



USING THE VPN SERVICE

Setting up the VPN User

You will receive an email with your VPN user credentials from the email address: servicedesk@krone.de. The first step is to change the initial password.

1. Open the webpage access.krone.group in your web browser. You will be automatically redirected and should see a login screen:

ANMELDEN
Krone Business Center

Anmelden

someone@example.com

[Sie können nicht auf Ihr Konto zugreifen?](#)

Zurück Weiter

If your browser tries to log you in with a saved account, you will see the following message. You need to log out from your account.

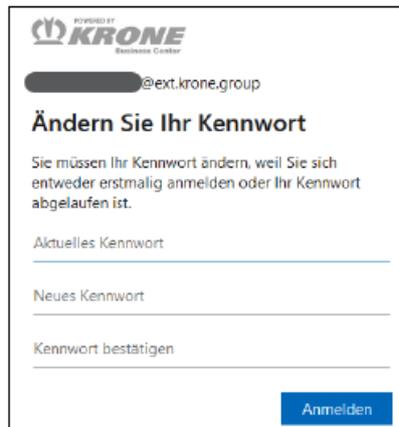
Hierauf haben Sie keinen Zugriff.

Ihre Anmeldung war erfolgreich, aber Sie haben keine Berechtigung für den Zugriff auf diese Ressource.

Melden Sie sich ab, und melden Sie sich mit einem anderen Konto an.

[Weitere Details](#)

2. Log in with your username (firstname.lastname@ext.krone.group) and your initial password from the email. After the first login, you need to change your initial password. Please follow the password guidelines on the next page.



POWERED BY
KRONE
Business Center

██████████@ext.krone.group

Ändern Sie Ihr Kennwort

Sie müssen Ihr Kennwort ändern, weil Sie sich entweder erstmalig anmelden oder Ihr Kennwort abgelaufen ist.

Aktuelles Kennwort

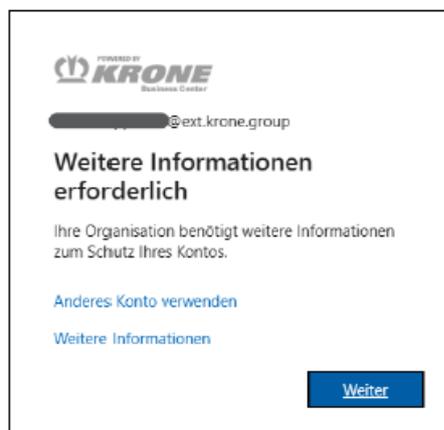
Neues Kennwort

Kennwort bestätigen

Anmelden

Password Guidelines:

- a) At least 8 characters
 - b) Must meet 3 out of the following 4 criteria:
 - i) Uppercase letters
 - ii) Lowercase letters
 - iii) Numbers
 - iv) Special characters
 - c) Must not contain words from the password list, such as:
 - i) Your own (first/last) name
 - ii) The company (Krone)
 - iii) Simple passwords like "Password123"
 - d) Must not be any of the previous passwords.
3. After choosing a new password, you should see the following message. You will be prompted to set up multi-factor authentication (MFA) for the user. Click "Next" and follow the on-screen instructions.



POWERED BY
KRONE
Business Center

██████████@ext.krone.group

Weitere Informationen erforderlich

Ihre Organisation benötigt weitere Informationen zum Schutz Ihres Kontos.

[Anderes Konto verwenden](#)

[Weitere Informationen](#)

Weiter

4. There are several ways to set up the second factor. The first and recommended way is to use the "Microsoft Authenticator" app on a smartphone. Click "Next" to proceed.

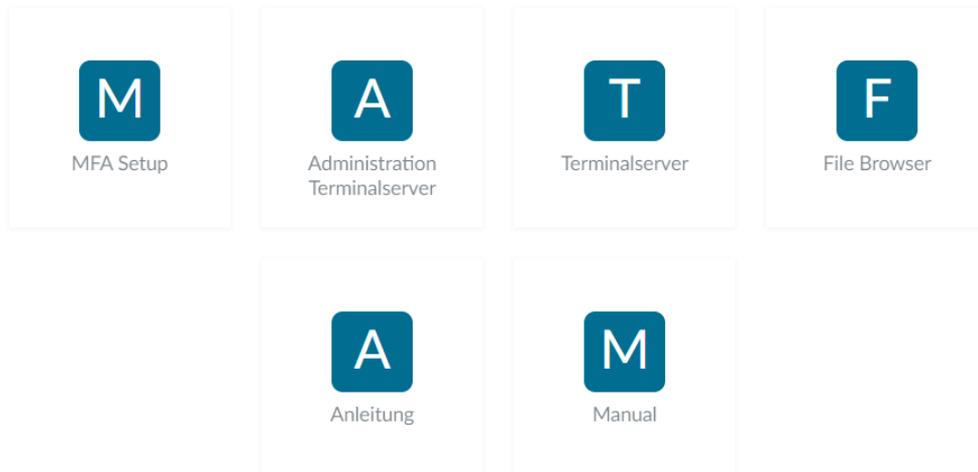
If using a smartphone is not possible, you can also confirm the second factor via a phone call. To set this up, click "I want to set up a different method."



5. After setting up and confirming the second factor, you will be automatically redirected and should see the following message. Click on the method you set up as the second factor and confirm it.



6. After confirming the second factor, you should see the following webpage. Here you can see all the resources available to you in the clientless VPN.

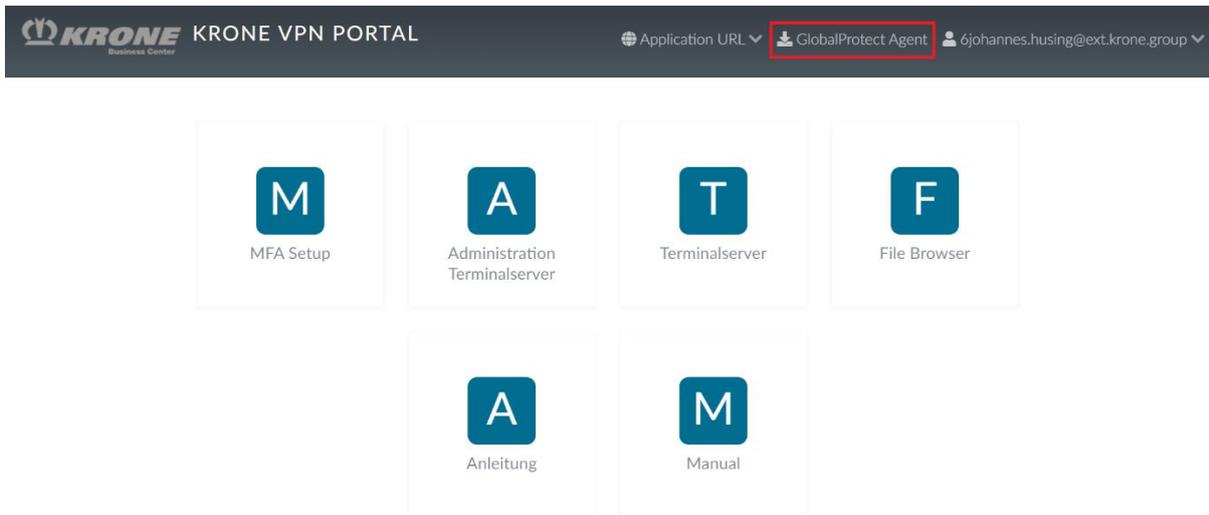


If the targets or resources you need are not accessible through the KRONE VPN Portal, you need to install the VPN client and establish a VPN connection to the KRONE network. (See the following section for VPN client installation)

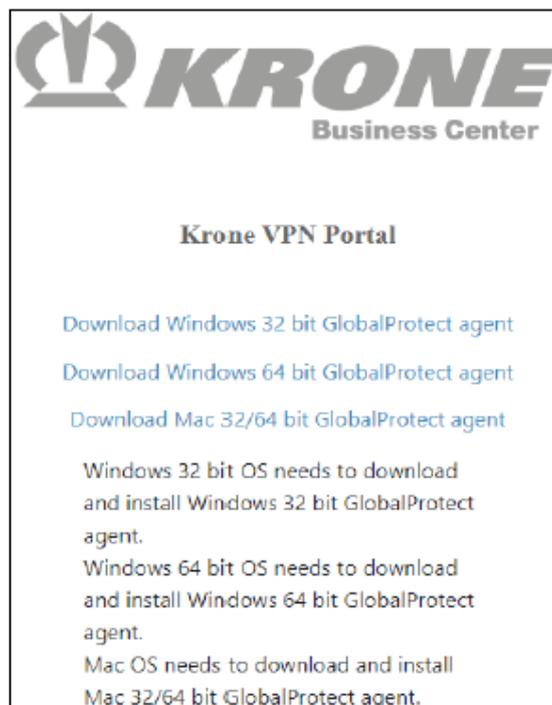
Installing the VPN Client

For certain resources, it is not possible to access them through the VPN Portal. In these cases, you need to install the Krone VPN client.

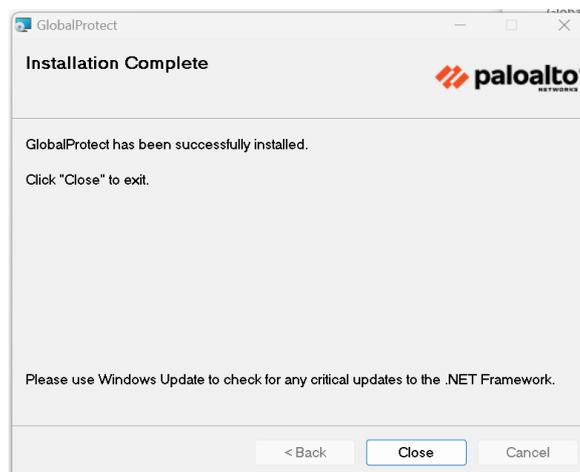
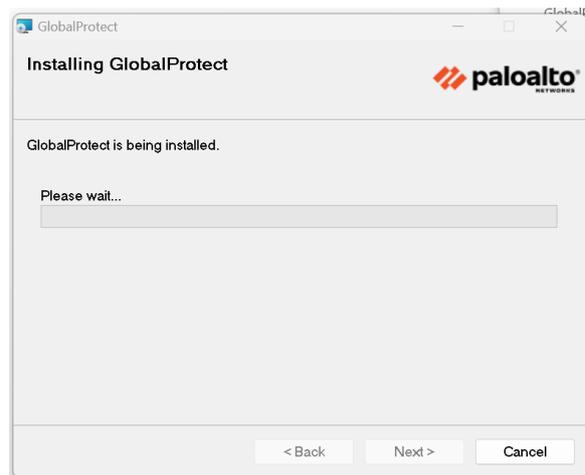
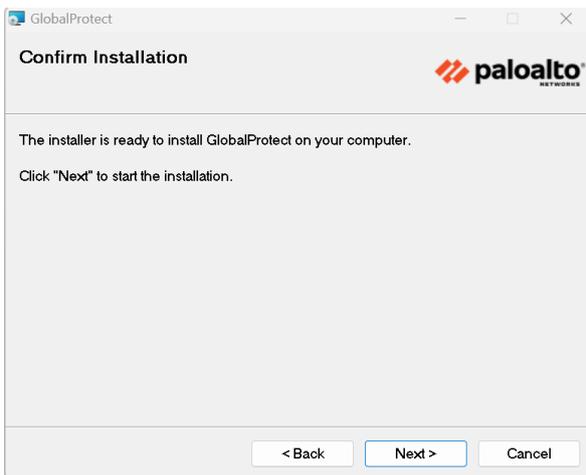
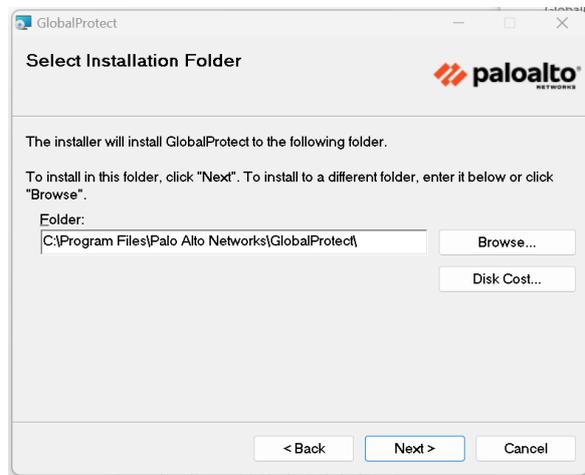
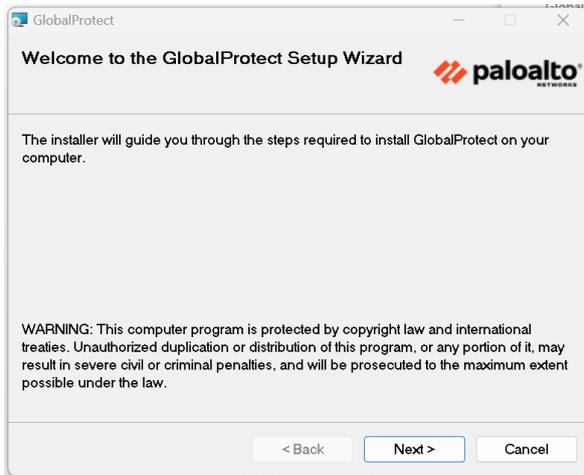
You can download the GlobalProtect client from the Krone VPN Portal (access.krone.group).



Download the appropriate VPN client for your device. Usually, this is the "Windows 64 bit GlobalProtect agent."



The installation can be completed by clicking through the prompts. No settings need to be adjusted.

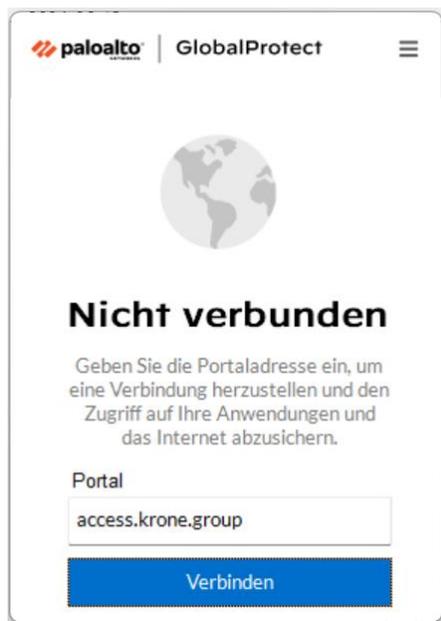


Establishing a VPN Connection

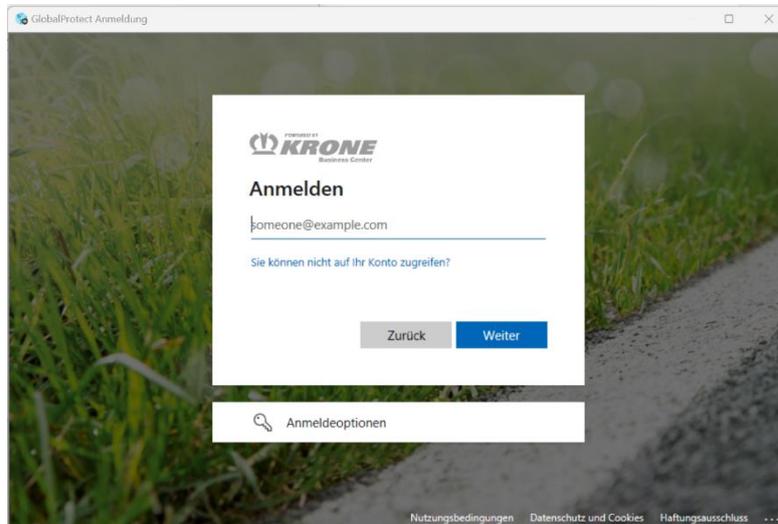
First, open the client via the system tray icon.



Enter the portal address `access.krone.group`. This address only needs to be entered for the first connection.



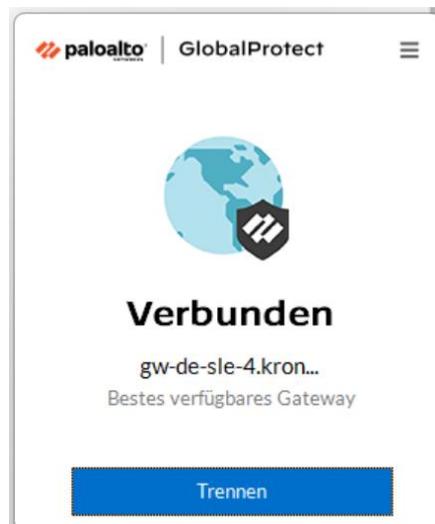
The client will open a login screen in an embedded browser. Log in with your VPN user (firstname.lastname@ext.krone.group).



If an automatic login occurs and the following message appears, select the highlighted text. Then you should be able to enter the correct username..



After a successful login, the client will switch to connected status. You should now be able to access Krone resources directly.



Troubleshooting

Password Expired

If the password has expired, it must be changed; otherwise, the remote apps will not be available. If the password cannot be changed, a new password must be requested from the ServiceDesk.

Resetting Multi-Factor Authentication

If there are issues with the MFA connection and it needs to be reset, this must be requested from servicedesk@krone.de.

When changing phones, the MFA connection can be transferred to the new phone via the MFA Setup tile. If the previously used device is no longer available, the reset can be requested from the ServiceDesk.

Logging in from a MacBook

There may be issues with logging in as the login does not go through the VPN tunnel. If logging in is not possible, enable the GlobalProtect system extensions checkbox during installation (disabled by default).