Verallia´s guideline how to use Zscale client connector

Overview

Zscaler Client Connector is an application installed on your device to ensure that your internet traffic and access to organization's internal apps are secure and in compliance with organization's policies, even when you're off corporate network.

No matter where you're accessing the web, Zscaler Client Connector ensures that your traffic is forwarded to and protected by the Zscaler Internet Access (ZIA) service. Additionally, with Zscaler Private Access (ZPA) enabled, you can also securely access organization's internal resources from any location. Finally, with the Zscaler Digital Experience (ZDX) service enabled, Zscaler Client Connector performs synthetic probing to a desired Software-as-a-Service (SaaS) application or internet-based service (e.g., OneDrive, Gmail, etc.) to triage and pinpoint the source of performance issues (just for Verallia internal users).

Prerequisite

Certificate Installation for Authentication:

First of all, you must get a valid certificate to use our RAS.

You will receive an E-Mail with the required credentials and certificate

including the instructions link to prepare the requirements on your computer.

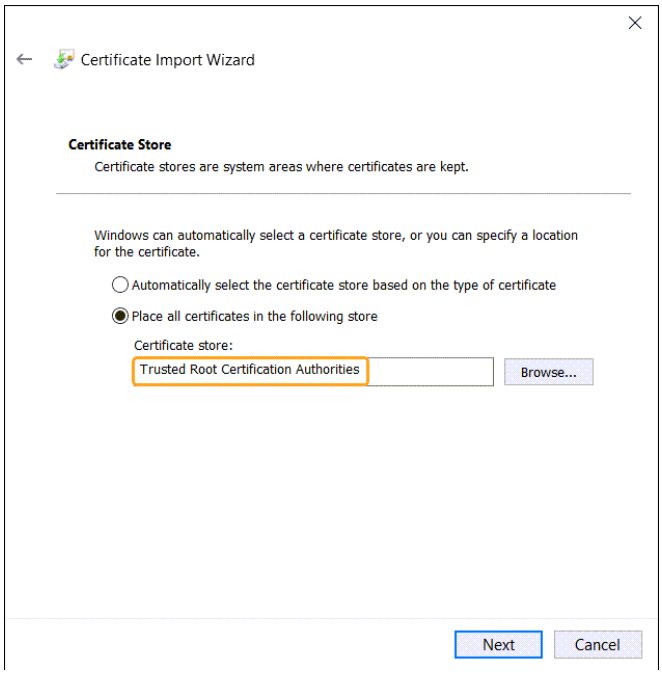
The certificate will allow you to be authenticated on our RAS Platform.

**Please note that each certificate can be installed on up to 3 devices.*

Certificate Installation

First run the certificate with required privilege

You will see the below page



For the rest of the wizard, you just need to click on next since the wizard would ask you to provide the password (you should use the one that has been sent to you via email)

After that no changes would be required since you will receive the notification that the certificate is installed successfully.

Remote Access Client Zscaler App - Installation

You must install the client Zscaler App on your computer.

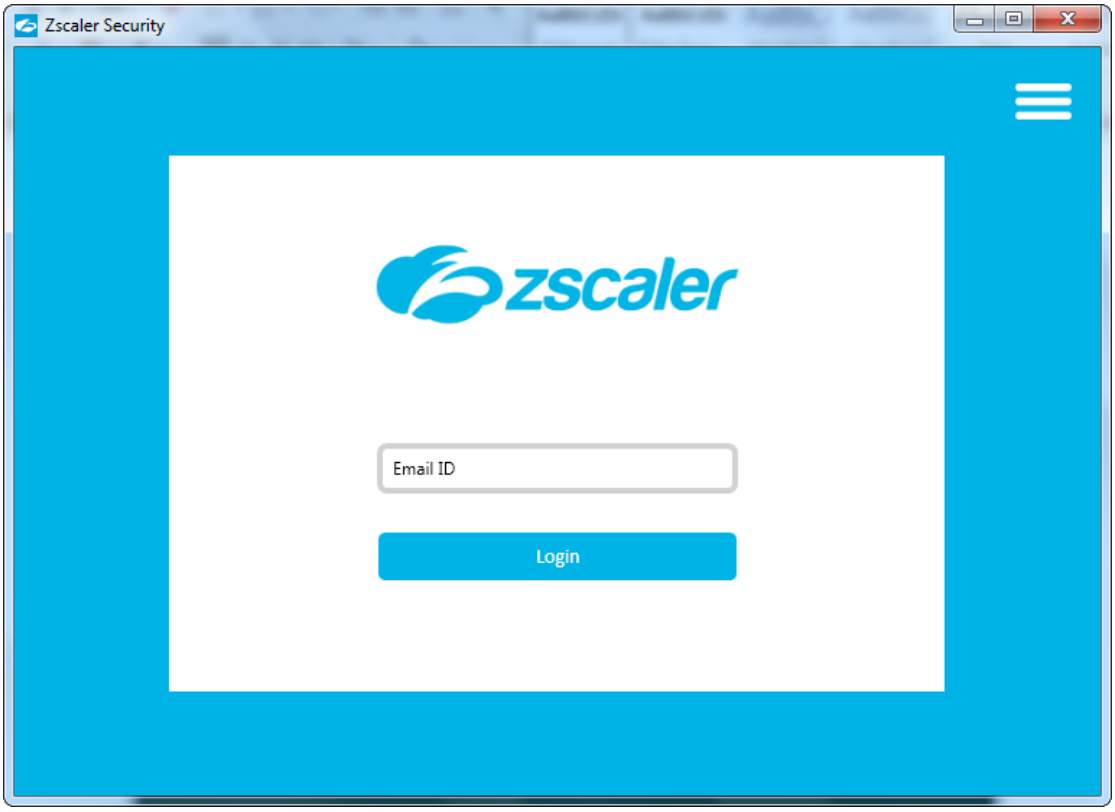
Please select the right version based on the machine.

The latest client Zscaler Application can be downloaded from the below link:

https://vpn-partners.verallia.com/

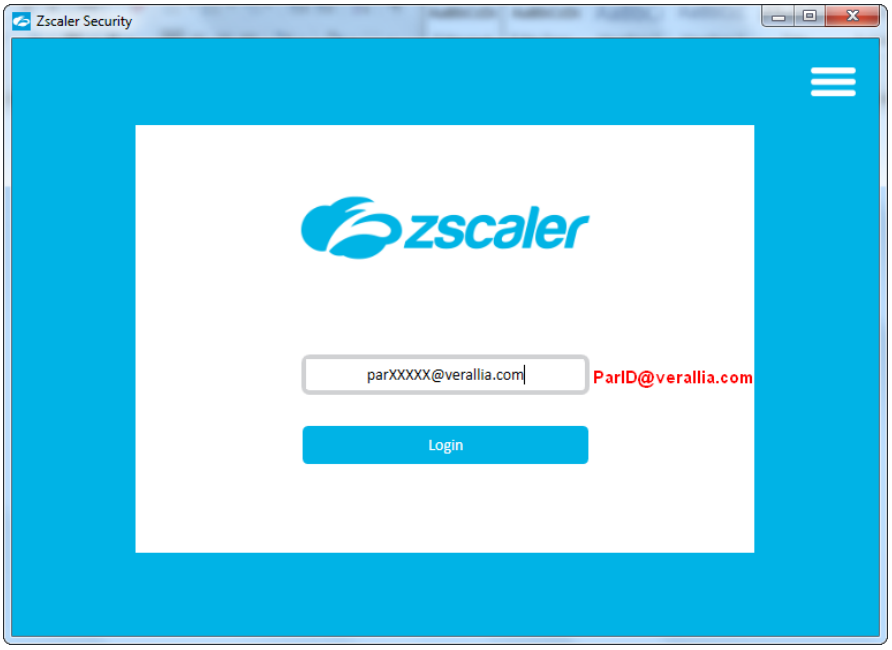
How to Use the Remote Access Service

After the installation, first Open Zscaler App.

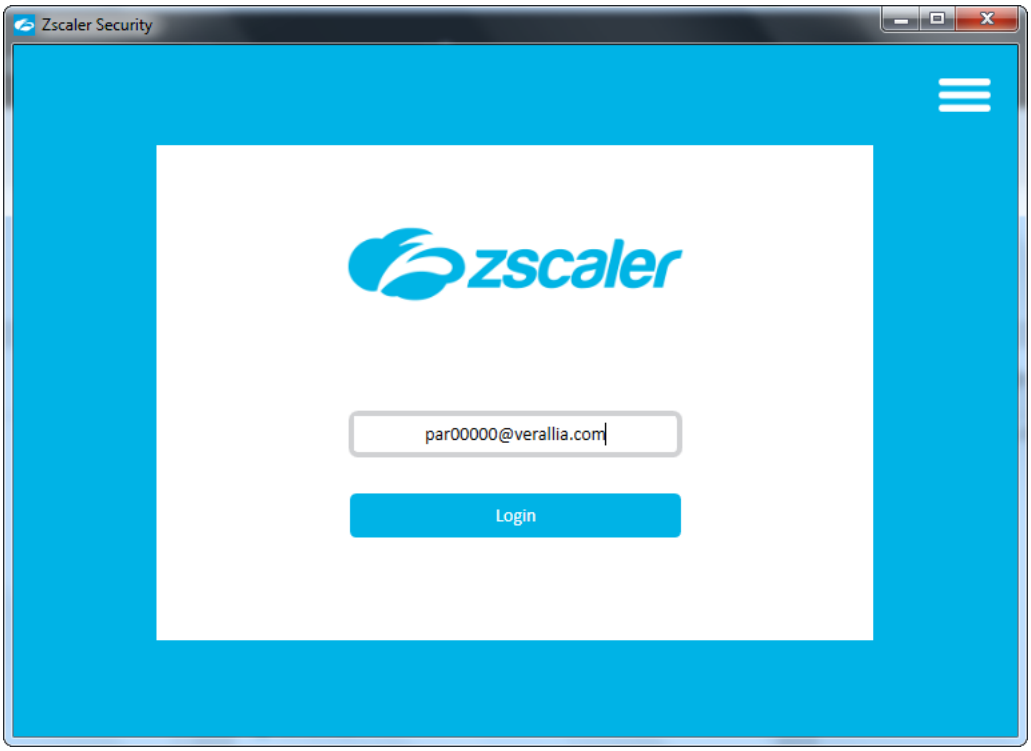


You will prompt to Enter your login credentials

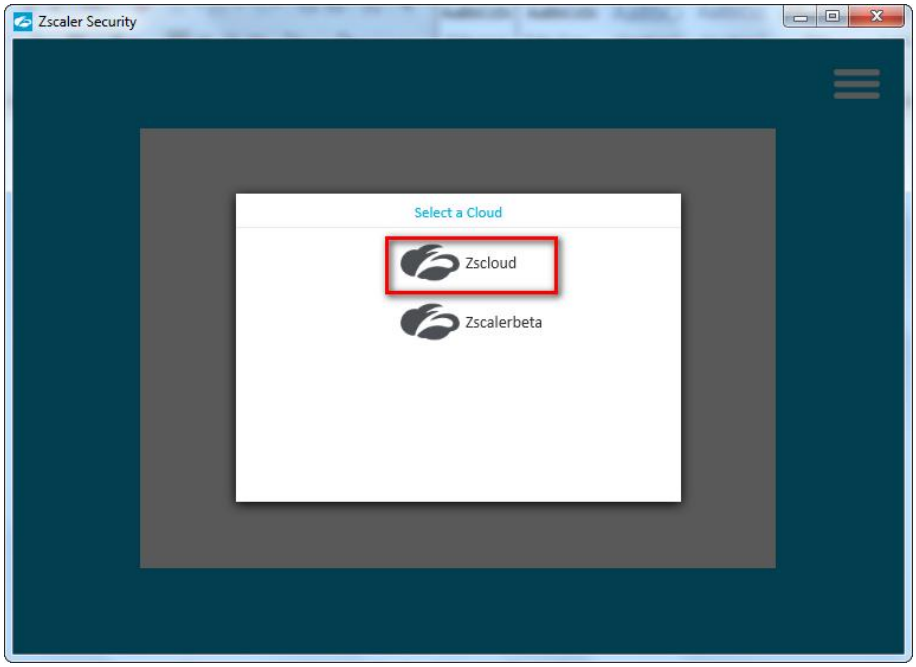
Please note that the right user format that should be used is shown as below:
yourParID@verallia.com



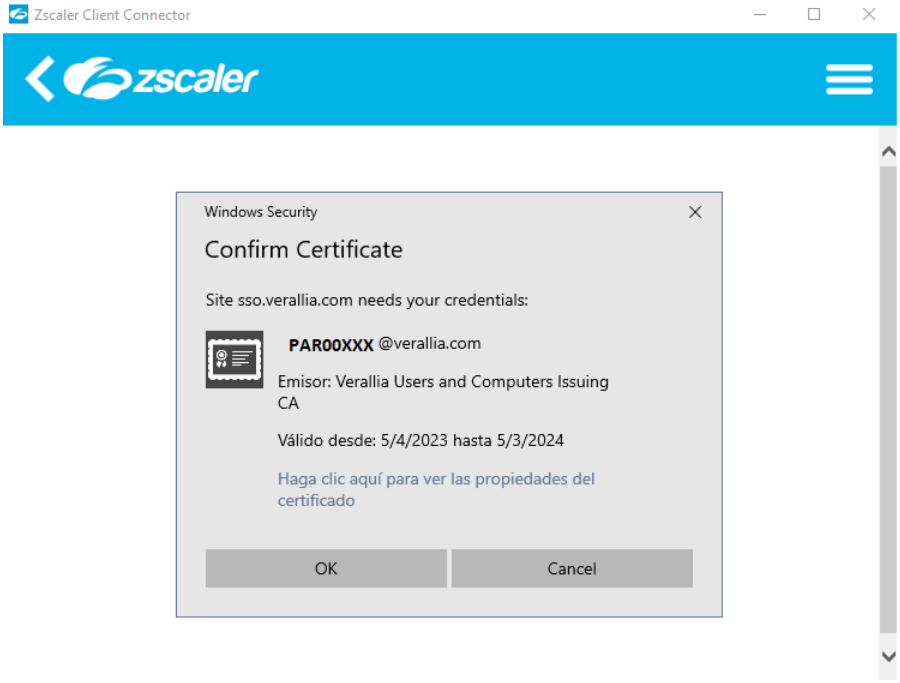
Example for the partner with ParID: par000555



3. Click on “Login”
4. Please select “Zscloud”

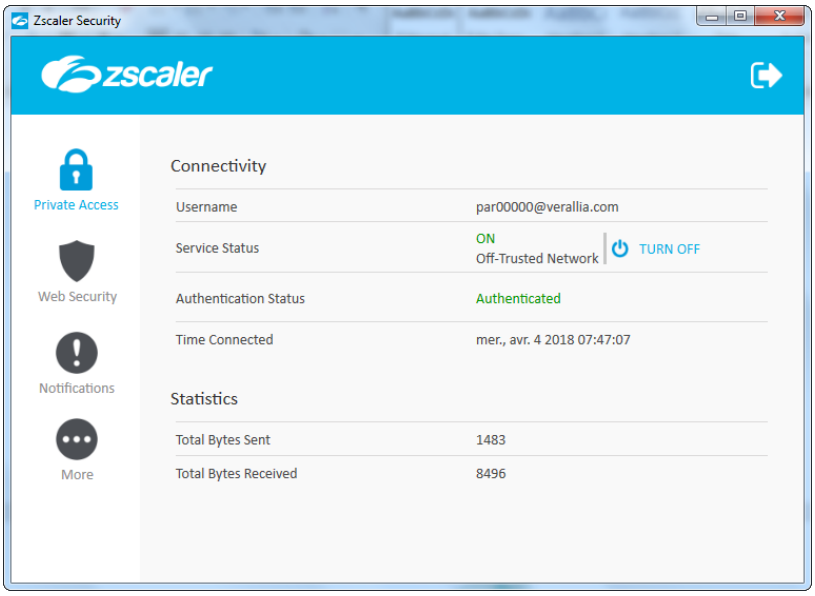


5. Then you should select the certificate issued by Verallia and Click “OK”



6. **You are now connected!**

You should have this screenshot.



You can access to the application you have requested.

Lease wait for some minutes and check if the sending and receiving bytes will be changed. This shows the tunnel is working properly.

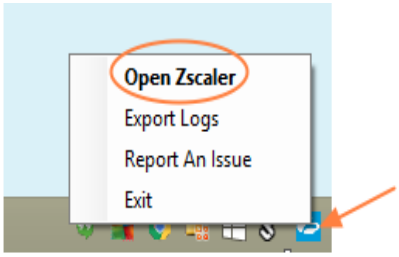
NOTE: Please follow the guidance as it is explained in order. The certificate should be installed on the device before the application installation.
When you have made the first connection, you must contact us to associate your PARID to a partner section so that when you stop carrying out the activity with Verallia, you can disconnect ZCC without problems. Otherwise, your terminal will become a standalone element within the Verallia network, and you only have access to the resources that your PARID belongs.

Please feel free to be in contact with Telecom team, In case of issue or question.
contact: v-telecom@verallia.com

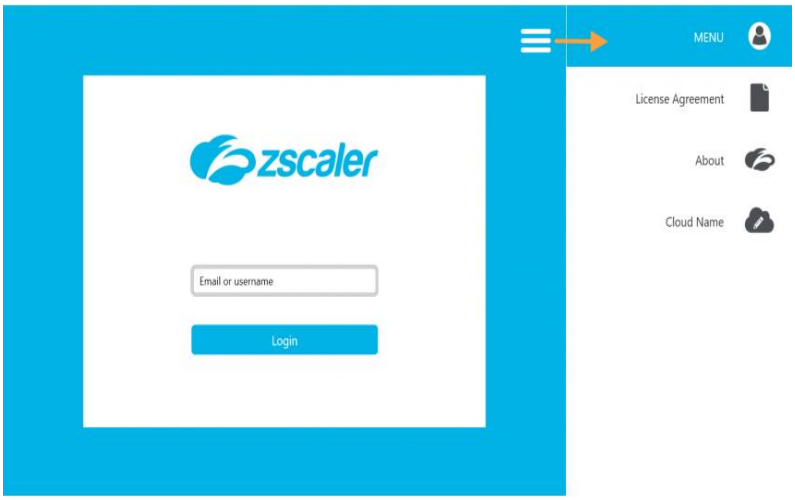
Enrollment

To enroll in the Zscaler service using the Windows version of Zscaler Client Connector:

1. When Zscaler Client Connector is installed on your device, open the app by right clicking the Zscaler Client Connector tray icon and selecting **Open Zscaler**.



2. An enrollment page appears, as shown below. The menu at the top right-hand corner enables you to:
   - View the license agreement.
   - View information about Zscaler Client Connector, including the version number.

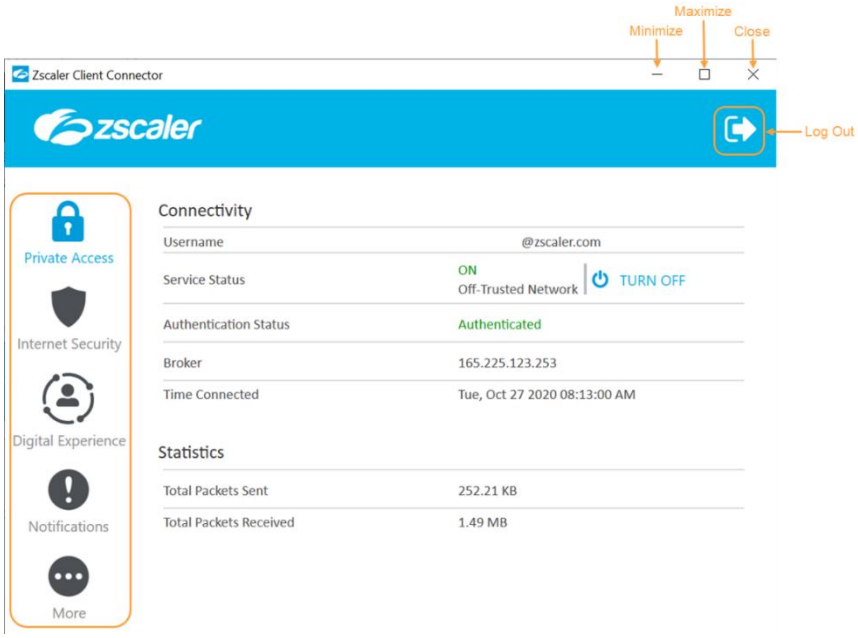


3. The procedure asks you for select the certificate after **Login**.
4. After you log in with your credentials and complete a one-step device enrollment process, you can begin safely connecting to the web and to organization's internal applications and services with Zscaler Client Connector.

NOTE: When you have made the first connection, you must contact us to associate your PARID to a partner section so that when you stop carrying out the activity with Verallia, you can disconnect ZCC without problems.
Otherwise, your terminal will become a standalone element within the Verallia network, and you only have access to the resources that your PARID belongs.

Zscaler Client Connector Features

After you enroll with the Zscaler service, you can view the features that are supported on your OS within the Zscaler Client Connector app interface:

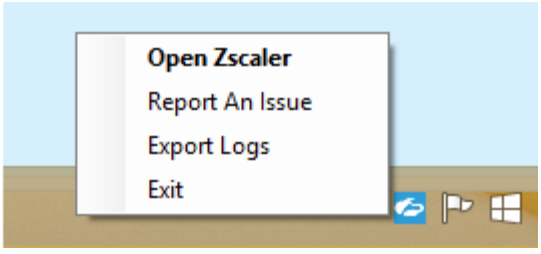


- Click the log out button on the top right-hand corner to log out of Zscaler Client Connector. You might be required to enter a password organization's admin has set for the app. If you log out of the app, you must complete enrollment again when you log back in.
    - **NOTE:** In Verallia is mandatory to request support and remote access from the IT management from Verallia to introduce this password to end the process.
- Click the minimize button to minimize the window without closing it.
- Click the maximize button to maximize the window.
- Click the close button to close the window. This does not log you out of the app.

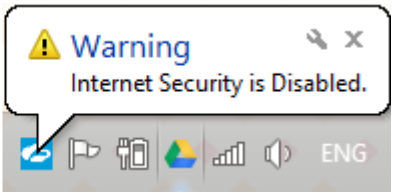
The app features Zscaler Client Connector's services in the menu on the left. The example above shows the menu options for an organization that has subscribed to the ZIA, ZPA, and ZDX services. If organization is not subscribed to one of these services, you will not see that option in the left menu.

- Zscaler Client Connector displays an icon in the system tray, as shown below:

- You can right-click the icon to display the following options:
    - **Open Zscaler**: Click to open the app window.
    - **Export Logs**: Click to export logs with this option. Logs will be saved as a text file on your device.
    - **Exit**: Click to exit the app and disable the Zscaler service. Depending on organization's policies, you might be required to enter a password configured by organization's admin.
        - **NOTE**: Verallia shouldn't allow user to exit the application with or without password.

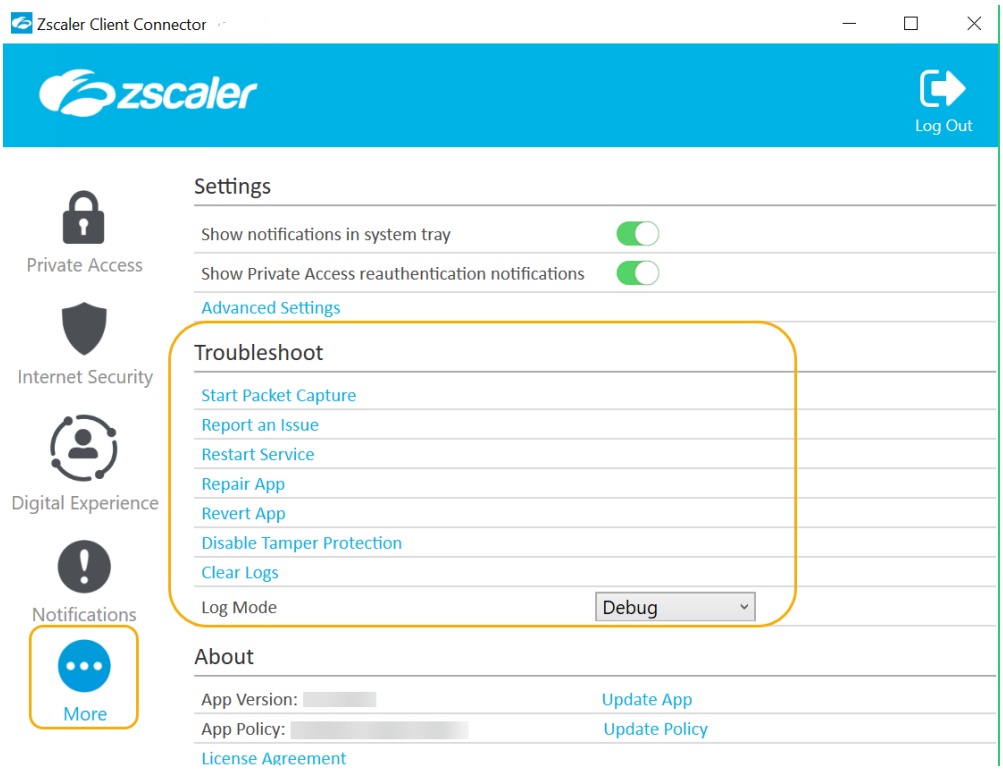


- If notifications are enabled, you will see notifications in the tray icon, as shown below.



Troubleshoot

Following is the **Troubleshoot** menu features of the Windows version of the Zscaler Client Connector:

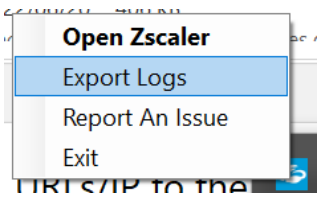


- **Start Packet Capture:** If organization's admin enabled packet captures, you can use this feature when reproducing an issue.

Using the Start Packet Capture Option

When reproducing an issue that requires packet capture:

- In Zscaler Client Connector, click **More**.
- In the **Troubleshoot** menu, click **Start Packet Capture**.
- Reproduce the issue.
- Click **Stop Packet Capture** after you resolve the issue.
- In the **toolbar** go to the **Zscaler icon**, right click, and select Export Logs



- **Choose a location** where you want to get these Logs
- Once the export is finished, please **attach ZIP file** in this mail thread.

Other options:

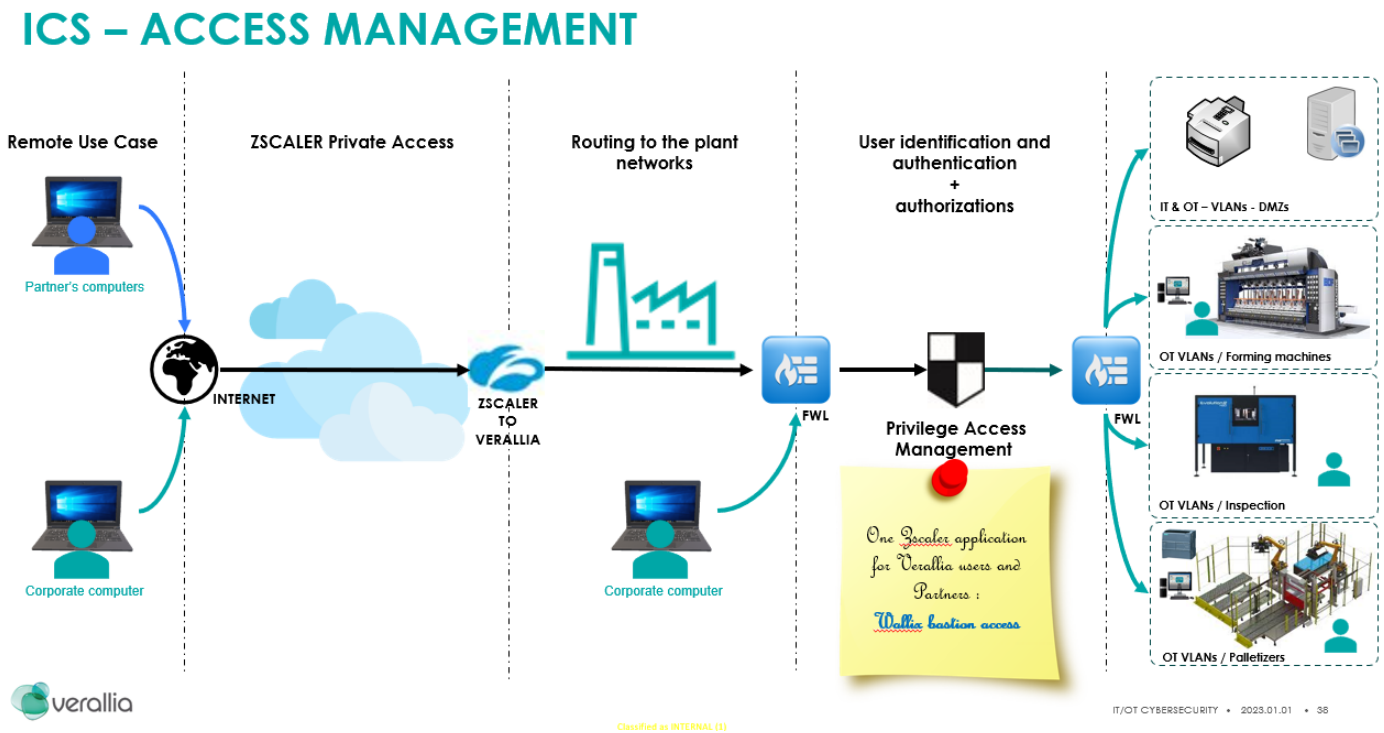
- **Restart Service:** You can click to restart the app. Restarting does not impact security enforcement.
- **Repair App:** If you select this option, the app will attempt to repair itself by reinstalling app drivers and services. Zscaler recommends trying this option before reporting an issue.
- **Disable Tamper Protection** (appears in older version).
- **Clear Logs:** You can clear stored logs.
- **Log Mode:** You can change the mode in which Zscaler Client Connector generates logs, but the change is effective for that connection session only. At the start of the next connection session, the app returns to the default log mode set by organization (debug). Below is a description of each log mode.
    - **Error:** Logs only when the app encounters an error and functionality is affected.
    - **Warn:** Logs when the app is functioning but is encountering potential issues, or logs when conditions for the Error log mode are met.
    - **Info:** Logs general app activity, or logs when conditions for the Warn log mode are met.
    - **Debug:** Logs all app activity that could assist Zscaler Support in debugging issues, or logs when conditions for the Info log mode are met.

HOW TO / CYBESECURITY / VPN PARTNER WITH ZSCALER & PAM WALLIX.

According to our Cybersecurity Strategy and compliance with the ISA/IEC 62443 norm, any **access to ICS is critical for IT security and foremost for Safety of Verallia employees**.

These accesses are managed by Privilege Access Management for identification, authentication, protocol relay, and traceability.

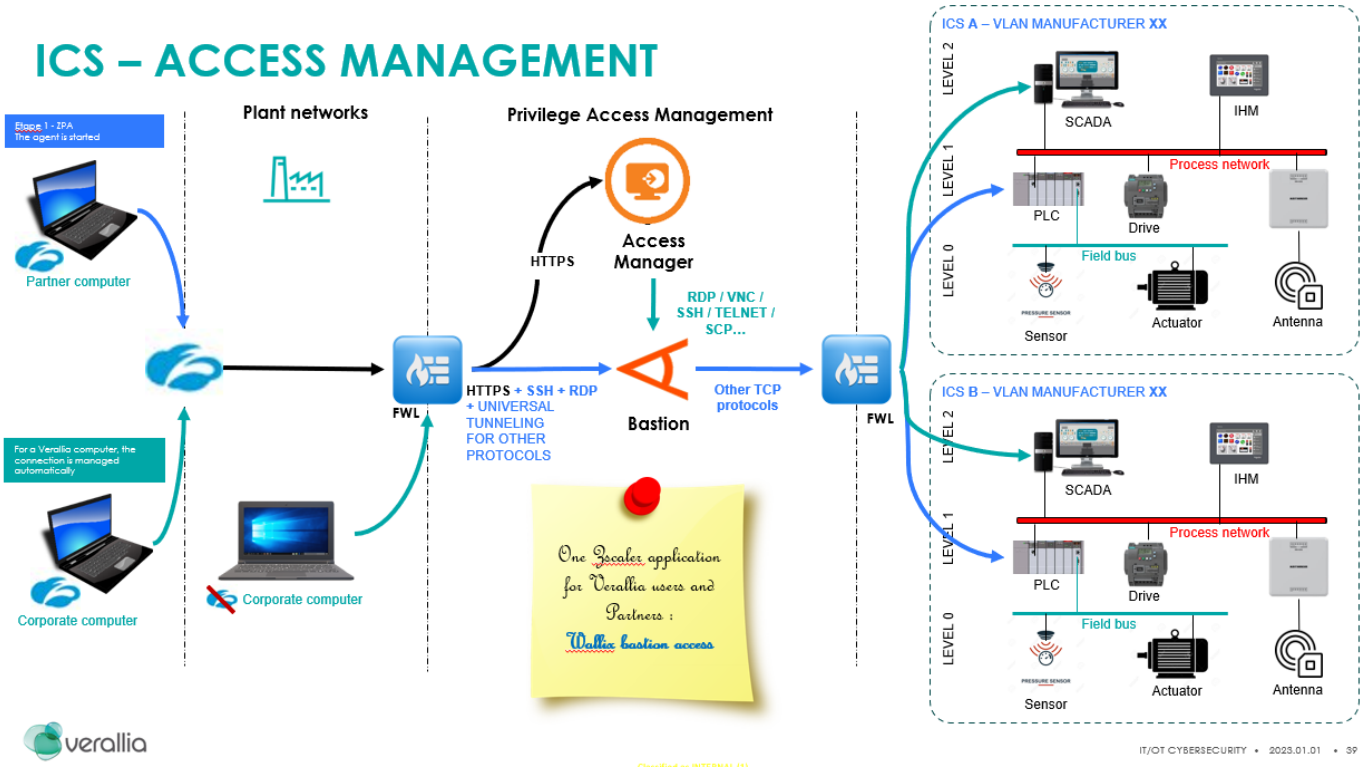
All Verallia Employees and Partners use the same access: with Zscaler for remote access and Wallix Access Bastion for connection to ICS systems.



From Zscaler, PAM access control is managed under this application: **Wallix Bestion Access** for all partners.

PAM WALLIX allows these protocols by default: RDP, VNC, SSH, TELNET, SCP & SFTP.

Any other protocols are managed by PAM under associated tool: Universal Tunneling.



Each Access Manager and Bastion only give access to ICS systems local to the site.

The Access Managers present a more user-friendly interface than Bastion; but the both can bu used..

Here you will find the right url for each access manager and bastion Verallia site:

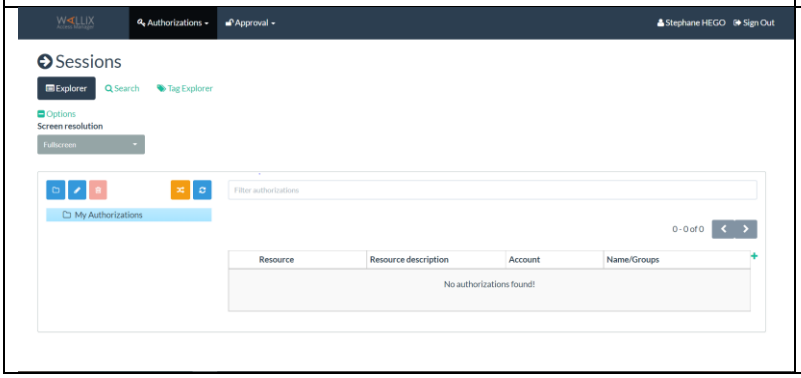
Pays / Country	Site / Location	SAP ID	Access Manager	Bastion	File server	Domain
ARGENTINA	Mendoza	W41	wamar0006	wabar0006	sftpar0006	pam.inpkg.net
BRAZIL	Campo Bom	V49	wambr0079	wabbr0079	sftpbr0079	pam.inpkg.net
	Jacutinga	V87	wambrp006	wabbrp006	sftpbrp006	pam.inpkg.net
	Porto Ferreira	V48	wambr0089	wabbr0089	sftpbr0089	pam.inpkg.net
CHILE	Rosario	X42	wamcl0003	wabcl0003	sftpcl0003	pam.inpkg.net
FRANCE	Chalon-sur-Saône	D11	wamfr0797	wabfr0797	sftpfr0797	pam.inpkg.net
	Cognac	D13	wamfr1764	wabfr1764	sftpfr1764	pam.inpkg.net
	Lagnieu	D21	wamfr1766	wabfr1766	sftpfr1766	pam.inpkg.net
	Oiry	D19	wamfr1768	wabfr1768	sftpfr1768	pam.inpkg.net

	Saint-Romain-le-Puy	D15	wamfr1771	wabfr1771	sftpfr1771	pam.inpkg.net
	Vauxrot (Cuffies)	D16	wamfr1773	wabfr1773	sftpfr1773	pam.inpkg.net
	VOA (Albi)	D71	wamfr0702	wabfr0702	sftpfr0702	pam.inpkg.net
DEUTSCHLAND	Bad Wurzach	H51	wamde0022	wabde0022	sftpde0022	pam.inpkg.net
	Essen	H53	wamde0101	wabde0101	sftpde0101	pam.inpkg.net
	Neuburg	H52	wamde0254	wabde0254	sftpde0254	pam.inpkg.net
	Wirges	H54	wamde0375	wabde0375	sftpde0375	pam.inpkg.net
ITALIA	Carcare	M62	wamit0008	wabit0008	sftpit0008	pam.inpkg.net
	Dego	M61	wamit0017	wabit0017	sftpit0017	pam.inpkg.net
	Gazzo Veronese	M65	wamit0022	wabit0022	sftpit0022	pam.inpkg.net
	Lonigo	M63	wamit0030	wabit0030	sftpit0030	pam.inpkg.net
	Pescia	M66	wamit0043	wabit0043	sftpit0043	pam.inpkg.net
	Villa Poma	M64	wamit0061	wabit0061	sftpit0061	pam.inpkg.net
PORTUGAL	Mondego	E45	wampt0005	wabpt0005	sftppt0005	pam.inpkg.net

ESPAÑA	Azuqueca	B30	wames0018	wabes0018	sftpes0018	pam.inpkg.net
	Burgos	B32	wames0029	wabes0029	sftpes0029	pam.inpkg.net
	Montblanc	B35	wames0083	wabes0083	sftpes0083	pam.inpkg.net
	Sevilla	B36	wames0006	wabes0006	sftpes0006	pam.inpkg.net
	Telde	F40	wames0058	wabes0058	sftpes0058	pam.inpkg.net
	Zaragoza	B38	wames0134	wabes0134	sftpes0134	pam.inpkg.net
УКРАЇНА	Zorya	J73	wamua0005	wabua0005	sftpua0005	pam.inpkg.net
РОССИЯ	Kavminstecklo	KMS	wamru0010	wabru0010	sftpru0010	pam.inpkg.net
	Kamyshin	KSZ	wamru0025	wabru0025	sftpru0025	pam.inpkg.net

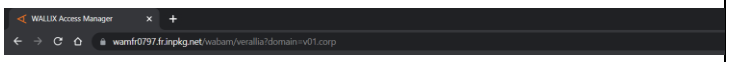
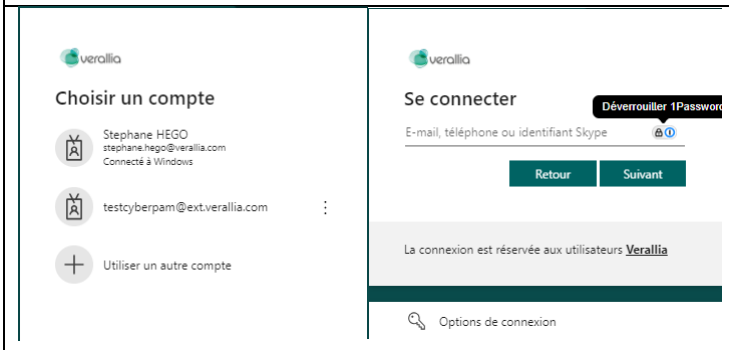
Connection to Wallix Access Manager [Local mode]

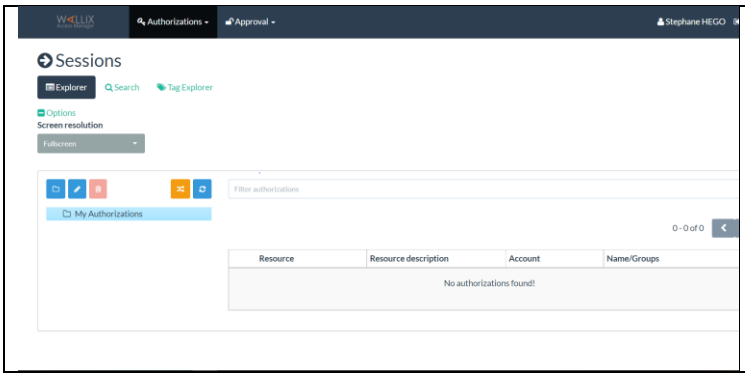
Local mode uses a local account/password managed by PAM for all site of Verallia. This is the first connection method; the credentials are communicated by IT Security team.

	Use the right url to connect the Wallix Access Manager corresponding to the right bastion: https://wamxxxxxx.pam.inpkg.net/wabam/verallia?domain=local
	**Primary authentication** Identification: Account Authentication: Password
	**Authorizations** Here, the list of your authorizations, you can manage the directories following your preferences. **Approvals** Here, you can see the requested approvals (only if required by the administrator)

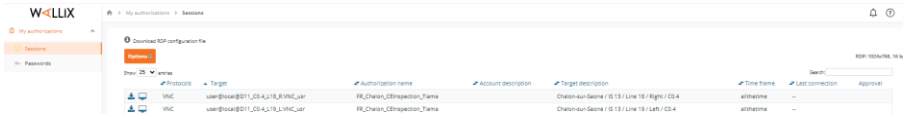
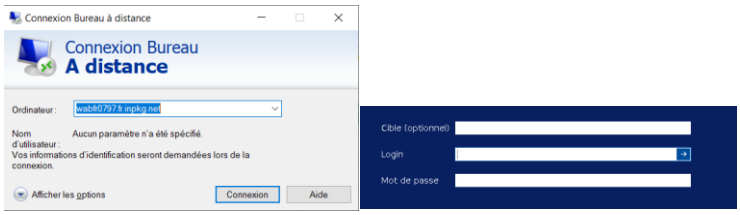
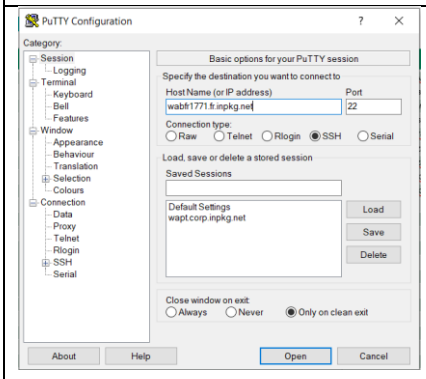
Connection to Wallix Access Manager [SSO / SAML V2]

This is the main method using Microsoft Entra ID. Invitation is sent by IT security, linked to Verallia Account for external user.

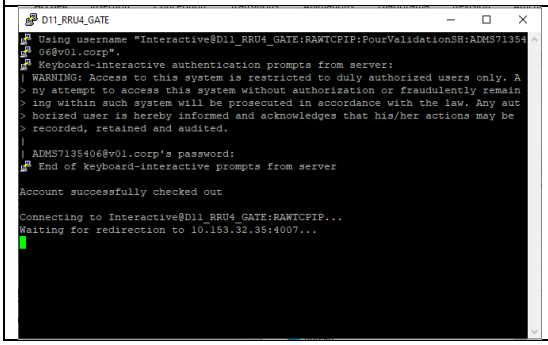
	Use the right url to connect the Wallix Access Manager corresponding to the right bastion: https://wamxxxxxx.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com
	**Primary authentication** **IT security team provides you a Microsoft account based on this structure:** [your prefix email company] @ext.verallia.com Select or put your account in the field

	**Authorizations** Here, the list of your authorizations, you can manage the directories following your preferences. **Approvals** Here, you can see the requested approvals (only if required by the administrator)

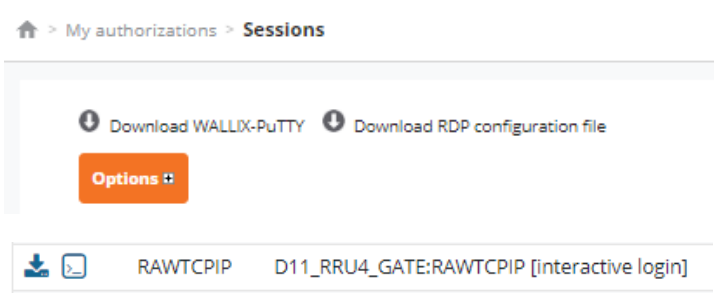
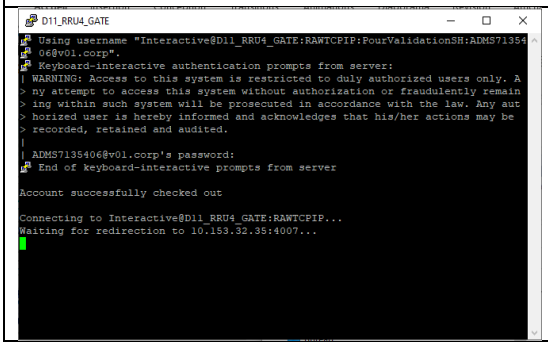
Connection to Wallix Bastion:

	**HTTPS access to the bastion will present all available resources** Use the right url to connect the Wallix Access Manager corresponding to the right bastion: https://wabxxxxxx.pam.inpkg.net Use the password button for the local connection ; or use the ext.verallia.com for SSO mode.
	In the menu, you will see the authorization for your account.
	**RDP access to the bastion will provide access to RDP or VNC protocols.** Use the right url to connect the Wallix Bastion corresponding to the right location: **wabxxxxxx.pam.inpkg.net** Insert your PARID and password
	**SSH (putty) access to the bastion will provide access to SSH, TELNET, SCP protocols**. Use the right url to connect the Wallix Bastion corresponding to the right location: **wabxxxxxx.pam.inpkg.net** Insert your PARID and password when asked.

Universal Tunneling by Access Manager

	**First connection** First connection requires to download AM Universal tunneling and install the msi package.
	**Open SSH tunnel** Now, open the ssh tunnel, enter your ID/Password or copy the url in your browser for validation (depending of the method Local connection or SSO). Now you can open your application, tcp port will be redirected.

Universal Tunneling by the Bastion

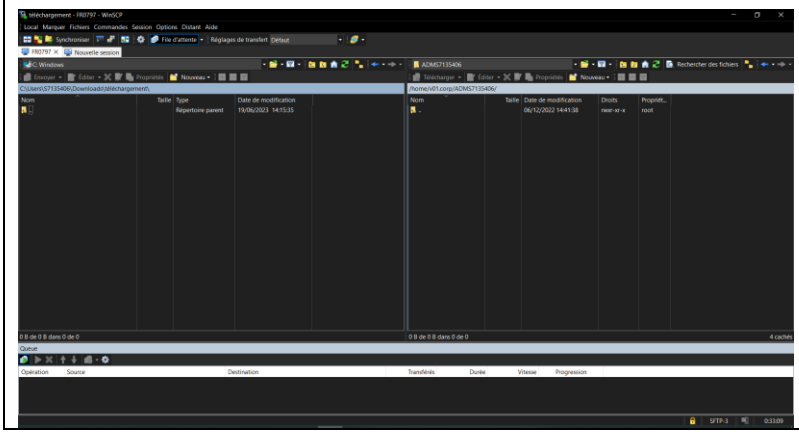
	**First connection** First connection requires to download Wallix Putty and install the msi package. **Target configuration** Download the configuration file and check this file will open the Wallix Putty Tools with administration rights.
	**Open SSH tunnel** Now, open the ssh tunnel, enter your ID/Password Now you can open your application, tcp port will be redirected.

Files transfer

Files transfer is allowed by the BASTION natively when using RDP protocol to connect to the ICS system. So, we invite the partner, to use RDP for a large maintenance and use the Clipboard buttons in the menu.

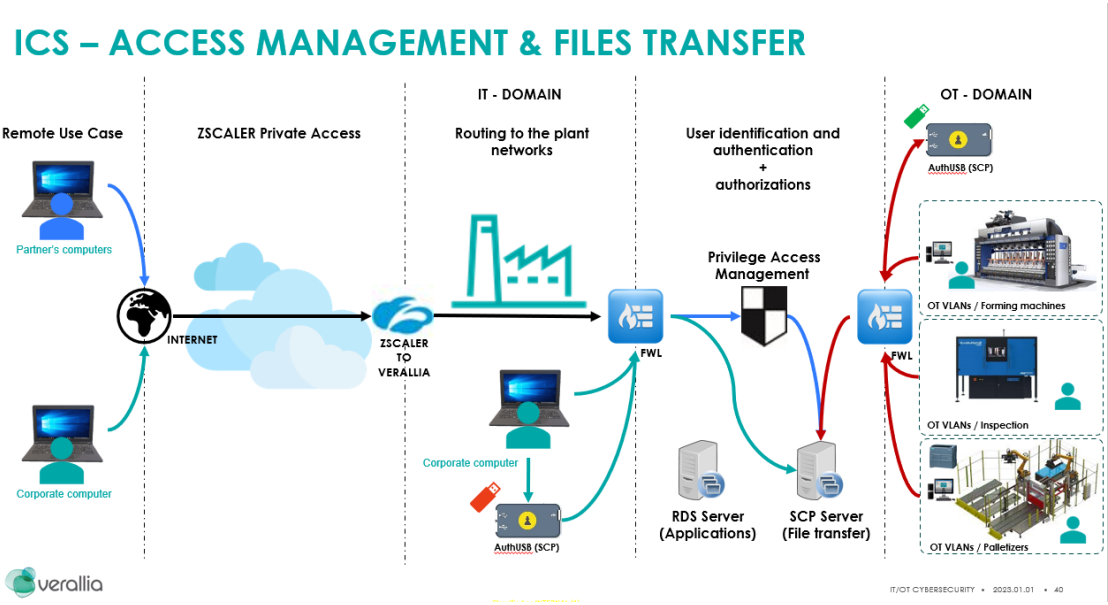
Other methods:

Use SFTP Server deployed by Verallia. In the authorization you can see this SFTP server (requires a configuration by local IT).

 	You can upload your file from your computer to the server. But from the machine you need to use WinScp tools. Please ask to the local IT for this configuration.

Use SFTP protocol directly. In the authorization you can see this SFTP server (requires a configuration by local IT).

	You can upload or download the file from your computer to the machine. This is the direct method for a linux machine. For a Windows machine, the OpenSSH tool must be deployed and configured. Please ask to the local IT for this configuration.



Pays / Country	Site / Location	Wallix Access Manager - Lien / URL links	IT/OT Region / Main contact
ARGENTINA	Mendoza	https://wamar0006.pam.inpkg.net/wabam/verallia?domain=local https://wamar0006.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	robson.ramos@verallia.com
BRAZIL	Campo Bom	https://wambr0079.pam.inpkg.net/wabam/verallia?domain=local https://wambr0079.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	robson.ramos@verallia.com
	Jacutinga	https://wambrp006.pam.inpkg.net/wabam/verallia?domain=local https://wambrp006.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	robson.ramos@verallia.com
	Porto Ferreira	https://wambr0089.pam.inpkg.net/wabam/verallia?domain=local https://wambr0089.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	robson.ramos@verallia.com
CHILE	Rosario	https://wamcl0003.pam.inpkg.net/wabam/verallia?domain=local https://wamcl0003.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	robson.ramos@verallia.com
FRANCE	Chalon-sur-Saône	https://wamfr0797.pam.inpkg.net/wabam/verallia?domain=local https://wamfr0797.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	steve.brunato@verallia.com
	Cognac	https://wamfr1764.pam.inpkg.net/wabam/verallia?domain=local https://wamfr1764.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	steve.brunato@verallia.com
	Lagnieu	https://wamfr1766.pam.inpkg.net/wabam/verallia?domain=local https://wamfr1766.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	steve.brunato@verallia.com
	Oiry	https://wamfr1768.pam.inpkg.net/wabam/verallia?domain=local https://wamfr1768.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	steve.brunato@verallia.com
	Saint-Romain-le-Puy	https://wamfr1771.pam.inpkg.net/wabam/verallia?domain=local	steve.brunato@verallia.com

		https://wamfr1771.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	
	Vauxrot (Cuffies)	https://wamfr1773.pam.inpkg.net/wabam/verallia?domain=local https://wamfr1773.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	steve.brunato@verallia.com
	VOA (Albi)	https://wamfr0702.pam.inpkg.net/wabam/verallia?domain=local https://wamfr0702.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	steve.brunato@verallia.com
DEUTSCHLAND	Bad Wurzach	https://wamde0022.pam.inpkg.net/wabam/verallia?domain=local https://wamde0022.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	roman.konrad@verallia.com
	Essen	https://wamde0101.pam.inpkg.net/wabam/verallia?domain=local https://wamde0101.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	roman.konrad@verallia.com
	Neuburg	https://wamde0254.pam.inpkg.net/wabam/verallia?domain=local https://wamde0254.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	roman.konrad@verallia.com
	Wirges	https://wamde0375.pam.inpkg.net/wabam/verallia?domain=local https://wamde0375.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	roman.konrad@verallia.com
ITALIA	Carcare	https://wamit0008.pam.inpkg.net/wabam/verallia?domain=local https://wamit0008.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	andrea.marchetto@verallia.com
	Dego	https://wamit0017.pam.inpkg.net/wabam/verallia?domain=local https://wamit0017.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	andrea.marchetto@verallia.com
	Gazzo Veronese	https://wamit0022.pam.inpkg.net/wabam/verallia?domain=local https://wamit0022.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	andrea.marchetto@verallia.com
	Lonigo	https://wamit0030.pam.inpkg.net/wabam/verallia?domain=local	andrea.marchetto@verallia.com

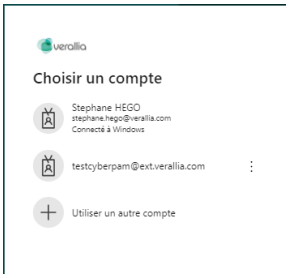
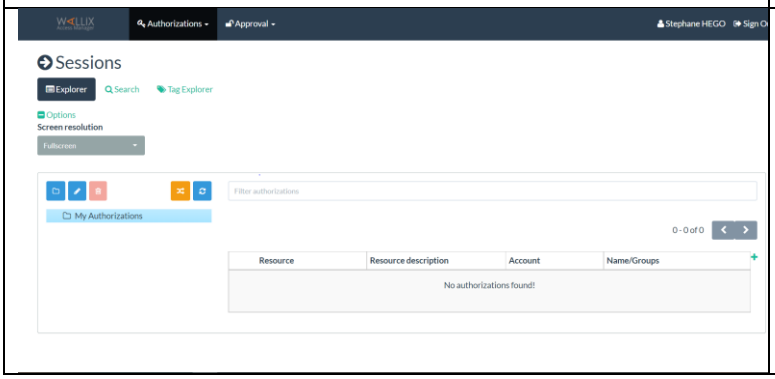
		https://wamit0030.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	
	Pescia	https://wamit0043.pam.inpkg.net/wabam/verallia?domain=local https://wamit0043.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	andrea.marchetto@verallia.com
	Villa Poma	https://wamit0061.pam.inpkg.net/wabam/verallia?domain=local https://wamit0061.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	andrea.marchetto@verallia.com
PORTUGAL	Mondego	https://wampt0005.pam.inpkg.net/wabam/verallia?domain=local https://wampt0005.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	antonio.galindo@verallia.com
ESPAÑA	Azuqueca	https://wames0018.pam.inpkg.net/wabam/verallia?domain=local https://wames0018.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	antonio.galindo@verallia.com
	Burgos	https://wames0029.pam.inpkg.net/wabam/verallia?domain=local https://wames0029.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	antonio.galindo@verallia.com
	Montblanc	https://wames0083.pam.inpkg.net/wabam/verallia?domain=local https://wames0083.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	antonio.galindo@verallia.com
	Sevilla	https://wames0006.pam.inpkg.net/wabam/verallia?domain=local https://wames0006.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	antonio.galindo@verallia.com
	Telde	https://wames0058.pam.inpkg.net/wabam/verallia?domain=local https://wames0058.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	antonio.galindo@verallia.com
	Zaragoza	https://wames0134.pam.inpkg.net/wabam/verallia?domain=local https://wames0134.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	antonio.galindo@verallia.com
УКРАЇНА	Zorya	https://wamua0005.pam.inpkg.net/wabam/verallia?domain=local	sergiy.yarosh@verallia.com

		https://wamua0005.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com	

HOW TO / CYBESECURITY / PARTNER CONNECTION TO THE CORPORATE PAM WALLIX.

This is an alternative mode, without installing a Zscaler agent. Our Corporate Access Manager can be accessible from Internet. The only prerequisite is installing the certificate as mentioned at the beginning of the document.

Local mode uses a local account/password managed by PAM for all sites of Verallia. This is the first connection method; the credentials are communicated by IT Security team. Invit to our tenant (SSO) is also managed by IT corporate (Infrastructure).

	Use the right url to connect the Wallix Access Manager corresponding to the right bastion: https://wallix.pam.inpkg.net/wabam/verallia?domain=local (require user/password) https://wallix.pam.inpkg.net/wabam/verallia?domain=ext.verallia.com (require to be invited for using your Entra ID company)
 	**Primary authentication.** **Local:** Identification: Account Authentication: Password SAML V2 (invit) Select the account linked to the certificate.
	**Authorizations** Here, the list of your authorizations, you can manage the directories following your preferences. **Approvals** Here, you can see the requested approvals (only if required by the administrator)