CYBERARK - PRIVILEGED REMOTE ACCESS

USER GUIDE

Editor:
Team Data Center Operations

Address:
Salzgitter Digital Solutions GmbH
Eisenhüttenstraße 99
38239 Salzgitter

Department:
IT-Infrastruktur

Version:
V1.15 I 20.09.2022

CYBERARK - PRIVILEGED REMOTE ACCESS

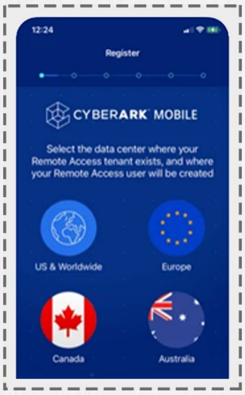
REGISTRATION AND SIGN IN VIA CYBERARK MOBILE APP

01. INSTALLATION OF THE CYBERARK MOBILE APP

The **CyberArk Mobile App** must be downloaded from the Google Play/Apple App Store and installed on the smartphone. Links for the app can be found at the bottom of the invitation email which was sent to the user.

02. REGISTER VIA CYBERARK MOBILE APP

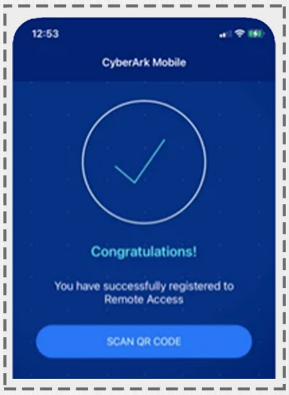
After installing and launching the app, the user needs to follow the instructions provided by the app. In addition to selecting the correct data center (*Europe*), this also includes entering personal profile information and specifying a six-digit security code. The user then follows the link in the invitation email to the CyberArk Alero website, which provides a QR code that must be scanned using the app's **Scan QR code** button.


12:24

Register

CYBERARK MOBILE

Select the data center where your Remote Access tenant exists, and where your Remote Access user will be created


12:53

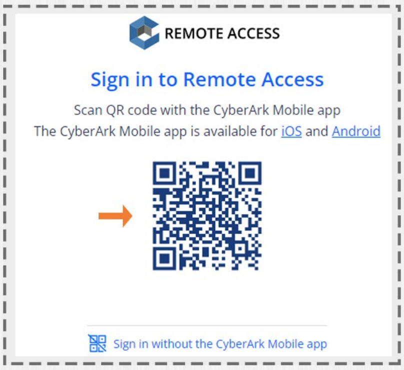
CyberArk Mobile

Congratulations!

You have successfully registered to Remote Access

03. SIGN IN VIA CYBERARK MOBILE APP

The user needs open the website **https://portal.alero.eu**. After opening it, the user scans the QR code shown with his **CyberArk Mobile App**. After the scan the user is logged into the system.


REMOTE ACCESS

Sign in to Remote Access

Scan QR code with the CyberArk Mobile app

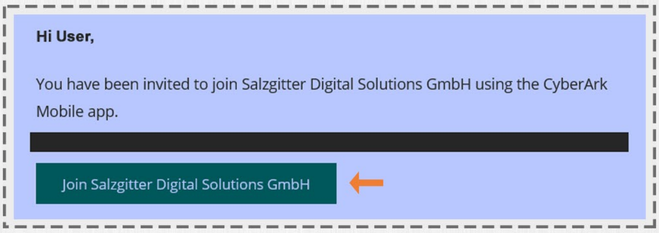
The CyberArk Mobile app is available for iOS and Android

CYBERARK - PRIVILEGED REMOTE ACCESS

REGISTER VIA SMS/PHONE CALL

01. ACCEPT THE CYBERARK INVITATION

After the invitation by an administrator the user will receive an email from CyberArk. The user must click the button "**Join Salzgitter Digital Solutions GmbH**" in the email.



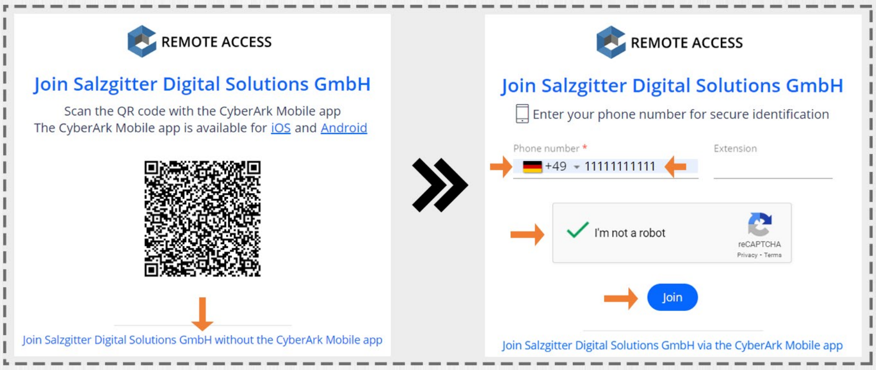
Hi User,

You have been invited to join Salzgitter Digital Solutions GmbH using the CyberArk Mobile app.

[redacted]

02. REGISTRATION

After clicking on "**Join Salzgitter Digital Solutions GmbH without the CyberArk Mobile App**" a new window appears in which the user needs to enter his or her **phone number**. The phone number must be identical to the number the user gave the administrator in advance in the registration email. After confirming the captcha, click on the "**Join**" button.



REMOTE ACCESS

Join Salzgitter Digital Solutions GmbH

Scan the QR code with the CyberArk Mobile app
The CyberArk Mobile app is available for iOS and Android

Join Salzgitter Digital Solutions GmbH without the CyberArk Mobile app

REMOTE ACCESS

Join Salzgitter Digital Solutions GmbH

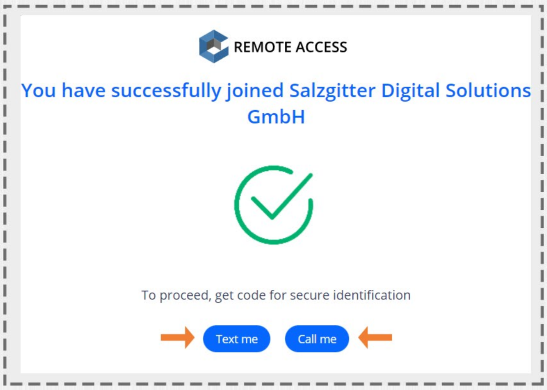
Enter your phone number for secure identification

Phone number * : +49 11111111111

Extension:

I'm not a robot
reCAPTCHA
Privacy - Terms
Join
Join Salzgitter Digital Solutions GmbH via the CyberArk Mobile app

After this step, the user has been successfully registered to CyberArk. Now the user can proceed directly with the registration by clicking on "**Text me**" (*code comes via SMS*) or "**Call me**" (*code comes via phone call*) and follow the instructions on the next page of this documentation.



REMOTE ACCESS

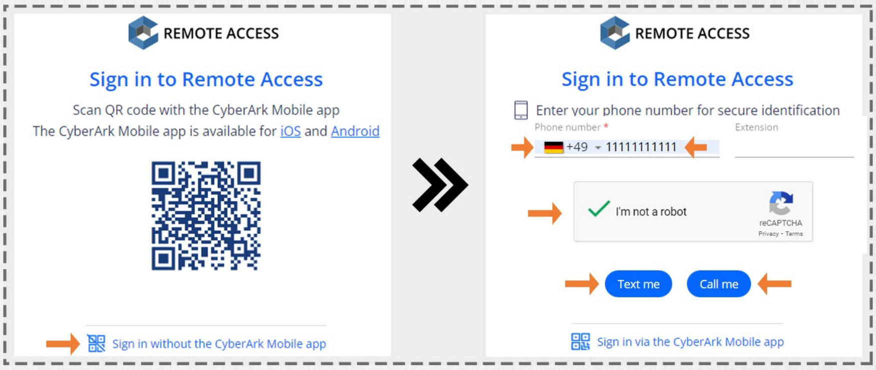
You have successfully joined Salzgitter Digital Solutions GmbH

To proceed, get code for secure identification

01. SIGN IN VIA SMS/PHONE CALL

The user needs open the website **https://portal.alero.eu**. After opening it, the user needs to click on **Sign in without the CyberArk Mobile App**. On the next page, the user needs to enter his **mobile number used for registration** and confirm the **captcha**.

There are now two ways to obtain the code needed for the login: either the user can have the code sent to him by **SMS** (*Text me*) or by an **automatic phone call** (*Call me*).



REMOTE ACCESS

Sign in to Remote Access

Scan QR code with the CyberArk Mobile app
The CyberArk Mobile app is available for iOS and Android

Sign in without the CyberArk Mobile app

REMOTE ACCESS

Sign in to Remote Access

Enter your phone number for secure identification

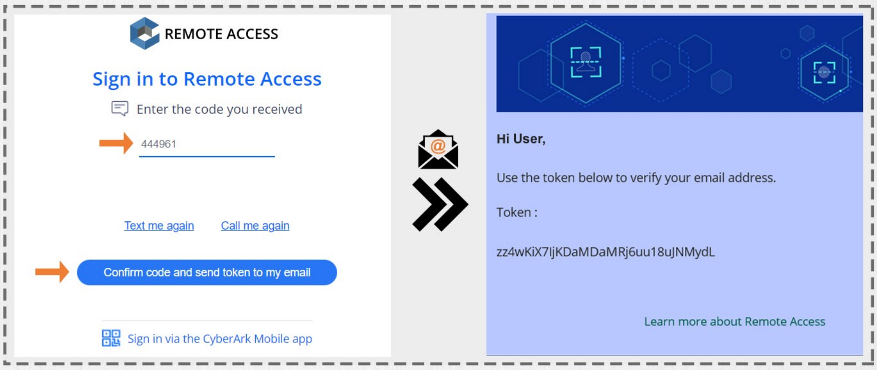
Phone number * +49 11111111111

Extension

I'm not a robot

Sign in via the CyberArk Mobile app

Then the user enters the obtained code on the following page. After clicking on **Confirm code and send token to my email** the user receives an email with a token.



REMOTE ACCESS

Sign in to Remote Access

Enter the code you received

444961

Sign in via the CyberArk Mobile app

Hi User,

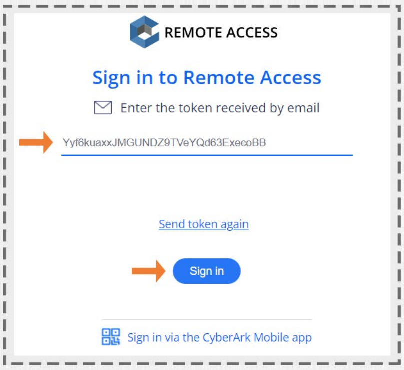
Use the token below to verify your email address.

Token :

zz4wKiX7IjKDaMDaMRj6uu18uJNMydL

Learn more about Remote Access

To complete the login, the token must be entered in the appropriate field on the website. After that, the user needs to click on the **Sign in** button.



REMOTE ACCESS

Sign in to Remote Access

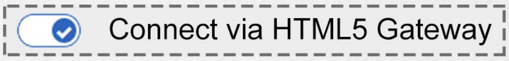
Enter the token received by email

Yyf6kuaxxJMGUNDZ9TVeYQd63ExecoBB

Sign in via the CyberArk Mobile app

01. ACCESS TO ACCOUNTS AND SYSTEMS

After the user has logged into the CyberArk system, a list of systems which he is allowed to connect to will be presented. To connect to a server, the user must click on the **Connect** button on the right side of the screen. After the click a popup window will be opened. Now the user has the choice of whether the connection should be established via RDP or HTML5 (*check the **Connect via HTML5 Gateway** box*).



☑ Connect via HTML5 Gateway

After clicking the Connect button once again, a connection will be established to the system.

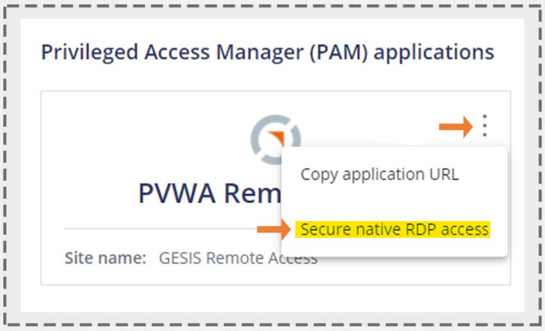
Note: If the connection isn't running stable, try a connection via **Secure Native RDP Access**. The process for this access variant is described in the next page of this documentary.

CYBERARK - PRIVILEGED REMOTE ACCESS

SECURE NATIVE RDP ACCESS

01. DOWNLOAD AND EXECUTE RDP-FILE

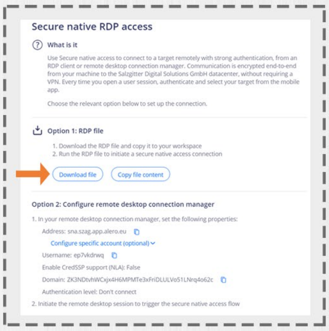
To access a server via Secure Native Access (RDP) the user has to open the menu by clicking on the 3-dot symbol and then select the menu item **Secure Native RDP Access**.



Privileged Access Manager (PAM) applications

PVWA Rem

Site name: GESIS Remote Access



Secure native RDP access

What is it

Use Secure native access to connect to a target remotely with strong authentication, from an RDP client or remote desktop connection manager. Communication is encrypted end-to-end from your machine to the Salzgitter Digital Solutions GmbH datacenter, without requiring a VPN. Every time you open a user session, authenticate and select your target from the mobile app.

Choose the relevant option below to set up the connection.

Option 1: RDP file

1. Download the RDP file and copy it to your workspace
2. Run the RDP file to initiate a secure native access connection

Option 2: Configure remote desktop connection manager

1. In your remote desktop connection manager, set the following properties:

Address: sna.szag.app.alero.eu

Configure specific account (optional)

Username: ep7vkdrwq

Enable CredSSP support (NLA): False

Domain: ZK3NDtvhWCxjx4H6MPMTe3xFriDLULVo51LNrq4o62c

Authentication level: Don't connect

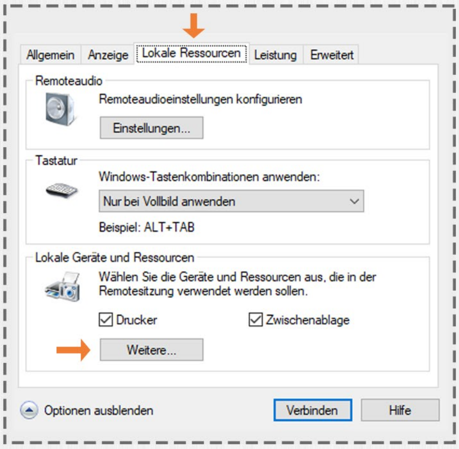
2. Initiate the remote desktop session to trigger the secure native access flow

Now a window opens, and the user needs to click on **Download File** to start downloading the RDP file. To login into a system the file needs to be executed after the download. *The instructions at the bottom of the window can be ignored.*

02. CONFIGURATION: FILE EXCHANGE *(OPTIONAL)*

If the user wants to exchange files with the server, he first needs to right click on the RDP file and select **edit**. In the **local resources** tab, click on the **more...** button which is located at the **local devices and resources** area. In the now appearing window, check the **drives** box and click ok to confirm.

Note: The user's local drives then appear in the target system as network drives *(„Z“)*.



Remoteaudio

Remoteaudioeinstellungen konfigurieren

Tastatur

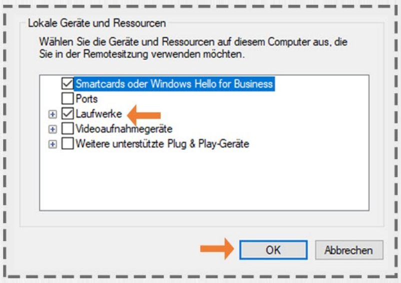
Windows-Tastenkombinationen anwenden: Nur bei Vollbild anwenden

Beispiel: ALT+TAB

Lokale Geräte und Ressourcen

Wählen Sie die Geräte und Ressourcen aus, die in der Remotesitzung verwendet werden sollen.

☑ Drucker ☑ Zwischenablage



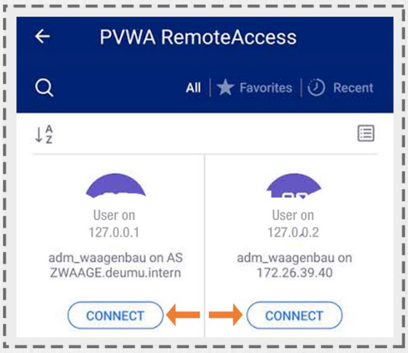
Lokale Geräte und Ressourcen

Wählen Sie die Geräte und Ressourcen auf diesem Computer aus, die Sie in der Remotesitzung verwenden möchten.

- ☑ Smartcards oder Windows Hello for Business
- ☐ Ports
- ☑ Laufwerke
- ☐ Videoaufnahmegeräte
- ☐ Weitere unterstützte Plug & Play-Geräte

03. ESTABLISH A CONNECTION

To establish a connection the user needs to click on the connect button in the RDP menu. Then the user receives a push message from the CyberArk Mobile App on his smartphone indicating that a connection is about to be established. Once the user has confirmed the access (*click on connect*), a target system needs to be selected (*also click on connect*). After the click a connection will be established via RDP.



PVWA RemoteAccess

User on 127.0.0.1

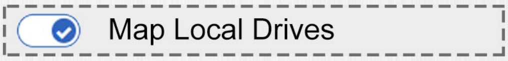
adm_waagenbau on AS ZWAAGE.deumu.intern

User on 127.0.0.2

adm_waagenbau on 172.26.39.40

01. ALLOW ACCESS TO LOCAL DRIVES

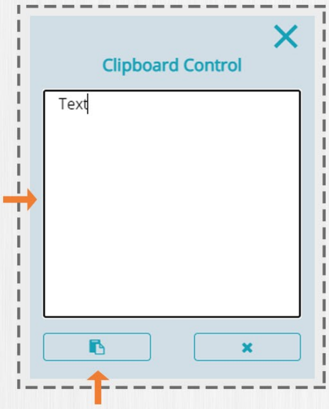
Access to the local drives must be allowed in CyberArk. To do so, it is necessary to check **Map Local Drives** in the popup window that appears after clicking the **Connect** button. This causes the drive **Z:\** to appear in the explorer of the target system.



Map Local Drives

02. CLIPBOARD USAGE

To copy text in a HTML5 session, it is necessary for the user to open the **Clipboard Control** window via **CTRL + ALT + SHIFT**. The contents of the system clipboard can be pasted into the window that appears via **right click + paste** or **CTRL + V** (*only characters; no files*). Then, at the bottom left, **copy to local clipboard** must be clicked to copy the local contents to the clipboard of the target system.

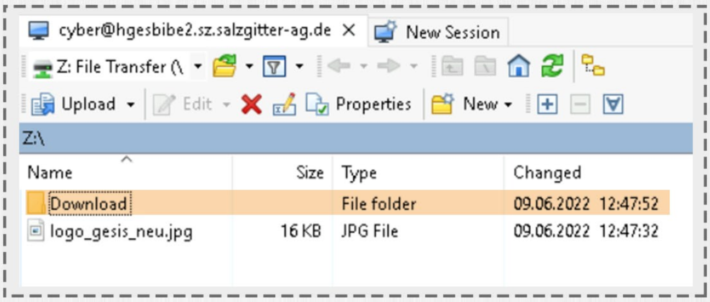


Clipboard Control

Text

03. FILE TRANSFER

If files need to be copied **from the local pc to the target system**, it is sufficient to open the drive **Z:\** in the explorer of the target system and to drag & drop the files from the local pc into the browser window. The files will then be uploaded to the drive **Z:\** of the target system.



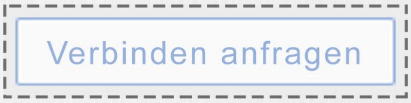
Z:\

Name	Size	Type	Changed
Download		File folder	09.06.2022 12:47:52
logo_gesis_neu.jpg	16 KB	JPG File	09.06.2022 12:47:32

If files need to be copied **from the target system to the local pc**, these files must be copied or moved to the folder **Z:\Download** on the target system. A download dialog will then appear on the local pc, which the user only needs to confirm in order to download the file.

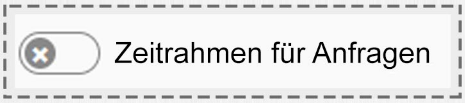
01. REQUEST A CONNECTION

In CyberArk, it may be necessary to request the connection to a desired system and have it confirmed by an administrator before the system can be accessed. This is done by clicking on the **Verbinden anfragen** button on the respective system.



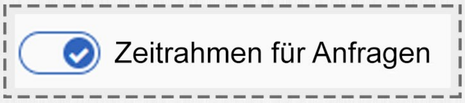
02. DEFINE SPECIFICATIONS FOR THE CONNECTION

In the now appearing window, the user can define the specifications for the connection. In addition to entering an (*optional*) **reason** for a connection, the user can also enter a **time frame**.



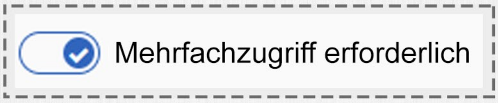
☐ Zeitrahmen für Anfragen

If the "**Zeitrahmen für Anfragen (*time frame*)**" checkbox is not activated, the user may once establish a **single connection** to the desired system after his request has been approved by an administrator. In doing so, he is not bound to a time limit.



☑ Zeitrahmen für Anfragen

Activating the "**Zeitrahmen für Anfragen (*time frame*)**" checkbox limits the time in which the user may establish a **single connection** - for this purpose, the fields "**Von (*from*)**" and "**Bis (*till*)**" needs to be filled. The user may now access the target system **exactly once** within the **time frame** defined in this way.



☑ Mehrfachzugriff erforderlich

If it is necessary that the user need to access the same system more than once within the specified time frame, the "**Mehrfachzugriff erforderlich (*multiple access required*)**" checkbox must be activated. the user may now access the target system **as often as desired** within the defined **time frame.**

03. SEND REQUEST

By clicking on "**Anfrage senden (*send request*)**" the user's access request is sent to the administrators. As soon as an administrator has granted access, the user is informed by an email and can now access the target system via CyberArk according to the previously defined specifications.