**Global Secure Access**

Contoso, whose IT infrastructure is all cloud-based, has recently acquired Tailwind Traders, which has not yet migrated its infrastructure to the cloud. Tailwind Traders has an on-premise environment with file servers containing private resources that Contoso users need to access. Until these resources can be migrated to the cloud, the security team wants to ensure secure access to these private resources, but wants to avoid using VPN technology.

**Design Approach**

Microsoft Entra Private Access allows its employees to securely remote into local servers within Tailwind Traders' local infrastructure and integrates with the existing cloud infrastructure of Contoso Ltd.

Microsoft Entra Private Access is part of the Microsoft Global Secure Access solution, which enables secure and seamless access to any app or resource from anywhere. It is built on the principles of Zero Trust and delivered from Microsoft's Wide Area Network. One compelling use case is remote access to private resources. Microsoft Entra Private Access allows users to securely access private resources hosted on-premises without exposing them to the internet or requiring a VPN. This reduces the attack surface and simplifies network configuration

**Proposed solution**

In this exercise, you'll set up a remote access connection from your client endpoint to a resource in your on-premise environment, using Microsoft Entra Private Access.

| **Requirement** | **Solution** | **Action plan** |
| --- | --- | --- |
| Enable secure remote access for an on-premises server, without VPN | Global Secure Access - Private Access | Enable Global Secure Access and deploy Private Access Network Connector |
| Remote users connect to private apps in the private network. | Global Secure Access - Private Access | Enable Private Access traffic profile, install GSA client, and assign users. |

**Task 1: Activate Global Secure Access**

The first step is to activate Global Secure Access in your tenant.

1. If you completed the setup lab, you should still be in the **LON-SC1** VM (the client endpoint). If not, log in to the **LON-SC1** VM as the local **Admin**. The password should be provided by your lab hosting provider.
2. Open a new browser tab in **Microsoft Edge**, select the address bar, and navigate to [**https://entra.microsoft.com**](https://entra.microsoft.com/). You should already be logged into the Entra Portal as **MOD Administrator** [admin@WWLxZZZZZZ.onmicrosoft.com](mailto:admin@WWLxZZZZZZ.onmicrosoft.com) (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). The user´s password should be provided by your lab hosting provider.
3. If you see an information box on the top right of the screen that says **Manage multifactor authentication**, close it by selecting the **X**.
4. In the left navigation pane, expand **Global Secure Access** and select **Dashboard**.
5. Under **Activate Global Secure Access in your Tenant,** select **Activate**.

You have successfully activated Global Secure Access.

**Task 2: Enable TLS and install the private network connector**

The private network connector is a lightweight agent that is installed on a Windows Server, in your on-premise environment, that has access to the backend resources and applications, and is used to facilitate the connection to the Global Secure Access service. The Windows server where the connector will be installed must have TLS 1.2 enabled before you install the private network connector.

1. Log into the Server VM, **LON-SC2**, using the local **Administrator** account. The password should be provided by your lab hosting provider.
2. When you log in to the VM, Server Manager will open. You can minimize this window.
3. Before you install the private network connector on the server, you need to enable TLS 1.2. There are several ways you can do this. For this exercise, you'll copy the commands to set the registry keys into a file and then run that file.
   1. Open **Microsoft Edge**.
   2. On a browser tab, enter the URL: **https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-connectors**, then press the enter key on your keyboard to open the product documentation.
   3. Scroll down to the section **Transport Layer Security (TLS) requirements** and from the code box listed under **Set registry keys**, select **Copy**
   4. From within the VM, you'll open Notepad. In the taskbar's search field, type **Notepad**, then select **Notepad** to open the application.
   5. Use **Ctrl + v** to paste the code into Notepad. Do NOT change anything in the pasted code. The first line of code is required.
   6. From Notepad, select **File**, then select **Save as**.
   7. In the **Save as type** field, select **All files** from the drop-down, and in the **File name** field, enter **EnableTLS.reg**, then select **Save**. You must save the file with the .reg extension. Take note of where the document is saved, then close Notepad.
   8. From the taskbar, open **File Explorer** and navigate to the folder where you saved the file (the default is This PC > Documents).
   9. Double-click the file name, **Enable-TLS**, to run it. Because you are changing the registry file, you are asked, **Are you sure you want to continue?** Select **Yes**, then select **Ok**.
   10. Since you updated the registry, you'll need to restart the server. From the taskbar of the Server VM, select the **Windows icon**, select **Power**, select **Restart**, then select **Continue**.
   11. After the restart, log back in to the Server VM, as the local **Administrator**.
   12. Minimize or close Server Manager.
4. Open **Microsoft Edge**, select the address bar, navigate to **https://entra.microsoft.com**, and log in to the Entra Portal as **MOD Administrator** [admin@WWLxZZZZZZ.onmicrosoft.com](mailto:admin@WWLxZZZZZZ.onmicrosoft.com) (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). User´s password should be provided by your lab hosting provider.
5. Dismiss the dialog boxes, as you did in the previous task.
6. From the left navigation panel, expand **Global Secure Access**, expand **Connect**, and select **Connectors**.
7. From the top of the Private Network connectors page, select **Download connector service**.
8. Review the information, then select **Accept terms & Download**.
9. From the downloads window on the top right corner of the page, when the download is complete, select **Open file**. If the downloads window closed before you were able to select Open file, select **File Explorer** from the taskbar, go to the **Downloads** folder, then run the file **MicrosoftEntraPrivateNetworkConnectorInstaller**.
10. Select the box next to **I agree to the license terms and conditions** then select **Install**.
11. During the installation process, you have to sign in with the username and password for the MOD Administrator. It can take a couple of minutes to complete the installation.
12. Once the installation is complete, **close** the installation window and refresh the browser page. You should see the connector listed and active.
13. In the Windows search bar, on the taskbar, enter **cmd** then select **Command Prompt**.
14. In the Administrator: Command Prompt window, run the **ipconfig** command, make note of the private IP address for your server, then close the Command Prompt window.

You've successfully installed the private network connector on your on-premise server.

**Task 3: Create a folder on the File Server**

In this task, you´ll create an SMB Share on the on-premise file server that will be accessed through GSA.

1. You should still be logged in to LON-SC2.
2. From the taskbar, open **File Explorer**, navigate to the C: Drive, and create a folder named **Share**.
3. Using the right mouse key, select the **Share** Folder and select **Properties**.
4. From the Share Properties window, select the **Sharing** tab.
5. Select **Share...**.
6. From the dropdown, select **Everyone** and select **Add**.
7. Select **Share**.
8. Select **No, make the network that I am connected to a private network**.
9. Select **Done**, then **Close**.
10. Minimize or close File Explorer.

You've created a shared folder on the server. It is this folder and its content that you'll access through GSA.

**Task 4: Set up Quick Access and assign User**

Private Access provides two ways to configure the private resources that you want to tunnel through the service. Quick Access or Global Secure Access applications. For this exercise, you'll use Quick Access.

Quick Access is the primary group of FQDNs and IP addresses that you want to secure. When you configure the Quick Access, you're creating a new enterprise application that serves as a container for the private resources that you want to secure.

For your users to access the resources on the file server through the GSA client, you need to enable Quick Access and assign it to your test users.

1. You can stay in LON-SC2 for this step.
2. In the left navigation pane, expand **Global Secure Access**, expand **Applications**, then select **Quick Access**. Enter the following information:
   * Name: **SMB to ContosoFS**
   * Connector Group: **Default**
3. Select **Add Quick Access application segment** and fill in the following information:
   * Destination type: **IP address**
   * IP address: the private IP address of your server that you noted in the earlier step, **192.168.2.100**.
   * Ports: **445**
4. Select **Apply**.
5. Select **Save**. Once you see the status field for the application segment show success, refresh the browser page. Upon refreshing the page, you're taken to the **Quick Access | Network access properties** page.
6. On the left, select **User and groups**.
7. Select **Add user/group**.
8. Select **None Selected**.
9. In the search field, enter **MOD Administrator**, then select it from the search results.
10. From the bottom of the page, press **Select**, then select **Assign**.

You have successfully enabled quick access for your test user.

**Task 5: Device join Entra ID**

To use Global Secure Access, you need to join the client endpoint, the LON-SC1 VM, to Microsoft Entra ID. Otherwise, the GSA client will not work.

1. Switch back to the **LON-SC1** VM (this is your client endpoint VM)
2. Using the right mouse key, select the Windows icon in the taskbar and select **Settings**.
3. From the left navigation panel, select **Accounts**.
4. From the Accounts page, select **Access work or school**.
5. To add a work or school account, select **Connect**.
6. From the bottom of the window, select **Join Device to Microsoft Entra ID**.
7. Sign in with your **MOD Administrator** admin credentials provided by the lab provider.
8. **Make sure this is your organization** window, review the information, then select **Join**.
9. Review the information on the **You're all set** window and select **Done**.
10. Now that your device is Entra ID joined with your MOD administrator account, you need to log in using that account.
    1. From the taskbar, select the **Windows** icon, select **Admin**, then select **Sign out**. Once the words **Signing out** disappear from the screen, select the display icon in the top left corner of the VM window and select **Reconnect**. Alternatively, you may hear an alert and see a pop-up in the instruction panel asking to reconnect.
    2. From the bottom left of the window, select **Other user**, then log in with your MOD administrator account.
    3. It will take a few minutes to set up the account, then you'll see a **More information required** window appear. This will initiate the process to set up multifactor authentication. Follow the instructions to set up MFA.

Once your endpoint is joined to Entra ID, you will be able to set up the GSA client, which is used to connect to any resources you are protecting with Global Secure Access.

**Task 6: Activate the traffic forwarding profile and download the GSA desktop client**

To enable access to private resources or applications in your on-premises environment, you need to enable the traffic forwarding profile for Private Access and assign users.

You also need to download and install the Global Secure Access desktop client.

Private access traffic can be forwarded to the service by connecting through the Global Secure Access desktop client.

1. You should still be on **LON-SC1**, to which you have signed in with your MOD Administrator account.
2. Open **Microsoft Edge**. You'll be prompted to set up Microsoft Edge.
3. From the Microsoft Edge, navigate to **https://entra.microsoft.com**.
4. From the left navigation panel, expand **Global Secure Access**, expand **Connect**, and choose **Traffic forwarding**. You may need to expand the left navigation panel by selecting **>>** to view the options.
5. Select the slider button next to **Private access profile**, then select **OK**.
6. Now that you've enabled the private access profile, you'll need to assign users.
   1. From the Private access profile card, under **User and group assignments**, select **View**.
   2. Select where it says **0 users, 0 groups assigned**
   3. Select **Add user/group**.
   4. Select **None Selected**.
   5. In the search bar, enter **MOD Administrator**, select **MOD Administrator**, press **Select**, then select **Assign**.
7. In the left navigation pane under **Connect,** choose **Client download**.
8. Under Windows 10/11, select **Download client**.
9. From the Downloads window, select **Open file**. If the downloads window closed before you were able to select Open file, select **File Explorer** from the taskbar, go to the **Downloads** folder, then run the file **GlobalSecureAccessClient**.
10. Select **I agree to the license terms and conditions**, then select **Install**. In the User Account Control window that pops up, select **Yes**.
11. Once the installation completes, **close** the window.
12. From the taskbar, select the up arrow to show hidden icons. Here you will see the Global Secure Access client icon. If it does not have a green checkmark, right-click the icon and select **Enable**. It may take several minutes to show with a green checkmark to indicate it is connected.
13. From the taskbar, select **File Explorer** and navigate to **This PC**. Select the ellipses (**...**) and select **Map network drive**.
14. In the Folder field, enter \\192.168.2.100\Share. Use the IP address you noted earlier AND select **Connect using different credentials**.
15. Select **Finish**.
16. To map the network drive, use the credentials for the local administrator account on LON-SC2.
    1. Email field: **Administrator** (this may vary by lab hoster).
    2. Password field: **Pa55w.rd** (this may vary by lab hoster).

[!NOTE] It's acknowledged that using the local Administrator account is not a typical scenario. It's used in this exercise due to the simplified on-premises environment. A more realistic scenario, with a more involved on-premises environment, would have the user access the private resources with their Entra ID account.

You have successfully connected to the file server by using Global Secure Access.