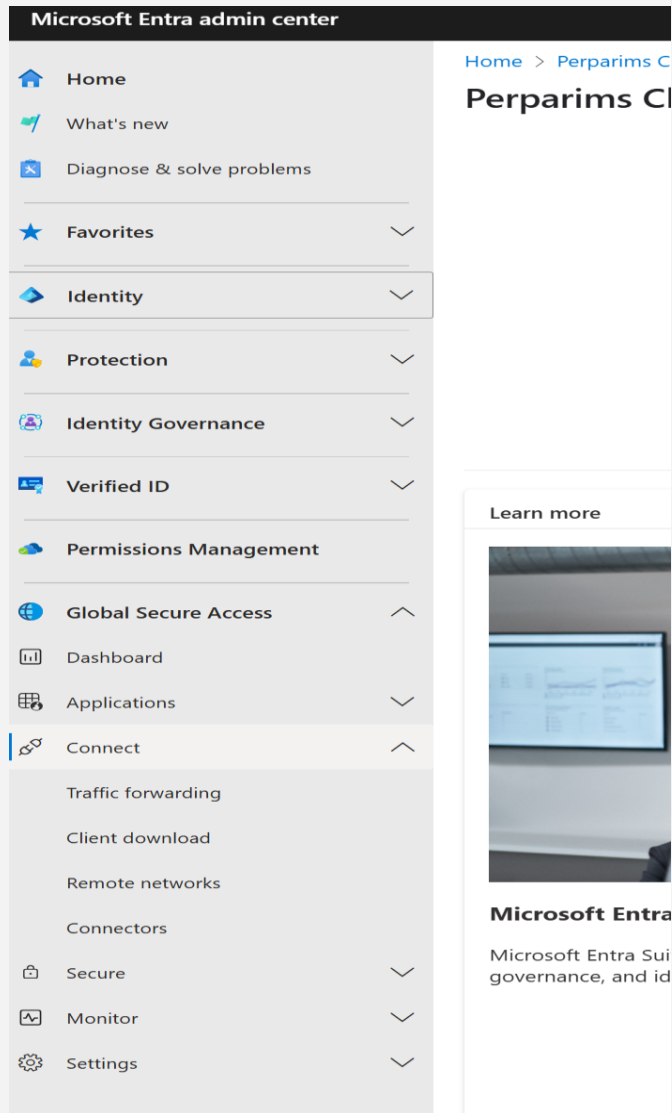


# Deploy Microsoft Global Secure Access Client

## Secure Internet and Microsoft 365 Access with Entra

[Home](#) > [Perparims Cloud Solutions](#) >  
Perparims Cloud Solutions



- Learn how to enable and deploy Microsoft's Global Secure Access client
- Explore Internet Access, Microsoft 365 Access, and Conditional Access policies
- Connect securely without relying on traditional VPN solutions
- Demonstrate Zero Trust enforcement through device and user authentication



#GlobalSecureAccess #ZeroTrust #MicrosoftEntra

# Activate Global Secure Access in Entra Portal

## Welcome to Global Secure Access

Microsoft Entra Internet Access and Microsoft Entra Private Access are unified under Global Secure Access. With Microsoft Entra Internet Access, secure access to all internet and software as a service (SaaS) apps and resources. Microsoft Entra Private Access is the new identity-centric Zero Trust Network Access (ZTNA) solution. [Learn more](#)

Activate

## Welcome to Global Secure Access

Microsoft Entra Internet Access and Microsoft Entra Private Access are unified under Global Secure Access. With Microsoft Entra Internet Access, secure access to all internet and software as a service (SaaS) apps and resources. Microsoft Entra Private Access is the new identity-centric Zero Trust Network Access (ZTNA) solution. [Learn more](#)

Get Started

[Home](#) > [Perparims Cloud Solutions](#) >

Perparims Cloud Solutions



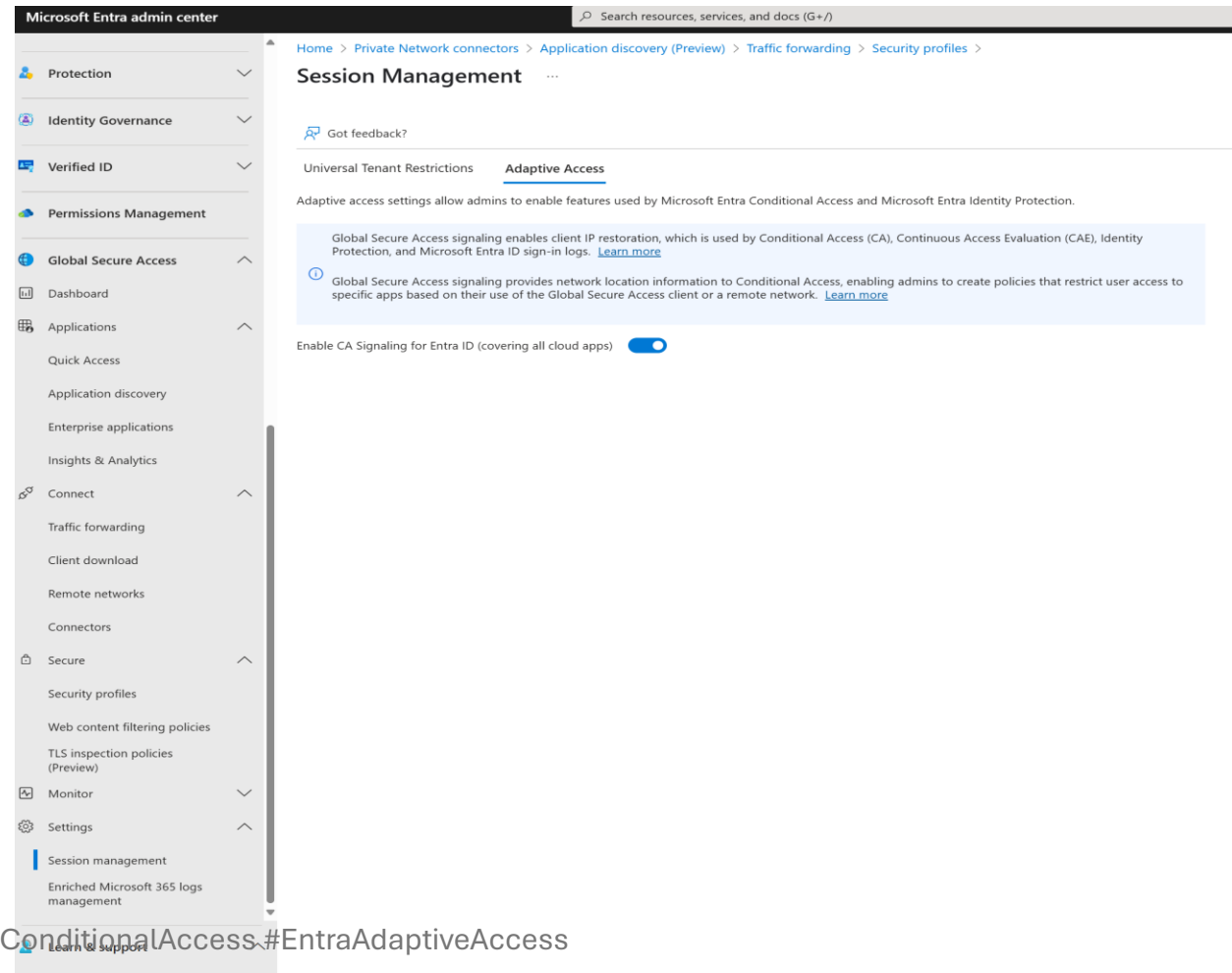
- Go to <https://entra.microsoft.com>
- In the left menu, scroll down to **Global Secure Access**
- Click on **Settings** → **Session Management**
- Under "Global Secure Access", click **Activate**
- Wait a few moments for activation to complete

# Turn On Adaptive Access for Conditional Policies

- In Entra Portal, stay in **Global Secure Access** → **Settings**
- Click **Session Management**
- Scroll to **Adaptive Access Settings**
- Enable the toggle:  
✅ *“Enable CA Signaling for Entra ID”*

## Why it Matters:

This lets Conditional Access policies recognize and work with the Global Secure Access client — key to Zero Trust enforcement.



# Activate the Microsoft Traffic Profile

Microsoft Entra admin center

Home > Traffic forwarding

To use these capabilities the following licenses may be required: Microsoft Entra Internet Access or Microsoft Entra Private Access. [Activate](#) or [Learn more](#)

Refresh | Got feedback?

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](#).

Profile Name	Status	Applies to	Microsoft traffic policies	Linked Conditional Access policies	User and group assignments	Remote network assignments
Microsoft traffic profile	Enabled	Internet traffic to Microsoft services	4 policies <a href="#">View</a>	2 policies <a href="#">View</a>	1 users, 0 groups assigned <a href="#">View</a>	0 assigned remote networks <a href="#">View</a>
Private access profile	Disabled	Private resources	Quick Access, 0 Applications	None	0 users, 0 groups assigned <a href="#">View</a>	Not applicable
Internet access profile	Disabled	All internet traffic, except for the Microsoft traffic profile	4 policies <a href="#">View</a>	2 policies <a href="#">View</a>	0 users, 0 groups assigned <a href="#">View</a>	Not applicable

- Navigate to **Global Secure Access > Connect > Traffic Forwarding**
- Locate the **Microsoft traffic profile** section
- Click the **toggle** to enable the profile
- Assign it to **your user account** to apply the settings
- This profile secures traffic to Microsoft 365 services like Entra ID, Exchange, and SharePoint

# Customize Microsoft 365 Traffic Forwarding

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > Traffic forwarding

To use these capabilities the following licenses may be required: Microsoft Entra Internet Access

Refresh | Got feedback?

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign users running the Global Secure Access client. For clientless devices, use the Microsoft profile to connect. [Learn more](#)

One or more profiles are configured and ready to use. To finish setup, Download [Global Secure Access](#)

**Microsoft traffic profile**  
Enabled  
Last modified on 06/07/2025, 12:54 PM

Applies to  
Internet traffic to Microsoft services

Microsoft traffic policies  
4 policies [View](#)

Linked Conditional Access policies  
2 policies [View](#)

User and group assignments  
1 users, 0 groups assigned [View](#)

Remote network assignments  
0 assigned remote networks [View](#)

Tenant is missing the needed license (Microsoft Entra Private Access) to use this profile.

Private access profile  
Disabled  
Last modified on 06/07/2025, 12:54 PM

Applies to  
Private resources

Private access policies  
Quick Access, 0 Applications

Linked Conditional Access policies  
None

User and group assignments  
0 users, 0 groups assigned [View](#)

Remote network assignments  
Not applicable

**Policies & rules (Microsoft access profile)**  
Traffic Profile

Remote networks acquire IP-identifiable traffic only.

Please note that we are working on acquiring additional Microsoft traffic. [Learn more](#)

Policy	Enable/Disable	Destination
> Exchange Online	<input checked="" type="checkbox"/>	
> Skype for Business Online and Microsoft Teams	<input checked="" type="checkbox"/>	
> SharePoint Online and OneDrive for Business	<input checked="" type="checkbox"/>	
> Microsoft 365 Common and Office Online	<input checked="" type="checkbox"/>	

- Click **View** under *Microsoft Traffic Policies*
- Expand services like:
  - **Exchange Online**
  - **SharePoint Online**
  - **Microsoft Entra ID & Microsoft Graph**
- Choose whether to **Forward** or **Bypass** each service
- Forwarding ensures traffic is inspected via Global Secure Access policies
- Save changes after setting your preferences

#SecureAccess #TrafficPolicy #ConditionalAccess  
#MicrosoftCloud

# Assign the Traffic Profile to Users

The screenshot displays the Microsoft Entra admin center interface. The left sidebar shows the navigation menu with 'Traffic forwarding' selected under 'Global Secure Access'. The main content area is titled 'Traffic forwarding' and includes a warning about required licenses, a 'Manage traffic forwarding profiles' section, and a list of three profiles: 'Microsoft traffic profile' (Enabled), 'Private access profile' (Disabled), and 'Internet access profile' (Disabled). The 'User and group assignments' pane on the right is open for the 'Microsoft traffic profile', showing 'Assign to all users' set to 'No' and '1 users, 0 groups assigned'.

- Still in the *Microsoft Traffic Profile* section
- Click **Assign** to specify who this profile applies to
- Choose **All users** or select **specific users/groups**
- Click **OK** to confirm assignment
- Assigned users will have traffic policies applied via Global Secure Access

UserAssignment #Microsoft365Security  
#GlobalSecureAccess

# Deploy the Global Secure Access Client

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

PerparimAbdullah@PERPARIMS CLOUD SOLUTIONS

Home > Traffic forwarding >

## Client download

A supported client or app can be used to tunnel network traffic from a device to the Global Secure Access service. The installation can be interactive or silent, using a mobile manager such as Microsoft Intune. [How to download the Global Secure Access Windows client](#)

Windows

Windows 10/11

[Download Client](#)

System requirements

- Windows 10/11
- Microsoft Entra joined
- Local admin permissions

> Android

> iOS [PREVIEW](#)

> macOS [PREVIEW](#)

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Downloads

GlobalSecureAccessClient.exe

[Open file](#)

[See more](#)

Global Secure Access Client Setup

Global Secure Access Client

Installation Successfully Completed

[Close](#)

Home > Traffic forwarding >

## Client download

A supported client or app can be used to tunnel network traffic from a device to the Global Secure Access service. The installation can be interactive or silent, using a mobile manager such as Microsoft Intune. [How to download the Global Secure Access Windows client](#)

Windows

Windows 10/11

[Download Client](#)

System requirements

- Windows 10/11
- Microsoft Entra joined
- Local admin permissions

> Android

> iOS [PREVIEW](#)

> macOS [PREVIEW](#)

Client download

Remote networks

Learn & support

- Go to [entra.microsoft.com](https://entra.microsoft.com)
- Navigate to: **Global Secure Access** → **Connect** → **Client Download**
- Download and run the client installer on a supported Windows device (physical or VM)
- Follow the installation steps to complete setup
- After install, the client appears in the system tray

#SecureAccessClient #Windows10 #CloudSecurity

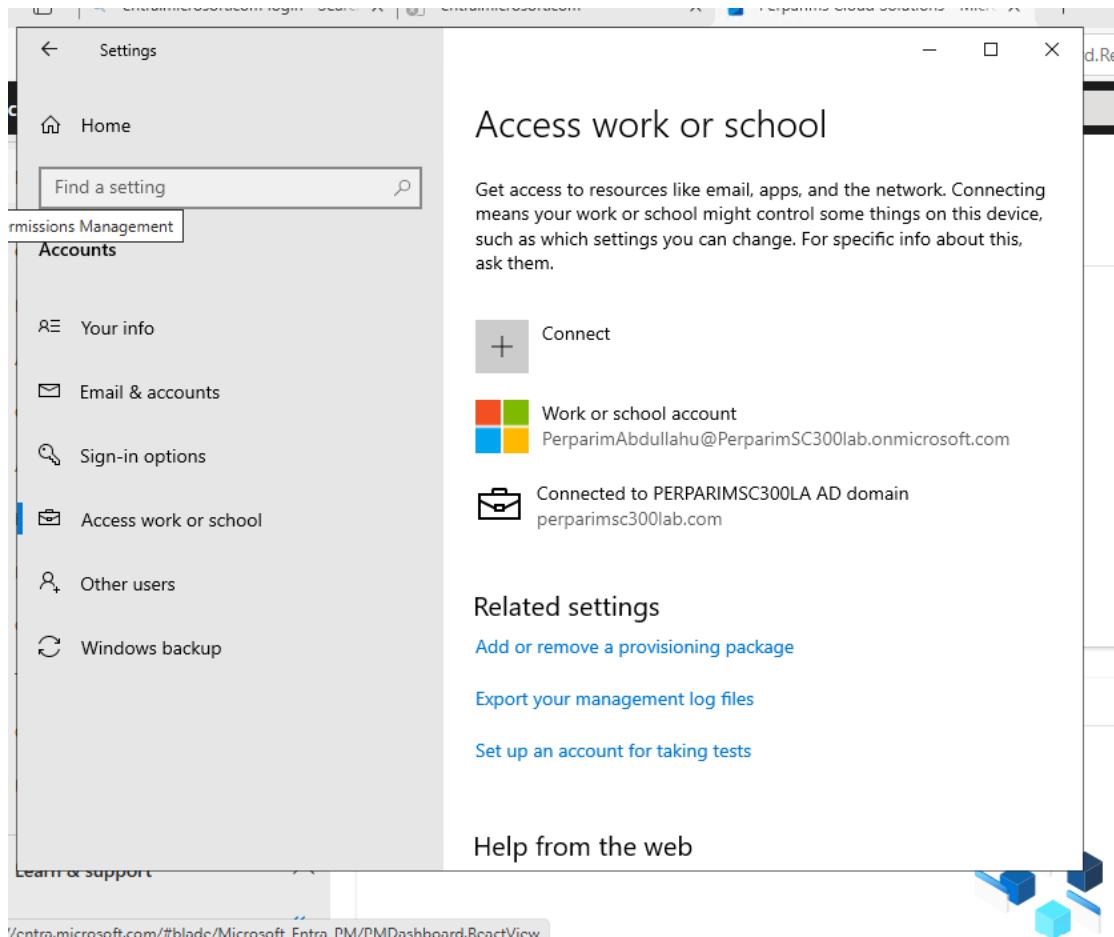


# Validate Client Connection & Health

- After installation, right-click the **Global Secure Access Client** in the system tray
- Select **Advanced Diagnostics**
- Check:
  - 🗝️ **Authentication Status** (should say “Authenticated”)
  - 💻 **Device Join Status** (should show Microsoft Entra ID joined)
  - 🌐 **Forwarding Profile** (should reflect your enabled profiles like Microsoft 365 Traffic)



# Global Secure Access Client – Entra ID Join Check

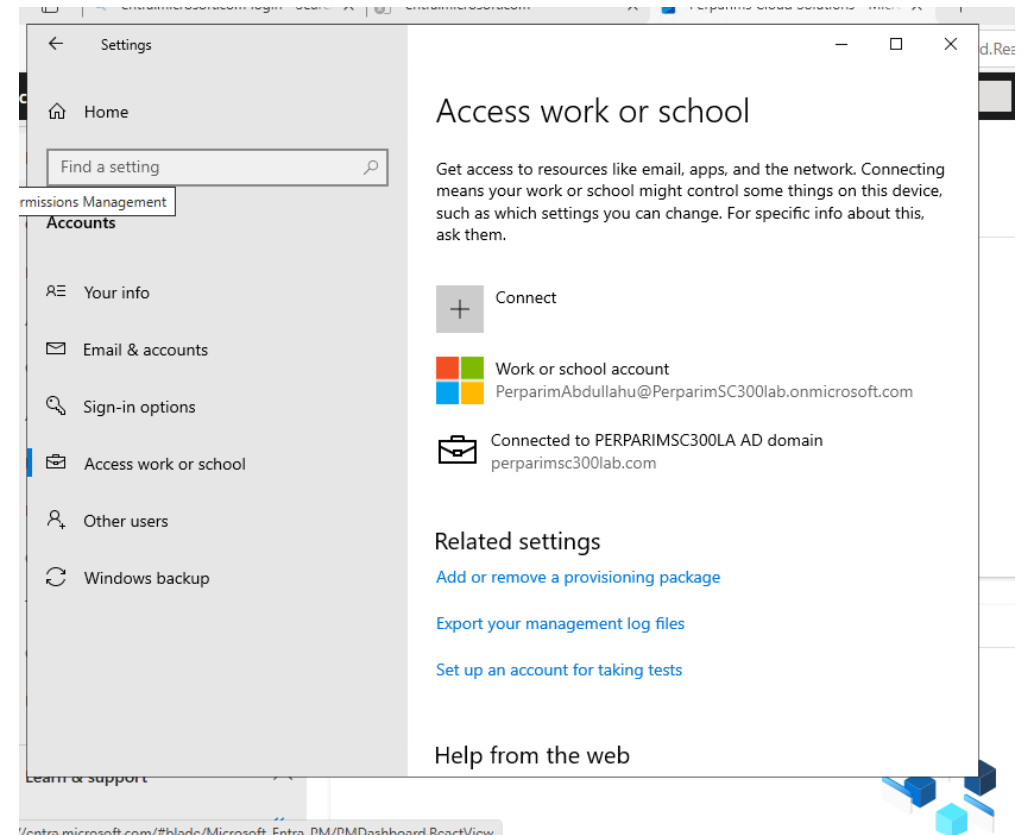


- Current VM is **not Entra ID Joined** (shows as MicrosoftEntraJoined: No)
- As a result, the **GSA Client displays a "Disconnected" error**
- In production, the device must be:
- **Microsoft Entra Joined**
- **Microsoft Entra Registered**
- **or Hybrid Joined**
- This join status is required for:
- Conditional Access to take effect
- Traffic Forwarding rules to apply
- For demo purposes, we're continuing without full join

"Note: In this lab, our test VM isn't joined to Entra ID, so the GSA client shows Disconnected. In real-world deployments, proper device registration ensures full integration with Conditional Access and Traffic Forwarding profiles."

# Why My Device Shows “Disconnected” in GSA Client?

- Client shows **Disconnected** because device is not Microsoft Entra Joined
- GSA requires device to be joined to Microsoft Entra ID to authenticate the user
- Common in lab VMs or personal machines not enrolled or joined
- Joining device would require using Microsoft Entra ID user during device setup or enrollment
- Since this is a test VM, we skipped device join intentionally



# Global Secure Access – Summary & Lessons Learned

- Global Secure Access provides **modern zero trust connectivity**
- Combines **Internet Access, Private Access, and Microsoft Traffic Access**
- Requires proper licensing (Microsoft 365 E5 or Entra P1/P2)
- Devices must be **Microsoft Entra Joined** for full functionality
- Conditional Access controls and traffic forwarding profiles increase security posture
- Ideal for **remote workers** and cloud-first organizations



[Home](#) > [Perparims Cloud Solutions](#) >  
Perparims Cloud Solutions ...

