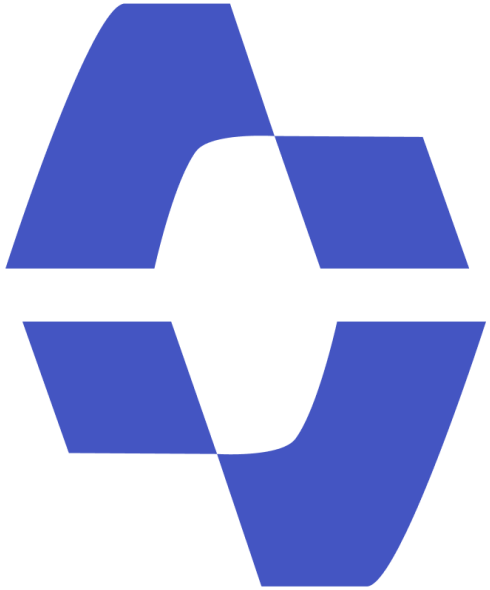


VISULOX 5

Installation Guide

14.08.2026

visulox

Table of Contents

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 Installation Guide** provides information about installation, configuration, upgrading and removing of this version of Visulox. Instructions on how to get started using Visulox is also provided. This document is intended for consultants and system administrators.

1.1 How this manual is organized

Preface
Requirements
Installing Visulox
Installing Visulox Cluster
Multi-Gateway Setup Guide
Updating Visulox
Visulox Hotfix (Core)
Uninstalling Visulox
Visulox License Agreement
Visulox Session Cookies

Troubleshooting & Glossary

1.2 Legend

Useful information

Recommended setting

Warning / use with caution

Tipps & tricks

1.3 Visulox documentation

Application	Title	Format
Release Notes	*Release Notes* *Platform Support and Release Notes*	HTML
Installation	*Installation Guide* *Installation / Update Guide*	HTML
Administration	*Admin Guide - VLX Portal* *Admin Guide - VLX Core* *Administration Guide*	HTML

Application	Title	Format
User	*User Guide* *User Guide*	HTML

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

1.4 Documentation feedback

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

2 Requirements

2.1 General

- Server requirements:
  - Visulox Portal Master: 2 Core CPU, 4GB RAM (8GB is recommended)
  - Visulox Gateway: 2 Core CPU, 2 GB RAM
  - Visulox Core: 2 Core CPU, 4 GB RAM (6GB is recommended)
- The recommended platform is **Oracle Linux / Red Hat 9.8** (for other versions contact amitego) with at least 10Gbyte for the OS and 30Gbyte for Visulox free space on the hard disc (small installation)
- The **/opt** directory must NOT be mounted with **-nosuid** parameter
- Visulox can be vitualized, the disk must NOT have "**Thin provisioning**" enabled
- **umask 022** is needed for installation and start of the Visulox Portal Service
- Symbolic links are not supported
- The recommended Visulox version is the latest Visulox 5 release
- The recommended user repositories are all repositories, that are supported by Visulox Portal Service
- Firewall configured properly or disabled
- /etc/hosts should look like: 127.0.0.1 localhost localhost.localdomain
- The nginx connection to Portal and Gateway needs DNS. With no DNS and only entries in /etc/hosts it is not working. Without DNS it is possible to install/enable **dnsmasq** and register 127.0.0.1 in nginx resolver.
- NTP **or** Chrony enabled
- For ports, see: Network communication within Visulox

⚠ Make sure that correct hostnames are used for the servers in the environment.
Hostnames **must not** contain underscores (because of RFC 952 and domain names with underscores)!
The FQDN of the host **must not** exceed 50 characters!
Capital letters **must not** be used in hostnames!
Changing hostnames after installation of Visulox **is not** supported!

2.2 Required packages

Choose the **minimal installation** without GUI for the base environment.

> The basic installation contains all necessary software for Visulox . Additional software should not be installed on a Visulox server.
> Runlevel 3 multi-user target is recommended.

> The recommended OS is **Oracle Linux 9.8**. As an alternative Red Hat Linux could be used,
> which will possibly need some other packages as listed here. See also: Installation Guide (Server Preparation OL9.8 / RHEL9.8)
> For other OS versions please contact amitego.

> At least **XPRA** version **6.5.2** is needed on the portal servers. With dnf update the latest version will be installed.

2.3 Additional libraries needed for Visulox on Oracle Linux 9.8

Installing Visulox on Linux platforms, the yum / dnf command has to be used to ensure that any package dependencies are resolved automatically.
This means that yum must be configured to use a suitable Linux package repository.

Make sure that **ol9_baseos_latest, ol9_appstream, ol9_codeready_builder, xpra** and **ol9_developer_epel** are in yum repolist as well.

```
dnf repolist
Repository ol9_appstream is listed more than once in the configuration
repo id                                                             repo name
ol9_UEKR7                                                           Oracle Linux 9 UEK Release 7 (x86_64)
ol9_appstream                                                       Oracle Linux 9 Application Stream (x86_64)
ol9_baseos_latest                                                   Oracle Linux 9 BaseOS Latest (x86_64)
ol9_codeready_builder                                               Oracle Linux 9 CodeReady Builder (x86_64) - (Unsupported)
ol9_developer_EPEL                                                  Oracle Linux 9 EPEL Packages for Development (x86_64)
xpra                                                                Xpra Repository for Oracle Linux 9
```

> ⚠ `xpra --version` must be equal to or greater than **xpra v6.5.2**

yum update is recommended before installing the new packages!

2.4 Disk layout

The platform disk layout can be as usual. We recommend at least 10 Gbyte for the OS,

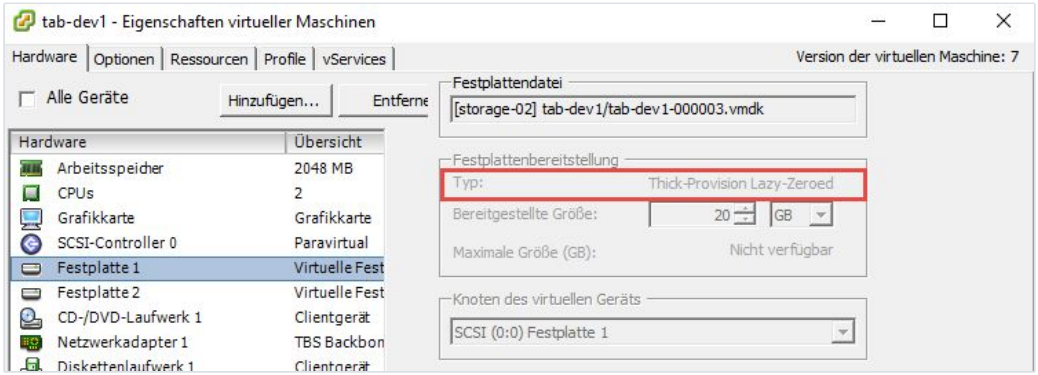
Further we recommend to have a partition of 30Gbyte under **/opt** (60 Gbyte with Archive) in a small environment.

For a large environment we recommend to have at least 50Gbyte under **/opt/visulox** (100Gbyte with Archive).

An additional partition for File store is also recommended, which is mounted under **/opt/visulox/data/filestore/0**.

⚠ VISULOX can be vitualized, the disk must NOT have "**Thin provisioning**" enabled.
See also: How to use VISULOX on virtualized VMWare disks, VISULOX disk space protection

⚠ The **/opt** directory must NOT be mounted with **-nosuid** parameter.



- Diskspace for the Postgresql database on Visulox Portal servers should be at least 25GB.
- Diskspace of VLX_DATADIR must have at least 2.5 of size of the database available because VACUUM creates a copy of the database.
  For example: a 4GB database needs 6 GB free diskspace. The diskspace is checked with integrity check.

2.5 Platform modification during installation

2.5.1 Visulox Service

The default Visulox installation directory is **/opt/visulox**.
The default Visulox Portal installation directories are **/opt/visulox-portal, /opt/visulox-portal**-rte, **/opt/visulox-connector, /opt/xpra-visulox.**

On group `vlxgroup` is generated on startup

On default 102 users are generated in for follwoing sequence: VISULOX user (`vlx`), VISULOX webservice user (`vlxwebservice`) and 100 Jump Users (`vlx000 .. vlx099`).

The users can be removed and recreated with an admin command by and a new start UID can be applied.

During Visulox Service installation the following users and groups are created:

Primary Visulox user and group

```
vlx:x:503:503:VISULOX user:/opt/visulox:/bin/bash
```

⚠ The vlxgroup **must** be a local group!

On every Visulox Access Node, the Visulox Service is attached to the Visulox Portal Service and the webservice user is created with:

```
visulox portal attach
```

Visulox Portal connection user

```
vlxwebservice:x:610:500:VISULOX Admin User in VISULOX PORTAL:/opt/visulox/var/vlxwebservice:/sbin/nologin
```

If the webservice user should be created with a given name and UID on a VISULOX Access Node, the following parameters have to be adjusted:

```
visulox config -name portal.admin
    ------------------------------------------------
    | changed | key               | value         |
    ------------------------------------------------
    |         | portal.admin.uid  | 610           |
    |         | portal.admin.user | vlxwebservice |
    ------------------------------------------------
```

This Visulox webservice user is created with an unknown password that never expires and **cannot** be modified!

100 Visulox jump users

```
vlx000:x:<next available user id>:503:Visulox transit user:/opt/visulox/users/vlx000:/bin/bash
...
vlx099:x:<next available user id>+100:503:Visulox transit user:/opt/visulox/users/vlx099:/bin/bash
```

The group is the same of the vlx user. The Visulox group

A Visulox PID is generated on each Visulox Node. This **vlxpid** is always **vlxgroup+1.**

During VISULOX Service installation, the set-user-id bit is set on the following binaries:

```
-r-sr-xr-x 1 root vlxgroup  18760 Sep 17 14:14 vlxchown
-r-sr-xr-x 1 root vlxgroup  38007 Sep 17 14:14 vlxsu
-r-sr-xr-x 1 root vlxgroup  16276 Sep 17 14:14 vlxsudo
```

Code for security review is available on request.

A file with the maximum number of processes and opened files for the vlx group is added: **/etc/security/limits.d/90_visulox.conf**

```
@vlx hard nproc 16000
@vlx soft nproc  4000
@vlx hard nofile 8000
@vlx soft nofile 2000
```

During setup, a log rotation entry for Visulox is added: **/etc/logrotate.d/visulox**

2.6 Optional enhancements

2.6.1 Visulox addons

The following VISULOX addons can be used, if the according packages are installed on the server:

2.6.2 Visulox Firefox

Firefox

```
yum install firefox
```

2.6.3 Visulox VNC

VNC Viewer

```
yum install tigervnc
```

2.6.4 Telnet

Telnet

```
 yum install telnet
```

2.6.5 Checksum in File Transfer

To display the checksum of transferred files in the Visulox Transit Area in the user's Workspace it is necessary to install **rhash**, which is available in the Epel repository.

3 Installing Visulox

This document describes the installation and setup procedure for the following components on a single Linux server:

- Visulox RTE (Portal & Core)
- Visulox Core
- Visulox Portal
- Visulox Connector
- Visulox Clients on the server side

During the Visulox Portal setup (`setup-master`), connections to Microsoft Entra, LDAP, and Active Directory can be configured.

This guide is primarily intended for:

- internal testing
- staging environments
- controlled production deployments

	• Bonus 2: Portal Configuration Modification After Installation • Bonus 3: Native Client - Supported Operating Systems & Installation

3.1 1. Prerequisites

3.1.1 1.1 RPMs

- **Visulox Portal RPMs**: vlx-portal-rte-5.0.2.el9.x86_64.rpm, vlx-portal-5.0.2.el9.x86_64.rpm, vlx-connector-5.0.2.el9.x86_64.rpm
- **Visulox Core RPMs**: visulox-rte-1.2.0-1.el9.x86_64.rpm, vlx-core-5.0.2.el9.x86_64.rpm

RPMs can be downloaded from Download Links.

3.1.2 1.2 PostgreSQL & KeyDB

During the interactive `setup-master` process, Visulox can automatically install and configure PostgreSQL and KeyDB.

Alternatively, you may install and configure these services manually before running setup.

If you choose manual installation, refer to:

PostgreSQL 16 Installation and Setup for Visulox
PostgreSQL Installation and Setup for Visulox on RHEL / Oracle Linux 9

KeyDB Installation and Setup for Visulox
KeyDB Installation and Setup for Visulox on RHEL / Oracle Linux 9

Both approaches are supported.

3.1.3 1.3 Time Synchronization (Mandatory)

⚠ Critical Requirement

The server system time must be correct and synchronized before running:

- `visulox start`
- `setup-master`
- Any Docker-based service initialization (e.g. PostgreSQL container)

Incorrect system time can cause:

- TLS certificate validation failures
- Docker image pull errors
- PostgreSQL container startup failure
- setup-master interruptions

Example failure:

```
tls: failed to verify certificate: x509: certificate has expired or is not yet valid
current time 2026-02-16T14:04:39+01:00 is before 2026-02-19T20:57:44Z
```

Check and synchronize:

```
REMOTE_TIME=$(curl -kfsSI https://www.google.com | awk -F': ' '/^[Dd]ate:/{print $2}' | tr -d '\r')
echo "$REMOTE_TIME"
sudo date -s "$REMOTE_TIME"
sudo hwclock --systohc
```

3.1.4 1.4 Connect to Server (once)

Run from your client:

```
ssh -p 22 <SERVER_USER>@<SERVER_HOST>
```

3.2 2. Server Preparation

This steps vary based on OS.

- For Oracle 9.8 run:

```
# 1. Install the official EPEL release package
sudo dnf install -y oracle-epel-release-el9

# 2. Add the official Xpra repo
sudo tee /etc/yum.repos.d/xpra.repo >/dev/null <<EOF
[xpra]
name=Xpra Repository for Oracle Linux 9
baseurl=https://xpra.org/stable/oraclelinux/9/x86_64/
enabled=1
gpgcheck=0
EOF

# 3. Add EXCLUDES to AppStream and EPEL via setopt
# This modifies the existing repo files instead of creating duplicates
sudo dnf config-manager --setopt="ol9_appstream.exclude=xpra*" --save
sudo dnf config-manager --setopt="ol9_developer_EPEL.exclude=xpra*" --save

# 4. Enable all required channels
sudo dnf config-manager --set-enabled ol9_appstream
sudo dnf config-manager --set-enabled ol9_developer_EPEL
sudo dnf config-manager --set-enabled ol9_codeready_builder
```

- For RHEL 9.8 run:

⚠ If you installed RHEL directly from the official Red Hat ISO image, you need to activate the Red Hat account/subscription before using online repositories, so that you can access the online resources. (Of course, you can also use a local repo -**RHEL DVD ISO as local repo**-, but to use the online repositories, follow the method below)

```
sudo subscription-manager register
```

and then:

```
sudo subscription-manager repos --enable=rhel-9-for-x86_64-baseos-rpms
sudo subscription-manager repos --enable=rhel-9-for-x86_64-appstream-rpms
```

```
# 0. Install config-manager if needed
sudo dnf install -y dnf-plugins-core

# 1. Enable RHEL CodeReady Builder repository. Change $(arch) based on your CPU architecture.
sudo subscription-manager repos --enable codeready-builder-for-rhel-9-$(arch)-rpms
# sudo subscription-manager repos --enable codeready-builder-for-rhel-9-x86_64-rpms

# 2. Install official EPEL release package for RHEL 9
sudo dnf install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm

# 3. Add the official Xpra repo for RHEL 9
sudo tee /etc/yum.repos.d/xpra.repo >/dev/null <<'EOF'
[xpra]
name=Xpra Repository for RHEL 9
baseurl=https://xpra.org/dists/RedHat/9/x86_64/
enabled=1
gpgcheck=0
EOF

# 4. Exclude xpra packages from AppStream and EPEL
# On RHEL the repo IDs are normally: rhel-9-for-x86_64-appstream-rpms and epel
sudo dnf config-manager --setopt="rhel-9-for-x86_64-appstream-rpms.exclude=xpra*" --save
sudo dnf config-manager --setopt="epel.exclude=xpra*" --save

# 5. Clean metadata
```

```
sudo dnf clean all
sudo dnf makecache

# 6. Check which xpra-common package will be selected
dnf info xpra-common
```

It is a good idea to use **dnf update** on the servers to get the latest packages before continuing with the setup.

3.3 3. Create Temporary Folders on Server

3.3.1 3.1 Clean-up old installation (if needed)

```
# Step 1: Uninstall any existing packages
sudo dnf remove vlx-connector vlx-portal vlx-portal-rte visulox-rte -y || true
sudo rm -rf /opt/visulox-portal* || true
sudo rm -rf /var/vlx-portal || true
sudo rm -rf /opt/visulox || true
sudo rm -f /opt/visulox-portal/.setup_done || true
sudo systemctl daemon-reload || true
```

3.3.2 3.2 Create temporary folders

```
rm -rf /tmp/vlx-core /tmp/vlx-portal || true && mkdir -p /tmp/vlx-core /tmp/vlx-portal
```

3.4 4. Visulox Core

3.4.1 4.1 Copy files to the vlx-core folder

```
- vlx-core-5.0.2.el9.x86_64.rpm
- visulox-rte-1.2.0-1.el9.x86_64.rpm
```

3.4.2 4.2 Install & Configure VISULOX Core

Install & configure Visulox Core:

```
cd /tmp/vlx-core
sudo dnf install -y visulox-*.rpm
sudo dnf install -y vlx-*.rpm
```

Start Visulox Core services:

```
sudo visulox start
```

3.5 5 Visulox Portal / Connector

3.5.1 5.1 Copy files to the vlx-portal folder

```
- vlx-portal-rte-5.0.2.el9.x86_64.rpm
- vlx-portal-5.0.2.el9.x86_64.rpm
```

```
- vlx-connector-5.0.2.el9.x86_64.rpm
```

3.5.2 5.2 Install & Setup Visulox Portal

Step 1 – Install RPM Packages

```
cd /tmp/vlx-portal
sudo dnf install vlx-portal-rte-*.rpm -y
sudo dnf install vlx-portal-*.rpm -y
sudo dnf install vlx-connector-*.rpm -y
```

Step 2 – Run Setup (Interactive)

Interactive Mode

`setup-master` interactively installs and configures IPs, host names, admin user, the main system components, such as the database and KeyDB. It also allows you to configure connections to Microsoft Entra, LDAP, and Active Directory. Most of these items can be modified later.

```
sudo /opt/visulox-portal/bin/vlx-portald setup-master
```

Optional: Running Setup (Non-interactive)

In some cases, you may not want to enter the inputs of the `setup-master` command interactively. For example, if you are writing a script, you need to run this command in a non-interactive mode to have control over the inputs.
To do so, you need to create template files for the setup command to run. Run the following command:

```
sudo /opt/visulox-portal/bin/vlx-portald setup-master --get-template /tmp/vlx-portal
```

After running the above command, a `setup_template.json` template file and a `setup_template_README.txt` file will be created in the `/tmp/vlx-portal` directory.
An example of a default-generated template file looks like this:

```
{
  "CurrentServerIP": "",
  "CurrentServerHost": "",
  "GatewayAddress": "",
  "GatewayPort": 8180,
  "RestAPIPort": 8080,
  "SOAPAPIPort": 8090,
  "MetricAPIPort": 9000,
  "ConnectorAPIPort": 8085,
  "ServerRegion": "default",
  "NGINXResolverIPs": [
    "172.17.3.1"
  ],
  "InstallPostgreSQL": true,
  "NewPostgreSQLConfig": {
    "Host": "",
    "Port": 5432,
    "User": "",
    "Password": "",
    "Database": "visuloxdb",
    "Secure": false,
    "InsecureSkipVerify": true,
    "CACertPath": "",
    "ClientCertPath": "",
    "ClientKeyPath": ""
  },
  "ExistPostgreSQLConfig": {
    "Host": "",
    "Port": 0,
    "User": "",
```

```
    "Password": "",
    "Database": "",
    "Secure": false,
    "InsecureSkipVerify": false,
    "CACertPath": "",
    "ClientCertPath": "",
    "ClientKeyPath": ""
  },
  "InstallKeyDB": true,
  "NewKeyDBConfig": {
    "Host": "",
    "Port": 6379,
    "User": "",
    "Password": "",
    "Database": "",
    "Secure": false,
    "InsecureSkipVerify": true,
    "CACertPath": "",
    "ClientCertPath": "",
    "ClientKeyPath": ""
  },
  "ExistKeyDBConfig": {
    "Host": "",
    "Port": 0,
    "User": "",
    "Password": "",
    "Database": "",
    "Secure": false,
    "InsecureSkipVerify": false,
    "CACertPath": "",
    "ClientCertPath": "",
    "ClientKeyPath": ""
  },
  "ConnectToLDAP": false,
```

```
  "LDAPConfig": {
    "enabled": false,
    "server_host": "",
    "server_port": 0,
    "admin_user": "",
    "admin_password": "",
    "use_tls": false,
    "insecure_skip_verify": false,
    "base_dn": "",
    "ldap_user_filter": ""
  },
  "ConnectToAD": false,
  "ADConfig": {
    "enabled": false,
    "server_host": "",
    "server_port": 0,
    "admin_user": "",
    "admin_password": "",
    "use_tls": false,
    "insecure_skip_verify": false,
    "base_dn": "",
    "ldap_user_filter": ""
  },
  "EntraLoginActive": false,
  "AzureTenantID": "",
  "AzureExpectedAUD": "",
  "AzureClientSecretID": "",
  "AzureCookieSecret": "",
  "Loki": {
    "Enabled": false,
    "URL": "",
    "TenantID": "",
    "AuthToken": "",
    "ServiceName": "vlx-portal",
```

```
    "HostLabel": "",
    "QueueSize": 5000,
    "BatchSize": 200,
    "FlushIntervalMS": 1000,
    "RequestTimeoutMS": 3000,
    "MaxRetries": 4,
    "InitialBackoffMS": 200,
    "MaxBackoffMS": 2000,
    "DropWhenQueueFull": true
  },
  "AdministratorUser": "root",
  "DefaultOtherProfileUsername": "vlx-default-user"
}
```

You need to fill in the required items of this template file by reading the README file. Then, consider you have prepared a setup JSON file using the template file named `setup.json`; You can run the `setup master` command non-interactively as follows:

```
sudo /opt/visulox-portal/bin/vlx-portald setup-master --file /path/to/setup.json
```

⚠ Regarding the `ExistKeyDBConfig.DBCACertPath`, `ExistKeyDBConfig.ClientCertPath`, and `ExistKeyDBConfig.DBClientKeyPath` configs, you only have to set them if your keydb is installed before, and it uses a TLS connection using a “self-signed” certificate. If your keydb certificates are not self-signed, leave these fields empty.
The same way, regarding `ExistPostgreSQLConfig.CACertPath`, `ExistPostgreSQLConfig.ClientCertPath`, and `ExistPostgreSQLConfig.ClientKeyPath` you have to set all of them if you have a self-signed cert and want to have `full-verification`.

Regarding PostgreSQL, if you are using a pre-installed instance, you should have an empty database named `visuloxdb`. The user you create must have full access to this database. For example, suppose you want to create a user with the username `visulox` and the password `your_secure_password`, and then create a database named `visuloxdb`. Make sure that the `visulox` user is granted all necessary privileges on this database, as shown below:

```
CREATE DATABASE visuloxdb;
```

```
CREATE USER visulox WITH PASSWORD 'your_password';

GRANT ALL PRIVILEGES ON DATABASE visuloxdb TO visulox;

ALTER DATABASE visuloxdb OWNER TO visulox;

\c visuloxdb

GRANT ALL ON SCHEMA public TO visulox;
ALTER SCHEMA public OWNER TO visulox;
```

LDAP/Active Directory integration

To integrate LDAP or Active Directory on this server, enter their addresses during interactive setup master mode or in the config file during non-interactive setup master mode.

Step 3 - Attach Portal

Run on the server:

```
sudo visulox portal attach -proxy
```

3.6 6. Providing the Visulox Client files on the Portal Server

3.6.1 6.1 Overview

This page covers how to install, update, and remove the **vlx-clients** RPM package on a target server.

3.6.2 6.2 Prerequisites

- **NGINX** must be installed — it is a required dependency of the RPM.

- The target system must be running RHEL/Rocky Linux 9 (el9, x86_64).

3.6.3 6.3 Installation

```
sudo dnf install vlx-clients-*.el9.x86_64.rpm
```

On install the RPM:

1. Creates `/etc/nginx/html/vlx/client/`
2. Copies all client files there
3. Runs `systemctl reload nginx`

Files are then served at `https://<host>/client/` via NGINX.

3.6.4 6.4 Update

```
sudo dnf update vlx-clients-*.el9.x86_64.rpm
```

Replaces client files in `/etc/nginx/html/vlx/client/` and reloads nginx. The NGINX rule is not changed.

3.6.5 6.5 Uninstall

```
sudo dnf remove vlx-clients
```

Removes all files from `/etc/nginx/html/vlx/client/` and reloads nginx.

> After installing the Visulox client files on the server, the client files are available for download via the login page (Install the client link) for users.

3.7 7. Reinstall XPRA Web Components (Optional)

> ⚠ This step is not necessary unless the XPRA version is incorrect (`xpra --version` must be equal to or greater than `xpra v6.5.2-r0) otherwise you may receive a 404 error when starting XPRA on the web or an issue with keyboard mapping can occur in applications.

In some cases, the XPRA **HTML5 / Web** components may not be installed correctly during the initial installation.

3.7.1 Step 1 – XPRA Components Installation

To ensure all required XPRA components are properly installed, run the following command:

```
dnf reinstall -y xpra-html5 xpra-common xpra-server
```

3.7.2 Step 2 – Verify XPRA Installation

Verify that XPRA is installed and accessible by checking its version:

```
xpra --version
```

If the command returns a version number, XPRA has been installed successfully.

```
xpra --version
xpra v6.5.2-r0R
```

3.8 8. Process Check

Run on the server:

```
ps auxwwf | grep "vlx\|visulox\|opt" | grep -v "ps auxwwf"
```

3.9 Bonus 1: Change Log Level to Debug

Portal:

```
vi /opt/visulox-portal/configs/config.json
# Change Logger.Level to "debug"
# Set `ExtraFilePath` to `/var/log/visulox-portal/portal.log`.

chown vlx:vlxgroup /var/log/visulox-portal/portal.log
chmod 777 /var/log/visulox-portal/portal.log
```

Connector:

```
vi /opt/visulox-portal-connector/configs/config.json
# Change Logger.Level to "debug"
# Set `ExtraFilePath` to `/var/log/visulox-portal-connector/connector.log`.
```

Restart services:

```
sudo visulox restart

systemctl restart vlx-portal
systemctl status vlx-portal

systemctl restart vlx-connector
systemctl status vlx-connector
```

Logs:

```
# Portal:
tail -f /var/log/visulox-portal/portal.log

# Connector:
tail -f /var/log/visulox-portal-connector/connector.log
```

3.10 Bonus 2: Portal Configuration Modification After Installation

To change the configuration provided during the setup, update the following config file:

```
/opt/visulox-portal/configs/config.json
```

Then restart the `vlx-portal` service:

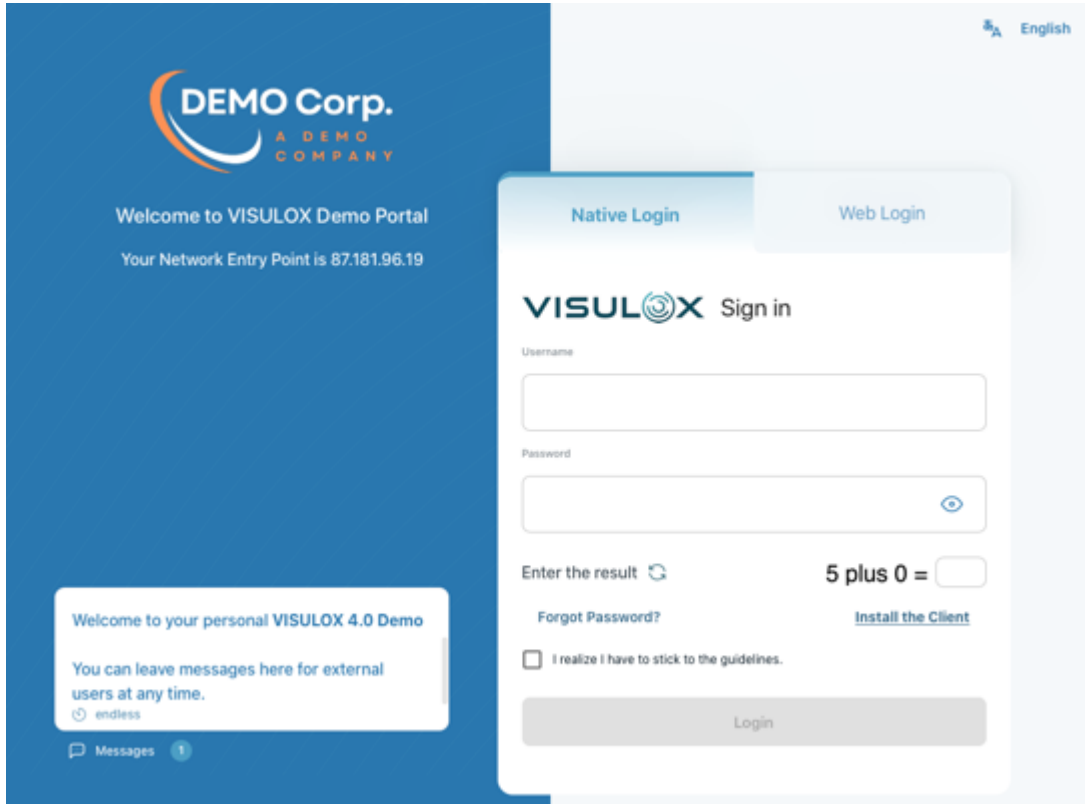
```
systemctl restart vlx-portal
```

Note: Make sure you know what you are doing before making any changes. Keep a backup of the configuration file before modifying it.

3.11 Bonus 3: Native Client - Supported Operating Systems & Installation

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

Login screen:



Choose "**Install the client**" link before the first login and download the client file.

> It is also possible to choose "**Web Login**" to use the HTML5 Client.

OS	Installation Steps

macOS	1. Open the `.dmg` file to mount it. 2. Copy `VisuloxClient.app` to your `/Applications` folder. 3. Open `VisuloxClient.app` and click the **Install** button.
Windows	1. Open the `.exe` file. 2. Click **Install**.
Linux (Partially)	1. Open the file to launch the GUI. 2. Click **Install**. 3. **XPRA** must be installed manually (refer to the official XPRA documentation). 4. Configure the XPRA path in: `~/.config/visulox/config.yaml` . **Compatibility Note:** XPRA version **6.4.3** has been successfully tested on **Ubuntu 24.04 LTS (Noble)**.

Versions

Using the latest version delivered with Visulox is recommended.

3.12 KeyDB Installation and Setup for Visulox on RHEL / Oracle Linux 9

3.12.1 Overview

This document describes installing KeyDB on a standalone RHEL / Oracle Linux 9 system using the EPEL repository, as required by Visulox.

Result:

- KeyDB Version: **6.x** (from EPEL 9)
- Service: **keydb**
- Host: **127.0.0.1**

- Port: **6379**
- Configuration File: **/etc/keydb/keydb.conf**

KeyDB does not use usernames. Authentication is optional and password-based only.

3.12.2 1. Enable EPEL Repository

Install EPEL:

```
sudo dnf install -y epel-release
```

Enable and refresh metadata:

```
sudo dnf config-manager --set-enabled epel
sudo dnf makecache
```

3.12.3 2. Install KeyDB

```
sudo dnf install -y keydb
```

This installs:

- keydb-server
- keydb-cli
- default configuration
- systemd service unit

3.12.4 3. Enable and Start KeyDB Service

```
sudo systemctl enable --now keydb
```

Verify:

```
sudo systemctl status keydb
```

3.12.5 4. Verify Installation

Check version:

```
keydb-server --version
```

Check listening port:

```
sudo ss -lntp | grep 6379
```

Default values:

- Port: `6379`
- Bind: `127.0.0.1`
- Authentication: disabled

3.12.6 5. Optional: Configure Password Authentication (Recommended)

Edit configuration:

```
sudo vi /etc/keydb/keydb.conf
```

Set:

```
requirepass StrongPasswordHere
```

Restart KeyDB:

```
sudo systemctl restart keydb
```

Test:

```
keydb-cli
AUTH StrongPasswordHere
PING
```

Expected:

```
PONG
```

3.12.7 Final Connection Values for Visulox

KeyDB does not use usernames. Leave the username field empty if prompted.

```
KeyDB Host: 127.0.0.1
KeyDB Port: 6379
KeyDB Username: (empty)
KeyDB Password: StrongPasswordHere   (only if configured)
```

3.13 PostgreSQL Installation and Setup for Visulox on RHEL / Oracle Linux 9

3.13.1 Overview

This document describes installing PostgreSQL 16 and preparing a standalone database for Visulox on RHEL / Oracle Linux 9, as required by the Visulox setup.

Result:

- PostgreSQL Version: **16**
- Service: **postgresql-16**
- Host: **127.0.0.1**
- Port: **5432**
- Application Database: **visuloxdb** (this is the exact database name required by Visulox setup)
- Application User: configurable (example: `visulox`)
- Required Extension Package: **postgresql16-contrib**

3.13.2 1. Enable PostgreSQL Repository

```
sudo dnf module enable postgresql:16
sudo dnf clean all
sudo dnf makecache
```

3.13.3 2. Install PostgreSQL

```
sudo dnf install -y postgresql-server postgresql postgresql-contrib
/usr/bin/postgresql-setup --initdb
```

Add a configuration parameter to authenticate via password.

/var/lib/pgsql/data/pg_hba.conf

```
# IPv4 local connections:
#host    all             all             127.0.0.1/32            ident
host    all             all             127.0.0.1/32            scram-sha-256
#For a VISULOX Cluster installation
host    all             all             0.0.0.0/0               scram-sha-256
# IPv6 local connections:
#host    all             all             ::1/128                 ident
host    all             all             ::1/128                 scram-sha-256
```

For a Visulox Cluster installation:

/var/lib/pgsql/data/postgresql.conf

```
# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
                                # comma-separated list of addresses;
                                # defaults to 'localhost'; use '*' for all
                                # (change requires restart)
```

3.13.4 3. Enable and Start PostgreSQL Service

```
sudo systemctl enable --now postgresql
```

Verify:

```
sudo systemctl status postgresql
```

3.13.5 4. Required Extension Package

Visulox migrations rely on `uuid-ossp`, which is provided by the contrib package.

Verify that the extension files exist:

```
ls -l /usr/pgsql-16/share/extension/uuid-ossp.control
```

3.13.6 5. Create Application User and Database

Login as postgres:

```
sudo -u postgres psql
```

Inside psql (replace `visulox` and password as needed):

```
-- Create application user (replace `visulox` with desired username)
CREATE USER visulox WITH PASSWORD 'StrongPasswordHere';

-- Create application database owned by that user
CREATE DATABASE visuloxdb OWNER visulox;

-- Ensure privileges
GRANT ALL PRIVILEGES ON DATABASE visuloxdb TO visulox;
\q
```

3.13.7 6. Verify Application Connection

(Replace `visulox` with your chosen username.)

```
psql -h 127.0.0.1 -U visulox -p 5432 -d visuloxdb -c "select 1;"
```

Expected:

```
1
```

3.13.8 7. Clean Database Reset (If Migrations Become Dirty)

If Visulox setup fails with:

```
Dirty database version XX
```

Reset the database (replace `visulox` with your chosen username):

```
sudo -u postgres dropdb visuloxdb
sudo -u postgres createdb -O visulox visuloxdb
```

Then re-run the Visulox setup master procedure.

3.13.9 Final Connection Values for Visulox

Use these in the installer (replace `visulox` as needed):

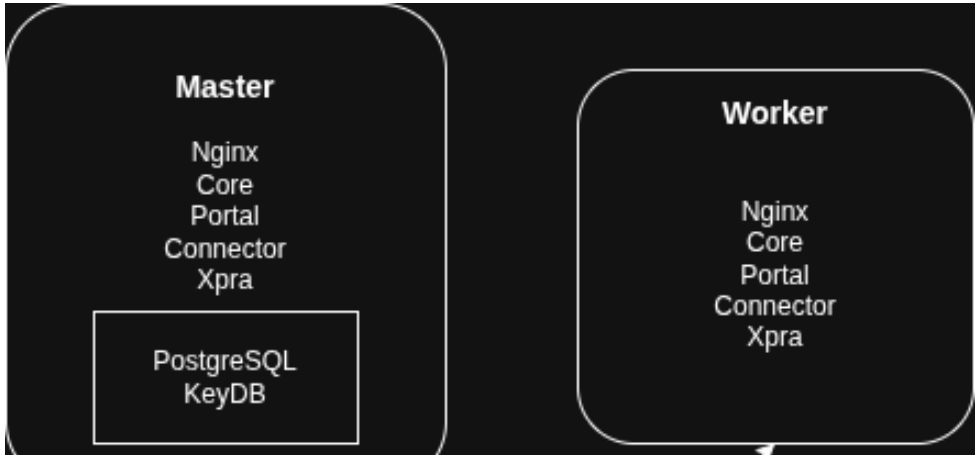
```
PostgreSQL Host: 127.0.0.1
```

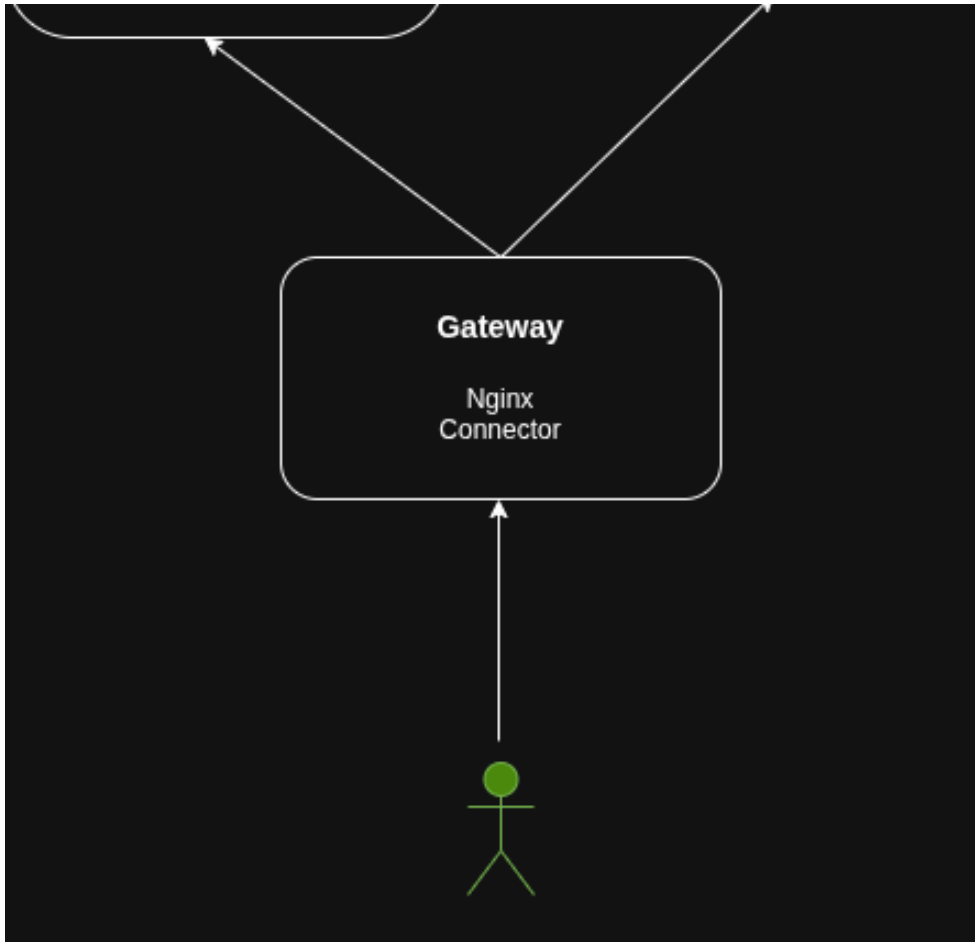
```
PostgreSQL Port: 5432
PostgreSQL User: visulox
PostgreSQL Password: StrongPasswordHere
Database Name: visuloxdb
```

4 Installing Visulox Cluster

This how-to explains how to design, provision, and validate a highly available Visulox Cluster consisting of Master, Gateway, and Worker nodes.

It covers prerequisites, recommended topologies, the cluster build process, health checks, scaling, and troubleshooting.




Gateway
Nginx
Connector

4.1 1. Introduction

This guide describes the process of provisioning and validating a highly available Visulox Cluster consisting of **Master, Gateway, and Worker nodes**. The setup follows a strict order, where each component depends on configuration and credentials created in earlier steps

4.2 2. Definitions

There are three types of server nodes in a Visulox Cluster, all served by NGINX installed on them:

4.2.1 Master

- Contains: Core, Portal, Connector
- Must be installed first
- Some Core logic runs only on the Master
- There can be only **one Master**

4.2.2 Gateway

- Contains: Connector
- Responsible for load balancing
- There can be **multiple Gateways**

4.2.3 Worker

- Contains: Core, Portal, Connector
- There can be **multiple Workers**

4.2.4 Core

- Core means the Visulox Core application. That's the amitego legacy app written in TCL language.

4.2.5 Portal

- Portal is the newly developed Visulox application written in Go. It includes several APIs and serves as the user contact point for both the UI4 panel and the dashboard panel. It communicates with Visulox Core via the Connector

4.2.6 Connector

- Connector is a Golang project that interfaces between the portal and core. Visulox core uses various protocols, including Socket, HTTP, and SOAP. The Connector project wraps all core APIs, regardless of protocol, into an HTTP REST API.

4.3 3. Dependencies

Visulox requires:

- PostgreSQL
- KeyDB

These can:

- Be installed separately before the Master installation
- OR be installed automatically during Master setup

4.4 4. Overview

Setting up a Visulox Cluster is a **step-by-step process** that builds a distributed system consisting of **Master, Gateway, and Worker nodes**. The setup must follow a strict order, as each stage depends on configuration and credentials created in earlier steps .

4.4.1 4.1 Conceptual Flow of the System

The cluster is composed of three roles:

- **Master Node** → Central control (Core, Portal, Connector)
- **Gateway Node(s)** → Entry point and traffic routing
- **Worker Node(s)** → Execution and scaling layer

Together, they form a system where the Master manages configuration, the Gateway exposes access, and Workers handle workload execution. This separation enables scalability and high availability.

4.4.2 4.2 Setup Process

The setup follows a **top-down approach**, where components are added and connected progressively.

Step 1 — Environment Preparation

Before installation:

- Ensure system time is synchronized
- Prepare at least three servers
- Verify required dependencies (PostgreSQL, KeyDB, networking)

This step is critical, as issues here affect the entire setup.

Step 2 — Master Installation

The Master is installed first and initializes the cluster.

- Sets up Core and Portal services
- Stores configuration and cluster state
- Defines the Gateway address

It also generates the credentials required for other nodes to join.

Step 3 — Gateway Setup

The Gateway is installed next and connects to the Master.

- Registers itself in the cluster
- Establishes secure communication
- Enables external access and request routing

At this stage, the system becomes accessible but not yet scalable.

Step 4 — Worker Deployment

Workers are added to provide execution capacity.

- Install required components
- Synchronize keys with the Master
- Attach to the cluster

This enables distributed execution and allows horizontal scaling.

Step 5 — Worker Registration & Integration

Each Worker is registered in the Portal layer and fully integrated.

- Makes Workers visible to the system
- Enables proper request routing
- Finalizes communication with the Master

4.5 5. Installation Order (Mandatory)

1. Master

2. Gateway
3. Worker

⚠ During Master installation:

- The gateway hostname and IP must be provided
- The master does not work properly before the Gateway installation is completed

4.6 6. Prerequisites

4.6.1 6.1 Servers

- At least 3 servers needed for clustering:
  - 1 Master
  - 1 Gateway
  - 1 Worker

4.6.2 6.2 Time Synchronization (Mandatory)

⚠ Critical Requirement

The server system time must be correct and synchronized before running:

- `visulox start`
- `setup-master`
- Any Docker-based service initialization (e.g., PostgreSQL container)

An incorrect system time can cause:

- TLS certificate validation failures
- Docker image pull errors
- PostgreSQL container startup failure

- setup-master interruptions

Example failure:

```
tls: failed to verify certificate: x509: certificate has expired or is not yet valid
current time 2026-02-16T14:04:39+01:00 is before 2026-02-19T20:57:44Z
```

Fix command:

```
REMOTE_TIME=$(curl -kfsSI https://www.google.com | awk -F': ' '/^[Dd]ate:/{print $2}' | tr -d '\r')
echo "$REMOTE_TIME"
sudo date -s "$REMOTE_TIME"
sudo hwclock --systohc
```

4.6.3 6.3 Installing & Using tmux (Optional)

Some installation operations can take a while; session disconnections or network issues may cause the process to fail. It is recommended to use tools like `tmux`, which allow running better work/SSH session management.

4.7 7. Master Setup

4.7.1 7.1 Minimum Requirements

- 2 Core CPU
- 4 GB RAM (**8 GB recommended**)

4.7.2 7.2 Installation

7.2.1 Setting up the Master server in cluster mode

The installation process is the same for single-instance mode (Installation Guide) with one exception: in `setup-master`, you must provide the **Gateway hostname.**

Required Version

```
Latest available Visulox 5 version.
```

When Master setup is completed, you should be able to browse UI4, Dashboard and login.

7.2.2 Generating Connector Secret for Master

A Connector should be defined on the Master server. The Main server generates a secret key for this Connector. The Gateway needs this key to connect to the Master Connector.

To create the Gateway connector, run this on Master:

```
sudo /opt/visulox-portal/bin/vlx-portald create-maingateway-connector -c /opt/visulox-portal/configs/config.json --output json
```

Sample output format would be like:

```
{"secret":"63301a03-3c1b-4ec5-9590-a84961304ba2"}
```

Parameters:

- Use `--output json` or `--output secret` to get the key in JSON or plain format.

- `-c /opt/visulox-portal/configs/config.json` provide the config file of the Portal server. It contains Portal database credentials which is needed to create Connector in Portal database.

Creating an additional maingateway connector:
If this command returns an error such as `connector server "gateway-connector" already exists`, it means a maingateway connector with that default name was already created on this Master. This is not a global "one maingateway only" restriction — the uniqueness check is scoped to the connector **name**.
To create another maingateway connector (for example, for a second Gateway), re-run the command with a unique `--name` value:

```
sudo /opt/visulox-portal/bin/vlx-portald create-maingateway-connector -c /opt/visulox-portal/configs/config.json --output
json --name gateway-connector-02
```

See **Section 8.2 → Multi-gateway** below for more details.

4.8 8. Gateway Setup

4.8.1 8.1 Installing Main Gateway (or Connector) RPM

Remove the old version, if it exists:

```
sudo dnf remove vlx-connector vlx-portal vlx-portal-rte -y || true
sudo rm -rf /opt/visulox-portal* || true
sudo rm -rf /var/vlx-portal || true
sudo rm -f /opt/visulox-portal/.setup_done || true
sudo systemctl daemon-reload || true
```

Which package should I install?

- `vlx-main-gateway` **(recommended)** contains only the components required for a Main Gateway deployment.

- `vlx-connector` contains Main Gateway functionality plus additional Connector-related components and dependencies.

For most deployments, `vlx-main-gateway` **is sufficient and recommended**. It is the newer, smaller package and avoids installing components that are not required for a Gateway-only setup.

Install the RPM on the target server:

```
cd /tmp/vlx-portal
sudo dnf install vlx-main-gateway-*.rpm -y
```

Alternatively, you can install the full Connector package:

```
cd /tmp/vlx-portal
sudo dnf install vlx-connector-*.rpm -y
```

Note that `vlx-connector` requires additional server preparation steps and dependencies.
Before installing it, complete the prerequisites described in the *Server Preparation* section of the Visulox Installation Guide: Installing Visulox (Server preparation).

4.8.2 8.2 Gateway Setup (`setup-maingateway`)

After installing the RPM, run the Gateway setup wizard.

The setup wizard guides you through the required configuration and generates the Gateway configuration files.

The setup can be used in two modes:

Interactive Setup

On the Gateway server, run:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway
```

Regarding the **Connector Secret** prompt, use the secret of the Gateway Connector that was created in **Section 7.2.2**.

During the setup, you will be asked:

```
Enter XPRA Route Type [safe/performant] (default safe):
```

XPRA Route Type

safe (recommended)**:**

- All XPRA traffic is routed through the Gateway over HTTPS (port 443).
- XPRA daemon ports do not need to be exposed externally.
- Simpler firewall configuration.
- Better security posture.
- Suitable for most deployments.

performant:

- The Gateway connects directly to the XPRA daemon ports.
- Eliminates one proxy hop and may provide slightly better performance.
- Requires multiple XPRA-related ports to be reachable between clients and the Gateway.
- Increases the number of exposed network ports and firewall rules.

In most cases, **safe** should be used unless there is a specific performance requirement that justifies exposing additional ports.

Non-Interactive Setup

In some situations, such as automated deployments or scripting, you may want to run the setup without interactive prompts.

Generate a template file:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway --get-template /tmp/vlx-portal
```

This command creates:

```
/tmp/vlx-portal/setup_maingateway_template.json
/tmp/vlx-portal/setup_maingateway_template.json_README.txt
```

A default-generated template looks similar to:

```
{
  "connector_secret": "",
  "gateway_host": "",
  "gateway_port": "8180",
  "main_server_host": "",
  "main_server_port": "8080",
  "dns_resolver": "172.17.3.1",
  "xpra_route_type": "safe"
}
```

Input definitions:

```
connector_secret – UUID of the Main Gateway connector from the Portal database (required).

gateway_host     – Public URL used by clients to access the Gateway
                   (for example: https://access.example.com) (required).

gateway_port     – HTTPS listen port used by NGINX on this host.
                   Default: 8180.

main_server_host – Portal hostname or IP address (required).

main_server_port – Portal REST API port.
```

```
                    Default: 8080.

dns_resolver      – Optional comma-separated DNS resolver IPs used by NGINX.
                    If empty, system DNS resolvers are used.

xpra_route_type   – Optional.
                    Values: "safe" or "performant".
                    Default: "safe".
```

After filling the template file, run the setup using the JSON file:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway \
  --file /tmp/vlx-portal/setup_maingateway_template.json
```

Multi-gateway:

For mulit-gateway setup, we need to add `--name {gateway_name}` at the end of `create-maingateway-connector` command:

```
sudo /opt/visulox-portal/bin/vlx-portald create-maingateway-connector -c /opt/visulox-portal/configs/config.json --output json --
name {gateway_name}
```

4.8.3 8.3 Verifying Installation

```
cat /etc/nginx/includes/visulox-gateway-main-upstream-servers.conf
```

Expected: Master server IP is listed.

4.8.4 8.4 Verifying Setup

Visit:

```
https://$gateway_domain:8180/ui4/login
```

Test both NativeClient and WebClient.

4.8.5 8.5 Verifying Network Accessibility (Troubleshooting)

This step is only required if sessions fail to start or applications become stuck during launch.

The required network connectivity depends on the selected **XPRA Route Type**:

Safe Mode

In **safe** mode, all XPRA traffic is routed through the Gateway using HTTPS. XPRA daemon ports are not exposed and do not need to be reachable from clients.

Verify that:

- the Gateway can reach the Master and Worker Portal services.
- HTTPS communication between Gateway, Master, and Worker nodes is working.
- DNS resolution is functioning correctly between cluster nodes.

Performant Mode

In **performant** mode, the Gateway connects directly to XPRA daemon ports on the Master and Worker nodes. Therefore, the Gateway must be able to reach the XPRA port range:

```
14600-15600/tcp
```

To verify connectivity, select a test port from this range.

On the Master or Worker server:

```
nc -l -p <PORT_NUMBER>
```

On the Gateway server:

```
nc -w 3 <SERVER_HOSTNAME_OR_IP> <PORT_NUMBER>
```

After the connection is established, type a test message such as:

```
Hello
```

If the message appears on the receiving server, connectivity is working correctly.

If the connection fails, traffic may be blocked by:

- the Gateway server firewall
- the Master or Worker server firewall
- a firewall between the servers
- network routing restrictions

> This test verifies only basic TCP connectivity and does not validate Visulox configuration or application functionality.

4.9 9. Worker Setup

4.9.1 9.1 Core and Portal RPM Installation

Only Core and Portal RPMs should be installed on Worker as explained in Installing Visulox from 1st step to Step 2.
So, it means that no `setup-master` is needed at this point

4.9.2 9.2 Starting and Attaching Core

Then start Core service and attach it:

```
# Start services
sudo visulox start
sudo visulox portal attach -proxy
```

4.9.3 9.3 Key synchronization

Both Visulox Core modules must have the same key; if their keys are not the same, they cannot be configured as a cluster.

> Here by Visulox key, we are not talking about `Visulox.key`. It is another key, that needs to be copied from Master to Worker.

Find the key on Master in this path:

`/opt/visulox/etc/key`

From the Master server, copy the VISULOX key to the Worker server:

```
sudo scp /opt/visulox/etc/key <SERVER_USER>@<WORKER_HOST>:/tmp/vlx-master-key
```

On the Worker server, replace the existing key with the one copied from the Master:

```
sudo rm -f /opt/visulox/etc/key
sudo cp /tmp/vlx-master-key /opt/visulox/etc/key
sudo chown vlx:vlxgroup /opt/visulox/etc/key
sudo chmod 644 /opt/visulox/etc/key
```

Restart Worker Visulox when key is copied from Master:

```
sudo visulox restart
```

4.10 9.4 Firewall Configuration

Visulox Core nodes communicate on specific port ranges. Required firewall rules depend on the selected XPRA Route Type.

Safe Mode

In safe mode, XPRA traffic is routed through the Gateway over HTTPS. XPRA daemon ports do not need to be exposed.

Open these ports on Master and Worker servers:

```
sudo touch /usr/lib/firewalld/services/vlx.xml
```

Content:

```
<service>
  <short>VISULOX Firewall Rules</short>
  <description>The following rules are needed for the VISULOX Service and the VISULOX Components.</description>
  <port protocol="tcp" port="6000-6500"/>
  <port protocol="tcp" port="7001-7010"/>
  <port protocol="tcp" port="21"/>
  <port protocol="tcp" port="1443"/>
  <port protocol="tcp" port="8114"/>
  <port protocol="tcp" port="8115"/>
</service>
```

Apply:

```
sudo firewall-cmd --permanent --zone=public --add-service=vlx
sudo firewall-cmd --reload
```

Performant Mode

In performant mode, XPRA daemon ports must also be reachable. Use this mode only when direct XPRA connectivity is required.

Open these ports on Master and Worker servers:

```
sudo touch /usr/lib/firewalld/services/vlx.xml
```

Content:

```
<service>
  <short>VISULOX Firewall Rules</short>
  <description>The following rules are needed for the VISULOX Service and the VISULOX Components.</description>
  <port protocol="tcp" port="6000-6500"/>
  <port protocol="tcp" port="7001-7010"/>
  <port protocol="tcp" port="21"/>
  <port protocol="tcp" port="1443"/>
  <port protocol="tcp" port="8114"/>
  <port protocol="tcp" port="8115"/>
  <port protocol="tcp" port="14600-15600"/>
</service>
```

Apply:

```
sudo firewall-cmd --permanent --zone=public --add-service=vlx
sudo firewall-cmd --reload
```

4.10.1 9.5 Attaching Worker to Master

At the final stage, we attach the Visulox Core of the Master server to that of the worker server(s).

Run on Master:

```
sudo -s
cd ~
visulox attach $domain_of_worker_server
```

Expected output:

```
attached node vSFTESTWORKERSERVER06 at location 'STANDARD' zone 'STANDARD'
etcd cluster: added vSFTESTMASTERSERVER06
etcd client started
```

Then check:

```
visulox status
```

Expected Output (Example)

```
-------------------------------------------------------------------------------------------------------------------
|                  node | location |     zone | nodeinfo | status | archive |    servicestarttime |         version |
-------------------------------------------------------------------------------------------------------------------
| vSFTESTMASTERSERVER05 | STANDARD | STANDARD | STANDARD |     up |         | 2026-03-05 12:47:39 | 5.alpha-vlxxpra |
| vSFTESTWORKERSERVER05 | STANDARD | STANDARD | STANDARD |     up |         | 2026-03-05 12:46:34 | 5.alpha-vlxxpra |
-------------------------------------------------------------------------------------------------------------------
```

4.10.2 9.6 Troubleshooting

Run these commands on Worker:

```
visulox integrity
journalctl -u visulox -n 100 -f
```

```
visulox log -l info
visulox log -l debug
visulox log -l error
```

`Example visulox integrity` output:

```
integrityXPRA:******************** no jet done *****************
Integrity-Check on vW1DEMO : VISULOX PRIVILEGED ACCESS MANAGEMENT EVALUATION / 5.0.2 / 2026-07-13 07:54:23 UTC
    ------------------------------------------------------------------------------------------------------------
    | option   | cat                                | info                                          | returnCode |
    ------------------------------------------------------------------------------------------------------------
    | -license | License                            | time limited in use                           | WARNING(2) |
    | -db      | connect                            | VISULOX cannot run from : /home/develadmin    | FAILURE(1) |
    | -db      | status                             | VISULOX cannot run from : /home/develadmin    | FAILURE(1) |
    | -vlx     | Cluster                            | offline                                       | WARNING(2) |
    | -sys     | Key vlxkey                         | perms not 00640                               | FAILURE(1) |
    | -sys     | Size of /opt/visulox/var/filearea | has 25.88GB. need 80.0GB                      | WARNING(2) |
    | -sys     | timedatectl                        | not synchronised                              | WARNING(2) |
    | -sys     | FQDN:w1demo.tbsol.de               | check DNS: No Reserse lookup answer for ::1   | FAILURE(1) |
    | -store   | Filestore                          | filestore warning (at 25.88GB) threshold 50.0GB | WARNING(2) |
    | -mail    | Mail                               | localhost:25 not reachable                    | WARNING(2) |
    ------------------------------------------------------------------------------------------------------------

ExitCode: FAILURE: One or more tests failed! For more information use <visulox log>
```

4.11 10. Registering Worker in Master

You should insert a Portal server in the database for the Worker server you want to attach to the cluster.

Run `create-worker-portal-server` and keep the `Portal server secret` that is displayed.

Note: `Portal server secret` will be shown to you once only.

There are three modes to run this command:

4.11.1 Plain text mode:

In the Master server, run the following command with the domain and IP address of the worker server:

```
sudo /opt/visulox-portal/bin/vlx-portald create-worker-portal-server -c /opt/visulox-portal/configs/config.json --domain
$WORKER_SERVER_HOSTNAME --server-ip $WORKER_SERVER_IP
```

You can also pass `--server-ip` to provide the IP of the worker server. Note that if DNS is not configured, or has no record linking `$WORKER_SERVER_DOMAIN` to `$WORKER_SERVER_IP`, you will receive an error.

4.11.2 JSON mode:

If you want to receive the command result in a JSON format, you can add the `--output json` argument. For example:

```
sudo /opt/visulox-portal/bin/vlx-portald create-worker-portal-server -c /opt/visulox-portal/configs/config.json --domain
<hostname.domain> --server-ip xxx.xxx.xxx.xxx --output json
{"server_name":"vSFTESTWORKERSERVER10","domain":"<hostname.domain>","server_ip":"xxx.xxx.xxx.xxx","secret":"<xxxxxxxxx>"}
```

4.11.3 Only secret mode:

If you only want to receive the portal secret by running the above command, you can add the `--output secret` switch to the first command. For example:

```
sudo /opt/visulox-portal/bin/vlx-portald create-worker-portal-server -c /opt/visulox-portal/configs/config.json --domain
<hostname.domain> --server-ip xxx.xxx.xxx.xxx --output secret
```

```
<xxxxxxxxx>
```

⚠️ Write down the secret of the created portal server, as it is only shown once.

4.12 11. Installing Portal On Worker

4.12.1 11.1 Portal Installation

Download the desired RTE, Portal, and Connector RPMs to `/tmp/vlx-portal/`.

Then run this from Worker:

```
cd /tmp/vlx-portal

sudo dnf install vlx-portal-rte-*.rpm -y
sudo dnf install vlx-portal-*.rpm -y
sudo dnf install vlx-connector-*.rpm -y
```

4.12.2 11.2 Portal Setup

From Worker run `setup-node`. You can run it in two modes:

Interactive

```
sudo /opt/visulox-portal/bin/vlx-portald setup-node
```

This command will ask for the portal secret. You should use the secret you received in last step.

Non-interactive

In some cases, you may not want to enter the inputs of the `setup-node` command interactively. For example, if you are writing a script, you need to run this command in a non-interactive mode to have control over the inputs.
To do so, you need to create template files for the setup command to run. You need to run the following command:

```
/opt/visulox-portal/bin/vlx-portald setup-node --get-template /tmp/vlx-portal
```

After running the above command, a `setup_node_template.json` template file and a `setup_node_template_README.txt` file will be created in the `/tmp/vlx-portal` directory.

An example of a default-generated template file looks like this:

```
{
  "master_ip": "",
  "master_port": "8080",
  "secret": "",
  "dns_resolver_ips": [
    "172.17.3.1"
  ],
  "keydb_tls": {
    "ca_cert_path": "",
    "client_cert_path": "",
    "client_key_path": ""
  },
  "postgresql_tls": {
    "ca_cert_path": "",
    "client_cert_path": "",
    "client_key_path": ""
  }
}
```

You need to fill in the required items of this template file by reading the README file.
Then, consider you have prepared a setup JSON file using the template file named `setup-node.json` ; You can run the `setup node` command non-interactively as follows:

```
sudo /opt/visulox-portal/bin/vlx-portald setup-node --file /path/to/setup-node.json
```

⚠ You should only set values for `keydb_ca_cert_path` , `keydb_client_cert_path` , and `keydb_client_key_path` fields in the setup-node.json file if you haven't installed KeyDB automatically via the `setup-master` command, and you use an external KeyDB that has a "self-signed" certificate.

4.12.3 11.3 Verifying network accessibility

If you have issues with setting up sessions, you can check what we did in **step 8.5** and check the range of 14600-15600/tcp.

4.13 12. Setting Up Additional Workers

- Recommended: at least **3 nodes (odd number)**
- Repeat worker setup

4.14 13. Final Testing

- Browse using Gateway address:

```
https://$gateway_domain:8180/ui4/login
```

- Run some apps using Vispra and WebClient.
- Run `health-check` command from all servers

5 Multi-Gateway Setup Guide

5.1 Introduction

This guide explains how to configure multiple Main Gateways in a Visulox Cluster to improve availability, load distribution, and fault tolerance.

This document assumes:

- A Visulox Master is already installed and operational.
- At least one Gateway has already been configured.
- UI4 and Dashboard are accessible through the existing Gateway.

For general cluster installation instructions, refer to the Visulox Cluster Installation Guide.

5.2 Architecture Overview

In a multi-gateway deployment:

- Each Gateway has its own Connector entry in Portal.
- All Gateways connect to the same Master.
- External traffic can be distributed across Gateways using DNS round-robin, load balancers, or reverse proxies.

5.3 Creating Additional Gateway Connectors

Each Gateway requires its own Connector definition in Portal.
To create this record, first generate a Connector secret on the Master server.

Run the following command on the Master server:

```
sudo /opt/visulox-portal/bin/vlx-portald \
  create-maingateway-connector \
  -c /opt/visulox-portal/configs/config.json \
```

```
  --output json \
  --name gateway-a
```

Example:

```
{
  "secret":"63301a03-3c1b-4ec5-9590-a84961304ba2"
}
```

Create one connector per Gateway:

```
--name gateway-a
--name gateway-b
--name gateway-c
```

Each command returns a unique secret.

Store each secret securely.

5.4 Installing Additional Gateway Nodes

Install the Main Gateway package on every Gateway server:

```
sudo dnf install vlx-main-gateway-*.rpm -y
```

The dedicated Main Gateway package is recommended for Gateway-only deployments.

5.5 Configuring Gateway Nodes

The Gateway setup command supports three configuration methods:

- Interactive mode

- Command-line mode
- JSON file mode

5.5.1 Interactive Mode

Run:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway
```

The setup wizard prompts for all required configuration values.

Use:

- The Connector secret created for this Gateway.
- The public hostname of this Gateway.
- The Master Portal hostname and port.
- The desired XPRA route type.

5.5.2 Command-Line Mode

Run:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway \
  --main-server-host master.company.com \
  --main-server-port 8080 \
  --gateway-host gateway-a.company.com \
  --gateway-port 443 \
  --connector-secret <SECRET> \
  --xpra-route-type safe
```

Parameters:

Parameter	Description
`--main-server-host`	Hostname or IP address of the Master Portal server
`--main-server-port`	REST API port of the Master Portal
`--gateway-host`	Public hostname of this Gateway
`--gateway-port`	HTTPS port exposed by the Gateway
`--connector-secret`	Connector secret generated on the Master
`--xpra-route-type`	XPRA routing mode (`safe` or `performant`)

Example:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway \
  --main-server-host master.company.com \
  --main-server-port 8080 \
  --gateway-host gateway-a.company.com \
  --gateway-port 443 \
  --connector-secret 63301a03-3c1b-4ec5-9590-a84961304ba2 \
  --xpra-route-type safe
```

5.5.3 JSON File Mode

Generate a template file:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway \
  --get-template /tmp
```

This creates a template JSON file in the specified folder.

Populate the generated file with the required values.

Example:

```
{
  "connector_secret": "",
  "gateway_host": "",
  "gateway_port": "8180",
  "main_server_host": "",
  "main_server_port": "8080",
  "dns_resolver": "127.0.0.11",
  "xpra_route_type": "safe"
}
```

Run the setup using the file:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway \
  -f /path/to/gateway-config.json
```

Optionally remove the file automatically after successful setup:

```
sudo /opt/visulox-portal-connector/bin/vlx-connectord setup-maingateway \
  -f /path/to/gateway-config.json \
```

```
  -remove-file-after-setup
```

This mode is recommended for automated deployments and configuration management tools.

5.6 Verifying Gateway Registration

On each Gateway:

```
cat /etc/nginx/includes/visulox-gateway-main-upstream-servers.conf
```

Verify that the Master server appears in the generated upstream configuration.

Verify NGINX configuration:

```
sudo nginx -t
```

Verify service status:

```
sudo systemctl status nginx
sudo systemctl status visulox-portal-connector
```

5.7 Portal Failure Behavior

If one Gateway becomes unavailable:

- Existing sessions routed through that Gateway may disconnect.
- New sessions can be established through healthy Gateways.
- Master and Worker nodes continue operating normally.

For high availability, at least two Portal Server are recommended.

5.8 Validation Checklist

For every Gateway verify:

- Gateway setup completed successfully.
- Connector secret is unique.
- NGINX configuration is valid.
- UI4 login page opens.
- Dashboard opens.
- Native Client sessions start successfully.
- Web Client sessions start successfully.
- Worker-hosted applications launch correctly.

Test access using:

```
https://<gateway-host>
```

Repeat the validation for every configured Gateway.

5.9 Recommendations

Production deployments should use:

- 2 or more Main Gateways
- 2 or more Portal Servers

Place the Main Gateways behind a load balancer or DNS round-robin configuration to improve availability and distribute incoming traffic.

6 Updating Visulox

This document describes the procedure to safely update Visulox using RPM packages:

- Visulox Portal (vlx-portal)
- Visulox Connector (vlx-connector)
- Visulox Runtime Environment (vlx-portal-rte)
- Visulox Core (vlx-core)
- Visulox Runtime Environment (visulox-rte)

The upgrade procedure ensures that:

- Existing configuration and data are preserved
- Database migrations are applied correctly
- Services are restarted in a controlled and auditable way
- Downtime is minimized

This guide applies to:

- Staging environments
- QA servers
- Production servers
- Developer test servers using RPM deployment

6.1 1. Transfer files to the Server

Create a temporary folder on the server:

```
mkdir -p /tmp/vlx-upgrade
```

Copy the following files to the **vlx-upgrade** folder:

```
- vlx-portal-rte-5.0.2.el9.x86_64.rpm
- vlx-portal-5.0.2.el9.x86_64.rpm
- vlx-connector-5.0.2.el9.x86_64.rpm

- visulox-rte-1.2.0-1.el9.x86_64.rpm
- vlx-core.5.0.2.el9.x86_64.rpm
```

6.2 2. Upgrade RPM Packages

Stop running services:

```
sudo systemctl stop vlx-portal
sudo systemctl stop vlx-connector
sudo visulox stop
```

Update Visulox :

```
cd /tmp/vlx-upgrade

# Visulox Portal
sudo dnf upgrade vlx-portal-rte-*.rpm -y
sudo dnf upgrade vlx-portal-*.rpm -y
sudo dnf upgrade vlx-connector-*.rpm -y

# Visulox Core
sudo dnf upgrade visulox-rte-1.2.0-1.el9.x86_64.rpm
sudo dnf upgrade vlx-5.0.2.el9.x86_64.rpm
```

This will:

- Replace binaries
- Preserve configuration files

- Keep database intact
- Maintain system users and permissions

Run portal attach command after update:

```
sudo visulox portal attach
```

Start services again:

```
sudo visulox start
sudo systemctl start vlx-portal
sudo systemctl start vlx-connector
```

6.3 3. Apply Database Migrations

Check current migration version:

```
sudo /opt/visulox-portal/bin/vlx-portald migrate \
  --migration-version \
  -c /opt/visulox-portal/configs/config.json
```

Apply pending migrations:

```
sudo /opt/visulox-portal/bin/vlx-portald migrate \
  --up \
  -c /opt/visulox-portal/configs/config.json
```

Notes:

- If no migrations are required, nothing will be applied.
- If migrations fail, the RPM may be missing required migration files.
- Check logs for errors:

```
sudo journalctl -u vlx-portal -n 50
```

6.4 4. Verify Upgrade

Check Portal status:

```
sudo systemctl status vlx-portal.service
```

Check Connector status:

```
sudo systemctl status vlx-connector.service
```

Check Core status:

```
sudo visulox integrity
sudo visulox status
```

Check Running Processes

```
ps auxwwf | grep "vlx\|visulox"
```

Check Portal logs

```
tail -f /var/log/visulox-portal/portal.log
```

Check Connector logs

```
tail -f /var/log/visulox-portal-connector/connector.log
```

Check system logs

```
sudo journalctl -u vlx-portal -n 100
sudo journalctl -u vlx-connector -n 100
```

6.5 5. Post-Upgrade Validation Checklist

Verify:

- Portal web interface loads
- Users can login
- Sessions can be started
- Connector connects correctly
- LDAP / AD authentication works (if enabled)
- No migration errors in logs
- No service restart loops

6.6 6 Rollback Procedure (if required)

If upgrade fails, reinstall the previous RPM version:

```
sudo dnf downgrade vlx-portal-<previous-version>.rpm -y
sudo dnf downgrade vlx-connector-<previous-version>.rpm -y
sudo dnf downgrade vlx-portal-rte-<previous-version>.rpm -y
```

Then restart services:

```
sudo systemctl restart vlx-portal
sudo systemctl restart vlx-connector
```

7 Visulox Hotfix (Core)

It can be reasonable to install an available hotfix for Visulox instead of using the Visulox update mechanism.

/opt/visulox/setup/hotfix.sh checks the status of all files on all Visulox Nodes, applies the hotfix files and creates a backup of the original files.

> **Requirement for Visulox Hotfix**
> Hotfix has to be applied on each node.
> **Depending on the hotfix**, the following scenarios are possible:
> - Total restart is needed
> - Service kill is needed
> - No restart is needed
>
> See attached Release Notes for the hotfix.

(See also: Manual restart of a missing VISULOX service)

Usage:

```
sh  /opt/visulox/setup/hotfix.sh <hotfix-file>
```

The backup files are copied to **/opt/visulox/setup/hotfix/hotfix-backup-<*date of installation*>.tgz** and can be re-established with Visulox Hotfix.

The backup history can be found in **/opt/visulox/setup/hotfix/history**.

> After a Visulox update to a new version, **/opt/visulox/setup/hotfix** will be deleted.

8 Uninstalling Visulox

Uninstall Visulox and remove all files from an existing installation with:

```
sudo dnf remove vlx-connector vlx-portal vlx-portal-rte visulox-rte -y || true

sudo rm -rf /opt/visulox-portal* || true
sudo rm -rf /var/vlx-portal || true
sudo rm -rf /opt/visulox || true
sudo rm -f /opt/visulox-portal/.setup_done || true

sudo systemctl daemon-reload || true
```

9 Visulox License Agreement

9.1 Visulox License Agreement

Version 6.0 · *Effective: 2026-05-05 Applicable to VISULOX version 5 and later*

amitego AG · Im Obstgarten 2b · 8602 Wangen-Brüttisellen · Switzerland

9.1.1 1. Object of the Agreement

1.1 The object of this licence shall be the standard data processing programme **Visulox** of amitego AG (the "**SOFTWARE**"), including all updates, upgrades, patches and documentation supplied by amitego AG ("**AMITEGO**").

1.2 The SOFTWARE includes certain third-party software components, including open-source components, which are governed by their respective licence terms. The applicable licence terms are summarised in Section 7 and listed in Exhibit B. Such third-party licences apply exclusively to the corresponding components and do not affect the proprietary nature of the SOFTWARE as a whole.

1.3 Should a portion of the object of the Agreement comprise the supply of standard software of a third-party manufacturer, the terms of use of that manufacturer shall apply exclusively in this respect. AMITEGO shall in this case solely arrange the licence agreement, which is then concluded directly between the manufacturer and the licensee. These terms of use shall be provided to the licensee on request.

1.4 AMITEGO is amitego AG, Im Obstgarten 2b, 8602 Wangen-Brüttisellen, Switzerland. Visulox is a registered trade mark of amitego AG.

9.1.2 2. Rights of Use

2.1 The licensee shall receive the non-transferable and non-exclusive right to use the SOFTWARE. The contractual grant of the licence shall occur according to the particular offer selected as a perpetual licence or as a time-limited licence as set forth in an applicable Order.

2.2 "**Order**" means any ordering instrument used for acquiring AMITEGO Software or Service under this Agreement, which once executed will become part of this Agreement. The initial Order shall be attached hereto as Exhibit A.

2.3 All use after expiry of the term of a time-limited licence (if applicable) shall be excluded. In the event of continued use in breach of the Agreement, payment of the then-valid list price of the licence in addition to a service fee according to Section 8 shall be due retrospectively as from the beginning of such use. This shall not affect the right of each contracting party to extraordinary termination of the Agreement without a period of notice for cause.

2.4 In the event of the termination of this Agreement, the licensee shall be obliged to delete the SOFTWARE and all copies thereof completely.

2.5 The licensee may use the SOFTWARE on the hardware available to it. If the licensee changes the hardware on which the SOFTWARE is operated, the licensee must delete the SOFTWARE from the hardware previously used.

2.6 The licensee shall be obliged to take suitable measures to prevent any unauthorised use by third parties. For the purposes of this Section, branch offices, companies associated with the licensee, partners or spatially or organisationally separate institutions of the same organisation shall be regarded as "**third parties**."

9.1.3 3. Object Code, Source Code and Backup Copies

3.1 AMITEGO shall not be obliged to transfer the object code on a data carrier.

3.2 The proprietary source code of the SOFTWARE constitutes a trade secret of AMITEGO. There shall not be any claim to the surrender or disclosure of the proprietary source code unless (a) a proceeding in bankruptcy, insolvency and/or liquidation is instituted by or against AMITEGO, or AMITEGO enters into a voluntary or involuntary receivership arrangement; (b) AMITEGO ceases to carry on business on a regular basis or fails to provide Services for the SOFTWARE for a period of three (3) days; or (c) any other event occurs as set forth under applicable mandatory law.

3.3 The licensee shall be entitled to make backup copies of the SOFTWARE if this is necessary for its proper use.

9.1.4 4. Copyright and Proprietary Rights

4.1 The licensee acknowledges that the SOFTWARE is protected by copyright, trade-secret laws and international agreements, and that all right, title and interest in and to the SOFTWARE remain with AMITEGO. The licensee shall not be entitled to change, process, copy, duplicate, translate, adapt or create derivative works of the SOFTWARE or text materials transferred to it (codes, documentation) beyond the scope required for the use of the SOFTWARE within the framework of the rights and obligations arising from this Agreement, whether on its own behalf or through third parties.

4.2 Copyright marks or registration features, including without limitation any registration numbers in the SOFTWARE, may not be removed or changed.

4.3 Any temporary transfer for use for direct or indirect economic or commercial benefit to third parties shall be prohibited without the prior written approval of AMITEGO. Any resale for independent use of the SOFTWARE to third parties shall only be permissible if (a) the licence acquired is not split up, i.e. the right to use the SOFTWARE is not resold for a number of users smaller than the number originally acquired by the licensee; (b) the licensee provides the data of the purchaser to AMITEGO in order to maintain the services pursuant to Section 8; and (c) the licensee ensures by all technical means at its disposal that any copy still available to it is rendered useless and that no possibility whatsoever of use of the SOFTWARE or its components remains with the licensee.

4.4 This Section 4 governs the proprietary portions of the SOFTWARE. Rights with respect to third-party open-source components are governed by Section 7.

9.1.5 5. Decompilation and Programme Changes

5.1 Disassembling the programme code of the SOFTWARE into other code forms (decompilation) and other forms of reverse engineering of the various production stages of the SOFTWARE, including programme changes, shall only be permissible without the express approval of AMITEGO to the extent permitted under applicable mandatory law (in particular for the purposes of achieving interoperability of an independently created computer program with other programs).

5.2 Copyright marks, serial numbers and other features serving programme identification may not be removed or changed under any circumstances.

5.3 This Section 5 governs the proprietary portions of the SOFTWARE. Rights with respect to third-party open-source components are governed by Section 7.

9.1.6 6. Permitted Uses and Restrictions

6.1 The licensee shall not:

- circumvent or attempt to circumvent any license-control, activation or anti-tampering mechanism of the SOFTWARE;
- use the SOFTWARE to provide commercial software-as-a-service offerings to third parties unless explicitly permitted in the applicable Order;
- combine, link or merge the proprietary portions of the SOFTWARE with any open-source software in a manner that would purport to subject the proprietary portions of the SOFTWARE, in whole or in part, to the terms of any open-source licence;
- use the SOFTWARE in violation of applicable export-control or sanctions laws; or
- remove, obscure or alter any proprietary notices, labels or trademarks contained in or affixed to the SOFTWARE.

6.2 This Section 6 governs the proprietary portions of the SOFTWARE. Rights with respect to third-party open-source components are governed by Section 7.

9.1.7 7. Third-Party and Open-Source Components

7.1 General

The SOFTWARE includes certain third-party open-source software components ("**Open-Source Components**"). The applicable licences, copyright notices and source-code availability information for the Open-Source Components are listed in Exhibit B and provided in the file NOTICE.txt or THIRD-PARTY-LICENSES.txt accompanying the SOFTWARE distribution. Each Open-Source Component is licensed to the licensee solely under the terms of its applicable open-source licence.

The Open-Source Components are functionally integrated into, but technically and legally separate from, the proprietary portions of the SOFTWARE: they are invoked through arms-length interfaces and are not statically linked into, nor incorporated as derivative works of, the proprietary portions of the SOFTWARE. The licensing of any Open-Source Component does not extend to the proprietary portions of the SOFTWARE, which remain licensed exclusively under this Agreement.

7.2 Notices and Licence Terms

AMITEGO provides with each copy of the SOFTWARE: (a) prominent notice that the SOFTWARE includes Open-Source Components; (b) the full text of each applicable open-source licence; and (c) the original copyright and licence notices for each Open-Source Component, in unmodified form.

7.3 Source Code Availability

For each Open-Source Component which is subject to a licence requiring the availability of source code (including without limitation components licensed under the GNU General Public License), AMITEGO shall make the complete corresponding source code (including any AMITEGO modifications, if any) available on request for at least three (3) years from the date the SOFTWARE was last distributed by AMITEGO. Source code may be obtained free of charge (other than the actual cost of physical media and shipping, if any) by written request to opensource@visulox.com, or, where available, by reference to the public source repository of the corresponding component as identified in Exhibit B.

7.4 Modifications and Replacement

The licensee's rights to copy, modify, reverse-engineer, redistribute and otherwise use any Open-Source Component are governed exclusively by the applicable open-source licence and are not limited or restricted by this Agreement. The licensee acknowledges, however, that AMITEGO's warranty

obligations under Section 9 and support obligations under Section 8 do not extend to any version of the SOFTWARE in which an Open-Source Component has been modified or replaced by the licensee or any third party.

7.5 No Warranty for Open-Source Components

The Open-Source Components are provided to the licensee on an "**AS IS**" basis under the terms of their respective open-source licences, without any warranty of any kind from AMITEGO. The warranty disclaimers and limitation-of-liability provisions of the applicable open-source licences shall apply with respect to such components.

9.1.8 8. Support and Maintenance

8.1 Support and maintenance of the SOFTWARE ("**Service**") may be acquired in addition to the SOFTWARE licence.

8.2 The Service period shall be renewed in each case for the same contractual period as the licence agreement if the Service agreement is not terminated by one contracting party in writing at the end of the initial or each succeeding contractual period. The period of notice in this respect shall be three (3) months.

8.3 If the Service is terminated without cancellation of the licence agreement and the licensee subsequently wishes to resume the Service, the period from the end of the last paid Service period to the actual date of resumption shall be paid for at an amount equal to fifty per cent (50%) of the regular Service fee.

8.4 This shall not affect the right of each contracting party to extraordinary termination of the Agreement without a period of notice for cause.

8.5 The Service includes the supply of cost-free updates of the SOFTWARE, e-mail support at support@visulox.com and telephone support pursuant to the particular support agreement separately concluded in this regard.

9.1.9 9. Guarantee

9.1 The parties agree that, according to the current state of technology, it is not possible to develop standard software free of defects for all application conditions. AMITEGO shall nevertheless be liable for ensuring that the SOFTWARE substantially corresponds with the functions described in the documentation and that it is free of defects that cancel or reduce its value or its suitability for the contractually stipulated purpose or the usual purpose. AMITEGO shall not be liable for insignificant deviations or reductions.

9.2 In the event of considerable defects, AMITEGO shall be entitled and obliged to eliminate the defects at its own expense or to provide an equivalent replacement (subsequent specific performance). AMITEGO shall be entitled to make the choice between rectification and replacement. If the subsequent

specific performance or replacement delivery fails a second time, the licensee may at its discretion either rescind the Agreement or reduce the agreed payment.

9.3 The guarantee period shall be one (1) year, calculated from the day of delivery or download of the SOFTWARE.

9.4 The guarantee under this Section 9 does not extend to: (a) Open-Source Components, which are provided on an "**AS IS**" basis under their respective open-source licences (see Section 7.5); (b) defects arising from modifications of the SOFTWARE or any Open-Source Component by the licensee or any third party; (c) defects caused by use of the SOFTWARE outside the documented operating environment; or (d) defects caused by hardware, network or third-party-software failures outside AMITEGO's control.

9.1.10 10. Liability Restriction and Contributory Negligence

10.1 AMITEGO shall only be liable for losses arising other than through injury to life, limb or health if such losses are based on intent or gross negligence or on a culpable infringement of an essential contractual obligation by AMITEGO or its agents. An obligation shall be regarded as contractually essential if its fulfilment is what makes proper implementation of the Agreement possible in the first place and on whose fulfilment the customer may normally rely.

10.2 AMITEGO shall only be liable for the loss of data according to Section 10.1 if such loss could not have been avoided by appropriate data backup measures on the part of the licensee. Inadequate data backup shall in particular exist if the licensee neglected to take precautions through backup measures corresponding to the current state of technology against external influences, especially against computer viruses and other phenomena that could endanger individual data sets or the entire database.

10.3 Additional liability for damages shall be excluded; this shall not affect claims arising from a guarantee provided by AMITEGO for the quality of the purchase object or from mandatory product-liability legislation, including the Swiss Federal Act on Product Liability (Produktehaftpflichtgesetz, PrHG).

10.4 In the event of ordinary negligence, AMITEGO shall only be liable for those losses that are foreseeable or typical.

10.5 The limitations set forth in this Section 10 shall not apply to: (i) AMITEGO's obligations under Section 12 (Confidentiality); (ii) AMITEGO's gross negligence or willful misconduct; or (iii) liability under mandatory statutory provisions.

10.6 AMITEGO shall have no liability whatsoever in respect of any Open-Source Component beyond what is expressly provided in the applicable open-source licence.

9.1.11 11. Price Adjustments

11.1 AMITEGO reserves the right, in the event of changes in salary or prime costs or other general cost changes in the IT industry that occur after the conclusion of this Agreement, to increase or reduce the agreed prices in accordance with such actual cost changes. The corresponding changes shall be communicated to the licensee before they take effect.

11.2 The change shall take effect at the beginning of the month following notification of the change. Should such changes lead to an increase in prices of more than five per cent (5%), the licensee shall be entitled to terminate the Agreement without notice in writing within one (1) month of receiving the notification of change.

9.1.12 12. Confidentiality

12.1 Each party agrees that during the term of this Agreement it may disclose confidential information to the other party ("**Confidential Information**") and that the receiving party shall not disclose such Confidential Information except as set forth herein. The proprietary source code, design documents, technical documentation and trade secrets of the SOFTWARE shall be deemed Confidential Information of AMITEGO.

12.2 Confidential Information shall not include information that the receiving party can demonstrate:

(a) is, as of the time of its disclosure, or thereafter becomes part of the public domain through a source other than the receiving party without an obligation of confidentiality;

(b) was known to the receiving party prior to the time of its disclosure without an obligation of confidentiality;

(c) is independently developed by the receiving party without use of, or reference to, the disclosing party's Confidential Information; or

(d) is subsequently learned from a third party not under a confidentiality obligation to the disclosing party.

12.3 If a receiving party is required by applicable law, regulation, court order or legal process to disclose any Confidential Information, the receiving party shall provide the disclosing party with prompt notice of such requirement and shall use reasonable efforts to ensure that all Confidential Information so disclosed is treated confidentially. Such disclosure of Confidential Information in accordance with this Section shall not violate the terms of this Section 12.

9.1.13 13. Final Provisions

13.1 Activation of the SOFTWARE licence shall only occur after complete payment of the usage fee for the licensed SOFTWARE and – if agreed – the additional fees.

13.2 This Agreement shall be governed by Swiss law to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG). The exclusive legal venue shall be Zurich, Switzerland.

13.3 The contractual language shall be English. Versions in other languages shall serve solely as additional information and shall not be binding.

13.4 Should any provision of this Agreement be or become invalid or unenforceable in whole or in part, the validity of the remaining provisions shall not be affected. The parties undertake to replace the invalid or unenforceable provision with a valid and enforceable provision that comes as close as possible to the economic intent of the invalid or unenforceable provision.

13.5 Amendments and supplements to this Agreement must be made in writing in order to be effective. This requirement of written form may itself only be waived in writing.

13.6 This Agreement, including any Order and the documents referenced herein, constitutes the entire agreement between the parties with respect to the SOFTWARE and supersedes all prior agreements, understandings or representations, whether written or oral.

9.1.14 Exhibit A – Order

If asked but not mandatory, the applicable Order shall be attached here. The Order shall set out, at a minimum: licence type (perpetual / time-limited), term, number of users / instances, applicable fees, Service options and any specific conditions agreed between AMITEGO and the licensee.

9.1.15 Exhibit B – Open-Source Components

The following Open-Source Components are included in the SOFTWARE. Each Open-Source Component is licensed solely under the terms of its respective open-source licence. The full text of each applicable licence, together with the respective copyright notices, is included in the file NOTICE.txt or THIRD-PARTY-LICENSES.txt distributed with the SOFTWARE.

B.1 Xpra

- **Component:** Xpra
- **Project URL:** https://github.com/Xpra-org/xpra
- **Licence:** GNU General Public License, Version 2, June 1991 (GPL v2). Individual files within the Xpra distribution may be made available under additional or alternative compatible licences as identified in the source headers and LICENSE files of the Xpra distribution.
- **Full licence text:** https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
- **Source code request:** opensource@visulox.com (available for at least three (3) years from last distribution)
- **AMITEGO modifications:** *Any modifications by AMITEGO are made available under the GPL v2.*

B.2 Further licence activated Open-Source Components

None

10 Visulox and Session Cookies

Visulox requires altogether four cookies, which are needed for **technical session controlling**. They are only used for functional purpose.

These cookies are used to assign a server side session to the user. This is a **basic** and **essential functionality** of the Visulox software.

Client or personal data is **not** collected/stored and **no** tracking to our company or to other services is done.

> Session cookies fall under the categorization of strictly necessary cookies under the General Data Protection Regulation (GDPR), applicable in the European Union and the UK. Strictly necessary cookies like session cookies are **exempt** from the consent requirements underlined in the GDPR. Therefore, session cookies are **GDPR compliant**.
> Strictly necessary cookies are essential to navigate a website and use its features and functionalities. Without them, a user wouldn't be able to use basic services like logging in on a website or adding items to a shopping cart etc. GDPR **exempts** these cookies from consent requirements as they do **not** gather any personal information about users.

If a customer nevertheless wants to have a cookie consent, this can be done with a **Visulox extended login consent**.

See: How to setup a standard form contract to commit on login (consent)

11 Appendix_IG

11.1 Appendix

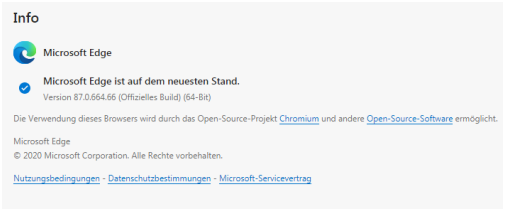
Troubleshooting and **Glossary**

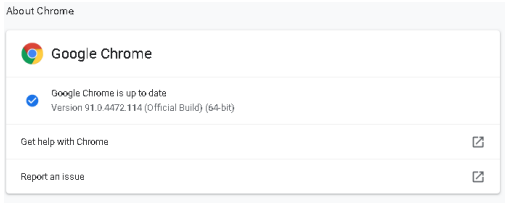
11.1.1 Troubleshooting

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
```

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:

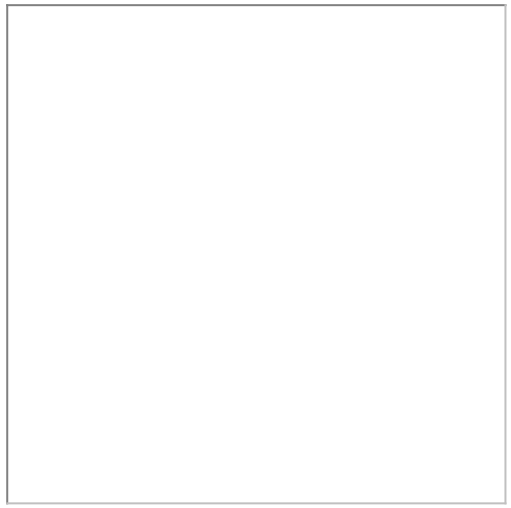
The allowed characters in a password can vary depending on the recommendations of the particular website, platform or system.
However, the following character types are generally recommended:

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.

Application start via Workspace

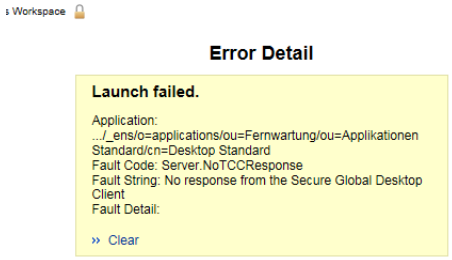
When an application is started via Workspace a small **Connection Progress** window is opened. Mostly this window disappears immediately and the application is launched. If there is a problem with the connection to the application, then this window stays open and shows the errors occurred.



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 Client Component 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:

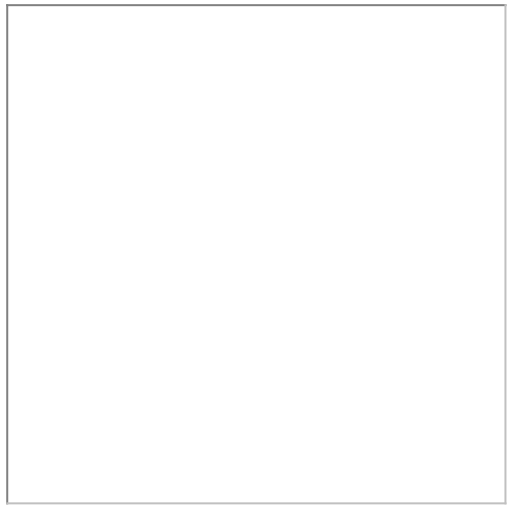
```
#!/bin/bash
# verify helpful lines
exec 99> <path to a log file>
BASH_XTRACEFD=99
set -x
```

Using Flash Player and checked out films

Flash is no longer supported.

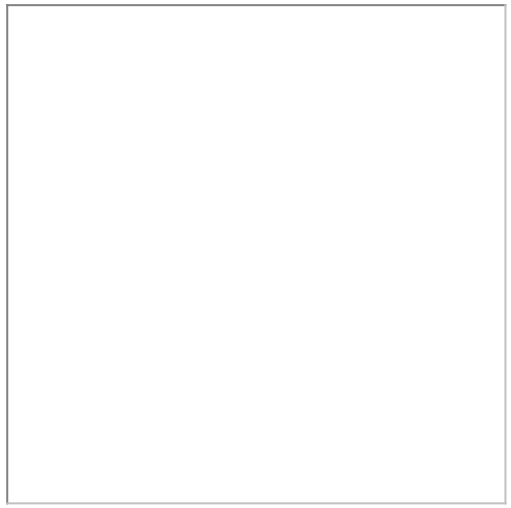
Citrix Receiver

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.

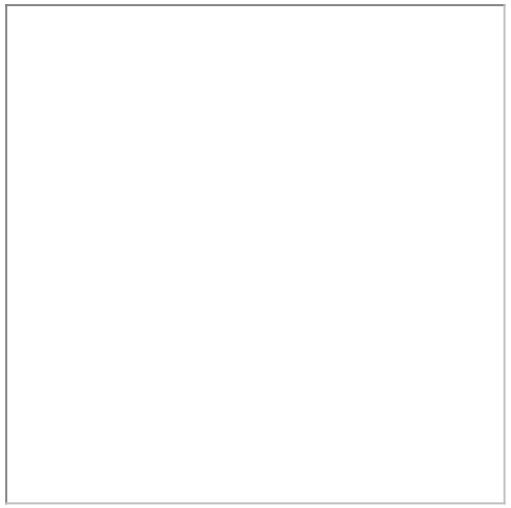
Also always take care, that the Citrix Receiver plugin is not blocked by the browser. Check plugin status via address bar icon in the browser:

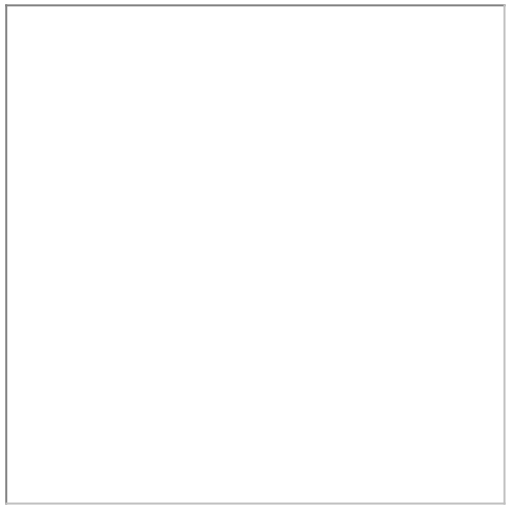


Copy & paste for Mac OS

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.
	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:

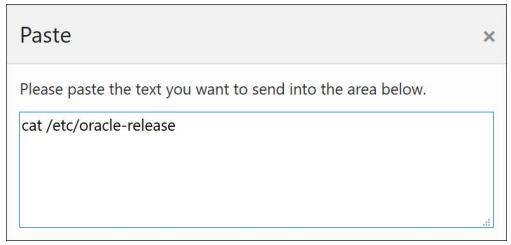
Copying from an application to a client device

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.

11.1.2 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.
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
NEP	Short form for **N**etwork **E**ntry **P**oint
Network Entry Point	See: **RIP**
NFS	**N**etwork **F**ile **S**ystem

NGINX	**NGINX** is an HTTP web server, reverse proxy, content cache, load balancer, TCP/UDP proxy server, and mail proxy server.
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)
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 Core	Visulox Core is responsible for: • Managing policies • Recording sessions • Managing session lifecycle • etc …
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	Visulox Portal is the main business logic controller responsible for defining and managing: • User Profiles • Applications • Application Servers • Relationships between them
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 Connector	Visulox Portal Connector acts as the execution arm of VISULOX Portal and consists of multiple components (*VISULOX Core, NGINX, XPRA*), each using different protocolisation. The responsibility of the Connector is to implement communication with each component and execute Visulox Portal commands accordingly. Also, if a new component is added or replaced in future versions of the software, it is the responsibility of the Connector to build the bridge between the Portal and that component.
Visulox Portal Dashboard	Web-based management console for the Visulox Portal Service
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_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
Xpra	**Xpra** is an open-source multi-platform persistent remote display server and client for forwarding applications and desktop screens.

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**