

CLAROTY SECURED REMOTE ACCESS

External User Guideline
Claroty v4.0.2

November 14, 2025

FORVIA
Inspiring mobility



Global
Information
Technologies

AGENDA

01

Introduction to
Claroty

02

Pre-requisites

03

Workflow to
use services

04

Server
Connection
service

05

Tunnel
Application
service

06

File transfer
(sFTP)

01 INTRODUCTION TO CLAROTY

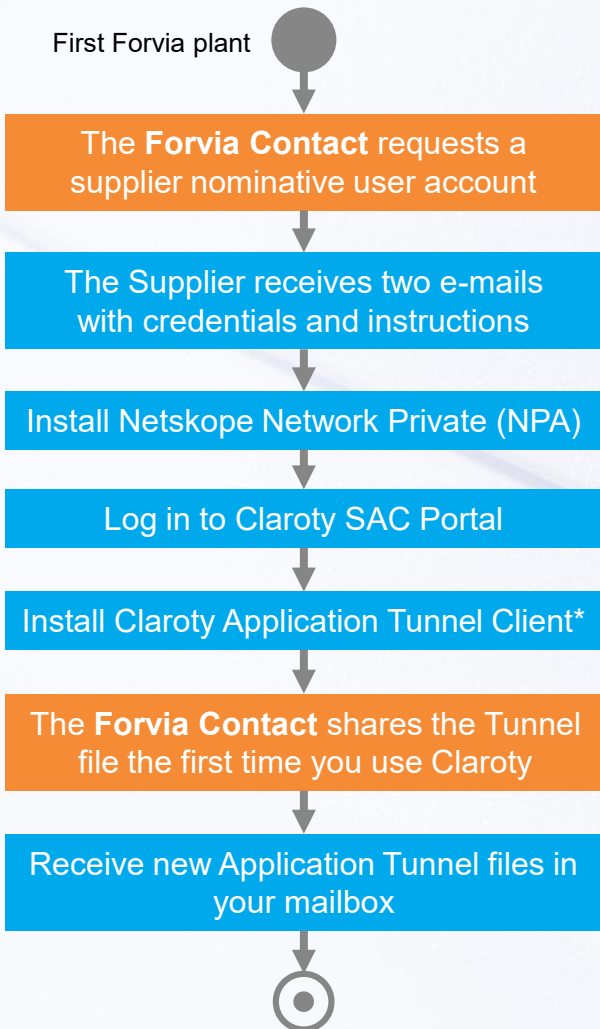
Claroty provides Secure Remote Access to Industrial Control Systems for maintenance, control and diagnostics

> Scope

- This external user guideline provides guidance to **external suppliers** providing remote support to Forvia industrial plants

02 PRE-REQUISITES: WORKFLOWS

Supplier nominative account creation

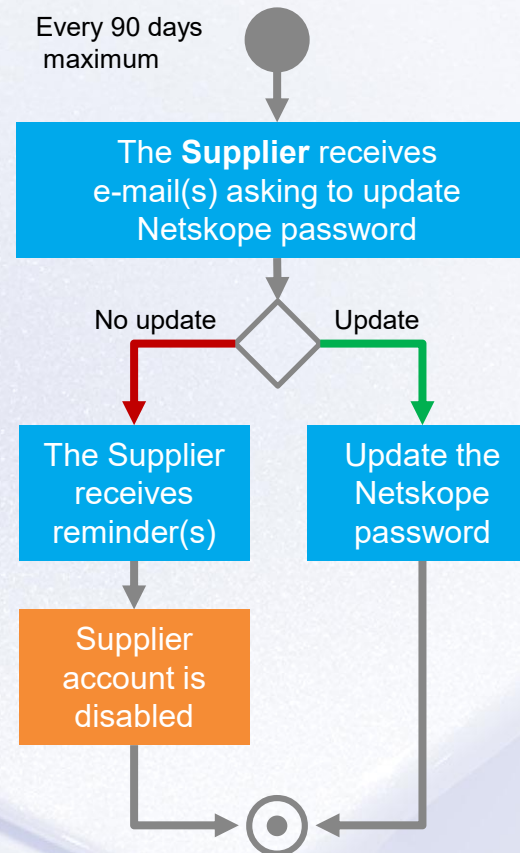


Supplier account extension

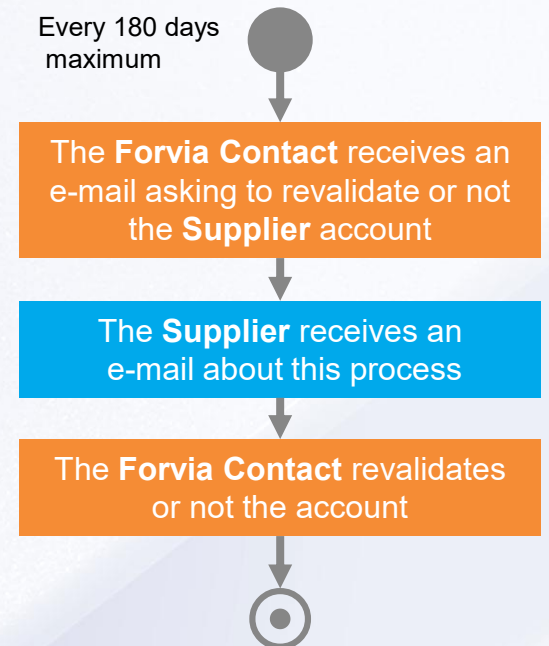


* Downloading App Tunnel client is only possible when your Supplier Group has been associated to an equipment tunnel you will access to

Supplier account update



Supplier account revalidation



Supplier

Forvia

FORVIA
Inspiring mobility



02 PRE-REQUISITES: NOMINATIVE ACCOUNT CREDENTIALS

- ❶ Once your **Forvia Contact** has requested the creation of a supplier account, you will receive two e-mails
- ❷ The first e-mail provides your **Account name** associated to your company e-mail address, along links to access resources to fulfill pre-requisites (see [next slide](#))
- ❸ The second e-mail provides the **Initial password**

2 Invitation to FORVIA Remote Access with Netskope NPA - User Account

From ExternalAccountManagement@faurecia.com <ExternalAccountManagement@faurecia.com>
To forvia.supplier@pm.me
Date Friday, October 24th, 2025 at 11:21

Dear FirstName LASTNAME

EXXXXXXX@b2b.ww.faurecia.com

an account for FORVIA Remote Access with Netskope Network Private (NPA) access has been generated for you.

Please use the following account:

Accountname: **EXXXXXXX@b2b.ww.faurecia.com**
Email: forvia.supplier@pm.me

Before you can access the resources at FORVIA, please install the Nets factor for authentication.

Please follow the instructions at <https://sec-ras.ww.faurecia.com/>, section

To enroll your user with Netskope/PING, visit the 'SEC-RAS Portal User Enrollment' at <https://sec-ras.ww.faurecia.com/documentation/userenrollment.html>

3 ## Invitation to FORVIA Remote Access with Netskope NPA

From ExternalAccountManagement@faurecia.com <ExternalAccountManagement@faurecia.com>
To forvia.supplier@pm.me
Date Friday, October 24th, 2025 at 11:22

Initial password: *********

Please change the password after successful enrollment.

All needed information how to do could be found here:
<https://sec-ras.ww.faurecia.com/documentation/specops.html>

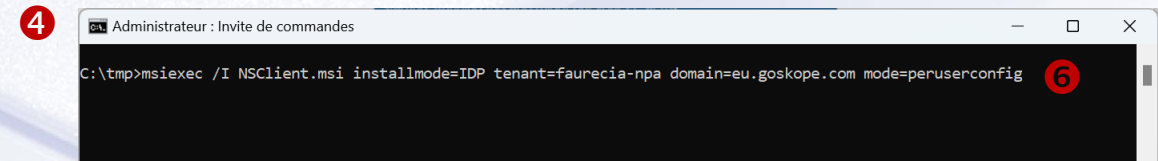
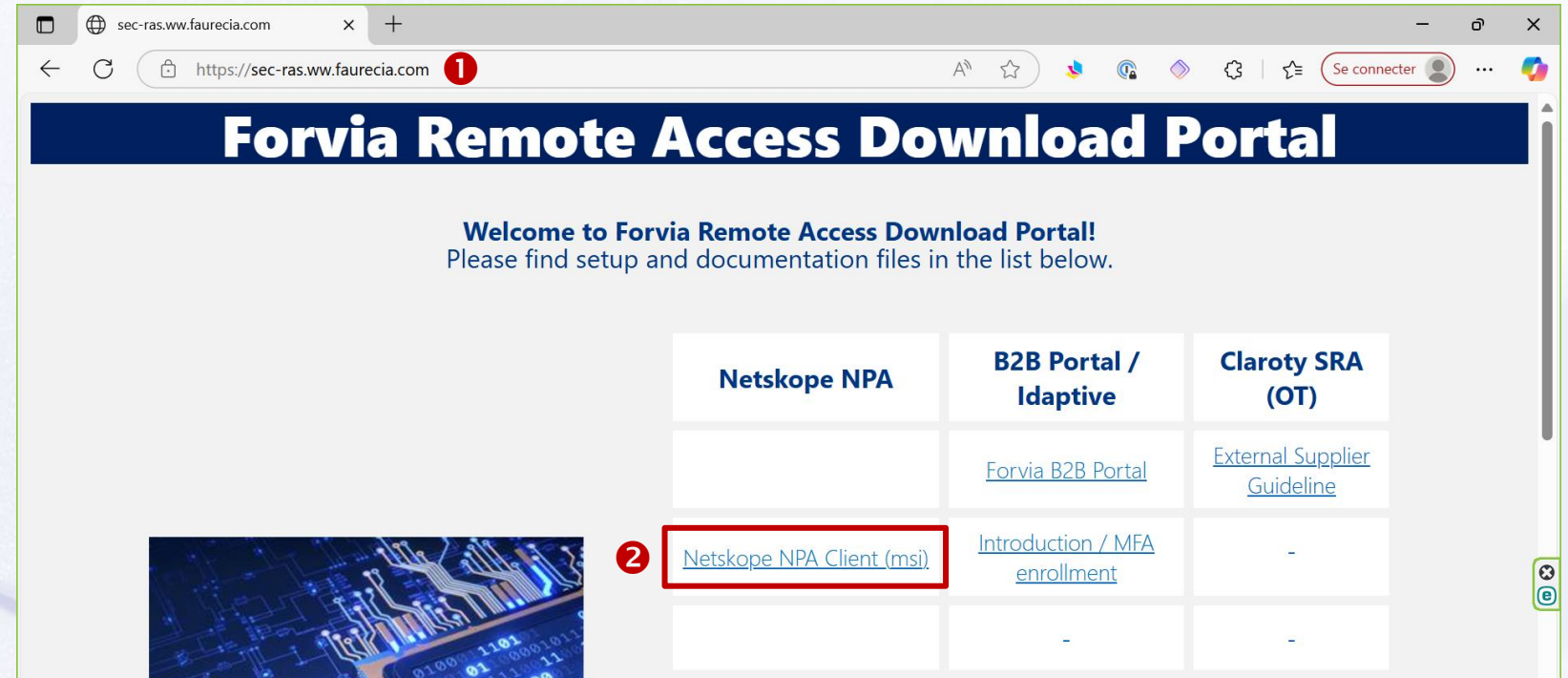
With best regards,
FORVIA Global Information Technologies (GIT)



02 PRE-REQUISITES: NETSKOPE (NPA) INSTALLATION

- ❶ Access to <https://sec-ras.ww.faurecia.com>
- ❷ Click on [Netskope NPA Client \(msi\)](#) to download the **NSClient.msi** installer
- ❸ Save it in a folder (for example C:\tmp)
- ❹ Launch a **Command Prompt** as an **Administrator**
- ❺ Navigate to C:\tmp
- ❻ Launch the following command to trigger the installation:

```
msiexec /I NSClient.msi installmode=IDP tenant=faurecia-npa domain=eu.goskope.com mode=peruserconfig
```



02 PRE-REQUISITES: NETSKOPE (NPA) INSTALLATION



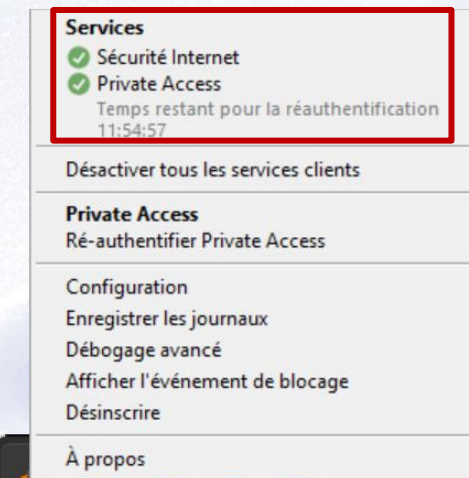
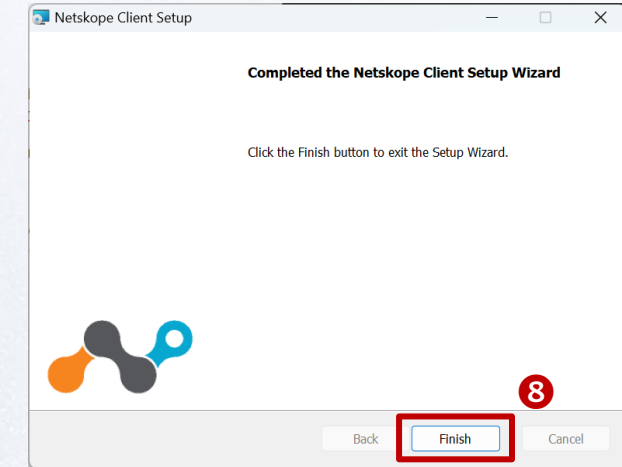
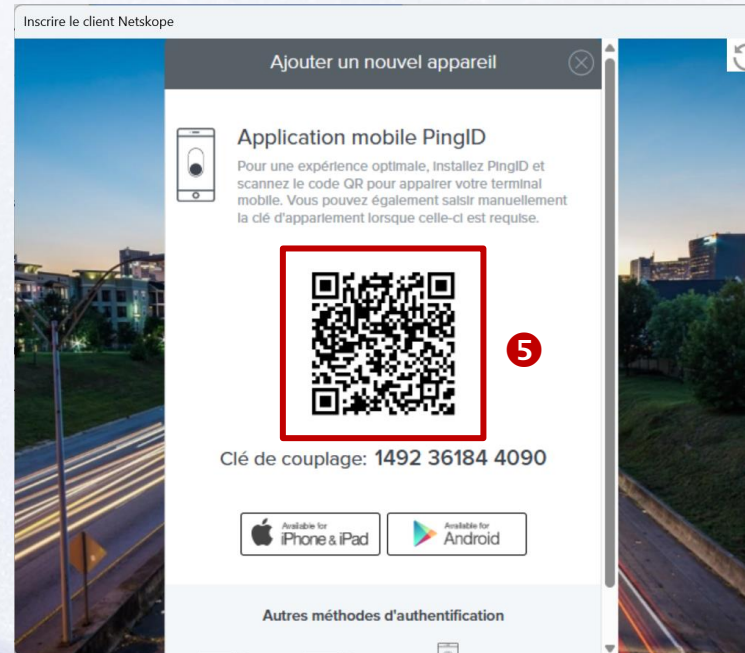
Pre-requisites
workflow

- ❶ The installation process is starting
- ❷ Enter the credentials provided by e-mail and click on **Sign On**
- ❸ To configure **2FA**, install **Ping ID** application from the app store available on your mobile phone
- ❹ Click on **Start** to pair your **Netskope** account with **Ping ID**



02 PRE-REQUISITES: NETSKOPE (NPA) INSTALLATION

- ⑤ A **QR code** and a pairing key are displayed
- ⑥ On your mobile phone, launch **Ping ID** and follow the process
- ⑦ **Scan** the QR code for pairing
- ⑧ The installation process is finishing, click on **Finish**
- ⑨ The **Netskope** client is setup (see taskbar) and **Services** activated



02 PRE-REQUISITES: PASSWORD RENEWAL

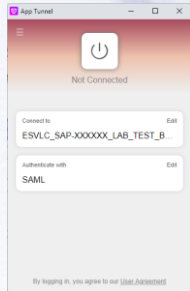


Pre-requisites
workflow

- ❶ Follow this [link](#) to start the process
- ❷ Enter your Netskope **account name** and click on **OK**
- ❸ Enter the code generated by **Ping ID** application on your mobile phone and click on **Verify**
- ❹ Enter **new password** two times to verify it, by following the required complexity, click on **OK**
- ❺ A **Success** message is displayed to confirm the update



02 PRE-REQUISITES: CLAROTY SERVICES

Service	Type of connection / protocols	Access	Requirements
Server connection	<ul style="list-style-type: none"> WEB HTTP(S) VNC RDP SSH 	<ul style="list-style-type: none"> Central SAC web access: https://sraotz.www.forvia.com <ul style="list-style-type: none"> z: SAC region (1: EMEA, 3: America, 5: Asia) 	<ul style="list-style-type: none"> Latest Google Chrome browser Latest Microsoft Edge browser
Application tunnel connection	<ul style="list-style-type: none"> Industrial protocols 	<ul style="list-style-type: none"> Application Tunnel client 	<ul style="list-style-type: none"> Supported OS: Microsoft Windows 11 OS 64-bit, Windows 10 64-bit, Windows 10 32-bit, Windows Server 2022, Windows Server 2019 (see full list slide 12)

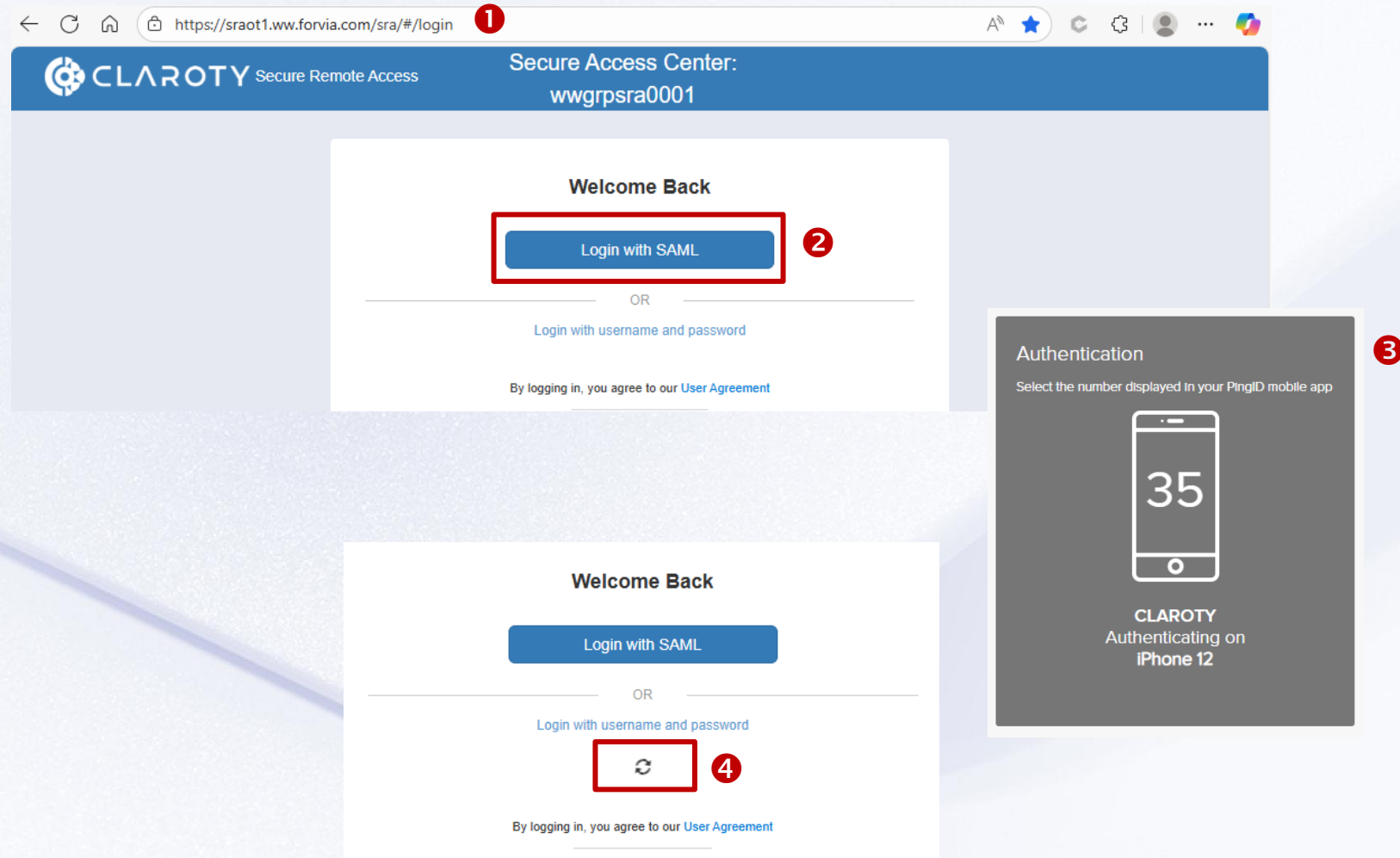
02 PRE-REQUISITES: LOGIN TO CLAROTY SAC



Pre-requisites
workflow

- ❶ Open the **Central SAC** URL in a supported browser window
- ❷ Click on **Login with SAML**
- ❸ Confirm with **PingID**
(it should be installed on your mobile phone to provide a second factor authentication)
- ❹ The connection process is taking some times before landing on the list of server connections

Caution: This step is mandatory to ensure proper activation of the mapping between your user account and the corresponding group in Claroty



02 PRE-REQUISITES: APPLICATION TUNNEL CLIENT



Pre-requisites
workflow

- ❶ Access to the **Central SAC** platform following [previous slide](#)
- ❷ In the menu, click on **Application Tunnel**
- ❸ Click on **Download Client**, and then on the needed Windows version
- ❹ Install the software

The screenshot displays the CLAROTY Secure Remote Access web interface. The top navigation bar includes the CLAROTY logo, the text 'Secure Remote Access', the 'Secure Access Center: wwgrpsra0001', the user email 'deniauds@forvia.com', a 'Logout' link, and the time 'All times are UTC+02:00'. On the left sidebar, the 'Application Tunnel' menu item is highlighted with a red box and a red circle labeled '2'. The main content area is titled 'Application Tunnel' and features a 'Download Client' button. A dropdown menu is open, showing a list of Windows operating systems. The first three items in the list are highlighted with a red box and a red circle labeled '3': 'Windows 11 64-bit', 'Windows 10 64-bit', and 'Windows 10 32-bit'. Other visible options include 'Windows 8 64-bit', 'Windows 7 64-bit', 'Windows 7 32-bit', 'Windows XP 32-bit', 'Windows Server 2022', 'Windows Server 2019', 'Windows Server 2016', 'Windows Server 2012', 'Windows Server 2008', and 'Windows Server 2003'.

Caution: In case your **Supplier Group** have not been assigned yet to a Tunnel, it is not possible to download the Application Tunnel client



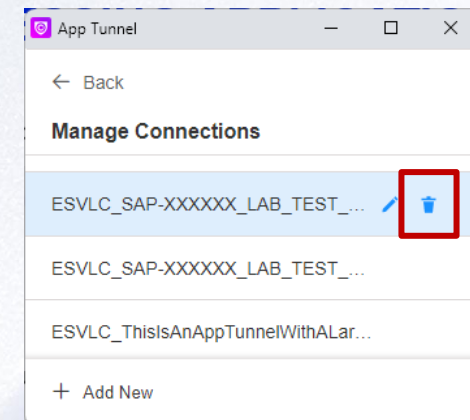
02 PRE-REQUISITES: APPLICATION TUNNEL FILES

- ❶ When you have never used Claroty, the Plant Contact should send the the tunnel file (.sra) by e-mail and organize a meeting to onboard you in the connection process using Claroty **Application Tunnel**
- ❷ Once onboarded in the Claroty usage, you received automatically the next tunnel files in your mailbox for any given plant you are working with
- ❸ One time per year (see month below), the certificate of each **Central SAC** server is renewed. As a consequence, all the tunnel files are regenerated and sent to your mailbox

Important: the former tunnel files must be deleted ❷ in **Application Tunnel** client and the new ones loaded (see also [slide 23](#))

- **EMEA** <https://sraot1.www.forvia.com> / January
- **NAO/SAO** <https://sraot3.www.forvia.com> / October
- **APAC** <https://sraot5.www.forvia.com> / April

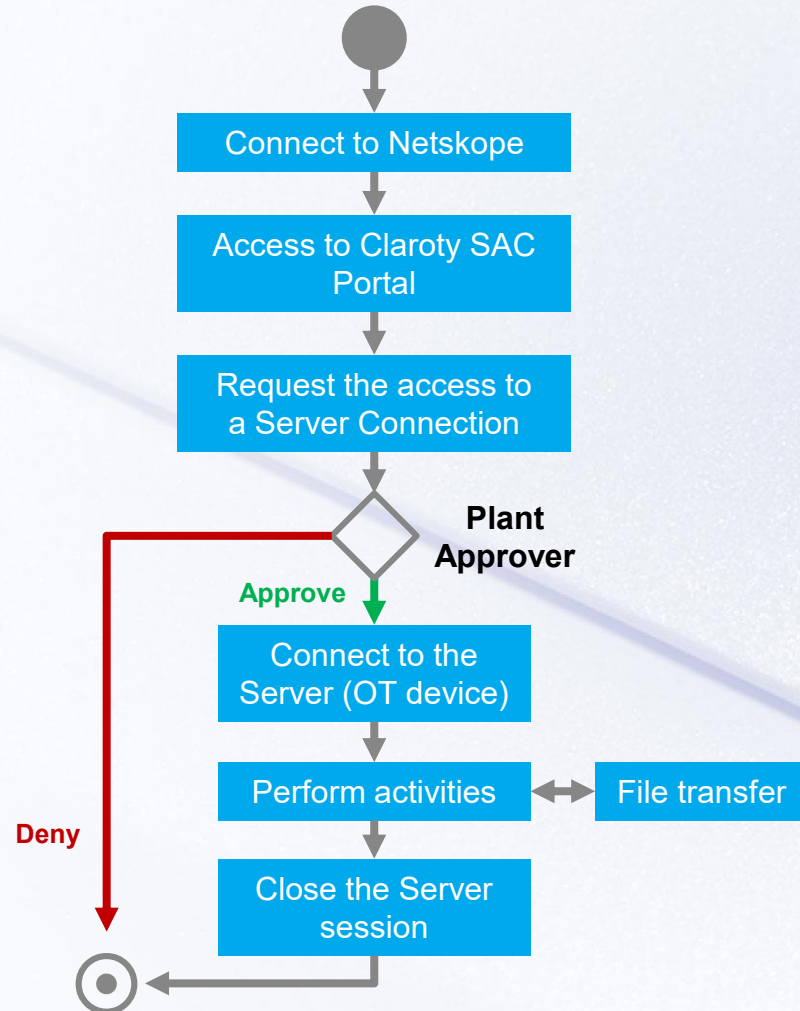
Caution: never rename a .sra tunnel file received by e-mail. It will break the tunnel and the connection will not work



03 CLAROTY SERVICES USAGE: WORKFLOWS

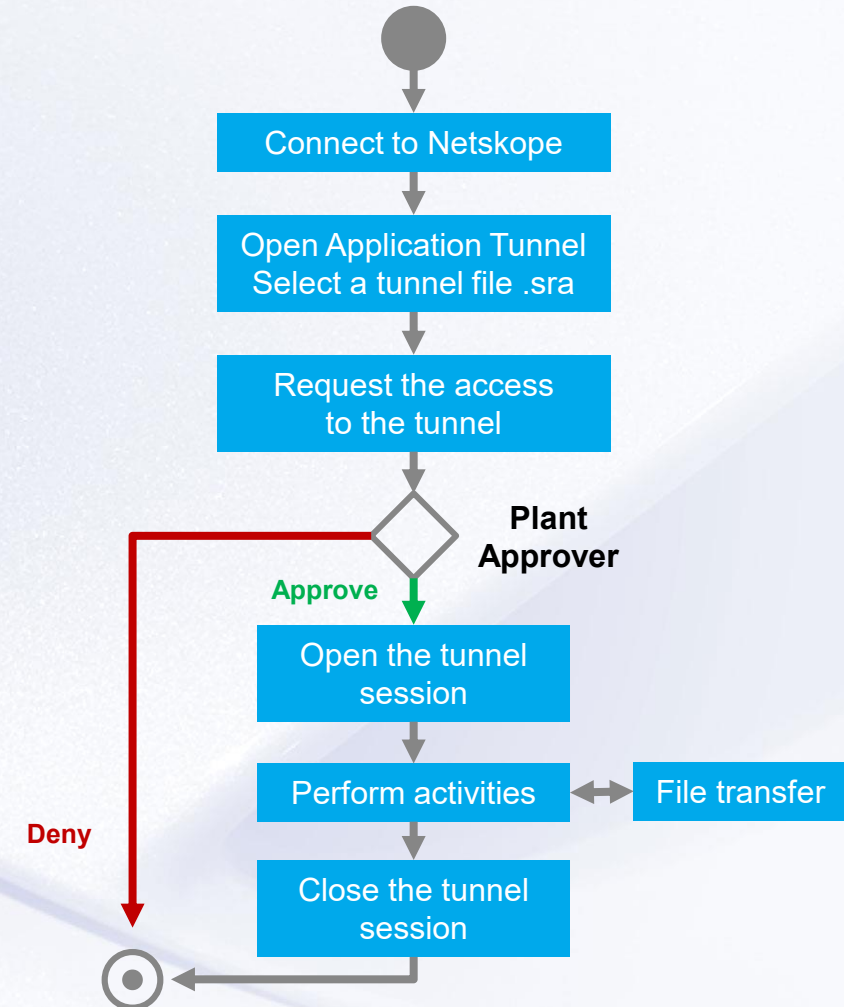
Server Connection Service

HTTPS, VNC, RDP, SSH protocols



Application Tunnel Service

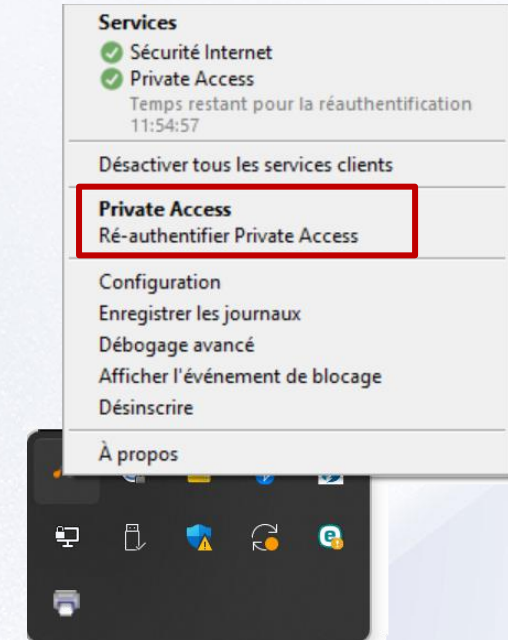
Industrial protocols (S7, Ethernet/IP, Modbus, etc.)





04 SERVER CONNECTION SERVICE

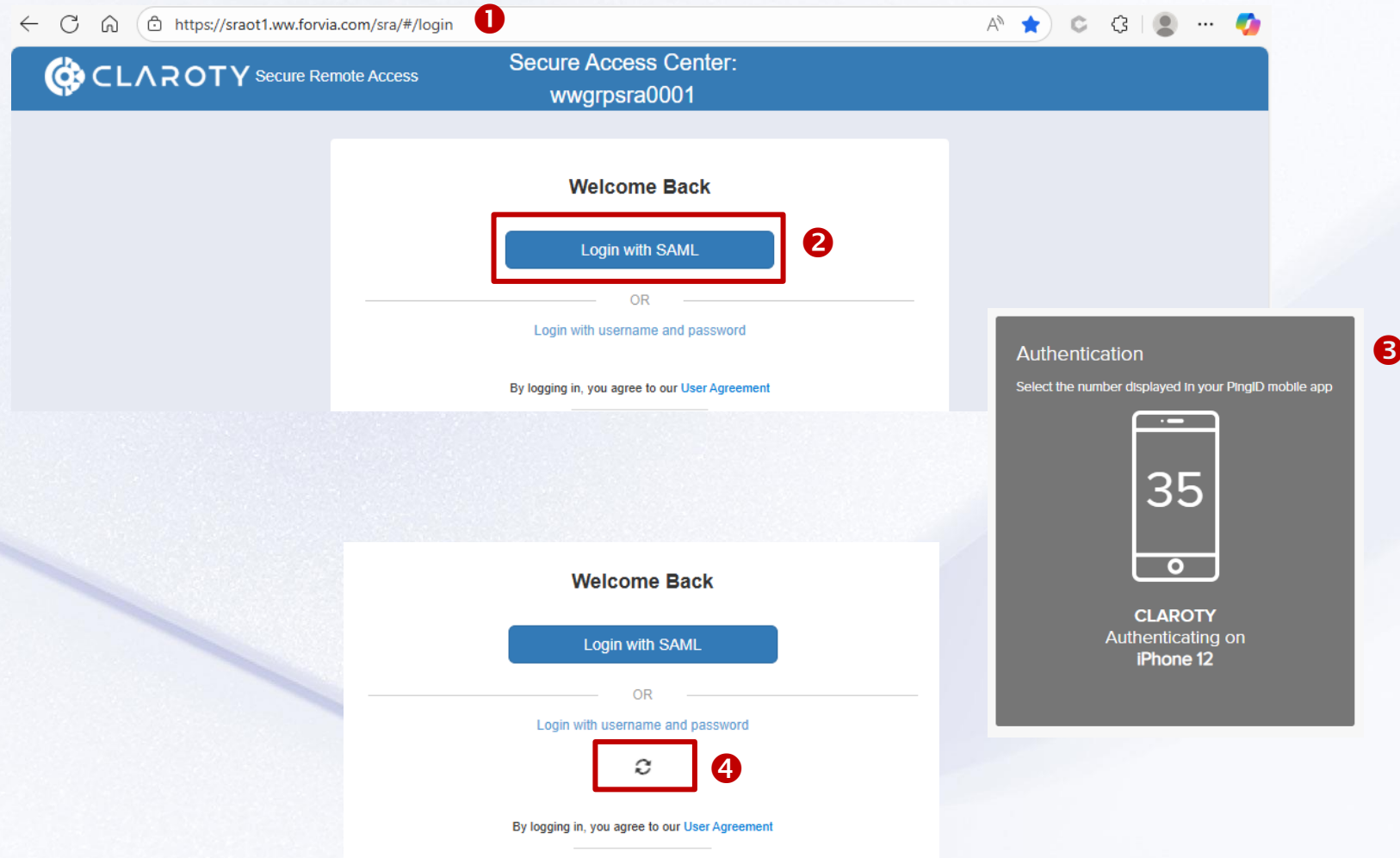
- Connect to **Netskope** service and re-authenticate **Private Access** using your credentials
- Access to Claroty **Central SAC** web interface by choosing the **Region** where is located the plant
 - **EMEA** <https://sraot1.ww.forvia.com>
 - **NAO / SAO** <https://sraot3.ww.forvia.com>
 - **APAC** <https://sraot5.ww.forvia.com>
- **2FA** (Two-factor Authentication) using **Ping ID** is required





04 ACCESS TO SERVER CONNECTION SERVICE

- ❶ Open the **Central SAC** URL (see [list](#)) in a supported browser window
- ❷ Click on **Login with SAML**
- ❸ Confirm with **PingID**
- ❹ The connection process is taking some times before landing on the list of server connections





04 LIST OF SERVER CONNECTIONS

- ⑤ The default landing page corresponds to the **Dashboard** menu
- ⑥ It consists in the **My servers** section which lists all device connections to which you can connect or request an access
- ⑦ A ● **green dot** in front of a server connection corresponds to an accessible device
- ⑧ A ● **red dot** in front of a server connection corresponds to a device currently unreachable
- ⑨ It also consists in a **My sessions** section which lists all your previous sessions

CLAROTY Secure Remote Access Secure Access Center: wwgrpsra0001 deniauds@forvia.com | Logout | All times are UTC+02:00

[Dashboard](#) ⑤
[Application Tunnel](#)

My servers ⑥

⑧	Name	Site	Address	Protocol	Username	
⑧	PTSJSCSW1001_E37_WEB	PTSJSSRA0001	https://10.80.110.108	WEB		Request access
	PTSJMCSW0001_LINE1_WEB	PTSJMSRA0001	https://10.80.32.11	WEB		Request access
⑦	PTSJSWID4701_RDP	PTSJSSRA0001	10.80.80.21	RDP		Request access
	PTSJMPLC0011_LINE1_WEB	PTSJMSRA0001	https://10.80.32.12	WEB		Request access

My sessions ⑨

ID	Origin	Site	Child Session	Server	State	Started	Length
145	wwgrpsra0001	PTSJSSRA0001		PTSJSCSW1024_E78_LC59_WEB	Ended, recording disabled	Mon Sep 23 2024 13:11:47	13 Seconds
144	wwgrpsra0001	PTSJSSRA0001		PTSJSCSW1001_E37_WEB	Ended, recording disabled	Thu Aug 22 2024 14:12:35	15 Seconds

04 REQUEST ACCESS TO A SERVER CONNECTION



Workflow

- 1 For a given server connection, click on **Request access**

The screenshot shows a 'My servers' table with the following columns: Name, Site, Address, Protocol, and Username. There are two server entries:

Name	Site	Address	Protocol	Username
PTSJSWID4701_RDP	PTSJSSRA0001	10.80.80.21	RDP	
PTSJMPLC0011_LINE1_WEB	PTSJMSRA0001	https://10.80.32.12	WEB	

Below the table, there are search filters for Name, Site, Address, Protocol, and Username. A red box highlights the 'Request access' button for the second server entry, with a red circle containing the number 1 next to it.

- 2 For an immediate access, select the **Expected duration**, enter a **Reason** and click on **Request**

The screenshot shows the 'Request access' form. A red circle with the number 2 is next to the 'Expected Duration' field, which contains '01' and '00'. The 'Reason' field contains 'Check application configuration'. The 'Scheduled session (optional)' checkbox is unchecked. The 'Session start time' is set to '2025-10-22' and '00:00'. The 'Session end time' is set to '2025-10-22' and '00:00'. A red box highlights the 'Request' button at the bottom right.

- 3 For a scheduled session, enter a **Reason**, check the box **Scheduled session**, select **Session date & time**, and click on **Request**

The screenshot shows the 'Request access' form. A red circle with the number 3 is next to the 'Expected Duration' field, which contains '01' and '00'. The 'Reason' field contains 'Check application configuration'. The 'Scheduled session (optional)' checkbox is checked. The 'Session start time' is set to '2025-10-22' and '14:00'. The 'Session end time' is set to '2025-10-22' and '15:00'. A red box highlights the 'Request' button at the bottom right.

04 GET ACCESS AND CONNECT TO A SERVER (OT DEVICE)



Workflow

- ④ Once the request is raised, it is **Pending the Plant Approver** feedback

The screenshot shows the 'My servers' interface with a sidebar containing 'Dashboard' and 'Application Tunnel'. The main table lists two servers. The second server, PTSJMPLC0011_LINE1_WEB, has a 'Pending' button highlighted with a red box. The first server, PTSJSWID4701_RDP, has a 'Request access' button.

Name	Site	Address	Protocol	Username	Action
PTSJSWID4701_RDP	PTSJSSRA0001	10.80.80.21	RDP		Request access
PTSMPLC0011_LINE1_WEB	PTSMJMSRA0001	https://10.80.32.12	WEB		Pending

- ⑤ In case of an immediate access: Once the request is approved, you get a **Connect** button. Click on the **Connect** button to open a session, it will last the requested duration

The screenshot shows the 'My servers' interface. The second server, PTSJMPLC0011_LINE1_WEB, now has a 'Connect' button highlighted with a red box, and a green 'Approved' status indicator is visible below it. The first server, PTSJSWID4701_RDP, still has a 'Request access' button.

Name	Site	Address	Protocol	Username	Action
PTSJSWID4701_RDP	PTSJSSRA0001	10.80.80.21	RDP		Request access
PTSMPLC0011_LINE1_WEB	PTSMJMSRA0001	https://10.80.32.12	WEB		Connect

- ⑥ In case of a scheduled session: Once the request is approved, the **Connect** button is displayed and will be available for opening the session at the **Start date and time** requested

The screenshot shows the 'My servers' interface. The second server, PTSJMPLC0011_LINE1_WEB, has a 'Connect' button highlighted with a red box. Below the table, a green status bar indicates: 'Approved, scheduled for Thu Oct 23 2025 14:00:00 and ends at Thu Oct 23 2025 15:00:00'. The first server, PTSJSWID4701_RDP, has a 'Request access' button.

Name	Site	Address	Protocol	Username	Action
PTSJSWID4701_RDP	PTSJSSRA0001	10.80.80.21	RDP		Request access
PTSMPLC0011_LINE1_WEB	PTSMJMSRA0001	https://10.80.32.12	WEB		Connect

- ⑦ At any time, you have the possibility to **Cancel request**

04 USE THE SERVER (OT DEVICE) SESSION



Workflow

- 1 Click on **Connect** button to open a session (see [previous slide](#))
- 2 Enter **credentials** and **Connect**

Enter credentials

Username	Not required
Password	<input type="password"/>
<div> 2 <input type="button" value="Connect"/> <input type="button" value="Cancel"/> </div>	

- 3 The display can be changed upon your needs to adapt the view to your screen
- 4 Depending on the type of protocol, buttons are available to interact remotely with the device
- 5 **Caution:** monitor regularly the **Time remaining** for your session. It cannot be extended!

04 USE THE SERVER (OT DEVICE) SESSION

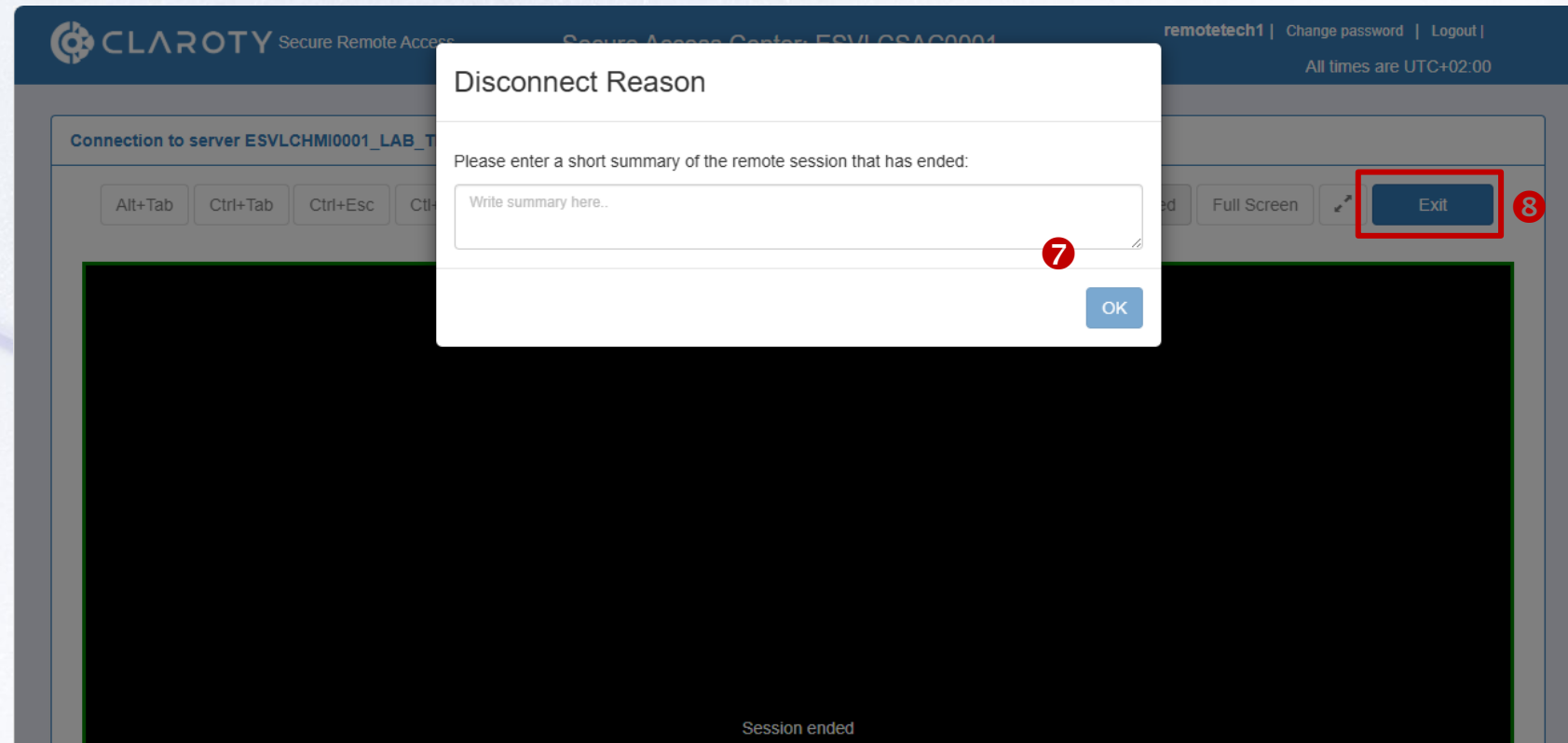
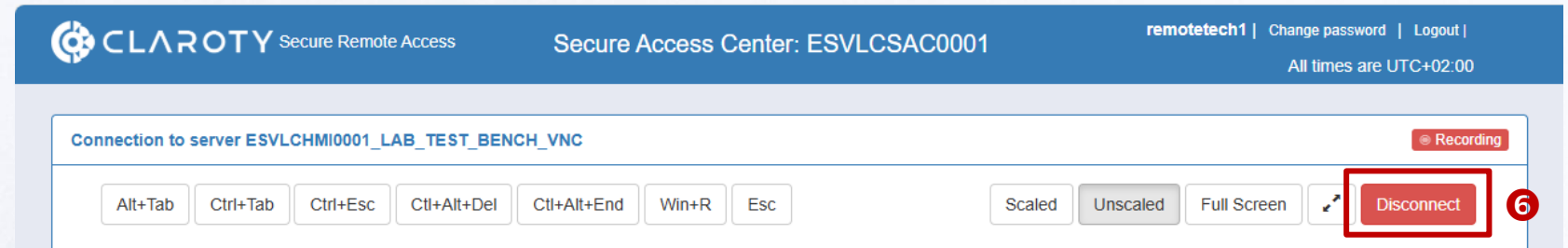


Workflow

⑥ When activity is done, click on the **Disconnect** button

⑦ Enter a summary of your activities, then click on **OK**

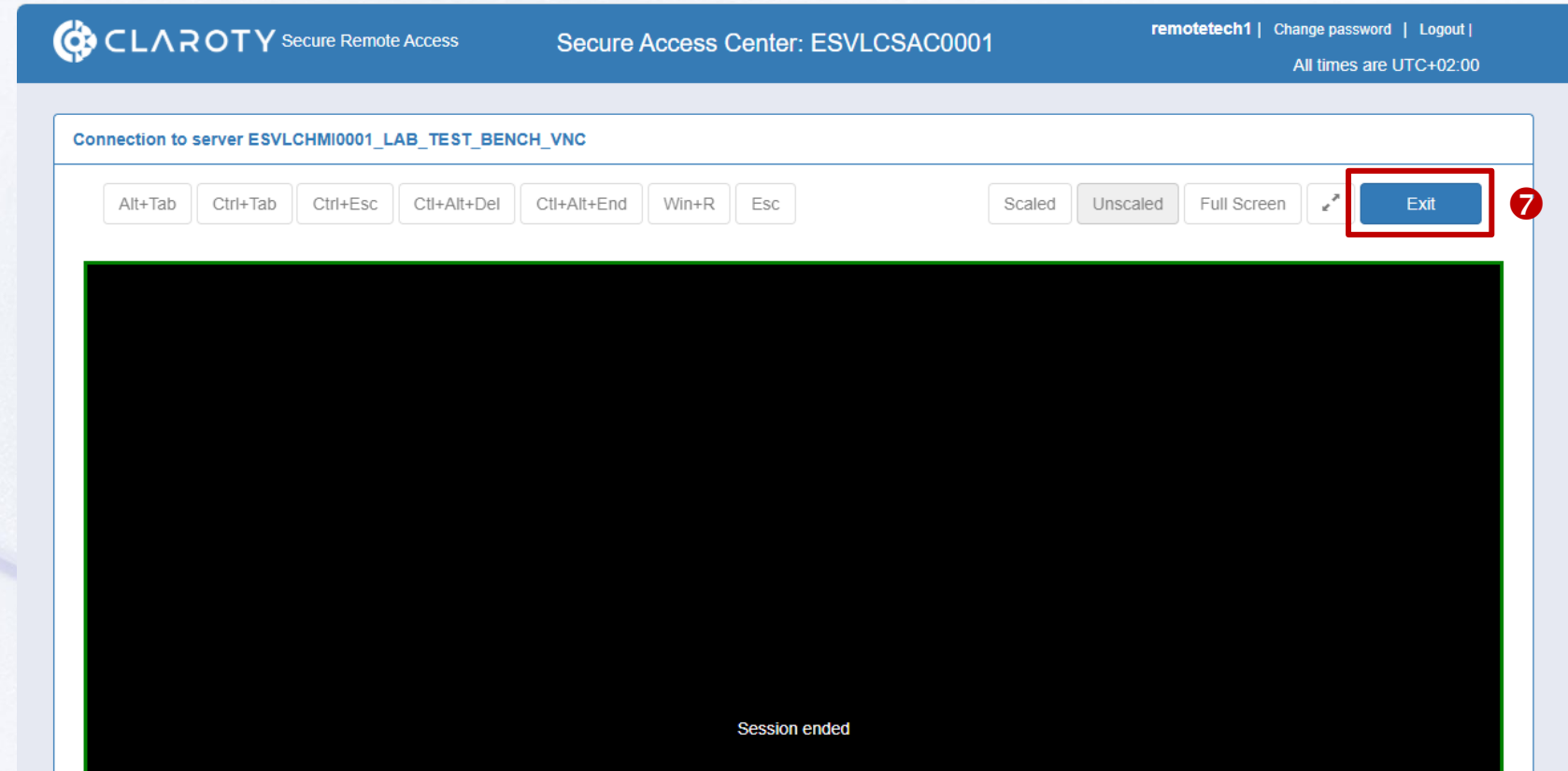
⑧ Click on **Exit** to close the window



04 USE THE SERVER (OT DEVICE) SESSION

**Workflow**


- ⑥ When the **Time remaining** is over, the session is automatically ending
- ⑦ Click on **Exit** to close the window

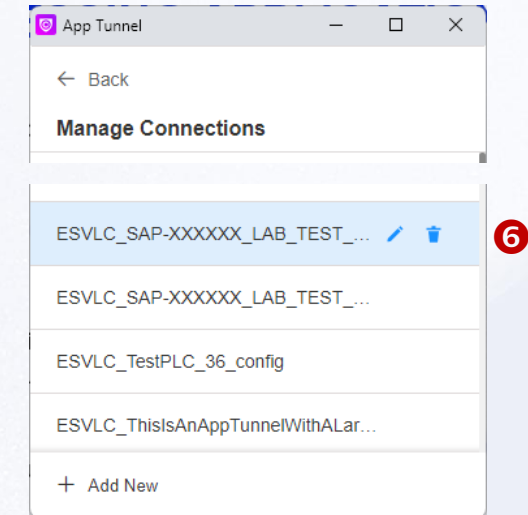
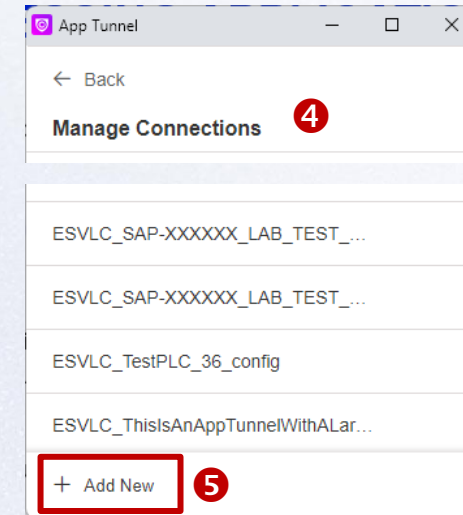
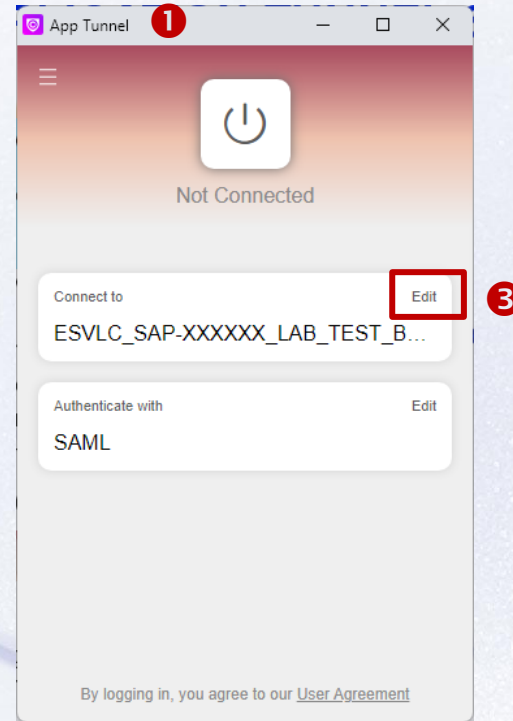




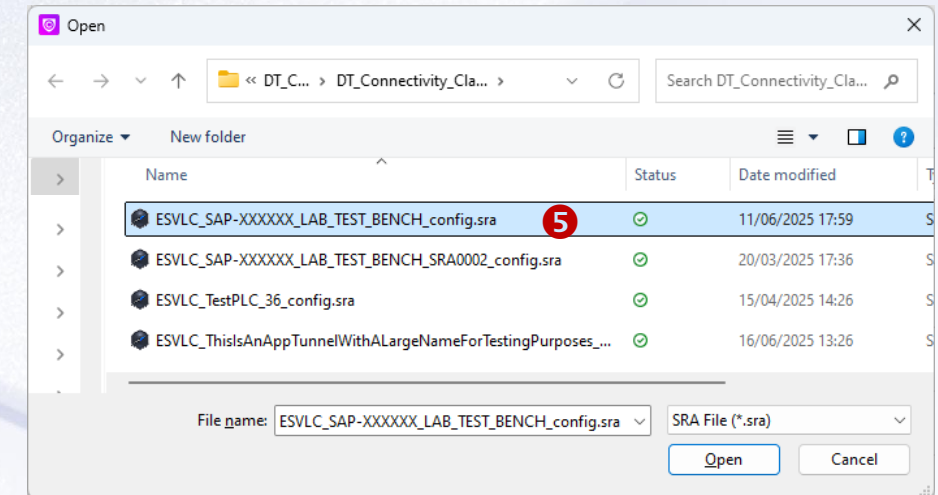
05 ACCESS TO APPLICATION TUNNEL SERVICE

Tunnel files management

- ❶ Open the **Application Tunnel** client 
- ❷ To be able to open a tunnel towards an equipment, you need to select **.sra** tunnel files in this client
- ❸ In the field **Connect to**, click on **Edit**
- ❹ The list of **Managed Connections** displayed all the .sra tunnel files already loaded in the client
- ❺ If needed, load a new file by clicking on **+Add New** and select a file saved on your computer
- ❻ Click the tunnel file corresponding to the machine / line you need to connect



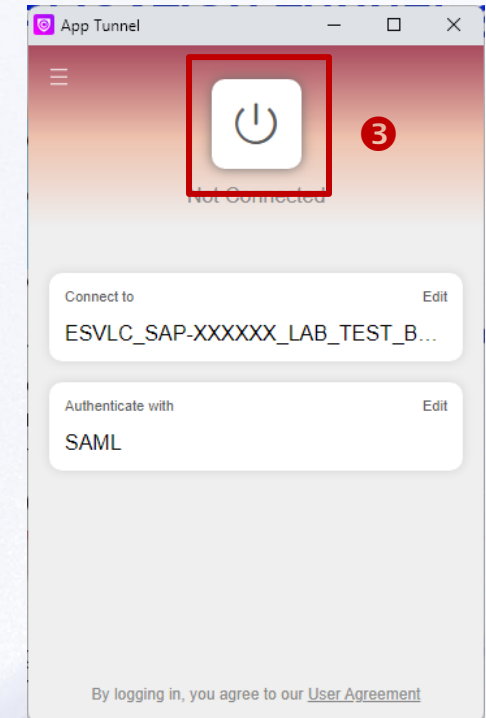
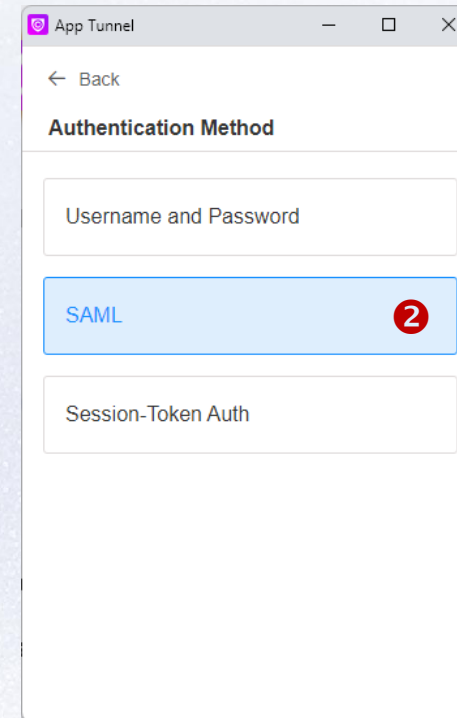
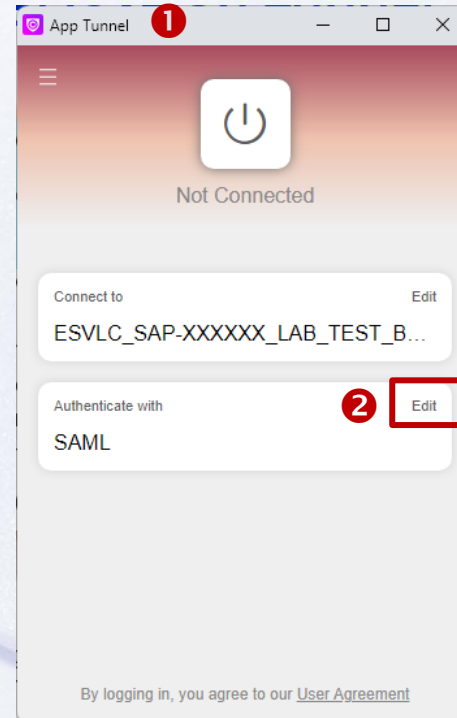
Caution: never rename a .sra tunnel file received automatically by e-mail. It will break the tunnel and the connection will not work anymore





05 REQUEST ACCESS TO AN EQUIPMENT TUNNEL

- ❶ Open the **Application Tunnel** client and select a **.sra** tunnel file as described on the [previous slide](#)
- ❷ Make sure the **Authenticate with** is set up to **SAML**. If not, click on **Edit** and select SAML
- ❸ Click on the connect button to request the access

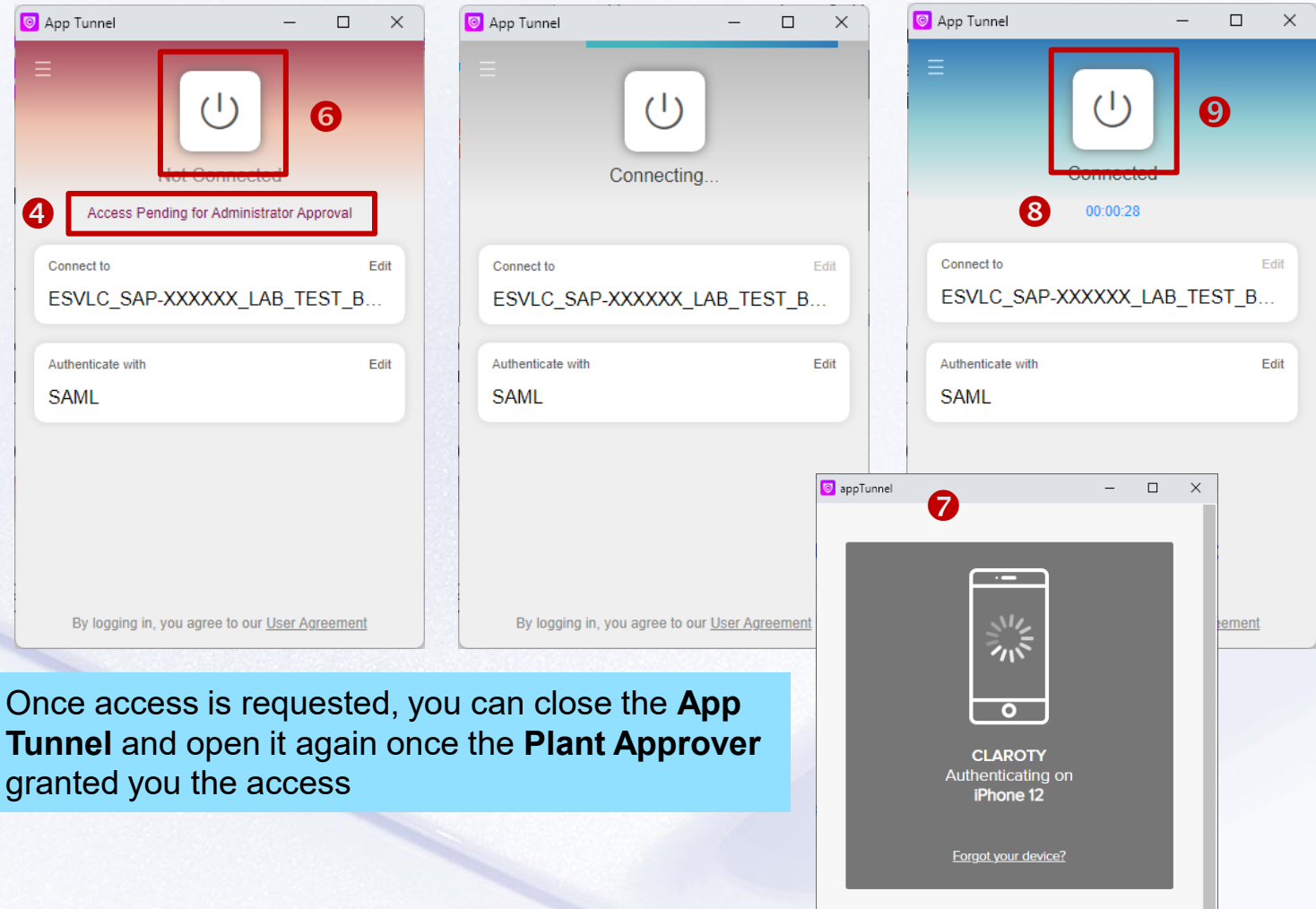


05 GET ACCESS AND OPEN AN EQUIPMENT TUNNEL



Workflow

- ④ Once the access is requested to the **Plant Approver**, the message **Access Pending for Administrator Approval** is displayed
- ⑤ **Caution:** you must liaise with the **Plant Approver** to know when the tunnel access has been approved. No confirmation will be displayed through the **App Tunnel** client
- ⑥ When you got the confirmation that it has been approved, click again on the **Connect** button
- ⑦ Confirm with **Ping ID**
- ⑧ Once connected, use the software needed to perform your activities
- ⑨ When activities are performed, click on the **Connect** button to close the tunnel



Once access is requested, you can close the **App Tunnel** and open it again once the **Plant Approver** granted you the access

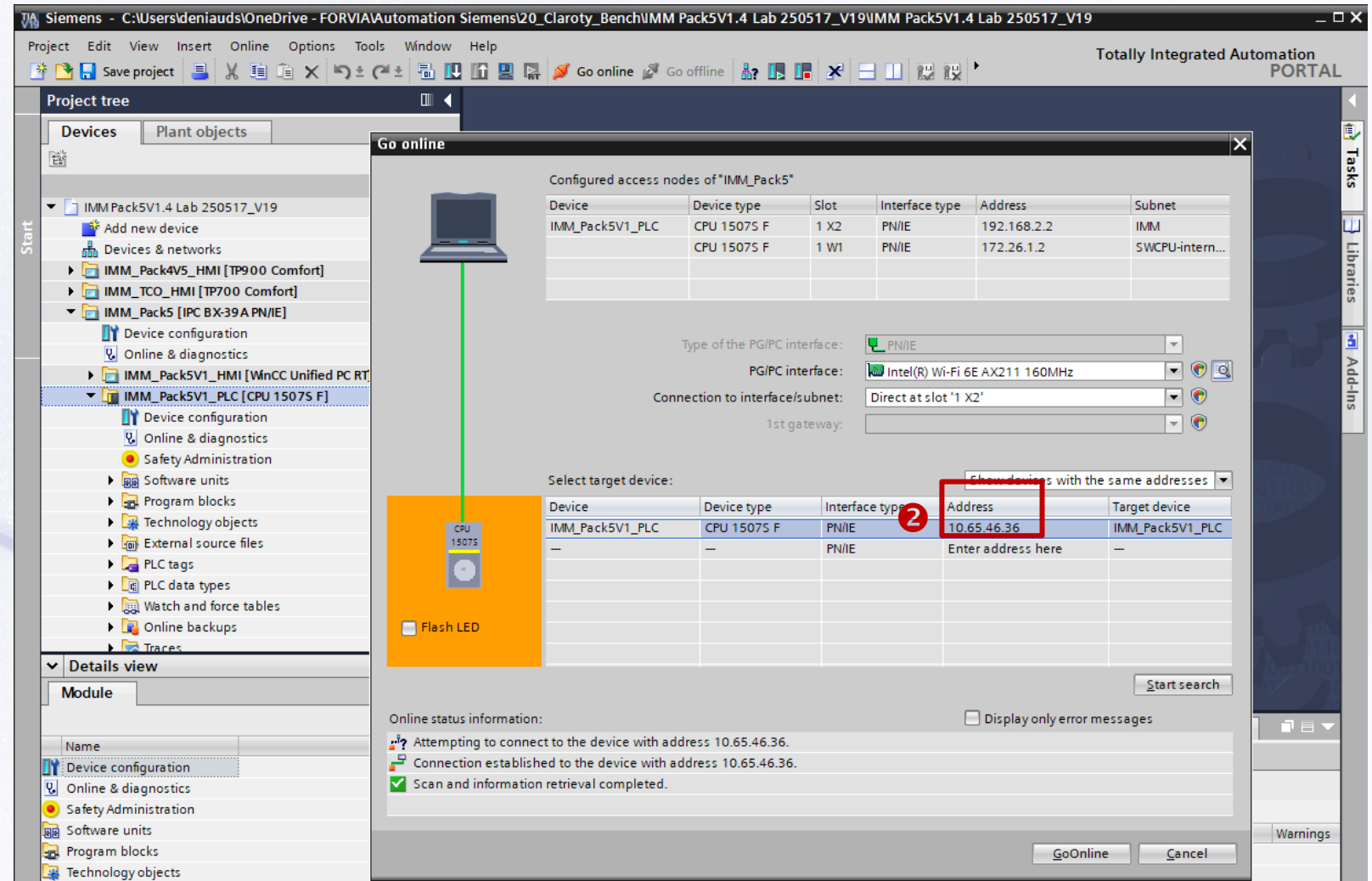
05 USE THE EQUIPMENT TUNNEL SESSION

Example: Siemens TIA Portal



Workflow

- ❶ Once the tunnel connected, open TIA Portal and the project
- ❷ In the case of a machine connected to the IT network with a NAT Router, you must use the command **Online > Extended Go online** in the menu and put the IT IP Address of the PLC exposed by the NAT Router
- ❸ In the case of a machine having a PLC interface directly connected to the IT network, simply use the usual **Go online** feature





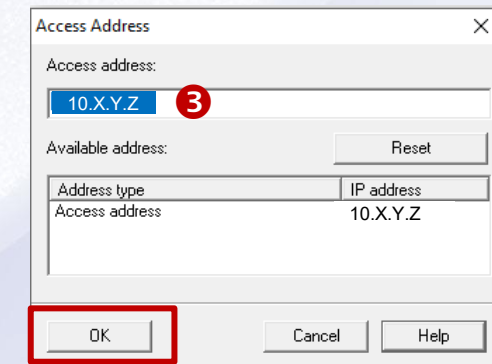
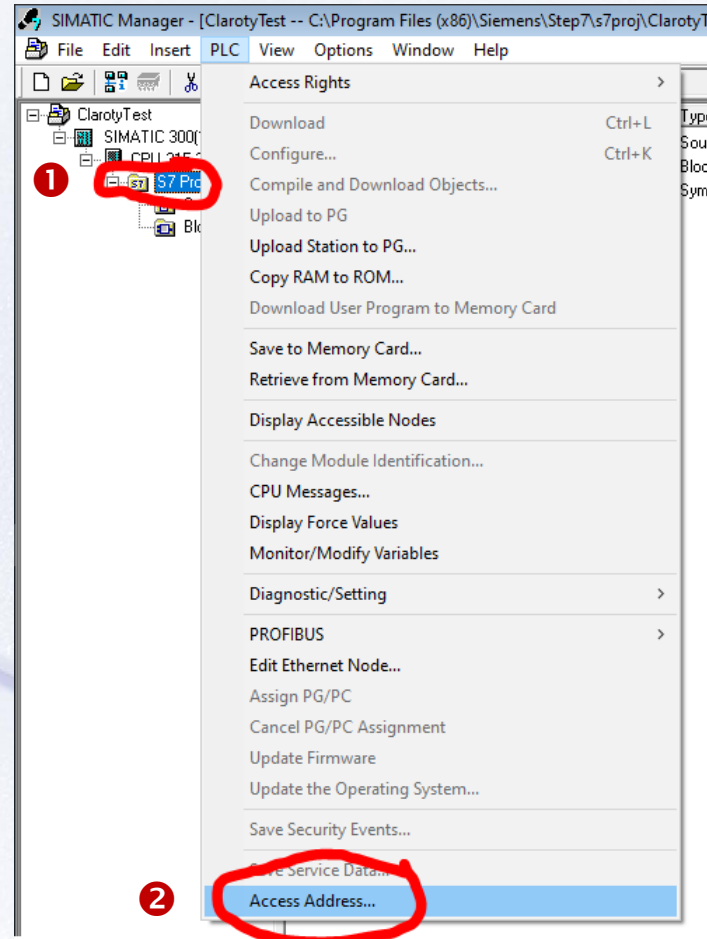
05 USE THE EQUIPMENT TUNNEL SESSION

Example: STEP7

In the case of a machine connected to the IT network with a NAT Router:

- ❶ In the SIMATIC Manager, select the S7 program of the CPU
- ❷ In the menu, select **PLC > Access Address**
- ❸ Enter the IT IP Address of the PLC exposed by the Scalance in the **Access Address** field. This address is used to reach the module

You have now specified the IP address of the module to which the connection should be established



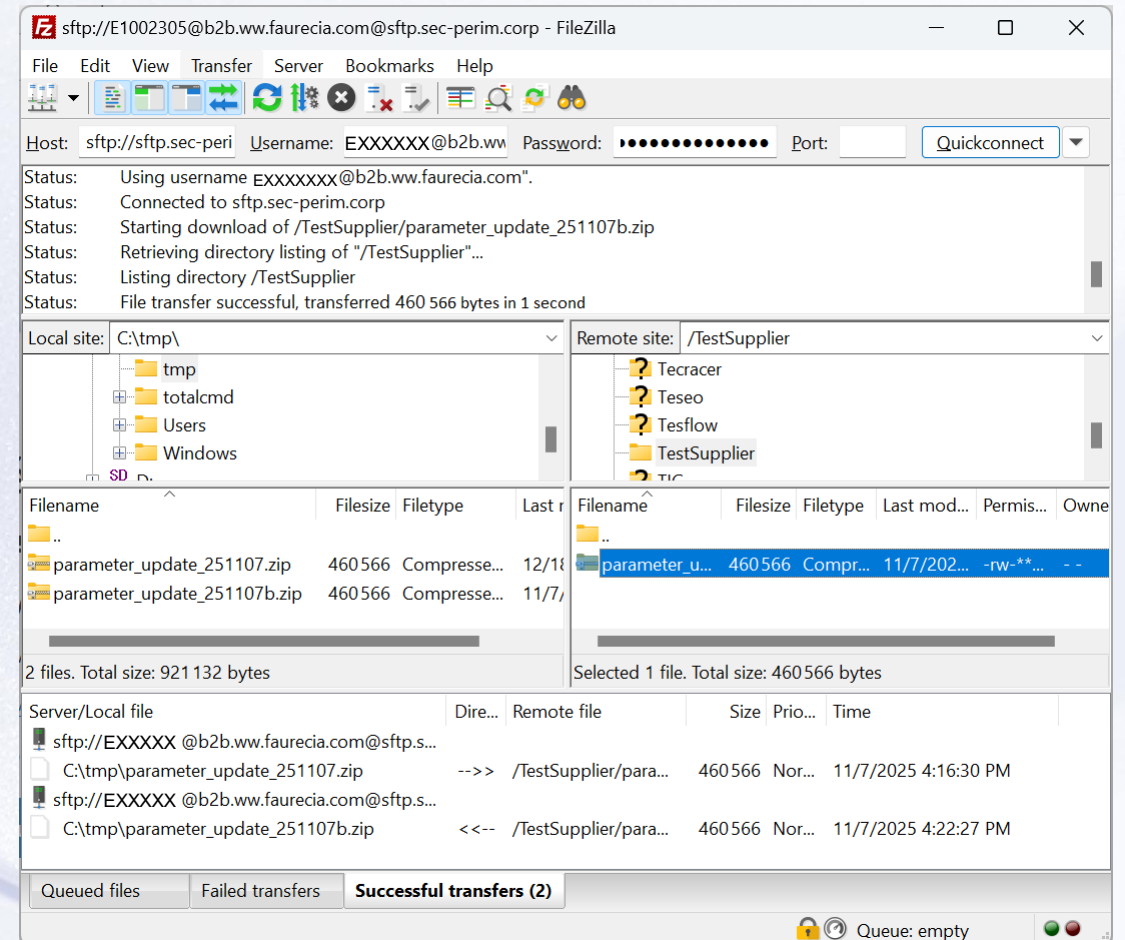


06 FILE TRANSFER (SFTP)

- ① Follow the instructions available at:

<https://sec-ras.ww.faurecia.com/documentation/ftpresource.html>

Note: This feature is only available if your **Plant Contact** has explicitly requested it to fulfill your remote access needs. Liaise with your **Plant Contact** to enable it





Global
Information
Technologies