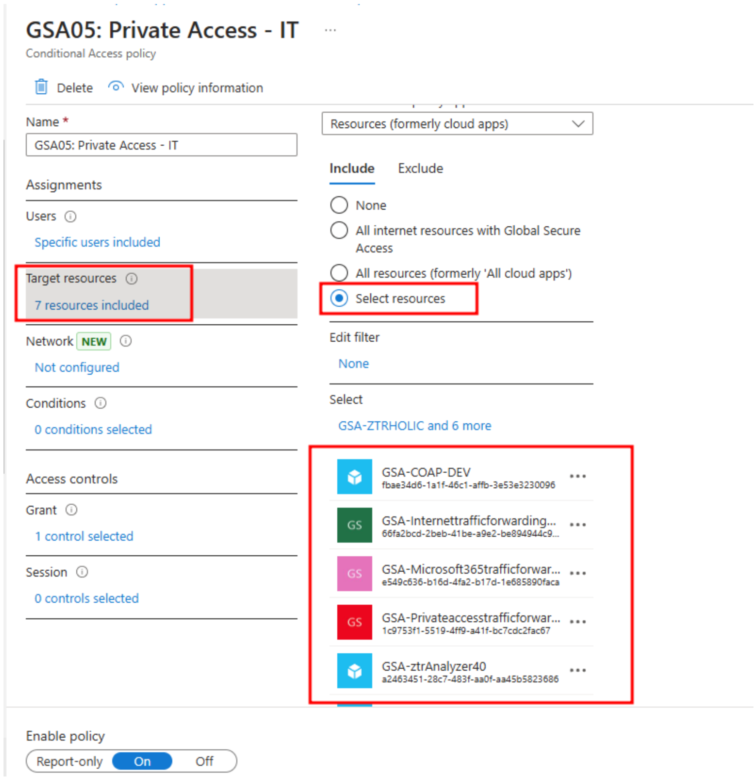
☑ Users and groups

Select

1 group

SG SGD-ITDept ...

Add Target resource :


GSA05: Private Access - IT ...

Conditional Access policy

Name *

GSA05: Private Access - IT

Assignments

Users

Specific users included

Target resources

7 resources included

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Resources (formerly cloud apps)

Include Exclude

○ None

○ All internet resources with Global Secure Access

○ All resources (formerly 'All cloud apps')

● Select resources

Edit filter

None

Select

GSA-ZTRHOLIC and 6 more

GSA-COAP-DEV
fbae34d6-1a1f-46c1-affb-3e53e3230096

GS GSA-Internettrafficforwarding...
66fa2bcd-2beb-41be-a9e2-be894944c9...

GS GSA-Microsoft365trafficforwar...
e549c636-b16d-4fa2-b17d-1e685890faca

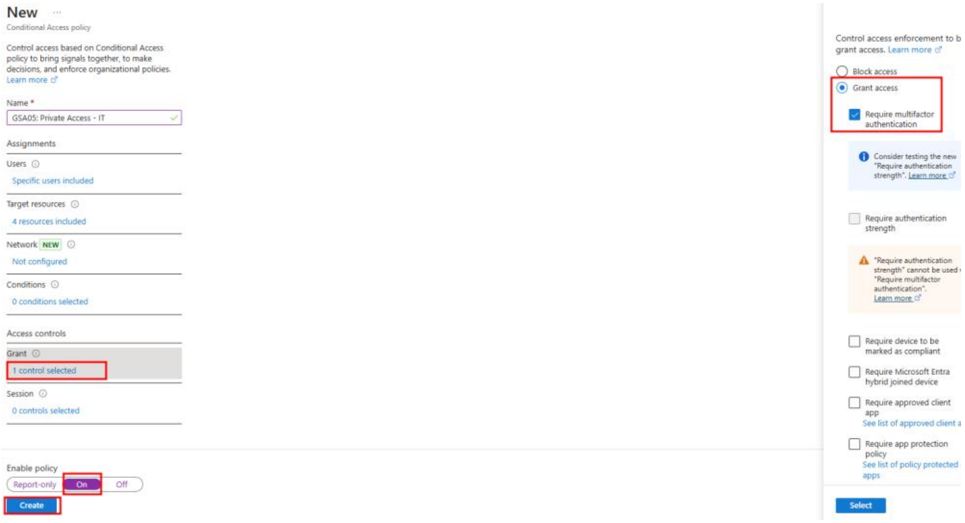
GS GSA-Privateaccesstrafficforwar...
1c9753f1-5519-4ff9-a41f-bc7cdc2fac67

GSA-ztrAnalyzer40
a2463451-28c7-483f-aa0f-aa45b5823686

Enable policy

Report-only [✓ On] Off

Grant Required access, enable policy and create the policy



New ···

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

GSA05: Private Access - IT

Assignments

Users ⓘ

Specific users included

Target resources ⓘ

4 resources included

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only [✓ On] Off

Create

Control access enforcement to b
grant access. Learn more

○ Block access

● Grant access

☑ Require multifactor authentication

Consider testing the new "Require authentication strength". Learn more

□ Require authentication strength

"Require authentication strength" cannot be used
"Require multifactor authentication".
Learn more

□ Require device to be marked as compliant

□ Require Microsoft Entra hybrid joined device

□ Require approved client app
See list of approved client a

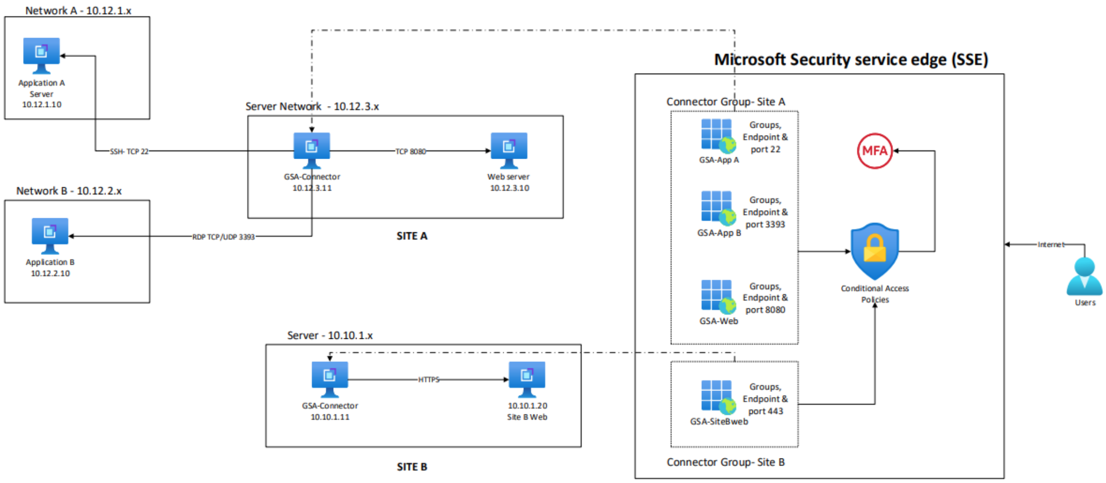
□ Require app protection policy
See list of policy protected
apps

Select

Implementation case:

Here we have two sites and four servers running different services. We will use Microsoft Entra Private access to allow these services.

Server	IP	Protocol	Site
Application A	10.12.1.10	TCP 22	SITE A
Application B	10.12.2.10	TCP/UDP 3389	SITE A
Web server	10.12.3.10	TCP 8080	SITE A
Site B web	10.10.1.20	TCP 443	SITE B



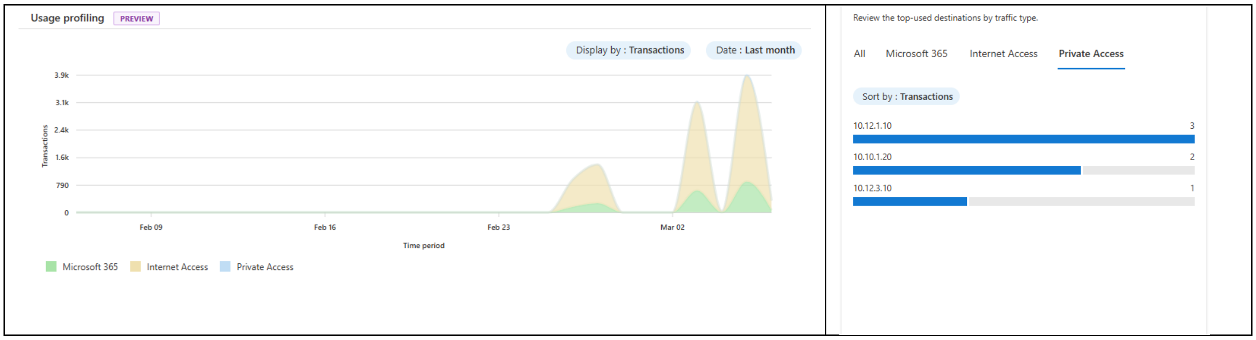
We have installed two connectors, one for each site. Then created two connector group named “SiteA-connector-group” and “SiteB-connector-group “

Now, we have created four “Enterprise Application” for all the four servers as follows;

Enterprise Application	Connector Group	App Segment	Protocol	Group
Application A	SiteA-connector	10.12.1.10	TCP 22	ITDept
Application B	SiteA-connector	10.12.2.10	TCP/UDP 3389	ITDept
Web server	SiteA-connector	10.12.3.10	TCP 8080	ITDept
Site B web	SiteB-connector	10.10.1.20	TCP 443	ITDept

Finally, Created a conditional access “GSA01: Private Access - IT” with User group “ITDept” and all the GSA Application as Target resource.

Now users can connect all the



Review the top-used destinations by traffic type.

10.12.1.10	3
10.10.1.20	2
10.12.3.10	1