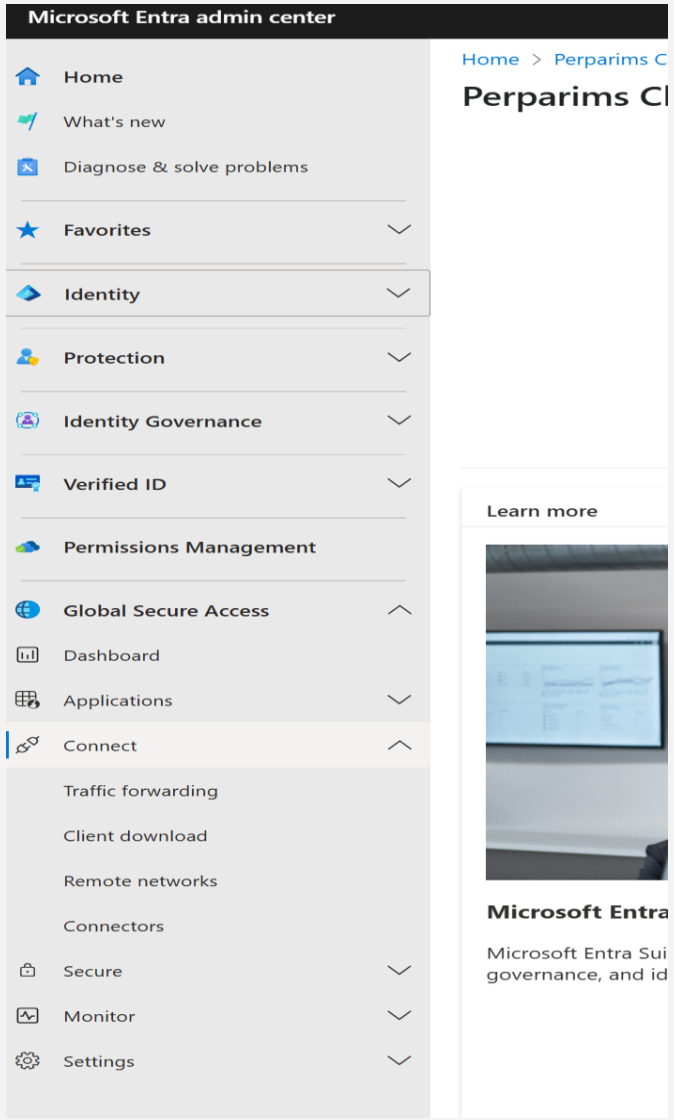
Deploy Microsoft Global Secure Access Client

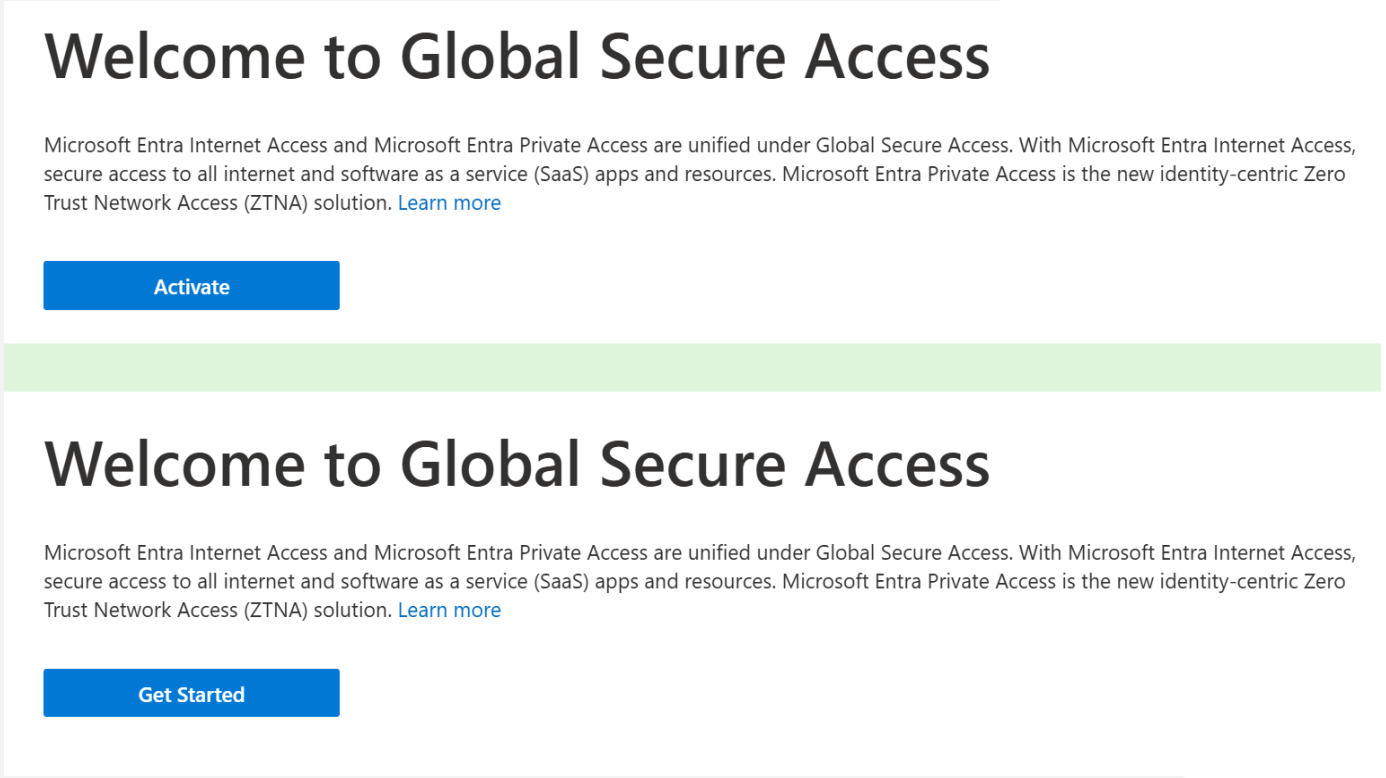
Secure Internet and Microsoft 365 Access with Entra



- 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

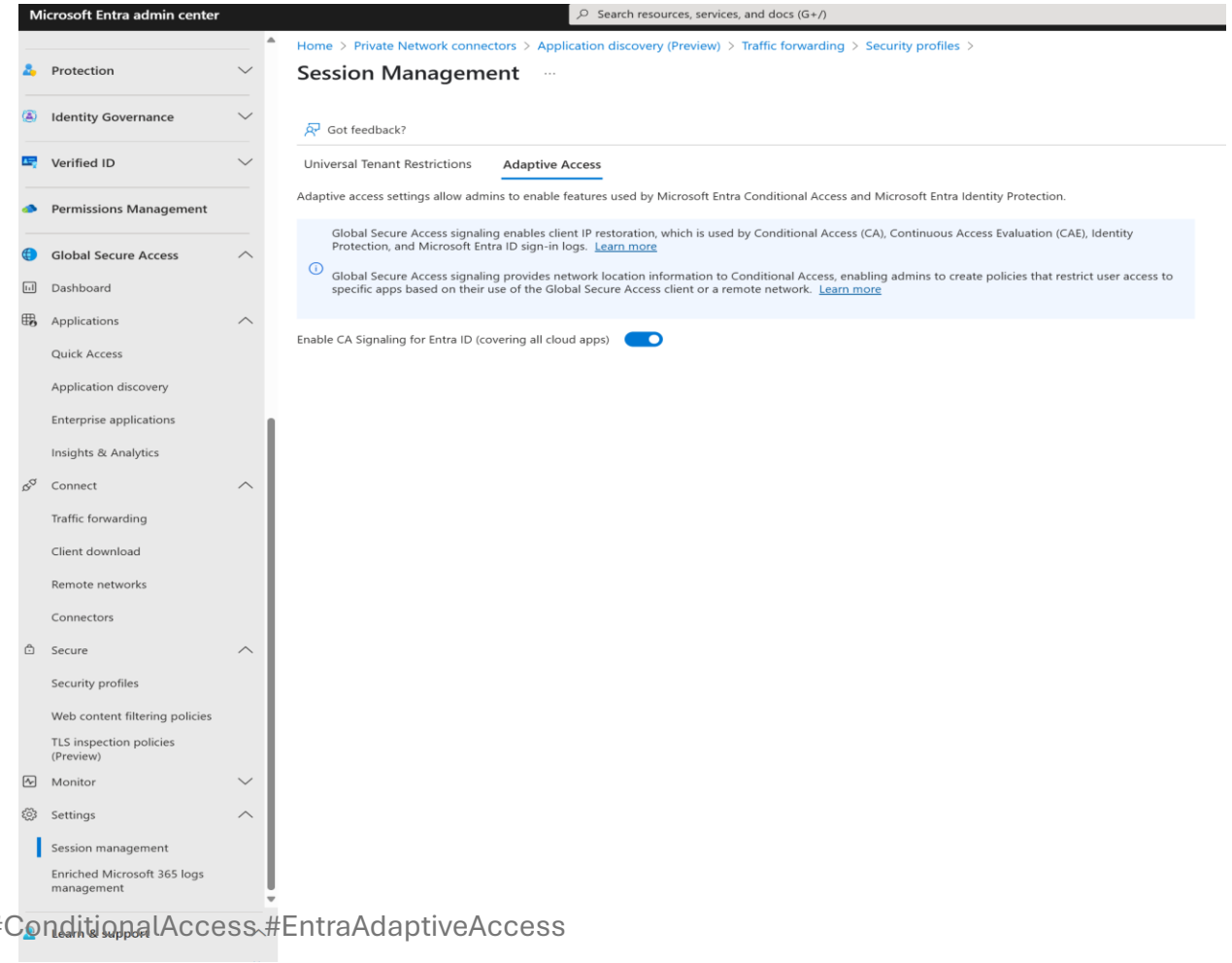


- Go to https://entra.microsoft.com
- In the left menu, scroll down to **Global Secure Access**
- Click on **Settings → Session Management**
- Under "Global Secure Access", click **Activate**
- Wait a few moments for activation to complete

#EntraPortal #SecureAccess #ActivationStep

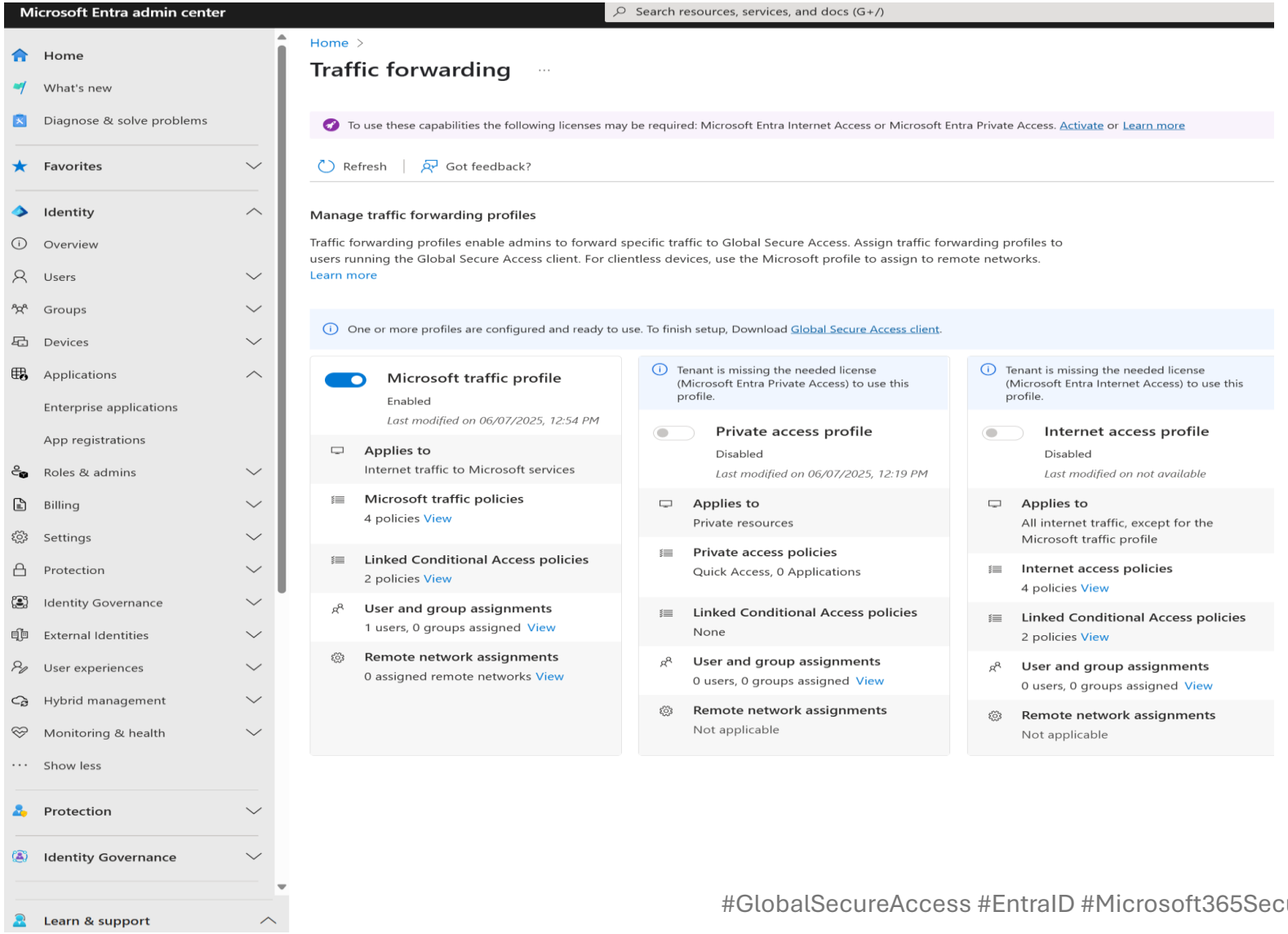
Turn On Adaptive Access for Conditional Policies

- 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.

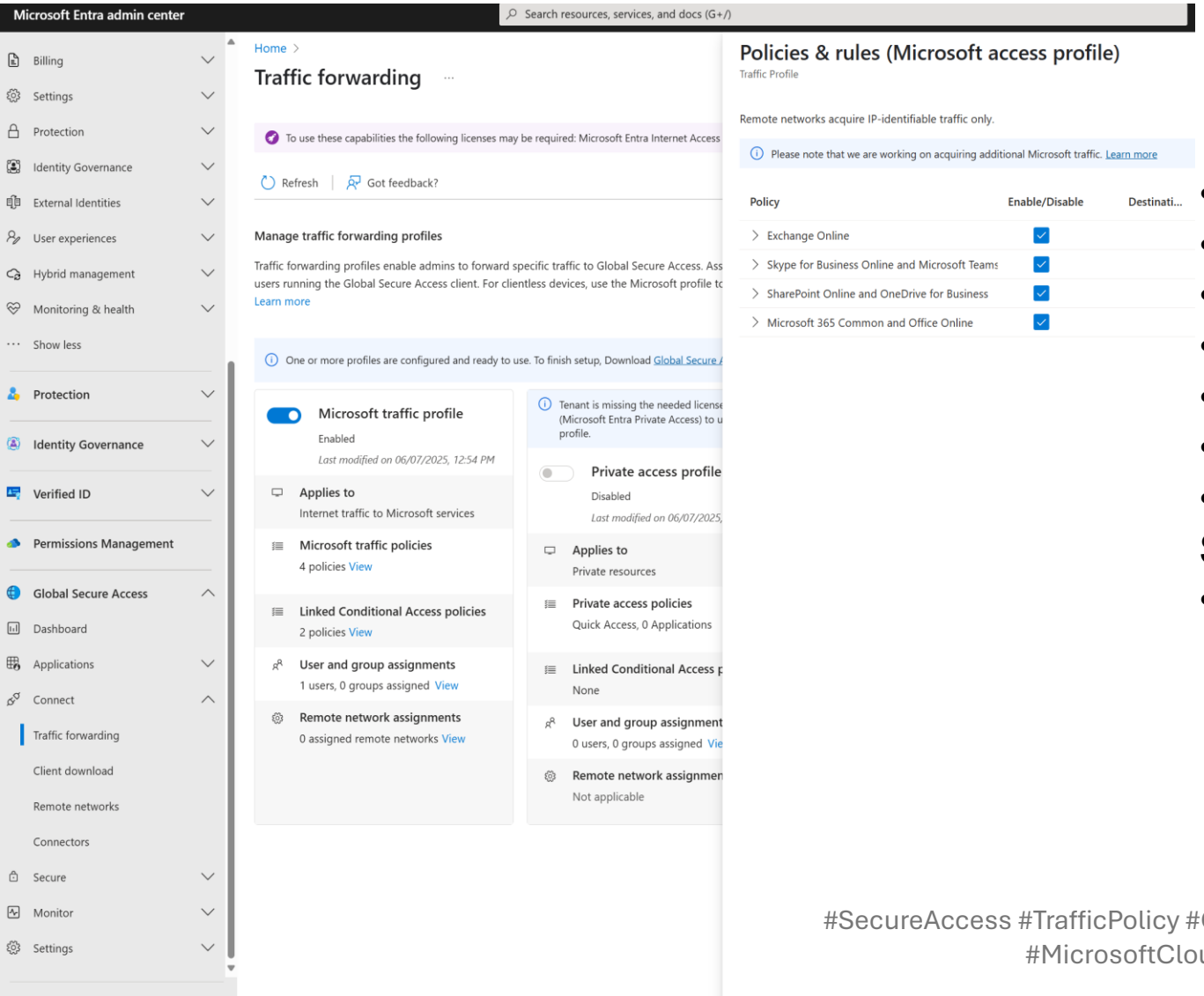
Activate the Microsoft Traffic Profile



- 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

#GlobalSecureAccess #EntraID #Microsoft365Security

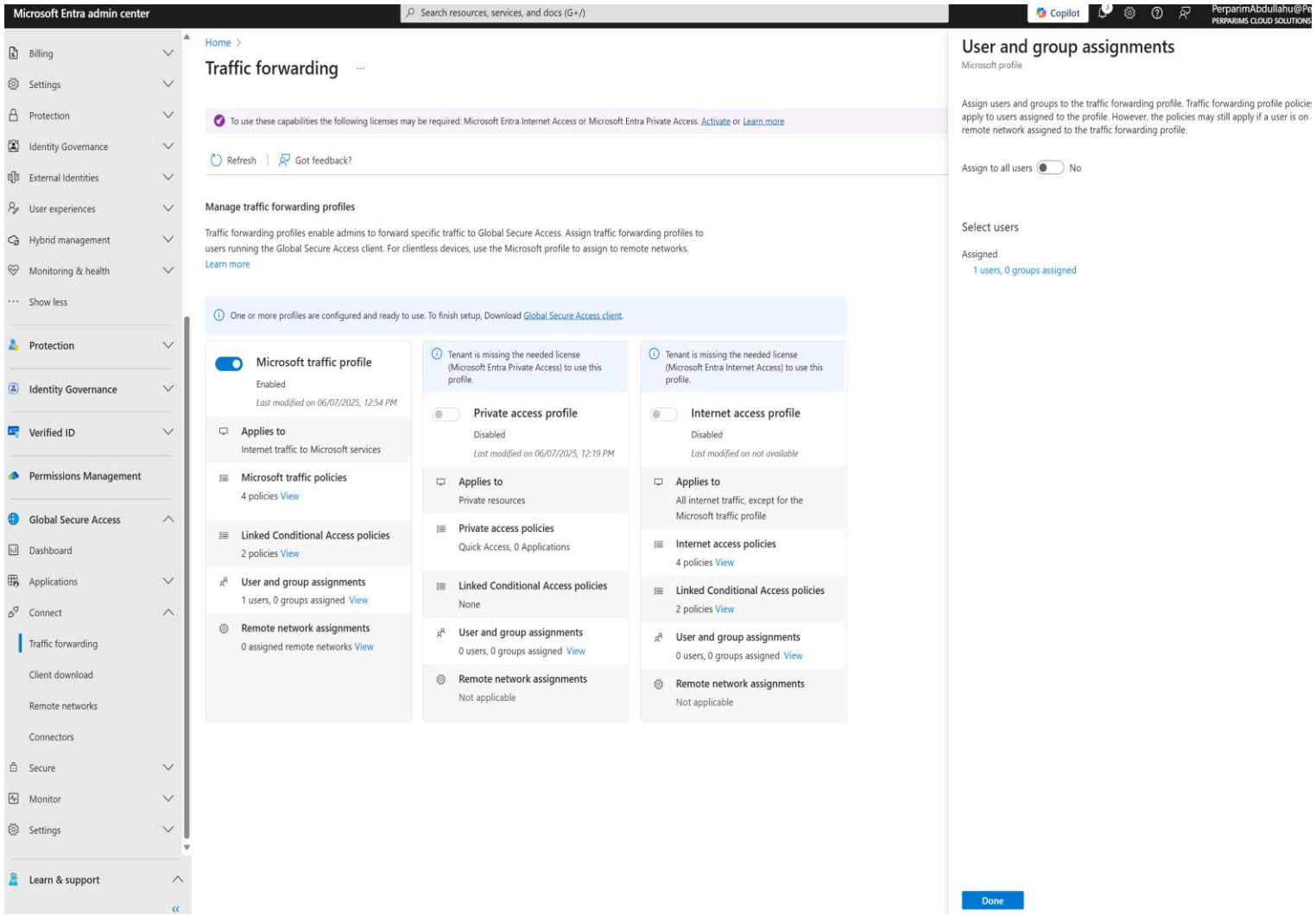
Customize Microsoft 365 Traffic Forwarding



- 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

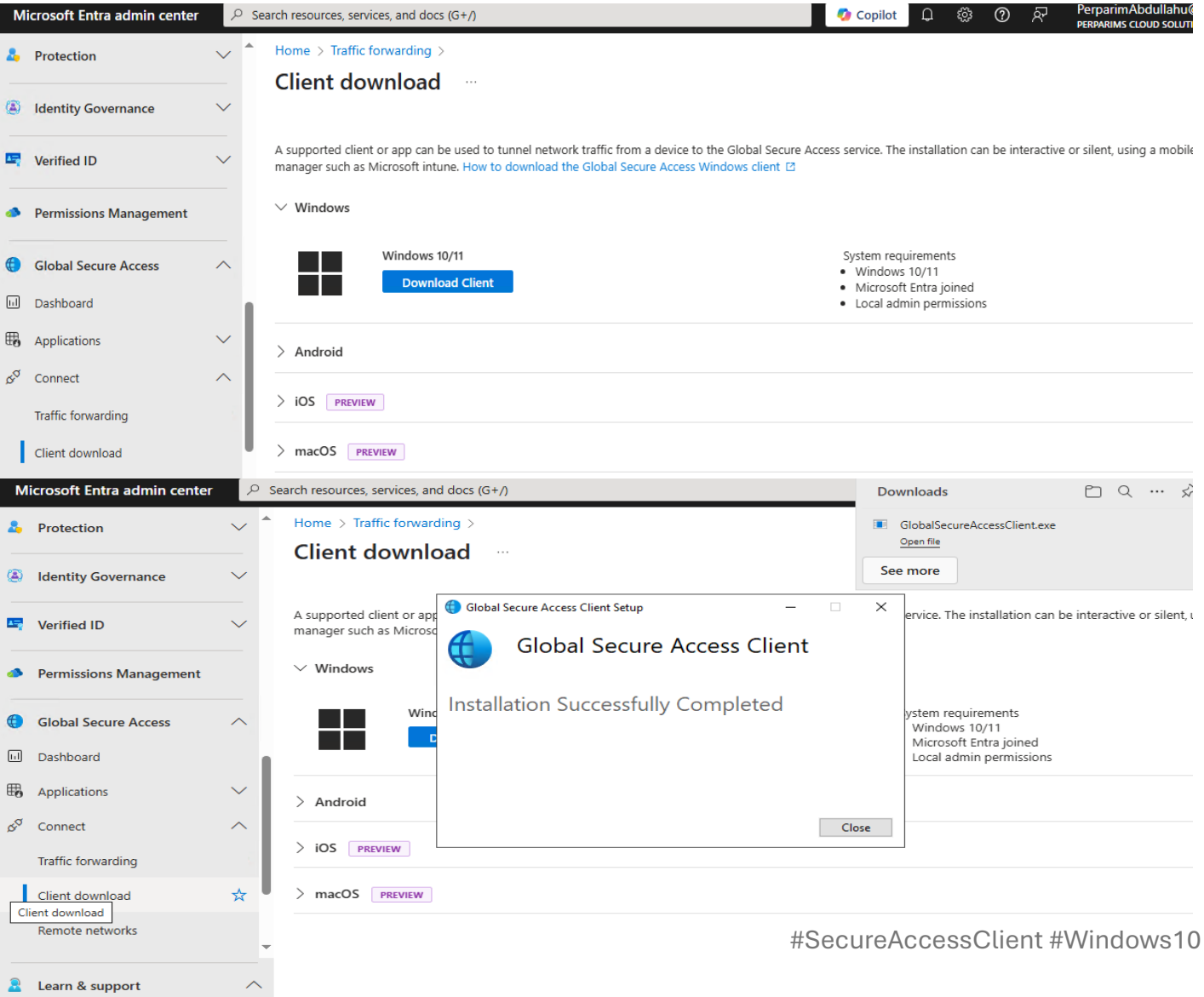
Assign the Traffic Profile to Users



- 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



- Go to 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

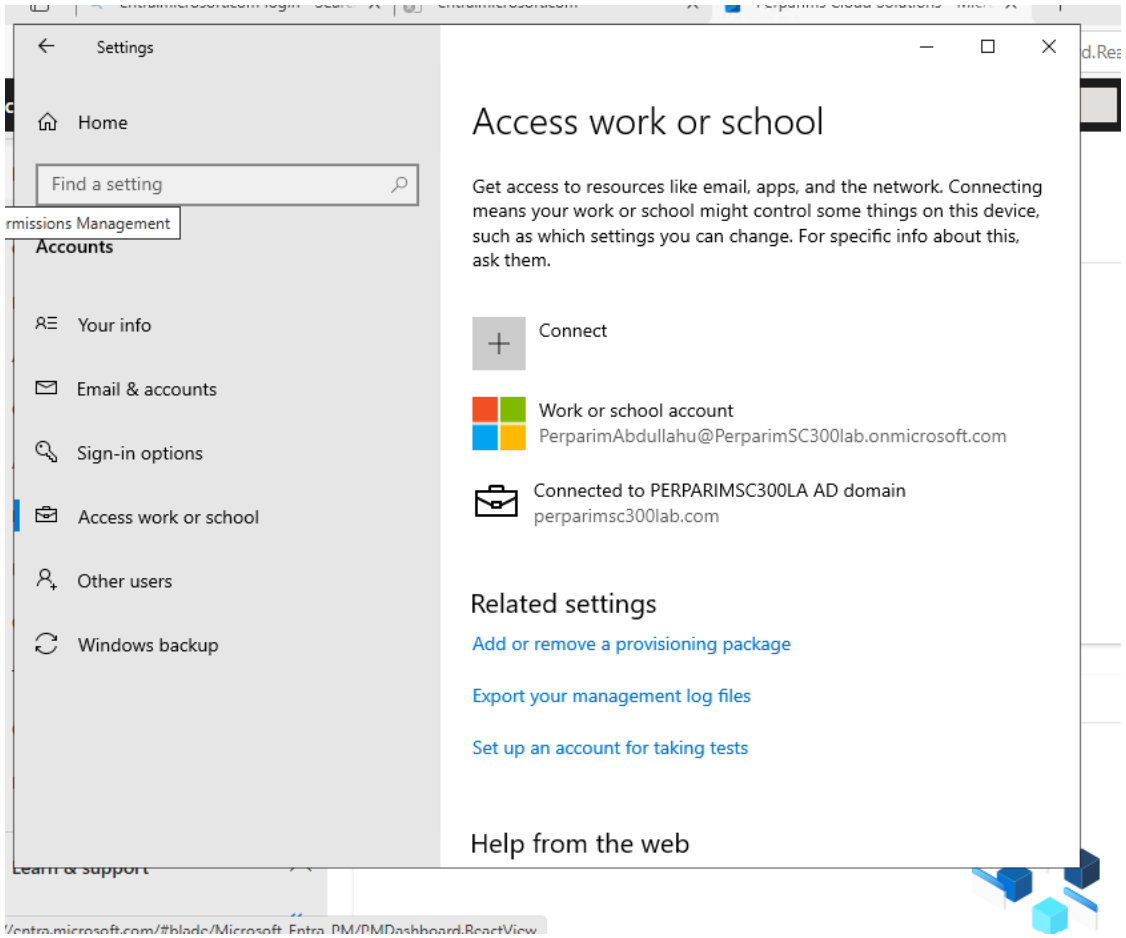
#SecureAccessClient #Windows10 #CloudSecurity

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)

✅ #ClientHealthCheck #EntraSecureAccess #Diagnostics

Global Secure Access Client – Entra ID Join Check



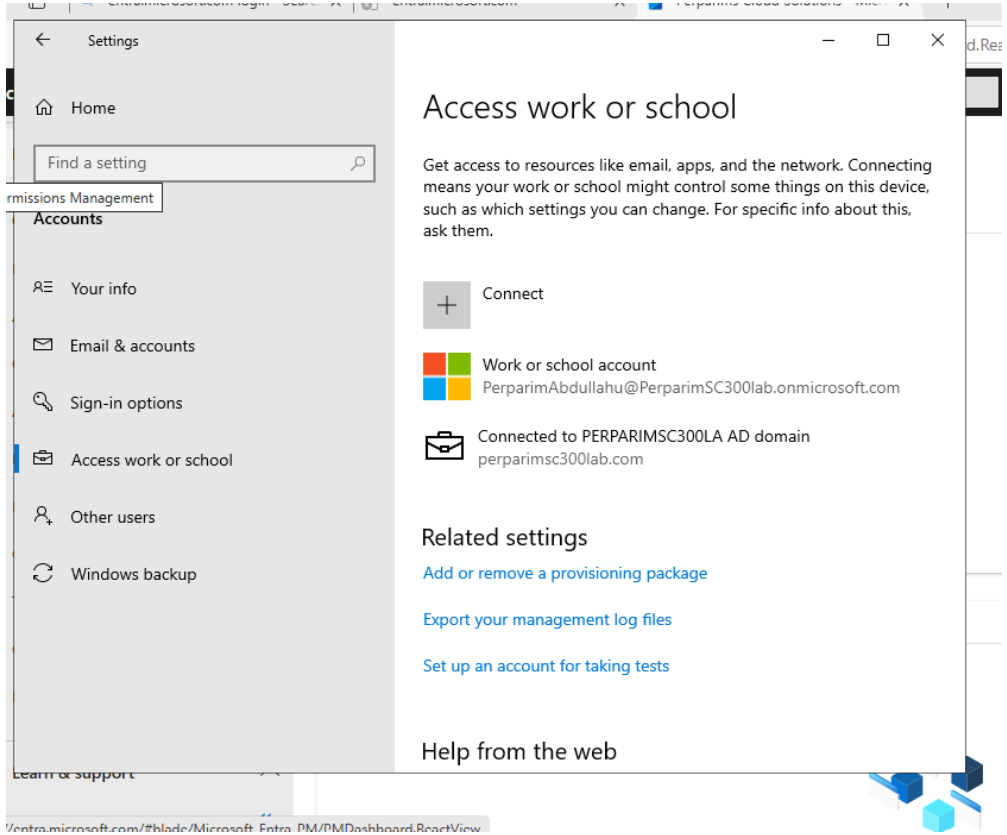
- Current VM is **not Entra ID Joined** (shows as MicrosoftEntraJoined: No)
- As a result, the **GSA Client displays a "Disconnected" error**
- In production, the device must be:
- **Microsoft Entra Joined**
- **Microsoft Entra Registered**
- or **Hybrid Joined**
- This join status is required for:
- 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."

#EntraIDJoin #LabDemo #GlobalSecureAccess #ZeroTrust

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

🔐 #ZeroTrust #MicrosoftSecureAccess #CloudSecurity #PerparimLabs