



# Using GPCS VPN (Global Protect Cloud Service)

---

This guide is aimed at **external or BYOD** users who need to securely access the Zurich network remotely.

The GPCS tool is the new VPN solution which will allow Zurich employees to securely access the Zurich network remotely.

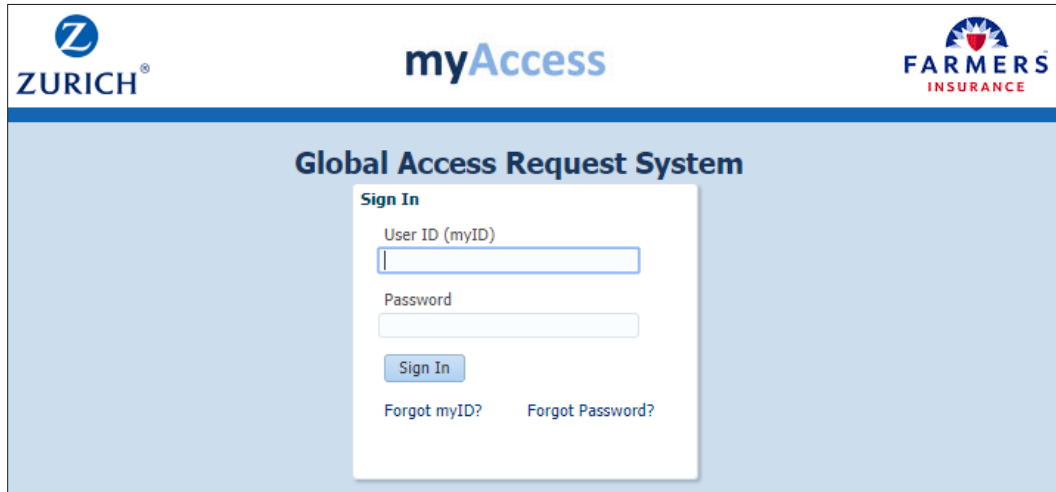
With GPCS, Zurich will have one global solution for the whole company which facilitates flexible work arrangements.

GPCS is always on and will open automatically when you power on your laptop. Once you login, you will be prompted for multi-factor authentication (MFA) using Okta.

# Request access to the Active Directory group

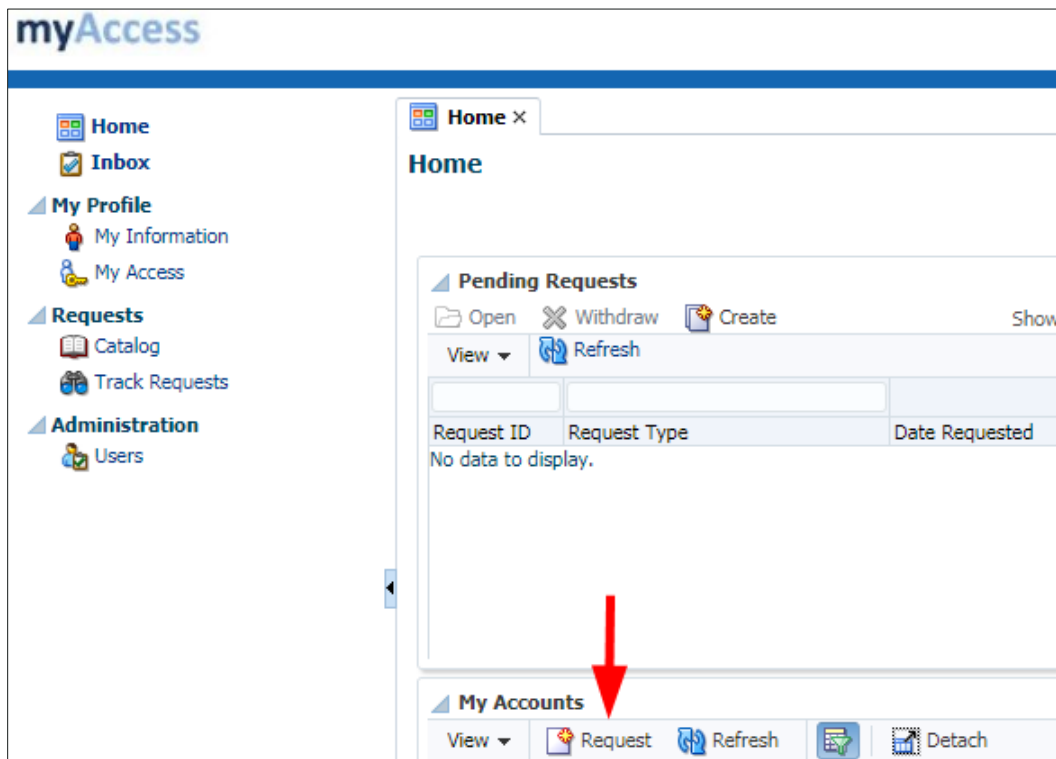
Before using the new GPCS VPN solution, external users or BYOD users must request access to the correct active directory group. **These steps must be performed while connected to either the corporate network or the current VPN.**

1. Open the internet and navigate to <https://myaccess.zurich.com> Login with your myID.



The screenshot shows the login page for the myAccess Global Access Request System. At the top, there are logos for ZURICH, myAccess, and FARMERS INSURANCE. The main heading is "Global Access Request System". Below this is a "Sign In" form with fields for "User ID (myID)" and "Password", a "Sign In" button, and links for "Forgot myID?" and "Forgot Password?".

2. In MyAccess, click on the **Request** button



The screenshot shows the myAccess dashboard. On the left is a navigation menu with links to Home, Inbox, My Profile, Requests, and Administration. The main content area shows a "Home" tab with a "Pending Requests" section. Below this is a "My Accounts" section where the "Request" button is highlighted with a red arrow. The "Request" button is located next to a "View" dropdown and a "Refresh" button.

3. In the search box type an Active group name from the list below. Choose the appropriate group for your region:

- **AMER PROD GlobalProtect SSL VPN** (North America)
- **APAC PROD GlobalProtect SSL VPN** (Asia – Pasific countries)
- **EMEA PROD GlobalProtect SSL VPN** (Europe, Middle East and Africa)
- **LATAM PROD GlobalProtect SSL VPN** (Latin America)

The screenshot shows a web interface for a 'Request Catalog'. At the top, there are tabs for 'Home' and 'Request Catalog'. Below the tabs, the 'Catalog' section features a search bar with a magnifying glass icon, a dropdown menu set to 'All', and a search input field containing 'EMEA PROD GlobalProtect SSL VPN'. To the right of the search bar is a 'Back To Catalog Home' link. Below the search bar, there is a 'Sort By' dropdown menu set to 'Entity Type'. The main content area displays a table with the following data:

#	Risk Level	Catalog Items
1		GITDIR~CN=EMEA PROD GlobalProtect SSL VPN,OU=Se... Entitlement

At the bottom right of the table row, there is an 'Add to Cart' button with a green plus icon.

4. Select **Add to Cart** next to the group name

5. A popup message will appear to confirm that your group has been **added to cart**

6. Click on **Checkout**

7. Then **Submit**

The screenshot shows the 'Cart Details' page. At the top, there are links for 'Back To Catalog', 'Submit', and 'Save as Draft'. The page is divided into two main sections: 'Target Users' and 'Cart Items'. The 'Target Users' section has a table with one row:

#	Name
1	EMEA PROD GlobalProtect SSL VPN

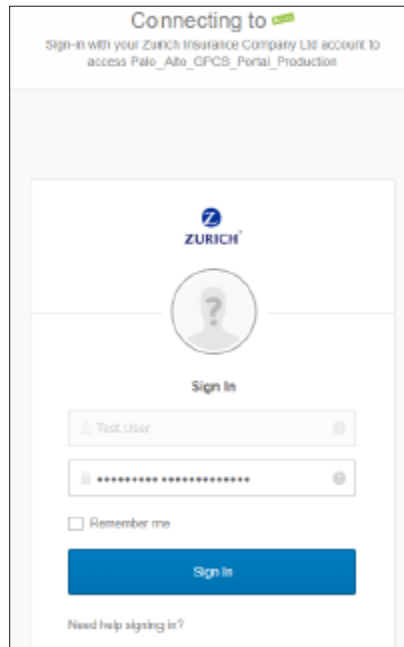
The 'Cart Items' section has a table with one row:

#	Display Name	Status
1	GITDIR~CN=EMEA PROD GlobalProtect SSL VPN,OU=Security Services,OU=Enterprise Services,DC=zurich,DC=com Target Account: MOIDMUSTAFA.ALI	Ready to submit

At the bottom of the 'Cart Items' table, there are buttons for 'Remove', 'Details', and 'Ready to submit'.

## Download and install the agent

1. Open internet explorer and navigate to <https://zurich.gpcloudservice.com>
2. Sign in with your myID and password then click **Next**



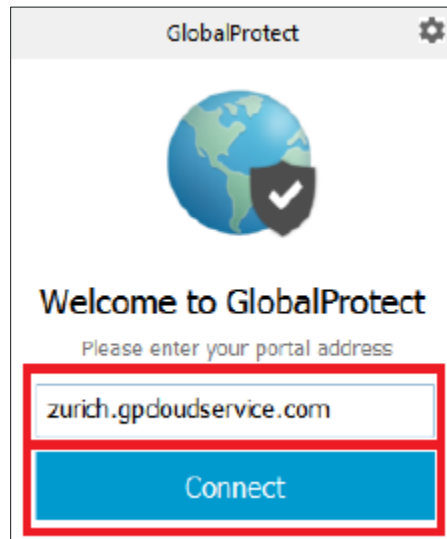
3. Click to download the **GlobalProtect Agent**



4. Select the appropriate agent



5. **Install** the agent (ensure that you have local admin privileges)
6. After the installation is finished enter **zurich.gpcloudservice.com** into the portal field and click **Connect**



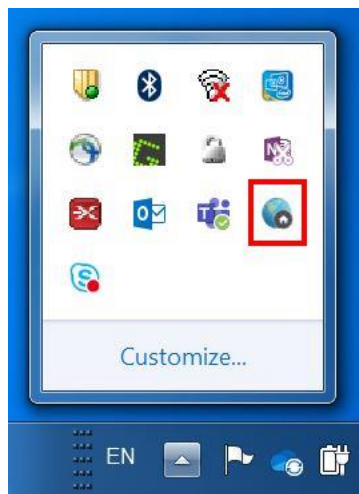
## Set up your Okta profile

To access the GPCS portal, you will need to configure an authentication factor in Okta. If you have not previously set up Okta, follow the steps in the [Okta set up guide](#) before continuing.

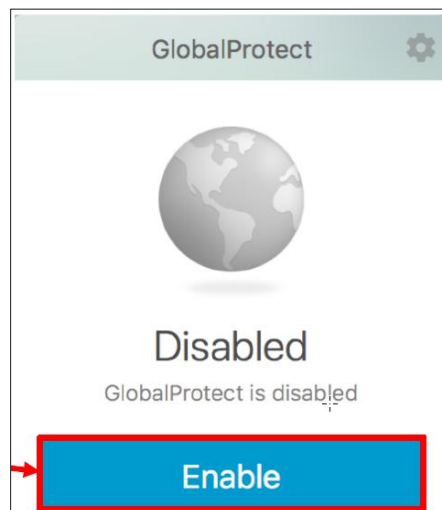
## Enable the Global Protect (GP) Agent

Initially the GP Agent will be disabled and you will need to enable the application.

1. You will find the GP Agent icon in your system tray by clicking on the **show hidden icons** arrow in your task bar. The correct icon is highlighted in the below picture:



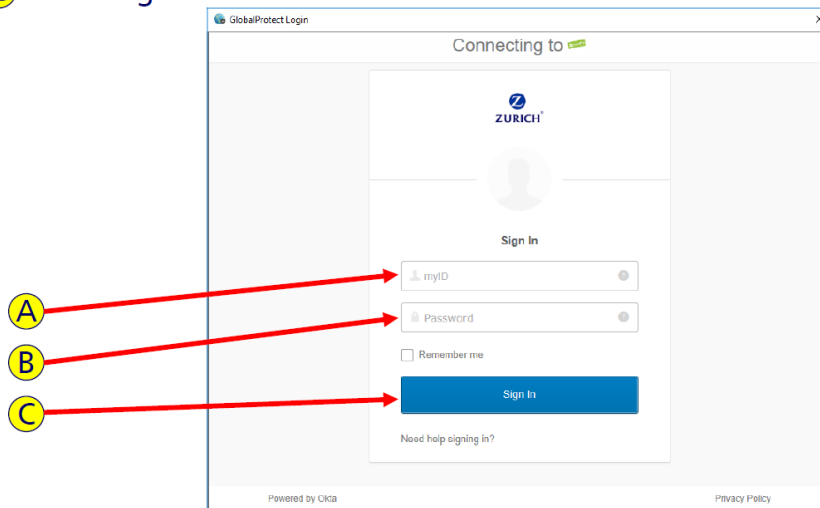
2. Once the GlobalProtect window opens, click **Enable**



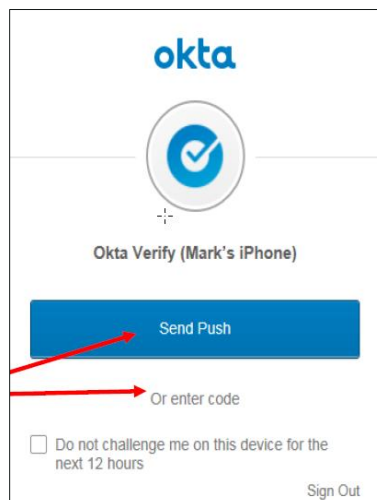
## Authenticate to GPCS with Okta

1. The Okta authentication interface will open automatically. You will now need to authenticate through Okta to gain access to GPCS VPN with your myID (zurich.com) credentials.
2. Follow the below sequence of instructions:

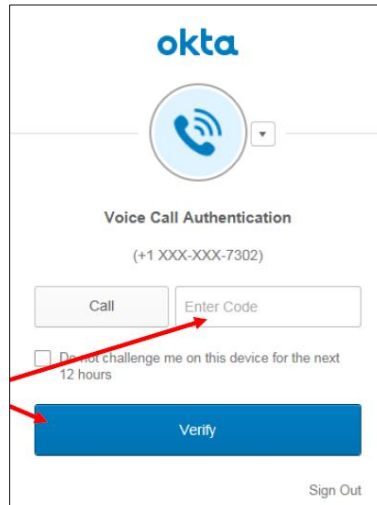
- A Type your zurich.com (or myID) Username
- B Type your zurich.com (or myID) Password
- C Click "Sign In"



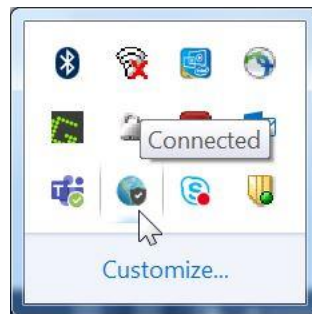
3. Once signed in successfully, you will be directed to either an **Okta Verify** screen or a **Voice Authentication** screen.
4. If you have configured **Okta Verify** as your multi-factor authentication you can push the **Send Push** button and the app on your phone will ask you to confirm the push.



- Alternatively if you selected **Voice Authentication** you push the call button and a call will be made to the configured number where you will receive a code. This code is then entered and you push verify.



- Once you have successfully authenticated you will be automatically logged into GPCS and the corporate network. You can check connectivity by opening the system tray where you should see the below GPCS icon which will say connected when you move the cursor over it.

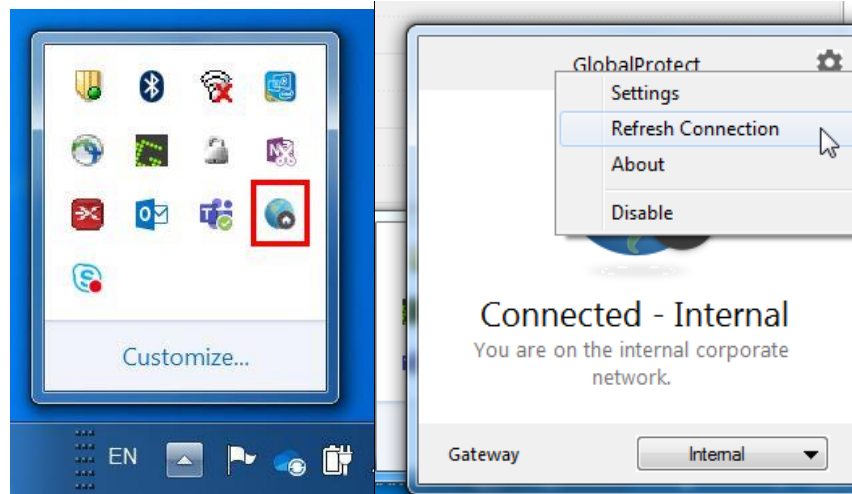




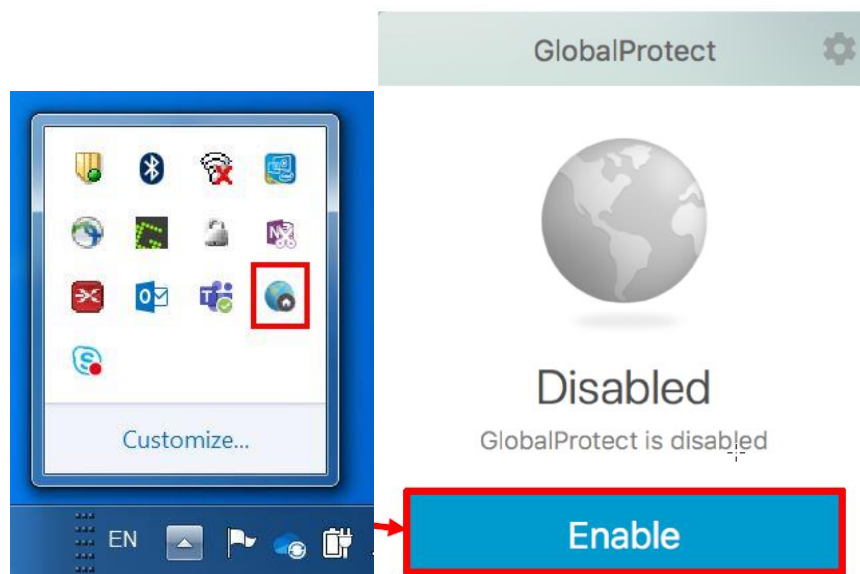
## Authentication Failure

Should the authentication to GPCS fail (incorrect code, verify timeout) there are a number of options you can take to reset the process.

**Refresh the connection:** the GPCS connection can be reset from the agent GUI located in the system tray. The pictures below illustrate how to do this.



**Disable and re-enable the GP Agent:** the agent can be disabled and re-enabled to reset the Authentication process.



**Reboot the machine:** the laptop can be rebooted to restart the authentication process.

# Troubleshooting

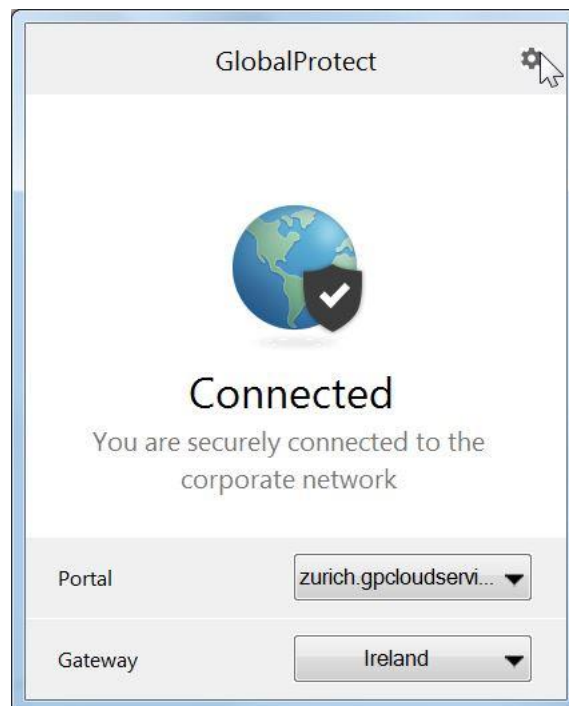
## How to get logs from the GlobalProtect Agent

In the event you have issues you may be asked to retrieve logs from your GP Agent. The steps below will take you through this:

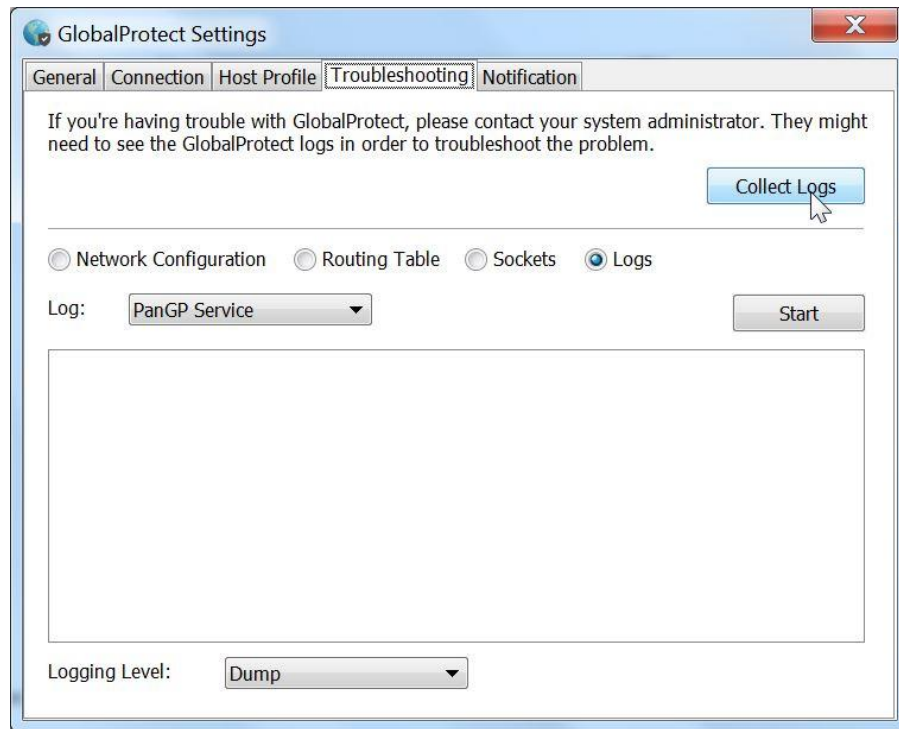
1. Open the **GP Agent** app by clicking on the icon in the system tray



2. Open the settings by clicking on the **cog** wheel on the top right hand corner and clicking settings



3. Select **Troubleshooting** and click on the **Collect Logs** button.



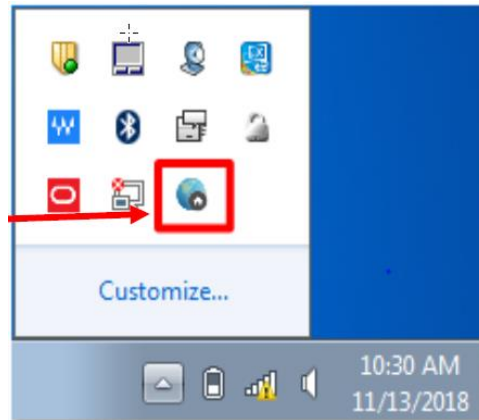
4. The logs will then be zipped and stored in your user directory. C:\Users\**User.Name** and will be called **GlobalProtectLogs.zip**

## Disabling the GlobalProtect Agent

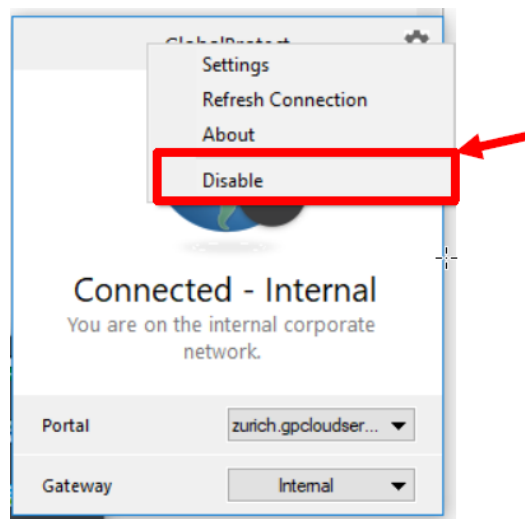
It should be noted that you will still have Cisco AnyConnect VPN to fall back on if GPCS VPN does not work.

Before disabling the GlobalProtect agent please contact the service desk to resolve any issues. If you need to disable GPCS in order to connect to the network please follow the below instructions.

1. Under the tool bar on your PC, right click on the GlobalProtect Icon



2. Click on cogwheel and select **Disable**



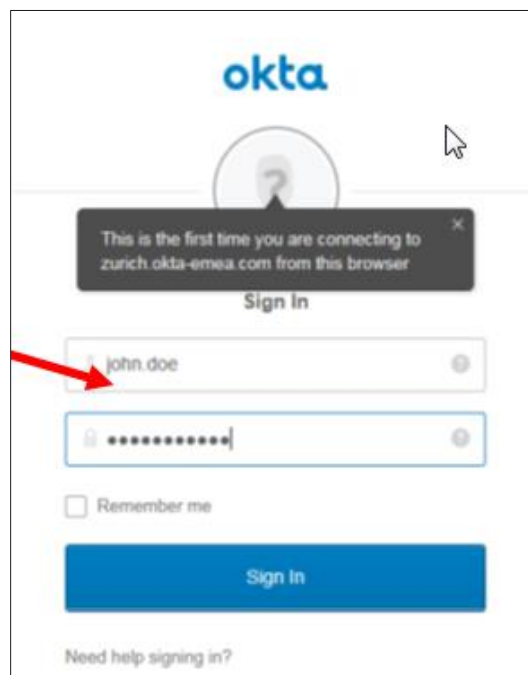
After successfully disabling the GPCS VPN agent, you can use Anyconnect VPN to connect to corporate network.

## OKTA – How to reset factors

### Why should I reset Okta Verify?

- Your phone was lost, you want to make sure unauthorized users can't access your account and you have another factor configured (e.g. you have lost your mobile but had previously configured an alternative number to use as MFA).
- You want to change your phone number for Voice Authentication.

1. Navigate to <https://zurich.okta-emea.com> and complete login as normal.



2. Once logged in successfully, look for your name and click on the down arrow next to your name to see the menu.

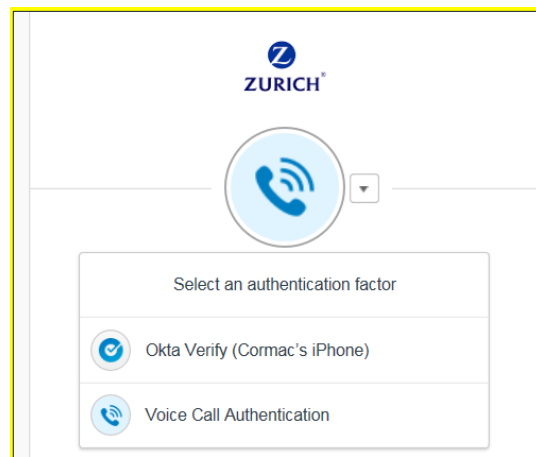


3. Click **Settings**

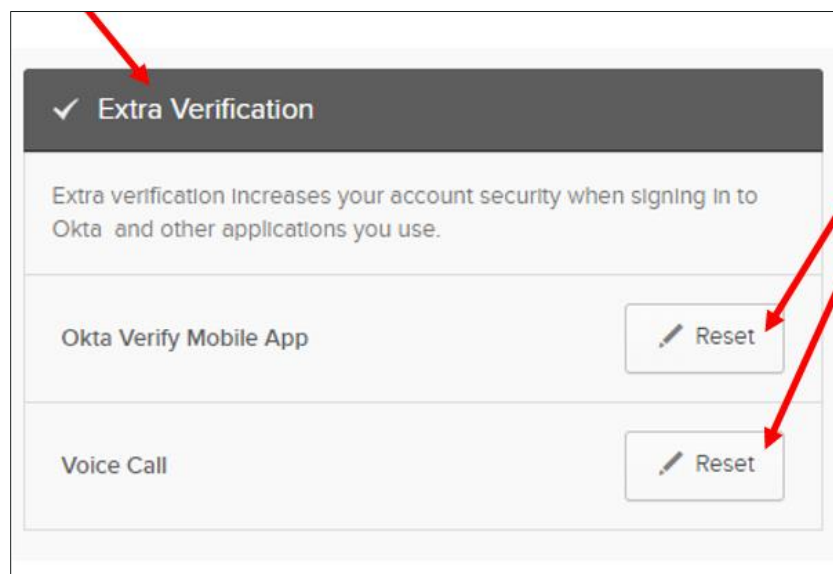
4. Click **Edit Profile**



5. You will be asked to login with your password and then to select an MFA factor. If you have more than one factor configured you can select the factor you have access to. If you do not have access to the factor (for instance you have only Okta Verify configured and have lost/replaced your phone) then you will need to log a SNOW ticket to have the factor reset.



6. Scroll down to the **Extra Verification** section



7. To confirm resetting of OKTA verify, click **Yes**

**Set Up Okta Verify**

Okta Verify has already been configured for your account. Please read below before reconfiguring.

Do you want to revoke your existing Okta Verify token and reconfigure?

Cases when you may want to revoke your Okta Verify token:

- Your phone was lost and you want to make sure unauthorized users can't access your account
- You want to install Okta Verify on a different phone

Yes No

8. To disable voice call click **Disable** and use **Update** button to enter your new number

**Set Up Voice Call Verification**

Your phone number 07875 388672 has been verified and is configured for extra verification via phone call.

Click Update to change your phone number.

Click Disable to stop using your phone for verification in the event your phone is lost or stolen.

Update Disable Cancel

**Set Up Voice Call Verification**

Enter the phone number you'll use to receive codes via phone call, then click Call to verify that it works.

Country: United Kingdom  
Select the country where your phone is registered.

Phone number: [Input field]  
Enter your number the way you normally dial it. Do not add your country code prefix.

Extension: [Input field]

Call

## Lost Phone

If you have lost your mobile phone and you do not have another authentication factor configured in Okta you will not be able to login to the Okta portal. In this instance you will need to open a SNOW ticket or ring your local IT service desk to have your Okta factors reset.