What methods can an external-company employee use to access the data network of Wacker Chemie AG and its subsidiaries?
Inhalt

1  General information .................................................. 3

2  VPN-Client based business partner access .......... 4
   2.1  Pre-requisites .................................................. 4
   2.2  Installation of the VPN client ......................... 4
   2.3  Logging on ...................................................... 6
   2.4  Logging off ..................................................... 7
   2.5  Using the token card in „New PVN“ mode .......... 7
   2.6  Changing the PVN ............................................. 7
   2.7  Technical information ......................................... 7

3  VPN access without VPN client for business
   partners with direct connection to the Wacker
   network .............................................................. 8
   3.1  Pre-requisites .................................................. 8
   3.2  Authentication .................................................. 8
   3.3  Using the token card in „new PVN“-Modus ........ 9
   3.4  Changing the PVN ............................................. 9
   3.5  Security restrictions .......................................... 9
   3.6  Alternative method .......................................... 9

4  Contact.............................................................. 10
1 General information

Wacker Chemie AG gives external-company employees of its business partners access to the WACKER data network. Depending on the requirements of the business partner there are different ways for remotely accessing the Wacker network.

1. **Citrix Access Gateway (CAG) – STANDARD**
   The preferred access method for business partners is the usage of the Citrix Access Gateway (CAG).

2. **VPN client based business partner access**
   If due to technical reasons the remote access by Citrix Access Gateway is not possible, the remote access to the Wacker network is also possible using a VPN (virtual private network) connection.

3. **VPN access without a VPN client for business partner companies with a direct connection to the Wacker network**
   For some special business partners it may also be necessary that the business partner company gets directly connected to the Wacker network by a permanent VPN connection between the Wacker network and the business partner’s network.

You will be informed via e-mail which type of access has been provided for you.

This document describes the two following access methods:

- **VPN client based business partner access**
- **VPN access without a VPN client for business partner companies with a direct connection to the Wacker network**

**Attention:** If you have access via the Citrix Access Gateway (CAG), please use the documentation for the Citrix Access Gateway (CAG).

Please refer to the Userhelpdesk (Chapter 4 Contact) to get the CAG documentation.
2 VPN-Client based business partner access

Users who want to access the Wacker network via VPN need a VPN client on their computer: the Palo Alto Global Protect client.

**Attention**: The Palo Alto Global Protect client is not necessary when the business partner is using a business partner direct connection which has explicitly been set up for the connection between the business partner’s company and Wacker Chemie AG. Please proceed with chapter 3 - VPN access without VPN client for business partners with direct connection to the Wacker network

2.1 Pre-requisites

Usage of the VPN client business partner access requires:

- Approved IDM USS "Request for VPN access for business partners"
- Computer with an internet connection
- Single-use administrative rights for the installation of the VPN client Palo Alto Global Protect
- User name and logon password
- Token card
- Access rights for the application.

**Attention: Initial setting of the logon password**

- **AD-Account**: If you logon to the Wacker network using an AD account please contact the Wacker UserHelpDesk for setting the initial AD password.
- **CD-Account**: If you logon to the Wacker network using a CD account please set your CD password according to the method described in the email, which you received after successful completion of the IDM USS „Request for VPN access for business partner”.

2.2 Installation of the VPN client

Start your web browser and enter the URL (web address) [https://bpa.vpn.wacker.com](https://bpa.vpn.wacker.com). Then enter your user name in the Name field and your logon password in the Password field.

After successfully logging on, you can download the VPN software. Select the version designed for your operating system.

Click Next > to launch the installation assistant.
After successful installation the configuration window appears automatically. In the Portal field enter „bpa.vpn.wacker.com“. Then click Connect to start logging on for the first time.

Logging on
Enter your user-id in the field Username and your password in the field Password. Click on Apply to start logging in.

In the GlobalProtect Gateway Authentication window, enter your 4-digit PVN number immediately followed by the 8-digit number generated by your token card to create a unique, single-use password. Click OK to confirm this.

Note
When you use the token card for the first time, it is in „New PVN“ mode. You must therefore specify a new PVN. Enter the default PVN „1234“ followed immediately by the 8-digit code number generated by your token card and immediately follow this with your new 4-digit PVN - entered twice. The format is: 1234[token code][new PVN][new PVN]. For more information on the „New PVN“ mode, please see section 2.5.

As soon as a VPN connection has been established the following window appears. The GlobalProtect icon in the taskbar also shows that the connection is established.

Note
From now, you log on to the WACKER VPN Gateway as described section 0 Logging on.
2.3 Logging on

To log on at the next VPN gateway start the GlobalProtect client and click on Connect.

In the GlobalProtect Gateway Authentication window, enter your 4-digit PVN number immediately followed by the 8-digit number generated by your token card to create a unique, single-use 12-digit password.

As soon as a VPN connection has been established the following window appears. The GlobalProtect icon in the taskbar also shows that the connection is established.

Enter your user-id in the field Username and your password in the field Password. Click on Apply to start logging in.
2.4 Logging off

To end the VPN connection, right-click the GlobalProtect icon in the taskbar and select Disconnect.

When you have been disconnected, the message Disconnected appears in the taskbar and a red „X“ appears on the GlobalProtect icon in the taskbar.

2.5 Using the token card in „New PVN“ mode

If the WACKER UserHelpDesk has reset your PVN or you are using the token card for the first time, you must enter additional information when logging on:

In the GlobalProtect Gateway Authentication window, enter the default PVN „1234“ immediately followed by the 8-digit code generated by your token card, immediately followed by your new PVN entered twice (one right after the other). Click OK.

Example
To define 4321 as your new PVN, enter 1234[8-digit token code]43214321 in the GlobalProtect Gateway Authentication window.

2.6 Changing the PVN

You can change your PVN when logging on. In the GlobalProtect Gateway Authentication window, enter your current 4-digit VPN immediately followed by the 8-digit code generated by your token card, immediately followed by your new PVN entered twice (one right after the other). Next, click OK.

Example
To define 4321 as your new PVN, enter 1234[8-digit token code]43214321 in the GlobalProtect Gateway Authentication window.

2.7 Technical information

Note
The installation and usage of the VPN software Palo Alto Networks GlobalProtect does not require a license.

WACKER uses the following networks, and after you have successfully logged on, the information you enter is transmitted in encrypted form to the WACKER VPN gateway:

10.0.0.0/8
57.195.8.0/24
172.16.0.0/12
192.168.0.0/16
193.18.0.0/16
193.19.0.0/19

The following networks are exempt, so the information you enter in these networks is not transmitted to WACKER and you can also use these networks locally:

169.254.0.0/16
192.168.0.0/24
192.168.1.0/24

The DNS configuration is handled automatically when you log on to the VPN gateway.

If you are using a firewall please make sure that this firewall is permitting SSL (TCP port 443) and IPsec-ESP-UDP (UDP port 4501) to the following WACKER networks:

193.18.240.0/24
193.18.92.128/25
193.18.191.128/25

Note
If you are using proxies they are automatically detected and used by the VPN software GlobalProtect. In case of a proxy authentication GlobalProtect is showing an additionally login window for requesting the login information for your proxy. Because it is difficult for users to distinguish between the proxy login window and the WACKER login window we recommend to allow the access to the above mentioned WACKER networks without authentication.
3 VPN access without VPN client for business partners with direct connection to the Wacker network

3.1 Pre-requisites

Usage of a VPN access without a VPN client requires the following:

- Direct connection between your company’s network and the network of WACKER Chemie AG
- User name and logon password
- Token card
- Access rights for the application.

Note
To find out if your company has a connection to WACKER’s Business Partner MPLS, please contact your IT department.

To access applications in the WACKER network, you must first authenticate yourself at the business partner firewall.

3.2 Authentication

In your web browser, enter the URL (web address) corresponding to the region in which you are located.

<table>
<thead>
<tr>
<th>Region</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td><a href="http://auth-bpa-emea.vpn.wacker.com">http://auth-bpa-emea.vpn.wacker.com</a></td>
</tr>
<tr>
<td>America</td>
<td><a href="http://auth-bpa-amer.vpn.wacker.com">http://auth-bpa-amer.vpn.wacker.com</a></td>
</tr>
<tr>
<td>Asia</td>
<td><a href="http://auth-bpa-apac.vpn.wacker.com">http://auth-bpa-apac.vpn.wacker.com</a></td>
</tr>
</tbody>
</table>

You are forwarded to the WACKER User Identification Portal. Enter your user name in the Name field and leave the Password field blank. Then click Login.

You are now prompted to enter your 4-digit PVN immediately followed by the 8-digit code generated by your token card to create a unique, single-use 12-digit password. Confirm your entries by clicking Login.

Note
When you use the token card for the first time, it is in New PVN mode. You must therefore specify a new PVN. Enter the default PVN „1234” followed immediately by the 8-digit code number generated by your token card and immediately follow this with your new 4-digit PVN - entered twice. The format is: 1234[token code][new PVN][new PVN].
For more information on the new PVN mode, please see section 3.3.

Your logon information is now authenticated. If the authentication is successful, the message You are authenticated appears.
3.3 Using the token card in „new PVN“-Modus

If the WACKER UserHelpDesk has reset your PVN or you are using the token card for the first time, you must enter different information when being authenticated for the first time:

Enter the default PVN „1234“ immediately followed by the 8-digit code generated by your token card, immediately followed by your new PVN entered twice (one right after the other). This represents a unique, single-use password comprised of 20 digits. Now, click Login.

Example
To define 4321 as your new PVN, enter in the field 1234[8-digit token code]43214321.

3.4 Changing the PVN

You can change your PVN when logging on. In the authentication window, enter your current 4-digit PVN immediately followed by the 8-digit code generated by your token card, immediately followed by your new PVN entered twice (one right after the other). This represents a unique, single-use password comprised of 20 digits. Now, click Login.

Example
To define 4321 as your new PVN, and enter in the field of the authentication window:
[current PVN][8-digit token card code]43214321.

3.5 Security restrictions

The authentication is valid for 10 hours, after which all connections are terminated for security reasons.

The authentication provides a 15-minute window for you while you can launch the applications.

As long as you keep the authentication window (the window with the message You are authenticated) open in your web browser and a recent update is displayed after the word [Last check:]. the start window’s timeout period is automatically extended.

3.6 Alternative method

For the authentication process (accessing the URL), your computer must be able to resolve the following host names and access these web sites using your web browser:

<table>
<thead>
<tr>
<th>Region</th>
<th>URL</th>
</tr>
</thead>
</table>

You can either resolve the DNS using the WACKER DNS or your company’s own DNS.

If this is not possible, an address-based authentication can be performed using the following URL:

Security warnings related to the certificates of the sites 193.18.64.19, 193.18.88.19 and 193.18.80.19 appear, but you can ignore these warnings.
4 Contact

If you experience a problem, please contact the WACKER UserHelpDesk.

**USA (Americas):**
Tel. +1 800 430-8374  
help.desk@wacker.com

**Asia (APAC):**
Tel. +86 21 6100-3456  
helpdesk.asiapac@wacker.com

**Europe (EMEA):**
Tel. +49 89 6279-1234  
userhelpdesk@wacker.com