VISULOX 4

VISULOX4_UserGuide

16.10.2026

visulox

Table of Contents

1 Preface 5
2 Connecting 7
3 Authentication 16
4 The Workspace 22
5 Password management 27
6 VISULOX Control Panel 30
7 Receiving a message 33
8 Recorded applications 34
9 Live player in session 36
10 Assistance 38
11 Dual Control 44
12 Application locked 47
13 File Transfer modules 49
14 Command Connect / Guard module 57
15 Appendix_U 66

Limitation of Liability Statement (Disclaimer)

The Visulox documentation is proprietary to amitego engineering GmbH and no ownership rights are hereby transferred. No part of the documentation shall be used, reproduced, translated, converted, adapted, stored in a retrieval system, communicated or transmitted by any means, for any commercial purpose, including without limitation, sale, resale, licence, rental or lease, without the prior express written consent of amitego engineering.

amitego engineering does not make any representations, warranties or guarantees, express or implied, as to the accuracy or completeness of the documentation. Users must be aware that updates and amendments will be made from time to time to the documentation. It is the user's responsibility to determine whether there have been any such updates or amendments. Neither amitego engineering nor any of its directors, officers, employees or agents shall be liable in contract, tort or in any other manner whatsoever to any person for any loss, damage, injury, liability, cost or expense of any nature, including without limitation incidental, special, direct or consequential damages arising out of or in connection with the use of the documentation.

1 Preface

The **VISULOX User Guide** provides an introduction to using the VISULOX PORTAL and VISULOX features. This manual provides information on how to use the portal to run applications and how the enhanced VISULOX features are handled. This document is intended for both new and existing users of VISULOX.

1.1 How this manual is organized

Preface
Connecting, Authentication, The Workspace, Password management, VISULOX Control Panel, Receiving a message, Recorded applications, Recorded applications, Live player in session, Assistance, Dual Control, Application locked, File Transfer modules, Command Connect / Guard module
Troubleshooting
(4.3.3) Glossary

1.2 Legend

- Useful information
- Recommended setting
- Warning / use with caution
- Tipps & tricks

1.3 Related documentation

1.4 VISULOX documentation

Application	Title	Format
Release Notes	*VISULOX Release Notes* *Platform Support and Release Notes*	HTML
Installation	*VISULOX Installation Guide* *Installation Guide*	HTML
Administration	*VISULOX Admin Guide* *Administration Guide*	HTML
User	*VISULOX User Guide* *User Guide*	HTML

The VISULOX Online Documentation is available at: **https://wiki.visulox.com/**

1.5 Documentation feedback

Submit comments about this document by sending a mail to: **support@visulox.com**

2 Connecting

To connect to the service, the URL has to be provided by the supervisor. With this URL, connection to the VISULOX PORTAL via browser is possible.

Supported browsers are **Firefox**, **Chrome**, **Edge** and **Safari**.

Supported Client Platform	Supported Browsers
Microsoft Windows 10 (64-bit only) Microsoft Windows 11	Microsoft Edge 130 Mozilla Firefox 131 Chrome 130
Oracle Linux 8 Oracle Linux 9	Mozilla Firefox 131 Chrome 130
Ubuntu Linux 20.04 Ubuntu Linux 22.04 Ubuntu Linux 24.04 (with client 22.04)	Mozilla Firefox 131 Chrome 130
macOS 10.13 or later	Safari 17.5 Mozilla Firefox 131 Chrome 130

The table shows the client platforms and browser versions that have been tested with this release.
The latest versions of the browsers listed in this table are supported. Browsers not shown in this table may be supported at a later stage.

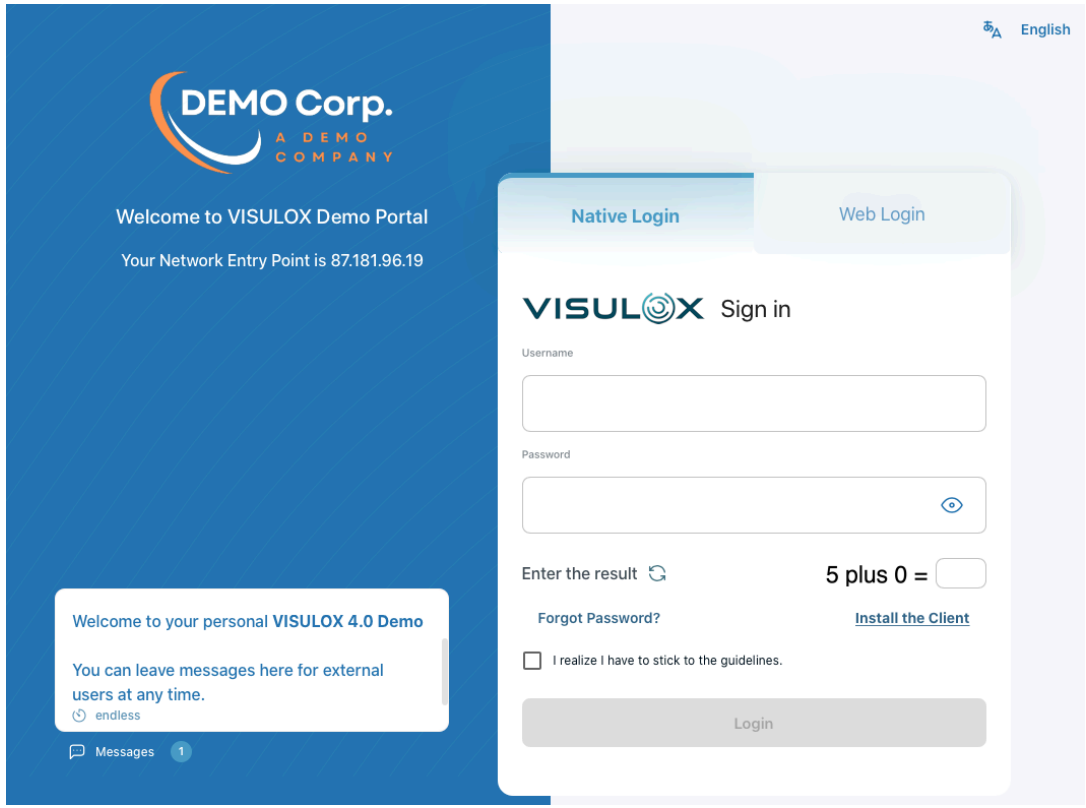
In a VISULOX environment direct login is configured by default, so the login mask of VISULOX PORTAL is displayed.

2.1 Access with Native Client

VISULOX PORTAL provides a modern login mechanism. Therefore a client side component has to be downloaded and registered in the browser.

The Native Client is provided by Oracle.

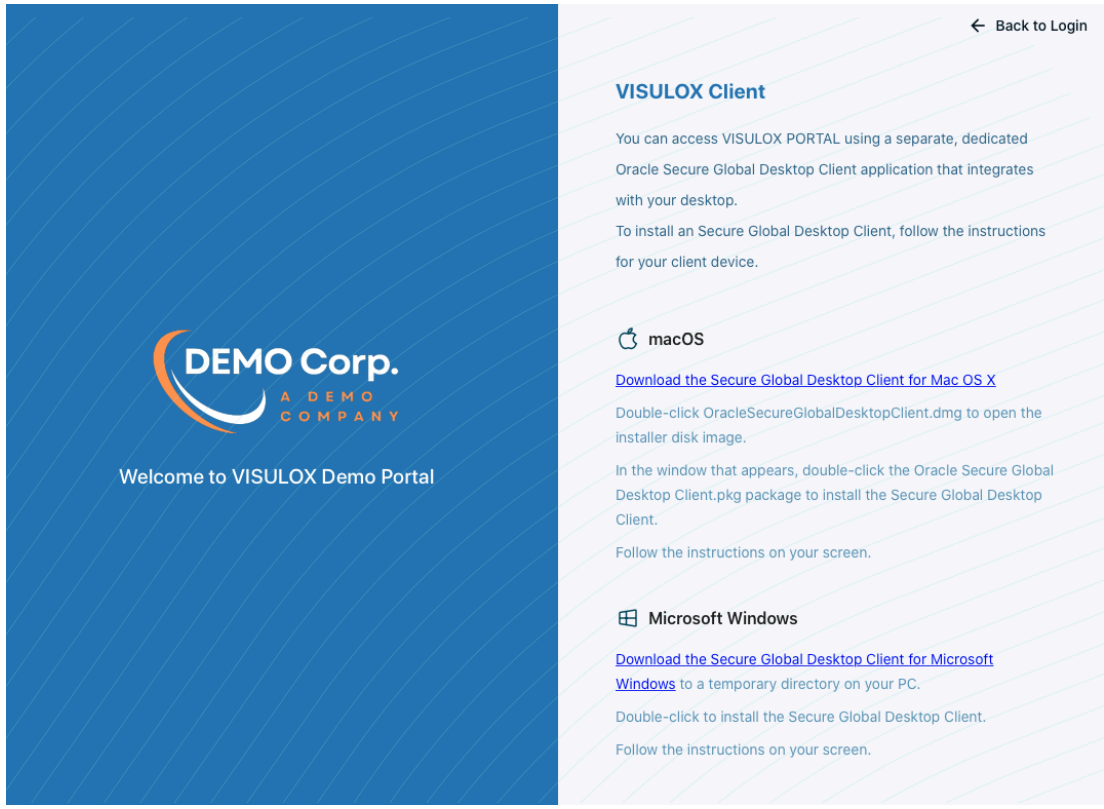
Login screen:



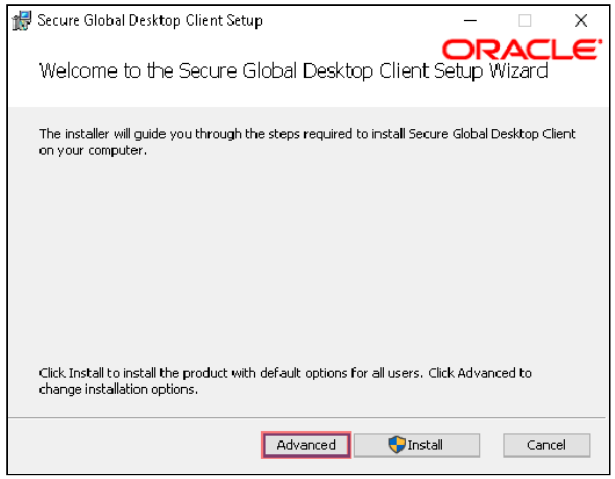
Choose "**Install the client**" link before the first login.

Choose "**Web Login**" to use the HTML5 Client.

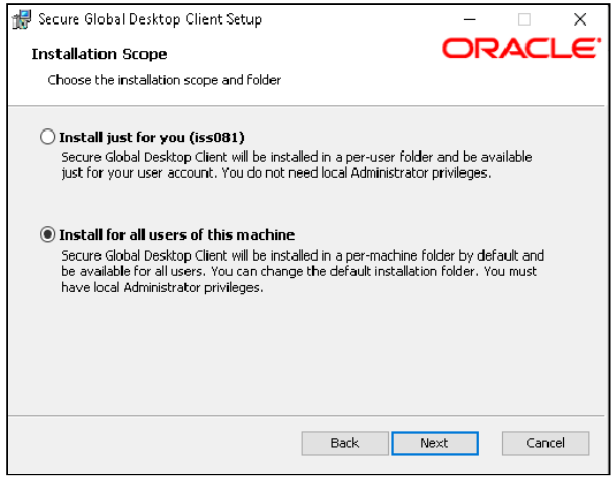
Download the client for your system:



For example: Installation on Windows



Follow the installation steps for the Native Client or use **"Advanced".**



User-Specific Installation
For a user-specific installation, the user must have permissions to write to the install location.
The default locations for a user-specific installation are as follows:

- Microsoft Windows platforms. The user's Home folder. For example:
  C:\Users\username\AppData\Local\Programs\Oracle\Secure Global Desktop Client
- Linux platforms (64-bit). User-specific installation is not supported for the 64-bit Linux versions of the Native Client.
- macOS platforms. There is not a default location for user-specific installation.
  Users can install the Native Client application in any installation folder.
  A common location is /Users/username/Applications.

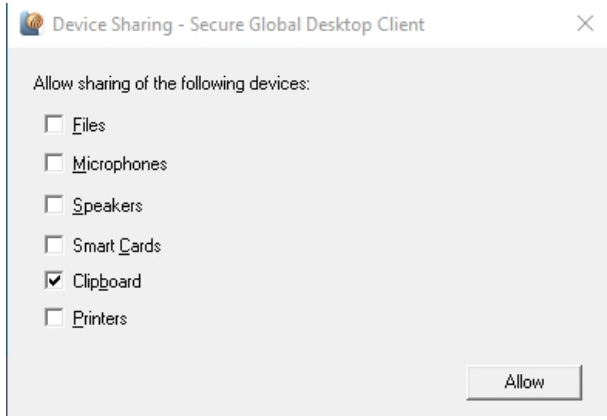
System-Wide Installation
This installation method can be used on a shared file system.
The default locations for a system-wide installation are as follows:

- Microsoft Windows platforms.
  C:\Program Files\Oracle\Secure Global Desktop Client
- Linux platforms (64-bit).
  /opt/oracle/sgdclient
- macOS platforms.
  /Applications

Loggin into Workspace with the client (version 5.60.550 or newer)

When users connect with a **5.60.550** or **later** installed client for the first time, they are prompted to give consent for access to resources on their client device.
The settings are saved and apply to all installations. The settings can be changed from the "'**Device Sharing...**" menu on the client icon.
The dialog box is not localized and presented in English.

A popup box for Device Sharing is displayed:



All settings except clipboard need further configuration steps to be enabled.

These settings can also be adjusted later, once they are needed.

2.2 JAVA based access

JAVA based access is no longer supported.

2.3 Other access methods

Access is also possible via HTML5, if not disabled.

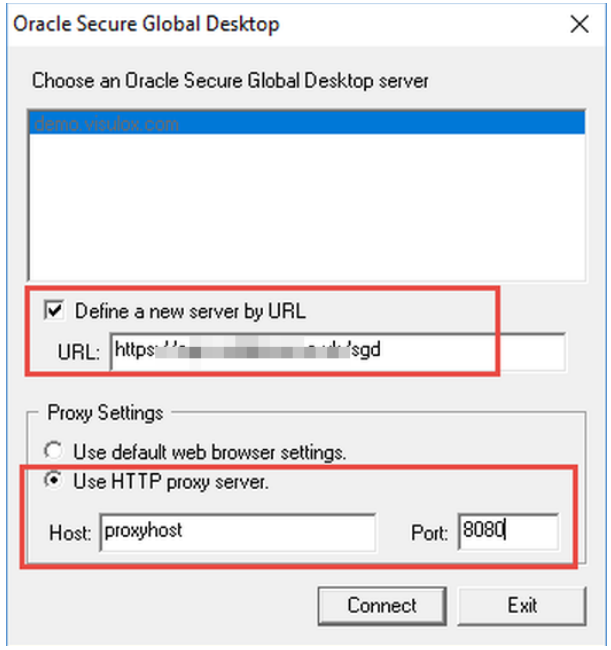
2.4 Proxy Handling

Client side proxies can be used. The proxy has to be configured for the browser.

Access with Native Client

Currently the native client does not support proxy directly. If proxy is needed, a manual start of the **tcc.exe** is needed for the first time.

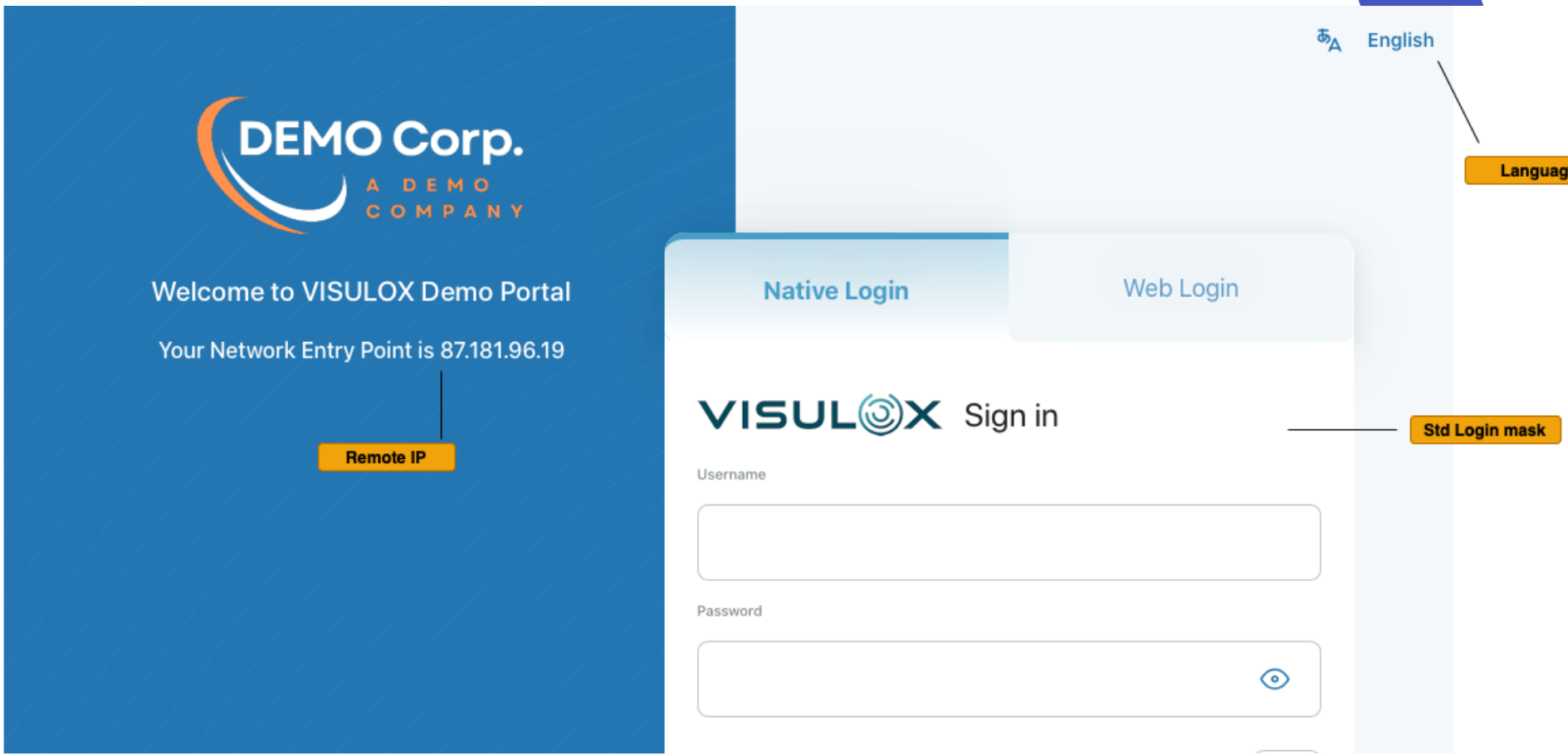
The **tcc.exe** can be found by using the Windows file search, for example: **C:\Program Files\Oracle\Secure Global Desktop Client\tcc.exe**

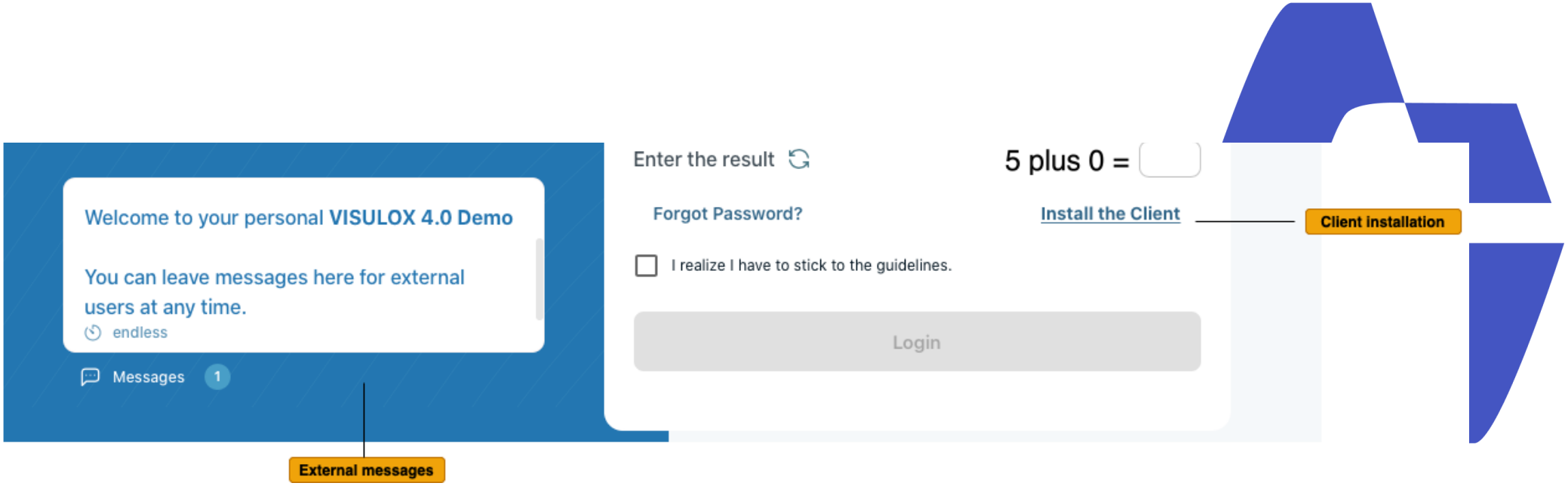


This is needed only for the first time. After a first successful connect, the browser can be used directly.

3 Authentication

Users with an account are able to log in, by entering their user ID and password into the login mask.



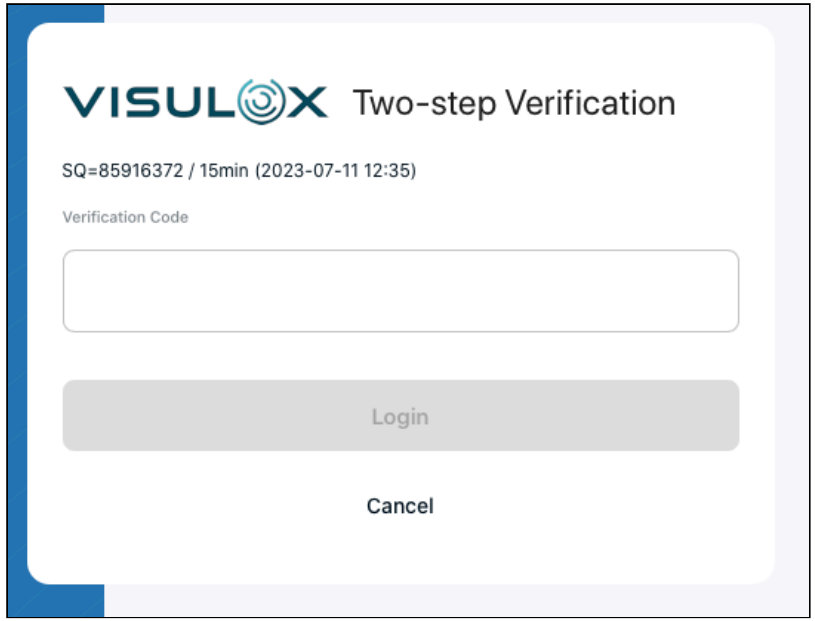


The available external messages are displayed in the message box of the login page.

3.1 Authentication via Access PIN

Users, that are registered for authentication with an Access PIN will get a second login mask and the PIN is sent via eMail or SMS.

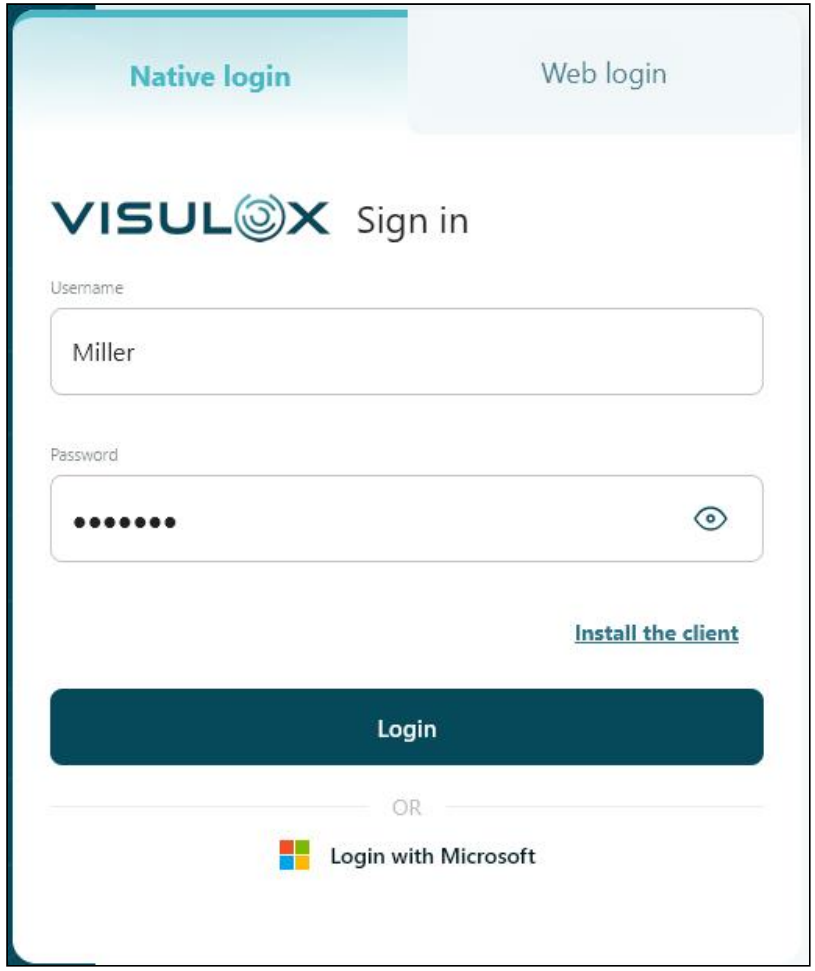
It is also possible to call the Helpdesk to ask for the generated Access PIN. The PIN has a configured length, format and lifetime.



Once the user has received the PIN, login is possible with the username, password and the Access PIN as long as the PIN is valid.
If the lifetime has run out, a new PIN is generated and sent, when the user tries to login the next time.

3.2 Authentication via Microsoft Entra

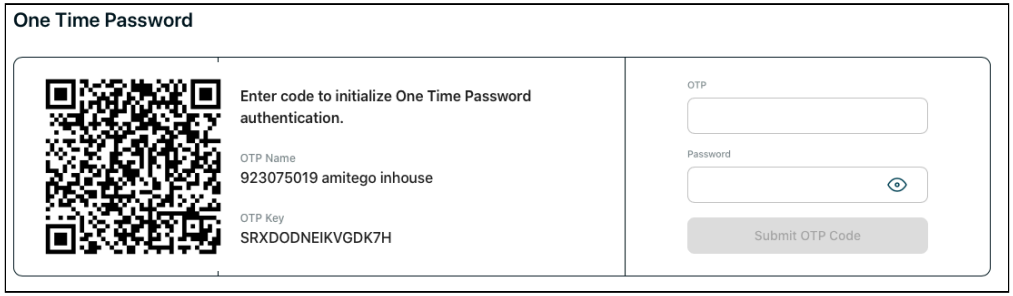
If configured, authentication with a Microsoft account is also possible using **Login with Microsoft**:


Native login
Web login
VISULOX Sign in
Username
Miller
Password
Install the client
Login
OR
Login with Microsoft

3.3 Authentication via One Time Password

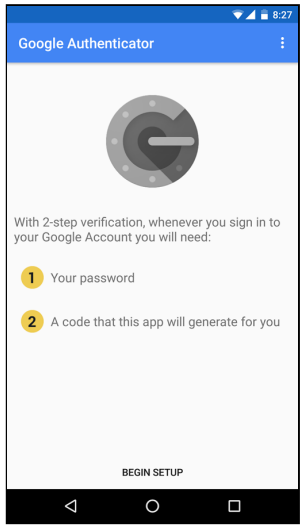
For the login with One Time Password (OTP) an initial key has to be created with a smartphone App before.

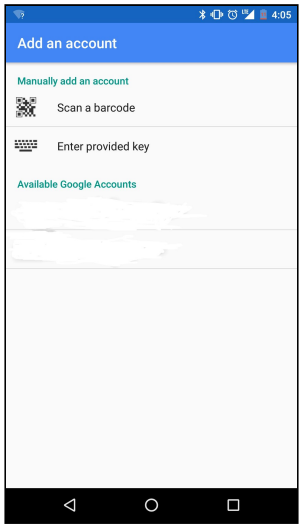
Initial key generation on the welcome page:

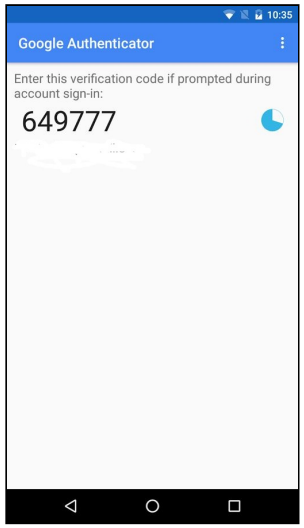
The QR code (and the OTP Key) is displayed in the Workspace.	

With a smartphone App (e.g. Google Authenticator) an initial OTP can be generated and submitted via the input field.

The initial code can be created via QR code scanner or with the OTP key.





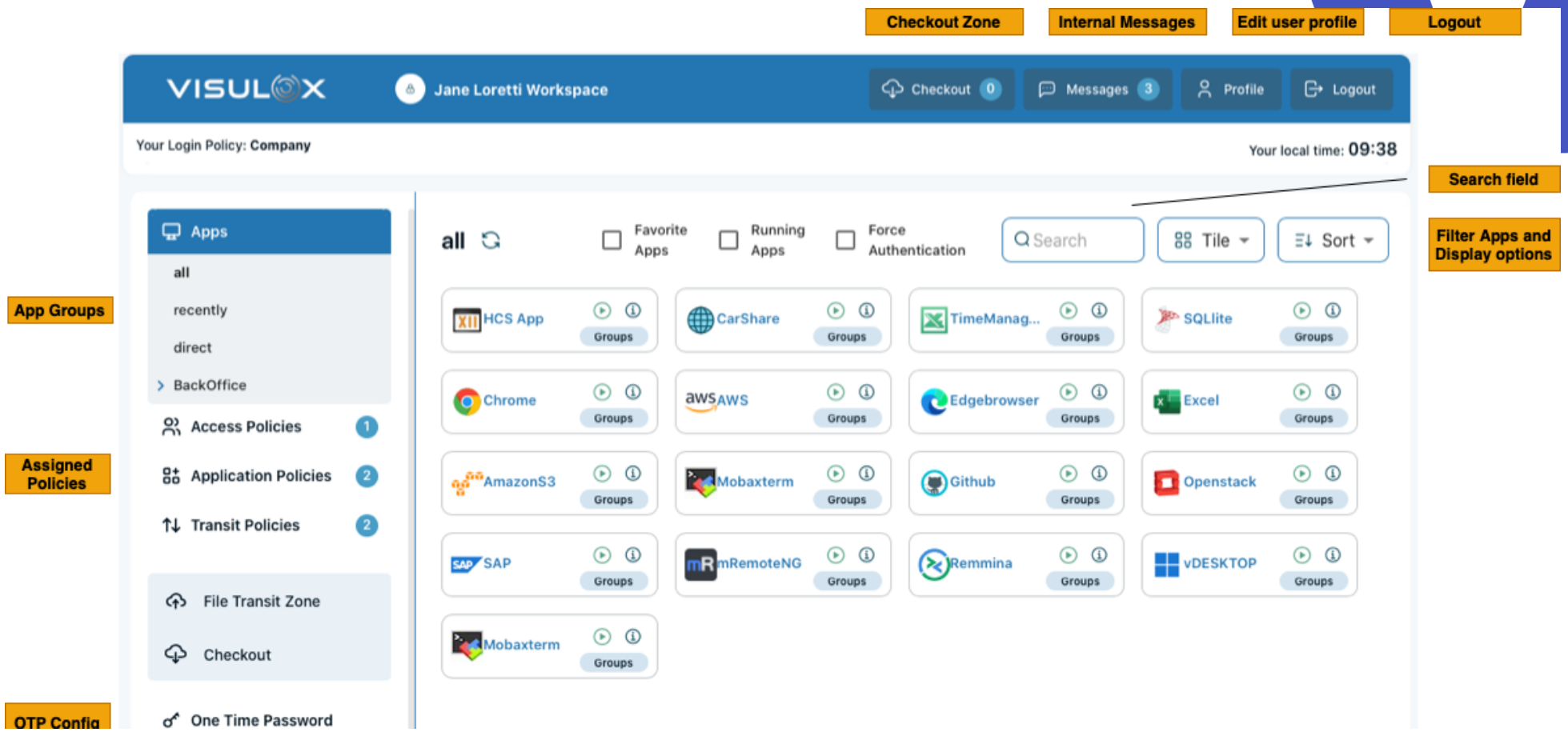


Once the user has entered the initial key, he is able to log into VISULOX PORTAL with the current key displayed in his authentication App and his password.

Login via verbal token will always be possible beside the OTP login.

4 The Workspace

After successfully logged in, the Workspace is displayed showing all applications, which are assigned to the user.



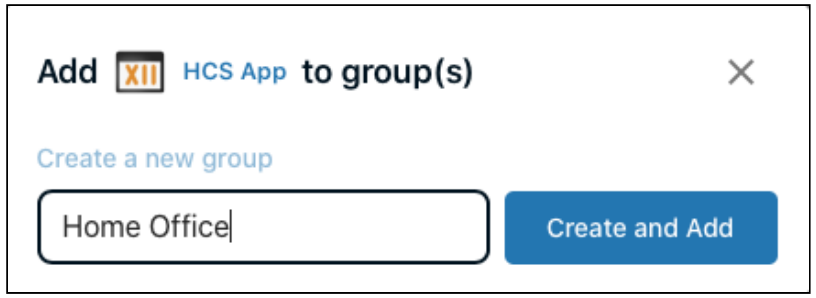
With the internal welcome message feature, it is possible to display a message for the logged in user in the Workspace ("**Messages**" - button).

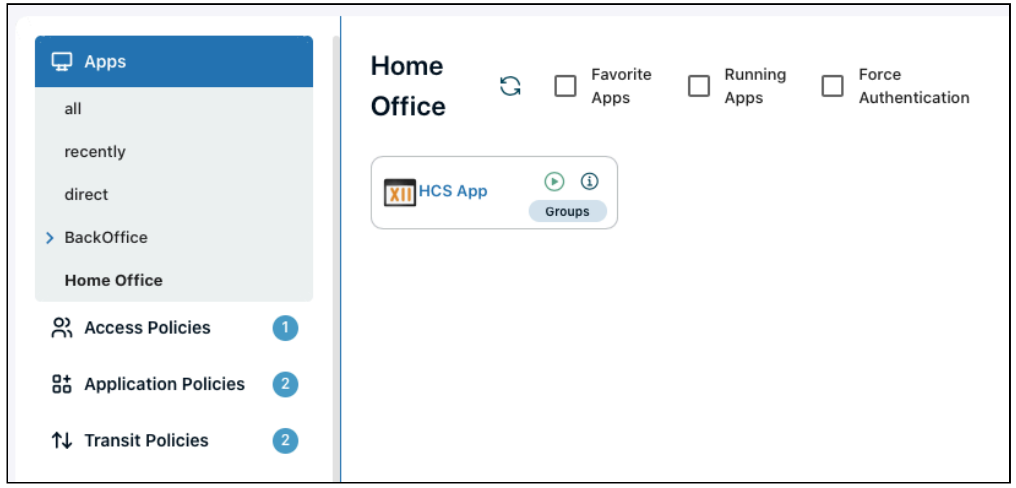
The matching policies (access, application, transit) of the user is displayed on the left side.

The Transit Zone for up/downloading files and the Checkout Zone for Reports and film checkouts is also integrated in the Workspace.

With the "**Quick Upload**" zone it is possible to drag & drop files to transfer them into the internal IT environment.

By clicking the "**Groups**" button within the application area it is possible to assign an application to a group or create a new application group:



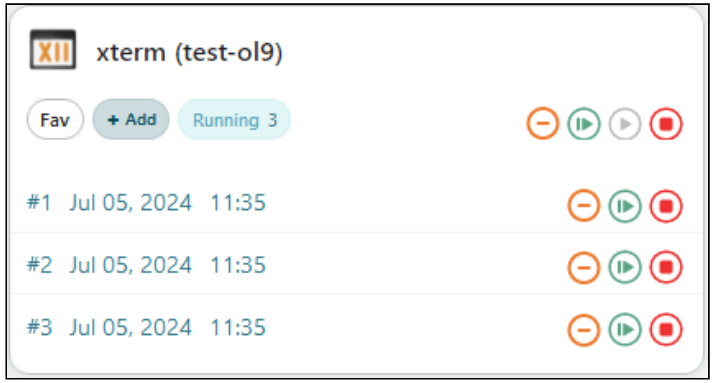


Applications can be added or removed from existing groups. If the last application is removed from a group, the group itself will be removed as well.

With the search field applications can be filtered and the applications can be controlled (**suspend** / **resume**, **cancel**, etc) all at once or each application on its own.

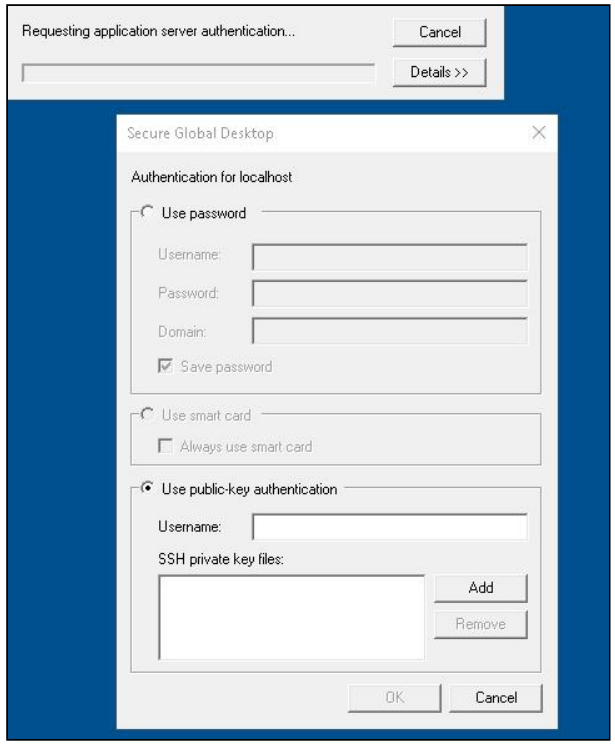
Status of the applications:

Application is running	

Hover over the application to see the running instances:	
	
Application(s) can be suspended, resumed, started or cancelled	
Depending on the status of the application some options are not available and greyed out	

After starting an application the authentication dialog is displayed (depending on the configuration).

If the dialog is not shown because the login user credentials are passed through, the display can be forced by checking "**Force Authentication**" in the Workspace.

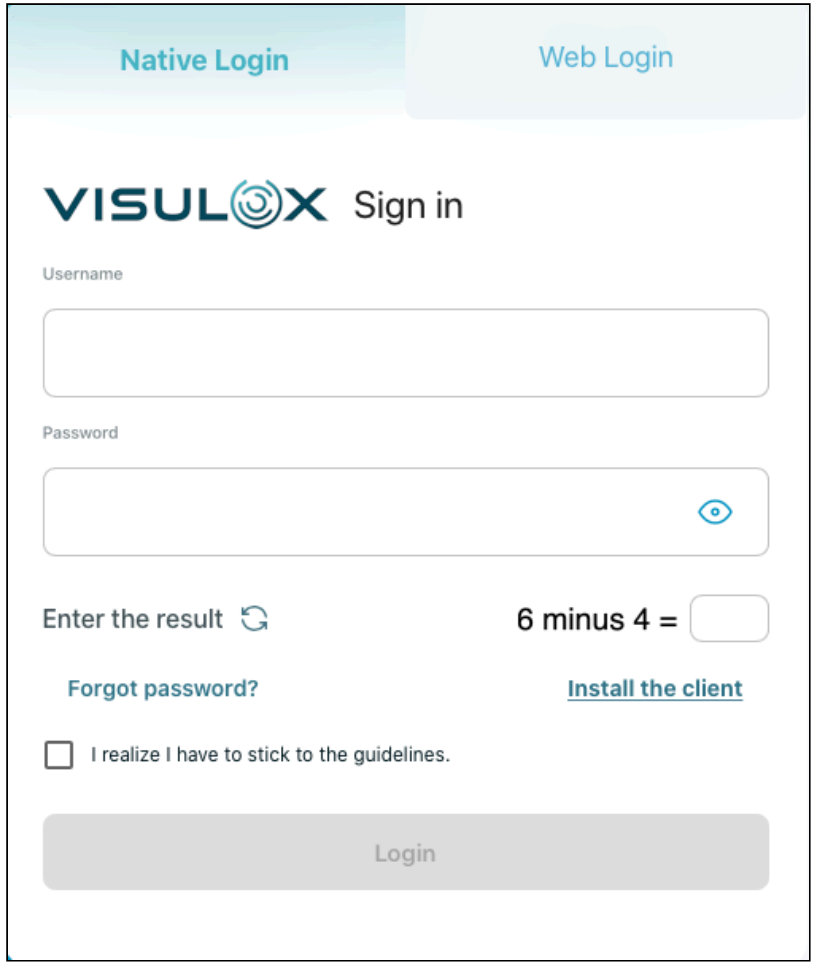

Requesting application server authentication...
Cancel
Details >>
Secure Global Desktop
Authentication for localhost
Use password
Username:
Password:
Domain:
Save password
Use smart card
Always use smart card
Use public-key authentication
Username:
SSH private key files:
Add
Remove
OK
Cancel

5 Password management

Active Directory (AD) and Oracle Unified Directory (OUD) users are able to change their password by themselves.

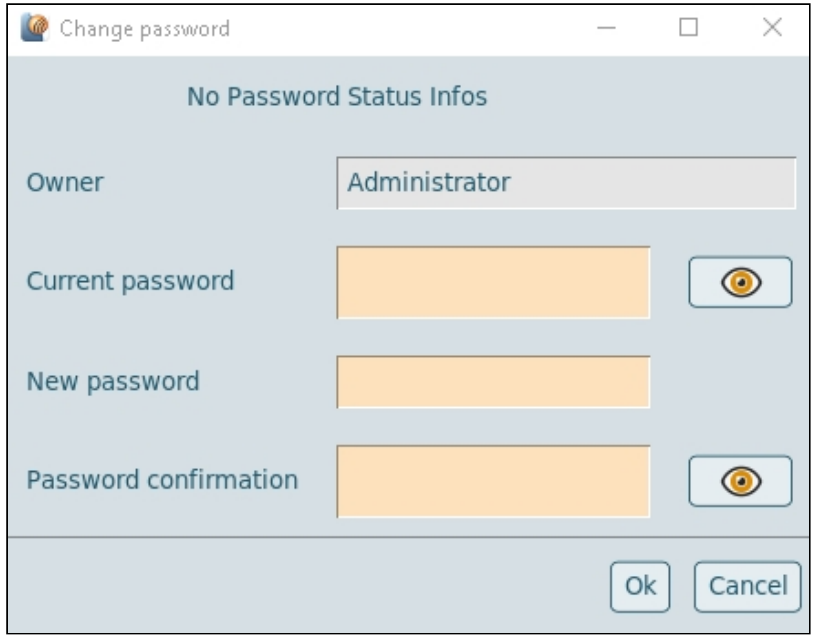
This feature must be configured and enabled by VISULOX admins.

If so, the "**Forgot Password?**" in the login mask is displayed:


Native Login
Web Login
VISULOX
Sign in
Username
Password
Enter the result
6 minus 4 =
Forgot password?
Install the client
I realize I have to stick to the guidelines.
Login

In the VISULOX Cockpit, the supervisor is able to reset passwords to a rolled random password for users.
Then the users will be informed via mail, that they have to set a new password with the Password SelfService application.

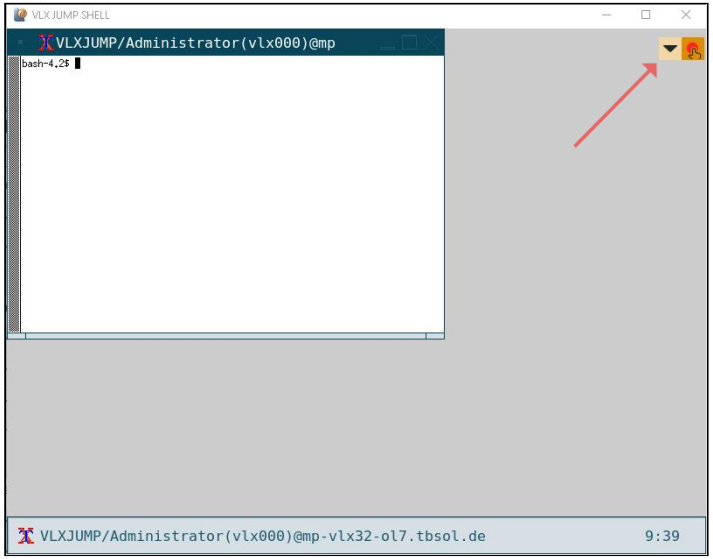
Therefore the "**VLX Password SelfService**" application must be assigned and has to be started from the Workspace.

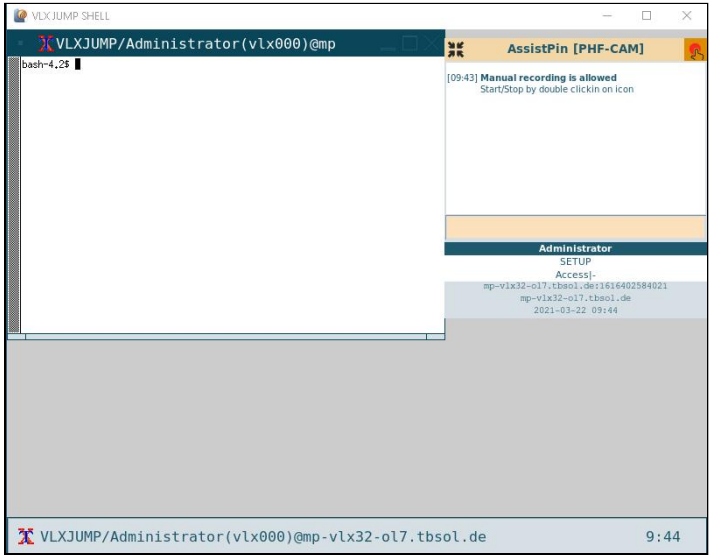


6 VISULOX Control Panel

The VISULOX control panel is always available in a launched application.

The panel is displayed, when the mouse pointer is placed over the trigger for the VISULOX control panel.

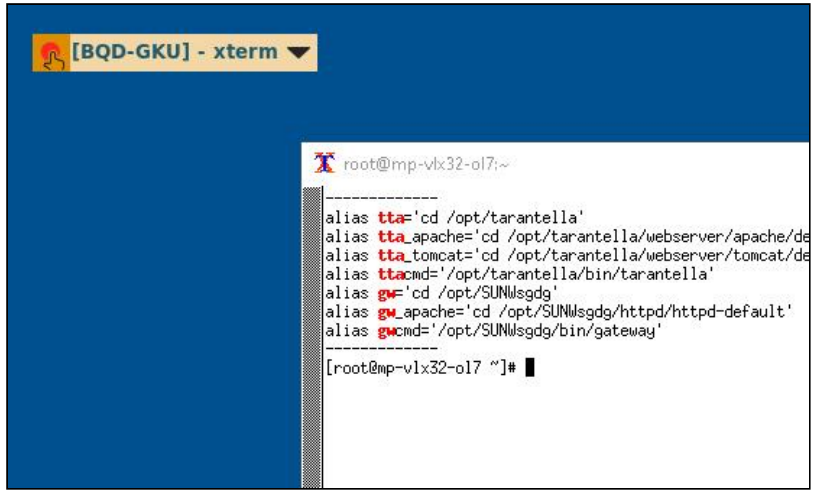




The panel can used for interactions between the application user and the VISULOX environment.

Depending on the mode of the application the look of the panel can be different.

The control panel can be moved with click on the title bar and holding down the left mouse button.
With a doubleclick on the title bar, the panel is moved back to upper right corner again.

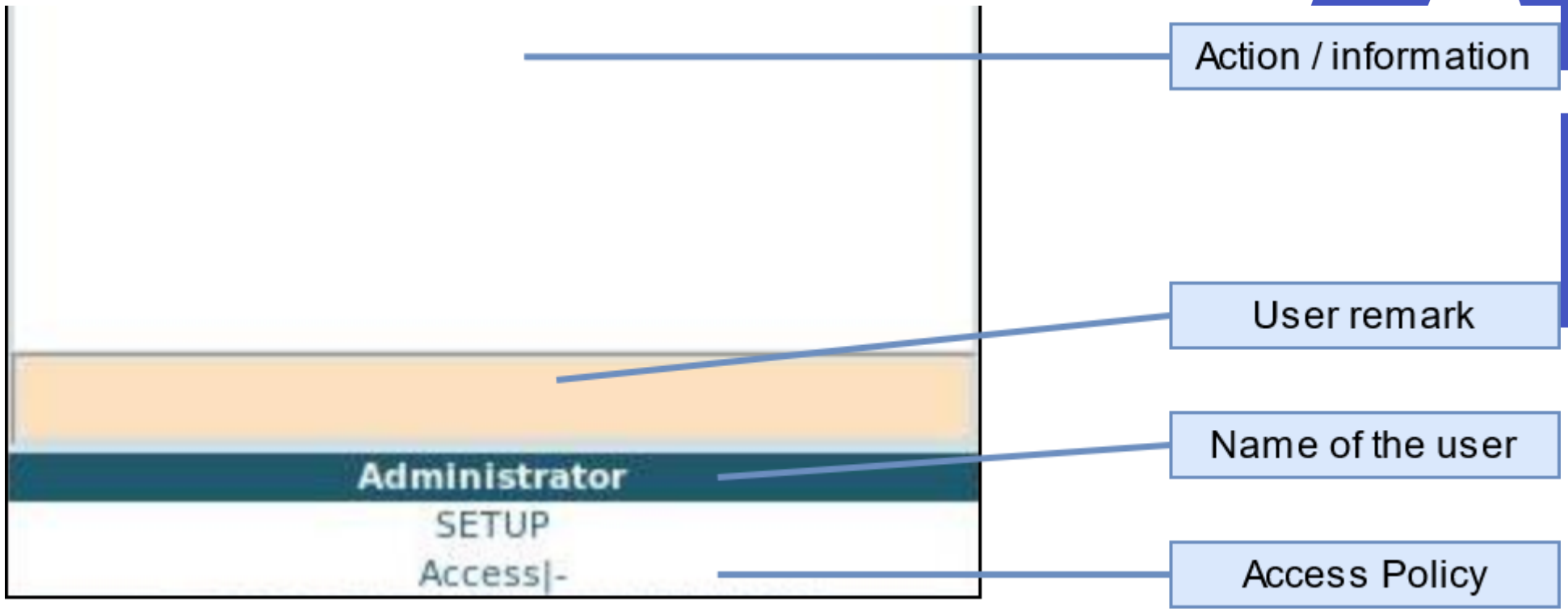


If the application is started in client side window mode,

the control panel is displayed outside of the application window.

The control panel can also be moved by holding down the left mouse button.

The default panel always shows the Assist PIN on top, that can be used by a supervisor to start an Assistance and a text box, where the user can enter a remark.

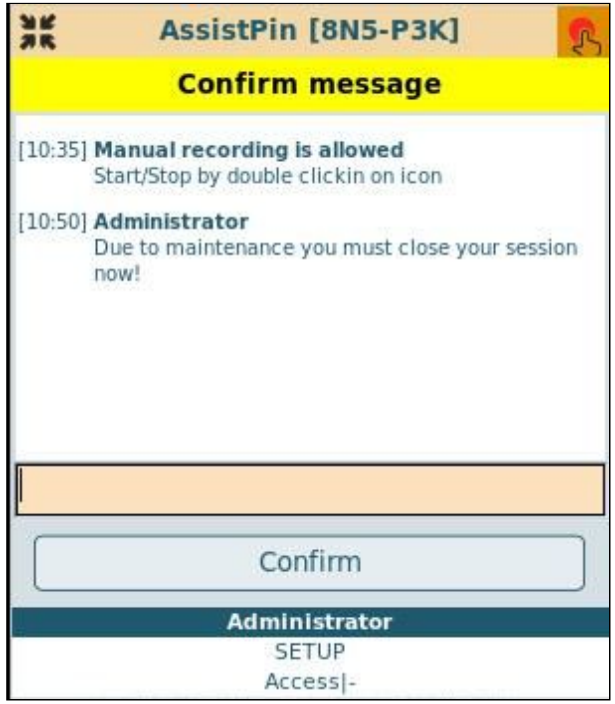


The user is able to record his application sesssion by double clicking on the manual recording icon.
With another double click the recording of the application session is stopped again.

7 Receiving a message

Supervisors, who have access to a VISULOX Cockpit are able to send messages to users, who are working with an application.

This message is displayed in the control panel and the application is locked. The user has to confirm message to continue working.



8 Recorded applications

If an application is configured for recording, the user has to acknowledge the recording.

The control panel is displayed and the application is locked.

When the "**Confirm**"-button is pressed, the application is no longer locked and will be recorded.

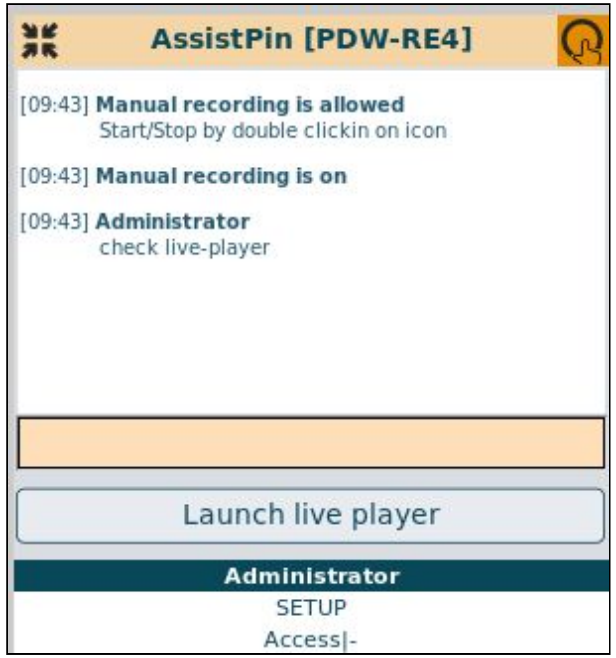
When the "**Reject**"-button is pressed or the message-box is closed, the application will be closed.

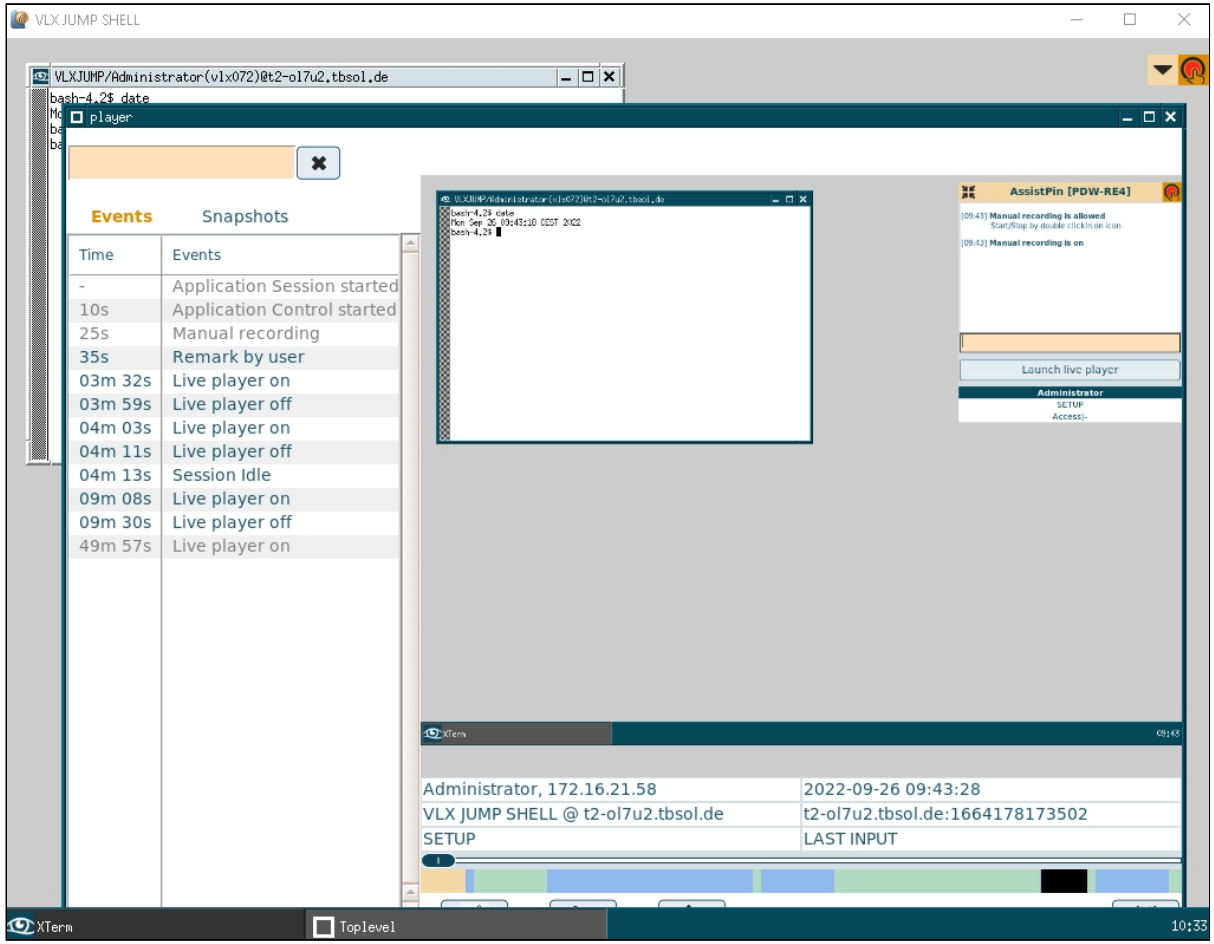
If the user doesn't press any button, it is possible to **auto-accept** or **auto-reject** the recording of the application after a period of time, depending on configuration.

The user can always enter a text in the field for remarks, before the window is confirmed or rejected.

9 Live player in session

If the live player is enabled in configuration, the "**Launch live player**" button is displayed in the session controller and the session can be watched from the beginning:





- The session is still recorded, when using the live player.
- Keyboard entries are not displayed in the live player

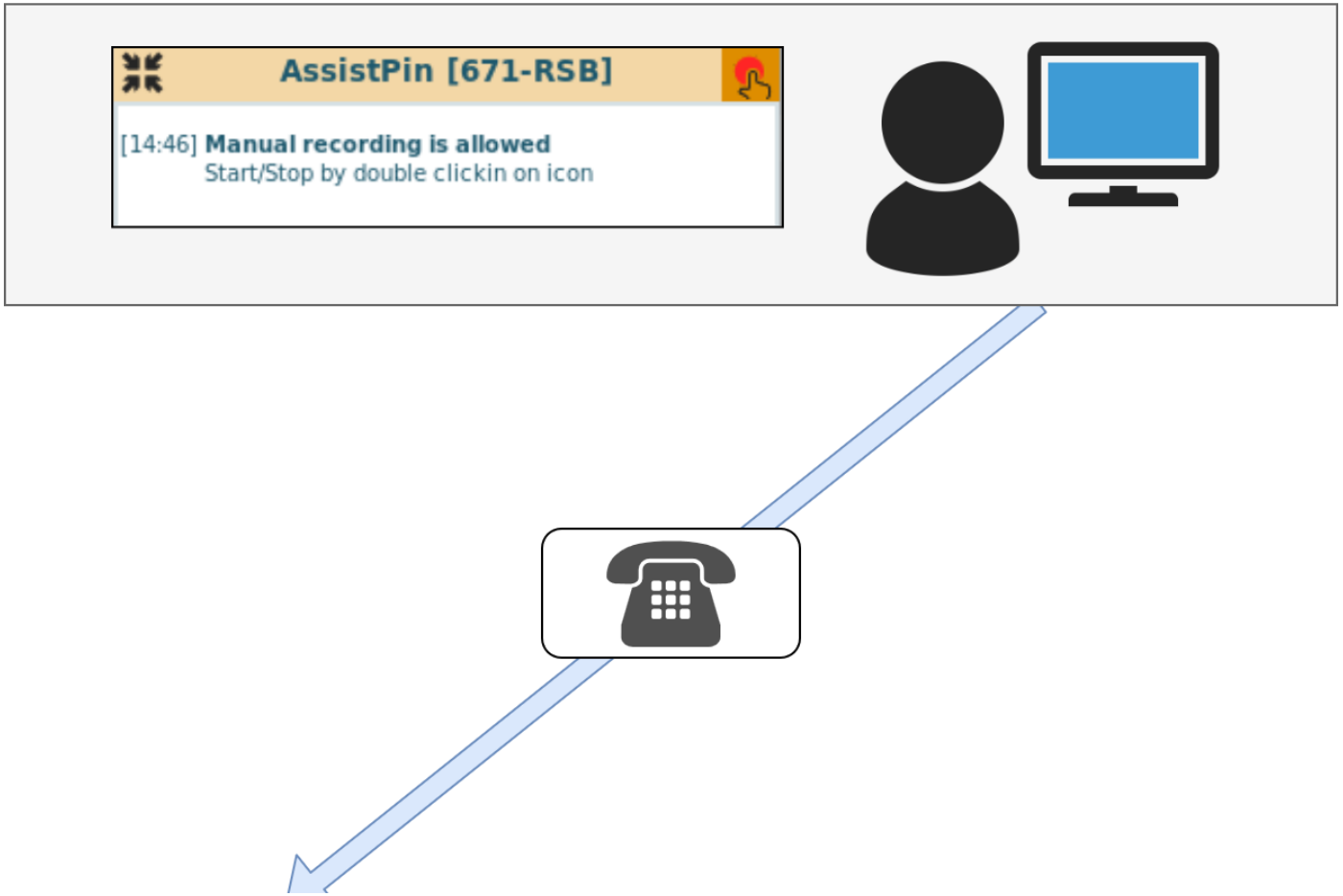
10 Assistance

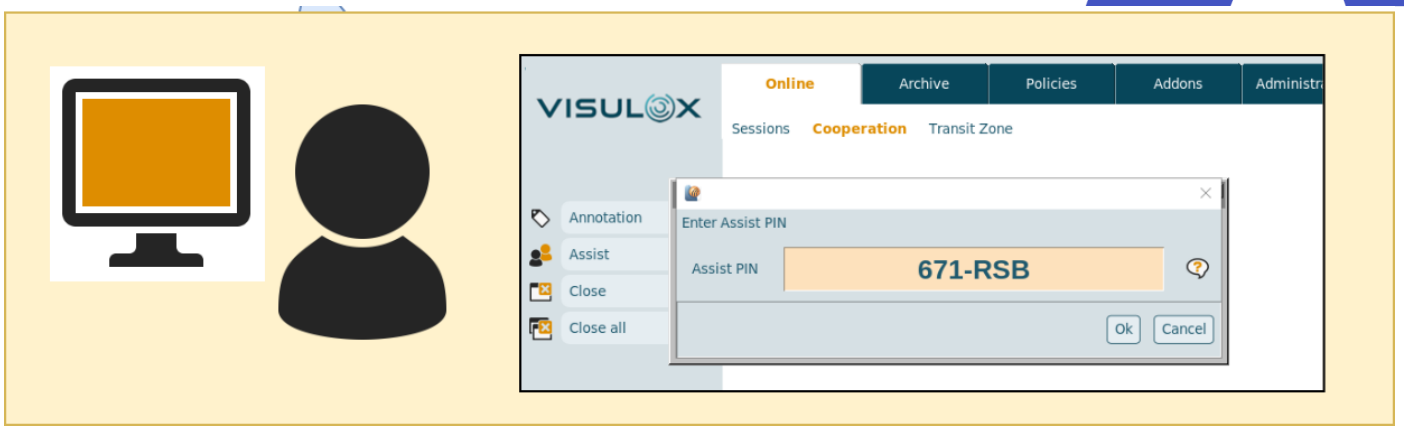
Assist process:

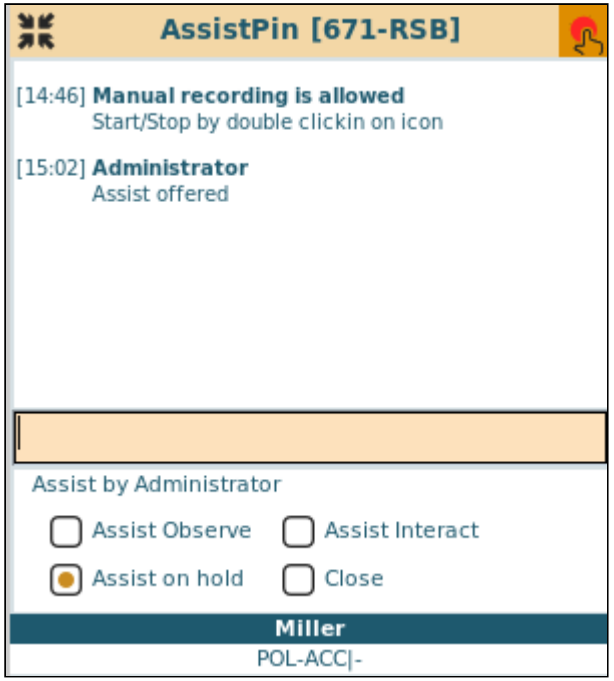
If the user wants to request an Assistance,

he can contact his supervisor or another user and with his unique session ID,

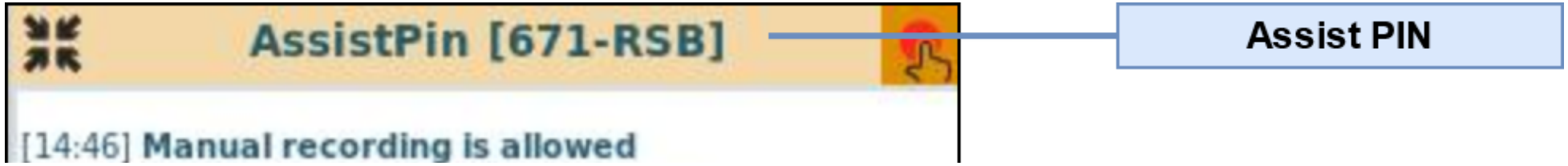
the cooperation partner is able to request the Assistance.

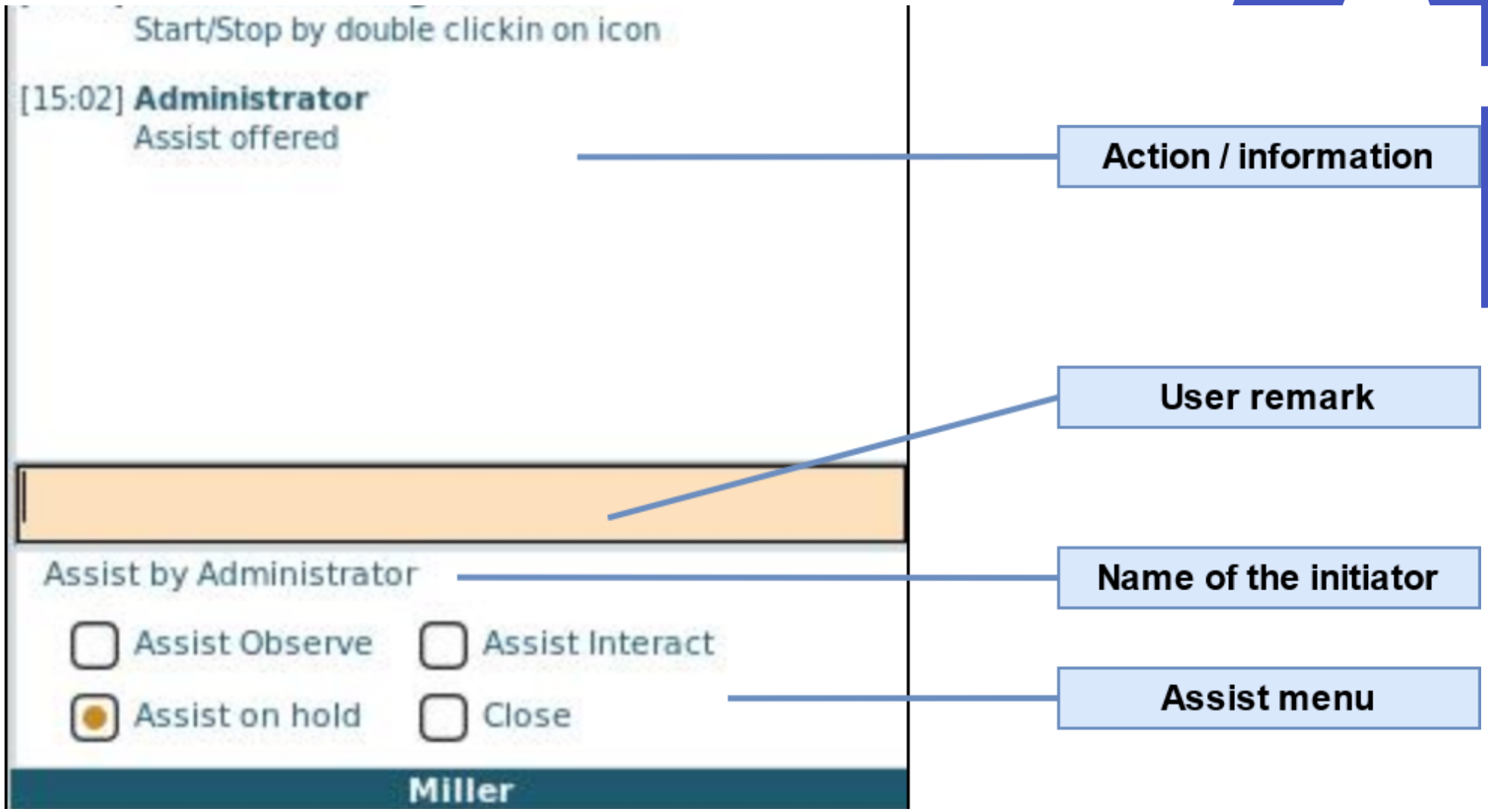



VISULOX
Online
Archive
Policies
Addons
Administra
Sessions
Cooperation
Transit Zone
Annotation
Assist
Close
Close all
Enter Assist PIN
Assist PIN
671-RSB
Ok
Cancel

The user receives the Assistance request via control panel. Assist on hold is selected by default and the user is now able to select the assist mode for the Assistance.	

Assistance request:



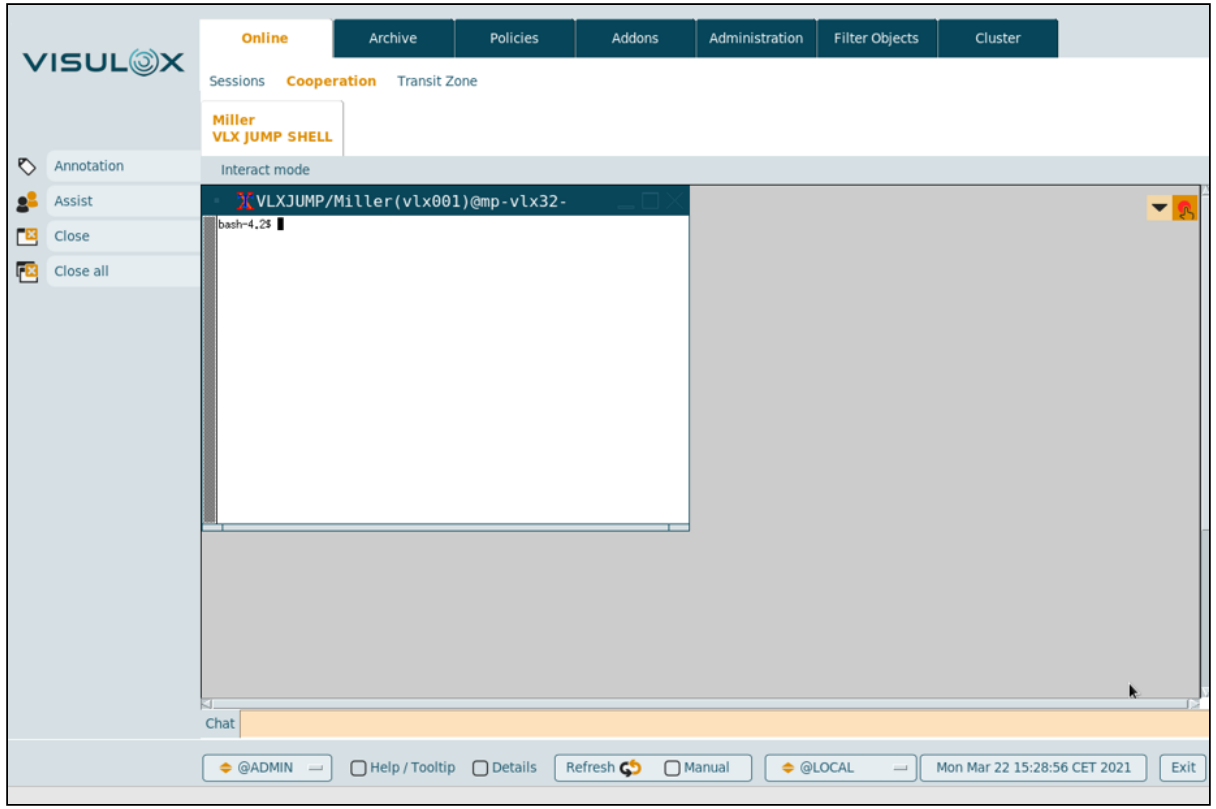

Start/Stop by double clickin on icon
[15:02] Administrator
Assist offered
Action / information
User remark
Assist by Administrator
Name of the initiator
Assist Observe
Assist Interact
Assist on hold
Close
Assist menu
Miller

Default mode on start of a Assistance request is "**Assist on hold**".

The user is able to choose the mode for the Assistance:

- **Assist Observe**:
  In observe mode, the supervisor is able to see the screen of the user, but he can not interact with the application, just displaying his mouse pointer and name is possible.
- **Assist Interact**:
  In interact mode, the supervisor has full access to the application of the user.
- **Assist on hold**:
  In standby mode, the cooperation is active, but the supervisor is not able to see the screen of the application user.
- **Close**:
  Assistance will be closed. The user can continue working without Assistance.

Assistance application:



The supervisor has a chat field beneath the Assistance screen to communicate with the user via control panel.

11 Dual Control

With the Dual Control feature a Cooperation can be established based on a real four-eye-principle.
Dual control ensures that highly sensitive applications can only be accessed when an authorized user is connected, supervising the participant.

In a Dual Control cooperation, there is always a supervisor and a participant, who is working with the application.
When the user starts the base application it is locked, until the supervisor starts his Dual Control application.

The user can now work with the application and Supervisor Master is watching in observe mode:

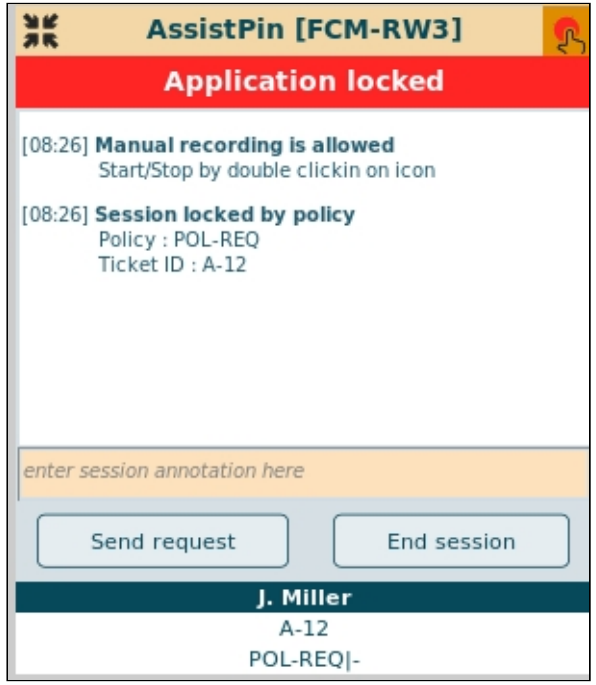
Miller is able to see the current Dual control state. The supervisor is present and the application is activ.	

If Master does not press the trigger, the access to the application is running out.	

Once the trigger time has run out, the application is locked again.	

12 Application locked

If the application is locked because the access period ran out, a message is displayed and the screen is locked.



The user is able to contact an administrator, who can expand the users access period or he can end the session.

It is also possible to send a request via the "**Send request**"-button (⚠️ only available, if a notification or request script is assigned!)

or use "**End session**" on the lock message window. After access is granted again, the lock message disappears

and the user can continue working with the application without loosing his data.

Depending on the configuration of an underlying request script it is possible that the user receives emails with the status of his request.

Approved	Rejected	Expired
Access is approved, Session is no longer locked. If **Full Session** has been chosen by the approver, the access to the application is possible until the session is closed.	Access is rejected by the approver. The session is closed.	When the approver does not react, the request will expire, a mail is sent to the requester and the approver. The session is closed.

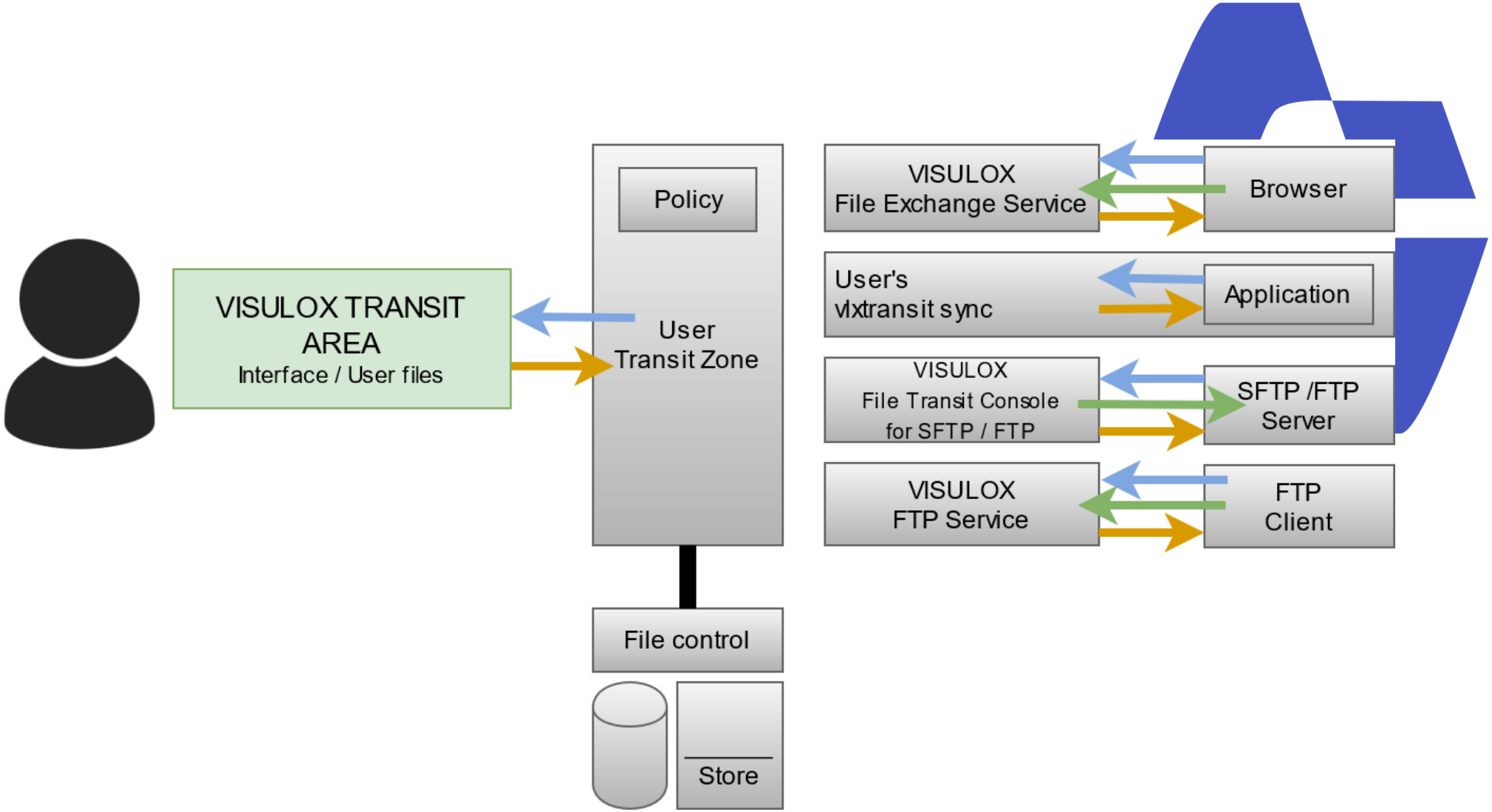
13 File Transfer modules

The modules provide access to the Transit Zone. There are several File Transfer modules, each providing a connection to the Transit Zone:

Transit Web in Workspace	File Transfer interface is presented in the user`s Workspace. The user can upload or download files from his client into the Transit Zone.
File Exchange	The user can connect to every VISULOX node, using the internal WEB browser and a known URL. The WEB Access PIN is needed to see the Transit Zone. Now the user is able to upload and download files from the Transit Zone. (⚠️ The File Exchange service has to be enabled by the administrator).
Sync	Depending on the configuration, the user has a local directory, where he has direct access to the Transit Zone.
Passon script / CLI (automated transfer)	Users are able to upload into the Transit Zone. Depending on the user, file name or file type these files can be passed on automatically to another location via script. It is also possible to copy a file into the Transit Zone of another user via VISULOX transit command line interface.
File Transit Client SFTP/FTP	Interface to interact between the Transit Zone and an SFTP/FTP endpoint. This allows to connect to a server using SFTP, FTP passive or FTP active protocol. Depending on the policy, the user gets a list of hosts he can connect to or he is able to configure his own host list for File Transfer.
FTP Service	Interface to interact between an application server side FTP client with the Transit Zone. (⚠️ The FTP Service has to be enabled , before the service can be used).

13.1 Usage

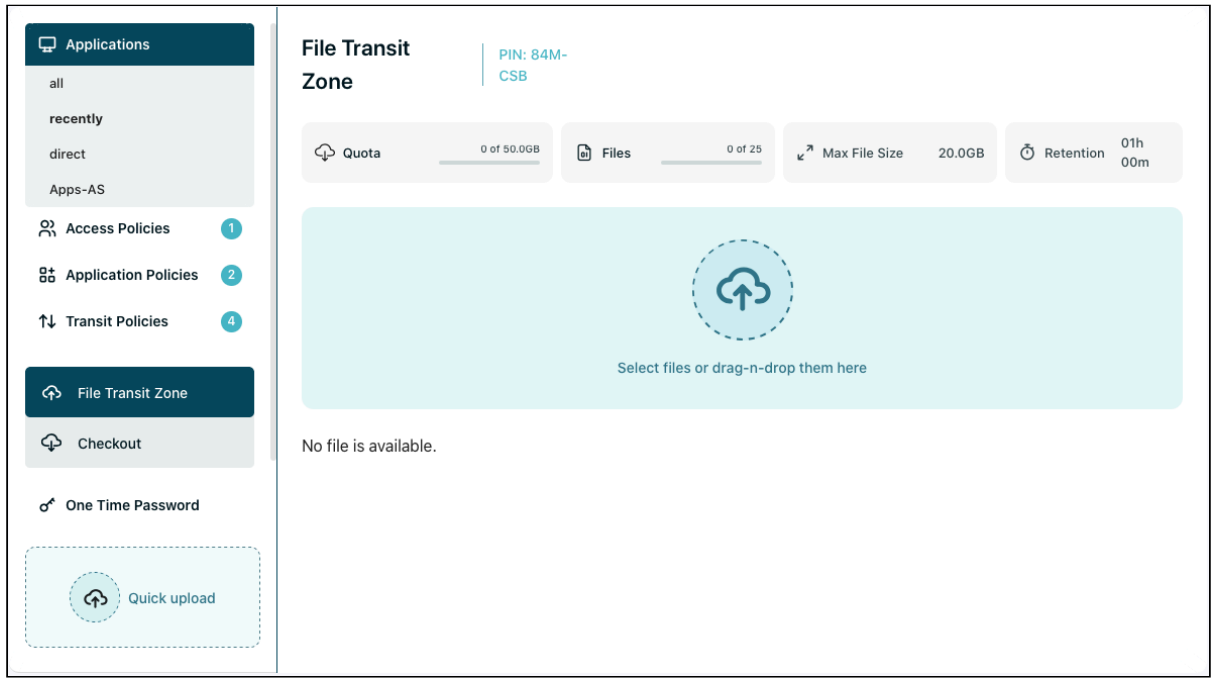
The heart of the VISULOX File Transfer is the user's Transit Zone. Every file a user transports in or outbounded is passing the Transit Zone.


VISULOX TRANSIT AREA
Interface / User files
Policy
User Transit Zone
File control
Store
VISULOX File Exchange Service
Browser
User's vlxtransit sync
Application
VISULOX File Transit Console for SFTP / FTP
SFTP /FTP Server
VISULOX FTP Service
FTP Client

13.1.1 VISULOX Transit Area in Workspace

The VISULOX Transit Area is displayed in the Workspace **(File Transit Zone**).

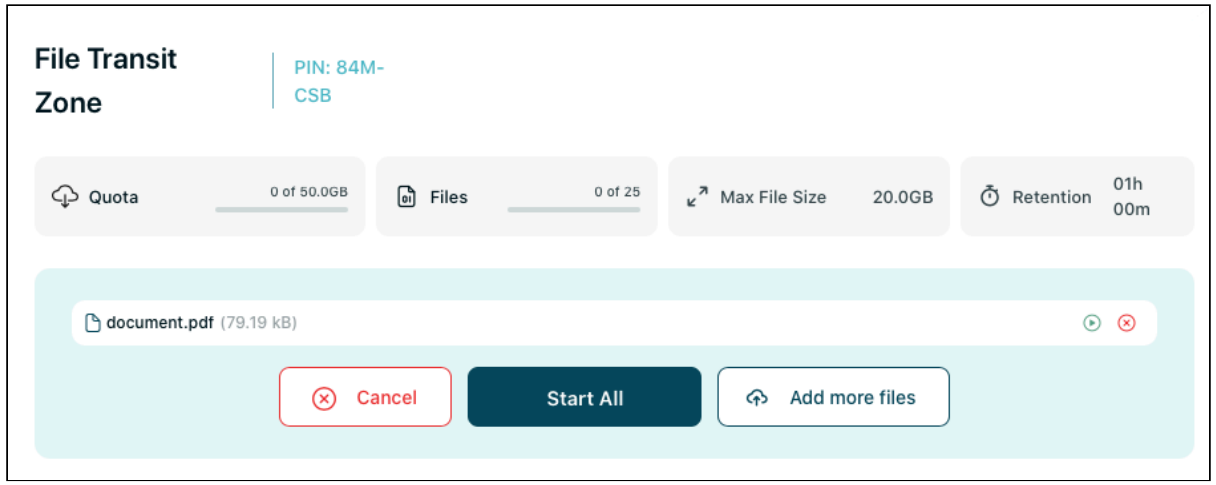
The **maximum quota**, **number of files** in the zone, **max file size** and the **retention time** are shown in the status line.



Within the File Transfer page, the user is able to upload or download files from the local PC into the Transit Zone.

With click on the drag & drop field files can be chosen from the local drives or using drag & drop of files into the area.

Using the "**Start All**" button, the files will be uploaded to the Transit Zone.



Detailed status information is available after uploading:

SOURCE	NAME	AVAILABLE	SIZE	FORMAT	STATUS		
user	doc.pdf	59m 44s	423.66kB	PDF document, version 1.3 sha256:c2fa7942021318adcf0c6fff9c59b571ca1f75e7a2405bf69856f783103d4bc0 md5:a37cd39f7581c1616aff3a42cfd7fda4	accepted:TRANSIT	Download	Delete

If a virus scanner is setup, the files are scanned and will be rejected, if a virus is found.

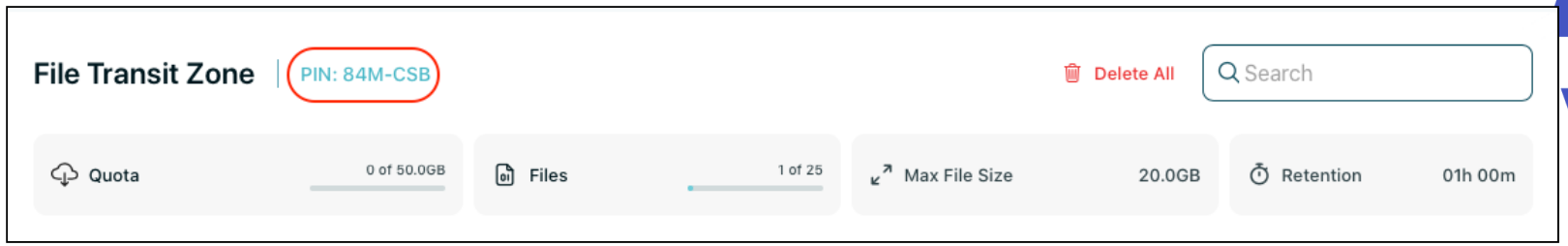
A file can be deleted manually by the user to gain more free diskspace, when the quota is reached.

The files will also be deleted automatically, if the lifetime (retention time) in the Transit Zone is reached.

13.1.2 File Exchange

The File Exchange module is used to upload and download files from the Transit Zone to application servers inside the datacenter.

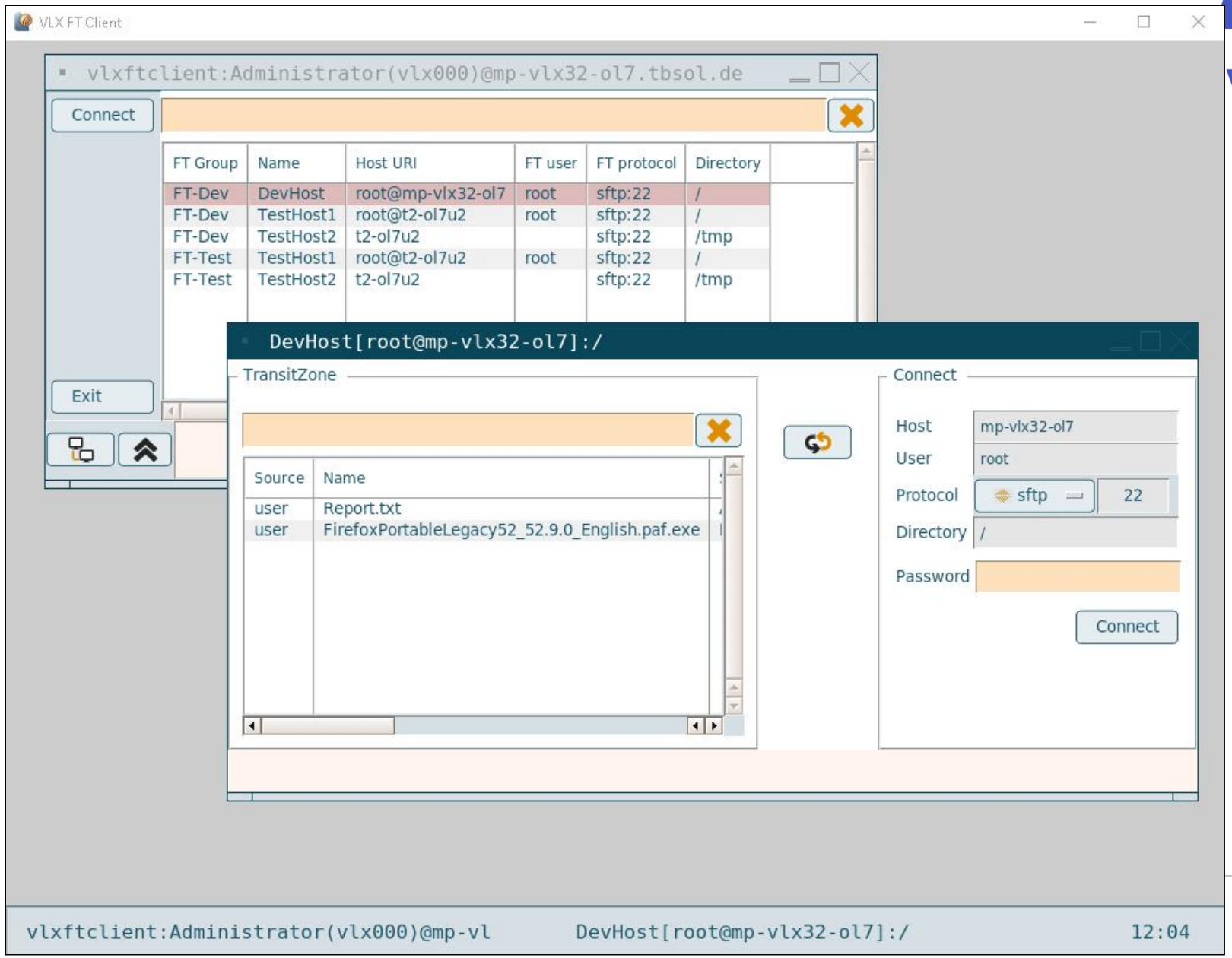
Starting a browser on the application server and entering the URL provided for example via the internal message and the PIN displayed in the Transit Zone.



13.1.3 FT Client

The FT Client is an interface to interact between the user's Transit Zone and an FTP / SFTP endpoint inside the system environment.

With valid credentials the user is able to login to a system with a running FTP / SFTP server. The files in the user's Transit Zone are visible and ready for further transferring.


VLX FT Client
vlxftclient:Administrator(vlx000)@mp-vlx32-ol7.tbsol.de
Connect
FT Group
Name
Host URI
FT user
FT protocol
Directory
FT-Dev DevHost root@mp-vlx32-ol7 root sftp:22 /
FT-Dev TestHost1 root@t2-ol7u2 root sftp:22 /
FT-Dev TestHost2 t2-ol7u2 sftp:22 /tmp
FT-Test TestHost1 root@t2-ol7u2 root sftp:22 /
FT-Test TestHost2 t2-ol7u2 sftp:22 /tmp
Exit
DevHost[root@mp-vlx32-ol7]:/
TransitZone
Source
Name
user Report.txt
user FirefoxPortableLegacy52_52.9.0_English.paf.exe
Connect
Host mp-vlx32-ol7
User root
Protocol sftp 22
Directory /
Password
Connect
vlxftclient:Administrator(vlx000)@mp-vl
DevHost[root@mp-vlx32-ol7]:/
12:04

Sync

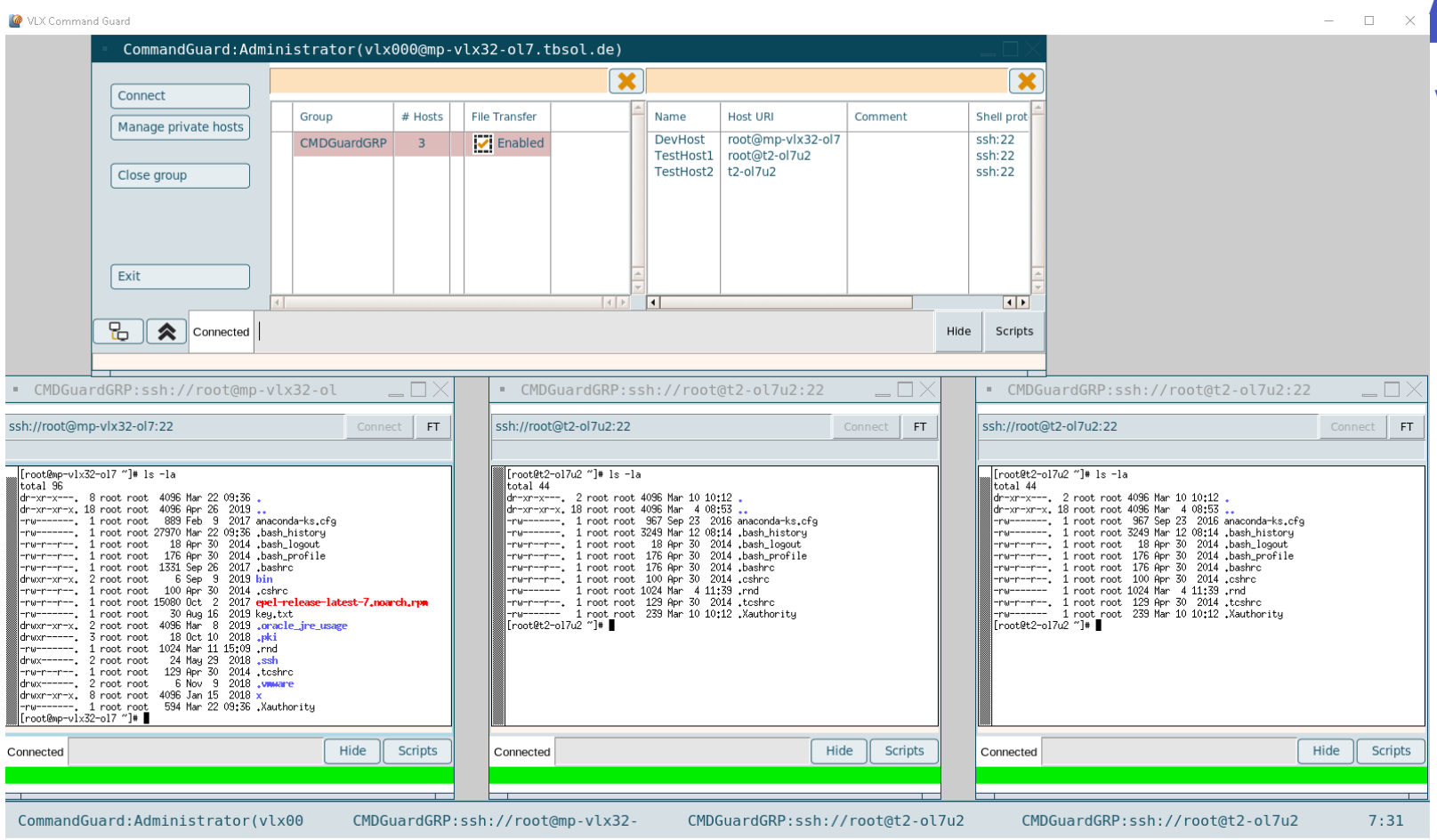
Using a VISULOX implementation of **rdesktop** client, the user's directory in the Transit Zone will be passed to the application server.

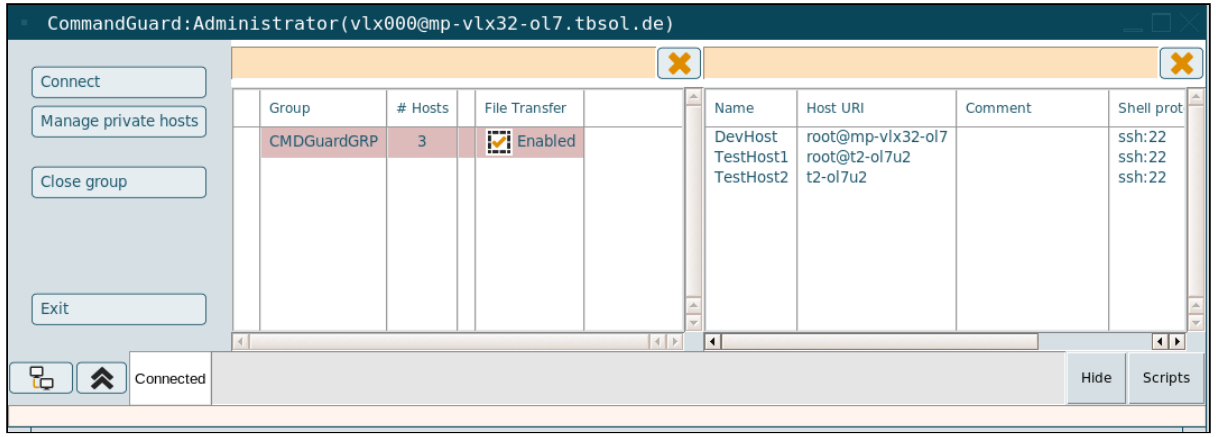
All files from Transit Zone belonging to the user are visible and accessible for further processing.

14 Command Connect / Guard module

Command Connect and **Command Guard** provide a flexible way to access endpoints using a shell interface. Command Connect and Command Guard handle flexible groups and allow the user to send commands to multiple endpoints simultaneously.

Additionally, Command Guard has command level controls for the application. It allows and denies the usage of certain commands entered by the user. Also client and server side scripts can be issued either to multiple endpoints or to a single one.

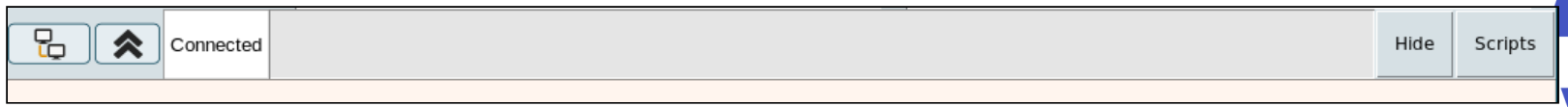

VLX Command Guard
CommandGuard:Administrator(vlx000@mp-vlx32-ol7.tbsol.de)
Connect
Manage private hosts
Close group
Exit
Group
Hosts
File Transfer
CMDGuardGRP
3
Enabled
Name
Host URI
Comment
Shell prot
DevHost
root@mp-vlx32-ol7
ssh:22
TestHost1
root@t2-ol7u2
ssh:22
TestHost2
t2-ol7u2
ssh:22
Connected
Hide
Scripts
CMDGuardGRP:ssh://root@mp-vlx32-ol
ssh://root@mp-vlx32-ol7:22
Connect
FT
[root@mp-vlx32-ol7 ~]# ls -la
total 96
dr-xr-x---. 8 root root 4096 Mar 22 09:36 .
dr-xr-xr-x. 18 root root 4096 Apr 26 2019 ..
-rw-------. 1 root root 889 Feb 9 2017 anaconda-ks.cfg
-rw-------. 1 root root 27970 Mar 22 09:36 .bash_history
-rw-r--r--. 1 root root 18 Apr 30 2014 .bash_logout
-rw-r--r--. 1 root root 176 Apr 30 2014 .bash_profile
-rw-r--r--. 1 root root 1331 Sep 26 2017 .bashrc
drwxr-xr-x. 2 root root 6 Sep 9 2019 bin
-rw-r--r--. 1 root root 100 Apr 30 2014 .cshrc
-rw-r--r--. 1 root root 15080 Oct 2 2017 epel-release-latest-7.noarch.rpm
-rw-------. 1 root root 30 Aug 16 2019 key.txt
drwxr-xr-x. 2 root root 4096 Mar 8 2019 .oracle_jre_usage
drwxr-----. 3 root root 18 Oct 10 2018 .pki
-rw-------. 1 root root 1024 Mar 11 15:09 .rnd
drwx------. 2 root root 24 May 29 2018 .ssh
-rw-r--r--. 1 root root 129 Apr 30 2014 .tcshrc
drwx------. 2 root root 6 Nov 9 2018 .vmware
drwxr-xr-x. 8 root root 4096 Jan 15 2018 x
-rw-------. 1 root root 594 Mar 22 09:36 .Xauthority
[root@mp-vlx32-ol7 ~]#
Connected
Hide
Scripts
CMDGuardGRP:ssh://root@t2-ol7u2:22
ssh://root@t2-ol7u2:22
Connect
FT
[root@t2-ol7u2 ~]# ls -la
total 44
dr-xr-x---. 2 root root 4096 Mar 10 10:12 .
dr-xr-xr-x. 18 root root 4096 Mar 4 08:53 ..
-rw-------. 1 root root 967 Sep 23 2016 anaconda-ks.cfg
-rw-------. 1 root root 3249 Mar 12 08:14 .bash_history
-rw-r--r--. 1 root root 18 Apr 30 2014 .bash_logout
-rw-r--r--. 1 root root 176 Apr 30 2014 .bash_profile
-rw-r--r--. 1 root root 176 Apr 30 2014 .bashrc
-rw-r--r--. 1 root root 100 Apr 30 2014 .cshrc
-rw------- 1 root root 1024 Mar 4 11:39 .rnd
-rw-r--r--. 1 root root 129 Apr 30 2014 .tcshrc
-rw------- 1 root root 239 Mar 10 10:12 .Xauthority
[root@t2-ol7u2 ~]#
Connected
Hide
Scripts
CMDGuardGRP:ssh://root@t2-ol7u2:22
ssh://root@t2-ol7u2:22
Connect
FT
[root@t2-ol7u2 ~]# ls -la
total 44
dr-xr-x---. 2 root root 4096 Mar 10 10:12 .
dr-xr-xr-x. 18 root root 4096 Mar 4 08:53 ..
-rw-------. 1 root root 967 Sep 23 2016 anaconda-ks.cfg
-rw-------. 1 root root 3249 Mar 12 08:14 .bash_history
-rw-r--r--. 1 root root 18 Apr 30 2014 .bash_logout
-rw-r--r--. 1 root root 176 Apr 30 2014 .bash_profile
-rw-r--r--. 1 root root 176 Apr 30 2014 .bashrc
-rw-r--r--. 1 root root 100 Apr 30 2014 .cshrc
-rw------- 1 root root 1024 Mar 4 11:39 .rnd
-rw-r--r--. 1 root root 129 Apr 30 2014 .tcshrc
-rw------- 1 root root 239 Mar 10 10:12 .Xauthority
[root@t2-ol7u2 ~]#
Connected
Hide
Scripts
CommandGuard:Administrator(vlx00
CMDGuardGRP:ssh://root@mp-vlx32-
CMDGuardGRP:ssh://root@t2-ol7u2
CMDGuardGRP:ssh://root@t2-ol7u2
7:31



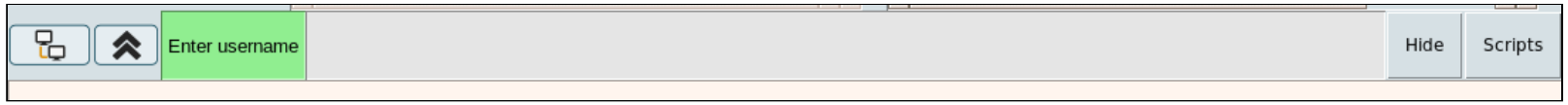
Available buttons:

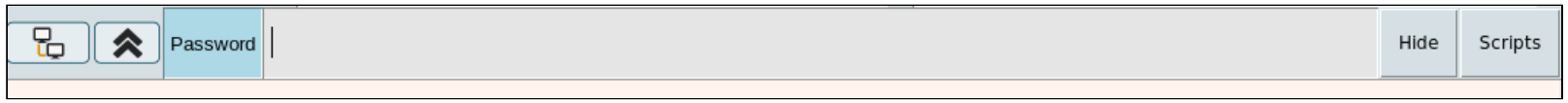
- **Connect:** Opens a shell to all hosts in the selected group
- **Manage private hosts:** Own hosts can be managed for a selected group
- **Close group:** All sessions of the selected group will be closed
- **Exit:** Command Connect / Guard application and all open sessions are closed
- **Arrange:** Connected session windows will be rearranged
- **Collapse:** Collapse the console
- **Hide:** Hide the input in the entryline
- **Scripts:** Shows all available scripts for this group, a selected script can be applied on all open shells

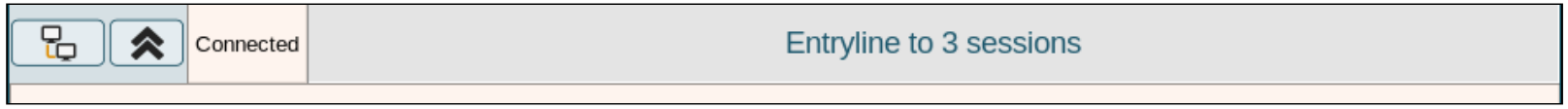
To send a command to all connected shells, the input field of the Command Connect / Guard application can be used.



The status of the terminals is also shown. (enter username, password, connected, etc).





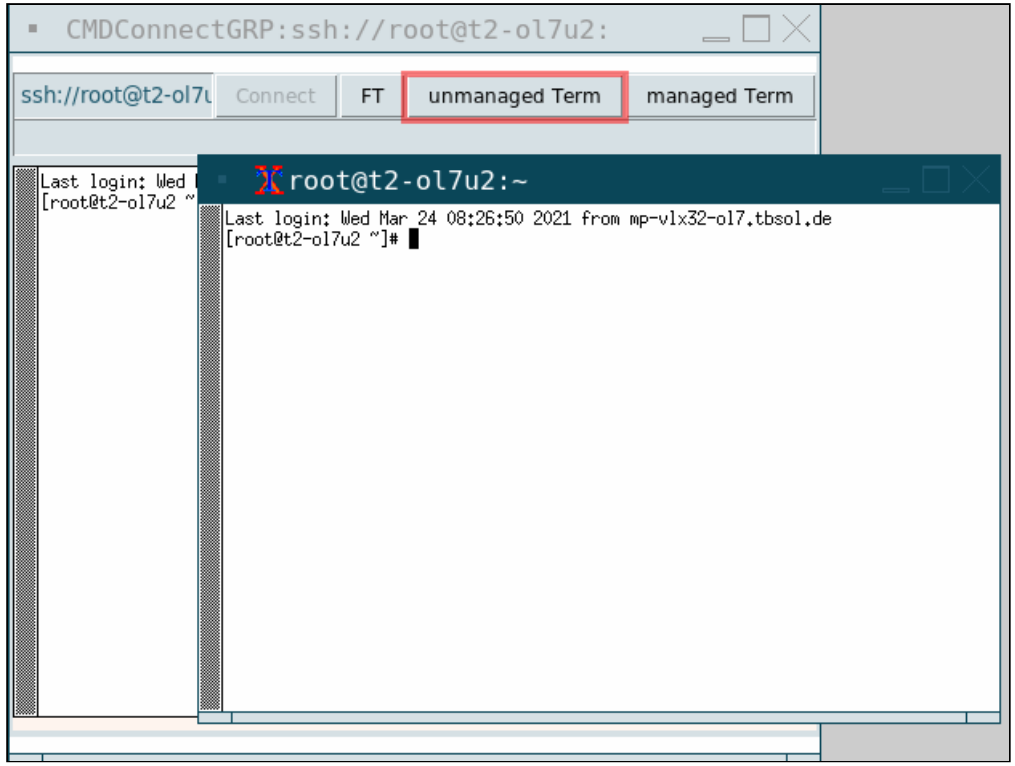


Each connection window also has its own input field and scripts button (CMD Guard), so that commands and scripts can be started only in this shell.

14.1 Unmanaged sessions (CMD Connect only)

In Command Connect one managed session per host is assigned to a Command Connect group. Additionally one more unmanaged session can be opened to a host via the "**Term**" button..

Such unmanaged sessions are closed together with the managed sessions. They are not taken into account with arrange, they are independent and unmanaged.



14.2 Temporary hosts group

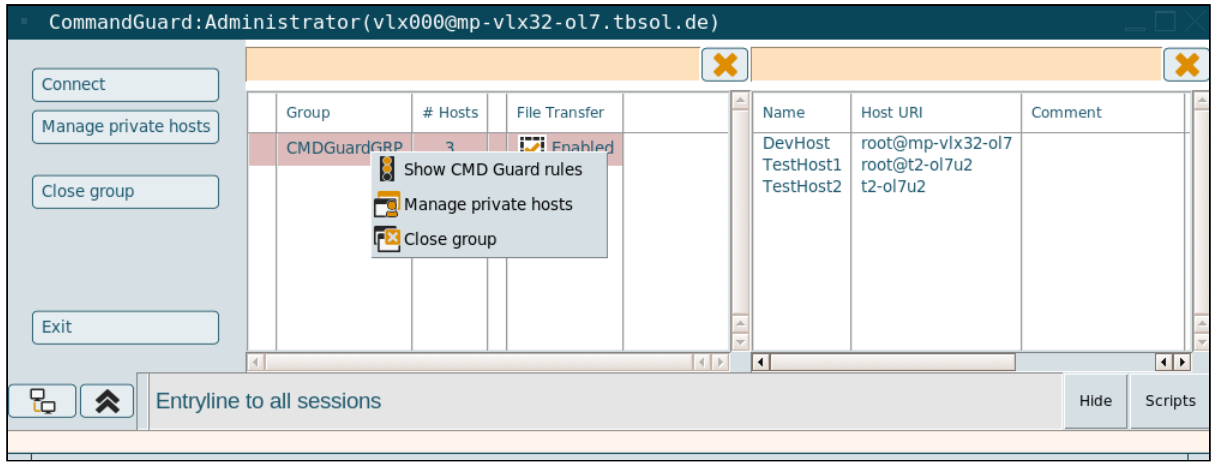
With a right click on an assigned host, the host can be added to a temporary group (@TMP).

Hosts can be added from any available groups to combine them in the new @TMP group.

14.3 Own hosts

Command Connect / Guard has the ability to manage own hosts.

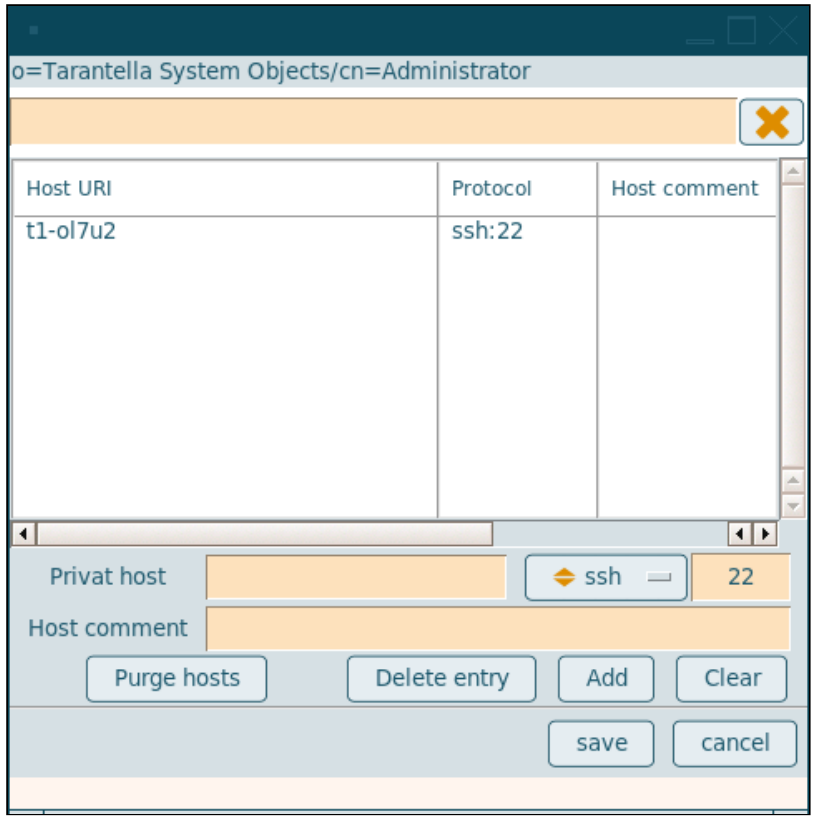
To keep this under control, the admin defines a ruleset, what kind of hosts can be added. The ruleset is part of the Command Connect / Guard group.



With a right click on a group in Command Connect / Guard, the Guard rules (Guard only) can be displayed, own private hosts can be added (depending on the rules) or the group can be closed.

The private hosts are based on rules, the user is a string and the host is a string or an IP address.

Command Connect / Guard tries to resolve the name, then the rule is checked. If there are private hosts that are no longer valid, because the rule has changed, the invalid hosts can be purged with the "Purge hosts" button.



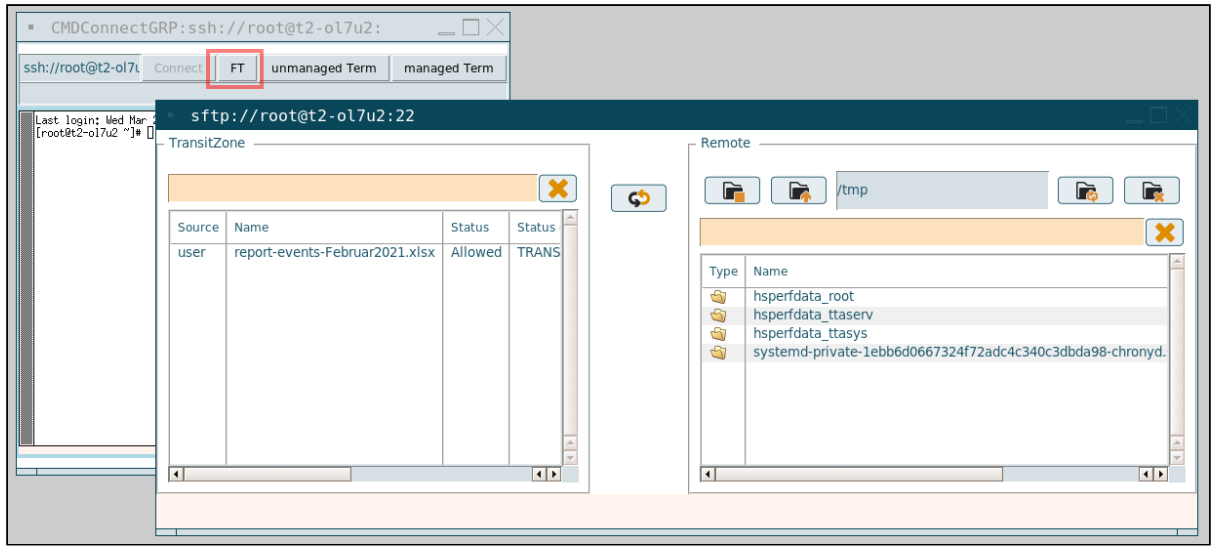
14.4 Command blocked (CMD Guard only)

In Command Guard a ruleset defines the allowed commands. If a command is not allowed, a **Stop** sign is displayed and the command will not be executed.

14.5 File Transfer

If File Transfer is enabled to the host of the connection, an FT button is available to start the FT Client to the host.

Depending on the configuration it can be necessary to enter a username, a base directory and a password for the File Transfer connection.



With the FT Client component, the user is able to transfer files between the Transit Zone and the application server according to the underlying File Transit rules. (See also: File Transfer modules)

15 Appendix_U

15.1 Appendix

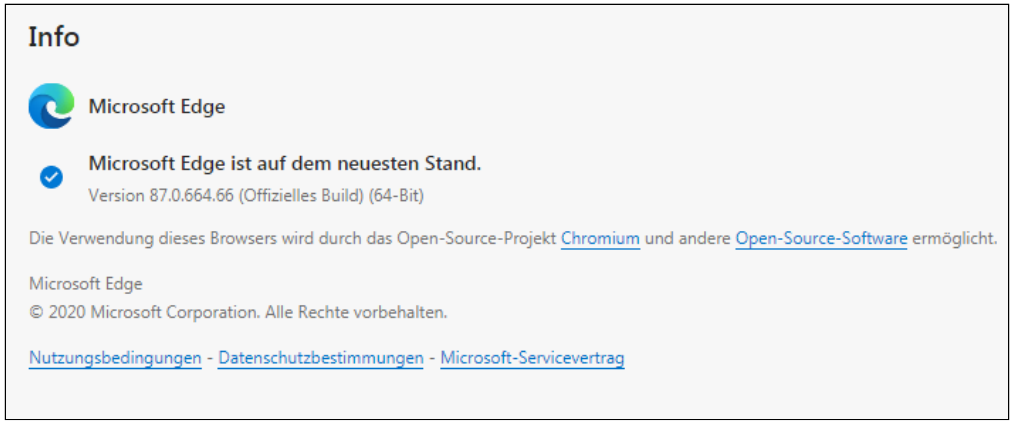
Troubleshooting and **Glossary**

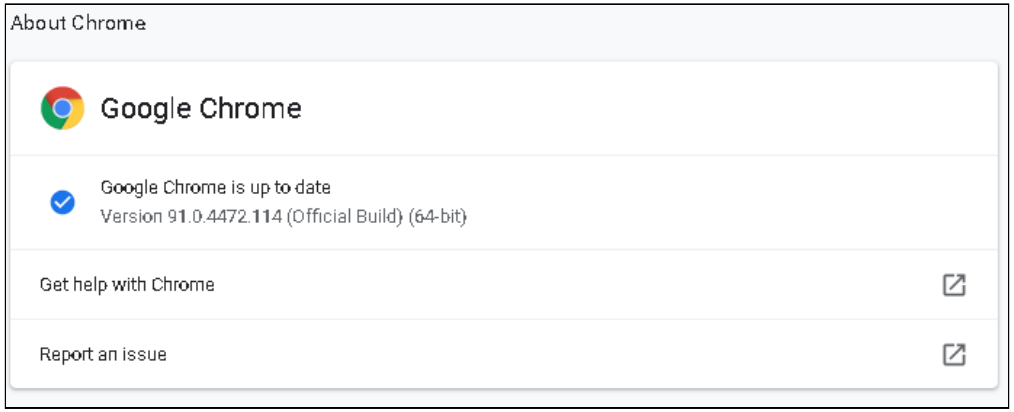
15.1.1 Troubleshooting

The following information can help to identify possible errors on the client side and it is useful to have them at hand, when contacting an administrator / support.

Version of the used browser

Displaying the version of the used browser (for example: Edge, Firefox and Chrome):

Microsoft Edge		Help and Feedback / Info about Microsoft Edge

Mozilla Firefox		Help / About Firefox
Google Chrome		Help / About Google Chrome

The supported browsers and browser versions by VISULOX are listed in the current documentation.

Other settings:
The settings of the used browser should be checked and possibly critical settings or addons should be disabled (e.g. popup blocker, noscript, etc).

Microsoft Edge
Edge's settings should be changed to prevent idle tabs from sleeping, which can disconnect the workspace:

Disable sleeping tabs in Microsoft Edge:

1. Open Microsoft Edge.
2. Click the **three dots (⋯)** in the top-right corner and select **Settings**.
3. In the left sidebar, click **System and performance**.
4. Scroll down to the **Optimize Performance** section.
5. Toggle **off** the switch for:
    - **"Save resources with sleeping tabs"**

Optional: If you want more control, you can also add sites to the "Never put these sites to sleep" list.

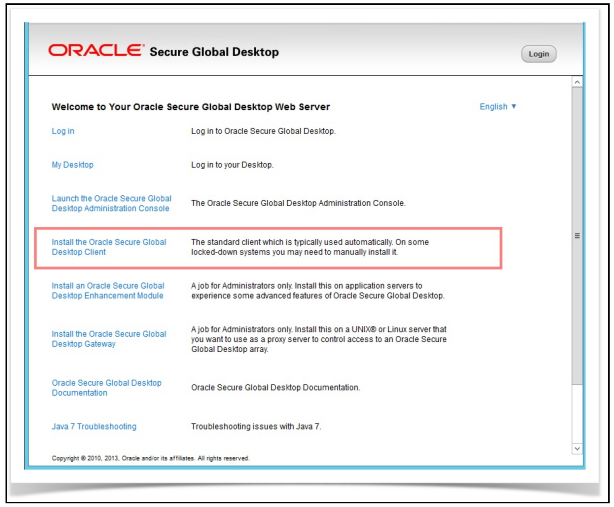
After these changes, please set the following parameter on the VISULOX side:

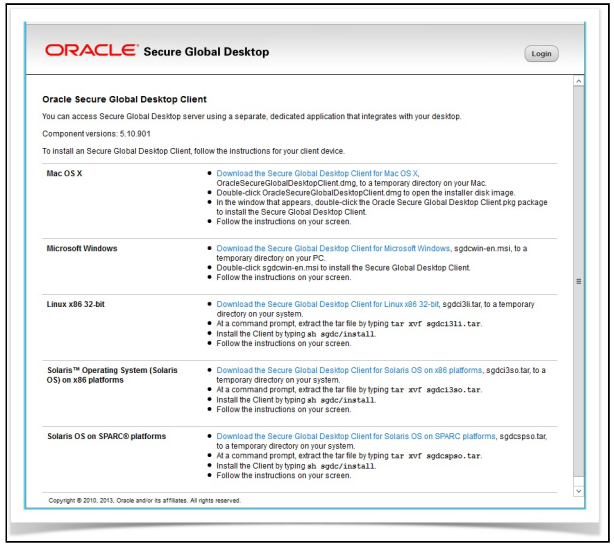
```
visulox config -name api.sessioncookie.lifetime=240
```

Native Client

In case of problems with the automatic download of the native client, it can be downloaded and installed manually, if no direct forwarding to the login page is configured.

> The Native Client is provided by Oracle.

Native Client	

Client versions	

ORACLE Secure Global Desktop

Login

Oracle Secure Global Desktop Client

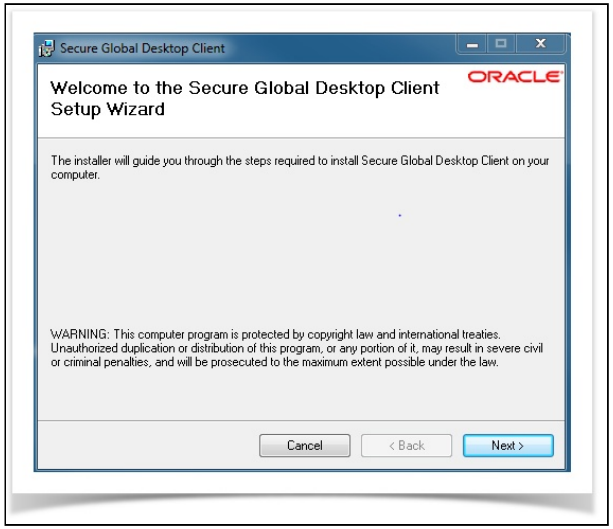
You can access Secure Global Desktop server using a separate, dedicated application that integrates with your desktop.

Component versions: 5.10.901

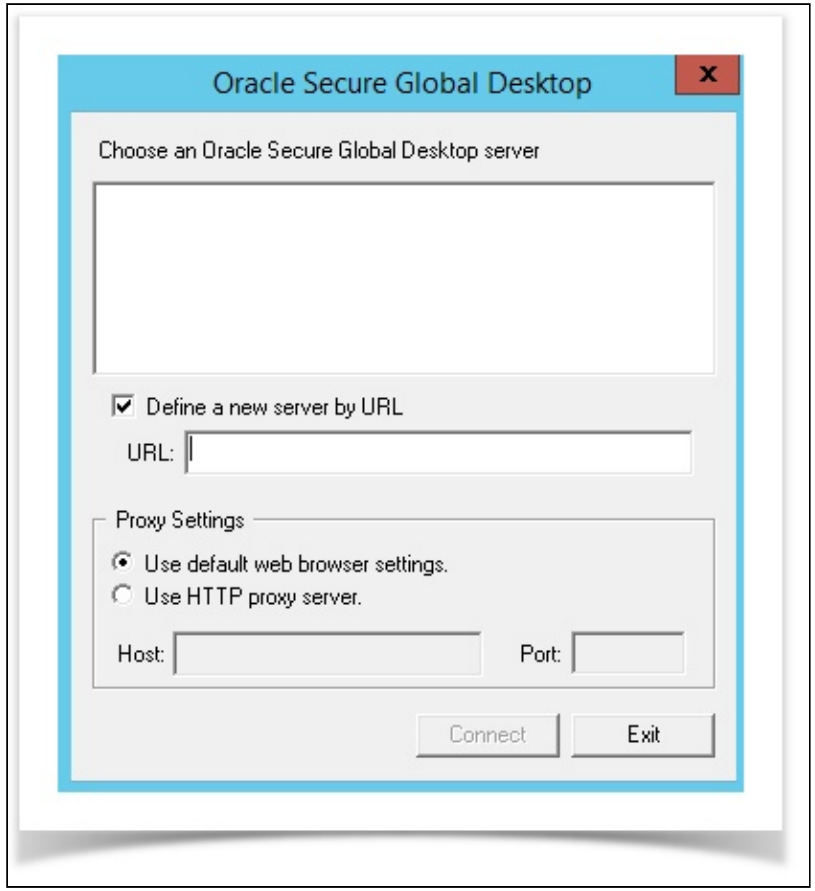
To install an Secure Global Desktop Client, follow the instructions for your client device.

Mac OS X	• Download the Secure Global Desktop Client for Mac OS X, OracleSecureGlobalDesktopClient.dmg, to a temporary directory on your Mac. • Double-click OracleSecureGlobalDesktopClient.dmg to open the installer disk image. • In the window that appears, double-click the Oracle Secure Global Desktop Client.pkg package to install the Secure Global Desktop Client. • Follow the instructions on your screen.
Microsoft Windows	• Download the Secure Global Desktop Client for Microsoft Windows, sgdcwin-en.msi, to a temporary directory on your PC. • Double-click sgdcwin-en.msi to install the Secure Global Desktop Client. • Follow the instructions on your screen.
Linux x86 32-bit	• Download the Secure Global Desktop Client for Linux x86 32-bit, sgdci3li.tar, to a temporary directory on your system. • At a command prompt, extract the tar file by typing `tar xvf sgdci3li.tar`. • Install the Client by typing `sh sgdc/install`. • Follow the instructions on your screen.
Solaris™ Operating System (Solaris OS) on x86 platforms	• Download the Secure Global Desktop Client for Solaris OS on x86 platforms, sgdci3so.tar, to a temporary directory on your system. • At a command prompt, extract the tar file by typing `tar xvf sgdci3so.tar`. • Install the Client by typing `sh sgdc/install`. • Follow the instructions on your screen.
Solaris OS on SPARC® platforms	• Download the Secure Global Desktop Client for Solaris OS on SPARC platforms, sgdcspso.tar, to a temporary directory on your system. • At a command prompt, extract the tar file by typing `tar xvf sgdcspso.tar`. • Install the Client by typing `sh sgdc/install`. • Follow the instructions on your screen.

Copyright © 2010, 2013, Oracle and/or its affiliates. All rights reserved.

Installation	

After installation, the Native Client can be started manually:

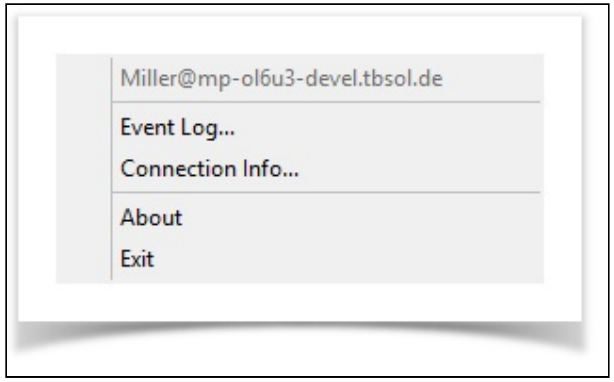


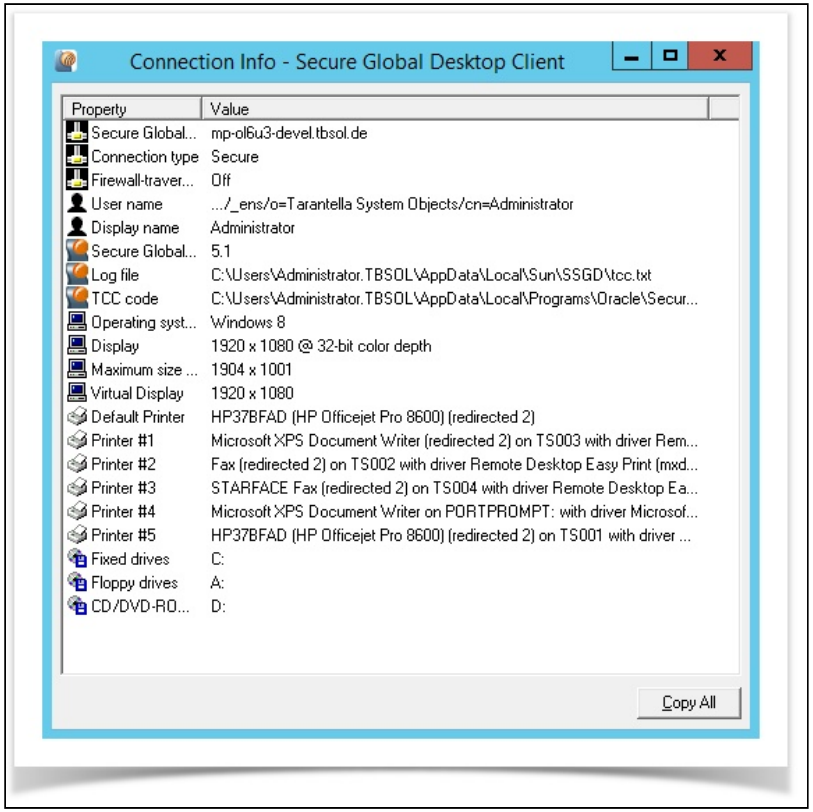
How to install the client for Linux Mint

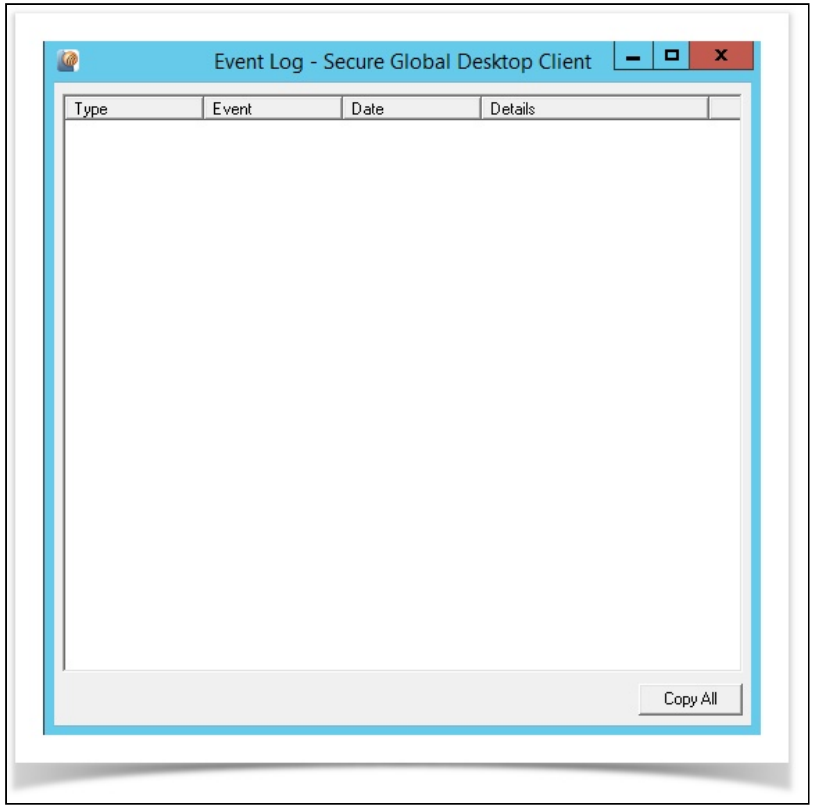
```
sudo dpkg -i ./sgdclient_5.60.567-ubuntu22.04_x86_x64.deb
sudo apt-get install libxm4 libmotif-common
```

Tarantella Client Component (TCC)

Once connected to a VISULOX PORTAL, a TCC connection icon ( ) is displayed in the taskbar:

TCC taskbar-menu	

Connection Info	

Event Log	

General: Special characters in passwords

In mixed environments (Windows / Linux and also cloud services) there are so called **interoperability issues**.

Therefore the following rules should be considered:

The allowed characters in a password can vary depending on the recommendations of the particular website, platform or system.
However, the following character types are generally recommended:

1. Characters: Upper case characters (A-Z) and lower case characters (a-z).
2. Numbers: (0-9).
3. Special characters:
   These may vary by system, but typically include:

- ! @ # $ % ^ & * ( ) _ - + = [ ] { } | \ : ' , . ? / ` ~ " ; < >.

VISULOX has been tested with these characters.

VISULOX PORTAL Login error codes

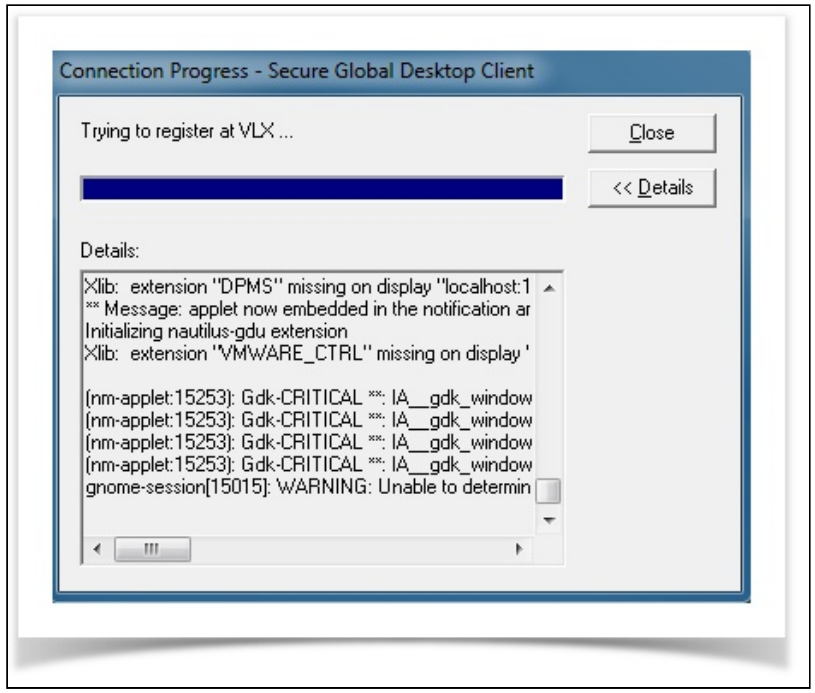
The **-1** error code is due to invalid data provided, so that it could not get a connection to the VISULOX PORTAL. Maybe due to an invalid profile.

The **-7** is more than likely a proxy problem, maybe due to proxy chaining.

```
#define EHTTPCONNECTFAILED -1
#define ENEEDPROXYAUTH -2
#define EHTTPERRORRESPONSE -3
#define EPROXYERRORRESPONSE -4
#define EPROXYNONBASICAUTH -5
#define EHTTPSSLHANDSHAKE -6
#define ESERVERCHAIN -7 // error occured in the server chain
#define EUSERCANCELLED -8 // user cancelled the request (e.g., by using
// the Cancel button on an Auth dialog)
#define EDOWNGRADEDSSL -9
```

Application start via Workspace

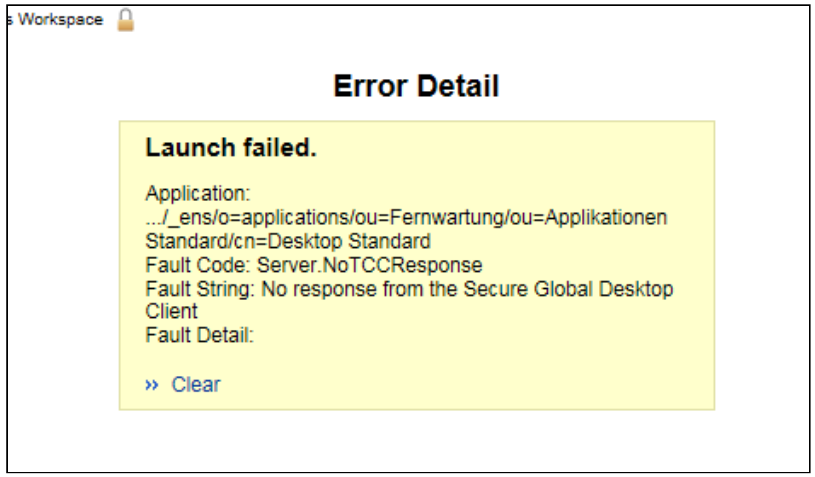
When an application is started via Workspace a small **Connection Progress** window is opened. Mostly this window disappears immediately and the application is launched. If there is a problem with the connection to the application, then this window stays open and shows the errors occurred.



With **Paste & Copy** the output can be copied to a text file and send to a supervisor / support.

Error during start of an application in Workspace

It may happen, that the Tarantella Client Component (TCC) disappears or has no connection to the VISULOX PORTAL, the following error is displayed in the Workspace:



In this case refreshing the Workspace (F5) or logging out and logging in again will solve the problem.

VISULOX shell script tracing

VISULOX Shell scripts are running in the background. Errors can be found in the log.

For testing, the following lines in the header of the shell scripts activate tracing:

```
#!/bin/bash
# verify helpful lines
exec 99> <path to a log file>
```

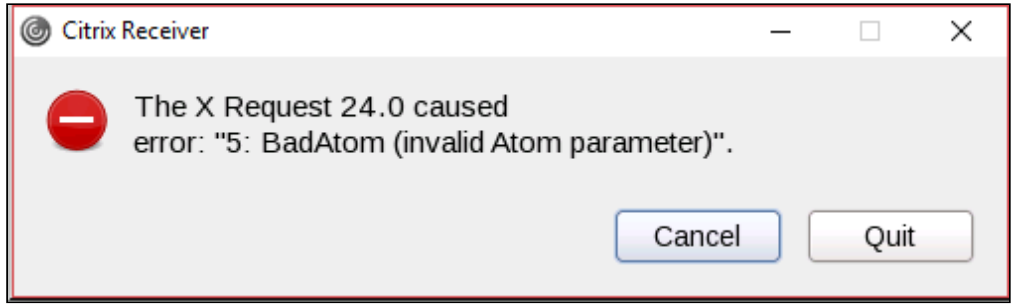
```
BASH_XTRACEFD=99
set -x
```

Using Flash Player and checked out films

Flash is no longer supported.

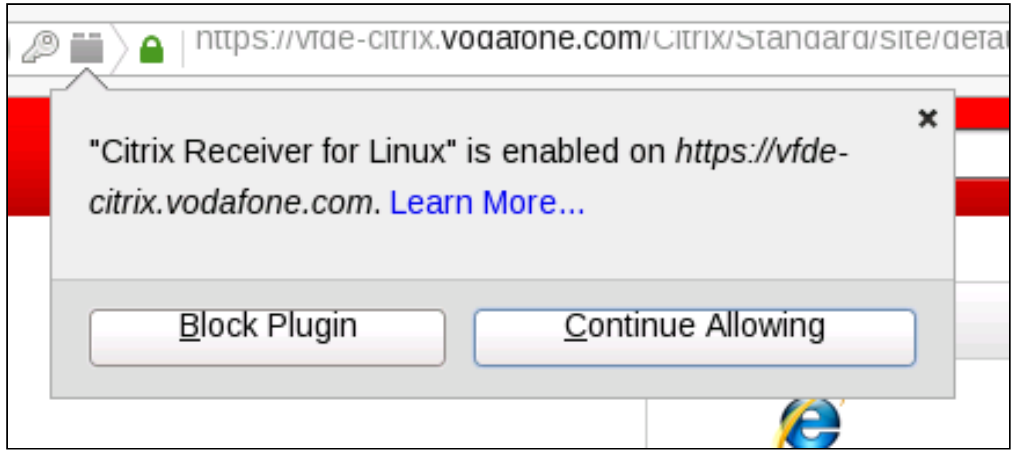
Citrix Receiver

Depending on the version of Citrix Receiver, the following error message can be shown:



The “**Cancel**”-button has to be used to close the window. The application starts as usual.

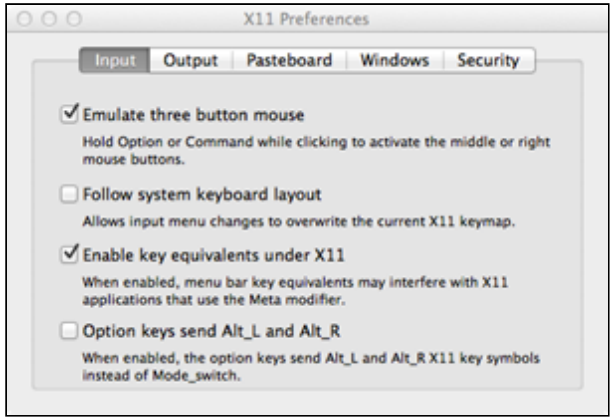
Also always take care, that the Citrix Receiver plugin is not blocked by the browser. Check plugin status via address bar icon in the browser:

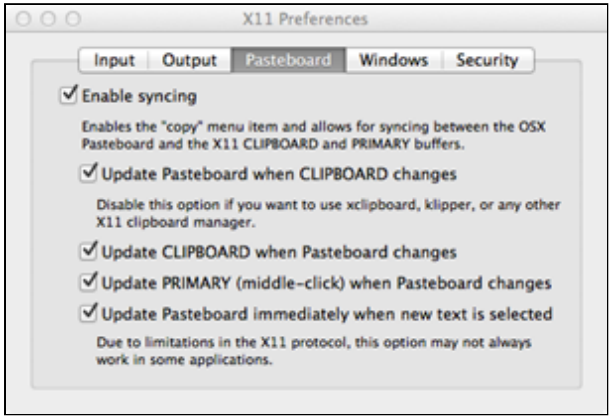


Copy & paste for Mac OS

Use the following configuration steps for X11 to activate the copy/paste function in command Connect / X11 windows for Mac OS + XQuartz:

- Open the X11 preferences and activate “Emulate three button mouse”
- Enable all actions for Pasteboard / Clipboard





Paste = ALT + click
Copy = Select the text to copy it to the clipboard

Copy & paste in HTML5 sessions / application toolbar

When you are displaying an application, a toolbar on the left side of the application tab is shown. The toolbar has icons that can be used for some operations, such as copy and paste.

Icon	Description
	Copies the selected text to the clipboard.

Icon	Description
	Pastes the selected text from the clipboard.
	Displays menu options for sending keyboard shortcuts to the application window.

Copying and pasting between applications

Copy and paste text to and from the client, and between applications. When the HTML5 Workspace is used, it is not allowed to access the local device's clipboard directly. This means for copy and paste on the HTML5 Workspace there are extra stages necessary, compared to the standard Workspace.

The following changes apply for copy and paste:

- Data must be placed on to the HTML5 Workspace clipboard first, before it can be pasted to a remote application or to the client device.
  The copy icon in the side toolbar can be used to retrieve the data that should be copied from an application and place it on the Workspace clipboard.
- The paste icon can be used to copy text to the client device's clipboard.

The following procedures describe how to copy and paste text for applications:

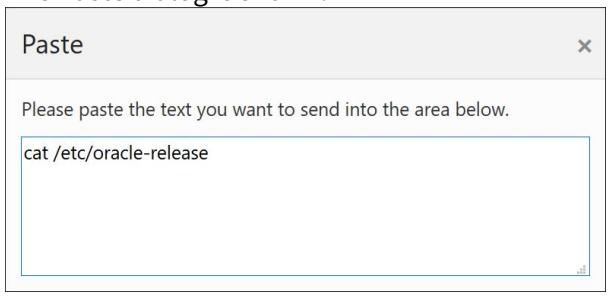
Copying from an application to a client device

1. Select and copy the text in the application.
   Use the normal method for the application you are copying from. For example, use a menu option in the application.
2. Retrieve the text from the application.
   Click the Copy icon in the application toolbar.
   Click Confirm to allow the application to copy text to the client device clipboard.
3. Paste the copied text into an application on the client device.

Use the normal method for the application you are pasting to. For example, use a menu option in the application.

Pasting to an application from a client device

1. Select and copy the text from the application on the client device. Use the normal method for the application you are copying from.
   For example, use a menu option in the application.
2. Retrieve the text from the client device clipboard.
   Click the Paste icon in the application toolbar.
   The Paste dialog is shown:



3. Paste the copied text into the text box on the paste dialog.
   Do either of the following:
   • Right-click and select paste.
   • Use the Ctrl-V keyboard shortcut.
   This will automatically close the paste dialog.
4. Paste the copied text into the pplication.
   Use the normal method for the application you are pasting to. For example, use a menu option in the application.

Copying between applications

1. Select and copy the text in the first application. Use the normal method for the application you are copying from.
   For example, use a menu option in the application.
2. Retrieve the text from the application.
   Click the Copy icon in the application toolbar.
3. Switch to the second application.
   The copied text is sent automatically to the second application.
4. Paste the copied text into the second application.
   Use the normal method for the application you are pasting to. For example, use a menu option in the application.

Sending local keyboard shortcuts to the remote application

The Windows key and keyboard shortcuts for managing windows can be sent to the remote session.

1. Click the keyboard icon in the application toolbar.
   Options are shown for inserting one of the following remote keyboard shortcuts:
   • Ctrl-Alt-Del
   • Windows key
2. Click the required remote keyboard shortcut.
   The key presses are sent to the remote application window.

15.1.2 Glossary

Expression	Description
3PA	Third Party Authentication / 3rd Party Authentication
Access Branding	With Access Branding it is possible to display different login page designs for different users according to their access point.
Access Management	Enhanced VISULOX Concept for administrating the access of users
AD	**A**ctive **D**irectory
AIP	**A**daptive **I**nternet **P**rotocol: Client communication protocol from the VISULOX PORTAL Service
Ambiguous login	The situation where an authentication mechanism has found more than one match for a user and cannot distinguish between them without further information from the user

Annotation	A short text, that can be entered before a recorded session is confirmed, during a recorded session or in VISULOX Cockpit / Archive for closed sessions
API	**A**pplication **P**rogramming **I**nterface
Application server	A server which provides applications, that can be accessed via the VISULOX PORTAL
Application session	See: **emulator session**
Args	The arguments an application is started with
Assist / Assistance	See: **Assisting Cooperation**
Assisting cooperation	Within the VISULOX Cockpit, the user can select an application and press assist to join the application. The owner of the application selects the cooperation mode
Chapter	A chapter equals 20 minutes film of a recorded session
CLI	**C**ommand **L**ine **I**nterface
CMD	The command / path an application is started with
Cooperation	When two or more users are watching or working with the same application in realtime on their own desktop
Cooperation master	The user, who has started the application (owner) will be the master of this application in a Cooperation

Cooperation member	A user, who is not owner of an application and who is not able to switch the cooperation modes
Cooperation modes	**On hold**: Member is assigned to a Cooperation, but does not participate **Observe:** Member is able to watch the Cooperation application, but can not interact **Interact:** Member can interact with the application
CP	Short form for **Cooperation**
Datastore	Internal VISULOX PORTAL Service database, where all defined objects (users, hosts, applications) are stored. A VISULOX PORTAL Array replicates the datastore between all members simultaneously
DMZ	Demilitarized zone (Perimeter zone)
DSI	**D**irectory **S**ervice **I**ntegration
Dual Control	Cooperation enforcing a real four-eye-principle
ELU	**E**xtended **L**icense **U**sage - When ELU has expired, its not possible to start more recorders or display more users than allowed under MD / Status, max users / recorders
Emulator session	The running session, when an application is started with the Workspace on an application server
Expect script	VISULOX PORTAL connection script started during the launch of an application
External DNS name	The name by which an VISULOX PORTAL Server is known to a client device. A VISULOX PORTAL Server can have multiple external DNS names.

File Exchange	File Transfer web access for transferring files between a client and the Transit Zone for users without access to the VISULOX PORTAL
File Transfer Client	VISULOX Component for transferring files securely from Transit Zone to application servers and back
Film	Summary of the recorded chapters
Forced authentication	When VISULOX PORTAL prompts for a user name or password, by displaying an authentication dialog box For example, if a user holds down the Shift key when clicking on an application's link on the Workspace
FQDN	**F**ully **Q**ualified **D**omain **N**ame - The full name of a system, containing its hostname and its domain name. For example: portal.visulox.com, where portal is the hostname of a server, and visulox.com is the domain name
Group Access	Group Access is used to define an Access Policy for a specific list of users. This is needed when users are working together in a project and the project is represented by a group object in the repository
Host object	Host objects can be assigned to File Transit, Command Guard and Command Connect groups.
Host Connect	See: **VISULOX Command Connect / VISULOX Command Guard**
IAR	**I**ntelligent **A**rray **R**outing
ICA	**I**ndependent **C**omputing **A**rchitecture: Client communication protocol from Citrix
Integrity-Check	Tool to check the VISULOX components and services
Internal / external message	The VISULOX Service supplies an external message for the login page and an internal message for the user's Workspace

Kiosk mode	VISULOX PORTAL display mode, where an application is displayed in full-screen
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
LDAPS	**L**ightweight **D**irectory **A**ccess **P**rotocol over **S**SL. Used for secure connections to an LDAP directory.
LID	Short form for **L**icense **ID** - Contains the date, the license started
Management Console	See: **VISULOX Cockpit**
MFA	**M**ulti **F**actor **A**uthentication
Native Client	A VISULOX PORTAL component that can be installed on client devices. The client maintains communication with the VISULOX PORTAL Server and is required to run applications The Native Client is provided by Oracle.
NEP	Short form for **N**etwork **E**ntry **P**oint
Network Entry Point	See: **RIP**
NFS	**N**etwork **F**ile **S**ystem
Notifications	Implemented notification system for access, Workspace / File Transfer and emulator sessions in the VISULOX Services
Object	A self-contained entity, defined by a number of attributes and values. VISULOX PORTAL Objects have different types, such as an X application. The available attributes for each type are defined by a schema

One Time Passcode	The One Time Passcode is used for authentication and will become invalid after usage. A provided OTP is based on a secret key and the time via a smartphone APP
Organization object	A VISULOX PORTAL Object used to represent the top level of an organizational hierarchy. Organization objects can contain **OU=** or user profile objects. Organization objects have an **O=** naming attribute.
Organizational hierarchy	The collection of objects in the VISULOX PORTAL Datastore, descending from one or more organization or domain component objects. Represents the collection of people, application servers, and applications within an organization.
Organizational unit object	A VISULOX PORTAL Object used to distinguish different departments, sites, or teams in an organizational hierarchy. Organizational unit (**OU**) objects can be contained in an organization or domain component object. Organizational unit objects have an **OU=** naming attribute
OTP	Short form for **O**ne **T**ime **P**asscode
Peer DNS name	The name by which an VISULOX PORTAL Server is known to other VISULOX PORTAL Servers in the same array
Primary server	The VISULOX PORTAL Server that acts as the authoritative source for global information, and maintains the definitive copy of the VISULOX PORTAL Datastore
RDP	**R**emote **D**esktop **P**rotocol: Client communication protocol from Microsoft
Remote IP	Remote IP address, the information, from where a client request is coming
Report	The VISULOX Service is collecting data about workspacesessions, emulatorsessions, recordings and cooperations. The information can be clearly arranged in reports. In VISULOX Cockpit a variety of possible reports can be created on several pages

Resume	To redisplay an application session that has been suspended. See also: **suspend**
RIP	Short form for **R**emote **IP** address
RVA	**R**emote **V**endor **A**ccess
S & M	Short form for **S**upport and **M**aintenance
Secondary server	An array member that is not the primary server. The primary server replicates information to secondary servers.
Session	The VISULOX PORTAL generates a session for any X11 or RDP application, which has an unique session ID
SIEM	**S**ecurity **I**nformation and **E**vent **M**anagement
SOX	Short form for **S**arbanes-**O**xley **A**ct
SSL certificate	A digital passport that establishes credentials on the web. In VISULOX PORTAL Service, allows client devices to trust the identity of a VISULOX PORTAL Server
Suspend	To pause an application session. A suspended application is not closed, it can be resumed. See also: **resume**
TAP	Short form for **T**emporary **A**ccess **P**IN, part of the Multi Factor Authentication (MFA)
TCC	Short form for **T**arantella **C**lient **C**omponent: Component for login into the VISULOX PORTAL via **Native Client**
TCL	Programming Language. Most of the VISULOX products are based on TCL

Temporary Access PIN	VISULOX method for the Multi Factor Authentication (**MFA**)
TFN	Tarantella Full Naming, X.500 format to address a VISULOX PORTAL object
Transit Zone	Zone, where files are transferred from/to application servers/clients
VAP	Short form for **V**irtual **A**ccess **P**oint
Virtual Access Point	VISULOX method to get an independent URL of the VISULOX Access Nodes for reliability and Workspace balancing
VISULOX Access Node	Node running the VISULOX PORTAL Service and the VISULOX Service
VISULOX Base	Single VISULOX Node
VISULOX Cluster	Two or more VISULOX Nodes, that are joined together because of scalability, redundancy and load balancing
VISULOX Cockpit	Central VISULOX application to control sessions, access, recording, cooperations and to generate reports
VISULOX Command Connect	VISULOX component, which provides the possibility to connect to multiple hosts and to open an X-Client on these hosts. The connection method can be SSH, RDP or telnet. Former: **Host Connect**
VISULOX Command Guard	VISULOX component, which provides the possibility to connect to multiple hosts and to open an X-Client on these hosts Command Guard has command level controls for the application. It allows and denies the usage of certain commands by the user Additionally server side scripts can be issued either to multiple endpoints or to a single one

VISULOX Common Access Platform	The whole environment, that is built with the VISULOX GATEWAY, VISULOX Portal Service, VISULOX Service and databases
VISULOX Data	VISULOX Database and VISULOX Filestore
VISULOX Filestore	File system which stores the films. 5 MByte per user and per hour. Recommended for VISULOX is a local disk with 150-250 GB, for VISULOX Archive Node depending on the lifetime of films, up to x TB on a NAS/SAN storage
VISULOX GATEWAY	The VISULOX GATEWAY is a proxy server designed to be deployed in front of a VISULOX PORTAL Array in a demilitarized zone (DMZ). This enables the VISULOX PORTAL Array to be located on the internal network of an organization. Additionally, all connections can be authenticated in the DMZ before any connections are made to the VISULOX PORTAL servers in the array. The VISULOX GATEWAY manages load balancing of HTTP connections for the VISULOX PORTAL Servers in the array.
VISULOX Host Connect	See: **VISULOX Command Connect**
VISULOX Hotfix	Tool to check the software status in the cluster, backup and apply hotfixes
VISULOX keystroke recording with analyzing engine	In this recording mode all user keyboard interactions are registered and can be checked for unwanted entries (analyzing engine)
VISULOX Node	Node running the VISULOX Service to control sessions, films and recorders
VISULOX PAM	**VISULOX P**rivileged **A**ccess **M**anagement
VISULOX PORTAL Array	Two or more VISULOX Access Nodes, that are joined together because of scalability, redundancy and load balancing

VISULOX PORTAL Benchmark	Tool to create a defined number of demo-users, who log into the VISULOX PORTAL and start recorded applications automatically. All settings can be configured easily within a GUI
VISULOX PORTAL Console	Web-based management console for the VISULOX PORTAL Service (Former: Administration Console)
VISULOX PORTAL Web Server	A pre-built web server installed and configured along with the VISULOX PORTAL Service, contains Apache, mod_ssl for HTTPS support, and Tomcat for Java Servlet and JSP support
VISULOX PORTAL Web Services	An API collection that allows developers to build their own applications to work with the VISULOX PORTAL Service. The APIs can be used to authenticate users, launch applications, and interact with the VISULOX PORTAL Datastore
VISULOX Revision Server	VISULOX Node which replicates the production database into Revision Server database and transfers the films from the production filestore into the Revision Server filestore (also known as Archive Server)
VISULOX Service Group	See: **VISULOX Cluster**
VISULOX Short Support Report	A Short Support Report to send via eMail created with **visulox support -info**. The Short Support Report should be sent to the VISULOX Support Team every time a new Support Request is opened
VISULOX Support Report	Package generated by the **visulox support** command, containing all information, necessary for support
VISULOX Transit Area	File Transfer component embedded in the Workspace to transfer files between client and Transit Zone
VISULOX Transit Mapping	To setup the VISULOX Transit Zone on Unix application servers, that are not a VISULOX Node, an RPM file is available for installation.
VISULOX Videolog Player	Player to view the recorded films inside the VISULOX Cockpit or checked out films in a browser

VISULOX Webservice User	Each VISULOX Service needs this user in the datastore to read the webservices on the VISULOX Access Nodes. The VISULOX webservice user has to be setup once in the datastore
VISULOX_Setup.xls	Excel-sheet, which has to be filled out in the planning phase by the responsible project leader, together with the amitego consultant
vlxMode	VISULOX variable set in the VISULOX PORTAL Console
VLX Password SelfService	Active Directory (AD) and Oracle Unified Directory (OUD) users are able to change their password by themselves with this appliction assigned.
Webtop	In the current version, the Webtop is called the **Workspace**. A Workspace is the term used to describe a user's applications, documents, and desktops. See: **Workspace**
WM	Short form for **W**indow **M**anager
Workspace	The Workspace is displayed after logging into the VISULOX PORTAL. It is a special web page, that lists the applications that are assigned to the user
Workspace balancing	VISULOX load balancing mechanism including a virtual access point
Workspace session	The running session, after a user has logged into the VISULOX PORTAL via browser or Native Client
X11 forwarding	The process of forwarding, or tunneling, the windows of a remotely started X application to a client desktop
X Window System	A distributed window system for UNIX platform operating systems, based on the X11 protocol. Also called X11, or X Windows
X.509 certificate	See: **SSL certificate**