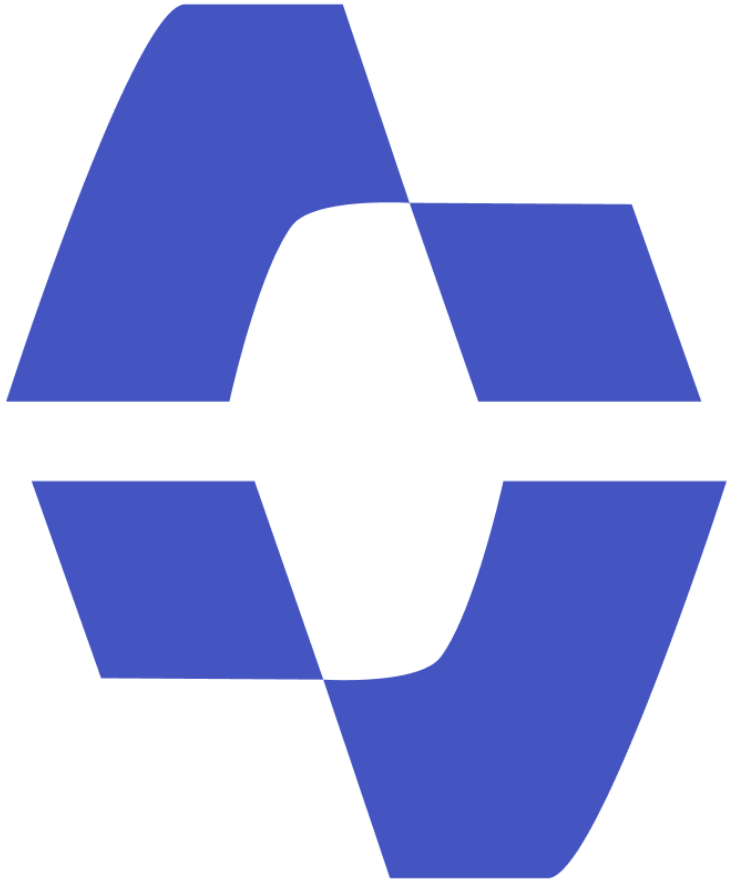
VISULOX 4

VISULOX4_AdminGuide

16.10.2026



visulox

Table of Contents

1 Preface 5
2 VISULOX Architecture 7
3 VISULOX Communication 15
4 VISULOX License 19
5 Configuration 24
6 VISULOX Command Line Interface (CLI) 37
7 Datasources 46
8 Login and Access Management 51
9 Application Configuration 60
10 VISULOX Cockpit 65
11 Events 73
12 Policies 76
13 Recording 81
14 VISULOX Player 86
15 Cooperations 88
16 Notifications 92

17 Reports 95
18 VISULOX Addons 98
19 Remote IP Detection 110
20 Monitoring & Logging 112
21 Exporting / Importing Data 118
22 Appendix_A 120
23 Appendix_Articles 191

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 Administration Guide** provides information about how to configure and administer this version of VISULOX. This document is intended for VISULOX Administrators.

1.1 How this manual is organized

Preface
Architecture, Communication, License, Configuration, Command Line Interface (CLI), Datasources, Login and Access Management, Application Configuration, Cockpit, Events, Policies, Recording, Player, Cooperations, Notifications, Reports, Addons, Remote IP Detection, Monitoring & Logging, Exporting / Importing Data
Reference Card
(4.3.3) Glossary

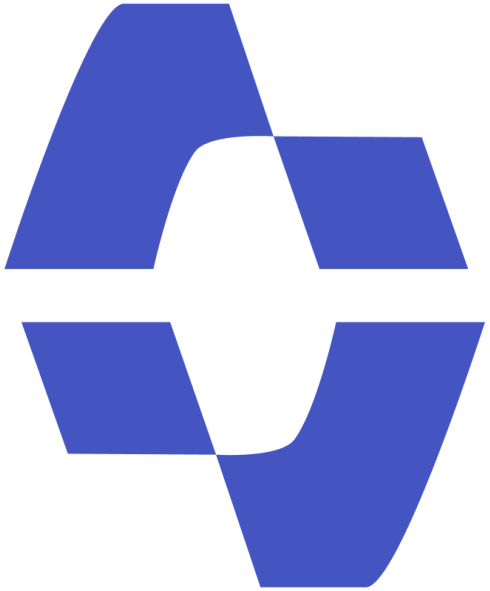
1.2 Legend

Useful information

Recommended setting

Warning / use with caution

Tipps & tricks



1.3 VISULOX documentation

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

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

1.4 Documentation feedback

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

2 VISULOX Architecture

The following articles describe the possible architectures and the setup of VISULOX environments.

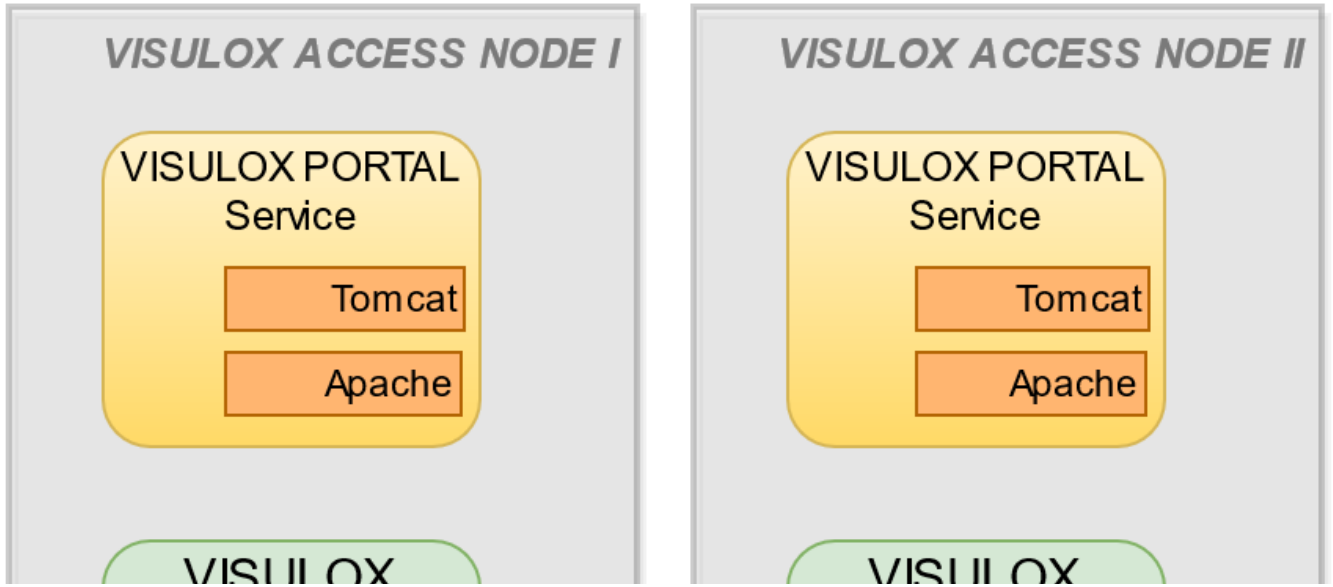
The VISULOX Service is an additional service to control and manage the VISULOX PORTAL Service. This is done by

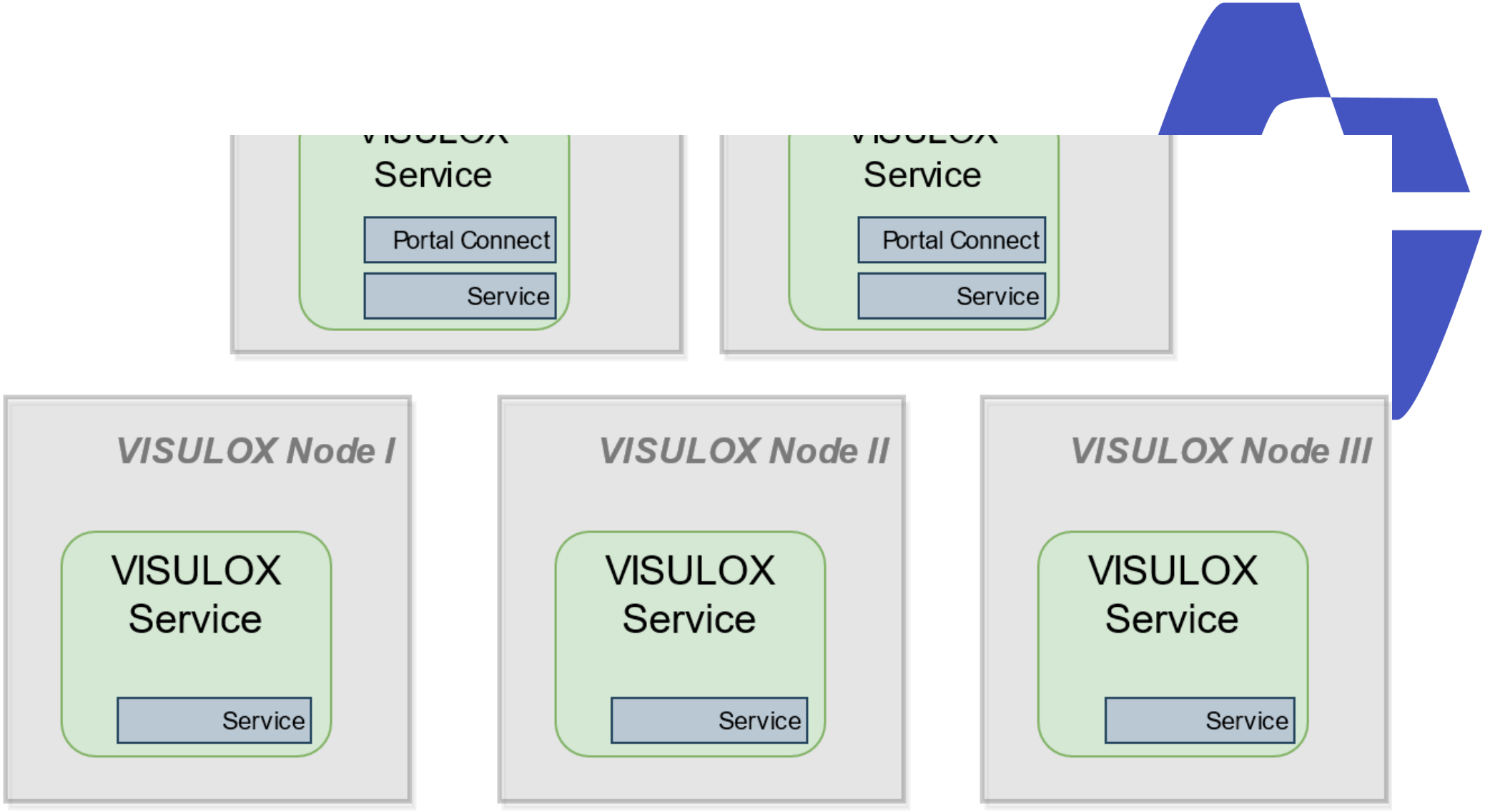
- using the VISULOX PORTAL webservices API
- adding registration from VISULOX PORTAL login interface to VISULOX
- modifying the VISULOX PORTAL webpages

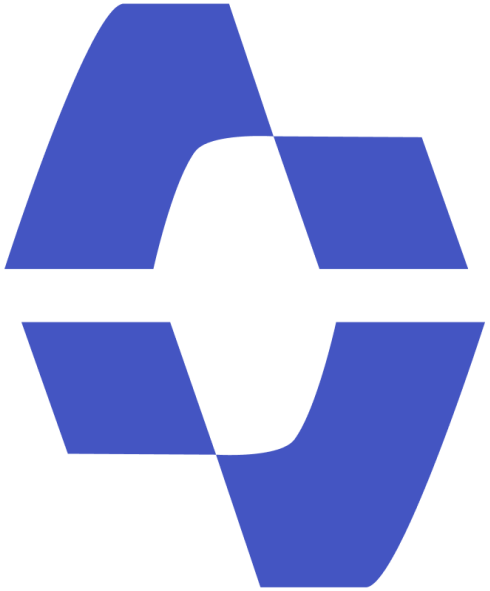
As a minimum requirement to control the VISULOX PORTAL Service, VISULOX Service has to be installed on any VISULOX Access Node.

Additional VISULOX Nodes can be provided for example as recorder or for VISULOX applications like VISULOX Cockpit, Firefox, Host Connect.

⚠ The VISULOX communication is dedicated to one interface.




Service
Portal Connect
Service
Service
Portal Connect
Service
VISULOX Node I
VISULOX
Service
Service
VISULOX Node II
VISULOX
Service
Service
VISULOX Node III
VISULOX
Service
Service



2.1 Available articles

(5.0.2) Visulox Node hierarchy

(5.0.2) Security information about vlxsu and vlxchown (SUID bit)

(5.0.2) Attaching Visulox Service to Visulox Portal Service

(5.0.2) Visulox layout of a node

(5.0.2) Visulox Architecture

(5.0.2) How to route a Visulox application to other nodes

(5.0.2) Visulox Portal Architecture

(5.0.2) Visulox Filestore

(5.0.2) Adding a Visulox Revision Server

(5.0.2) Visulox Cluster

(5.0.1) Adding a VISULOX Revision Server

(5.0.1) Security information about vlxsu and vlxchown (SUID bit)

(5.0.1) How to route a VISULOX application to other nodes

(5.0.1) VISULOX Node hierarchy

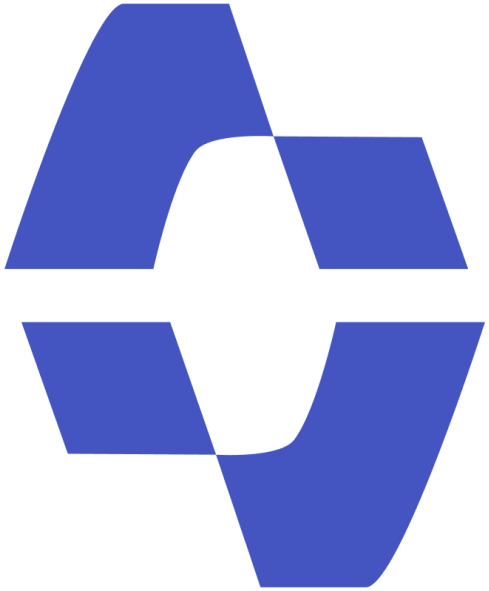
(5.0.1) VISULOX Filestore

(5.0.1) VISULOX Portal Architecture

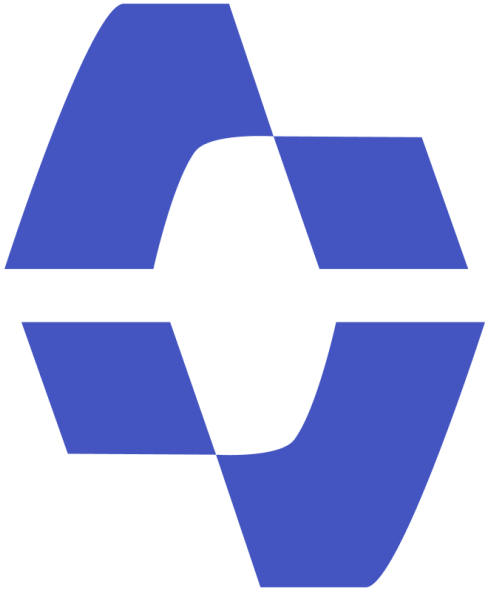
(5.0.1) VISULOX layout of a node

(5.0.1) Attaching VISULOX Service to VISULOX PORTAL Service

(5.0.1) VISULOX Cluster



(5.0.1) VISULOX Architecture
Visulox Portal Architecture
(4.2.0) How to route a VISULOX application to other nodes
(4.2.0) Gateway Session Balancing
(4.2.0) VISULOX Filestore
(4.2.0) VISULOX layout of a node
(4.2.0) VISULOX PORTAL Server Array
(4.2.0) Adding a VISULOX Revision Server
(4.2.0) Setup architecture
(4.2.0) VISULOX Cluster
(4.2.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.2.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.2.0) VISULOX Node hierarchy
(4.2.0) VISULOX Architecture
(4.2.0) Security information about vlxsu and vlxchown (SUID bit)
Visulox Node hierarchy
Visulox layout of a node
Visulox Cluster
How to route a Visulox application to other nodes
Adding a Visulox Revision Server
Visulox Filestore
Security information about vlxsu and vlxchown (SUID bit)



Attaching Visulox Service to Visulox Portal Service

Visulox Architecture

(4.3.2) VISULOX Architecture

(4.3.2) Setup architecture

(4.3.2) VISULOX Portal maintenance mode

(4.3.2) VISULOX Cluster

(4.3.2) VISULOX layout of a node

(4.3.2) VISULOX Node hierarchy

(4.3.2) How to route a VISULOX application to other nodes

(4.3.2) Adding a VISULOX Revision Server

(4.3.2) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

(4.3.2) Attaching VISULOX Service to VISULOX PORTAL Service

(4.3.2) Security information about vlxsu and vlxchown (SUID bit)

(4.3.2) VISULOX PORTAL Server Array

(4.3.2) VISULOX Filestore

(4.1.1) VISULOX Node hierarchy

(4.1.1) VISULOX Cluster

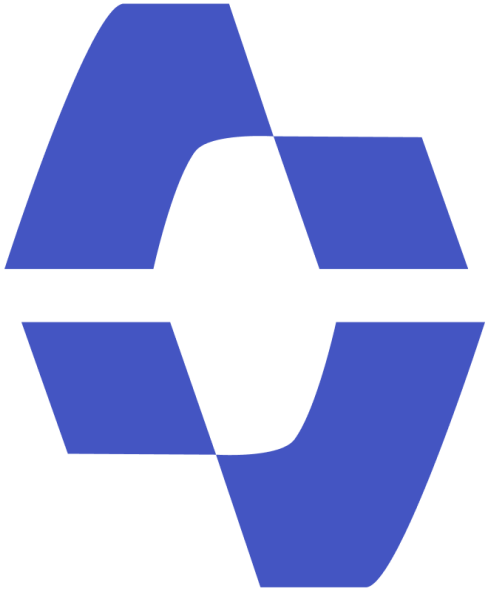
(4.1.1) VISULOX layout of a node

(4.1.1) Attaching VISULOX Service to VISULOX PORTAL Service

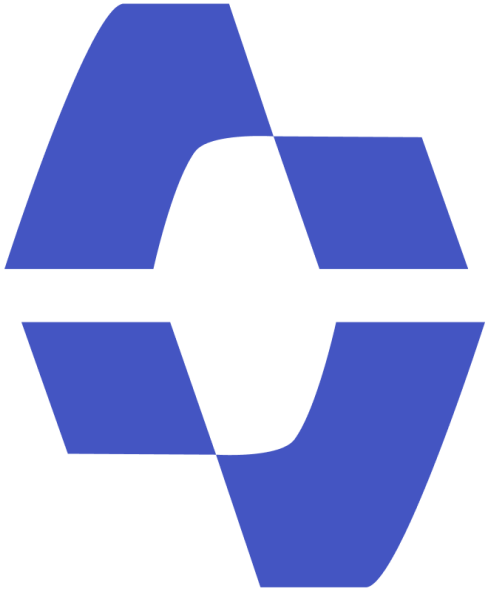
(4.1.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

(4.1.1) How to route a VISULOX application to other nodes

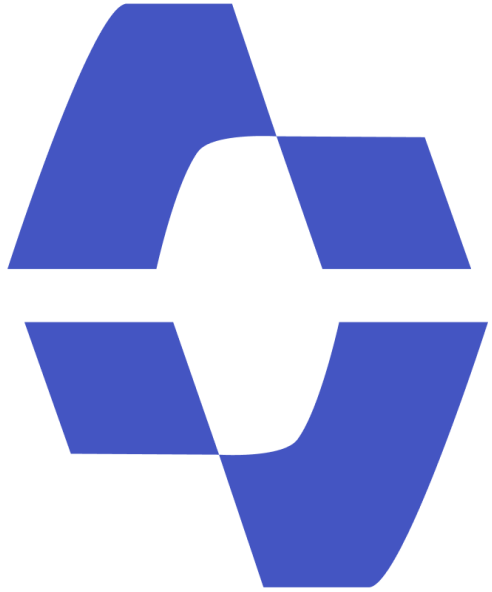
(4.1.1) Setup architecture



(4.1.1) Gateway Session Balancing
(4.1.1) VISULOX Filestore
(4.1.1) Adding a VISULOX Revision Server
(4.1.1) Security information about vlxsu and vlxchown (SUID bit)
(4.1.1) VISULOX PORTAL Server Array
(4.1.1) VISULOX Architecture
(4.3.1) Setup architecture
(4.3.1) VISULOX Portal maintenance mode
(4.3.1) VISULOX layout of a node
(4.3.1) How to route a VISULOX application to other nodes
(4.3.1) Adding a VISULOX Revision Server
(4.3.1) VISULOX Node hierarchy
(4.3.1) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.1) VISULOX Architecture
(4.3.1) Security information about vlxsu and vlxchown (SUID bit)
(4.3.1) VISULOX PORTAL Server Array
(4.3.1) VISULOX Cluster
(4.3.1) VISULOX Filestore
(4.3.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.0) VISULOX Cluster
(4.3.0) VISULOX Node hierarchy
(4.3.0) VISULOX Filestore



(4.3.0) Security information about vlxsu and vlxchown (SUID bit)
(4.3.0) VISULOX PORTAL Server Array
(4.3.0) VISULOX layout of a node
(4.3.0) How to route a VISULOX application to other nodes
(4.3.0) VISULOX Architecture
(4.3.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.0) Setup architecture
(4.3.0) VISULOX Portal maintenance mode
(4.3.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.0) Adding a VISULOX Revision Server
Setup architecture
VISULOX PORTAL Server Array
VISULOX Portal maintenance mode
How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
VISULOX Node hierarchy
VISULOX layout of a node
VISULOX Cluster
How to route a VISULOX application to other nodes
Adding a VISULOX Revision Server
VISULOX Filestore
Security information about vlxsu and vlxchown (SUID bit)
Attaching VISULOX Service to VISULOX PORTAL Service



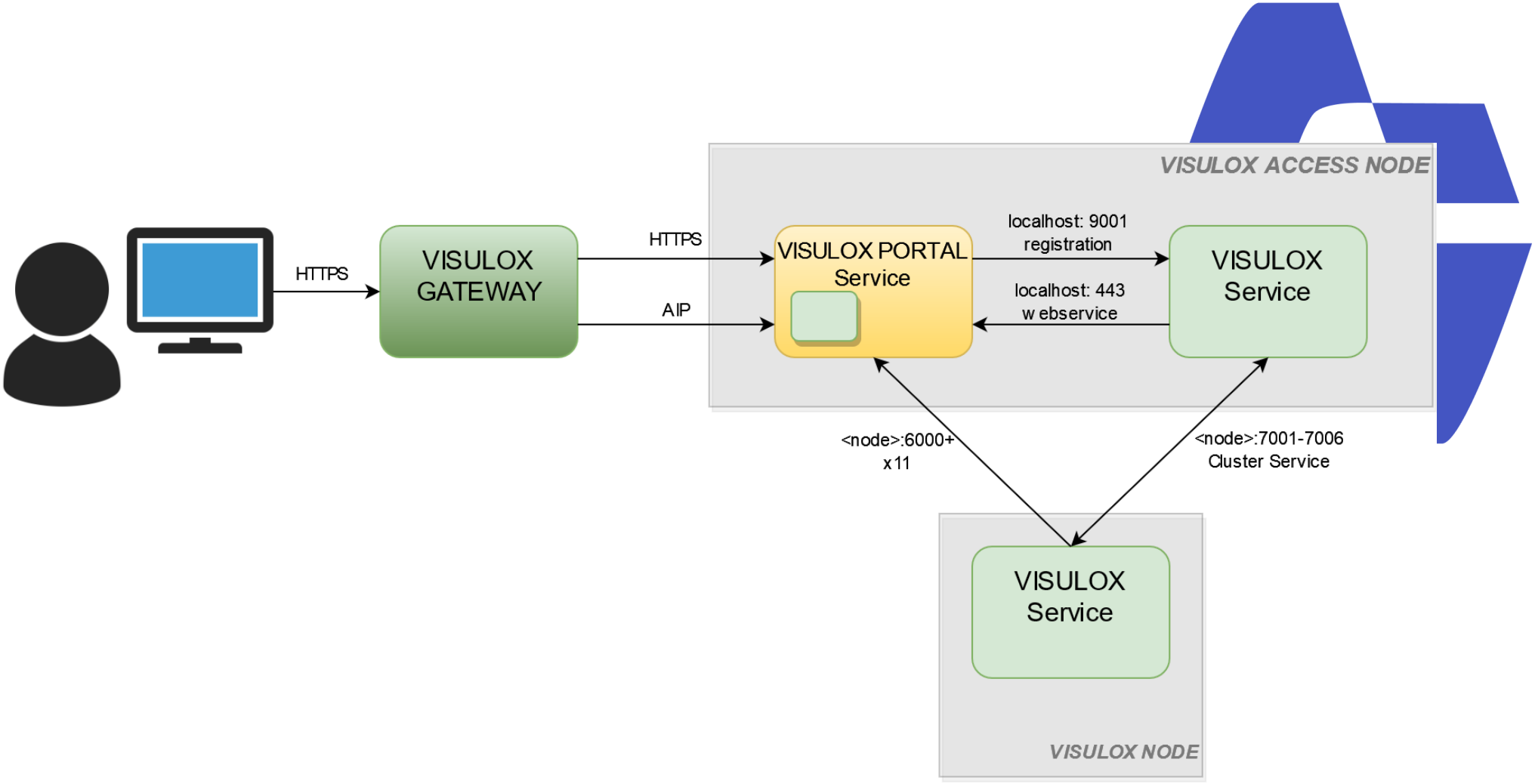
VISULOX Architecture
VISULOX layout of a node
VISULOX Node hierarchy
VISULOX Cluster
VISULOX Filestore
How to route a VISULOX application to other nodes
Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.3) Setup architecture
VISULOX Architecture
Adding a VISULOX Revision Server
How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
VISULOX PORTAL Server Array
Security information about vlxsu and vlxchown (SUID bit)
VISULOX Portal maintenance mode

3 VISULOX Communication

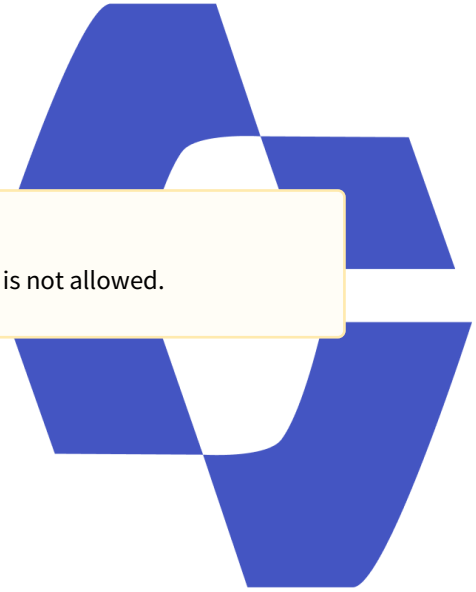
There are several communication paths **into**, **within** or **out** of a VISULOX system.

These articles describe the communication paths within the platform.

The articles are based on the standard communication parameters within the VISULOX PORTAL Service and VISULOX Service.



A firewall between nodes in the cluster (VISULOX Service and the VISULOX PORTAL Service) must be configured with the following setting "**session time out=never**".



Statement regarding **W**eb **A**pplication **F**irewall (**WAF**)
VISULOX supports the use of a Web Application Firewall, but currently only the HTML5 client is supported.
The Native Client cannot be used in conjunction with a WAF because a proprietary protocol is used via the HTTPS port and SSL offloading is not allowed.
Full support of a WAF is planned for future releases, so that VISULOX can be used behind a WAF without restrictions.

3.1 Available articles

(4.2.0) VISULOX Communication

(4.2.0) Network communication within VISULOX

(4.2.0) VISULOX SSH X11 Forwarding to VISULOX Application Nodes

(4.3.2) VISULOX SSH X11 Forwarding to VISULOX Application Nodes

(4.3.2) VISULOX Communication

(4.3.2) Network communication within VISULOX

(4.1.1) Network communication within VISULOX

(4.1.1) VISULOX Communication

(4.1.1) VISULOX SSH X11 Forwarding to VISULOX Application Nodes

(4.3.1) VISULOX SSH X11 Forwarding to VISULOX Application Nodes

(4.3.1) VISULOX Communication

(4.3.1) Network communication within VISULOX

(4.3.0) Network communication within VISULOX

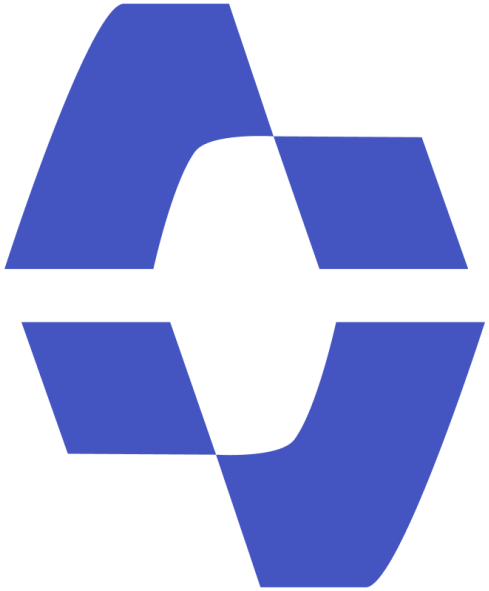
(4.3.0) VISULOX Communication

(4.3.0) VISULOX SSH X11 Forwarding to VISULOX Application Nodes

VISULOX SSH X11 Forwarding to VISULOX Application Nodes

Network communication within VISULOX

VISULOX Communication
Network communication within VISULOX
VISULOX SSH X11 Forwarding to VISULOX Application Nodes
VISULOX Communication



4 VISULOX License

4.1 Overview

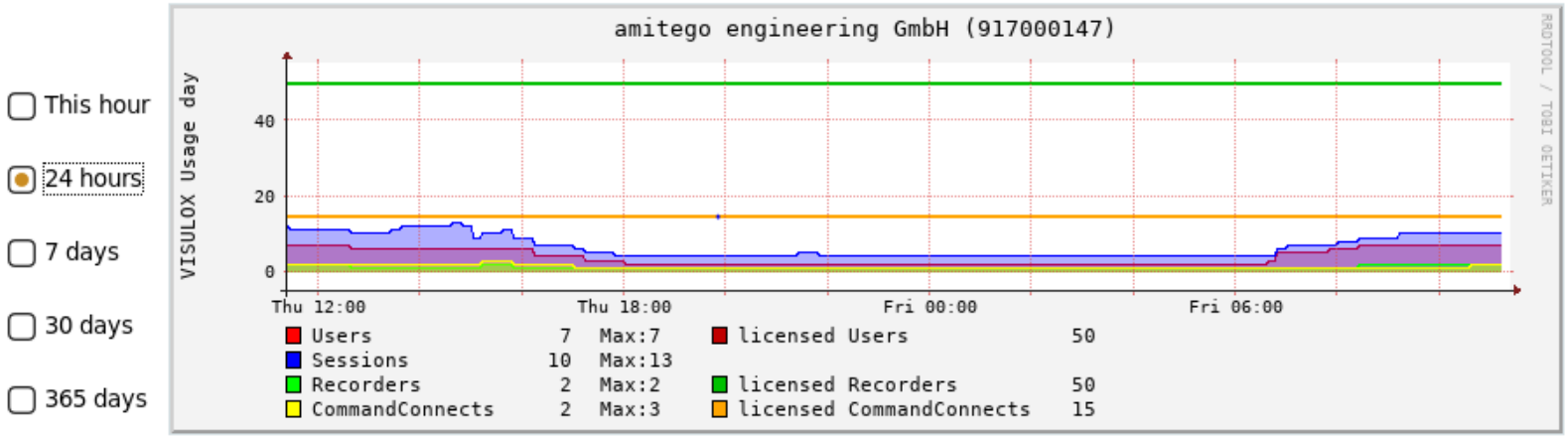
To use VISULOX a license is needed. The license can be tailored to the customer.

4.1.1 License control / impact

License	Control / impact
Base / Cluster	VISULOX Base Licence (one VISULOX Node) or VISULOX Cluster License (unlimited VISULOX Nodes).
Users	The number of users are controlled on startup of any VISULOX application (VISULOX Cockpit,, File Transfer, Cooperation). If more users are online than licensed, the VISULOX application can not be used any more. A warning message will be displayed.
Multi Factor Authentication	Multi Factor Authentication for users.
Session recorders	If the number of licensed recorders is reached during session control, the session will be locked and can not be used anymore (Manual recording is always possible).
OCR Keyword Detection	OCR component to detect configured keywords in applications.
Redact	Optional license for Redact Mode
Host Control	If the number of licensed Command Connects / Guards is reached, the session will be locked and can not be used anymore.

License	Control / impact
Revision Server	Optional license for a Revision Server (Archive Server).
Support & Maintenance	If the support and maintenance time is is reached, the environment should only be updated, when a new valid license is available within the next 21 days. In an environment with a license where support and maintenance (S&M) has expired, VISULOX can still be used as usual. Once an environment without S&M is updated to a newer VISULOX version a timer is set and displayed in the VISULOX Cockpit. After 21 days of running the new version, a valid license for the new version has to be installed. Without a valid license installed after 21 days access is no longer possible and the VISULOX Cockpit can not be used anymore. There is also the possibility that a license is set to **time limited**. With such a license VISULOX can no longer be used when support and maintenance (S&M) has expired.

A graph of the license usage is displayed in **VISULOX Cockpit / Cluster**:



A **Demo / Evaluation** license is available and valid for **10 days** including a VISULOX Base Node operating in total with **5** users, **5** session recorders and **2** Host Control applications.

A perpetual VISULOX License file is provided in a TAR archive from amitego. The license command understands this TAR file. There is no need to extract the tar files.

A perpetual VISULOX License file is provided by **amitego Sales & Service**. Contact: sales@amitego.com.

4.2 Installation / configuration of the license file

4.2.1 **Show the current license**

```
visulox license list
```

4.2.2 Check a provided license file

```
visulox license test -file <path to license file>
```

4.2.3 Replace the current installed license

```
visulox license replace -file <path to license file>
```

If a license is replaced on a node, it is replicated to all other nodes in the cluster.

If a new node is installed and attached to the VISULOX Cluster, it will get the license of the cluster. The Demo / Evaluation license is discarded.

If the tar archive can not be delivered to a customer via eMail, there is also the possibility to send the license as text XML/JSON to add it via copy & paste to STDN IN.

- visulox license replace -file - [RETURN]
- Copy & paste:

Base64 license hash in eMail:

```
- VISULOX License start
asdfsdfasdfasdfasdfasdfasdfasdfsadfasdfasdfasdfsadfasdfasdfasdfasdfasdff
asdasadasadasadasadasadasafdasfdasdafasdfdadfdaddafaddafadadfdadadfafdadfafa
sdgfhjsgdfjkashfjkghkaufghukahghukahghafdghaidghilafdhfgijgigfdahfghfduighuh
MX0gbXRhbiB7MX0gaGFzQ0cgezF9IG1vZHVsZXMge1ZMWDNBQywgMkZBLCBDR30gbGljZW5zYnVp
bGQgezE1MDM1NjA1NjJ9IEhBU0ggezE0NzNFQjJENTk2MjFGMDEyMTRFNkQ3MzhFM0EyQzA2fSBj
b21tYW5kY29ubmVjdHMgey0xfSBzbSB7MTUwMzQzOTasdarasdfadasdasdasd
-- VISULOX License end
```

- [RETURN]

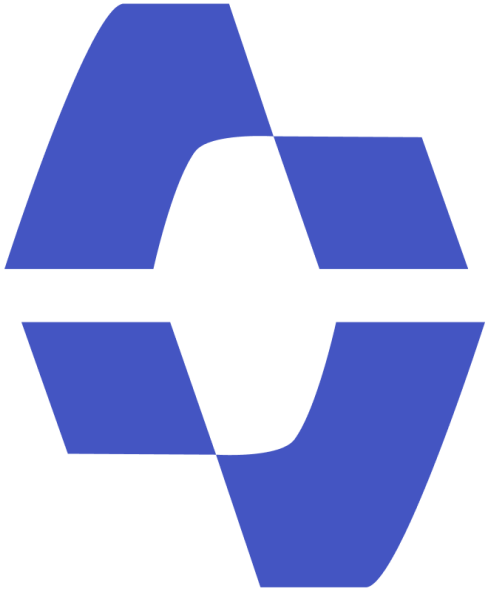
4.2.4 Get the usage of the installation

```
visulox license usage
```

Available parameters: **-component** <users|sessions|recorders|hostcontrols> **-unit** <week|month|year>

With these parameters the maximum usage of a component can be displayed in the unit.

⚠ After installing a new license a restart of the VISULOX Service is necessary!



5 Configuration

These articles describe how to configure a VISULOX environment in general.

5.1 Available articles

VISULOX Service

(4.1.1) Access Branding

(4.1.1) Application Configuration

(4.1.1) Configuration

(4.1.1) Custom vlxuser ID for transit users

(4.1.1) Enable events for VLX Shell, FreeRDP and File Transit connections

(4.1.1) General command line configuration

(4.1.1) How to assign a fixed username

(4.1.1) How to change the license name / banner

(4.1.1) How to change the VISULOX logos and colors

(4.1.1) How to configure FreeRDP for VISULOX PORTAL

(4.1.1) How to control the VISULOX Cockpit

(4.1.1) How to customize values in the database

(4.1.1) How to increase the log level

(4.1.1) How to setup MFA with SMS response from the SMS Provider

(4.1.1) How to use Unix user profiles

(4.1.1) How to use VISULOX on virtualized VMWare disks

(4.1.1) How to use VISULOX with multiple network cards

VISULOX PORTAL Service

(4.1.1) Attaching VISULOX Service to VISULOX PORTAL Service

(4.1.1) Gateway Session Balancing

(4.1.1) How to configure a user account as a group account

(4.1.1) How to configure FreeRDP for VISULOX PORTAL

(4.1.1) How to exclude single datastore users from import

(4.1.1) How to import users as VISULOX PORTAL administrators

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

(4.1.1) How to use an LDAP/AD or a Unix account to access the Webservice

(4.1.1) How to work with VISULOX Datasources

(4.1.1) Modify VISULOX PORTAL Datastore via CLI

(4.1.1) Printing configuration VISULOX Portal / application server

(4.1.1) Printing in VISULOX

(4.1.1) Security aspects

(4.1.1) VISULOX PORTAL application color depth

(4.1.1) VISULOX PORTAL ATTACH Command

(4.1.1) VISULOX PORTAL Console

(4.1.1) VISULOX PORTAL Server Array

(4.1.1) VISULOX-GATEWAY Command

(4.1.1) VISULOX-PORTAL Command

(4.1.1) How to work with VISULOX Datasources
(4.1.1) Login page configuration options
(4.1.1) Manual restart of a missing VISULOX service
(4.1.1) Printing configuration VISULOX Portal / application server
(4.1.1) Printing in VISULOX
(4.1.1) Starting VISULOX Cockpit with parameter -grant
(4.1.1) VISULOX Certificates
(4.1.1) VISULOX Cluster
(4.1.1) VISULOX disk space protection
(4.1.1) VISULOX Filestore
(4.1.1) VISULOX layout of a node
(4.1.1) VISULOX Lifetimes
(4.1.1) VISULOX Node hierarchy
(4.1.1) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.2.0) Access Branding
(4.2.0) Application Configuration
(4.2.0) Configuration
(4.2.0) Customizable action buttons in VISULOX Cockpit / Objects
(4.2.0) Disable Workspace elements
(4.2.0) Enable events for VLX Shell, FreeRDP and File Transit connections
(4.2.0) Extended VISULOX PORTAL Service commands
(4.1.1) VISULOX-PORTAL OBJECT Command
(4.2.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.2.0) Extended VISULOX PORTAL Service commands
(4.2.0) Gateway Session Balancing
(4.2.0) How to configure a user account as a group account
(4.2.0) How to configure FreeRDP for VISULOX PORTAL
(4.2.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.2.0) How to exclude single datastore users from import
(4.2.0) How to import users as VISULOX PORTAL administrators
(4.2.0) How to setup a standard form contract to commit on login (consent)
(4.2.0) How to work with VISULOX Datasources
(4.2.0) Modify VISULOX PORTAL Datastore via CLI
(4.2.0) Printing in VISULOX
(4.2.0) VISULOX PORTAL application color depth
(4.2.0) VISULOX PORTAL ATTACH Command
(4.2.0) VISULOX PORTAL Console
(4.2.0) VISULOX-PORTAL Command
(4.3.0) 3rdParty configuration parameters
(4.3.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.0) CORS adjustment on VISULOX Gateway
(4.3.0) Custom application icons
(4.3.0) How to configure a user account as a group account

(4.2.0) General command line configuration
(4.2.0) How to assign a fixed username
(4.2.0) How to change the license name / banner
(4.2.0) How to change the VISULOX logos and colors
(4.2.0) How to configure FreeRDP for VISULOX PORTAL
(4.2.0) How to control the VISULOX Cockpit
(4.2.0) How to customize values in the database
(4.2.0) How to increase the log level
(4.2.0) How to route a VISULOX application to other nodes
(4.2.0) How to setup MFA with SMS response from the SMS Provider
(4.2.0) How to use Unix user profiles
(4.2.0) How to use VISULOX on virtualized VMWare disks
(4.2.0) How to use VISULOX with multiple network cards
(4.2.0) How to work with VISULOX Datasources
(4.2.0) Login page configuration options
(4.2.0) Manual restart of a missing VISULOX service
(4.2.0) Printing in VISULOX
(4.2.0) VISULOX Cluster
(4.2.0) VISULOX disk space protection
(4.2.0) VISULOX Filestore
(4.2.0) VISULOX layout of a node
(4.2.0) VISULOX Node hierarchy
(4.3.0) How to configure FreeRDP for VISULOX PORTAL
(4.3.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.0) How to exclude single datastore users from import
(4.3.0) How to import users as VISULOX PORTAL administrators
(4.3.0) How to setup a standard form contract to commit on login (consent)
(4.3.0) How to setup keepalived
(4.3.0) How to work with VISULOX Datasources
(4.3.0) Modify VISULOX PORTAL Datastore via CLI
(4.3.0) Printing configuration VISULOX Portal / application server
(4.3.0) Security aspects
(4.3.0) VISULOX PORTAL application color depth
(4.3.0) VISULOX PORTAL ATTACH Command
(4.3.0) VISULOX PORTAL Console
(4.3.0) VISULOX Portal maintenance mode
(4.3.0) VISULOX-GATEWAY Command
(4.3.0) VISULOX-PORTAL Command
(4.3.0) VISULOX-PORTAL OBJECT Command
(4.3.0) Web server basic authentication with VISULOX
(4.3.1) 3rdParty configuration parameters
(4.3.1) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.1) Browser agent switch for TCC file or URL call
(4.3.1) CORS adjustment on VISULOX Gateway

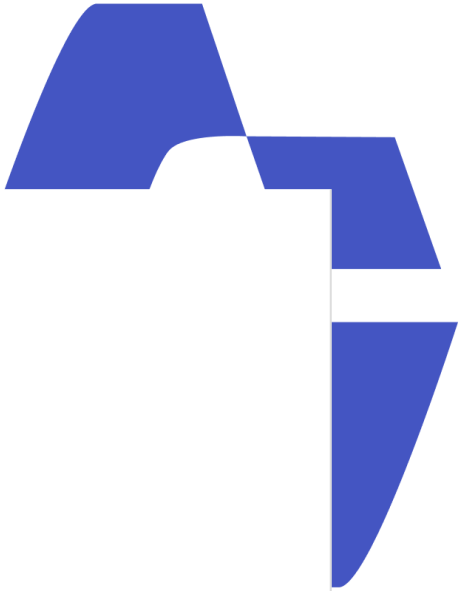
(4.2.0) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.2.0) VISULOX Webservice
(4.3.0) 3rdParty configuration parameters
(4.3.0) Access Branding
(4.3.0) Application Configuration
(4.3.0) Configuration
(4.3.0) Enable events for VLX Shell, FreeRDP and File Transit connections
(4.3.0) General command line configuration
(4.3.0) How to assign a fixed username
(4.3.0) How to change the license name / banner
(4.3.0) How to change the VISULOX logos and colors
(4.3.0) How to configure FreeRDP for VISULOX PORTAL
(4.3.0) How to control the VISULOX Cockpit
(4.3.0) How to customize values in the database
(4.3.0) How to setup MFA with SMS response from the SMS Provider
(4.3.0) How to use Unix user profiles
(4.3.0) How to use VISULOX on virtualized VMWare disks
(4.3.0) How to use VISULOX with multiple network cards
(4.3.0) How to work with VISULOX Datasources
(4.3.0) Login page configuration options
(4.3.1) Custom application icons
(4.3.1) Extended VISULOX PORTAL Service commands
(4.3.1) How to change the VISULOX Portal Favicon
(4.3.1) How to configure a user account as a group account
(4.3.1) How to configure FreeRDP for VISULOX PORTAL
(4.3.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.1) How to disable indexing by search engines
(4.3.1) How to exclude single datastore users from import
(4.3.1) How to import users as VISULOX PORTAL administrators
(4.3.1) How to setup a standard form contract to commit on login (consent)
(4.3.1) How to setup keepalived
(4.3.1) How to use an LDAP/AD or Unix account to access the webservice
(4.3.1) How to work with VISULOX Datasources
(4.3.1) Modify VISULOX PORTAL Datastore via CLI
(4.3.1) Printing configuration VISULOX Portal / application server
(4.3.1) Printing in VISULOX
(4.3.1) Security aspects
(4.3.1) VISULOX PORTAL application color depth
(4.3.1) VISULOX PORTAL ATTACH Command
(4.3.1) VISULOX PORTAL Console
(4.3.1) VISULOX Portal maintenance mode
(4.3.1) VISULOX PORTAL Server Array

(4.3.0) Manual restart of a missing VISULOX service
(4.3.0) Microsoft LAPS integration
(4.3.0) Object ID
(4.3.0) Printing configuration VISULOX Portal / application server
(4.3.0) VISULOX Cluster
(4.3.0) VISULOX database backup, restore and performance
(4.3.0) VISULOX disk space protection
(4.3.0) VISULOX Filestore
(4.3.0) VISULOX layout of a node
(4.3.0) VISULOX Lifetimes
(4.3.0) VISULOX Node hierarchy
(4.3.0) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.3.1) 3rdParty configuration parameters
(4.3.1) Access Branding
(4.3.1) Application Configuration
(4.3.1) Browser agent switch for TCC file or URL call
(4.3.1) Configuration
(4.3.1) Custom vlxuser ID for transit users
(4.3.1) Customizable action buttons in VISULOX Cockpit / Objects
(4.3.1) Disable Workspace elements
(4.3.1) Enable events for VLX Shell, FreeRDP and File Transit connections
(4.3.1) VISULOX-GATEWAY Command
(4.3.1) VISULOX-PORTAL Command
(4.3.1) VISULOX-PORTAL OBJECT Command
(4.3.1) Web server basic authentication with VISULOX
(4.3.2) 3rdParty configuration parameters
(4.3.2) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.2) Browser agent switch for TCC file or URL call
(4.3.2) CORS adjustment on VISULOX Gateway
(4.3.2) Custom application icons
(4.3.2) Extended VISULOX PORTAL Service commands
(4.3.2) How to change the VISULOX Portal Favicon
(4.3.2) How to configure a user account as a group account
(4.3.2) How to configure FreeRDP for VISULOX PORTAL
(4.3.2) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.2) How to disable indexing by search engines
(4.3.2) How to exclude single datastore users from import
(4.3.2) How to import users as VISULOX PORTAL administrators
(4.3.2) How to setup a standard form contract to commit on login (consent)
(4.3.2) How to setup keepalived
(4.3.2) How to use an LDAP/AD or Unix account to access the webservice
(4.3.2) How to work with VISULOX Datasources
(4.3.2) Modify VISULOX PORTAL Datastore via CLI

(4.3.1) Extended VISULOX PORTAL Service commands
(4.3.1) General command line configuration
(4.3.1) How to assign a fixed username
(4.3.1) How to change the license name / banner
(4.3.1) How to change the VISULOX logos and colors
(4.3.1) How to change the VISULOX Portal Favicon
(4.3.1) How to check Policy, Datastore and LDAP assignments
(4.3.1) How to configure FreeRDP for VISULOX PORTAL
(4.3.1) How to control the VISULOX Cockpit
(4.3.1) How to customize values in the database
(4.3.1) How to increase the log level
(4.3.1) How to route a VISULOX application to other nodes
(4.3.1) How to setup MFA with SMS response from the SMS Provider
(4.3.1) How to use Unix user profiles
(4.3.1) How to use VISULOX on virtualized VMWare disks
(4.3.1) How to use VISULOX with multiple network cards
(4.3.1) How to work with VISULOX Datasources
(4.3.1) Login check against an external system
(4.3.1) Login page configuration options
(4.3.1) Manual restart of a missing VISULOX service
(4.3.1) Microsoft LAPS integration
(4.3.1) Object ID
(4.3.2) Printing configuration VISULOX Portal / application server
(4.3.2) Printing in VISULOX
(4.3.2) Secure HTTP Gateway headers
(4.3.2) VISULOX PORTAL application color depth
(4.3.2) VISULOX PORTAL ATTACH Command
(4.3.2) VISULOX PORTAL Console
(4.3.2) VISULOX Portal maintenance mode
(4.3.2) VISULOX PORTAL Server Array
(4.3.2) VISULOX-GATEWAY Command
(4.3.2) VISULOX-PORTAL Command
(4.3.2) VISULOX-PORTAL OBJECT Command
(4.3.2) Web server basic authentication with VISULOX
3rdParty configuration parameters
Attaching VISULOX Service to VISULOX PORTAL Service
Browser agent switch for TCC file or URL call
CORS adjustment on VISULOX Gateway
Custom application icons
Extended VISULOX PORTAL Service commands
How to change the VISULOX Portal Favicon
How to configure a user account as a group account
How to configure FreeRDP for VISULOX PORTAL
How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

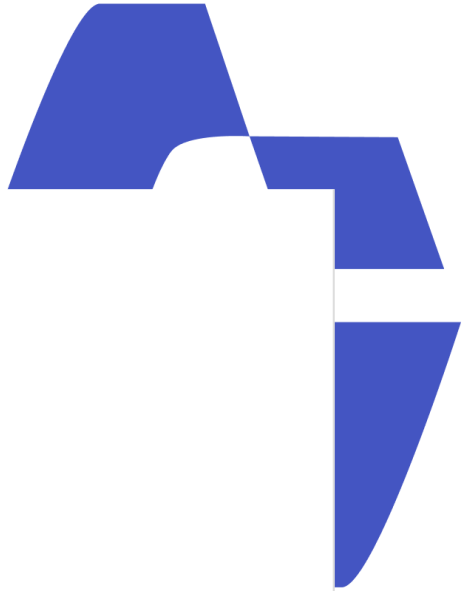
(4.3.1) Printing configuration VISULOX Portal / application server
(4.3.1) Printing in VISULOX
(4.3.1) Recorder configuration
(4.3.1) RSA SecureID Implementation via RSA API
(4.3.1) Starting VISULOX Cockpit with parameter -grant
(4.3.1) VISULOX Certificates
(4.3.1) VISULOX Cluster
(4.3.1) VISULOX database backup, restore and performance
(4.3.1) VISULOX disk space protection
(4.3.1) VISULOX Filestore
(4.3.1) VISULOX layout of a node
(4.3.1) VISULOX Lifetimes
(4.3.1) VISULOX Node hierarchy
(4.3.1) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.3.1) VISULOX Webservice
(4.3.2) 3rdParty configuration parameters
(4.3.2) Access Branding
(4.3.2) Access termination enforced
(4.3.2) Application Configuration
(4.3.2) Browser agent switch for TCC file or URL call
(4.3.2) Configuration
(4.3.2) Custom vlxuser ID for transit users
How to disable indexing by search engines
How to exclude single datastore users from import
How to import users as VISULOX PORTAL administrators
How to setup a standard form contract to commit on login (consent)
How to setup keepalived
How to use an LDAP/AD or Unix account to access the webservice
How to work with VISULOX Datasources
Modify VISULOX PORTAL Datastore via CLI
Printing configuration VISULOX Portal / application server
Printing in VISULOX
Secure HTTP Gateway headers
VISULOX PORTAL application color depth
(4.3.3) VISULOX PORTAL ATTACH Command
VISULOX PORTAL Console
VISULOX Portal maintenance mode
VISULOX PORTAL Server Array
(4.3.3) VISULOX-GATEWAY Command
(4.3.3) VISULOX-PORTAL Command
(4.3.3) VISULOX-PORTAL OBJECT Command
Web server basic authentication with VISULOX
(4.1.1) CORS adjustment on VISULOX Gateway
(4.1.1) Custom application icons

(4.3.2) Customizable action buttons in VISULOX Cockpit / Objects
(4.3.2) Disable Workspace elements
(4.3.2) Enable events for VLX Shell, FreeRDP and File Transit connections
(4.3.2) Extended VISULOX PORTAL Service commands
(4.3.2) General command line configuration
(4.3.2) How to assign a fixed username
(4.3.2) How to change the license name / banner
(4.3.2) How to change the VISULOX logos and colors
(4.3.2) How to change the VISULOX Portal Favicon
(4.3.2) How to check Policy, Datastore and LDAP assignments
(4.3.2) How to configure FreeRDP for VISULOX PORTAL
(4.3.2) How to control the VISULOX Cockpit
(4.3.2) How to customize values in the database
(4.3.2) How to increase the log level
(4.3.2) How to route a VISULOX application to other nodes
(4.3.2) How to setup MFA with SMS response from the SMS Provider
(4.3.2) How to use Unix user profiles
(4.3.2) How to use VISULOX on virtualized VMWare disks
(4.3.2) How to use VISULOX with multiple network cards
(4.3.2) How to work with VISULOX Datasources
(4.3.2) Login check against an external system
(4.1.1) Extended VISULOX PORTAL Service commands
(4.1.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.1.1) How to disable indexing by search engines
(4.1.1) How to setup keepalived
(4.2.0) CORS adjustment on VISULOX Gateway
(4.2.0) Custom application icons
(4.2.0) How to disable indexing by search engines
(4.2.0) How to setup keepalived
(4.2.0) How to use an LDAP/AD or Unix account to access the webservice
(4.2.0) Printing configuration VISULOX Portal / application server
(4.2.0) Security aspects
(4.2.0) VISULOX PORTAL Server Array
(4.2.0) VISULOX-GATEWAY Command
(4.2.0) VISULOX-PORTAL OBJECT Command
(4.3.0) Browser agent switch for TCC file or URL call
(4.3.0) Extended VISULOX PORTAL Service commands
(4.3.0) How to change the VISULOX Portal Favicon
(4.3.0) How to disable indexing by search engines
(4.3.0) How to use an LDAP/AD or Unix account to access the webservice
(4.3.0) Printing in VISULOX
(4.3.0) VISULOX PORTAL Server Array
3rdParty configuration parameters

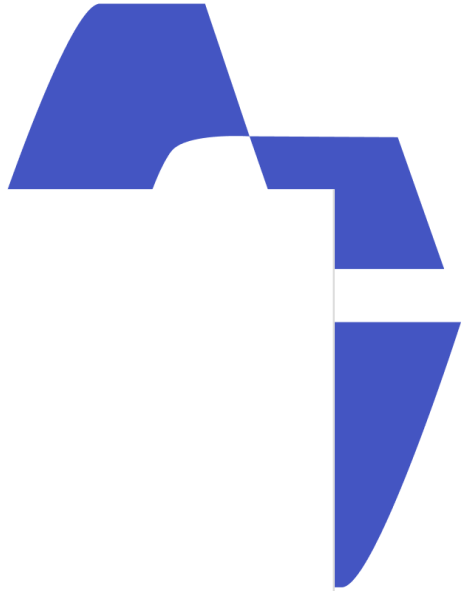


(4.3.2) Login page configuration options
(4.3.2) Manual restart of a missing VISULOX service
(4.3.2) Microsoft LAPS integration
(4.3.2) Object ID
(4.3.2) Printing configuration VISULOX Portal / application server
(4.3.2) Printing in VISULOX
(4.3.2) Recorder configuration
(4.3.2) RSA SecureID Implementation via RSA API
(4.3.2) Starting VISULOX Cockpit with parameter -grant
(4.3.2) VISULOX Certificates
(4.3.2) VISULOX Cluster
(4.3.2) VISULOX database backup, restore and performance
(4.3.2) VISULOX disk space protection
(4.3.2) VISULOX Filestore
(4.3.2) VISULOX layout of a node
(4.3.2) VISULOX Lifetimes
(4.3.2) VISULOX Node hierarchy
(4.3.2) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.3.2) VISULOX Webservice
3rdParty configuration parameters
Access Branding
Access termination enforced
Attaching VISULOX Service to VISULOX PORTAL Service
Browser agent switch for TCC file or URL call
CORS adjustment on VISULOX Gateway
Custom application icons
Extended VISULOX PORTAL Service commands
How to change the VISULOX Portal Favicon
How to configure a user account as a group account
How to configure FreeRDP for VISULOX PORTAL
How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
How to disable indexing by search engines
How to exclude single datastore users from import
How to import users as VISULOX PORTAL administrators
How to setup a standard form contract to commit on login (consent)
How to setup keepalived
How to use an LDAP/AD or Unix account to access the webservice
How to work with VISULOX Datasources
Modify VISULOX PORTAL Datastore via CLI
Printing configuration VISULOX Portal / application server
Printing in VISULOX
Secure HTTP Gateway headers
VISULOX PORTAL application color depth
VISULOX PORTAL ATTACH Command

Application Configuration
Browser agent switch for TCC file or URL call
Configuration
Custom vlxuser ID for transit users
Customizable action buttons in VISULOX Cockpit / Objects
Disable Workspace elements
Enable events for VLX Shell, FreeRDP and File Transit connections
Extended VISULOX PORTAL Service commands
General command line configuration
How to assign a fixed username
How to change the license name / banner
How to change the VISULOX logos and colors
How to change the VISULOX Portal Favicon
How to check Policy, Datastore and LDAP assignments
How to configure FreeRDP for VISULOX PORTAL
How to control the VISULOX Cockpit
How to customize values in the database
How to increase the log level
How to route a VISULOX application to other nodes
How to setup MFA with SMS response from the SMS Provider
How to use Unix user profiles
How to use VISULOX on virtualized VMWare disks
VISULOX PORTAL Console
VISULOX Portal maintenance mode
VISULOX PORTAL Server Array
VISULOX-GATEWAY Command
VISULOX-PORTAL Command
VISULOX-PORTAL OBJECT Command
Web server basic authentication with VISULOX



How to use VISULOX with multiple network cards
How to work with VISULOX Datasources
Login check against an external system
Login page configuration options
Manual restart of a missing VISULOX service
Microsoft LAPS integration
Object ID
Printing configuration VISULOX Portal / application server
Printing in VISULOX
Recorder configuration
RSA SecureID Implementation via RSA API
Starting VISULOX Cockpit with parameter -grant
VISULOX Certificates
VISULOX Cluster
VISULOX database backup, restore and performance
VISULOX disk space protection
VISULOX Filestore
VISULOX layout of a node
VISULOX Lifetimes
VISULOX Node hierarchy
VISULOX SSH X11 Forwarding to VISULOX Application Nodes
VISULOX Webservice



(4.1.1) Customizable action buttons in VISULOX Cockpit / Objects
(4.1.1) Disable Workspace elements
(4.1.1) Extended VISULOX PORTAL Service commands
(4.1.1) How to check Policy, Datastore and LDAP assignments
(4.1.1) How to route a VISULOX application to other nodes
(4.1.1) Login check against an external system
(4.1.1) Microsoft LAPS integration
(4.1.1) Object ID
(4.1.1) Recorder configuration
(4.1.1) RSA SecureID Implementation via RSA API
(4.1.1) VISULOX database backup, restore and performance
(4.1.1) VISULOX Webservice
(4.2.0) Custom vlxuser ID for transit users
(4.2.0) How to check Policy, Datastore and LDAP assignments
(4.2.0) Login check against an external system
(4.2.0) Microsoft LAPS integration
(4.2.0) Object ID
(4.2.0) Printing configuration VISULOX Portal / application server

6 VISULOX Command Line Interface (CLI)

These articles describe how to control VISULOX from the command line.

Nearly all settings that can be configured in the VISULOX Cockpit GUI can also be set via the VISULOX Command Line Interface (e.g. Policies, Addons, Cockpit roles, etc.).

6.1 Available articles

General

(4.1.1) Command "visulox support" - Creating a VISULOX Support Report
(4.1.1) General command line configuration
(4.1.1) How to work with VISULOX Datasources
(4.1.1) VISULOX Command
(4.1.1) VISULOX PORTAL ATTACH Command
(4.1.1) VISULOX-GATEWAY Command
(4.1.1) VISULOX-PORTAL Command
(4.1.1) VISULOX-PORTAL OBJECT Command
(4.2.0) Command "visulox support" - Creating a VISULOX Support Report
(4.2.0) General command line configuration
(4.2.0) How to work with VISULOX Datasources
(4.2.0) VISULOX Command
(4.2.0) VISULOX PORTAL ATTACH Command
(4.2.0) VISULOX-PORTAL Command
(4.3.0) Command "visulox support" - Creating a VISULOX Support Report
(4.3.0) General command line configuration
(4.3.0) How to work with VISULOX Datasources
(4.3.0) Integrity-Check
(4.3.0) Object ID

Policies

(4.1.1) How to control access from the command line
(4.1.1) How to control groupaccess from the command line
(4.2.0) How to control access from the command line
(4.2.0) How to control applications from the command line
(4.2.0) How to control external messages from the command line
(4.2.0) How to control File Transit Policy from the command line
(4.2.0) How to control groupaccess from the command line
(4.2.0) How to control login from the command line
(4.3.0) How to control access from the command line
(4.3.0) How to control groupaccess from the command line
(4.3.0) How to control internal messages from the command line
(4.3.1) How to control access from the command line
(4.3.1) How to control applications from the command line
(4.3.1) How to control external messages from the command line
(4.3.1) How to control File Transit Policy from the command line
(4.3.1) How to control groupaccess from the command line
(4.3.1) How to control internal messages from the command line
(4.3.1) How to control login from the command line
(4.3.2) How to control access from the command line

(4.3.0) VISULOX Command
(4.3.0) VISULOX PORTAL ATTACH Command
(4.3.0) VISULOX-GATEWAY Command
(4.3.0) VISULOX-PORTAL Command
(4.3.0) VISULOX-PORTAL OBJECT Command
(4.3.1) Command "visulox support" - Creating a VISULOX Support Report
(4.3.1) General command line configuration
(4.3.1) How to check Policy, Datastore and LDAP assignments
(4.3.1) How to work with VISULOX Datasources
(4.3.1) Integrity-Check
(4.3.1) Object ID
(4.3.1) VISULOX Command
(4.3.1) VISULOX PORTAL ATTACH Command
(4.3.1) VISULOX-GATEWAY Command
(4.3.1) VISULOX-PORTAL Command
(4.3.1) VISULOX-PORTAL OBJECT Command
(4.3.2) Command "visulox support" - Creating a VISULOX Support Report
(4.3.2) General command line configuration
(4.3.2) How to check Policy, Datastore and LDAP assignments
(4.3.2) How to work with VISULOX Datasources
(4.3.2) Integrity-Check
(4.3.2) Object ID
(4.3.2) How to control applications from the command line
(4.3.2) How to control external messages from the command line
(4.3.2) How to control File Transit Policy from the command line
(4.3.2) How to control groupaccess from the command line
(4.3.2) How to control internal messages from the command line
(4.3.2) How to control login from the command line
How to control access from the command line
How to control applications from the command line
How to control external messages from the command line
How to control File Transit Policy from the command line
How to control groupaccess from the command line
How to control internal messages from the command line
How to control login from the command line
(4.1.1) How to control applications from the command line
(4.1.1) How to control external messages from the command line
(4.1.1) How to control File Transit Policy from the command line
(4.1.1) How to control internal messages from the command line
(4.1.1) How to control login from the command line
(4.2.0) How to control internal messages from the command line
(4.3.0) How to control applications from the command line
(4.3.0) How to control external messages from the command line
(4.3.0) How to control File Transit Policy from the command line

(4.3.2) VISULOX Command
(4.3.2) VISULOX PORTAL ATTACH Command
(4.3.2) VISULOX-GATEWAY Command
(4.3.2) VISULOX-PORTAL Command
(4.3.2) VISULOX-PORTAL OBJECT Command
Command "visulox support" - Creating a VISULOX Support Report
General command line configuration
How to check Policy, Datastore and LDAP assignments
How to work with VISULOX Datasources
Integrity-Check
Object ID
(4.3.3) VISULOX Command
(4.3.3) VISULOX PORTAL ATTACH Command
(4.3.3) VISULOX-GATEWAY Command
(4.3.3) VISULOX-PORTAL Command
(4.3.3) VISULOX-PORTAL OBJECT Command
(4.1.1) How to check Policy, Datastore and LDAP assignments
(4.1.1) Integrity-Check
(4.1.1) Object ID
(4.2.0) How to check Policy, Datastore and LDAP assignments
(4.2.0) Integrity-Check
(4.2.0) Object ID
(4.3.0) How to control login from the command line
How to control access from the command line
How to control applications from the command line
How to control external messages from the command line
How to control File Transit Policy from the command line
How to control groupaccess from the command line
How to control internal messages from the command line
How to control login from the command line

Misc

(4.1.1) Command "visulox log" - Analyzing log files
(4.1.1) How to control OTP from the command line
(4.1.1) How to control passcache from the command line
(4.1.1) How to control Password Management from the command line
(4.1.1) How to control reports from the command line
(4.1.1) How to export information from VISULOX on the command line
(4.1.1) Modify VISULOX PORTAL Datastore via CLI
(4.1.1) Setting the min/max length for messages, contents and comments
(4.2.0) Command "visulox log" - Analyzing log files
(4.2.0) How to configure input idle detection
(4.2.0) How to control OTP from the command line
(4.2.0) How to control passcache from the command line

(4.2.0) VISULOX-GATEWAY Command
(4.2.0) VISULOX-PORTAL OBJECT Command
(4.3.0) How to check Policy, Datastore and LDAP assignments
Command "visulox support" - Creating a VISULOX Support Report
General command line configuration
How to check Policy, Datastore and LDAP assignments
How to work with VISULOX Datasources
Integrity-Check
Object ID
VISULOX Command
VISULOX PORTAL ATTACH Command
VISULOX-GATEWAY Command
VISULOX-PORTAL Command
VISULOX-PORTAL OBJECT Command

Admin

(4.1.1) How to control action scripts from the command line
(4.1.1) How to control Cockpit roles from the command line
(4.1.1) How to control mailinggroups from the command line
(4.1.1) How to control messages from the command line
(4.2.0) How to control action scripts from the command line
(4.2.0) How to control Cockpit roles from the command line
(4.2.0) How to control Password Management from the command line
(4.2.0) How to control reports from the command line
(4.2.0) How to export information from VISULOX on the command line
(4.2.0) Modify VISULOX PORTAL Datastore via CLI
(4.2.0) Setting the min/max length for messages, contents and comments
(4.3.0) Command "visulox log" - Analyzing log files
(4.3.0) How to control OTP from the command line
(4.3.0) How to control passcache from the command line
(4.3.0) How to control Password Management from the command line
(4.3.0) How to control reports from the command line
(4.3.0) How to export information from VISULOX on the command line
(4.3.0) Modify VISULOX PORTAL Datastore via CLI
(4.3.0) Setting the min/max length for messages, contents and comments
(4.3.1) Command "visulox log" - Analyzing log files
(4.3.1) How to adjust the Jump Shell
(4.3.1) How to configure input idle detection
(4.3.1) How to control OTP from the command line
(4.3.1) How to control passcache from the command line
(4.3.1) How to control Password Management from the command line
(4.3.1) How to control reports from the command line
(4.3.1) How to export information from VISULOX on the command line
(4.3.1) How to limit the granting endtime in Access Policies

(4.2.0) How to control mailinggroups from the command line
(4.2.0) How to control messages from the command line
(4.2.0) How to control regions from the command line
(4.2.0) How to control timeprofiles from the command line
(4.3.0) How to control action scripts from the command line
(4.3.0) How to control Cockpit roles from the command line
(4.3.0) How to control mailinggroups from the command line
(4.3.0) How to control messages from the command line
(4.3.0) How to control regions from the command line
(4.3.0) How to control timeprofiles from the command line
(4.3.1) How to control action scripts from the command line
(4.3.1) How to control Cockpit roles from the command line
(4.3.1) How to control mailinggroups from the command line
(4.3.1) How to control messages from the command line
(4.3.1) How to control regions from the command line
(4.3.1) How to control timeprofiles from the command line
(4.3.2) How to control action scripts from the command line
(4.3.2) How to control Cockpit roles from the command line
(4.3.2) How to control mailinggroups from the command line
(4.3.2) How to control messages from the command line
(4.3.2) How to control regions from the command line
(4.3.2) How to control timeprofiles from the command line
(4.3.1) How to set and reset the inital VISULOX Cockpit refresh state
(4.3.1) How to set auto commit or auto reject for recording
(4.3.1) Modify VISULOX PORTAL Datastore via CLI
(4.3.1) Setting the min/max length for messages, contents and comments
(4.3.1) The VISULOX PIN Service
(4.3.2) Command "visulox log" - Analyzing log files
(4.3.2) How to adjust the Jump Shell
(4.3.2) How to configure input idle detection
(4.3.2) How to control OTP from the command line
(4.3.2) How to control passcache from the command line
(4.3.2) How to control Password Management from the command line
(4.3.2) How to control reports from the command line
(4.3.2) How to export information from VISULOX on the command line
(4.3.2) How to limit the granting endtime in Access Policies
(4.3.2) How to set and reset the inital VISULOX Cockpit refresh state
(4.3.2) How to set auto commit or auto reject for recording
(4.3.2) Modify VISULOX PORTAL Datastore via CLI
(4.3.2) Setting the min/max length for messages, contents and comments
(4.3.2) The VISULOX PIN Service
Command "visulox log" - Analyzing log files
How to adjust the Jump Shell
How to configure input idle detection

How to control action scripts from the command line
How to control Cockpit roles from the command line
How to control mailinggroups from the command line
How to control messages from the command line
How to control regions from the command line
How to control timeprofiles from the command line
(4.1.1) How to control regions from the command line
(4.1.1) How to control timeprofiles from the command line
How to control action scripts from the command line
How to control Cockpit roles from the command line
How to control mailinggroups from the command line
How to control messages from the command line
How to control regions from the command line
How to control timeprofiles from the command line

Addons

(4.1.1) Automated transfer of files into Transit Zone (Passon)
(4.1.1) How to control FT Client from the command line
(4.1.1) How to control host objects from the command line
(4.1.1) How to control script objects from the command line
(4.1.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.2.0) Automated transfer of files into Transit Zone (Passon)
How to control OTP from the command line
How to control passcache from the command line
How to control Password Management from the command line
How to control reports from the command line
How to export information from VISULOX on the command line
How to limit the granting endtime in Access Policies
How to set and reset the inital VISULOX Cockpit refresh state
How to set auto commit or auto reject for recording
Modify VISULOX PORTAL Datastore via CLI
Setting the min/max length for messages, contents and comments
The VISULOX PIN Service
(4.1.1) How to adjust the Jump Shell
(4.1.1) How to configure input idle detection
(4.1.1) How to limit the granting endtime in Access Policies
(4.1.1) How to set and reset the inital VISULOX Cockpit refresh state
(4.1.1) How to set auto commit or auto reject for recording
(4.1.1) The VISULOX PIN Service
(4.2.0) How to adjust the Jump Shell
(4.2.0) How to limit the granting endtime in Access Policies
(4.2.0) How to set and reset the inital VISULOX Cockpit refresh state
(4.2.0) How to set auto commit or auto reject for recording
(4.2.0) The VISULOX PIN Service

(4.2.0) How to control FT Client from the command line
(4.2.0) How to control host objects from the command line
(4.2.0) How to control script objects from the command line
(4.2.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.0) Automated transfer of files into Transit Zone (Passon)
(4.3.0) How to control FT Client from the command line
(4.3.0) How to control host objects from the command line
(4.3.0) How to control script objects from the command line
(4.3.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.1) Automated transfer of files into Transit Zone (Passon)
(4.3.1) File Transfer via command line
(4.3.1) How to control FT Client from the command line
(4.3.1) How to control host objects from the command line
(4.3.1) How to control script objects from the command line
(4.3.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.2) Automated transfer of files into Transit Zone (Passon)
(4.3.2) File Transfer via command line
(4.3.2) How to control FT Client from the command line
(4.3.2) How to control host objects from the command line
(4.3.2) How to control script objects from the command line
(4.3.2) VISULOX addon command line interface (CMD Connect / Guard, etc)
Automated transfer of files into Transit Zone (Passon)
(4.3.0) How to adjust the Jump Shell
(4.3.0) How to configure input idle detection
(4.3.0) How to limit the granting endtime in Access Policies
(4.3.0) How to set and reset the inital VISULOX Cockpit refresh state
(4.3.0) How to set auto commit or auto reject for recording
(4.3.0) The VISULOX PIN Service
Command "visulox log" - Analyzing log files
How to adjust the Jump Shell
How to configure input idle detection
How to control OTP from the command line
How to control passcache from the command line
How to control Password Management from the command line
How to control reports from the command line
How to export information from VISULOX on the command line
How to limit the granting endtime in Access Policies
How to set and reset the inital VISULOX Cockpit refresh state
How to set auto commit or auto reject for recording
Modify VISULOX PORTAL Datastore via CLI
Setting the min/max length for messages, contents and comments
The VISULOX PIN Service

File Transfer via command line
How to control FT Client from the command line
How to control host objects from the command line
How to control script objects from the command line
VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.1.1) File Transfer via command line
(4.2.0) File Transfer via command line
(4.3.0) File Transfer via command line
Automated transfer of files into Transit Zone (Passon)
File Transfer via command line
How to control FT Client from the command line
How to control host objects from the command line
How to control script objects from the command line
VISULOX addon command line interface (CMD Connect / Guard, etc)

7 Datasources

VISULOX handles users, groups and applications. These are the so called datasources and they are imported by the VISULOX Importer Service.

Applications and user profiles are defined in the VISULOX PORTAL Datastore and are imported by default.

7.1 Available articles

(4.1.1) Creating VISULOX user groups based on an AD/LDAP attribute

(4.1.1) Datasources

(4.1.1) How to configure alternate mappings for datasources

(4.1.1) How to exclude single datastore users from import

(4.1.1) How to import users as VISULOX PORTAL administrators

(4.1.1) How to test and check an LDAP datasource in VISULOX

(4.1.1) How to use an LDAP/AD or a Unix account to access the Webservice

(4.1.1) How to work with VISULOX Datasources

(4.1.1) Troubleshooting: LDAPS

(4.1.1) VISULOX Cockpit / Objects

(4.2.0) Creating VISULOX user groups based on an AD/LDAP attribute

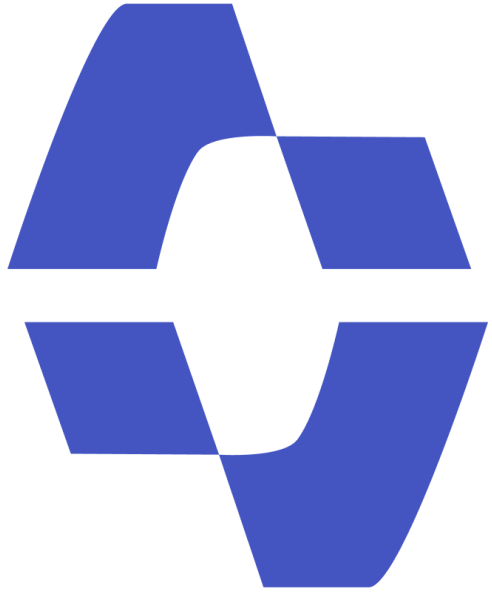
(4.2.0) Datasources

(4.2.0) How to configure alternate mappings for datasources

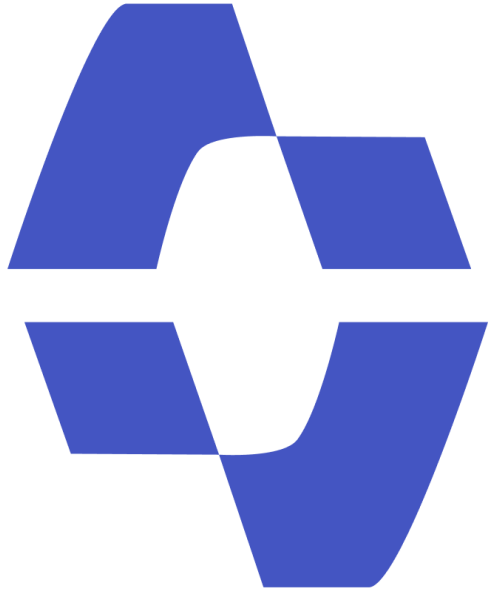
(4.2.0) How to exclude single datastore users from import

(4.2.0) How to import users as VISULOX PORTAL administrators

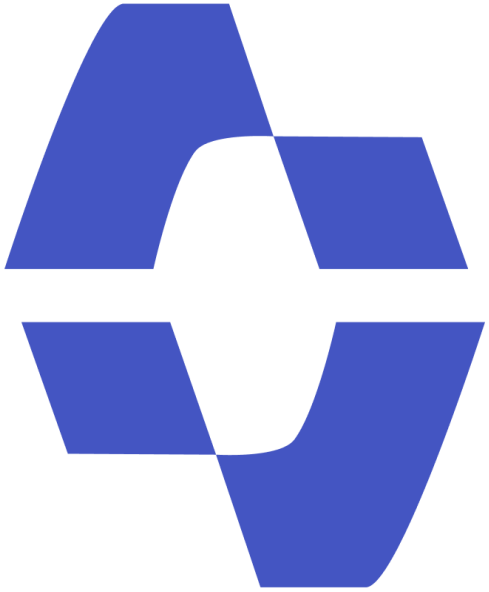
(4.2.0) How to test and check an LDAP datasource in VISULOX



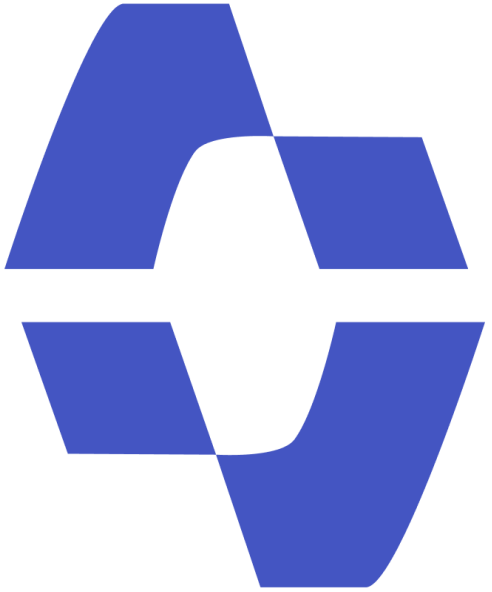
(4.2.0) How to work with VISULOX Datasources
(4.2.0) Troubleshooting: LDAPS
(4.2.0) VISULOX Cockpit / Objects
(4.3.0) Creating VISULOX user groups based on an AD/LDAP attribute
(4.3.0) Datasources
(4.3.0) How to configure alternate mappings for datasources
(4.3.0) How to exclude single datastore users from import
(4.3.0) How to import users as VISULOX PORTAL administrators
(4.3.0) How to test and check an LDAP datasource in VISULOX
(4.3.0) How to work with VISULOX Datasources
(4.3.0) Microsoft LAPS integration
(4.3.0) Troubleshooting: LDAPS
(4.3.0) VISULOX Cockpit / Objects
(4.3.1) Creating VISULOX user groups based on an AD/LDAP attribute
(4.3.1) Datasources
(4.3.1) How to check Policy, Datastore and LDAP assignments
(4.3.1) How to configure alternate mappings for datasources
(4.3.1) How to exclude single datastore users from import
(4.3.1) How to import users as VISULOX PORTAL administrators
(4.3.1) How to test and check an LDAP datasource in VISULOX
(4.3.1) How to use an LDAP/AD or Unix account to access the webservice
(4.3.1) How to work with VISULOX Datasources



(4.3.1) Microsoft LAPS integration
(4.3.1) Troubleshooting: LDAPS
(4.3.1) VISULOX Cockpit / Objects
(4.3.2) Creating VISULOX user groups based on an AD/LDAP attribute
(4.3.2) Datasources
(4.3.2) How to check Policy, Datastore and LDAP assignments
(4.3.2) How to configure alternate mappings for datasources
(4.3.2) How to exclude single datastore users from import
(4.3.2) How to import users as VISULOX PORTAL administrators
(4.3.2) How to test and check an LDAP datasource in VISULOX
(4.3.2) How to use an LDAP/AD or Unix account to access the webservice
(4.3.2) How to work with VISULOX Datasources
(4.3.2) Microsoft LAPS integration
(4.3.2) Troubleshooting: LDAPS
(4.3.2) VISULOX Cockpit / Objects
Creating VISULOX user groups based on an AD/LDAP attribute
Datasources
How to check Policy, Datastore and LDAP assignments
How to configure alternate mappings for datasources
How to exclude single datastore users from import
How to import users as VISULOX PORTAL administrators
How to test and check an LDAP datasource in VISULOX



How to use an LDAP/AD or Unix account to access the webservice
How to work with VISULOX Datasources
Microsoft LAPS integration
Troubleshooting: LDAPS
VISULOX Cockpit / Objects
(4.1.1) How to check Policy, Datastore and LDAP assignments
(4.1.1) Microsoft LAPS integration
(4.2.0) How to check Policy, Datastore and LDAP assignments
(4.2.0) How to use an LDAP/AD or Unix account to access the webservice
(4.2.0) Microsoft LAPS integration
(4.3.0) How to check Policy, Datastore and LDAP assignments
(4.3.0) How to use an LDAP/AD or Unix account to access the webservice
Creating VISULOX user groups based on an AD/LDAP attribute
Datasources
How to check Policy, Datastore and LDAP assignments
How to configure alternate mappings for datasources
How to exclude single datastore users from import
How to import users as VISULOX PORTAL administrators
How to test and check an LDAP datasource in VISULOX
How to use an LDAP/AD or Unix account to access the webservice
How to work with VISULOX Datasources
Microsoft LAPS integration



8 Login and Access Management

With VISULOX Access Management it is possible to assign controlled access to the IT infrastructure for internal and external employees, administrators and IT service providers. This is limited to defined times or time periods and always booked under their own individual reference numbers.

8.1 Available articles

Login / MFA / OTP

(4.1.1) How to configure a user account as a group account
(4.1.1) How to control OTP from the command line
(4.1.1) How to enable, configure and use MFA
(4.1.1) How to pass multiple login failures to external
(4.1.1) How to setup MFA with SMS response from the SMS Provider
(4.1.1) How to use Unix user profiles
(4.1.1) Login and Access Management
(4.1.1) Login page configuration options
(4.1.1) Login Policy
(4.1.1) Login with One Time Password (OTP)
(4.1.1) MFA via external service
(4.1.1) Migrating to One Time Password Authentication
(4.2.0) Authentication with Microsoft Entra
(4.2.0) How to configure a user account as a group account
(4.2.0) How to control login from the command line
(4.2.0) How to control OTP from the command line
(4.2.0) How to enable, configure and use MFA
(4.2.0) How to pass multiple login failures to external
(4.2.0) How to setup MFA with SMS response from the SMS Provider

Access to applications

(4.1.1) Access and transit request via actionlink
(4.1.1) Access Branding
(4.1.1) Access Policy
(4.1.1) Access request and access to applications
(4.1.1) Handling ticket IDs from external systems
(4.1.1) How to control access from the command line
(4.1.1) How to control groupaccess from the command line
(4.1.1) How to enable access to applications
(4.1.1) How to handle access for groups
(4.1.1) How to lock a user permanently for using an application after keyword detection
(4.1.1) How to use the VISULOX Command Line Interface from a remote server
(4.1.1) In-time access
(4.1.1) Login and Access Management
(4.2.0) Access and transit request via actionlink
(4.2.0) Access Branding
(4.2.0) Access Policy
(4.2.0) Access request and access to applications

(4.2.0) How to use Unix user profiles
(4.2.0) Login and Access Management
(4.2.0) Login page configuration options
(4.2.0) Login Policy
(4.2.0) Login with One Time Password (OTP)
(4.2.0) Migrating to One Time Password Authentication
(4.2.0) VISULOX Mail Client and Send PIN
(4.3.0) 3rdParty configuration parameters
(4.3.0) Authentication with Microsoft Entra
(4.3.0) How to configure a user account as a group account
(4.3.0) How to control OTP from the command line
(4.3.0) How to enable, configure and use MFA
(4.3.0) How to pass multiple login failures to external
(4.3.0) How to setup MFA with SMS response from the SMS Provider
(4.3.0) How to use Unix user profiles
(4.3.0) Login and Access Management
(4.3.0) Login page configuration options
(4.3.0) Login Policy
(4.3.0) Login with One Time Password (OTP)
(4.3.0) MFA via external service
(4.3.0) Migrating to One Time Password Authentication
(4.3.0) Object ID
(4.2.0) Handling ticket IDs from external systems
(4.2.0) How to control access from the command line
(4.2.0) How to control groupaccess from the command line
(4.2.0) How to enable access to applications
(4.2.0) How to handle access for groups
(4.2.0) How to lock a user permanently for using an application after keyword detection
(4.2.0) How to use the VISULOX Command Line Interface from a remote server
(4.2.0) In-Time Access
(4.2.0) Login and Access Management
(4.3.0) Access and transit request via actionlink
(4.3.0) Access Branding
(4.3.0) Access Policy
(4.3.0) Access request and access to applications
(4.3.0) Handling ticket IDs from external systems
(4.3.0) How to control access from the command line
(4.3.0) How to control groupaccess from the command line
(4.3.0) How to enable access to applications
(4.3.0) How to handle access for groups
(4.3.0) How to lock a user permanently for using an application after keyword detection
(4.3.0) How to use the VISULOX Command Line Interface from a remote server

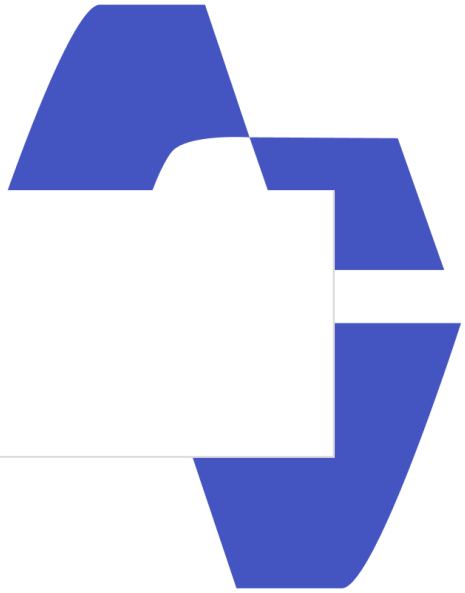
(4.3.0) VISULOX Mail Client and Send PIN
(4.3.0) Web server basic authentication with VISULOX
(4.3.1) 3rdParty configuration parameters
(4.3.1) Authentication with Microsoft Entra
(4.3.1) Browser agent switch for TCC file or URL call
(4.3.1) How to configure a user account as a group account
(4.3.1) How to control login from the command line
(4.3.1) How to control OTP from the command line
(4.3.1) How to enable, configure and use MFA
(4.3.1) How to pass multiple login failures to external
(4.3.1) How to setup MFA with SMS response from the SMS Provider
(4.3.1) How to use Unix user profiles
(4.3.1) Login and Access Management
(4.3.1) Login check against an external system
(4.3.1) Login page configuration options
(4.3.1) Login Policy
(4.3.1) Login with One Time Password (OTP)
(4.3.1) MFA via external service
(4.3.1) Migrating to One Time Password Authentication
(4.3.1) Object ID
(4.3.1) RSA SecureID Implementation via RSA API
(4.3.1) The VISULOX PIN Service
(4.3.0) In-Time Access
(4.3.0) Login and Access Management
(4.3.1) Access and transit request via actionlink
(4.3.1) Access Branding
(4.3.1) Access Policy
(4.3.1) Access request and access to applications
(4.3.1) Handling ticket IDs from external systems
(4.3.1) How to control access from the command line
(4.3.1) How to control groupaccess from the command line
(4.3.1) How to enable access to applications
(4.3.1) How to handle access for groups
(4.3.1) How to limit the granting endtime in Access Policies
(4.3.1) How to lock a user permanently for using an application after keyword detection
(4.3.1) How to use the VISULOX Command Line Interface from a remote server
(4.3.1) In-Time Access
(4.3.1) Login and Access Management
(4.3.1) Time zones, holidays and time profiles
(4.3.2) Access and transit request via actionlink
(4.3.2) Access Branding
(4.3.2) Access Policy
(4.3.2) Access request and access to applications

(4.3.1) VISULOX Mail Client and Send PIN
(4.3.1) VISULOX Webservice
(4.3.1) Web server basic authentication with VISULOX
(4.3.2) 3rdParty configuration parameters
(4.3.2) Authentication with Microsoft Entra
(4.3.2) Browser agent switch for TCC file or URL call
(4.3.2) How to configure a user account as a group account
(4.3.2) How to control login from the command line
(4.3.2) How to control OTP from the command line
(4.3.2) How to enable, configure and use MFA
(4.3.2) How to pass multiple login failures to external
(4.3.2) How to setup MFA with SMS response from the SMS Provider
(4.3.2) How to use Unix user profiles
(4.3.2) Login and Access Management
(4.3.2) Login check against an external system
(4.3.2) Login page configuration options
(4.3.2) Login Policy
(4.3.2) Login with One Time Password (OTP)
(4.3.2) MFA via external service
(4.3.2) Migrating to One Time Password Authentication
(4.3.2) Object ID
(4.3.2) RSA SecureID Implementation via RSA API
(4.3.2) Access termination enforced
(4.3.2) Handling ticket IDs from external systems
(4.3.2) How to control access from the command line
(4.3.2) How to control groupaccess from the command line
(4.3.2) How to enable access to applications
(4.3.2) How to handle access for groups
(4.3.2) How to limit the granting endtime in Access Policies
(4.3.2) How to lock a user permanently for using an application after keyword detection
(4.3.2) How to use the VISULOX Command Line Interface from a remote server
(4.3.2) In-Time Access
(4.3.2) Login and Access Management
(4.3.2) Time zones, holidays and time profiles
Access and transit request via actionlink
Access Branding
Access Policy
Access request and access to applications
Access termination enforced
Handling ticket IDs from external systems
How to control access from the command line
How to control groupaccess from the command line
How to enable access to applications

(4.3.2) The VISULOX PIN Service
(4.3.2) VISULOX Mail Client and Send PIN
(4.3.2) VISULOX Webservice
(4.3.2) Web server basic authentication with VISULOX
3rdParty configuration parameters
Authentication with Microsoft Entra
Browser agent switch for TCC file or URL call
How to configure a user account as a group account
How to control login from the command line
How to control OTP from the command line
How to enable, configure and use MFA
How to pass multiple login failures to external
How to setup MFA with SMS response from the SMS Provider
How to use Unix user profiles
Login and Access Management
Login check against an external system
Login page configuration options
Login Policy
Login with One Time Password (OTP)
MFA via external service
Migrating to One Time Password Authentication
Object ID
How to handle access for groups
How to limit the granting endtime in Access Policies
How to lock a user permanently for using an application after keyword detection
How to use the VISULOX Command Line Interface from a remote server
In-Time Access
Login and Access Management
Time zones, holidays and time profiles
(4.1.1) How to limit the granting endtime in Access Policies
(4.1.1) Time zones, holidays and time profiles
(4.2.0) How to limit the granting endtime in Access Policies
(4.2.0) Time zones, holidays and time profiles
(4.3.0) How to limit the granting endtime in Access Policies
(4.3.0) Time zones, holidays and time profiles
Access and transit request via actionlink
Access Branding
Access Policy
Access request and access to applications
Access termination enforced
Handling ticket IDs from external systems
How to control access from the command line
How to control groupaccess from the command line
How to enable access to applications

RSA SecureID Implementation via RSA API
The VISULOX PIN Service
VISULOX Mail Client and Send PIN
VISULOX Webservice
Web server basic authentication with VISULOX
(4.1.1) How to control login from the command line
(4.1.1) Login check against an external system
(4.1.1) Object ID
(4.1.1) RSA SecureID Implementation via RSA API
(4.1.1) The VISULOX PIN Service
(4.1.1) VISULOX Mail Client and Send PIN
(4.1.1) VISULOX Webservice
(4.2.0) Login check against an external system
(4.2.0) MFA via external service
(4.2.0) Object ID
(4.2.0) RSA SecureID Implementation via RSA API
(4.2.0) The VISULOX PIN Service
(4.2.0) VISULOX Webservice
(4.3.0) Browser agent switch for TCC file or URL call
(4.3.0) How to control login from the command line
(4.3.0) Login check against an external system
(4.3.0) RSA SecureID Implementation via RSA API
How to handle access for groups
How to limit the granting endtime in Access Policies
How to lock a user permanently for using an application after keyword detection
How to use the VISULOX Command Line Interface from a remote server
In-Time Access
Login and Access Management
Time zones, holidays and time profiles

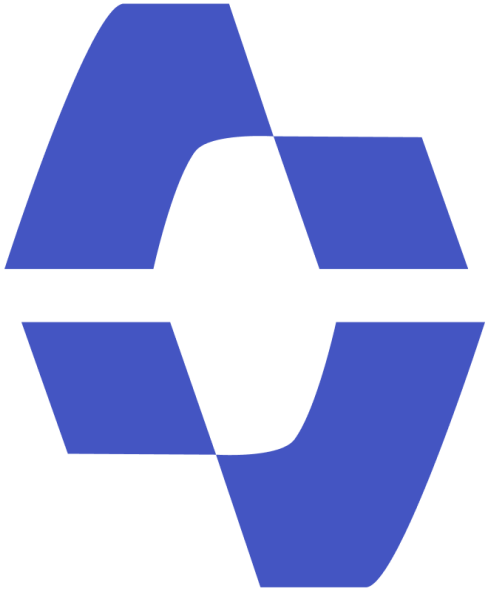
(4.3.0) The VISULOX PIN Service
(4.3.0) VISULOX Webservice
3rdParty configuration parameters
Authentication with Microsoft Entra
Browser agent switch for TCC file or URL call
How to configure a user account as a group account
How to control login from the command line
How to control OTP from the command line
How to enable, configure and use MFA
How to pass multiple login failures to external
How to setup MFA with SMS response from the SMS Provider
How to use Unix user profiles
Login and Access Management
Login check against an external system
Login page configuration options
Login Policy
Login with One Time Password (OTP)
MFA via external service
Migrating to One Time Password Authentication
Object ID
RSA SecureID Implementation via RSA API
The VISULOX PIN Service



VISULOX Mail Client and Send PIN

VISULOX Webservice

Web server basic authentication with VISULOX



9 Application Configuration

These articles describe special applications and how they are configured in VISULOX.

9.1 Available articles

(4.1.1) How to assign a fixed username

(4.1.1) How to configure FreeRDP for VISULOX PORTAL

(4.1.1) How to pass user credentials to an application - VISULOX Single Sign On - SSO

(4.1.1) The application control variable "vlxMode"

(4.1.1) VISULOX Chrome and Chromium integration

(4.1.1) VISULOX Firefox CITRIX / ICA integration

(4.1.1) VISULOX Firefox integration

(4.1.1) VISULOX PORTAL application color depth

(4.1.1) VISULOX SSH X11 Forwarding to VISULOX Application Nodes

(4.1.1) VISULOX VNC integration

(4.2.0) How to assign a fixed username

(4.2.0) How to configure FreeRDP for VISULOX PORTAL

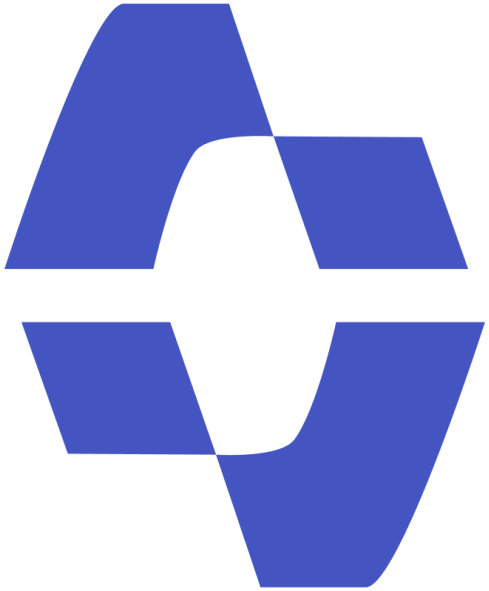
(4.2.0) How to pass user credentials to an application - VISULOX Single Sign On - SSO

(4.2.0) The application control variable "vlxMode"

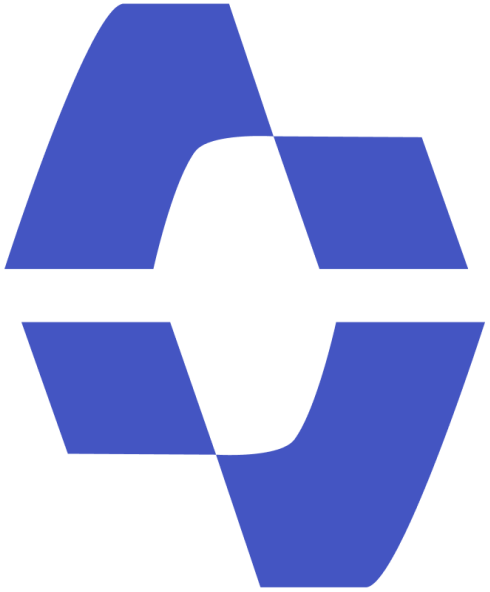
(4.2.0) VISULOX Chrome and Chromium integration

(4.2.0) VISULOX Firefox CITRIX / ICA integration

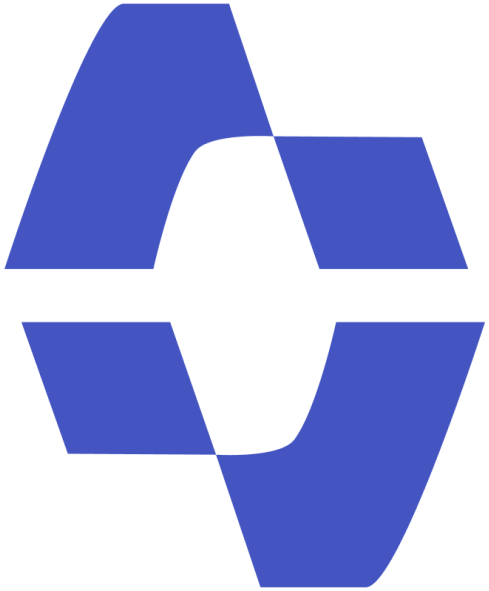
(4.2.0) VISULOX Firefox integration



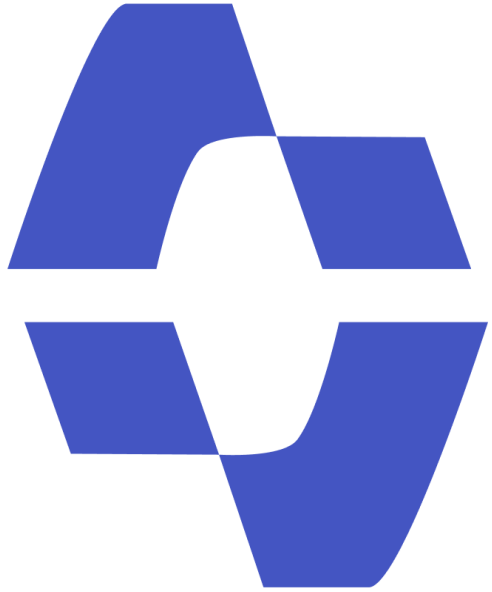
(4.2.0) VISULOX PORTAL application color depth
(4.2.0) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.2.0) VISULOX VNC integration
(4.3.0) Custom application icons
(4.3.0) How to assign a fixed username
(4.3.0) How to configure FreeRDP for VISULOX PORTAL
(4.3.0) How to pass user credentials to an application - VISULOX Single Sign On - SSO
(4.3.0) Microsoft LAPS integration
(4.3.0) The application control variable "vlxMode"
(4.3.0) VISULOX Chrome and Chromium integration
(4.3.0) VISULOX Firefox CITRIX / ICA integration
(4.3.0) VISULOX Firefox integration
(4.3.0) VISULOX PORTAL application color depth
(4.3.0) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.3.0) VISULOX VNC integration
(4.3.1) Custom application icons
(4.3.1) freeRDP with NLA support statement
(4.3.1) How to assign a fixed username
(4.3.1) How to configure FreeRDP for VISULOX PORTAL
(4.3.1) How to pass user credentials to an application - VISULOX Single Sign On - SSO
(4.3.1) Microsoft LAPS integration
(4.3.1) The application control variable "vlxMode"



(4.3.1) VISULOX Chrome and Chromium integration
(4.3.1) VISULOX Firefox CITRIX / ICA integration
(4.3.1) VISULOX Firefox integration
(4.3.1) VISULOX PORTAL application color depth
(4.3.1) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.3.1) VISULOX VNC integration
(4.3.2) Custom application icons
(4.3.2) freeRDP with NLA support statement
(4.3.2) How to assign a fixed username
(4.3.2) How to configure FreeRDP for VISULOX PORTAL
(4.3.2) How to pass user credentials to an application - VISULOX Single Sign On - SSO
(4.3.2) Microsoft LAPS integration
(4.3.2) The application control variable "vlxMode"
(4.3.2) VISULOX Chrome and Chromium integration
(4.3.2) VISULOX Firefox CITRIX / ICA integration
(4.3.2) VISULOX Firefox integration
(4.3.2) VISULOX PORTAL application color depth
(4.3.2) VISULOX SSH X11 Forwarding to VISULOX Application Nodes
(4.3.2) VISULOX VNC integration
Custom application icons
freeRDP with NLA support statement
How to assign a fixed username



How to configure FreeRDP for VISULOX PORTAL
How to pass user credentials to an application - VISULOX Single Sign On - SSO
Microsoft LAPS integration
The application control variable "vlxMode"
VISULOX Chrome and Chromium integration
VISULOX Firefox CITRIX / ICA integration
VISULOX Firefox integration
VISULOX PORTAL application color depth
VISULOX SSH X11 Forwarding to VISULOX Application Nodes
VISULOX VNC integration
(4.1.1) Custom application icons
(4.1.1) freeRDP with NLA support statement
(4.1.1) Microsoft LAPS integration
(4.2.0) Custom application icons
(4.2.0) freeRDP with NLA support statement
(4.2.0) Microsoft LAPS integration
(4.3.0) freeRDP with NLA support statement
Custom application icons
freeRDP with NLA support statement
How to assign a fixed username
How to configure FreeRDP for VISULOX PORTAL
How to pass user credentials to an application - VISULOX Single Sign On - SSO

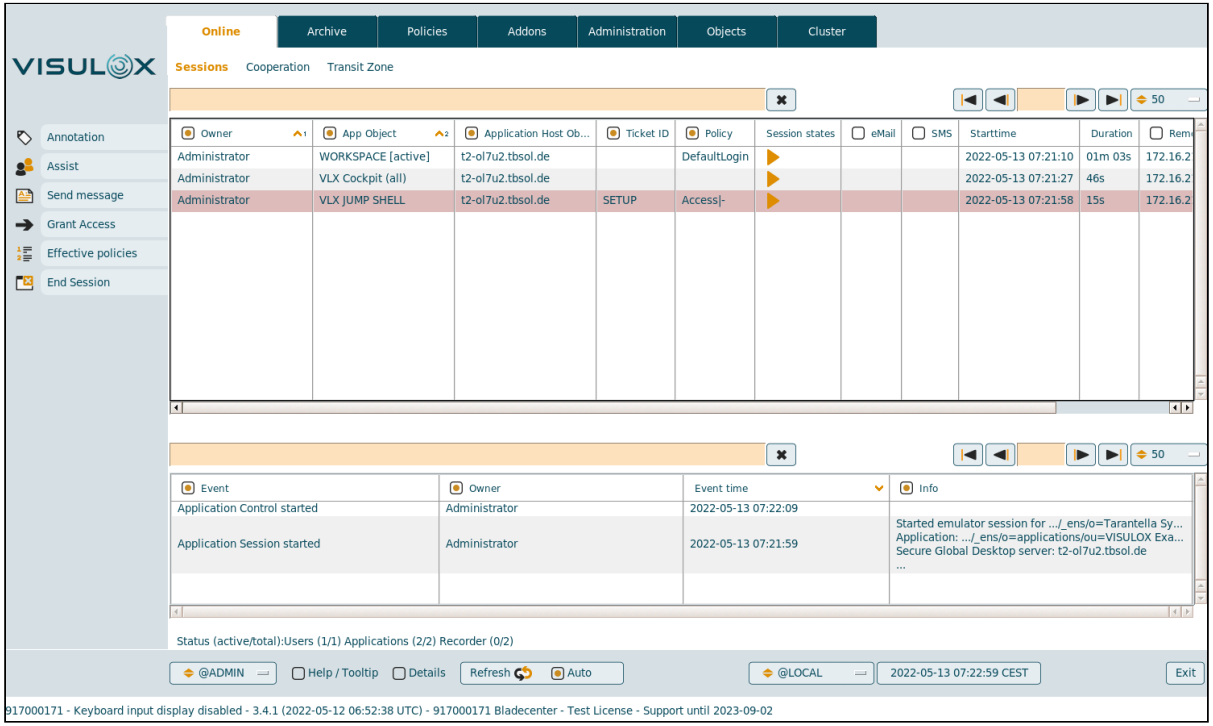


Microsoft LAPS integration
The application control variable "vlxMode"
VISULOX Chrome and Chromium integration
VISULOX Firefox CITRIX / ICA integration
VISULOX Firefox integration
VISULOX PORTAL application color depth
VISULOX SSH X11 Forwarding to VISULOX Application Nodes
VISULOX VNC integration

10 VISULOX Cockpit

The VISULOX Cockpit is the central application to control sessions.

The Cockpit displays all available information about users, groups, Workspace- and emulator sessions.



10.1 An authorized user has the ability to

- Control the access of users
- Configure notifications for access, applications, etc.
- Configure recording and keystroke recording of applications
- Configure File Transfer, CMD Connect/Guard and Citrix
- Create / edit scripts and messages
- Create / edit shell scripts and host objects
- Create / edit time zone information, holidays and time profiles
- Show effective policies of users
- Start assisting cooperations
- Send messages to users
- End running applications
- Play or download recorded films

- Display and checkout transferred files
- Acknowledge / reject files
- Logout users
- Create role profiles for the Cockpit
- Display or export Single Session Checkouts
- Display or export Reports
- Display events of the sessions
- Display / export user, recorder and server statistics
- Create or configure external and internal message
- Enter annotations for archived sessions
- **...**

10.2 Available articles

General	Addons
(4.1.1) How to control the VISULOX Cockpit	(4.1.1) Configuration of File Transfer in the VISULOX Cockpit
(4.1.1) How to create and use notifications	(4.1.1) Configuration of Host Control in the VISULOX Cockpit
(4.1.1) How to enable Dual Control in the VISULOX Cockpit	(4.1.1) Host objects
(4.1.1) Restrict default VISULOX Cockpit	(4.1.1) Passcache
(4.1.1) Starting VISULOX Cockpit with parameter -grant	(4.1.1) Script objects
(4.2.0) How to control the VISULOX Cockpit	(4.2.0) Configuration of File Transfer in the VISULOX Cockpit
(4.2.0) How to create and use notifications	(4.2.0) Configuration of Host Control in the VISULOX Cockpit
(4.2.0) How to enable Dual Control in the VISULOX Cockpit	(4.2.0) Host objects
(4.2.0) Restrict default VISULOX Cockpit	(4.2.0) Passcache
(4.3.0) How to control the VISULOX Cockpit	(4.2.0) Script objects
(4.3.0) How to create and use notifications	(4.3.0) Configuration of File Transfer in the VISULOX Cockpit
(4.3.0) How to enable Dual Control in the VISULOX Cockpit	(4.3.0) Configuration of Host Control in the VISULOX Cockpit
(4.3.0) Restrict default VISULOX Cockpit	(4.3.0) Host objects
(4.3.1) How to control the VISULOX Cockpit	(4.3.0) Passcache
(4.3.1) How to create and use notifications	(4.3.0) Script objects
(4.3.1) How to enable Dual Control in the VISULOX Cockpit	(4.3.1) Configuration of File Transfer in the VISULOX Cockpit
(4.3.1) How to set and reset the inital VISULOX Cockpit refresh state	(4.3.1) Configuration of Host Control in the VISULOX Cockpit
(4.3.1) Restrict default VISULOX Cockpit	(4.3.1) Host objects
(4.3.1) Starting VISULOX Cockpit with parameter -grant	(4.3.1) Passcache

(4.3.2) How to control the VISULOX Cockpit
(4.3.2) How to create and use notifications
(4.3.2) How to enable Dual Control in the VISULOX Cockpit
(4.3.2) How to set and reset the inital VISULOX Cockpit refresh state
(4.3.2) Restrict default VISULOX Cockpit
(4.3.2) Starting VISULOX Cockpit with parameter -grant
How to control the VISULOX Cockpit
How to create and use notifications
How to enable Dual Control in the VISULOX Cockpit
How to set and reset the inital VISULOX Cockpit refresh state
Restrict default VISULOX Cockpit
Starting VISULOX Cockpit with parameter -grant
(4.1.1) How to set and reset the inital VISULOX Cockpit refresh state
(4.2.0) How to set and reset the inital VISULOX Cockpit refresh state
(4.2.0) Starting VISULOX Cockpit with parameter -grant
(4.3.0) How to set and reset the inital VISULOX Cockpit refresh state
(4.3.0) Starting VISULOX Cockpit with parameter -grant
How to control the VISULOX Cockpit
How to create and use notifications
How to enable Dual Control in the VISULOX Cockpit
How to set and reset the inital VISULOX Cockpit refresh state
Restrict default VISULOX Cockpit

(4.3.1) Script objects
(4.3.2) Configuration of File Transfer in the VISULOX Cockpit
(4.3.2) Configuration of Host Control in the VISULOX Cockpit
(4.3.2) Host objects
(4.3.2) Passcache
(4.3.2) Script objects
Configuration of File Transfer in the VISULOX Cockpit
Configuration of Host Control in the VISULOX Cockpit
Host objects
Passcache
Script objects
Configuration of File Transfer in the VISULOX Cockpit
Configuration of Host Control in the VISULOX Cockpit
Host objects
Passcache
Script objects

Administration

(4.1.1) How to configure role profiles for the VISULOX Cockpit
(4.1.1) Mailinggroups
(4.1.1) Messages in VISULOX
(4.2.0) How to configure role profiles for the VISULOX Cockpit

Starting VISULOX Cockpit with parameter -grant

Online

(4.1.1) In-time access
(4.1.1) VISULOX Cockpit / Online
(4.2.0) In-Time Access
(4.2.0) VISULOX Cockpit / Online
(4.3.0) In-Time Access
(4.3.0) VISULOX Cockpit / Online
(4.3.1) In-Time Access
(4.3.1) VISULOX Cockpit / Online
(4.3.2) In-Time Access
(4.3.2) VISULOX Cockpit / Online
In-Time Access
VISULOX Cockpit / Online
In-Time Access
VISULOX Cockpit / Online

Archive

(4.3.0) VISULOX Cockpit / Archive
(4.3.1) VISULOX Cockpit / Archive
(4.3.2) VISULOX Cockpit / Archive

(4.2.0) Mailinggroups
(4.2.0) Messages in VISULOX
(4.3.0) How to configure role profiles for the VISULOX Cockpit
(4.3.0) How VISULOX handles presentation roles
(4.3.0) Mailinggroups
(4.3.0) Messages in VISULOX
(4.3.1) How to configure role profiles for the VISULOX Cockpit
(4.3.1) How VISULOX handles presentation roles
(4.3.1) Mailinggroups
(4.3.1) Messages in VISULOX
(4.3.1) Time zones, holidays and time profiles
(4.3.2) How to configure role profiles for the VISULOX Cockpit
(4.3.2) How VISULOX handles presentation roles
(4.3.2) Mailinggroups
(4.3.2) Messages in VISULOX
(4.3.2) Time zones, holidays and time profiles
How to configure role profiles for the VISULOX Cockpit
How VISULOX handles presentation roles
Mailinggroups
Messages in VISULOX
Time zones, holidays and time profiles
(4.1.1) How VISULOX handles presentation roles

VISULOX Cockpit / Archive
VISULOX Cockpit / Archive

Policies

(4.1.1) Access Policy
(4.1.1) Application Policy
(4.1.1) Login Policy
(4.1.1) Transit Policy
(4.1.1) VISULOX Policies - Overview
(4.1.1) Welcome EXT Policy
(4.1.1) Welcome INT
(4.2.0) Access Policy
(4.2.0) Application Policy
(4.2.0) Login Policy
(4.2.0) Transit Policy
(4.2.0) VISULOX Policies - Overview
(4.2.0) Welcome EXT Policy
(4.2.0) Welcome INT
(4.3.0) Access Policy
(4.3.0) Application Policy
(4.3.0) Login Policy
(4.3.0) Transit Policy
(4.1.1) Time zones, holidays and time profiles
(4.2.0) How VISULOX handles presentation roles
(4.2.0) Time zones, holidays and time profiles
(4.3.0) Time zones, holidays and time profiles
How to configure role profiles for the VISULOX Cockpit
How VISULOX handles presentation roles
Mailinggroups
Messages in VISULOX
Time zones, holidays and time profiles

Filter Objects

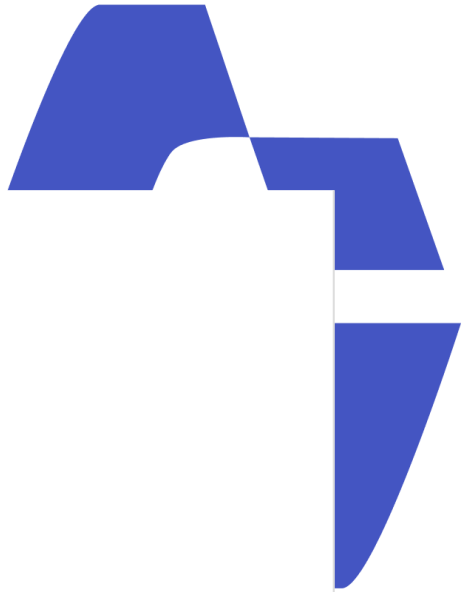
(4.1.1) VISULOX Cockpit / Objects
(4.2.0) Customizable action buttons in VISULOX Cockpit / Objects
(4.2.0) VISULOX Cockpit / Objects
(4.3.0) VISULOX Cockpit / Objects
(4.3.1) Customizable action buttons in VISULOX Cockpit / Objects
(4.3.1) VISULOX Cockpit / Objects
(4.3.2) Customizable action buttons in VISULOX Cockpit / Objects
(4.3.2) VISULOX Cockpit / Objects
Customizable action buttons in VISULOX Cockpit / Objects
VISULOX Cockpit / Objects
(4.1.1) Customizable action buttons in VISULOX Cockpit / Objects

(4.3.0) VISULOX Policies - Overview
(4.3.0) Welcome EXT Policy
(4.3.0) Welcome INT
(4.3.1) Access Policy
(4.3.1) Application Policy
(4.3.1) Login Policy
(4.3.1) Transit Policy
(4.3.1) VISULOX Policies - Overview
(4.3.1) Welcome EXT Policy
(4.3.1) Welcome INT
(4.3.2) Access Policy
(4.3.2) Application Policy
(4.3.2) Login Policy
(4.3.2) Transit Policy
(4.3.2) VISULOX Policies - Overview
(4.3.2) Welcome EXT Policy
(4.3.2) Welcome INT
Access Policy
Application Policy
Login Policy
Transit Policy
VISULOX Policies - Overview

(4.3.0) Customizable action buttons in VISULOX Cockpit / Objects
Customizable action buttons in VISULOX Cockpit / Objects
VISULOX Cockpit / Objects

Misc

(4.1.1) VISULOX Filters
(4.2.0) VISULOX Filters
(4.3.0) VISULOX Filters
(4.3.0) Why is it not possible to sort some views in the GUI?
(4.3.1) VISULOX Filters
(4.3.1) Why is it not possible to sort some views in the GUI?
(4.3.2) VISULOX Filters
(4.3.2) Why is it not possible to sort some views in the GUI?
VISULOX Filters
Why is it not possible to sort some views in the GUI?
(4.1.1) Why is it not possible to sort some views in the GUI?
(4.2.0) Why is it not possible to sort some views in the GUI?
VISULOX Filters
Why is it not possible to sort some views in the GUI?

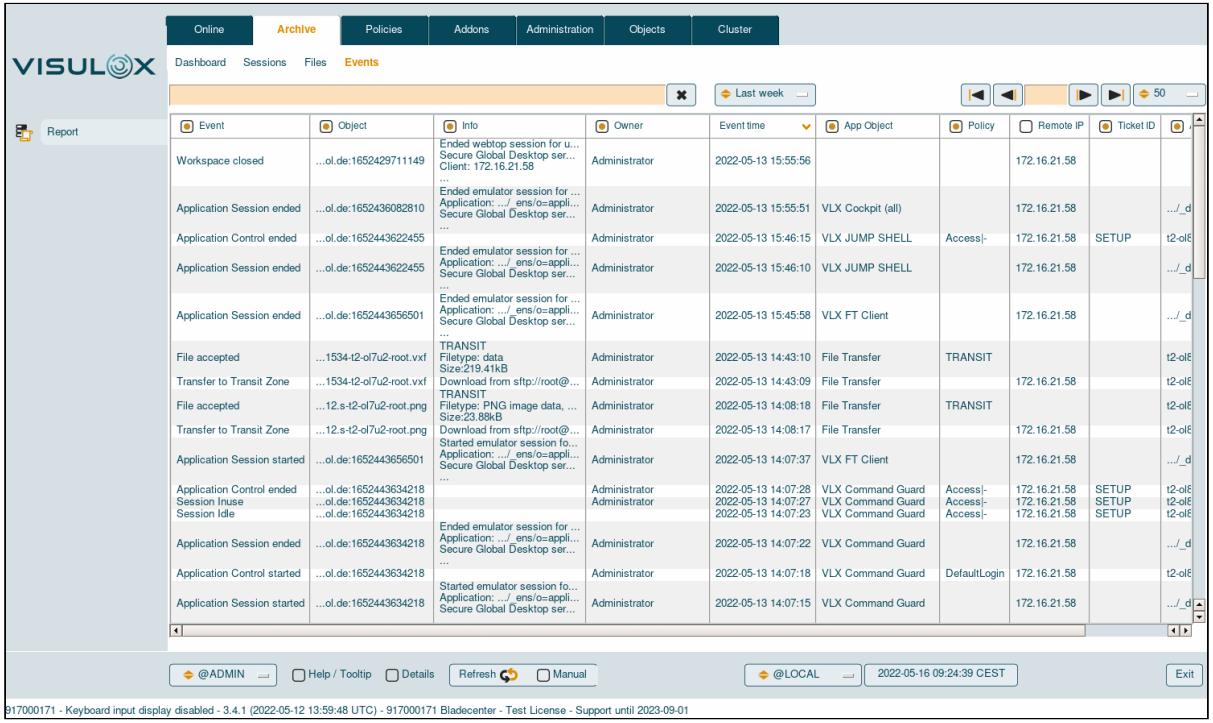


Welcome EXT Policy
Welcome INT
Access Policy
Application Policy
Login Policy
Transit Policy
VISULOX Policies - Overview
Welcome EXT Policy
Welcome INT

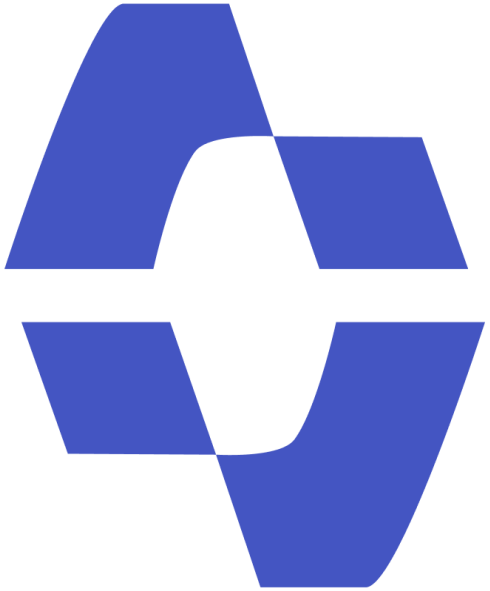
11 Events

VISULOX Service events are generated in several parts of the software. VISULOX PORTAL Service events are displayed as well.

All events are stored in the database and can be seen in the VISULOX Cockpit.



Each event is also seen in the event script and can be delivered to external systems.



11.1 Available articles

(4.1.1) Enable events for VLX Shell, FreeRDP and File Transit connections

(4.1.1) Events

(4.1.1) How to pass multiple login failures to external

(4.1.1) How to send VISULOX Events to external services

(4.1.1) Overview of VISULOX Events

(4.2.0) Enable events for VLX Shell, FreeRDP and File Transit connections

(4.2.0) Events

(4.2.0) How to configure input idle detection

(4.2.0) How to pass multiple login failures to external

(4.2.0) How to send VISULOX Events to external services

(4.2.0) Overview of VISULOX Events

(4.3.0) Enable events for VLX Shell, FreeRDP and File Transit connections

(4.3.0) Events

(4.3.0) How to pass multiple login failures to external

(4.3.0) How to send VISULOX Events to external services

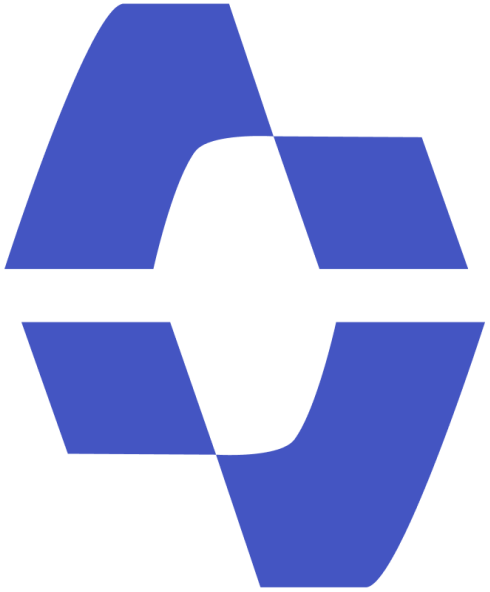
(4.3.0) Overview of VISULOX Events

(4.3.1) Enable events for VLX Shell, FreeRDP and File Transit connections

(4.3.1) Events

(4.3.1) How to configure input idle detection

(4.3.1) How to pass multiple login failures to external



(4.3.1) How to send VISULOX Events to external services
(4.3.1) Overview of VISULOX Events
(4.3.2) Enable events for VLX Shell, FreeRDP and File Transit connections
(4.3.2) Events
(4.3.2) How to configure input idle detection
(4.3.2) How to pass multiple login failures to external
(4.3.2) How to send VISULOX Events to external services
(4.3.2) Overview of VISULOX Events
Enable events for VLX Shell, FreeRDP and File Transit connections
Events
How to configure input idle detection
How to pass multiple login failures to external
How to send VISULOX Events to external services
Overview of VISULOX Events
(4.1.1) How to configure input idle detection
(4.3.0) How to configure input idle detection
Enable events for VLX Shell, FreeRDP and File Transit connections
Events
How to configure input idle detection
How to pass multiple login failures to external
How to send VISULOX Events to external services
Overview of VISULOX Events

12 Policies

With VISULOX everything is controlled by VISULOX Policies. A VISULOX Policy has a VISULOX Filter and a time, how long the policy is valid, depending of the object.

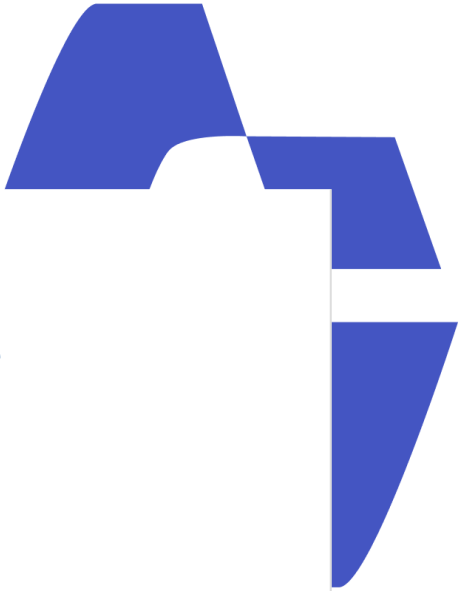
Policies are defined in the VISULOX Cockpit or via Command Line Interface.

See also: VISULOX Policies overview

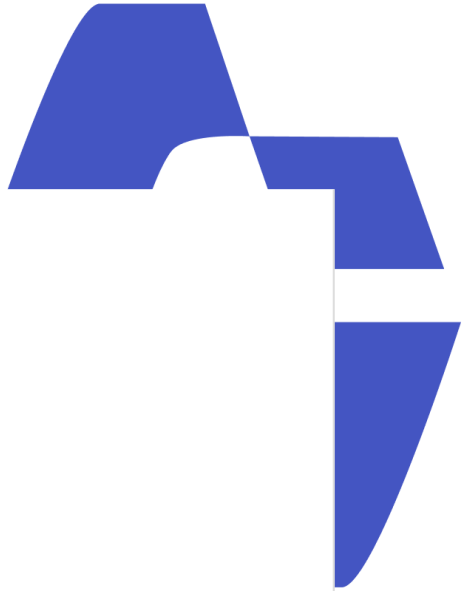
12.1 Available articles

VISULOX Cockpit	Command Line Interface
(4.1.1) Access Policy	(4.1.1) How to control access from the command line
(4.1.1) Application Policy	(4.1.1) How to control groupaccess from the command line
(4.1.1) How to create and use notifications	(4.2.0) How to control access from the command line
(4.1.1) How to enable access to applications	(4.2.0) How to control applications from the command line
(4.1.1) How to enable, configure and use cooperations	(4.2.0) How to control external messages from the command line
(4.1.1) How to enable, configure and use recording	(4.2.0) How to control File Transit Policy from the command line
(4.1.1) Login Policy	(4.2.0) How to control groupaccess from the command line
(4.1.1) Transit Policy	(4.2.0) How to control login from the command line
(4.1.1) VISULOX Policies - Overview	(4.3.0) How to control access from the command line
(4.1.1) Welcome EXT Policy	(4.3.0) How to control groupaccess from the command line
(4.1.1) Welcome INT	(4.3.0) How to control internal messages from the command line
(4.2.0) Access Policy	(4.3.1) How to control access from the command line
(4.2.0) Application Policy	(4.3.1) How to control applications from the command line
(4.2.0) How to create and use notifications	(4.3.1) How to control external messages from the command line
(4.2.0) How to enable access to applications	(4.3.1) How to control File Transit Policy from the command line
(4.2.0) How to enable, configure and use cooperations	(4.3.1) How to control groupaccess from the command line
(4.2.0) How to enable, configure and use recording	(4.3.1) How to control internal messages from the command line
(4.2.0) Login Policy	(4.3.1) How to control login from the command line
(4.2.0) Transit Policy	(4.3.2) How to control access from the command line

(4.2.0) VISULOX Policies - Overview
(4.2.0) Welcome EXT Policy
(4.2.0) Welcome INT
(4.3.0) Access Policy
(4.3.0) Application Policy
(4.3.0) How to create and use notifications
(4.3.0) How to enable access to applications
(4.3.0) How to enable, configure and use cooperations
(4.3.0) How to enable, configure and use recording
(4.3.0) Login Policy
(4.3.0) Transit Policy
(4.3.0) VISULOX Policies - Overview
(4.3.0) Welcome EXT Policy
(4.3.0) Welcome INT
(4.3.1) Access Policy
(4.3.1) Application Policy
(4.3.1) How to create and use notifications
(4.3.1) How to enable access to applications
(4.3.1) How to enable, configure and use cooperations
(4.3.1) How to enable, configure and use recording
(4.3.1) Login Policy
(4.3.1) Transit Policy
(4.3.2) How to control applications from the command line
(4.3.2) How to control external messages from the command line
(4.3.2) How to control File Transit Policy from the command line
(4.3.2) How to control groupaccess from the command line
(4.3.2) How to control internal messages from the command line
(4.3.2) How to control login from the command line
How to control access from the command line
How to control applications from the command line
How to control external messages from the command line
How to control File Transit Policy from the command line
How to control groupaccess from the command line
How to control internal messages from the command line
How to control login from the command line
(4.1.1) How to control applications from the command line
(4.1.1) How to control external messages from the command line
(4.1.1) How to control File Transit Policy from the command line
(4.1.1) How to control internal messages from the command line
(4.1.1) How to control login from the command line
(4.2.0) How to control internal messages from the command line
(4.3.0) How to control applications from the command line
(4.3.0) How to control external messages from the command line
(4.3.0) How to control File Transit Policy from the command line



(4.3.1) VISULOX Policies - Overview
(4.3.1) Welcome EXT Policy
(4.3.1) Welcome INT
(4.3.2) Access Policy
(4.3.2) Application Policy
(4.3.2) How to create and use notifications
(4.3.2) How to enable access to applications
(4.3.2) How to enable, configure and use cooperations
(4.3.2) How to enable, configure and use recording
(4.3.2) Login Policy
(4.3.2) Transit Policy
(4.3.2) VISULOX Policies - Overview
(4.3.2) Welcome EXT Policy
(4.3.2) Welcome INT
Access Policy
Application Policy
How to create and use notifications
How to enable access to applications
How to enable, configure and use cooperations
How to enable, configure and use recording
Login Policy
Transit Policy
(4.3.0) How to control login from the command line
How to control access from the command line
How to control applications from the command line
How to control external messages from the command line
How to control File Transit Policy from the command line
How to control groupaccess from the command line
How to control internal messages from the command line
How to control login from the command line



VISULOX Policies - Overview
Welcome EXT Policy
Welcome INT
Access Policy
Application Policy
How to create and use notifications
How to enable access to applications
How to enable, configure and use cooperations
How to enable, configure and use recording
Login Policy
Transit Policy

VISULOX Policies - Overview
Welcome EXT Policy
Welcome INT

13 Recording

Recording is a task that is performed in the background and does not affect the user performance.

Whenever a session should be recorded (automatically or manually) VISULOX Service starts a task. This task records the session presentation by using the shadow command.

13.1 Available articles

(4.1.1) Example: Application based recording via vlxMode parameter

(4.1.1) Example: Keyboard recording

(4.1.1) Example: Policy based recording

(4.1.1) How to enable, configure and use recording

(4.1.1) Recorded applications

(4.1.1) Recording

(4.1.1) The application control variable "vlxMode"

(4.1.1) Useful database queries: Size of film chapters, snapshots, files, usage

(4.2.0) Example: Keyboard recording

(4.2.0) Example: Policy based recording

(4.2.0) How to enable, configure and use recording

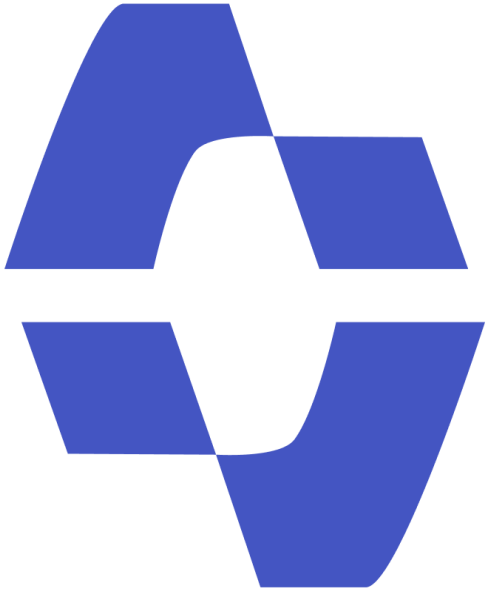
(4.2.0) Recorded applications

(4.2.0) Recording

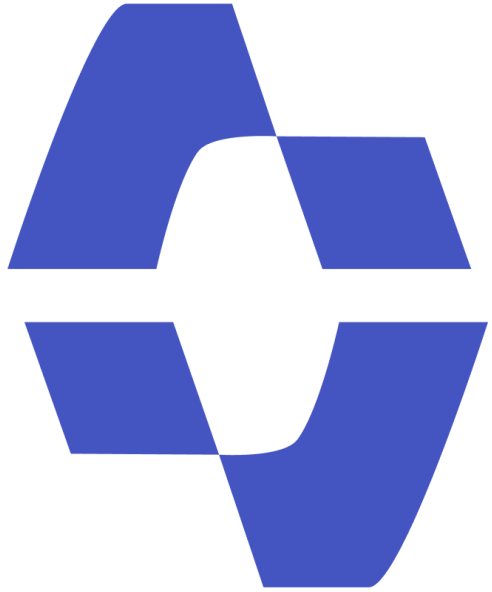
(4.2.0) The application control variable "vlxMode"

(4.2.0) Useful database queries: Size of film chapters, snapshots, files, usage

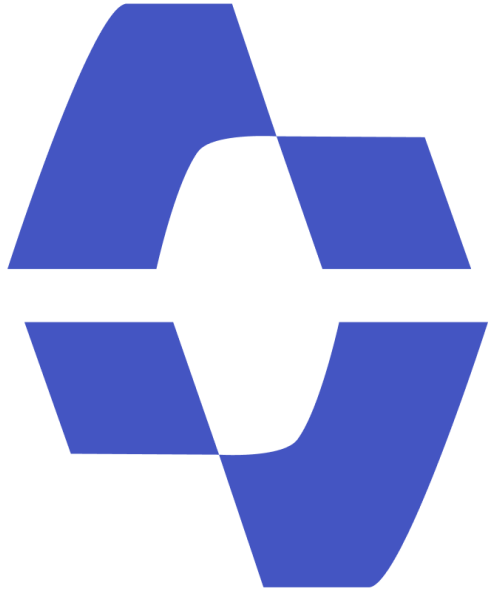
(4.3.0) Example: Keyboard recording



(4.3.0) Example: Policy based recording
(4.3.0) How to enable, configure and use recording
(4.3.0) Recorded applications
(4.3.0) Recording
(4.3.0) The application control variable "vlxMode"
(4.3.0) Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.1) Example: Application based recording via vlxMode parameter
(4.3.1) Example: Keyboard recording
(4.3.1) Example: Manual recording
(4.3.1) Example: Policy based recording
(4.3.1) How to enable, configure and use recording
(4.3.1) How to set auto commit or auto reject for recording
(4.3.1) Recorded applications
(4.3.1) Recorder configuration
(4.3.1) Recording
(4.3.1) The application control variable "vlxMode"
(4.3.1) Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.1) Watching films recorded before version 3.2 with Flash support
(4.3.2) Example: Application based recording via vlxMode parameter
(4.3.2) Example: Keyboard recording
(4.3.2) Example: Manual recording
(4.3.2) Example: Policy based recording

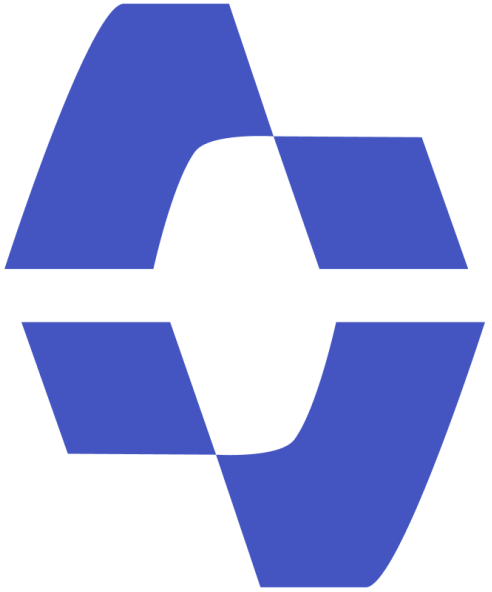


(4.3.2) How to enable, configure and use recording
(4.3.2) How to set auto commit or auto reject for recording
(4.3.2) Recorded applications
(4.3.2) Recorder configuration
(4.3.2) Recording
(4.3.2) The application control variable "vlxMode"
(4.3.2) Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.2) Watching films recorded before version 3.2 with Flash support
Example: Application based recording via vlxMode parameter
Example: Keyboard recording
Example: Manual recording
Example: Policy based recording
How to enable, configure and use recording
How to set auto commit or auto reject for recording
(4.3.3) Recorded applications
Recorder configuration
Recording
The application control variable "vlxMode"
Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.3) Watching films recorded before version 3.2 with Flash support
(4.1.1) Example: Manual recording
(4.1.1) How to set auto commit or auto reject for recording



(4.1.1) Recorder configuration
(4.1.1) Watching films recorded before version 3.2 with Flash support
(4.2.0) Example: Application based recording via vlxMode parameter
(4.2.0) Example: Manual recording
(4.2.0) How to set auto commit or auto reject for recording
(4.2.0) Recorder configuration
(4.2.0) Watching films recorded before version 3.2 with Flash support
(4.3.0) Example: Application based recording via vlxMode parameter
(4.3.0) Example: Manual recording
(4.3.0) How to set auto commit or auto reject for recording
(4.3.0) Recorder configuration
(4.3.0) Watching films recorded before version 3.2 with Flash support
Example: Application based recording via vlxMode parameter
Example: Keyboard recording
Example: Manual recording
Example: Policy based recording
How to enable, configure and use recording
How to set auto commit or auto reject for recording
Recorded applications
Recorder configuration
Recording
The application control variable "vlxMode"

Useful database queries: Size of film chapters, snapshots, files, usage
Watching films recorded before version 3.2 with Flash support



14 VISULOX Player

In VISULOX Cockpit / Archive / Sessions all ended recorded sessions are displayed. Selecting a recorded session and pressing the "**Player**" button starts the integrated player. Checked out recorded sessions can be viewed with an integrated offline player in a browser on the client.

The VISULOX player has several views, controls and presents all information available for the recorded film.

14.1 Available articles

(4.1.1) How to enable the VISULOX Cockpit for Dual Control and view films in player

(4.1.1) VISULOX Player

(4.1.1) VISULOX Player: integrated or client side

(4.1.1) Watching recorded films with the VISULOX player

(4.2.0) How to enable the VISULOX Cockpit for Dual Control and view films in player

(4.2.0) VISULOX Player

(4.2.0) VISULOX Player: integrated or client side

(4.2.0) Watching recorded films with the VISULOX player

(4.3.0) How to enable the VISULOX Cockpit for Dual Control and view films in player

(4.3.0) VISULOX Player

(4.3.0) VISULOX Player: integrated or client side

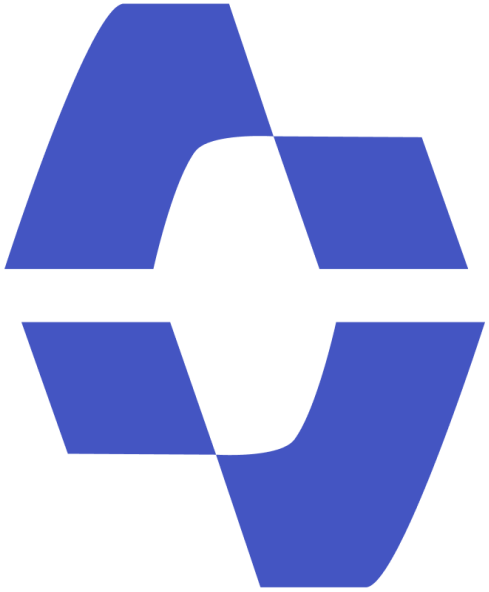
(4.3.0) Watching recorded films with the VISULOX player

(4.3.1) How to enable the VISULOX Cockpit for Dual Control and view films in player

(4.3.1) VISULOX Player

(4.3.1) VISULOX Player: integrated or client side

(4.3.1) Watching recorded films with the VISULOX player



(4.3.2) How to enable the VISULOX Cockpit for Dual Control and view films in player
(4.3.2) VISULOX Player
(4.3.2) VISULOX Player: integrated or client side
(4.3.2) Watching recorded films with the VISULOX player
How to enable the VISULOX Cockpit for Dual Control and view films in player
VISULOX Player
VISULOX Player: integrated or client side
Watching recorded films with the VISULOX player
How to enable the VISULOX Cockpit for Dual Control and view films in player
VISULOX Player
VISULOX Player: integrated or client side
Watching recorded films with the VISULOX player

15 Cooperations

A cooperation is useful to work together with the same view on one application. In a cooperation is always the owner of the application and a cooperation partner. A cooperation partner is a participant, who can look at what the owner is doing (observe) or he can use keyboard and mouse as well (interact).

15.1 Assistance

An assisting cooperation is started by a supervisor, selecting a running session and using the "Assist" button in the VISULOX Cockpit.
The user is the owner of the application and he is able to control or close the cooperation.

15.2 Dual control

With the Dual Control feature a cooperation can be established based on a real four-eye-principle. The supervisor has to acknowledge the cooperation within a configured period of time. If the supervisor does not acknowledge the cooperation, the cooperation window will be locked for the participant.

With Dual Control it is guaranteed, that the supervisor is always in front of the screen.

⚠ In applications started without a session controller (nosc) an Assistance or a Dual Control cooperation can only consist of two participants.

⚠ Cooperations without recording cannot determine the user, who did the last input.

15.3 Available articles

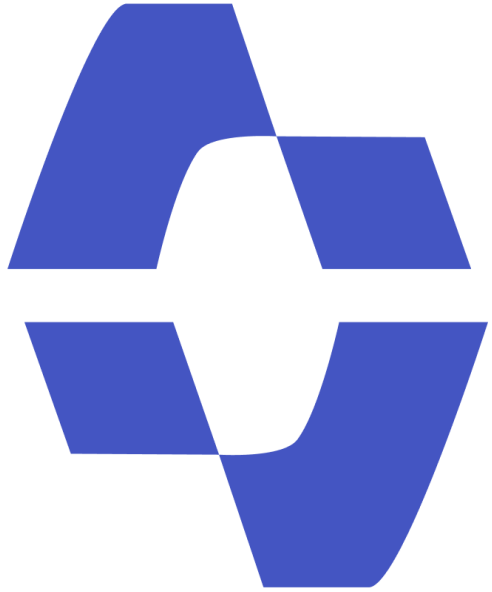
(4.1.1) Assistance

(4.1.1) Cooperations

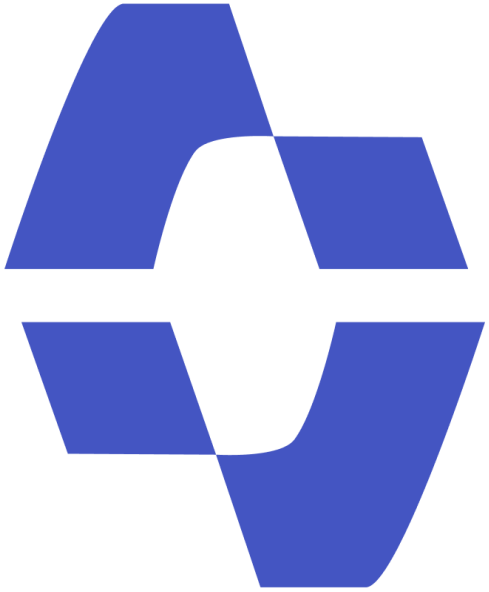
(4.1.1) Dual Control

(4.1.1) Example: Assistance

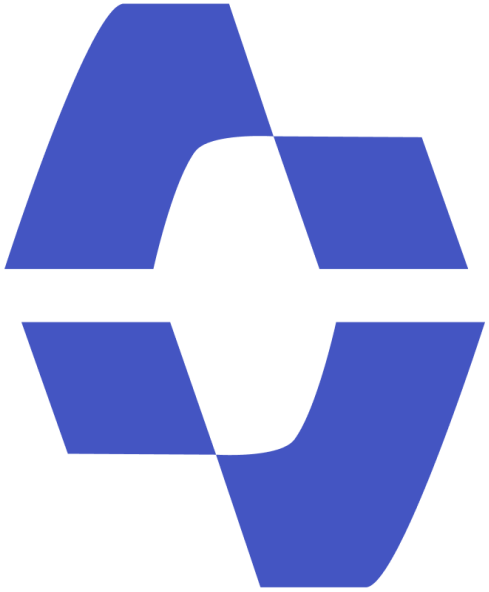
(4.1.1) How to enable Dual Control in the VISULOX Cockpit



(4.1.1) How to enable the VISULOX Cockpit for Dual Control and view films in player
(4.1.1) How to enable, configure and use cooperations
(4.2.0) Assistance
(4.2.0) Cooperations
(4.2.0) Dual Control
(4.2.0) Example: Assistance
(4.2.0) How to enable Dual Control in the VISULOX Cockpit
(4.2.0) How to enable the VISULOX Cockpit for Dual Control and view films in player
(4.2.0) How to enable, configure and use cooperations
(4.3.0) Assistance
(4.3.0) Cooperations
(4.3.0) Dual Control
(4.3.0) Example: Assistance
(4.3.0) How to enable Dual Control in the VISULOX Cockpit
(4.3.0) How to enable the VISULOX Cockpit for Dual Control and view films in player
(4.3.0) How to enable, configure and use cooperations
(4.3.1) Assistance
(4.3.1) Cooperations
(4.3.1) Dual Control
(4.3.1) Example: Assistance
(4.3.1) Example: Dual Control
(4.3.1) How to enable Dual Control in the VISULOX Cockpit



(4.3.1) How to enable the VISULOX Cockpit for Dual Control and view films in player
(4.3.1) How to enable, configure and use cooperations
(4.3.2) Assistance
(4.3.2) Cooperations
(4.3.2) Dual Control
(4.3.2) Example: Assistance
(4.3.2) Example: Dual Control
(4.3.2) How to enable Dual Control in the VISULOX Cockpit
(4.3.2) How to enable the VISULOX Cockpit for Dual Control and view films in player
(4.3.2) How to enable, configure and use cooperations
(4.3.3) Assistance
Cooperations
(4.3.3) Dual Control
Example: Assistance
Example: Dual Control
How to enable Dual Control in the VISULOX Cockpit
How to enable the VISULOX Cockpit for Dual Control and view films in player
How to enable, configure and use cooperations
(4.1.1) Example: Dual Control
(4.2.0) Example: Dual Control
(4.3.0) Example: Dual Control
Assistance



Cooperations
Dual Control
Example: Assistance
Example: Dual Control
How to enable Dual Control in the VISULOX Cockpit
How to enable the VISULOX Cockpit for Dual Control and view films in player
How to enable, configure and use cooperations

16 Notifications

Notifications are used to inform supervisors and users about a variety of actions via eMail or SMS, e.g. login, application start/stop, recording start/stop, access ending, keystroke detected, etc.

It is possible to create individual notification scripts, that can be enriched with a bunch of variables.

16.1 Available articles

(4.1.1) How to control action scripts from the command line

(4.1.1) How to create and use notifications

(4.1.1) Notifications

(4.1.1) Transit script variables

(4.1.1) Variables in notifications

(4.2.0) How to control action scripts from the command line

(4.2.0) How to create and use notifications

(4.2.0) Notifications

(4.2.0) Transit script variables

(4.2.0) Variables in notifications

(4.2.0) VISULOX Mail Client and Send PIN

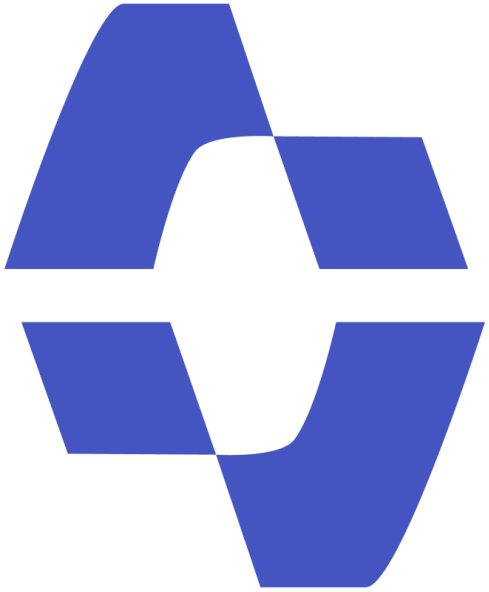
(4.3.0) How to control action scripts from the command line

(4.3.0) How to create and use notifications

(4.3.0) Notifications

(4.3.0) Transit script variables

(4.3.0) Variables in notifications



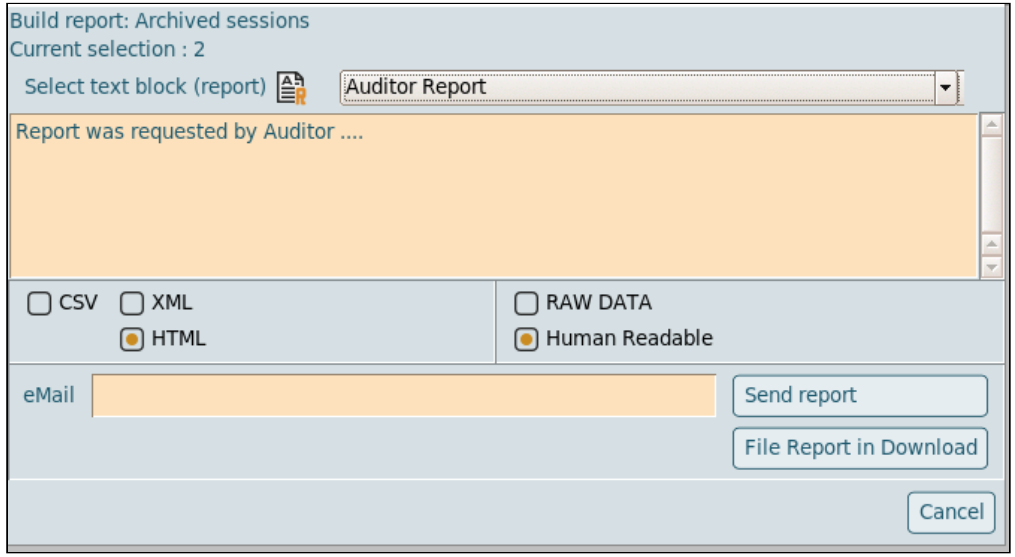
(4.3.0) VISULOX Mail Client and Send PIN
(4.3.1) How to control action scripts from the command line
(4.3.1) How to create and use notifications
(4.3.1) Notifications
(4.3.1) Transit script variables
(4.3.1) Variables in notifications
(4.3.1) VISULOX Mail Client and Send PIN
(4.3.2) How to control action scripts from the command line
(4.3.2) How to create and use notifications
(4.3.2) Notifications
(4.3.2) Transit script variables
(4.3.2) Variables in notifications
(4.3.2) VISULOX Mail Client and Send PIN
How to control action scripts from the command line
How to create and use notifications
Notifications
Transit script variables
Variables in notifications
VISULOX Mail Client and Send PIN
(4.1.1) VISULOX Mail Client and Send PIN
How to control action scripts from the command line
How to create and use notifications

Notifications
Transit script variables
Variables in notifications
VISULOX Mail Client and Send PIN

17 Reports

A variety of reports can be generated within the VISULOX Cockpit or via the command line.

It is possible to generate the reports and file them in the File Transit Zone of the user or to send them via eMail.

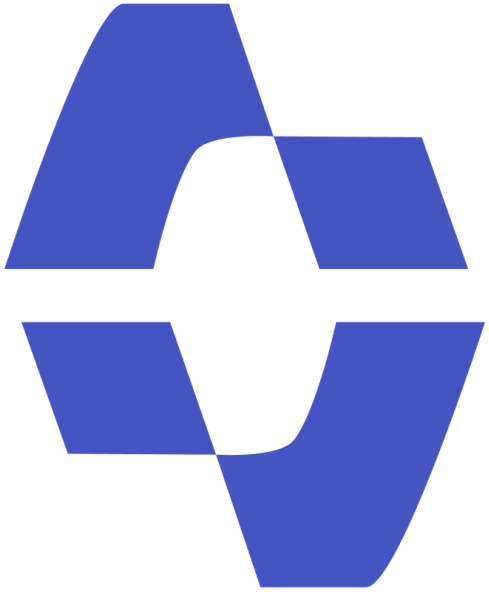


17.1 Available articles

(4.1.1) Command "visulox support" - Creating a VISULOX Support Report

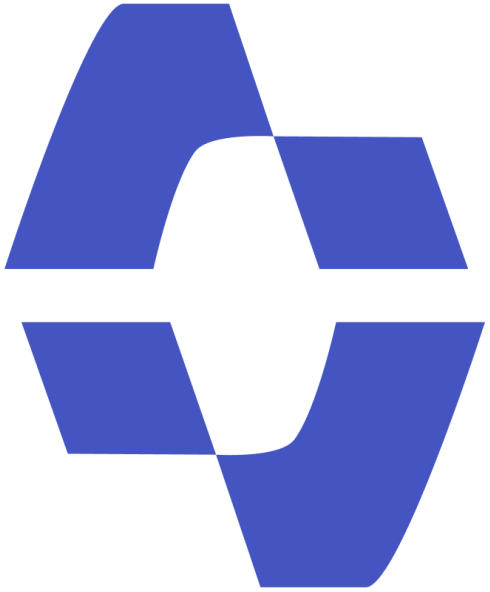
(4.1.1) How to control reports from the command line

(4.1.1) How to export information interactive from VISULOX



(4.1.1) Reports
(4.2.0) Command "visulox support" - Creating a VISULOX Support Report
(4.2.0) How to control reports from the command line
(4.2.0) How to export information interactive from VISULOX
(4.2.0) Reports
(4.3.0) Command "visulox support" - Creating a VISULOX Support Report
(4.3.0) How to control reports from the command line
(4.3.0) How to export information interactive from VISULOX
(4.3.0) Reports
(4.3.1) Command "visulox support" - Creating a VISULOX Support Report
(4.3.1) How to control reports from the command line
(4.3.1) How to export information interactive from VISULOX
(4.3.1) Reports
(4.3.2) Command "visulox support" - Creating a VISULOX Support Report
(4.3.2) How to control reports from the command line
(4.3.2) How to export information interactive from VISULOX
(4.3.2) Reports
Command "visulox support" - Creating a VISULOX Support Report
How to control reports from the command line
How to export information interactive from VISULOX
Reports
Command "visulox support" - Creating a VISULOX Support Report

How to control reports from the command line
How to export information interactive from VISULOX
Reports



18 VISULOX Addons

18.1 Host Control (Command Connect / Guard)

Host Control consist of two applications named **Command Connect** and **Command Guard** that provide a more flexible way to access endpoints using a shell interface. Command Connect and Command Guard handle flexible groups and allows the user to send commands to multiple endpoints simultaneously. Additionally, Command Guard has command level controls for the application. It allows and denies the usage of certain commands by the user. Additionally, client and server side scripts can be issued either to multiple endpoints or to a single one. Remaining faithful to the whole VISULOX concept, no agents are needed on the endpoints to achieve this.

18.2 File Transfer

VISULOX File Transfer guarantees that security zones are not connected and remain separate. In contrast to other solutions this is a true logical split of secure protocols. Multiple transfer policies to different endpoints can be defined. (direction, content, size). Also, the transferred files are provided to the users through their home directory or via a FTP server in a controlled manner.

18.3 File Transit Zone

The directory "**vlxtransit**" is available in the VISULOX Addons and handles the connection between the user from the remote side and the internal systems. Between these components is the VISULOX File Transfer faciltiy, which controls the transfer of files.

- Files are placed into **vlxtransit**
- A protocol file regarding the synced files is created in the Transit Zone for the user.

VISULOX provides interfaces to the following connections via the **VLX Tranist User** and **VLX Jump**.

In this shell die File Transit Zone is seen and can be used, either directly or via drive redirection.

18.4 Host Objects

Host objects define the connection to a host and are available for File Transit, Command Guard and Command Connect groups.
Private hosts can be added to a Command Connect group by the user according to the underlying rules.

18.5 Script objects

Shell scripts can be used in Command Guard on the **system side**.
System side scripts are assigned to Command Guard and can be issued to the terminals at any time. As long the terminals belong to the group.

RDP files can be used for a freerdp connection in a vlxshell application.

18.6 Available articles

Host Control (Command Connect / Guard)	File Tansfer / File Exchange
(4.1.1) Additional events for Command Connect / Guard	(4.1.1) Accessing the File Exchange web page
(4.1.1) Command Connect / Guard and FT Client with empty filters	(4.1.1) Allowing File Transfer from internal to internal
(4.1.1) Configuration of Host Control in the VISULOX Cockpit	(4.1.1) Automated transfer of files into Transit Zone (Passon)
(4.1.1) Host Control (Command Connect / Guard)	(4.1.1) Command Connect / Guard and FT Client with empty filters
(4.1.1) How to use SSH-Keys within Command Connect / Guard and FT Client	(4.1.1) Configuration of File Transfer in the VISULOX Cockpit
(4.1.1) Private host tool	(4.1.1) Custom vlxuser ID for transit users
(4.1.1) VISULOX addon command line interface (CMD Connect / Guard, etc)	(4.1.1) Extended Transit Policy with hash check by provided hash file
(4.2.0) Command Connect / Guard and FT Client with empty filters	(4.1.1) File Transfer
(4.2.0) Configuration of Host Control in the VISULOX Cockpit	(4.1.1) File Transfer features
(4.2.0) Host Control (Command Connect / Guard)	(4.1.1) File Transfer modules
(4.2.0) How to use SSH-Keys within Command Connect / Guard and FT Client	(4.1.1) File Transfer recommendations
(4.2.0) Private host tool	(4.1.1) File Transit with approval
(4.2.0) VISULOX addon command line interface (CMD Connect / Guard, etc)	(4.1.1) How to configure File Transfer content check
(4.3.0) Command Connect / Guard and FT Client with empty filters	(4.1.1) How to control FT Client from the command line
(4.3.0) Configuration of Host Control in the VISULOX Cockpit	(4.1.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.0) Host Control (Command Connect / Guard)	(4.1.1) How to use SSH-Keys within Command Connect / Guard and FT Client
	(4.1.1) Transit Policy
	(4.1.1) Transit script variables

(4.3.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.0) Private host tool
(4.3.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.1) Additional events for Command Connect / Guard
(4.3.1) Command Connect / Guard - X11 statement
(4.3.1) Command Connect / Guard and FT Client with empty filters
(4.3.1) Command Guard limitations
(4.3.1) Configuration of Host Control in the VISULOX Cockpit
(4.3.1) Host Control (Command Connect / Guard)
(4.3.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.1) Private host tool
(4.3.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.2) Additional events for Command Connect / Guard
(4.3.2) Command Connect / Guard - X11 statement
(4.3.2) Command Connect / Guard and FT Client with empty filters
(4.3.2) Command Guard limitations
(4.3.2) Configuration of Host Control in the VISULOX Cockpit
(4.3.2) Host Control (Command Connect / Guard)
(4.3.2) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.1.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.1.1) VISULOX Transit mapping
(4.1.1) VISULOX Transit Mapping and Ubuntu application servers
(4.1.1) VISULOX4_FileTransfer_(VFT)
(4.2.0) Accessing the File Exchange web page
(4.2.0) Automated transfer of files into Transit Zone (Passon)
(4.2.0) Command Connect / Guard and FT Client with empty filters
(4.2.0) Configuration of File Transfer in the VISULOX Cockpit
(4.2.0) Extended Transit Policy with hash check by provided hash file
(4.2.0) File Transfer
(4.2.0) File Transfer features
(4.2.0) File Transfer modules
(4.2.0) File Transit with approval
(4.2.0) How to configure File Transfer content check
(4.2.0) How to control File Transit Policy from the command line
(4.2.0) How to control FT Client from the command line
(4.2.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.2.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.2.0) Transit Policy
(4.2.0) Transit script variables
(4.2.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.2.0) VISULOX Transit mapping

(4.3.2) Private host tool
(4.3.2) VISULOX addon command line interface (CMD Connect / Guard, etc)
Additional events for Command Connect / Guard
Command Connect / Guard - X11 statement
Command Connect / Guard and FT Client with empty filters
Command Guard limitations
Configuration of Host Control in the VISULOX Cockpit
Host Control (Command Connect / Guard)
How to use SSH-Keys within Command Connect / Guard and FT Client
Private host tool
VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.1.1) Command Connect / Guard - X11 statement
(4.1.1) Command Guard limitations
(4.2.0) Additional events for Command Connect / Guard
(4.2.0) Command Connect / Guard - X11 statement
(4.2.0) Command Guard limitations
(4.3.0) Additional events for Command Connect / Guard
(4.3.0) Command Connect / Guard - X11 statement
(4.3.0) Command Guard limitations
Additional events for Command Connect / Guard
Command Connect / Guard - X11 statement
Command Connect / Guard and FT Client with empty filters
(4.2.0) VISULOX Transit Mapping and Ubuntu application servers
(4.2.0) VISULOX4_FileTransfer_(VFT)
(4.3.0) Accessing the File Exchange web page
(4.3.0) Automated transfer of files into Transit Zone (Passon)
(4.3.0) Command Connect / Guard and FT Client with empty filters
(4.3.0) Configuration of File Transfer in the VISULOX Cockpit
(4.3.0) Extended Transit Policy with hash check by provided hash file
(4.3.0) File Transfer
(4.3.0) File Transfer features
(4.3.0) File Transfer modules
(4.3.0) File Transit with approval
(4.3.0) How to configure File Transfer content check
(4.3.0) How to control FT Client from the command line
(4.3.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.0) Object ID
(4.3.0) Transit Policy
(4.3.0) Transit script variables
(4.3.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.0) VISULOX FTP Service
(4.3.0) VISULOX Transit mapping
(4.3.0) VISULOX Transit Mapping and Ubuntu application servers

Command Guard limitations
Configuration of Host Control in the VISULOX Cockpit
Host Control (Command Connect / Guard)
How to use SSH-Keys within Command Connect / Guard and FT Client
Private host tool
VISULOX addon command line interface (CMD Connect / Guard, etc)

Firefox / Chrome / Chromium / Jump Shell

(4.1.1) How to attach Chrome/Chromium download directory to vlxtransit
(4.1.1) How to install Google Chrome
(4.1.1) VISULOX Chrome and Chromium integration
(4.1.1) VISULOX Firefox and Firefox extensions
(4.1.1) VISULOX Firefox CITRIX / ICA integration
(4.1.1) VISULOX Firefox integration
(4.1.1) VISULOX Firefox Wrapper setup
(4.1.1) VISULOX user sandbox (vlxjail)
(4.2.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.2.0) How to install Google Chrome
(4.2.0) VISULOX Chrome and Chromium integration
(4.2.0) VISULOX Firefox and Firefox extensions
(4.2.0) VISULOX Firefox CITRIX / ICA integration
(4.3.0) VISULOX4_FileTransfer_(VFT)
(4.3.1) Accessing the File Exchange web page
(4.3.1) Allowing File Transfer from internal to internal
(4.3.1) Automated transfer of files into Transit Zone (Passon)
(4.3.1) Command Connect / Guard and FT Client with empty filters
(4.3.1) Configuration of File Transfer in the VISULOX Cockpit
(4.3.1) Custom vlxuser ID for transit users
(4.3.1) Extended Transit Policy with hash check by provided hash file
(4.3.1) File Transfer
(4.3.1) File Transfer features
(4.3.1) File Transfer modules
(4.3.1) File Transfer recommendations
(4.3.1) File Transfer via command line
(4.3.1) File Transit with approval
(4.3.1) How to configure File Transfer content check
(4.3.1) How to control File Transit Policy from the command line
(4.3.1) How to control FT Client from the command line
(4.3.1) How to discard filetypes from the Transit Zone synchronisation
(4.3.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.1) Object ID
(4.3.1) Transit Policy

(4.2.0) VISULOX Firefox integration
(4.2.0) VISULOX Firefox Wrapper setup
(4.2.0) VISULOX user sandbox (vlxjail)
(4.3.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.0) How to install Google Chrome
(4.3.0) VISULOX Chrome and Chromium integration
(4.3.0) VISULOX Firefox and Firefox extensions
(4.3.0) VISULOX Firefox CITRIX / ICA integration
(4.3.0) VISULOX Firefox integration
(4.3.0) VISULOX Firefox Wrapper setup
(4.3.0) VISULOX user sandbox (vlxjail)
(4.3.1) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.1) How to create a persistent Firefox profile for VISULOX integration
(4.3.1) How to install Google Chrome
(4.3.1) VISULOX Chrome and Chromium integration
(4.3.1) VISULOX Firefox and Firefox extensions
(4.3.1) VISULOX Firefox CITRIX / ICA integration
(4.3.1) VISULOX Firefox integration
(4.3.1) VISULOX Firefox Wrapper setup
(4.3.1) VISULOX user sandbox (vlxjail)
(4.3.1) Transit script variables
(4.3.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.1) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.1) VISULOX FTP Service
(4.3.1) VISULOX Transit mapping
(4.3.1) VISULOX Transit Mapping and Ubuntu application servers
(4.3.1) VISULOX4_FileTransfer_(VFT)
(4.3.2) Accessing the File Exchange web page
(4.3.2) Allowing File Transfer from internal to internal
(4.3.2) Automated transfer of files into Transit Zone (Passon)
(4.3.2) Command Connect / Guard and FT Client with empty filters
(4.3.2) Configuration of File Transfer in the VISULOX Cockpit
(4.3.2) Custom vlxuser ID for transit users
(4.3.2) Extended Transit Policy with hash check by provided hash file
(4.3.2) File Transfer
(4.3.2) File Transfer features
(4.3.2) File Transfer modules
(4.3.2) File Transfer recommendations
(4.3.2) File Transfer via command line
(4.3.2) File Transit with approval
(4.3.2) How to configure File Transfer content check
(4.3.2) How to control File Transit Policy from the command line

(4.3.2) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.2) How to create a persistent Firefox profile for VISULOX integration
(4.3.2) How to install Google Chrome
(4.3.2) VISULOX Chrome and Chromium integration
(4.3.2) VISULOX Firefox and Firefox extensions
(4.3.2) VISULOX Firefox CITRIX / ICA integration
(4.3.2) VISULOX Firefox integration
(4.3.2) VISULOX Firefox Wrapper setup
(4.3.2) VISULOX user sandbox (vlxjail)
How to attach Chrome/Chromium download directory to vlxtransit
How to create a persistent Firefox profile for VISULOX integration
How to install Google Chrome
VISULOX Chrome and Chromium integration
VISULOX Firefox and Firefox extensions
VISULOX Firefox CITRIX / ICA integration
VISULOX Firefox integration
VISULOX Firefox Wrapper setup
VISULOX user sandbox (vlxjail)
(4.1.1) How to create a persistent Firefox profile for VISULOX integration
(4.2.0) How to create a persistent Firefox profile for VISULOX integration
(4.3.2) How to control FT Client from the command line
(4.3.2) How to discard filetypes from the Transit Zone synchronisation
(4.3.2) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.2) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.2) Object ID
(4.3.2) Transit Policy
(4.3.2) Transit script variables
(4.3.2) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.2) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.2) VISULOX FTP Service
(4.3.2) VISULOX Transit mapping
(4.3.2) VISULOX Transit Mapping and Ubuntu application servers
(4.3.2) VISULOX4_FileTransfer_(VFT)
Accessing the File Exchange web page
Allowing File Transfer from internal to internal
Automated transfer of files into Transit Zone (Passon)
Command Connect / Guard and FT Client with empty filters
Configuration of File Transfer in the VISULOX Cockpit
Custom vlxuser ID for transit users
Extended Transit Policy with hash check by provided hash file
File Transfer
File Transfer features

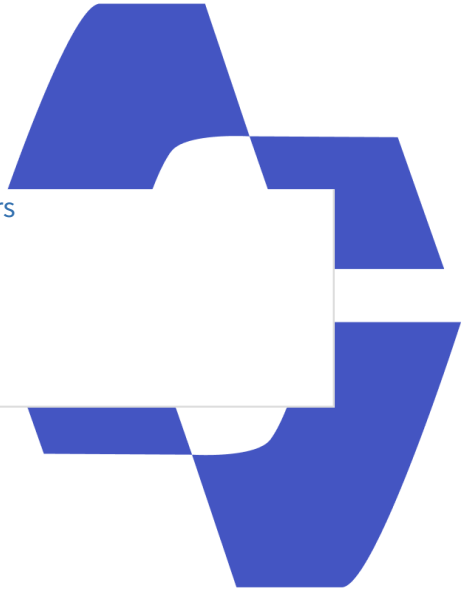
(4.3.0) How to create a persistent Firefox profile for VISULOX integration
How to attach Chrome/Chromium download directory to vlxtransit
How to create a persistent Firefox profile for VISULOX integration
How to install Google Chrome
VISULOX Chrome and Chromium integration
VISULOX Firefox and Firefox extensions
VISULOX Firefox CITRIX / ICA integration
VISULOX Firefox integration
VISULOX Firefox Wrapper setup
VISULOX user sandbox (vlxjail)

Host objects / Script objects

(4.1.1) Host objects
(4.1.1) How to control host objects from the command line
(4.1.1) How to control script objects from the command line
(4.1.1) Private host tool
(4.1.1) Script objects
(4.2.0) Host objects
(4.2.0) How to control host objects from the command line
(4.2.0) How to control script objects from the command line
(4.2.0) Private host tool
(4.3.3) File Transfer modules
File Transfer recommendations
File Transfer via command line
File Transit with approval
How to configure File Transfer content check
How to control File Transit Policy from the command line
How to control FT Client from the command line
How to discard filetypes from the Transit Zone synchronisation
How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
How to use SSH-Keys within Command Connect / Guard and FT Client
Object ID
Transit Policy
Transit script variables
VISULOX addon command line interface (CMD Connect / Guard, etc)
VISULOX File Transit and Sophos Endpoint Security and Control
VISULOX FTP Service
VISULOX Transit mapping
VISULOX Transit Mapping and Ubuntu application servers
(4.3.3) VISULOX4_FileTransfer_(VFT)
(4.1.1) File Transfer via command line
(4.1.1) How to control File Transit Policy from the command line
(4.1.1) How to discard filetypes from the Transit Zone synchronisation

(4.2.0) Script objects
(4.3.0) Host objects
(4.3.0) How to control host objects from the command line
(4.3.0) How to control script objects from the command line
(4.3.0) Private host tool
(4.3.0) Script objects
(4.3.1) Host objects
(4.3.1) How to control host objects from the command line
(4.3.1) How to control script objects from the command line
(4.3.1) Private host tool
(4.3.1) Script objects
(4.3.2) Host objects
(4.3.2) How to control host objects from the command line
(4.3.2) How to control script objects from the command line
(4.3.2) Private host tool
(4.3.2) Script objects
Host objects
How to control host objects from the command line
How to control script objects from the command line
Private host tool
Script objects
Host objects
(4.1.1) Object ID
(4.1.1) VISULOX File Transit and Sophos Endpoint Security and Control
(4.1.1) VISULOX FTP Service
(4.2.0) Allowing File Transfer from internal to internal
(4.2.0) Custom vlxuser ID for transit users
(4.2.0) File Transfer recommendations
(4.2.0) File Transfer via command line
(4.2.0) How to discard filetypes from the Transit Zone synchronisation
(4.2.0) Object ID
(4.2.0) VISULOX File Transit and Sophos Endpoint Security and Control
(4.2.0) VISULOX FTP Service
(4.3.0) Allowing File Transfer from internal to internal
(4.3.0) Custom vlxuser ID for transit users
(4.3.0) File Transfer recommendations
(4.3.0) File Transfer via command line
(4.3.0) How to control File Transit Policy from the command line
(4.3.0) How to discard filetypes from the Transit Zone synchronisation
(4.3.0) VISULOX File Transit and Sophos Endpoint Security and Control
Accessing the File Exchange web page
Allowing File Transfer from internal to internal
Automated transfer of files into Transit Zone (Passon)
Command Connect / Guard and FT Client with empty filters

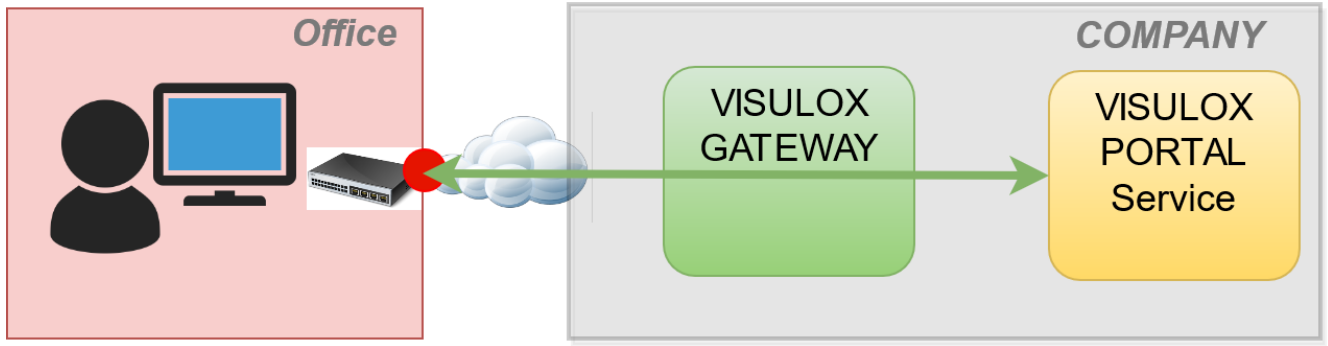
How to control host objects from the command line
How to control script objects from the command line
Private host tool
Script objects
Configuration of File Transfer in the VISULOX Cockpit
Custom vlxuser ID for transit users
Extended Transit Policy with hash check by provided hash file
File Transfer
File Transfer features
File Transfer modules
File Transfer recommendations
File Transfer via command line
File Transit with approval
How to configure File Transfer content check
How to control File Transit Policy from the command line
How to control FT Client from the command line
How to discard filetypes from the Transit Zone synchronisation
How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
How to use SSH-Keys within Command Connect / Guard and FT Client
Object ID
Transit Policy
Transit script variables
VISULOX addon command line interface (CMD Connect / Guard, etc)
VISULOX File Transit and Sophos Endpoint Security and Control
VISULOX FTP Service
VISULOX Transit mapping



19 Remote IP Detection

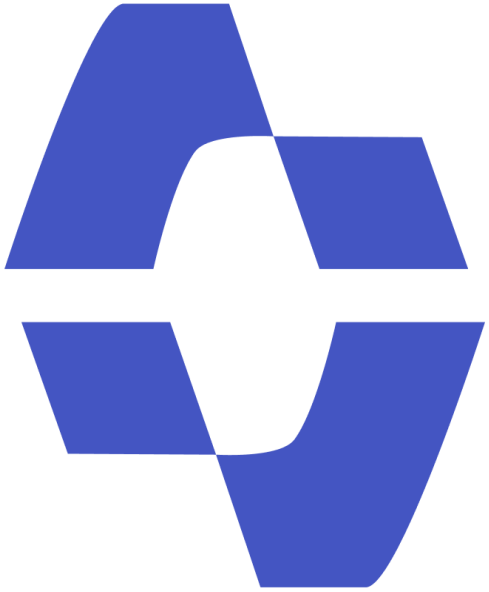
RIP, or Remote IP address, serves as the identifier for where a client request originates from. It essentially provides information about the source of the request.

- Client via nating router via VISULOX GATEWAY to VISULOX PORTAL



VISULOX PORTAL Service: Connection source is the **VISULOX GATEWAY**

VISULOX GATEWAY: Connection source IP is the **router**. GW must forward to VISULOX PORTAL



Available articles:

(4.1.1) How to disable/modify the presentation of the remote IP address on the login page

(4.1.1) Remote IP Detection

(4.2.0) How to disable/modify the presentation of the remote IP address on the login page

(4.2.0) Remote IP Detection

(4.3.0) How to disable/modify the presentation of the remote IP address on the login page

(4.3.0) Remote IP Detection

(4.3.1) How to disable/modify the presentation of the remote IP address on the login page

(4.3.1) Remote IP Detection

(4.3.2) How to disable/modify the presentation of the remote IP address on the login page

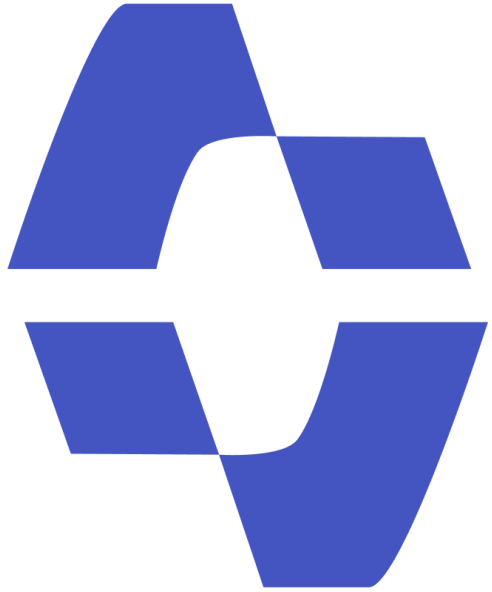
(4.3.2) Remote IP Detection

How to disable/modify the presentation of the remote IP address on the login page

Remote IP Detection

How to disable/modify the presentation of the remote IP address on the login page

Remote IP Detection



20 Monitoring & Logging

The following articles describe how monitoring and logging can be used in VISULOX.

More detailed information about logging and debugging for integrators / administrators is available on request.

20.1 Available articles

Monitoring	Logging
Service fingerprinting via expect script	(4.1.1) Command "visulox log" - Analyzing log files
Monitoring VISULOX	(4.1.1) Enable logging of SQL queries in database service
Monitoring tool: checkPortal.sh	(4.1.1) How to increase the log level
Monitoring & Logging	(4.1.1) Monitoring & Logging
Interface for current usage - stats.sh	(4.2.0) Command "visulox log" - Analyzing log files
Integrity-Check	(4.2.0) How to increase the log level
How to setup VISULOX end2end monitoring	(4.2.0) Monitoring & Logging
How to check VISULOX PORTAL ports 443 & 5307	(4.3.0) Command "visulox log" - Analyzing log files
(4.3.0) Service fingerprinting via expect script	(4.3.0) Enable logging of SQL queries in database service
(4.3.0) Monitoring tool: checkPortal.sh	(4.3.0) Monitoring & Logging
(4.2.0) Service fingerprinting via expect script	(4.3.1) Command "visulox log" - Analyzing log files
(4.2.0) Monitoring tool: checkPortal.sh	(4.3.1) Enable logging of SQL queries in database service
(4.2.0) Integrity-Check	(4.3.1) How to increase the log level
(4.2.0) How to setup VISULOX end2end monitoring	(4.3.1) Monitoring & Logging
(4.1.1) Service fingerprinting via expect script	(4.3.2) Command "visulox log" - Analyzing log files
(4.1.1) Integrity-Check	(4.3.2) Enable logging of SQL queries in database service
Service fingerprinting via expect script	(4.3.2) How to increase the log level
Monitoring VISULOX	(4.3.2) Monitoring & Logging
Monitoring tool: checkPortal.sh	Command "visulox log" - Analyzing log files

Monitoring & Logging
Interface for current usage - stats.sh
Integrity-Check
How to setup VISULOX end2end monitoring
How to check VISULOX PORTAL ports 443 & 5307
(4.3.2) Service fingerprinting via expect script
(4.3.2) Monitoring VISULOX
(4.3.2) Monitoring tool: checkPortal.sh
(4.3.2) Monitoring & Logging
(4.3.2) Interface for current usage - stats.sh
(4.3.2) Integrity-Check
(4.3.2) How to setup VISULOX end2end monitoring
(4.3.2) How to check VISULOX PORTAL ports 443 & 5307
(4.3.1) Service fingerprinting via expect script
(4.3.1) Monitoring VISULOX
(4.3.1) Monitoring tool: checkPortal.sh
(4.3.1) Monitoring & Logging
(4.3.1) Interface for current usage - stats.sh
(4.3.1) Integrity-Check
(4.3.1) How to setup VISULOX end2end monitoring
(4.3.1) How to check VISULOX PORTAL ports 443 & 5307
(4.3.0) Monitoring VISULOX
Enable logging of SQL queries in database service
How to increase the log level
Monitoring & Logging
(4.2.0) Enable logging of SQL queries in database service
(4.3.0) How to increase the log level
Command "visulox log" - Analyzing log files
Enable logging of SQL queries in database service
How to increase the log level
Monitoring & Logging

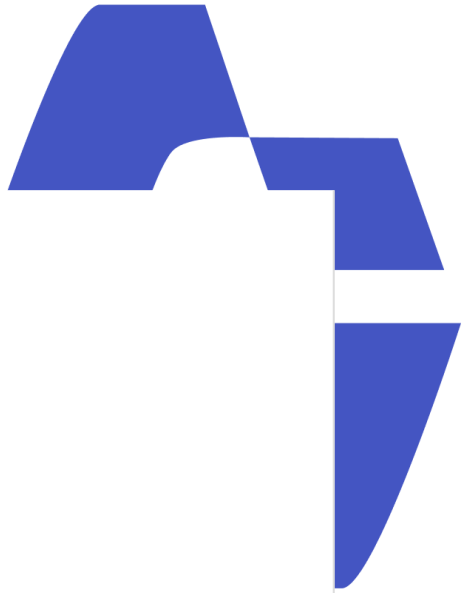
Reporting

(4.1.1) Command "visulox support" - Creating a VISULOX Support Report
(4.1.1) How to control reports from the command line
(4.1.1) How to export information interactive from VISULOX
(4.1.1) Reports
(4.2.0) Command "visulox support" - Creating a VISULOX Support Report
(4.2.0) How to control reports from the command line
(4.2.0) How to export information interactive from VISULOX
(4.2.0) Reports
(4.3.0) Command "visulox support" - Creating a VISULOX Support Report
(4.3.0) How to control reports from the command line
(4.3.0) How to export information interactive from VISULOX
(4.3.0) Reports

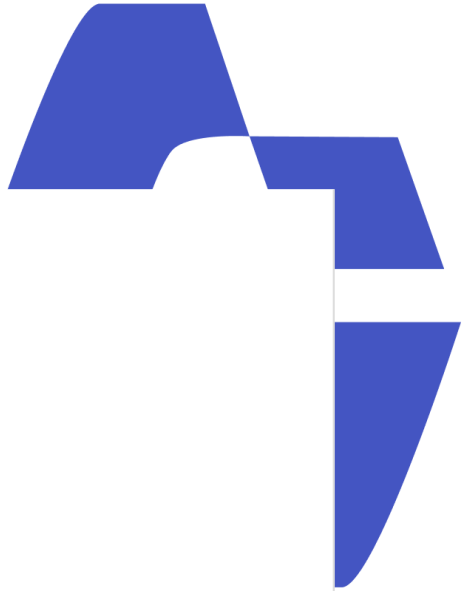
(4.3.0) Monitoring & Logging
(4.3.0) Interface for current usage - stats.sh
(4.3.0) Integrity-Check
(4.3.0) How to setup VISULOX end2end monitoring
(4.3.0) How to check VISULOX PORTAL ports 443 & 5307
(4.2.0) Monitoring VISULOX
(4.2.0) Monitoring & Logging
(4.2.0) Interface for current usage - stats.sh
(4.2.0) How to check VISULOX PORTAL ports 443 & 5307
(4.1.1) Monitoring VISULOX
(4.1.1) Monitoring tool: checkPortal.sh
(4.1.1) Monitoring & Logging
(4.1.1) Interface for current usage - stats.sh
(4.1.1) How to setup VISULOX end2end monitoring
(4.1.1) How to check VISULOX PORTAL ports 443 & 5307

Maintenance

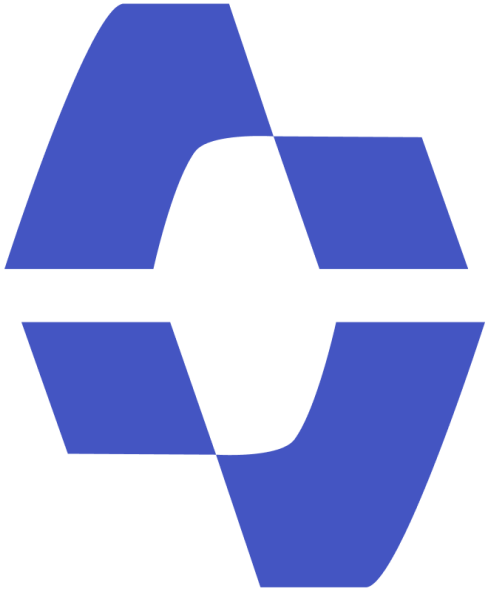
(4.1.1) Gateway Session Balancing
(4.1.1) How to test and check an LDAP datasource in VISULOX
(4.1.1) Private host tool
(4.1.1) Useful database queries: Size of film chapters, snapshots, files, usage
(4.1.1) VISULOX Lifetimes
(4.2.0) Gateway Session Balancing
(4.3.1) Command "visulox support" - Creating a VISULOX Support Report
(4.3.1) How to control reports from the command line
(4.3.1) How to export information interactive from VISULOX
(4.3.1) Reports
(4.3.2) Command "visulox support" - Creating a VISULOX Support Report
(4.3.2) How to control reports from the command line
(4.3.2) How to export information interactive from VISULOX
(4.3.2) Reports
Command "visulox support" - Creating a VISULOX Support Report
How to control reports from the command line
How to export information interactive from VISULOX
Reports
Command "visulox support" - Creating a VISULOX Support Report
How to control reports from the command line
How to export information interactive from VISULOX
Reports



(4.2.0) How to test and check an LDAP datasource in VISULOX
(4.2.0) Private host tool
(4.2.0) Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.0) How to test and check an LDAP datasource in VISULOX
(4.3.0) Private host tool
(4.3.0) Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.0) VISULOX database backup, restore and performance
(4.3.0) VISULOX Lifetimes
(4.3.0) VISULOX Portal maintenance mode
(4.3.1) How to check Policy, Datastore and LDAP assignments
(4.3.1) How to test and check an LDAP datasource in VISULOX
(4.3.1) Private host tool
(4.3.1) Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.1) VISULOX database backup, restore and performance
(4.3.1) VISULOX Lifetimes
(4.3.1) VISULOX Portal maintenance mode
(4.3.2) How to check Policy, Datastore and LDAP assignments
(4.3.2) How to test and check an LDAP datasource in VISULOX
(4.3.2) Private host tool
(4.3.2) Useful database queries: Size of film chapters, snapshots, files, usage
(4.3.2) VISULOX database backup, restore and performance
(4.3.2) VISULOX Lifetimes



(4.3.2) VISULOX Portal maintenance mode
How to check Policy, Datastore and LDAP assignments
How to test and check an LDAP datasource in VISULOX
Private host tool
Useful database queries: Size of film chapters, snapshots, files, usage
VISULOX database backup, restore and performance
VISULOX Lifetimes
VISULOX Portal maintenance mode
(4.1.1) How to check Policy, Datastore and LDAP assignments
(4.1.1) VISULOX database backup, restore and performance
(4.2.0) How to check Policy, Datastore and LDAP assignments
(4.2.0) VISULOX database backup, restore and performance
(4.2.0) VISULOX Lifetimes
(4.3.0) How to check Policy, Datastore and LDAP assignments
How to check Policy, Datastore and LDAP assignments
How to test and check an LDAP datasource in VISULOX
Private host tool
Useful database queries: Size of film chapters, snapshots, files, usage
VISULOX database backup, restore and performance
VISULOX Lifetimes
VISULOX Portal maintenance mode



21 Exporting / Importing Data

These articles describe the export and import of VISULOX data and information via VISULOX Cockpit and the command line.

21.1 **Available articles**

(4.1.1) Exporting / Importing Data

(4.1.1) How to export information from VISULOX on the command line

(4.1.1) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x

(4.1.1) Migrating from VISULOX 3.x to 4.x

(4.1.1) Modify VISULOX PORTAL Datastore via CLI

(4.2.0) Exporting / Importing Data

(4.2.0) How to export information from VISULOX on the command line

(4.2.0) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x

(4.2.0) Migrating from VISULOX 3.x to 4.x

(4.2.0) Modify VISULOX PORTAL Datastore via CLI

(4.3.0) Exporting / Importing Data

(4.3.0) How to export information from VISULOX on the command line

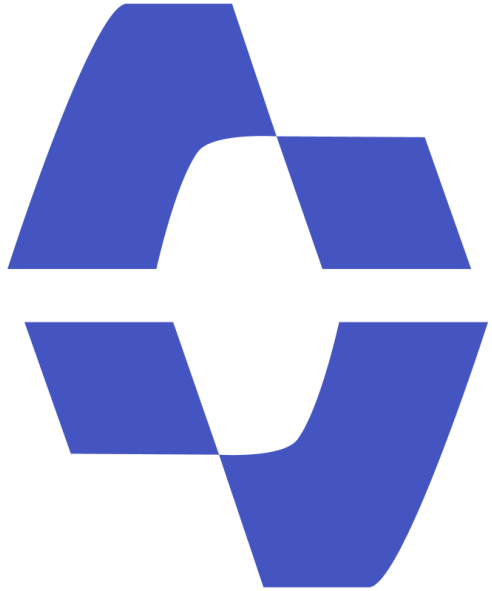
(4.3.0) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x

(4.3.0) Migrating from VISULOX 3.x to 4.x

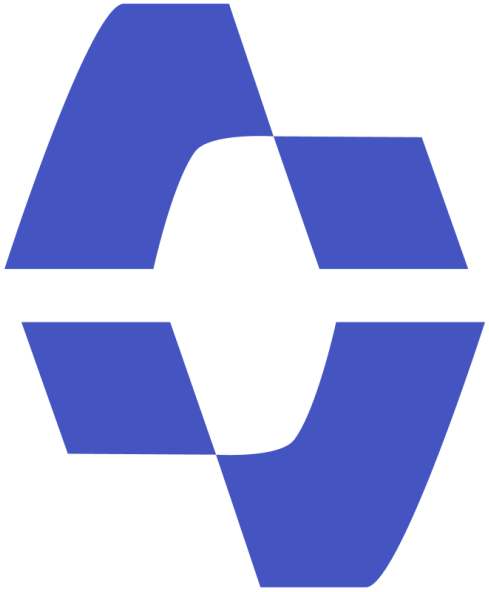
(4.3.0) Modify VISULOX PORTAL Datastore via CLI

(4.3.1) Exporting / Importing Data

(4.3.1) How to export information from VISULOX on the command line



(4.3.1) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.1) Migrating from VISULOX 3.x to 4.x
(4.3.1) Modify VISULOX PORTAL Datastore via CLI
(4.3.2) Exporting / Importing Data
(4.3.2) How to export information from VISULOX on the command line
(4.3.2) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.2) Migrating from VISULOX 3.x to 4.x
(4.3.2) Modify VISULOX PORTAL Datastore via CLI
Exporting / Importing Data
How to export information from VISULOX on the command line
Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
Migrating from VISULOX 3.x to 4.x
Modify VISULOX PORTAL Datastore via CLI
Exporting / Importing Data
How to export information from VISULOX on the command line
Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
Migrating from VISULOX 3.x to 4.x
Modify VISULOX PORTAL Datastore via CLI



22 Appendix_A

22.1 **Appendix**

Reference Card and **Glossary**

- Appendix
  - Events
    - VISULOX Service Events
    - VISULOX PORTAL Service Events
  - Script Interface & Variables
  - Exit Codes
  - Command line parameter
    - VISULOX Command
    - VISULOX PORTAL ATTACH Command
    - VISULOX-PORTAL Command
    - VISULOX-GATEWAY Command
    - Integrity-Check
  - Troubleshooting
  - Glossary

22.1.1 Events

VISULOX Service Events

Type	Event	Description	Event variable
Login	Multiple login failures detected	Default warning setting for failed login attempts: 5 per minute, 20 per hour and 50 per day	multipleloginfailures
Login	Access PIN accepted	Login with Access PIN accepted	2faPinAccepted
Login	Access PIN requested	Access PIN for login requested	2faPinRequested
Login	Access PIN rejected	Access PIN was rejected	2faPinRejected
Login	OTP requested	One Time Passcode for login requested	otpRequested
Login (Webtop)	Logged out by supervisor	Application session ended by supervisor via VISULOX Cockpit	webtopSessionEndedByAdmin
Application	Application started	Application session has been started with session controller	sessionControllerStarted
Application	Application started (uncontrolled)	Application session has been started without session controller	sessionUncontolledStarted

Type	Event	Description	Event variable
Application	Application ended	Application session ended	sessionControllerEnded
Application	Session locked	Application session locked	lock
Application	Session unlocked	Application session unlocked	unlock
Application	Session locked by supervisor	Application session locked by supervisor via VISULOX Cockpit	lockedbyadmin
Application	Session unlocked by supervisor	Application session unlocked by supervisor via VISULOX Cockpit	unlockedbyadmin
Application	Ended by supervisor	Application session ended by supervisor via VISULOX Cockpit	sessionEndedByAdmin
Application	Message sent	Message from supervisor is sent via Cockpit to the user	message
Application	Accepted by user	Message, recording, etc. acknowledged by the user	accept
Application	Rejected	Recording rejected by user	reject
Notification	Notification sent	A notification was sent based on the selected script	scriptsend
Access	Access will expire	Warning, that access to applications will expire soon	
Access	User request	Access requested by the user	accessRequestedByUser

Type	Event	Description	Event variable
Application	Remark by user	Session annotation created by the user	annotationByUser
Application	Remark by supervisor	Annotation created by the supervisor in the VISULOX Cockpit for the session	annotationBySupervisor
Cooperation	Assistance request	Request for a cooperation	assistrequested
Cooperation	Assist observe	Assist mode switched to observe	assistobserve
Cooperation	Assist interact	Assist mode switched to interact	assistinteract
Cooperation	Assist Standby	Assist mode switched to standby	assiststandby
Cooperation	Dual Control	Dual Control cooperation started	dualcontrol
Cooperation	Assistance closed	Cooperation closed	assistclosed
Recording	Manual recording	Manual recording of the session started by the supervisor via VISULOX Cockpit	sessionManuallyRecordingStarted
Recording	Recording stopped	Manual recording stopped by the supervisor via VISULOX Cockpit	sessionManuallyRecordingStopped
Recording	Recording started by Policy	Predefined recording started by Application Policy	sessionRecordingStarted

Type	Event	Description	Event variable
Keyboard control	In use	Input changed to this user	inputFocusChanged
Keyboard control	Inputline	The user entered a line of characters	keyboardControlInputline
Keyboard control	Responsible	Input changed to this user	inputResponsibility
Keyboard control	Idle	Keyboard idle	InputFocusIdle
Keyboard control	Keyboard control started	Keyboard input detection started	keyboardControlStarted
Keyboard control	Keyword detected	Keyword detected by keystroke detection control	keywordDetected
Checkout	Checkout	Session checkout via Cockpit	checkout
Checkout	Checkout with keystrokes	Checkout of the session information in a ZIP file with displayed keystrokes	checkoutwithkeystrokes
Checkout	Report in browser	Report created via Cockpit and displayed in browser	reportGeneratedByGuiBrowser

Type	Event	Description	Event variable
Checkout	Report via eMail	Report created via Cockpit and sent via eMail	reportGeneratedByGuiEmail
Checkout	Player started	Browser-based player started via Cockpit	player
Checkout	Player with keystrokes started	Browser based player with displayed keystrokes started	playerwithkeystrokes
System	Auto accepted	Accepted automatically by the system	autoaccept
System	Auto rejected	Rejected automatically by the system	autoreject
System	Object created	A VISULOX object has been created	objectNew
System	Object copied	A VISULOX object has been copied	objectCopied
System	Object changed	A VISULOX object has been changed	objectChanged
System	Object deleted	A VISULOX object has been deleted	objectDeleted
System	Object attached	A VISULOX object has been attached	objectAttached
System	Object detached	A VISULOX object has been detached	objectDetached
File Transfer	Synced to folder	Files synchronized with the folder	syncput

Type	Event	Description	Event variable
File Transfer	Synced to Transit Zone	Files synchronized with the Transit Zone	syncget
File Transfer	Transfer to server	File transferred from Transit Zone to the application server via SFTP/FTP	ftput
File Transfer	Transfer to Transit Zone	File transferred from application server to the Transit Zone via SFTP/FTP	ftget
File Transfer	Upload (internal web page)	File uploaded via internal web page	webput
File Transfer	Download (internal web page)	File downloaded via internal web page	webget
File Transfer	Upload	File uploaded from client into Transit Zone	userput
File Transfer	Download	File transferred from Transit Zone to the client	userget
File Transfer	File checked	Transferred file has been checked	checked
File Transfer	Approved	Transferred file has been approved	approved
File Transfer	File rejected	File rejected after check	rejected
File Transfer	Pending	File not approved yet	pending
File Transfer	Conditionally accepted	File accepted depending on endpoint rules	tmpaccepted

VISULOX PORTAL Service Events

Type	Event	Description	Event variable
Server	Server started	Server has been started / details	serverStart
Server	Server stopped	Server was stopped / details	serverStop
Server	SSL started	VISULOX PORTAL Security SSL has been started	securitySSLStart
Server	SSL stopped	VISULOX PORTAL Security SSL has been stopped	securitySSLStop
Login	Login rejected	VISULOX PORTAL login was rejected for the user / details	loginResultRejected
Login	Login ambigious	Login information ambiguous, common name needed	loginResultAmbiguous
Login	Anonymous login not supported	Login failed, Anonymous login not supported	loginResultAnonymous
Login	Unresolveable user	Login failed, unresolvable user	loginResultUnresolveable
Workspace	Workspace opened	Workspace session has been started / details	webtopSessionStartedDetails
Workspace	Workspace closed	Workspace session has been stopped / details	webtopSessionEndedDetails
Application	Application session started	Application session has been started / details	sessionStartedDetails

Type	Event	Description	Event variable
Application	Application session stopped	Application session was stopped / details	sessionEndedDetails
VISULOX PORTAL Object	Object modified	VISULOX PORTAL object has been changed	modifySuccess
VISULOX PORTAL Object	Object created	A new VISULOX PORTAL object was created	createSuccess
VISULOX PORTAL Object	Object create failed	Creating an VISULOX PORTALobject failed	createFailure
VISULOX PORTAL Object	Rename successful	VISULOX PORTAL object renamed successfully	renameSuccess
VISULOX PORTAL Object	Object deleted	An VISULOX PORTAL object was deleted	deleteSuccess

22.1.2 Script Interface & Variables

Available script categories

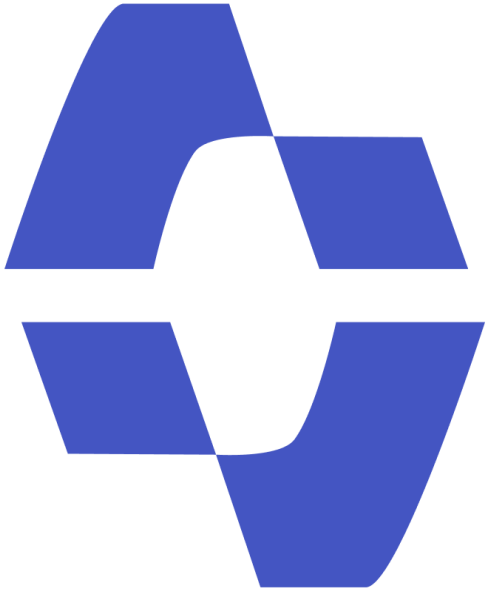
Category	Used as
Notification	These action scripts can be chosen, where application notifications are used (Application Policy).
Pin	These action scripts deliver information for the Multi Factor Authentication (Login Policy).
Report	These are report actions scripts.

Category	Used as
Validate	These action scripts can be chosen for validation.
*	These action scripts are available everywhere scripts can be used. The setup provides one script in this category, which allows to dump all variables provided to an action script. This is helpful for testing.

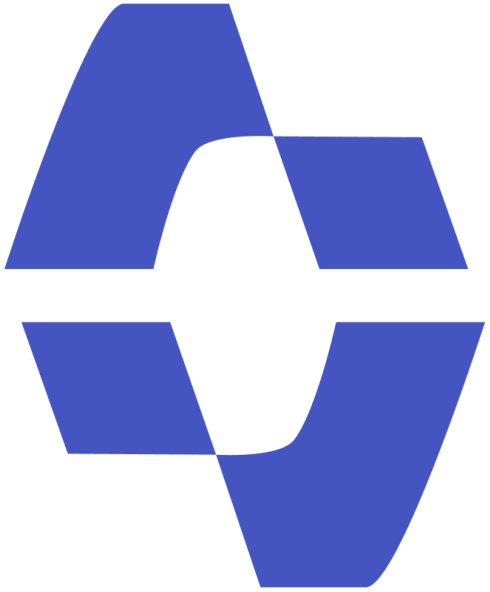
Notification script variables (examples)

The following list contains some useful examples for script variables.
To get the complete list of available variables for a certain action script, the dump script should be used.

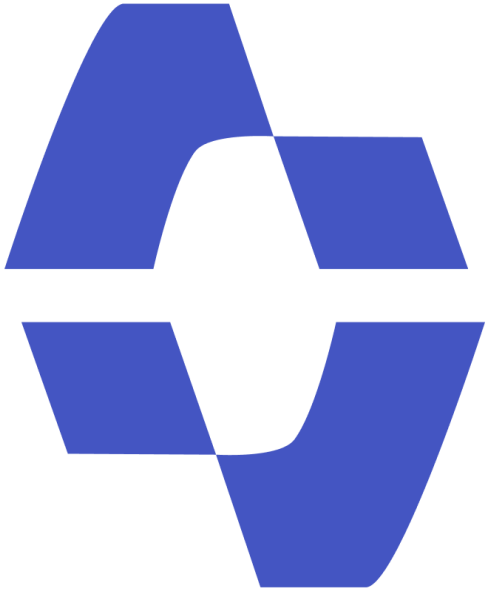
Variable	Description
VLXFULLNAME	Full name of the user
VLXSURNAME	Surname of the user
VLXEMAIL	eMail address of the user
VLXSMS	SMS address of the user
VLXOWNER	Owner of the application
VLXGROUPLIST	Group list



Variable	Description
VLXUSERPROFILE	Profile of the user
VLXPIN	PIN for Multi Factor Authentication
VLXPIN_FMT	Formatted PIN for Multi Factor Authentication
VLXPIN_SEQUENCE	Sequence number for PIN
VLXPIN_EXPIRATIONTIME	Expiration time with date for the PIN
VLXPIN_LIFETIME	Lifetime for the PIN
VLXPIN_TEXT	PIN text
VLXACCESSPOIN	Access Point
VLXCREATETIME	Creation time
VLXLOG	Path to logs
VLXLOGINUSER	Logged in user
VLXMANAGER	Manager of the user



Variable	Description
VLXOBJECT	Name of the object
VLXOWNERID	Owner ID
VLXOWNERSHORT	Short name of the owner
VLXPOLICY	VISULOX policy
VLXREMOTEIP	Remote IP
VLXSMS	SMS of the user
VLXLISTHASH	Hash
VLXCLIENTIP	Client IP address
VLXLANG	Language
VLXSESSIONHOST	Host, where the session was started
VLXCREATETIME_FMT	Time of creation (readable)
VLXSESSIONSTARTTIME	Start time of the sesssion



Variable	Description
VLXSESSIONDURATION	Duration of the session
VLXSESSIONDURATION_FMT	Duration of the session (readable)
VLXSESSIONENDTIME	Endtime of the session
VLXSESSIONENDTIME_FMT	Endtime of the session (readable)
VLXAPPLICATION	Application name
VLXRECIPENT	Recipient
VLXTICKETID	Ticket ID of the user
VLXLOGINSCRIPT	Login script
VLXAPPLICATIONUSER	User of the application
VLXBADWORD	Detected keyword in Keyboard recording
VLXEVENTINFO	Event info
VLXCREATEDBY	Created by

Variable	Description
VLXCREATEDBYSHORT	Short name of creator

See also:

- Variables in notifications
- Transit script variables
- How to control action scripts from the command line

22.1.3 Exit Codes

In the following table all VISULOX Exit Codes are listed with a short description and the meaning of the code.

Exit code	Short description	Comment
0	SUCCESS	Success
1	FAILURE	Failure
2	WARNING	Warning
3	REJECT	Policy
4	ACCEPT	Policy
5	PASSON	Policy

6	APPLY	Policy
7	EXCLUDE	Policy
8	APPROVAL	Rule
9	ALLOW	Rule
10	ALLOWSPONTAN	Rule
11	ALLOWENDPOINT	Transit rule matches, but endpoint has to be taken into account
12	DENY	Deny action
13	DENYTOOLARGE	Transit: file is too large
14	DENYDIRECTION	Transit: file can not be transferred in this direction
15	DENYFORENDPOINT	Transit: file cannot be handled with this endpoint
16	DENYVIRUS	Transit: file has a virus
17	DENYEMPTY	Transit: file is empty
18	DENYPASSON	Transit: script denies Passon

19	NOMATCHPOLICY	Policy
20	USAGE	Command line usage error
21	DATAERR	Data format error
22	NOINPUT	Cannot open input
23	UNKNOWNUSER	User unknown
24	UNKNOWNHOST	Host name unknown
25	UNAVAILABLE	Service unavailable
26	SOFTWARE	Internal software error
27	LICENSE	License error
28	OSERR	System error (e.g. can't fork)
29	OSFILE	Critical OS file missing
30	CANTCREAT	Can't create (user) output file
31	IOERR	Input/output error

32	TEMPFAIL	Temp failure; user is invited to retry
33	PROTOCOL	Remote error in protocol
34	NOPERM	Permission denied
35	CONFIG	Configuration error
36	INIT	Initialization error
37	SCRIPTERROR	Script execution with error
38	DATABASE	Error during database interaction
39	TIMEOUT	Timeout
40	REGISTRATION	Error on registration
41	XAUTH	Error on setting x11 cookie
42	ZMQERROR	ZeroMQ error
43	CRYPTOERROR	Crypto error
44	STARTREJECTED	Start rejected

45	ALREADYRUNNING	Program already running
46	NOTIMPLEMENTED	Not implemented
47	UNDEFINED	Operation has no defined state yet
48	EXHAUSTED	No resource available anymore
49	LOOKUP	Item not found
50	EMPTY	Unexpected empty result
51	RESTART	Restarting...
52	RETRY	Try again
53	OLDREQUEST	Received reply to a previous request
54	TRANSPORT	Error in transport layer
55	QUORUM	No etcd leader
56	ACCESSPOINTCHECK	Access validation
57	BUSY	Resource temporarily unavailable

100	ACCESSREQUEST	Access Policy Request
200	DISABLED	LDAP cannot get data, because the datasource is disabled
210	APPROVALPASSON	Rule
1000	INFO	Info line in integrity test

22.1.4 Command line parameter

VISULOX Command

```
visulox <command> [<command-specific args>]
```

During installation **/usr/sbin/visulox** is created, which makes it possible to execute the VISULOX Service Command without using the whole path.

Available parameters

Command	Description	Additional commands / args
addon	Command Line Interface to VISULOX Addons	cmdconnect, cmdguard, ftclient, host, script, template
admin	Manage the VISULOX Administration	cockpit, action, message, region, timeprofile

Command	Description	Additional commands / args
archive	Manage VISULOX Archive Node	-node <>, -set
assignments	Check assignments in policies and applications	app, datastore, policy
attach	Attach a node to the VISULOX Cluster	<hostname>, -location, -zone
cluster	Builds a VISULOX Cluster	data, layout, build -f <> | -template
cockpit	Start of the VISULOX Cockpit	title <>, lang <>, roles <>, grant <>, groupaccess <>,owner <>, ksr, cdm, kiosk, personal
config	Manage the VISULOX configuration	accesspoint, datasources, dump, edit, env, list, locations,logo, mynodename, rebuild, reset, vap
database	Query the VISULOX Database	list, backup, restore, fields, query, integrity, status -vacuum, rename <>, node <>, table <>, timeout <>
datasource	Manage the VISULOX Datasources	add, check, copy, delete, edit, list
detach	Detach a node from the VISULOX Cluster	server <>, timeout <>
end2end	VISULOX end2end check	off, on, status
etcd	Manage ETCD instances	benchmark, client, del, get, instance, member, node, put, test

Command	Description	Additional commands / args
export	Export from VISULOX	events, files, sessions
integrity	VISULOX Integrity-Check	sys, lib, cmd, users, portal, ulimit, store, recorder, datasources, license
license	Manage the VISULOX License	list, replace, test, usage (-component <users|sessions|recorders|hostcontrols> -unit <week|month|year>)
log	Query VISULOX log database	since <>, until <>, loglevel <>, follow
online	VISULOX online status	getpin, fields (list available fields), -i (ignore case), -object <> (owner or group mask), -application <>, -fields <>, sortby <> (sort by field)
otp	Manage the VISULOX OTP configuration	check <>, key, reset <>, set <>
passcache	Manage the VISULOX Passcache	list, fields, edit, delete
ping	Ping local master or designated worker	id <> (outdated), -retries <>
policy	Command line interface to the VISULOX Policies	external, login, internal, access, application, transit

Command	Description	Additional commands / args
portal	Attach / detach VISULOX Service from VISULOX PORTAL Service (See also: (4.3.3) VISULOX PORTAL ATTACH Command)	array, config, discover, drop, admin, mode, etc (see: (4.3.3) VISULOX-PORTAL Command) visulox portal --help shows all available VISULOX PORTAL and VISULOX commands. With visulox portal admin -user <*unixuser*> a Unix user can be activated as VISULOX Portal Admin (⚠ It is recommended to set a different user than root!)
pwdmgmt	Manage / list account passwords	expired, mustchange, notify <>, warn
report	Command line interface to VISULOX Report	title <>, mctitle <>, name <>, type <>, xslt <>, metadata <>, query <>, tframe <>, -from<>. -to <>, sql <>, lang <>, filename <>, mailto <>, mailsubject <>, maildescription <>, maildescriptionfile <>, archive <>
reset	Reset local cluster state	
restart	Restart VISULOX Service (locally) ⛔ Use with caution, all sg, sc and scx will be stopped.	-service <>, -timeout <>
start	Start VISULOX Service (locally)	debug
status	Query VISULOX status	diskfree, features, load, monitor, next, servers, services, sessions, uptime, usage, users, workers, server <>, serverfilter <>, retries <>, print, fields <>

Command	Description	Additional commands / args
stop	Stop VISULOX Service (locally)	id <>
store	Manage the VISULOX store	attach, changed, detach, disable, enable, extras, get, migrate, missing, next, put, status, slot <>
support	Gather information for support (-info: short report)	directory <>, sys, dump, etc, rt, logs, net, integrity, config, tta
transit	Command line interface to VISULOX Transit Zone (list, import)	list, import, owner, path, rtime
version	Display versions of installed VISULOX packages	

With **-help** or **-?** the detailed options for a basic command can be displayed.
If more parameters are needed for a command, the available options are always displayed by entering the basic command.

General commands

Parameter	Description
-format <*value*>	Format of output (text,xml,csv,json,tcl) / Default: <text>
-log <*value*>	Set loglevel to error, verbose, info or debug / Default: <>
-verbose	More messages on stdout

Parameter	Description
-run	Run an operation (use only on application request)
-stdin	Get arguments from stdin
--	Forcibly stop option processing
-help / -?	Display commands

Usage

The following examples show the usage of the VISULOX Service Command:

Show VISULOX status
`visulox status`

Show license information
`visulox license`

Replace license

```
visulox license replace -file <path to license file>
```

List sessions

```
visulox status sessions
visulox online
```

List unassigned applications

```
visulox database query -sql "select vlxapplication from external_applications WHERE vlxapplicationgroups = '' AND
vlxapplicationusers = ''" -format csv -raw
```

Transit import & list

```
visulox transit import -path /tmp/file.txt  -owner "o=Tarantella System Objects/cn=TestUser"
visulox transit list  -owner "o=Tarantella System Objects/cn=TestUser"
```

Detach VISULOX Node

```
visulox detach <vlx-node.domain>
```

VISULOX PORTAL ATTACH Command

```
visulox portal attach [<command-specific args>]
```

During installation **/usr/sbin/visulox** is created, which makes it possible to execute the VISULOX Service Command without using the whole path.

Available parameters

Command	Description
-all	Install all (default)
-portal	Modify VISULOX PORTAL only, write configuration
-examples	setup examples
-attach	Attach VISULOX Service to VISULOX PORTAL Service
-expect	Install expect script only
-webtop	Install webtop script only
-jspconfig	Create VISULOX JSP configuration file
-apacheport <*value*>	Local port to address Apache. If empty, discovered by webservice configuration <>

Command	Description
-externalport <*value*>	External port to address Apache. If empty, discovered by httpd.conf <>
-serviceonline <*value*>	Enable/disable Webtop Enhancements <true>
-adminuser <*value*>	UNIX user for the VISULOX webservice user in VISULOX PORTAL<vlxwebservice> **Deprecated**! Configuration parameter **portal.admin.user** should be used instead.
-adminuid <*value*>	User ID for the VISULOX admin user in VISULOX PORTAL <610> **Deprecated**! Configuration parameter **portal.admin.uid** should be used instead.
-adminpwd <*value*>	Password for the VISULOX admin user in VISULOX PORTAL <generate>
-adminou <*value*>	OrgUnit for Webservice user cn=<*host name*>/<adminou> <>
-version <*value*>	Force VISULOX PORTAL version <>

General commands

Parameter	Description
-format <*value*>	Format of output (text,xml,csv,json,tcl) / Default: <text>
-verbose	More messages on stdout
-run	Run an operation (use only on application request)

Parameter	Description
--	Forcibly stop option processing
-help / -?	Display commands

Usage

The following examples show the usage of the attach command:

Attaching VISULOX Service to VISULOX PORTAL Service

```
visulox portal attach
```

This command checks if login-ens is enabled. If this is the case a local user vlxwebservice (610) with group ttaserv (500) was added to the system. A password was also generated and stored secure.

VISULOX-PORTAL Command

```
visulox-portal <command> [<command-specific args>]
```

During installation **/usr/sbin/visulox-portal** is created, which makes it possible to execute the VISULOX PORTAL Service Command without using the whole path.

Available parameters

Command	Description
array	Creates and manages arrays of VISULOX PORTAL servers
config	Edits array-wide and server-specific configuration
discover	Discover available resources
drop	Drop discovered resources
emulatorsession	Lists and controls emulator sessions
gateway	Manipulates the VISULOX GATEWAY store
help	Displays this list of commands
info	Shows status information for the local server
object	Manipulates objects in the datastore
passcache	Manipulates the password cache
restart	Restarts VISULOX PORTAL services

Command	Description
role	Configures role occupants and their extra webtop links
security	Controls security services, manages certificates
serverrename	Change the server's peer or external DNS name
service	Edits service object configuration
start	Starts VISULOX PORTAL services
status	Shows the current status of VISULOX PORTAL array members
stop	Stops VISULOX PORTAL services
tokencache	Manipulates the token cache
version	Displays versions of installed VISULOX PORTAL packages
webserver	Controls the VISULOX PORTAL Web Server
webtopsession	Lists and controls webtop sessions

With **visulox-portal <subcommand> --help** the detailed options for a command can be displayed.
If more parameters are needed for a command, the available options are always displayed by entering the basic command.

Usage

The following examples show the usage of the VISULOX-PORTAL Command:

Show VISULOX PORTAL status

```
visulox-portal status
```

Show version information

```
visulox-portal version
```

List webtop sessions

```
visulox-portal webtopsession list
```

List VISULOX Array members

```
visulox-portal array list
```

Join VISULOX Array member

```
visulox-portal array join --primary <hostname> --secondary <hostname>
```

VISULOX-GATEWAY Command

```
visulox-gateway <command> [<command-specific args>]
```

During installation **/usr/sbin/visulox-gateway** is created, which makes it possible to execute the VISULOX GATEWAY Command without using the whole path.

Available parameters

Command	Description
start	Start VISULOX GATEWAY
stop	Stop VISULOX GATEWAY
restart	Restart VISULOX GATEWAY
config	Configuration options: create, list, edit, enable, disable
server	Server options: add, add-array, remove, list, list-array
status	Show VISULOX GATEWAY status
version	Show VISULOX GATEWAY version
sslcert	Export, print sslcert

Command	Description
sslkey	Import, export sslkey
cert	Export the VISULOX GATEWAY certificate
clientcert	Import, list, remove clientcert
key	Import private key and its corresponding certificate
patch	Add, remove, list VISULOX GATEWAY patches
connection	List connections
support	VISULOX Gateway Support Report

With **visulox-gateway <subcommand> --help** the detailed options for a command can be displayed.
If more parameters are needed for a command, the available options are always displayed by entering the basic command.

Usage

The following examples show the usage of the VISULOX-GATEWAY Command:

Show VISULOX GATEWAY status

```
visulox-gateway status
```

Show version information

```
visulox-gateway version
```

List VISULOX PORTAL Servers / certificates

```
visulox-gateway server list
```

Show VISULOX GATEWAY configuration

```
visulox-gateway config list
```

Add the VISULOX Portal Array on external Gateway

```
visulox-gateway server add-array --name osgd --serverurl <https://fqdn of the primary portal server>
```

Integrity-Check

The Integrity-Check is started automatically during installation of VISULOX to make sure, that all requirements are met for a properly running system.

However Integrity-Check can also be used in an already running environment for diagnose purpose.

Integrity-Check can be started via the visulox command:

```
visulox integrity
```

In the quiet mode no shell output and no log entries in **/tmp/visulox-integrity.log** are written.

Only the Integrity-Check exit code will be returned:

```
visulox integrity -quiet
```

Available Integrity-Check commands

Command	Description
-sw	Check of online software status
-vlx	Check the VLX Services and cluster ports
-sys	Check the system environment
-lib	Check for missing libs
-cmd	Check command for missing libraries
-disk	Check disk
-users	Check VISULOX transit users

Command	Description
-portal	Check the VISULOX PORTAL Service
-cert	Check certificates within VISULOX and VISULOX PORTAL
-store	Check store
-recorder	Check recorder
-datasources	Check datasources
-assignments	Check datastore assignments and dynamic applications
-license	Check license
-policies	Check policies (VISULOX must be online)
-index	Check index
-scripts	Check scripts
-x11forward	Check x11forward
-gate	Check gate config

Command	Description
-mail	Check mail configuration

General commands

Command	Description
-format <*value*>	Format of output (text,xml,csv,json,tcl) <*text*>
-verbose	More messages on stdout
--	Forcibly stop option processing
-help	Print this message
-?	Print this message

Usage

```
visulox integrity

Please wait ....
```

```
Integrity-Check: amitego engineering  - in house license / beta2-3.1.1 / 2016-07-12 12:46:32 UTC
    ------------------------------------------------------------------------------
    | option   | cat                                    | info           | returnCode |
    ------------------------------------------------------------------------------
    | -license | check                                  | Evaluation     | WARNING(2) |
    | -sys     | Script /opt/visulox/tools/filecheck.sh | not configured | WARNING(2) |
    | -sys     | Script /opt/visulox/tools/event.sh     | not configured | WARNING(2) |
    | -portal  | 5.60 Warnings                          | see logfile    | WARNING(2) |
    ------------------------------------------------------------------------------

ExitCode: WARNING
Check the warnings. For more information see /tmp/visulox-integrity.log
```

Only warnings and errors are displayed by default. All Integrity checks can be shown with the **-verbose** parameter.

visulox integrity -portal

```
    ------------------------------------------------------------------------
    | option  | cat              | info                        | returnCode |
    ------------------------------------------------------------------------
    | -portal | core             | PORTAL 5.60                 | SUCCESS(0) |
    | -portal | connect          | yes                         | SUCCESS(0) |
    | -portal | webtop           | ok                          | SUCCESS(0) |
    | -portal | var              | security-xsecurity ok       | SUCCESS(0) |
    | -portal | var              | xpe-maxsessions ok          | SUCCESS(0) |
    | -portal | var              | xpe-maxusers ok             | SUCCESS(0) |
    | -portal | role             | administrator is root       | WARNING(2) |
    | -portal | array            | P: mp-vlx32-ol7.tbsol.de    | SUCCESS(0) |
    | -portal | security-gateway | mp-vlx32-ol7.tbsol.de is good | SUCCESS(0) |
    ------------------------------------------------------------------------
```

visulox integrity -cert

```
-----------------------------------------------------------------------------------------------
 | option | cat       | info                                                          | returnCode |
 ----------------------------------------------------------------------------------------------
 | -cert  | SSL-CERT  | issuer  =  /C=de/ST=de/O=amitego/CN=test.tbsol.de             | SUCCESS(0) |
 | -cert  | SSL-CERT  | subject = test.tbsol.de                                       | SUCCESS(0) |
 | -cert  | SSL-CERT  | serial  = EA8628EF3B3A7F44                                    | SUCCESS(0) |
 | -cert  | SSL-CERT  | from    = 2016-12-16 09:12                                    | SUCCESS(0) |
 | -cert  | SSL-CERT  | until   = 2017-12-16 09:12                                    | SUCCESS(0) |
 | -cert  | SSL-CERT  | remain  = 360d 21h                                            | SUCCESS(0) |
 | -cert  | PEER-CERT | issuer  =  /CN=mp-ol6u3-devel.tbsol.de CA Cert                | SUCCESS(0) |
 | -cert  | PEER-CERT | subject = test.tbsol.de CA Cert                               | SUCCESS(0) |
 | -cert  | PEER-CERT | serial  = 9F3D8E05D8800F22                                    | SUCCESS(0) |
 | -cert  | PEER-CERT | from    = 2013-07-15 12:20                                    | SUCCESS(0) |
 | -cert  | PEER-CERT | until   = 2023-07-13 12:20                                    | SUCCESS(0) |
 | -cert  | PEER-CERT | remain  = 2395d 23h                                           | SUCCESS(0) |
 | -cert  | SSL-CA    | issuer  =  /C=de/ST=de/O=amitego/CN=test.tbsol.de             | SUCCESS(0) |
 | -cert  | SSL-CA    | subject = test.tbsol.de                                       | SUCCESS(0) |
 | -cert  | SSL-CA    | serial  = EA8628EF3B3A7F44                                    | SUCCESS(0) |
 | -cert  | SSL-CA    | from    = 2016-12-16 09:12                                    | SUCCESS(0) |
 | -cert  | SSL-CA    | until   = 2017-12-16 09:12                                    | SUCCESS(0) |
 | -cert  | SSL-CA    | remain  = 360d 21h                                            | SUCCESS(0) |
 ----------------------------------------------------------------------------------------------
```

Integrity check with the parameter **-cert** shows the status of the both VISULOX PORTAL certificates. PEER-CERT and SSL-CERT.

The serials can be displayed on the local VISULOX GATEWAY with the command **visulox-gateway server list** and have to match with the serials of the VISULOX PORTAL certificates.

Integrity check shows a warning, when the lifetime is lower than 30 days or an error when the lifetime is expired.

visulox integrity -disk

```
Please wait ...Integrity-Check: VISULOX EVALUATION / xdevelopment / development
    ------------------------------------------------------------------------------------------
    | option | cat          | info                                                  | returnCode |
    ------------------------------------------------------------------------------------------
    | -disk  | Diskspace    | ok in base (base threshold at 2.0GB has 39.67GB)  | SUCCESS(0) |
    | -disk  | Diskspace    | ok in var (var threshold at 5.0GB has 39.67GB)    | SUCCESS(0) |
    | -disk  | Diskspace    | ok in data (data threshold at 20.0GB has 39.67GB) | SUCCESS(0) |
    | -disk  | Diskspace    | ok                                                | SUCCESS(0) |
    | -disk  | DB Partition | ok fileserver.tbsol.de:/home/users/xxx            | SUCCESS(0) |
    | -disk  | DB Partition | needs atleast 157.30MB - has 39.67GB              | SUCCESS(0) |
    ------------------------------------------------------------------------------------------
ExitCode: SUCCESS
```

Among the checks also the diskspace for the database is checked. 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 integriy check.

Troubleshooting

- **VISULOX PORTAL connect failure**

  On servers, where VISULOX Service is installed together with VISULOX PORTAL Service, the connection to the VISULOX PORTAL Service can be checked with a small tool:

```
/opt/visulox/lib/utils/sgd.tcl check

Check connections

-------------------------------------------------------------------------------------------------------------------------------
```

```
    |                                        scottasessionid |                                        scottasessionowner
|

-----------------------------------------------------------------------------------------------------------------------------
    | test-ol6u5.tbsol.de:1434362892796:1108252004568201775 | {.../_ens/o=Tarantella System Objects/ou=Visulox/cn=test-ol6u5}
|

-----------------------------------------------------------------------------------------------------------------------------
```

The following command reinstalls the necessary VISULOX PORTAL Service components on the server and mostly fixes connection errors:

```
visulox portal attach
```

- **VISULOX PORTAL Service warnings**

  More details can be found in visulox-integrity.log. The Java tuning values should be adjusted for the environment.
  Mostly, the following settings will be adequate:
  - tuning-jvm-initial: 1024
  - tuning-jvm-max: 2048
  - tuning-jvm-scale: 150

Adjust the values, with:

```
visulox-portal config edit --tuning-jvm-initial 2048
visulox-portal config edit --tuning-jvm-max 2048
visulox-portal config edit --tuning-jvm-scale 150
```

The following VISULOX PORTAL Service default values should also be checked:

- sessions-timeout-always
- sessions-timeout-session

- webtop-session-idle-timeout

Changes of VISULOX PORTAL Service configurations is known to VISULOX after "**visulox portal attach -portal**".

- **"Administrator is root" warning**

  The warning can be disabled by adding a new administrator to VISULOX PORTAL:

  Add a user

  ```
  useradd <name of the new portal administrator>
  passwd <name of the new portal administrator>
  ```

  Add the new administrator to the VISULOX PORTAL administrators

  ```
  visulox-portal object edit --name "/o=tarantella system objects/cn=administrator" --user admin
  ```

  After changes to the VISULOX PORTAL, VISULOX needs to be reregistered

  ```
  visulox portal attach
  ```

  Doing a VISULOX Integrity-Check again, the warning has disappeared. root can be removed from the administrators list.

- **event.sh and filecheck.sh missing**

  The files event.sh.template and filecheck.sh.template in **/opt/visulox/tools/** must be copied to event.sh and filecheck.sh, if needed.

The correct permission (**0550 / vlx:vlxgroup**) has to be set as well for these files.

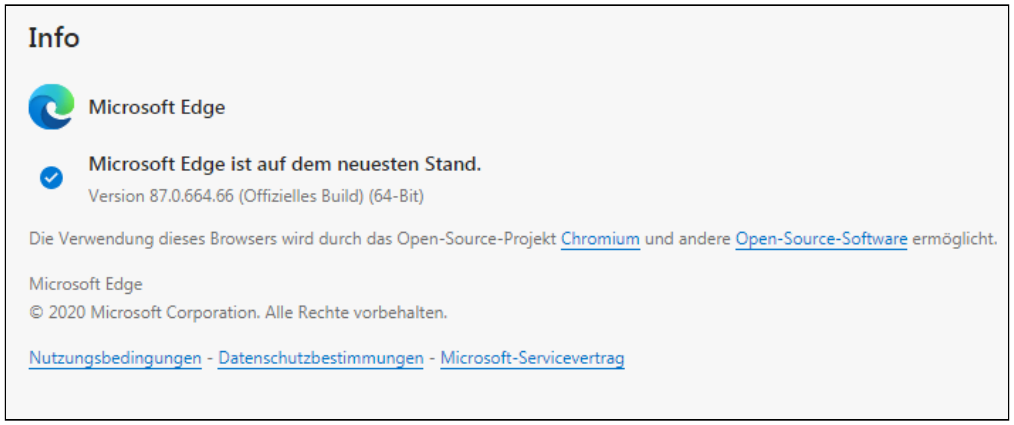
```
cd /opt/visulox/tools
cp events.sh.tmplate events.sh
cp filecheck.sh.template filecheck.sh
chown vlx: events.sh filecheck.sh
chmod 0550 events.sh filecheck.sh
```

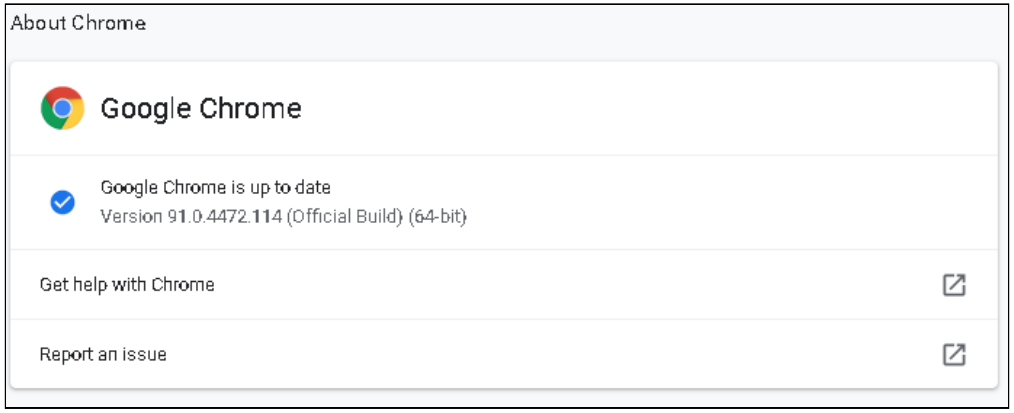
22.1.5 Troubleshooting

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

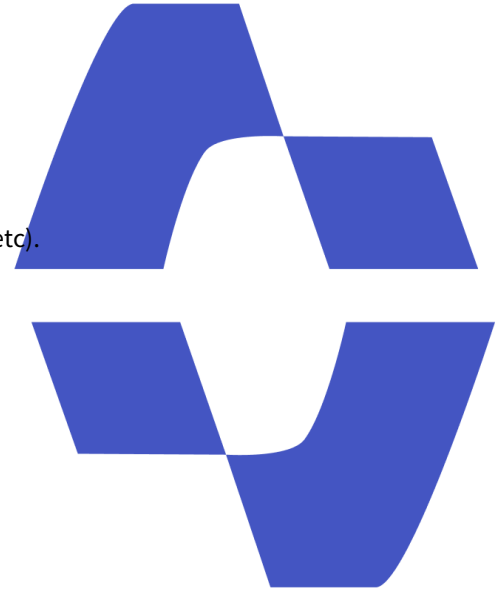
Version of the used browser

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

Microsoft Edge		Help and Feedback / Info about Microsoft Edge

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

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



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

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

Disable sleeping tabs in Microsoft Edge:

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

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

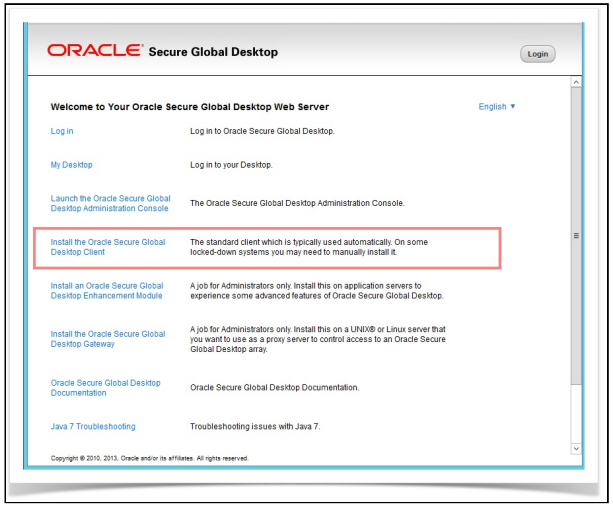
After these changes, please set the following parameter on the VISULOX side:

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

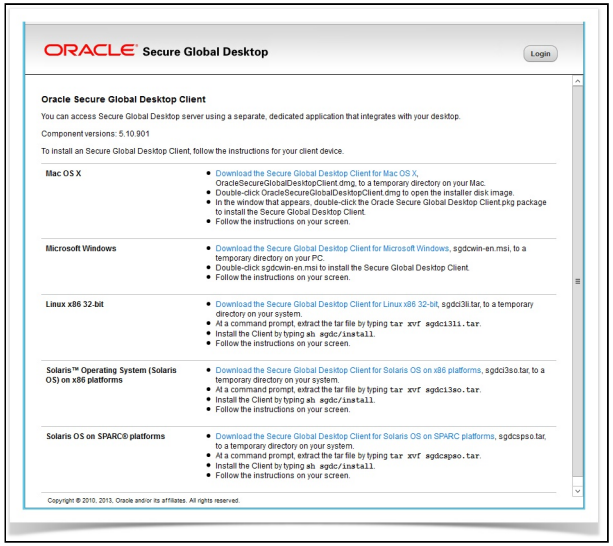
Native Client

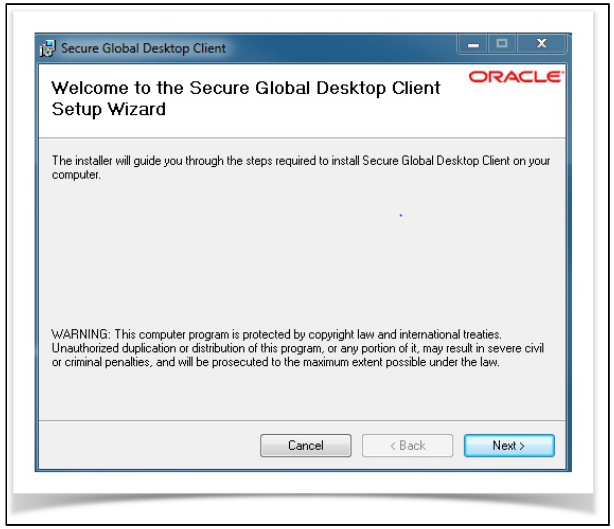
In case of problems with the automatic download of the native client, it can be downloaded and installed manually, if no direct forwarding to the login page is configured.

> The Native Client is provided by Oracle.

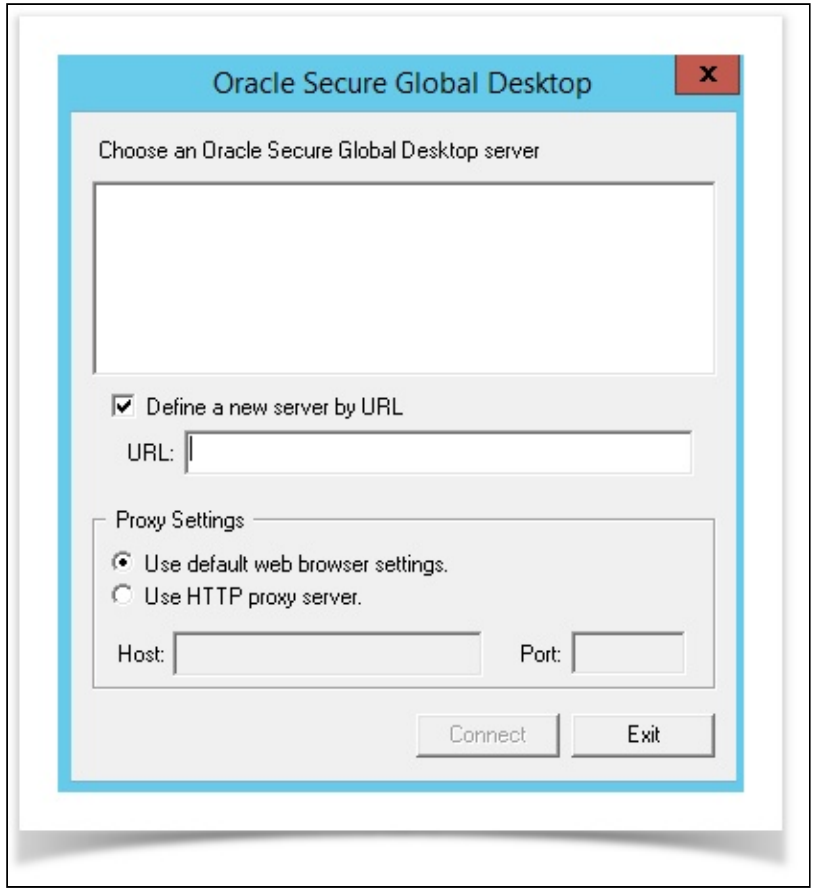
Native Client	

Client versions



Installation	

After installation, the Native Client can be started manually:

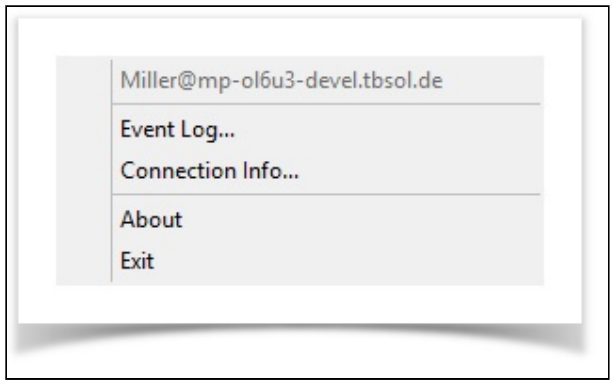


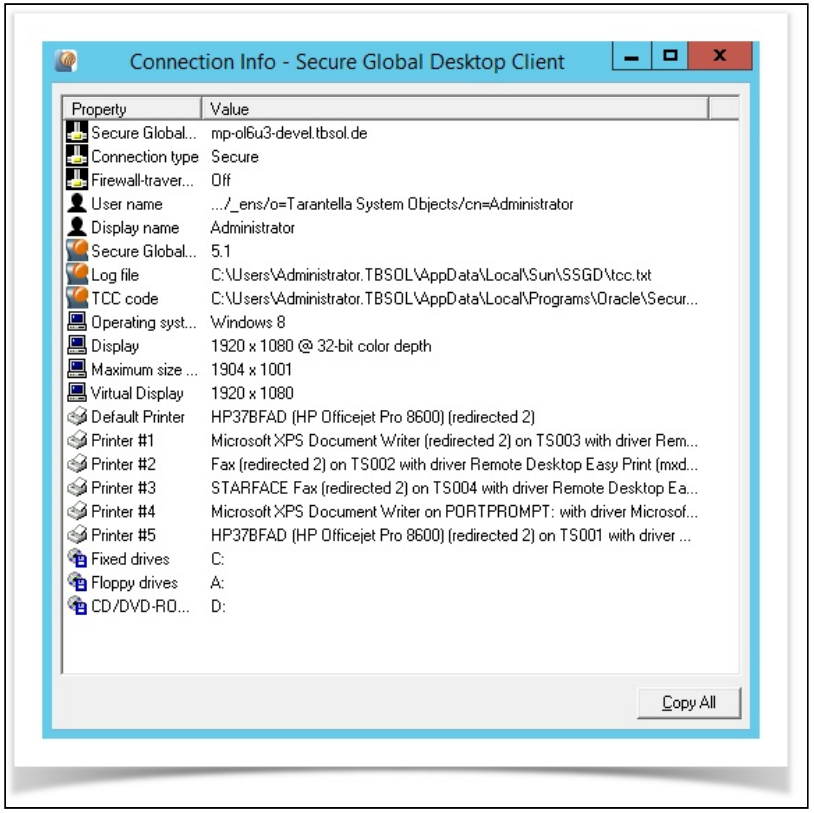
How to install the client for Linux Mint

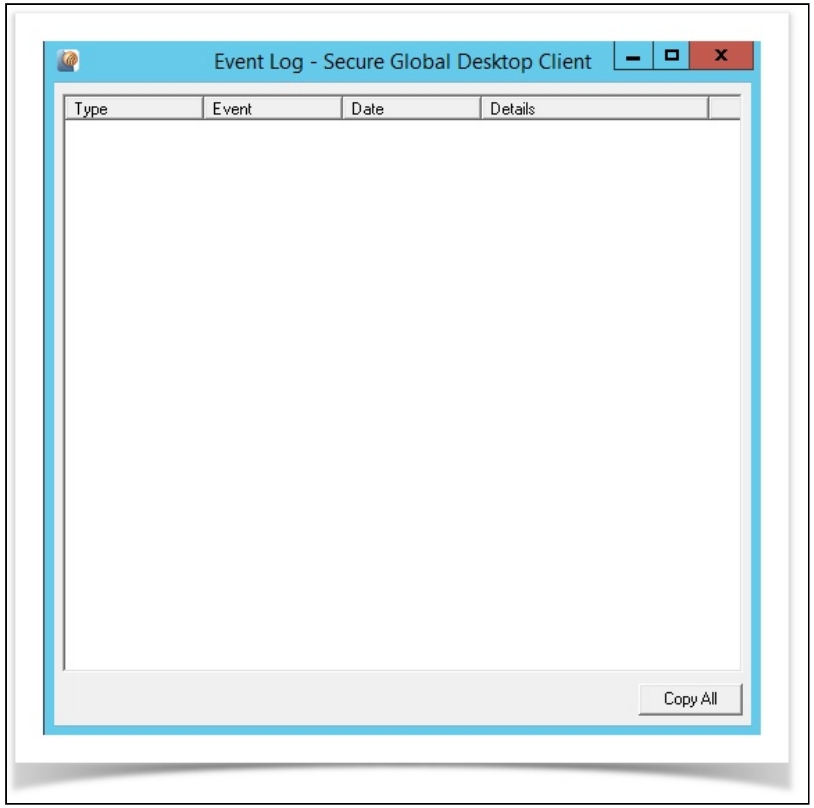
```
sudo dpkg -i ./sgdclient_5.60.567-ubuntu22.04_x86_x64.deb
sudo apt-get install libxm4 libmotif-common
```

Tarantella Client Component (TCC)

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

TCC taskbar-menu	

Connection Info	

Event Log	

General: Special characters in passwords

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

Therefore the following rules should be considered:

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

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

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

VISULOX has been tested with these characters.

VISULOX PORTAL Login error codes

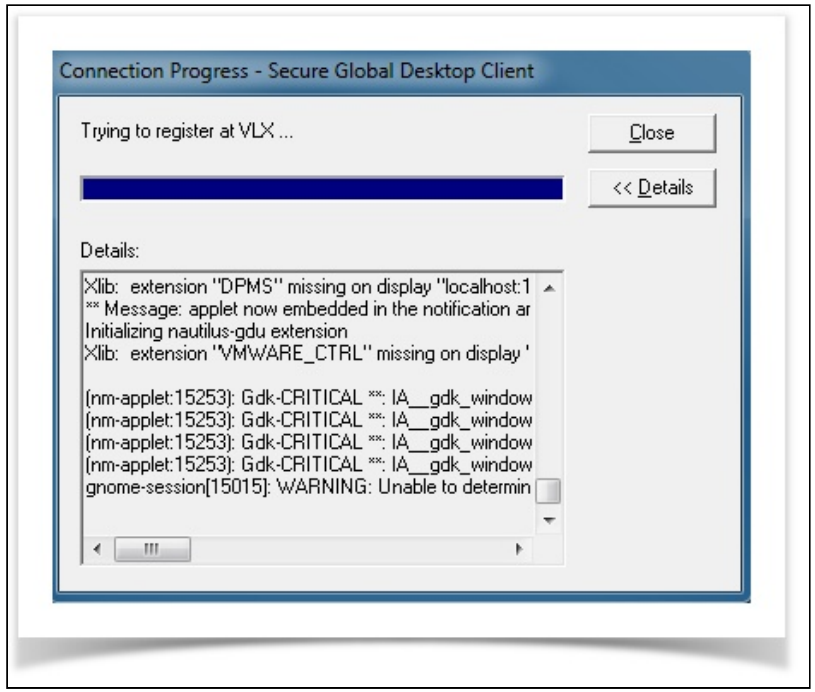
The **-1** error code is due to invalid data provided, so that it could not get a connection to the VISULOX PORTAL. Maybe due to an invalid profile.

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

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

Application start via Workspace

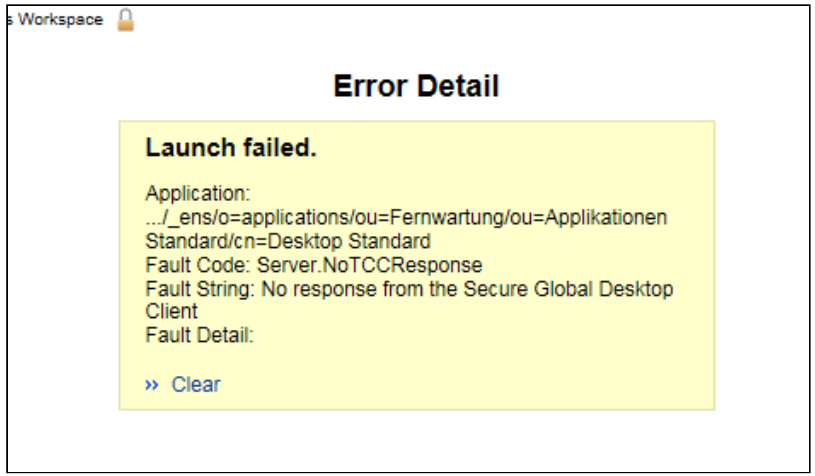
When an application is started via Workspace a small **Connection Progress** window is opened. Mostly this window disappears immediately and the application is launched. If there is a problem with the connection to the application, then this window stays open and shows the errors occurred.



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

Error during start of an application in Workspace

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



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

VISULOX shell script tracing

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

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

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

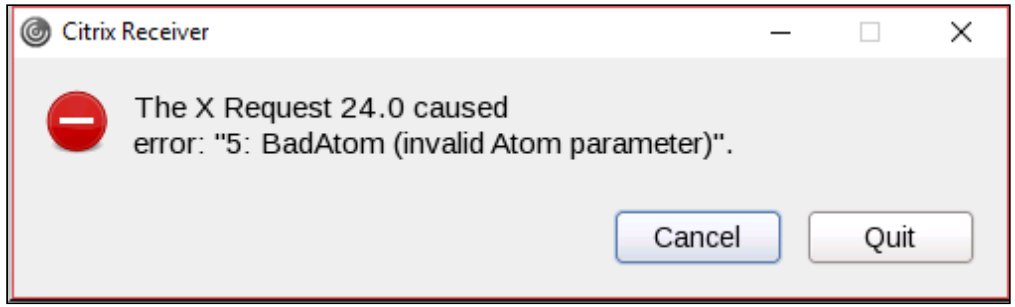
```
BASH_XTRACEFD=99
set -x
```

Using Flash Player and checked out films

Flash is no longer supported.

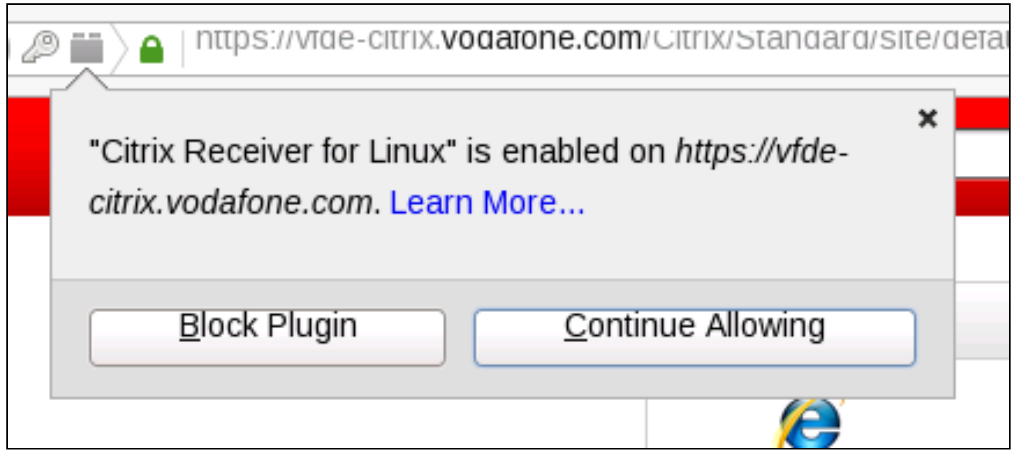
Citrix Receiver

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



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

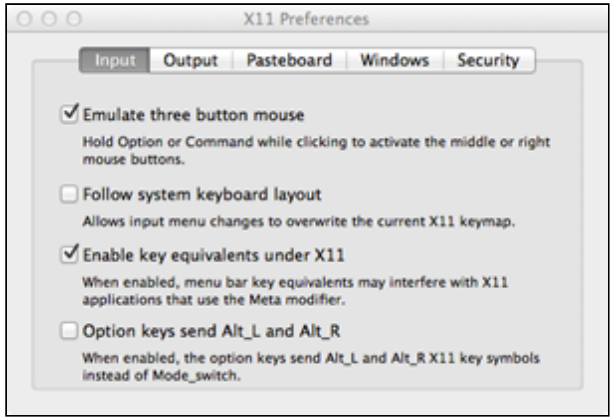
Also always take care, that the Citrix Receiver plugin is not blocked by the browser. Check plugin status via address bar icon in the browser:

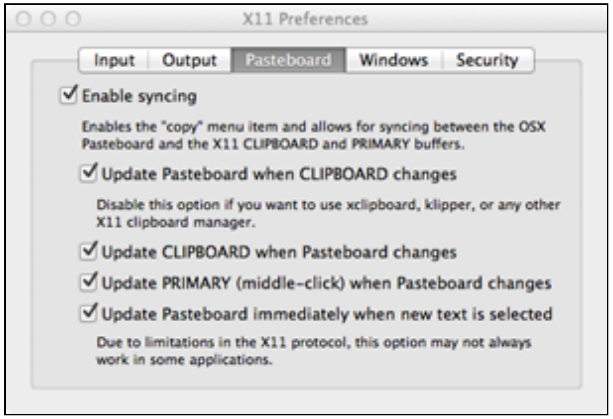


Copy & paste for Mac OS

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

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





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

Copy & paste in HTML5 sessions / application toolbar

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

Icon	Description
	Copies the selected text to the clipboard.

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

Copying and pasting between applications

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

The following changes apply for copy and paste:

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

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

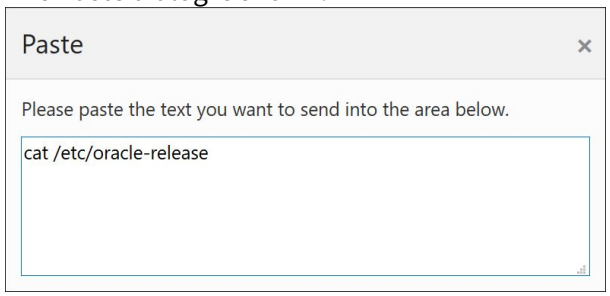
Copying from an application to a client device

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

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

Pasting to an application from a client device

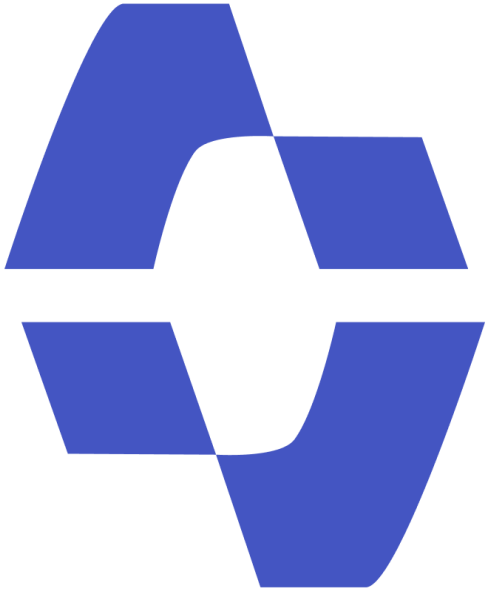
1. Select and copy the text from the application on the client device. Use the normal method for the application you are copying from.
   For example, use a menu option in the application.
2. Retrieve the text from the client device clipboard.
   Click the Paste icon in the application toolbar.
   The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



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

Copying between applications

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



Sending local keyboard shortcuts to the remote application

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

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

22.1.6 Glossary

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

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

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

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

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

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

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

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

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

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

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

23 Appendix_Articles

23.1 VLX4 Articles

23.1.1 How to customize values in the database

- Overview
- Configuration
- Related information

Overview

VISULOX has several standard files in **/opt/visulox/setup/database** for the messages, views, applications etc.

The installation order is imported. The files can not be changed. If any special customizations are needed,
new files can be put into that directory and the extension must be "**.cust**".
This allows to modify or add parameters after applying.

Modifications must be applied on any node with the command

```
/opt/visulox/setup/loadconfig.tcl -config <custfile>
```

The VISULOX update process loads these files automatically.

Configuration

The format of such files is

```
{
    presql {
        -- ANY SQL STATEMENT BEFORE DATA
```

```
    }
    <tablename> {
        columns {<list of columns>}
        rows  {
                {<list of values>}
              }
    }
    postsql {
        -- ANY SQL STATMENT AFTER DATA
    }
}
```

Example to modify a text in the text catalog

```
{
    textcatalog {
        columns {lang var icon shorttext description}
        rows  {
                {en {WrongOtp} {sign_warning} {OTP not valid!} {The OTP entered is not correct}}
                {de {WrongOtp} {sign_warning} {OTP nicht gültig!} {Der eingegebene OTP ist falsch}}
              }
    }
}
```

Example to change the error message, if a script fails

```
{
 textcatalog {
   columns {lang var icon shorttext description}
   rows    {
            {de {loginscripterror} {} {Wenden Sie sich bitte an Ihren Administrator} {}}
```

```
            {en {loginscripterror} {} {Call Administrator} {}}
            }
    }
}
```

⚠ After change, a total service reboot is needed ⚠.

Before such a modification is applied we recommend:

- to ask support@visulox.com for assistance
- to make a backup of the database
- no changings are done, when the environment is online

Related information

How to configure alternate mappings for datasources

23.1.2 How to configure alternate mappings for datasources

Overview

VISULOX reads from datasources and uses a mapping to map the datasource fields to internal names.

VISULOX has a mapping for standard Active Directory (MSAD) and LDAP Servers (LDAP).

Depending of the data, which has to be imported a different mapping could be necessary. This article explains how to create such a mapping file.

- Overview
- Usage
- How to provide a list of eMails from AD to the VISULOX 2FA interface
- Related information

Usage

The default mapping file is `$VLXDIR/setup/database/mapping.data` and **should not be changed**. This file will be overwritten by update.

For a new mapping create a file in `$VLXDIR/setup/database` with the extension `.cust` and make necessary changing. This file will not not be overwritten by update.

A new mapping must have a new mapping source. The mapping source in this example is **MYMAP**.

The mapping has to be added then with:

```
visulox datasource add ... -mapping MYMAP
```

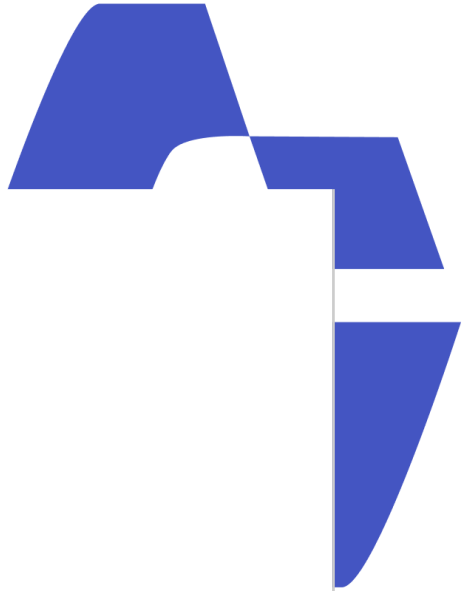
See also: How to work with VISULOX Datasources

$VLXDIR/setup/database/mymap.cust: Example for a new mapping named "MYMAP"

```
{
    varmapping {
        columns {source external internal convert}
        rows {
            {# Customized mapping}
            {{MYMAP.USER} {type}                    {vlxobjecttype}   {}}
            {{MYMAP.USER} {source}                  {vlxobjectsource} {}}
            {{MYMAP.USER} {object}                  {vlxobjectname}   {}}
            {{MYMAP.USER} {object}                  {vlxowner}        {}}
            {{MYMAP.USER} {cn}                      {vlxfullname}     {listvar}}
            {{MYMAP.USER} {givenName}               {vlxsurname}      {}}
            {{MYMAP.USER} {email}                   {vlxemail}        {}}
            {{MYMAP.USER} {unixusername}            {vlxloginuser}    {}}
            {{MYMAP.USER} {textmessage}             {vlxsms}          {}}
            {{MYMAP.USER} {uniqueMember}            {vlxgrouplist}    {}}
```

```
            {{MYMAP.USER} {manager}                 {vlxmanager}      {}}
            {{MYMAP.USER} {uidNumber}               {vlxuid}          {}}
            {{MYMAP.USER} {gidNumber}               {vlxgid}          {}}
            {{MYMAP.USER} {unixHomeDirectory}       {vlxhome}         {}}

            {{MYMAP.GROUP} {type}                   {vlxobjecttype}   {}}
            {{MYMAP.GROUP} {source}                 {vlxobjectsource} {}}
            {{MYMAP.GROUP} {object}                 {vlxobjectname}   {}}
            {{MYMAP.GROUP} {object}                 {vlxgroup}        {}}
            {{MYMAP.GROUP} {member}                 {vlxuserlist}     {}}
          }
    }
}
```

Copy the new mapping on each node, load the new mapping with **./loadconfig.tcl** and restart VISULOX.



This new mapping must be applied on all VISULOX nodes.

How to provide a list of eMails from AD to the VISULOX 2FA interface

The default configuration of VISULOX maps the LDAP attribute "**email**" as a single value to **vlxemail**.

Available LDAP attributes can be checked with:

```
./ldap.tcl -name <source> -print
```

If another attribute holds the eMail address to send the PIN, it can be configured with an alternate attribute mapping.

If the eMail field contains more than one eMail address, the possible delimiter has to be configured in the **regexp.email** field.

Related information

How to work with VISULOX Datasources

Active Directory Attributes

Creating VISULOX user groups based on an AD/LDAP attribute

23.1.3 How to send VISULOX Events to external services

Overview

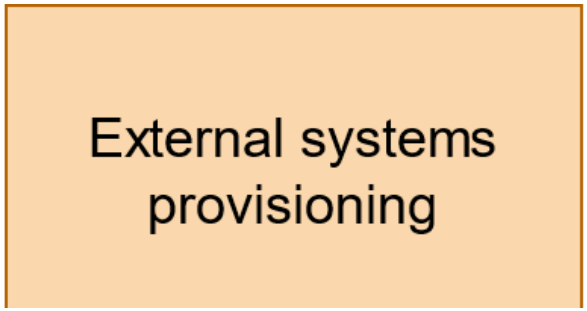
VISULOX Events are generated in several parts of the software. All events are stored in the database.

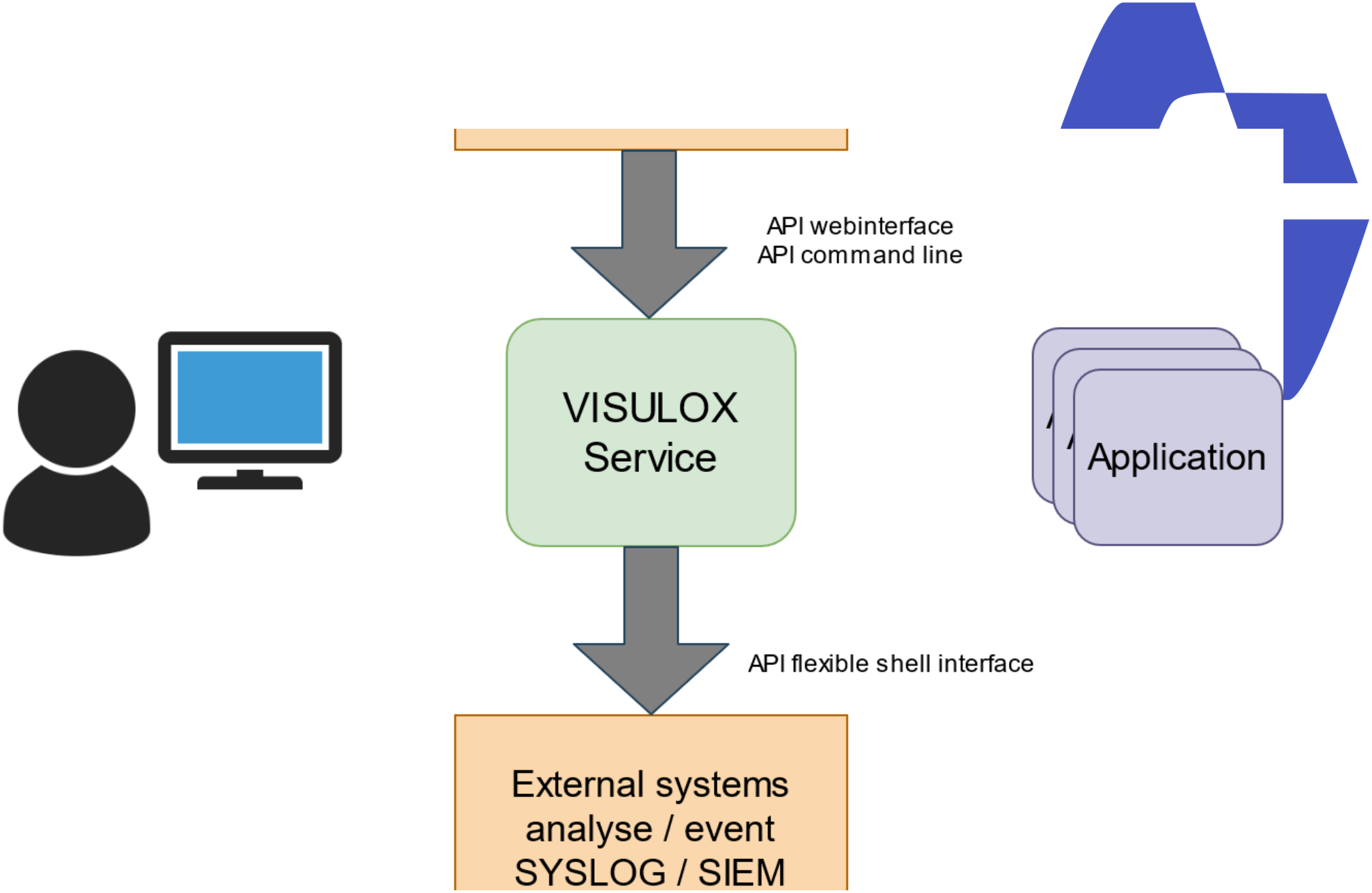
Every event is also seen in the event script and can be delivered to external systems.

The script is placed in **$VLXDIR/tools/event.sh**. The results are ignored. The file permissions must be **vlx/vlxgroup/0550**.

This can be used for external systems like **Syslog** or **SIEM integration** (SIEM: **S**ecurity **I**nformation and **E**vent **M**anagement).

- Overview
- Usage
- Event information
- Configuration
- Related information




API webinterface
API command line
VISULOX
Service
Application
API flexible shell interface
External systems
analyse / event
SYSLOG / SIEM

Usage

The use case on this is the syslog integration. Sending information to a syslog server.

Send all events to syslog

```
#!/bin/bash
subject="$VLXEVENT $VLXOWNER $VLXAPPLICATION $VLXAPPLICATIONHOST $VLXEVENTINFO"
tag="VISULOX"
logger -t $tag -p user.err "$subject"
```

Event information

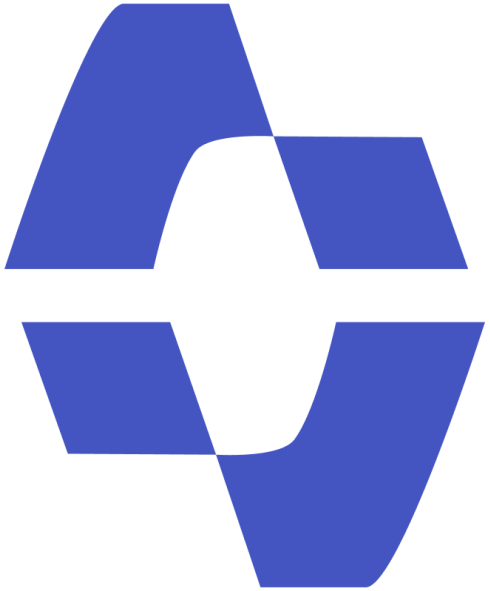
The event information is seen in the script as shell environment information. Depending of the event type different information is provided.

Configuration

The script **$VLXDIR/tools/event.sh** has to be adjusted.

This script is not replicated to other VISULOX Nodes.

Only those events are seen in that script which are generated on that node.



Related information

How to pass multiple login failures to external

Overview of VISULOX Events

Variables in notifications

Interface for current usage - stats.sh

Monitoring VISULOX

How to pass multiple login failures to external

Overview

If a user tries to login with a wrong password, this is documented as **loginFailure** and **loginRejected**.
If this happens several times, it will be also documented as **multipleLoginFailures**.

- Overview
- Configuration
  - failedLoginScript
- Related information

Configuration

The login detection interval and the script can be configured:

```
visulox config -name login.failed
    ------------------------------------------------------
    | changed | key                 | value             |
    ------------------------------------------------------
    |         | login.failed.rate   | 5:20:50           |
    |         | login.failed.script | failedLoginScript |
    ------------------------------------------------------
```

In this example **failedLoginScript** is triggered, if login fails five times in a minute, 20 times in an hour or 50 times a day. This is the default setting.
If login fails because of the configured settings, the login will no longer be passed to the authenication server until the rate falls below the configured rate.

Example action script, that triggers on "**multipleLoginFailuers**" and sends the event:

failedLoginScript

```
#!/bin/bash
VLXRECIPIENT=${VLXRECIPIENT:- root}
$VLXUTIL/mailclient.tcl -file stdin -subject "[TOKEN] FailedLogin $VLXLOGINUSER" -to $VLXRECIPIENT << EOF
Failures by $VLXLOGINUSER: $VLXEVENTINFO
EOF
# If the script should be treated as successful in VISULOX, the exit code must be 0
true
exit $?
```

Related information

Overview of VISULOX events

How to send VISULOX Events to external services

VISULOX PORTAL Service Events

Type	Event	Description	Event variable	Available information
Server	Server started	Server has been started / details	serverStart	VLXKEYWORD=sgdaudit VLXEVENTINFO=The server has started. VLXEVENT=serverStart VLXEVENTTIMEMS=1410873066664
Server	Server stopped	Server was stopped / details	serverStop	VLXKEYWORD=sgdaudit VLXEVENTINFO=The server has received a signal to stop. Reason: VLXEVENT=serverStop VLXEVENTTIMEMS=1410958910574
Server	SSL started	VISULOX PORTAL Security SSL has been started	securitySSLStart	VLXKEYWORD=sgdaudit VLXEVENTINFO=Starting SSL security. VLXEVENT=securitySSLStart VLXEVENTTIMEMS=1410958962561
Server	SSL stopped	VISULOX PORTAL Security SSL has been stopped	securitySSLStop	VLXKEYWORD=sgdaudit VLXEVENTINFO=Stopping SSL security. VLXEVENT=securitySSLStop VLXEVENTTIMEMS=1410958962591

Type	Event	Description	Event variable	Available information
Login	Login rejected	VISULOX PORTAL login was rejected for the user / details	loginResultRejected	VLXKEYWORD=sgdaudit VLXEVENTINFO=Login attempt for root. VLXOWNER=root VLXEVENT=loginResultRejected VLXEVENTTIMEMS=1410873847134
Login	Login ambigious	Login information ambiguous, common name needed	loginResultAmbiguous	VLXKEYWORD=sgdaudit VLXEVENTINFO=Login attempt for root. VLXOWNER=root VLXEVENT=loginResultAmbiguous VLXEVENTTIMEMS=1411459362599
Login	Anonymous login not supported	Login failed, Anonymous login not supported	loginResultAnonymous	VLXKEYWORD=sgdaudit VLXEVENTINFO=Login attempt for . VLXEVENT=loginResultAnonymous VLXEVENTTIMEMS=1412674627823
Login	Unresolveable user	Login failed, unresolvable user	loginResultUnresolveable	VLXKEYWORD=sgdaudit VLXEVENTINFO=Login attempt for <*User*>. VLXOWNER=<*User*> VLXEVENT=loginResultUnresolveable VLXEVENTTIMEMS=1411458638608

Type	Event	Description	Event variable	Available information
Workspace	Workspace opened	Workspace session has been started / details	webtopSessionStartedDetails	VLXEVENTHOST=<*Host*> VLXCLIENTIP=<*IP*> VLXKEYWORD=sgdaudit VLXEVENTINFO=Started webtop session for user .../_ens/o=Tarantella System Objects/cn=<*User*>. VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=webtopSessionStartedDetails VLXEVENTTIMEMS=1410949200749
Workspace	Workspace closed	Workspace session has been stopped / details	webtopSessionEndedDetails	VLXEVENTHOST=<*Host*> VLXCLIENTIP=<*IP*> VLXKEYWORD=sgdauditVLXEVENTINFO=Ended webtop session for user .../_ens/o=Tarantella System Objects/cn=<*User*>. VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=webtopSessionEndedDetails VLXEVENTTIMEMS=1410873810203
Application	Application session started	Application session has been started / details	sessionStartedDetails	VLXEVENTHOST=<*Host*> VLXAPPLICATION=o=applications/ou=VISULOX Examples/cn=VLX Management (all) VLXAPPLICATIONHOST=.../_dns/<*Host*> VLXCLIENTIP=<*IP*> VLXKEYWORD=sgdaudit VLXEVENTINFO=Started emulator session for .../_ens/o=Tarantella System Objects/cn=<*User*>. VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=sessionStartedDetails VLXEVENTTIMEMS=1411021021152

Type	Event	Description	Event variable	Available information
Application	Application session stopped	Application session was stopped / details	sessionEndedDetails	VLXEVENTHOST=<*Host*> VLXAPPLICATION=o=applications/ou=VISULOX Examples/cn=VLX Management (all) VLXAPPLICATIONHOST=.../_dns/<*Host*> VLXCLIENTIP=<*IP*> VLXKEYWORD=sgdaudit VLXEVENTINFO=Ended emulator session for user .../_ens/o=Tarantella System Objects/cn=<*User*>. VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=sessionEndedDetails VLXEVENTTIMEMS=1410873923906
VISULOX PORTAL Object	Object modified	VISULOX PORTAL object has been changed	modifySuccess	VLXOBJECT=o=Tarantella System Objects/cn=Global Administrators VLXKEYWORD=sgdaudit VLXEVENTINFO=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 VLXOWNER=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 VLXEVENT=modifySuccess VLXEVENTTIMEMS=1410958605810
VISULOX PORTAL Object	Object created	A new VISULOX PORTAL object was created	createSuccess	VLXOBJECT=o=VISULOX Examples VLXKEYWORD=sgdaudit VLXEVENTINFO=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 VLXOWNER=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 VLXEVENT=createSuccess VLXEVENTTIMEMS=1410937362976

Type	Event	Description	Event variable	Available information
VISULOX PORTAL Object	Object create failed	Creating an VISULOX PORTAL object failed	createFailure	VLXOBJECT=o=Tarantella System Objects/ou=VISULOX VLXKEYWORD=sgdaudit VLXEVENTINFO=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 failed to create an object in diskens: o=Tarantella System Objects/ou=VISULOX VLXOWNER=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 VLXEVENT=createFailure VLXEVENTTIMEMS=1410937323669
VISULOX PORTAL Object	Rename successful	VISULOX PORTAL object renamed successfully	renameSuccess	VLXOBJECT=o=TBS Sample Organization/ou=SuviAdmin/cn=<*User*>&o=TBS Sample Organization/ou=SuviAdmin/cn=<*User*> VLXKEYWORD=sgdaudit VLXEVENTINFO=.../_ens/o=Tarantella System Objects/cn=<*User*> VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=renameSuccess VLXEVENTTIMEMS=1411459092333
VISULOX PORTAL Object	Object deleted	An VISULOX PORTAL object was deleted	deleteSuccess	VLXOBJECT=o=appservers/ou=VISULOX Examples VLXKEYWORD=sgdaudit VLXEVENTINFO=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 VLXOWNER=A user authenticated by com.sco.jndi.auth.PermissiveAuthAgent@b2bde5 VLXEVENT=deleteSuccess VLXEVENTTIMEMS=1410937358862

Type	Event	Description	Event variable	Available information
Login	Multiple login failures detected	Default warning setting for failed login attempts: 5 per minute, 20 per hour and 50 per day	multipleloginfailures	VLXKEYWORD=sgdaudit VLXEVENTINFO=multiple login failures: {1413294071918 1413294077974 1413294082566 1413294087774 1413294093867 1413294099964} {5 {1 minute}} VLXOWNER=root VLXEVENT=multipleLoginFailures VLXEVENTTIMEMS=1413294099992
Login	Access PIN accepted	Login with Access PIN accepted	2faPinAccepted	VLXAPPLICATION=WORKSPACE VLXOBJECT=login_policy.POL-LOGIN VLXKEYWORD=login VLXEVENTINFO=policymode : <allowloginwithverbaltoken.map> VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=2faPinAccepted VLXEVENTTIMEMS=1411716395671 VLXSESSIONID=<*Host*>:1411716395653
Login	Access PIN requested	Access PIN for login requested	2faPinRequested	VLXAPPLICATION=WORKSPACE VLXOBJECT=login_policy.POL-LOGIN VLXKEYWORD=login VLXEVENTINFO=policymode : <allowloginwithverbaltoken.map> VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=2faPinRequested VLXEVENTTIMEMS=1411716227907 VLXSESSIONID=<*Host*>:1411716227890

Type	Event	Description	Event variable	Available information
Login	Access PIN rejected	Access PIN was rejected	2faPinRejected	VLXAPPLICATION=WORKSPACE VLXOBJECT=login_policy.POL-LOGIN VLXKEYWORD=login VLXEVENTINFO=policymode : <allowloginwithverbaltoken.map> VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<User> VLXEVENT=2faPinRejected VLXEVENTTIMEMS=1411716286853 VLXSESSIONID=<*Host*>:1411716286832
Login	OTP requested	One Time Passcode for login requested	otpRequested	VLXAPPLICATION=WORKSPACE VLXOBJECT=login_policy.POL-LOGIN VLXKEYWORD=login VLXEVENTINFO=policymode : <allowloginwithotp.map> VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=otpRequested VLXEVENTTIMEMS=1411716228107 VLXSESSIONID=<*Host*>:1411716287890
Login (Webtop)	Logged out by supervisor	Application session ended by supervisor via Cockpit	webtopSessionEndedByAdmin	VLXAPPLICATION=WORKSPACE VLXOBJECT=<*Host*>:1410958815363 VLXKEYWORD=webtop VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=webtopSessionEndedByAdmin VLXEVENTTIMEMS=1410961658581 VLXSESSIONID=<*Host*>:1410958815363

Type	Event	Description	Event variable	Available information
Application	Application started	Application session has been started with session controller	sessionControllerStarted	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1410959578219 VLXKEYWORD=application VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=sessionControllerStarted VLXEVENTTIMEMS=1410959585444 VLXSESSIONID=<*Host*>:1410959578219
Application	Application ended	Application session ended	sessionControllerEnded	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1410959578219 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=sessionControllerEnded VLXEVENTTIMEMS=1410960655168 VLXSESSIONID=<*Host*>:1410959578219

Type	Event	Description	Event variable	Available information
Application	Session locked	Application session locked	lock	VLXAPPLICATION=o=applications/cn=xterm (portalsgdv3) VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411374290302 VLXKEYWORD=application VLXEVENTINFO=Application locked by <POL-ACC:24x7> VLXREMOTEIP=unknown VLXEVENT=lock VLXEVENTTIMEMS=1411374646039 VLXSESSIONID=<*Host*>:1411374290302
Application	Session unlocked	Application session unlocked	unlock	VLXAPPLICATION=o=applications/cn=xterm (portalsgdv3) VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411374290302 VLXKEYWORD=application VLXEVENTINFO=Application unlocked by <POL-ACC:24x7> VLXREMOTEIP=unknown VLXEVENT=unlock VLXEVENTTIMEMS=1411375275254 VLXSESSIONID=<*Host*>:1411374290302

Type	Event	Description	Event variable	Available information
Application	Ended by supervisor	Application session ended by supervisor via Cockpit	sessionEndedByAdmin	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1410959578219 VLXKEYWORD=application VLXEVENTINFO=grzuirt VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=sessionEndedByAdmin VLXEVENTTIMEMS=1410960649806 VLXSESSIONID=<*Host*>:1410959578219
Application	Message sent	Message from supervisor is sent via Cockpit to the user	message	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1410959578219 VLXKEYWORD=application VLXEVENTINFO=Message text - test VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=message VLXEVENTTIMEMS=1410960603925 VLXSESSIONID=<*Host*>:1410959578219

Type	Event	Description	Event variable	Available information
Application	Accepted by user	Message, recording, etc. acknowledged by the user	accept	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1410959578219 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=accept VLXEVENTTIMEMS=1410960619532 VLXSESSIONID=<*Host*>:1410959578219
Application	Rejected	Recording rejected by user	reject	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411040749860 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=reject VLXEVENTTIMEMS=1411040772306 VLXSESSIONID=<*Host*>:1411040749860

Type	Event	Description	Event variable	Available information
Notification	Notification sent	A notification was sent based on the selected script	scriptsend	VLXAPPLICATION=WORKSPACE VLXOBJECT=<*Host*>:1411733892002 VLXKEYWORD=script VLXEVENTINFO=Scriptname: PINScript Args: sendpin ReturnCode:0 VLXEMAIL=<*eMail*> VLXREMOTEIP=unknown VLXACCESSPOINT=<*VAPHost*> VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=scriptsend VLXEVENTTIMEMS=1411733892169 VLXSESSIONID=<*Host*>:1411733892002
Access	Access will expire	Warning, that access to applications will expire soon		VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*Host*> VLXCLIENTIP=<*IP*> VLXOBJECT=<*Host*>:1414482063061 VLXKEYWORD=application VLXEVENTINFO=mc(warnbypolicy:POL-ACC:24x7)en VLXREMOTEIP=unknown VLXPOLICY=POL-ACC:24x7|- VLXEVENT=warn VLXEVENTTIMEMS=1414482068469 VLXSESSIONID=<*Host*>:1414482063061

Type	Event	Description	Event variable	Available information
Access	User request	Access requested by the user	accessRequestedByUser	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411374290302 VLXKEYWORD=application VLXEVENTINFO=Need access ... VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=accessRequestedByUser VLXEVENTTIMEMS=1411375073275 VLXSESSIONID=<*Host*>:1411374290302
Application	Remark by user	Session annotation created by the user	annotationByUser	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411032143563 VLXKEYWORD=application VLXEVENTINFO=annotation from user VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=annotationByUser VLXEVENTTIMEMS=1411032920902 VLXSESSIONID=<*Host*>:1411032143563

Type	Event	Description	Event variable	Available information
Application	Remark by supervisor	Annotation created by the supervisor in the Cockpit for the session	annotationBySupervisor	VLXAPPLICATION=o=applications/cn=xterm VLXOBJECT=<*Host*>:1411032143563 VLXKEYWORD=application VLXEVENTINFO=annotation by admin VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=annotationBySupervisor VLXEVENTTIMEMS=1411033345120 VLXSESSIONID=<*Host*>:1411032143563
Cooperation	Assistance request	Request for a cooperation	assistrequested	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411032143563 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=assistrequested VLXEVENTTIMEMS=1411032254790 VLXSESSIONID=<*Host*>:1411032143563

Type	Event	Description	Event variable	Available information
Cooperation	Assist observe	Assist mode switched to observe	assistobserve	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411032143563 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=assistobserve VLXEVENTTIMEMS=1411032295006 VLXSESSIONID=<*Host*>:1411032143563
Cooperation	Assist interact	Assist mode switched to interact	assistinteract	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1410941092420 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=assistinteract VLXEVENTTIMEMS=1410941435289 VLXSESSIONID=<*Host*>:1410941092420

Type	Event	Description	Event variable	Available information
Cooperation	Assist Standby	Assist mode switched to standby	assiststandby	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411032143563 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=assiststandby VLXEVENTTIMEMS=1411032833036 VLXSESSIONID=<*Host*>:1411032143563
Cooperation	Dual Control	Dual Control cooperation started	dualcontrol	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411377310603 VLXKEYWORD=application VLXEVENTINFO=Dual Control observe VLXREMOTEIP=unknown VLXEVENT=dualcontrol VLXEVENTTIMEMS=1411377323809 VLXSESSIONID=<*Host*>:1411377310603

Type	Event	Description	Event variable	Available information
Cooperation	Assistance closed	Cooperation closed	assistclosed	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1410941092420 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=assistclosed VLXEVENTTIMEMS=1410941493392 VLXSESSIONID=<*Host*>:1410941092420
Recording	Manual recording	Manual recording of the session started by the supervisor via Cockpit	sessionManuallyRecordingStarted	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411031490574 VLXKEYWORD=application VLXEVENTINFO=Recording will be started VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=sessionManuallyRecordingStarted VLXEVENTTIMEMS=1411031608223 VLXSESSIONID=<*Host*>:1411031490574

Type	Event	Description	Event variable	Available information
Recording	Recording stopped	Manual recording stopped by the supervisor via Cockpit	sessionManuallyRecordingStopped	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411032143563 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=sessionManuallyRecordingStopped VLXEVENTTIMEMS=1411033471825 VLXSESSIONID=<*Host*>:1411032143563
Recording	Recording started by Policy	Predefined recording started by Application Policy	sessionRecordingStarted	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411040749860 VLXKEYWORD=application VLXREMOTEIP=unknown VLXEVENT=sessionRecordingStarted VLXEVENTTIMEMS=1411040764946 VLXSESSIONID=<*Host*>:1411040749860

Type	Event	Description	Event variable	Available information
Keyboard control	In use	Input changed to this user	inputFocusChanged	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411031490574 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=inputFocusChanged VLXEVENTTIMEMS=1411031610245 VLXSESSIONID=<*Host*>:1411031490574
Keyboard control	Inputline	The user entered a line of characters	keyboardControlInputline Based on roles and settings, this event can be suppressed	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411378872936 VLXKEYWORD=application VLXEVENTINFO=line entered VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=keyboardControlInputline VLXEVENTTIMEMS=1411378890000 VLXSESSIONID=<*Host*>:1411378872936

Type	Event	Description	Event variable	Available information
Keyboard control	Responsible	Input changed to this user	inputResponsibility	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411378872936 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=inputResponsibility VLXEVENTTIMEMS=1411378877939 VLXSESSIONID=<*Host*>:1411378875939
Keyboard control	Idle	Keyboard idle	InputFocusIdle	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411378872936 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=InputFocusIdle VLXEVENTTIMEMS=1411378894000 VLXSESSIONID=<*Host*>:1411378872976

Type	Event	Description	Event variable	Available information
Keyboard control	Keyboard control started	Keyboard input detection started	keyboardControlStarted	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411378633981 VLXKEYWORD=application VLXREMOTEIP=unknown VLXEVENT=keyboardControlStarted VLXEVENTTIMEMS=1411378647356 VLXSESSIONID=<*Host*>:1411378633981
Keyboard control	Keyword detected	Keyword detected by keystroke detection control	keywordDetected	VLXAPPLICATION=o=applications/cn=xterm VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411378633981 VLXKEYWORD=application VLXEVENTINFO=Pattern: \yvisulox|\ybadword\y VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXOWNER=o=TBS Sample Organization/ou=User/cn=<*User*> VLXEVENT=keywordDetected VLXEVENTTIMEMS=1411378782000 VLXSESSIONID=<*Host*>:1411378633981
Checkout	Checkout	Session checkout via Cockpit	checkout	VLXAPPLICATION=o=applications/cn=xterm VLXOBJECT=<*Host*>:1411374290302 VLXKEYWORD=application VLXEVENTINFO=<*URL*>: Checkout 22.09.14 VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=checkout VLXEVENTTIMEMS=1411379292989 VLXSESSIONID=<*Host*>:1411374290302

Type	Event	Description	Event variable	Available information
Checkout	Checkout with keystrokes	Checkout of the session information in a ZIP file with displayed keystrokes	checkoutwithkeystrokes	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXOBJECT=<*Host*>:1411130994028 VLXKEYWORD=application VLXEVENTINFO=<*URL*>: checkout VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=checkoutwithkeystrokes VLXEVENTTIMEMS=1411132574072 VLXSESSIONID=<*Host*>:1411130994028
Checkout	Report in browser	Report created via Cockpit and displayed in browser	reportGeneratedByGuiBrowser	VLXAPPLICATION=o=applications/ou=VISULOX Examples/cn=VLX Devel GUI () VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=report.html.sessions VLXKEYWORD=system VLXEVENTINFO=Send to browser <*URL*> VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=reportGeneratedByGuiBrowser VLXEVENTTIMEMS=1411132896942 VLXSESSIONID=<*Host*>:1411130967068

Type	Event	Description	Event variable	Available information
Checkout	Report via eMail	Report created via Cockpit and sent via eMail	reportGeneratedByGuiEmail	VLXAPPLICATION=o=applications/ou=VLX-Examples/cn=VLX Devel GUI () VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=report.html.sessions VLXKEYWORD=system VLXEVENTINFO=eMail to <*eMail*> VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=reportGeneratedByGuiEmail VLXEVENTTIMEMS=1411717118126 VLXSESSIONID=<*Host*>:1411715620908
Checkout	Player started	Browser-based player started via Cockpit	player	VLXAPPLICATION=o=applications/cn=xterm VLXOBJECT=<*Host*>:1411374290302 VLXKEYWORD=application VLXEVENTINFO=to browser <*URL*> VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=player VLXEVENTTIMEMS=1411379236101 VLXSESSIONID=<*Host*>:1411374290302
Checkout	Player with keystrokes started	Browser based player with displayed keystrokes started	playerwithkeystrokes	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXOBJECT=<*Host*>:1411130994028 VLXKEYWORD=application VLXEVENTINFO=to browser <*URL*> VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=playerwithkeystrokes VLXEVENTTIMEMS=1411132491657 VLXSESSIONID=<*Host*>:1411130994028

Type	Event	Description	Event variable	Available information
System	Auto accepted	Accepted automatically by the system	autoaccept	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411727335516 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXEVENT=autoaccept VLXEVENTTIMEMS=1411727344674 VLXSESSIONID=<*Host*>:1411727335516
System	Auto rejected	Rejected automatically by the system	autoreject	VLXAPPLICATION=o=applications/ou=VLX-OFFICE/cn=OFFICE-WTS VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=<*Host*>:1411727763275 VLXKEYWORD=application VLXTICKETID=SETUP VLXREMOTEIP=unknown VLXEVENT=autoreject VLXEVENTTIMEMS=1411727771812 VLXSESSIONID=<*Host*>:1411727763275

Type	Event	Description	Event variable	Available information
System	Object created	A VISULOX object has been created	objectNew	VLXAPPLICATION=o=applications/ou=VISULOX Examples/cn=VLX Devel GUI () VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=application_policy.POL-APP VLXKEYWORD=system VLXEVENTINFO=kbi_enabled : <> -> <disabled.map> VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=objectNew VLXEVENTTIMEMS=1411039893729 VLXSESSIONID=<*Host*>:1411034909556
System	Object copied	A VISULOX object has been copied	objectCopied	VLXAPPLICATION=o=applications/ou=VISULOX Examples/cn=VLX Devel GUI () VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=application_policy.POL-APP COPY1 VLXKEYWORD=system VLXEVENTINFO=POL-APP -> POL-APP COPY1 VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=objectCopied VLXEVENTTIMEMS=1411040177161 VLXSESSIONID=<*Host*>:1411034909556

Type	Event	Description	Event variable	Available information
System	Object changed	A VISULOX object has been changed	objectChanged	VLXAPPLICATION=o=applications/ou=VISULOX Examples/cn=VLX Devel GUI () VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=application_policy.POL-APP COPY1 VLXKEYWORD=system VLXEVENTINFO=comment : <> -> <...> VLXREMOTEIP=unknown VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=objectChanged VLXEVENTTIMEMS=1411040278394 VLXSESSIONID=<*Host*>:1411034909556
System	Object deleted	A VISULOX object has been deleted	objectDeleted	VLXOBJECT=application_policy.POL-APP COPY1 VLXKEYWORD=system VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=objectDeleted VLXEVENTTIMEMS=1411040394689
System	Object attached	A VISULOX object has been attached	objectAttached	VLXOBJECT=host_objects.t2-ol6u5 VLXKEYWORD=system VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=objectAttached VLXEVENTTIMEMS=1411040394783
System	Object detached	A VISULOX object has been detached	objectDetached	VLXOBJECT=host_objects.t2-ol6u5 VLXKEYWORD=system VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=objectDetached VLXEVENTTIMEMS=1411040394856

Type	Event	Description	Event variable	Available information
File Transfer	Synced to folder	Files synchronized with the folder	syncput	VLXAPPLICATION=File Transfer SYNC VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=documentation.txt VLXKEYWORD=filetransfer VLXEVENTINFO=TZ >> sync VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=syncput VLXEVENTTIMEMS=1412929078589 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C
File Transfer	Synced to Transit Zone	Files synchronized with the Transit Zone	syncget	VLXAPPLICATION=File Transfer SYNC VLXAPPLICATIONHOST=<*ApplicationHost*> VLXLISTHASH=FD04DD3A4282B0E8A991127E7F229C77 VLXOBJECT=vlx.data VLXKEYWORD=filetransfer VLXEVENTINFO=sync >> TZ VLXOWNER=CN=<*User*>,OU=Mitarbeiter,OU=ToolBox,DC=tbsol,DC=de VLXEVENT=syncget VLXEVENTTIMEMS=1412928632525 VLXSESSIONID=33499AD5A4472407E1C3F4E9EC8742B1

Type	Event	Description	Event variable	Available information
File Transfer	Transfer to server	File transferred from Transit Zone to the application server via SFTP/FTP	ftput	VLXAPPLICATION=File Transfer sftp/ftp VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=script4158 VLXKEYWORD=filetransfer VLXEVENTINFO=TZ >> FTALL:root@<*Host*>:. VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=ftput VLXEVENTTIMEMS=1412756831802 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C
File Transfer	Transfer to Transit Zone	File transferred from application server to the Transit Zone via SFTP/FTP	ftget	VLXAPPLICATION=File Transfer sftp/ftp VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=install.log VLXKEYWORD=filetransfer VLXEVENTINFO=FTALL:root@mp-ol6u3-devel:. >> TZ VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=ftget VLXEVENTTIMEMS=1412755064794 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C
File Transfer	Upload (internal web page)	File uploaded via internal web page	webput	VLXAPPLICATION=File Transfer Internal VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=RAM.jpg VLXKEYWORD=filetransfer VLXEVENTINFO=Upload from <*IP*> VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=webput VLXEVENTTIMEMS=1412757089891 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C

Type	Event	Description	Event variable	Available information
File Transfer	Download (internal web page)	File downloaded via internal web page	webget	VLXAPPLICATION=File Transfer Internal VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=documentation.txt VLXKEYWORD=filetransfer VLXEVENTINFO=Download to <*IP*> VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=webget VLXEVENTTIMEMS=1412757685562 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C
File Transfer	Upload	File uploaded from client into Transit Zone	userput	VLXAPPLICATION=File Transfer External VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=documentation.txt VLXKEYWORD=filetransfer VLXEVENTINFO=upload from client VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=userput VLXEVENTTIMEMS=1412755432592 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C

Type	Event	Description	Event variable	Available information
File Transfer	Download	File transferred from Transit Zone to the client	userget	VLXAPPLICATION=File Transfer External VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=script4158 VLXKEYWORD=filetransfer VLXEVENTINFO=Download to client: o=Tarantella System Objects/cn=<*User*> VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=userget VLXEVENTTIMEMS=1412755236681 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C
File Transfer	File checked	Transferred file has been checked	checked	VLXAPPLICATION=File Transfer VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=install.log VLXKEYWORD=filetransfer VLXEVENTINFO=ASCII text VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=checked VLXEVENTTIMEMS=1411462593768 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C
File Transfer	Approved	Transferred file has been approved	approved	VLXAPPLICATION=File Transfer VLXOBJECT=install.log.syslog VLXKEYWORD=filetransfer VLXEVENTINFO=File is requested by support VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=approved VLXEVENTTIMEMS=1412926191255 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C

Type	Event	Description	Event variable	Available information
File Transfer	File rejected	File rejected after check	rejected	VLXAPPLICATION=File Transfer VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=winhlp32.exe VLXKEYWORD=filetransfer VLXEVENTINFO=PE32 executable for MS Windows (GUI) Intel 80386 32-bit VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=rejected VLXEVENTTIMEMS=1411462980138 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C
File Transfer	Pending	File not approved yet	pending	VLXAPPLICATION=File Transfer VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=winhlp32.exe VLXKEYWORD=filetransfer VLXEVENTINFO=PE32 executable for MS Windows (GUI) Intel 80386 32-bit VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=pending VLXEVENTTIMEMS=1411463918288 VLXSESSIONID=6F69AFB4EFD0B179724F330FCB81A65C

Type	Event	Description	Event variable	Available information
File Transfer	Conditionally acepted	File acception depending on rules	tmpaccepted	VLXAPPLICATION=File Transfer VLXAPPLICATIONHOST=<*ApplicationHost*> VLXOBJECT=test.exe VLXKEYWORD=filetransfer VLXEVENTINFO=no virus check script configured:PE32 executable for MS Windows (GUI) Intel 80386 32-bit VLXOWNER=o=Tarantella System Objects/cn=<*User*> VLXEVENT=tmpaccepted VLXEVENTTIMEMS=1490351093411 VLXSESSIONID=64BAE0AEE039003AF38030C6B2BC7A66

23.1.4 Login check against an external system

About

Additional fields and tooltips can be added to the login page.

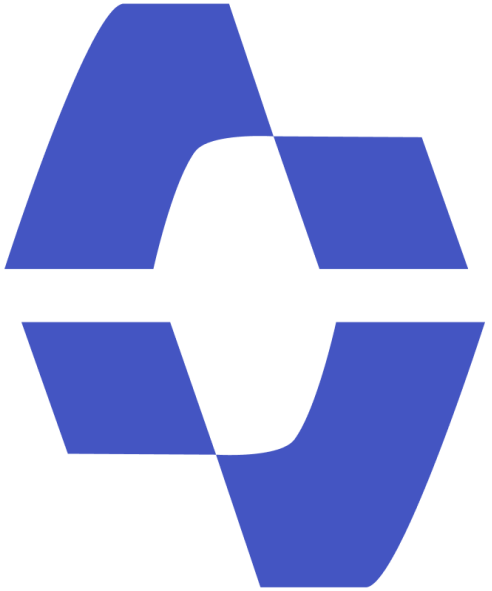
VISULOX is able to validate these fields and provides an interface e.g. to an external ticket system. Two scripts (validate and notification script) must be customized and attached to a Login Policy to check the values against the external system and to update the information.

The design of the scripts depends on the interface to the external system.

Other VISULOX login authentication mechanisms (e.g. MFA, verbal, etc) can be used additionally.

⚠ An MFA License is required to use the login check against an external system feature.

- About
- Interface to the external system
  - Ticket validation
  - Ticket update
- New available interface of the MFA shell script
- Additional fields and tooltips on login page
  - Additional fields and tooltips
  - For example



Interface to the external system

Ticket validation

The VISULOX Login Policy is extended to use a check script. The interface to the script provides the following VISULOX internal data:

- VLXOWNER (the used account)
- VLXTICKETID (which is the user provided ticket)
- other VLX parameters

The script talks to the external system and gets a feedback.

The check / validation script can be added to the VISULOX action scripts with:

```
visulox admin action add -name CHECK -scriptfile  <checkscript.sh> -force -category validate
```

Once the script is added, it can be selected in **Login Policy / Notification / Validation Script.**

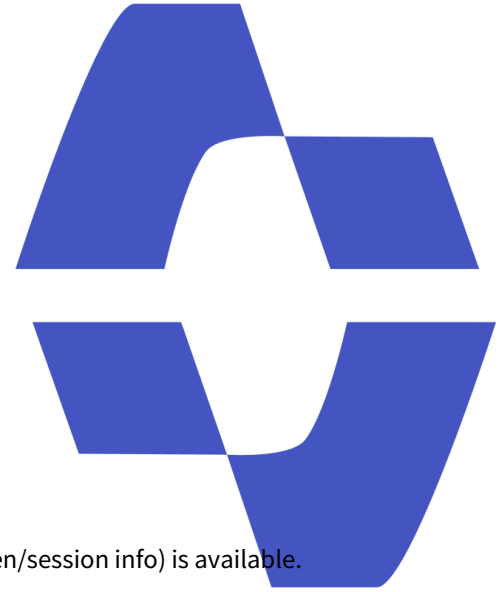
Ticket update

The interface to the script provides the following VISULOX internal data:

- VLXOWNER (the used account)
- VLXTICKETID (which is already validated)
- other VLX parameters

The update / notification script can be added to the VISULOX action scripts with:

```
visulox admin action add -name UPDATE -scriptfile  <update-script.sh> -force  -category login
```



Once the script is added, it can be selected in **Login Policy / Notification / Notification Script.**

New available interface of the MFA shell script

The redesigned script needs a base64 string with the return code <VLX ERROR CODE> info <info> data <data>.

With scriptAnswer.tcl the return string can be easily created within the shell script.
This applies also to confirmStatus.tcl (built-in).

External MFA has the following sequences:
For evaluation in the script VLXMFATOKEN (provided by the user after MFAREQUST) and VLXMFADATA (provided by the external service as token/session info) is available.

VLXMFATOKEN is always empty for the first time. After one init cycle the answer VLXMFADATA (-data) is returned.
VLXMFATOKEN always has a value from the VLXREQUEST cycle.

- MFAWAIT (Another init cycle occurs)
- MFAREQUEST (User provides value, that will be in VLXMFATOKEN)
- MFADENY (Rejected)
- SUCCESS (Successful, next)

Program for testing:

```
#!/bin/bash
   # verify helpful lines
   #exec 19> /tmp/apiExternalPinScript.log
   #BASH_XTRACEFD=19
   #set -x

   # VLXMFATOKEN - provided by user from MFA EXTERNAL PAGE
   # VLXMFADATA  - provided by backend / can be set by answer to backend

   # exitcode 0: script run without error
   # any other exitcode: script error
   # The internal answer is converted using scriptAnswer.tcl
```

```
    # Example with pin request:
    examplePinRequest () {
    noteData="(has <${VLXMFADATA}>)"
    note="0000=WAIT / 5678=REQUEST / 1234=OK / other=DENY / ${noteData}"

      if [[ "$VLXMFATOKEN" = "" ]]
        then
         # create session / init a session
         sessionData=SD$$
         $VLXUTIL/scriptAnswer.tcl -format base64 -code MFAREQUEST -info "$note / (init <${sessionData}>)" -data
"$sessionData"
       elif [[ "$VLXMFATOKEN" = "0000" ]]
        then
         $VLXUTIL/scriptAnswer.tcl -format base64 -code MFAWAIT -info "$note" -data "$VLXMFADATA"
       elif [[ "$VLXMFATOKEN" = "5678" ]]
        then
         $VLXUTIL/scriptAnswer.tcl -format base64 -code MFAREQUEST -info "$note" -data "$VLXMFADATA"
       elif [[ "$VLXMFATOKEN" = "1234" ]]
        then
         $VLXUTIL/scriptAnswer.tcl -format base64 -code SUCCESS -info "OK / ${noteData}"
       else
         $VLXUTIL/scriptAnswer.tcl -format base64 -code MFADENY -info "Your request was denied / ${noteData}"
       fi
    }
    # $VLXUTIL/rsasecureid test -resource rsaUrl.tcl ...

    examplePinRequest
    exit $?
```

Additional fields and tooltips on login page

Additional fields and tooltips

```
visulox config -name extendsession
    ------------------------------------------------------
    | changed | key                                | value |
    ------------------------------------------------------
    |         | extendsession.login.entry1         |       |
    |         | extendsession.login.entry1.usertip |       |
    |         | extendsession.login.entry2         |       |
    |         | extendsession.login.entry2.usertip |       |
    |         | extendsession.login.entry3         |       |
    |         | extendsession.login.entry3.usertip |       |
    |         | extendsession.scx.entry1           |       |
    |         | extendsession.scx.entry1.usertip   |       |
    |         | extendsession.scx.entry2           |       |
    |         | extendsession.scx.entry2.usertip   |       |
    |         | extendsession.scx.entry3           |       |
    |         | extendsession.scx.entry3.usertip   |       |
    ------------------------------------------------------
```

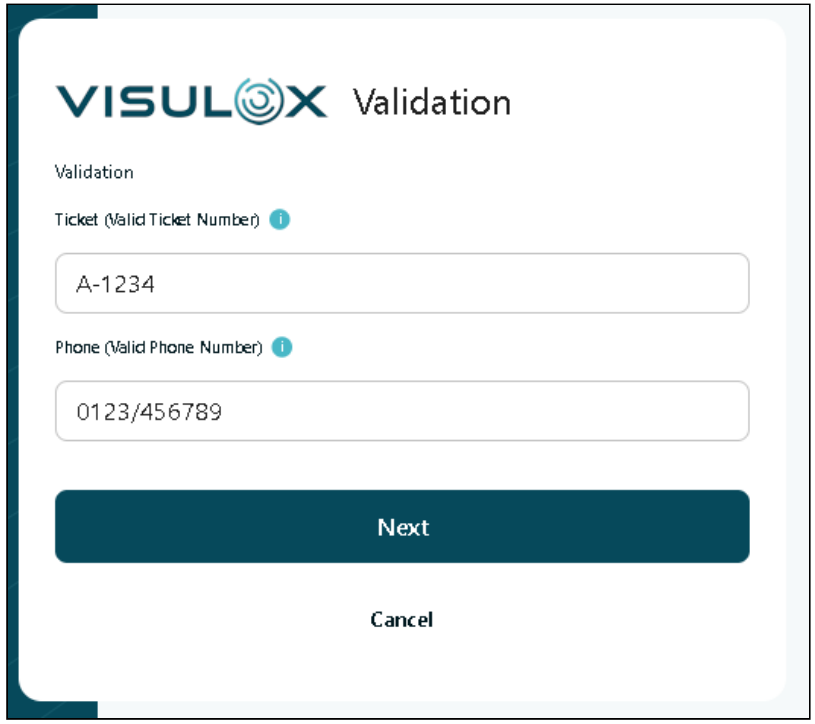
extendsession.**scx** entries belong to information on application start, which can also be used to send updates to the external system.

For example

```
visulox config -name extendsession.login.entry1="Ticket (Valid Ticket Number)"
visulox config -name extendsession.login.entry1.usertip="Registered users have to provide a valid ticket number."

visulox config -name extendsession.login.entry2="Phone (Valid Phone Number)"
visulox config -name extendsession.login.entry2.usertip="Users can leave this empty."
```

```
visulox portal attach -jspconf
```

With these configuration settings the following login mask is displayed after the initial login:



23.1.5 The VISULOX PIN Service

Overview

VISULOX provides an internal PIN service for Multi Factor Authentication,

the assistance to a session and for the access to the File Transit Zone.

The PIN has the following criteria:

- Length
- Symbols
- Presentation

- Overview
- PIN configuration (MFA, assist, transit)
- Display PINs via CLI (getpin)

PIN configuration (MFA, assist, transit)

List of available configuration parameters for VISULOX PINs

```
visulox config list -name pin -force
    ------------------------------------------------------------
    | parameter          |  type | value                       |
    ------------------------------------------------------------
    | pin.2fa.format     | SETUP | 3                           |
    | pin.2fa.length     | SETUP | 6                           |
    | pin.assist.format  | SETUP | 3                           |
    | pin.assist.length  | SETUP | 6                           |
    | pin.symbols        | SETUP | 123456789ABCDEFGHKMNPQRSTUWX |
    | pin.transit.format | SETUP | 3                           |
    | pin.transit.length | SETUP | 6                           |
```

```
    ------------------------------------------------------------
```

Length = Number of characters used for the PIN

Format = Number of characters in a bunch for better reading

Symbols = Allowed characters

To reduce the symbols list to numbers only:

```
visulox config edit -name pin.symbols="1234567890" -force
    -------------------------------------
    | parameter   |  type | value      |
    -------------------------------------
    | pin.symbols | SETUP | 1234567890 |
    -------------------------------------
```

Display PINs via CLI (getpin)

It is possible to display the PINs for the sequence numbers via the Command Line Interface.

```
visulox online getpin -sq <sequence number> -out <format string>
```

Placeholders like **%OWNER%**, **%OWNERSHORT%**, **%PIN%** can be used in the format string.

So the output format can be defined by the customer.

23.1.6 How to set and reset the inital VISULOX Cockpit refresh state

- Overview
- Configuration

Overview

The VISULOX Cockpit has an automatic refresh, if information changes in the environment.

On large systems this can lead to an unusable Cockpit.

This article describes how to set this refresh state for the default @ADMIN role.

Configuration

List the current refresh state

```
visulox config list -name guidefaults.global_mdroleheader.refresh
```

Set the refresh state to true on Cockpit startup

```
visulox config edit -name guidefaults.global_mdroleheader.refresh=1
```

Set the refresh state to false on Cockpit startup

```
visulox config edit -name guidefaults.global_mdroleheader.refresh=0
```

23.1.7 VISULOX 4 Requirements

General

- The recommended platform is **Oracle Linux / Red Hat 9** (for other versions contact amitego) with at least 10Gbyte for the OS, 20Gbyte for VISULOX PORTAL Service and 30 Gbyte for the VISULOX Service 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
- If **autofs** is used wiith **transit mapping**, Selinux has to be disabled
- The users ttasys and ttaserv are placed in the **/home** directory during installation.
- The recommended VISULOX version is the latest VISULOX 4 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
- 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!
Checking the hostname (must be identical):

```
nslookup $(hostname -f) --> Hostname and IP address is displayed
nslookup <IP address> --> IP address and hostname is displayed

getent ahosts $(/opt/tarantella/bin/bin/ttahostname) --> IP address and hostname is displayed
```

```
getent hosts <IP address> --> IP address and hostname is displayed

getent ahost localhost --> IP address is displayed (127.0.0.1)
getent hosts 127.0.0.1 --> IP address (127.0.0.1) and hostname (localhost) is displayed
```

Required packages

Choose **Server** or **Server with GUI** for the base environment.

The basic server 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**. As an alternative Red Hat Linux could be used, which will possibly need some other packages as listed here.
For other OS versions please contact amitego.

For **Oracle Linux 9** the following adjustment is necessary after an array installation:
Delete **SHA1** in /etc/crypto-policies/back-ends/java.config:

```
jdk.certpath.disabledAlgorithms=MD2, MD5, DSA, RSA keySize < 2048
```

This setting should be checked again after yum update.

Disk layout

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

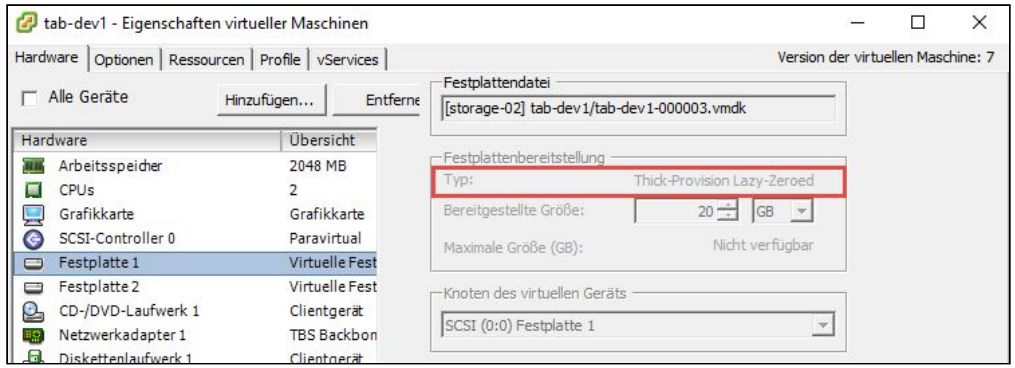
Further we recommend to have a partition of 20Gbyte under **/opt/tarantella**, 30Gbyte under **/opt/visulox** (60Gbyte with Archive) in a small environment.

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 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 integriy check.

Libraries needed for VISULOX on Oracle Linux 8

oracle_appstream_latest ol8-epel

```
dnf repolist
This system is receiving updates from Unbreakable Linux Network or Spacewalk.

repo id                                                                repo name

ol8-codeready                                                          ol8-codeready
```

```
ol8-epel                                                    ol8-epel
ol8_addons                                                  ol8_addons
ol8_appstream_latest                                        ol8_appstream_latest
ol8_x86_64                                                  ol8_x86_64
```

ol8-codeready is needed for transitmapping.

For the Epel repository on Red Hat 8 use:

```
dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

```
dnf install java-11-openjdk
dnf update
```

Installing VISULOX 4 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 and are in yum repolist as well.

yum update is recommended before installing the new packages!

Platform modification during installation

VISULOX PORTAL Service

Before installation of the VISULOX PORTAL Service, the following libraries should be installed: `xterm xclock xauth`

umask 022 is recommended for installation and start of the VISULOX PORTAL Service.

VISULOX PORTAL Service must be installed **without** symlinks.

During VISULOX PORTAL Service installation two users and a group will be created:

```
uid=500(ttasys) gid=500(ttaserv) groups=500(ttaserv)
uid=501(ttaserv) gid=500(ttaserv) groups=500(ttaserv)
```

VISULOX PORTAL and VISULOX service are also adding files for PAM authentication: **/etc/pam.d/tarantella** and **/etc/pam.d/visulox**.

⚠ With **visulox portal admin -user <*unixuser*>** a Unix user can be activated as VISULOX Portal Administrator. It is recommended to set a different user than root!.

VISULOX Service

The default VISULOX installation directory is **/opt/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 avalaible 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**

Optional enhancements

VISULOX addons

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

VISULOX Firefox

Firefox

```
yum install firefox
```

VISULOX VNC

VNC Viewer

```
yum install tigervnc
```

Telnet

Telnet

```
 yum install telnet
```

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.

23.1.8 VISULOX 4 License

Overview

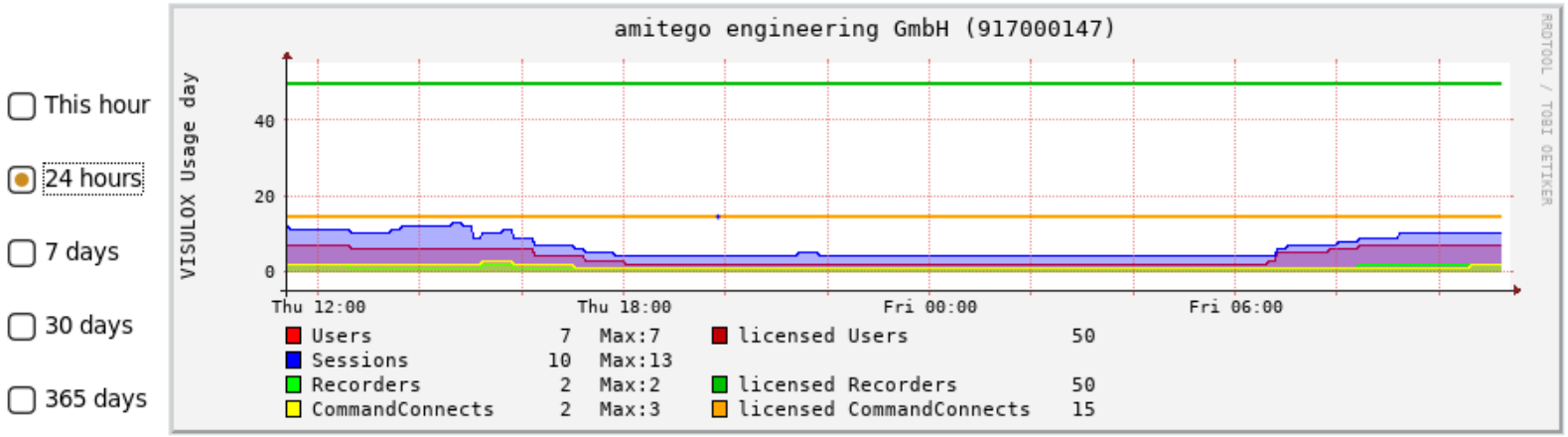
To use VISULOX a license is needed. The license can be tailored to the customer.

License control / impact

License	Control / impact
Base / Cluster	VISULOX Base Licence (one VISULOX Node) or VISULOX Cluster License (unlimited VISULOX Nodes).
Users	The number of users are controlled on startup of any VISULOX application (VISULOX Cockpit,, File Transfer, Cooperation). If more users are online than licensed, the VISULOX application can not be used any more. A warning message will be displayed.
Multi Factor Authentication	Multi Factor Authentication for users.
Session recorders	If the number of licensed recorders is reached during session control, the session will be locked and can not be used anymore (Manual recording is always possible).
OCR Keyword Detection	OCR component to detect configured keywords in applications.
Redact	Optional license for Redact Mode
Host Control	If the number of licensed Command Connects / Guards is reached, the session will be locked and can not be used anymore.

License	Control / impact
Revision Server	Optional license for a Revision Server (Archive Server).
Support & Maintenance	If the support and maintenance time is is reached, the environment should only be updated, when a new valid license is available within the next 21 days. In an environment with a license where support and maintenance (S&M) has expired, VISULOX can still be used as usual. Once an environment without S&M is updated to a newer VISULOX version a timer is set and displayed in the VISULOX Cockpit. After 21 days of running the new version, a valid license for the new version has to be installed. Without a valid license installed after 21 days access is no longer possible and the VISULOX Cockpit can not be used anymore. There is also the possibility that a license is set to **time limited**. With such a license VISULOX can no longer be used when support and maintenance (S&M) has expired.

A graph of the license usage is displayed in **VISULOX Cockpit / Cluster**:



A **Demo / Evaluation** license is available and valid for **10 days** including a VISULOX Base Node operating in total with **5** users, **5** session recorders and **2** Host Control applications.

A perpetual VISULOX License file is provided in a TAR archive from amitego. The license command understands this TAR file. There is no need to extract the tar files.

A perpetual VISULOX License file is provided by **amitego Sales & Service**. Contact: sales@amitego.com.

Installation / configuration of the license file

Show the current license

```
visulox license list
```

Check a provided license file

```
visulox license test -file <path to license file>
```

Replace the current installed license

```
visulox license replace -file <path to license file>
```

If a license is replaced on a node, it is replicated to all other nodes in the cluster.

If a new node is installed and attached to the VISULOX Cluster, it will get the license of the cluster. The Demo / Evaluation license is discarded.

If the tar archive can not be delivered to a customer via eMail, there is also the possibility to send the license as text XML/JSON to add it via copy & paste to STDN IN.

- visulox license replace -file - [RETURN]
- Copy & paste:

Base64 license hash in eMail:

```
- VISULOX License start
asdfsdfasdfasdfasdfasdfasdfasdfsadfasdfasdfasdfsadfasdfasdfasdfasdfasdff
asdasadasadasadasadasadasafdasfdasdafasdfdadfdaddafaddafadadfdadadfafdadfafa
sdgfhjsgdfjkashfjkghkaufghukahghukahghafdghaidghilafdhfgijgigfdahfghfduighuh
MX0gbXRhbiB7MX0gaGFzQ0cgezF9IG1vZHVsZXMge1ZMWDNBQywgMkZBLCBDR30gbGljZW5zYnVp
bGQgezE1MDM1NjA1NjJ9IEhBU0ggezE0NzNFQjJENTk2MjFGMDEyMTRFNkQ3MzhFM0EyQzA2fSBj
b21tYW5kY29ubmVjdHMgey0xfSBzbSB7MTUwMzQzOTasdarasdfadasdasdasdasd
-- VISULOX License end
```

- [RETURN]

Get the usage of the installation

```
visulox license usage
```

Available parameters: **-component** <users|sessions|recorders|hostcontrols> **-unit** <week|month|year>

With these parameters the maximum usage of a component can be displayed in the unit.

⚠ After installing a new license a restart of the VISULOX Service is necessary!

23.1.9 How to set auto commit or auto reject for recording

Overview

If an Application Policy enables the recording, the user can confirm or reject recording.

Confirm will open the application for usage. Reject will close it.

- Overview
- Usage
- Configuration

Usage

There is a general parameter to auto confirm or auto reject the recording of applications.

Depending on companies security policy an auto confirm is requested. Users know, that they are recorded and an additional confirmation is not needed.

Configuration

```
visulox config -name recorder.auto_acknowledge
```

The default valute is 0. This means neither commit nor reject will be done automatically. The user has to decide.

A negative value is auto reject. A postive value is auto commit.

For example:

Close application, if user does not confirm within 10 secondes

```
visulox config edit -name recorder.auto_acknowledge=-10
```

Open application without confirmation of the user

```
visulox config edit -name recorder.auto_acknowledge=1
```

Open application without confirmation of the user within 10 seconds, so reject is also possible.

```
visulox config edit -name recorder.auto_acknowledge=10
```

23.1.10 How to configure role profiles for the VISULOX Cockpit

General

With the Cockpit role editor a customized Cockpit can be configured and assigned to users.

Prerequisites

For this example setup two users have to be registered in the VISULOX PORTAL with the following settings:

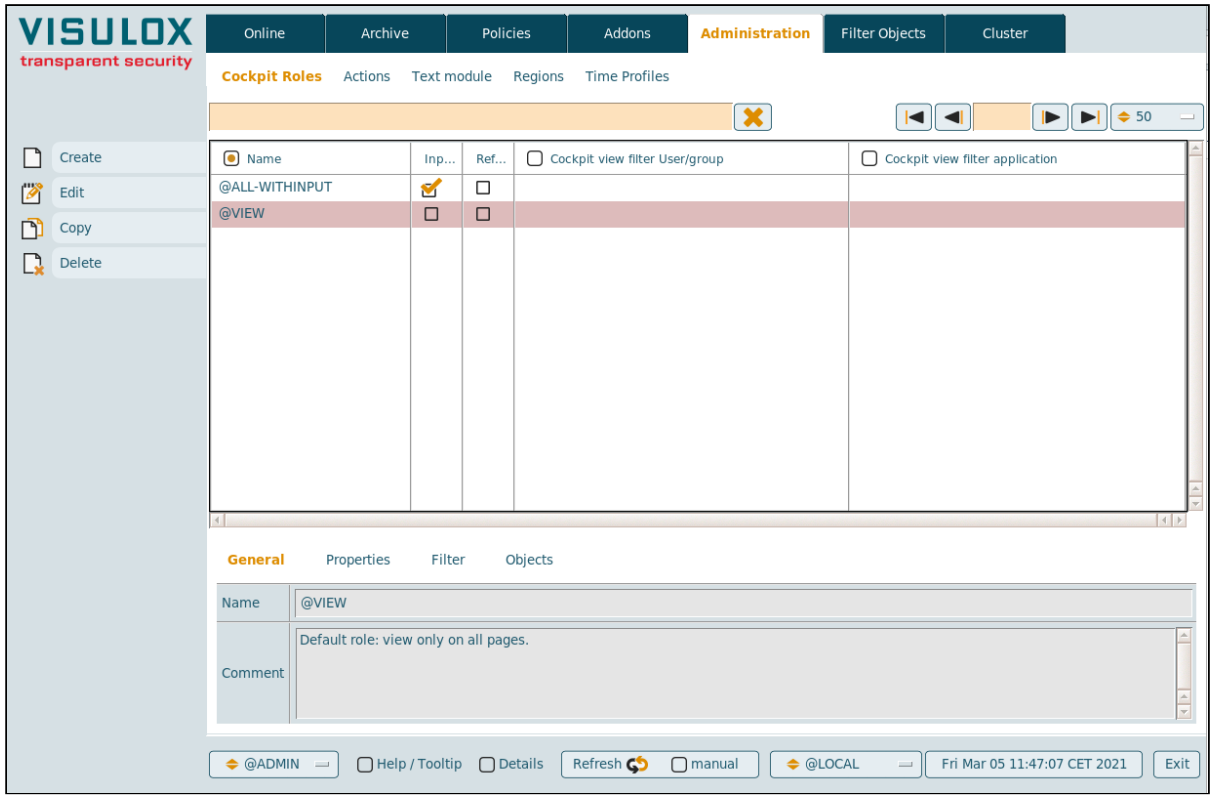
User	Role	eMail	SMS	Application	Other
Master	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	-
Miller	User	*<user>@company*.com	-	VISULOX Cockpit	-

Supervisor Master creates a new role profile for user Miller.

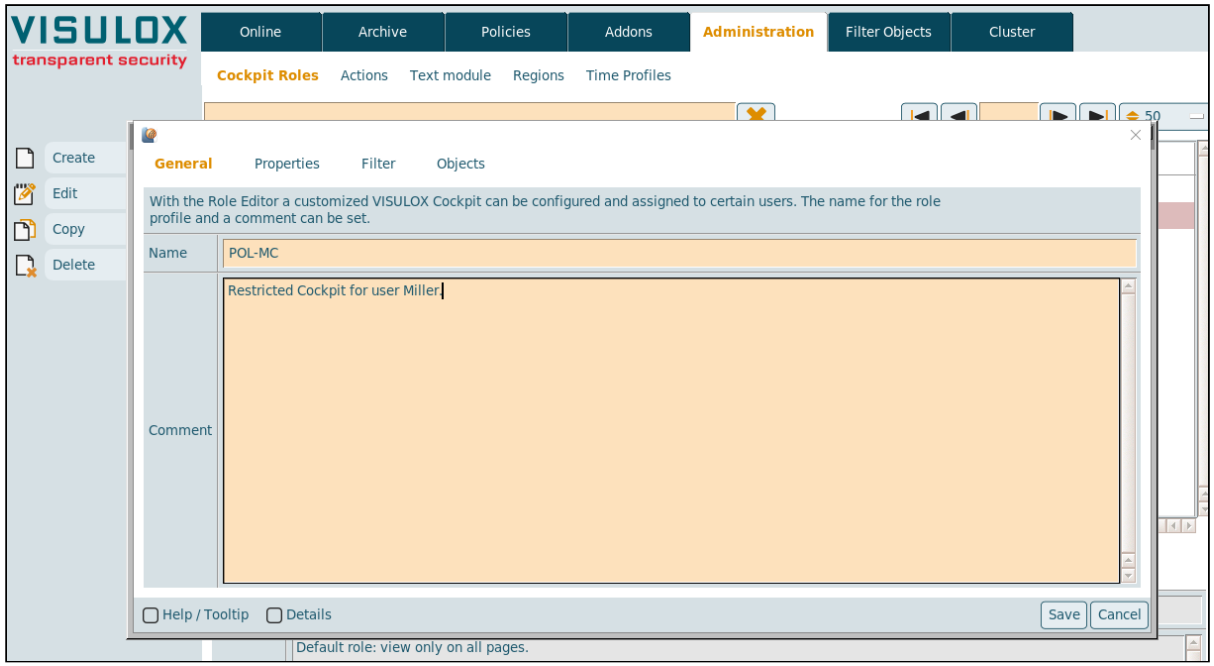
User Miller logs into the VISULOX PORTAL and starts his restricted Cockpit.

Creating a new role profile in Cockpit

1. User Master starts the "**VLX Cockpit**" application from his Workspace
2. Supervisor Master opens "**Cockpit / Administration / Cockpit Roles**":

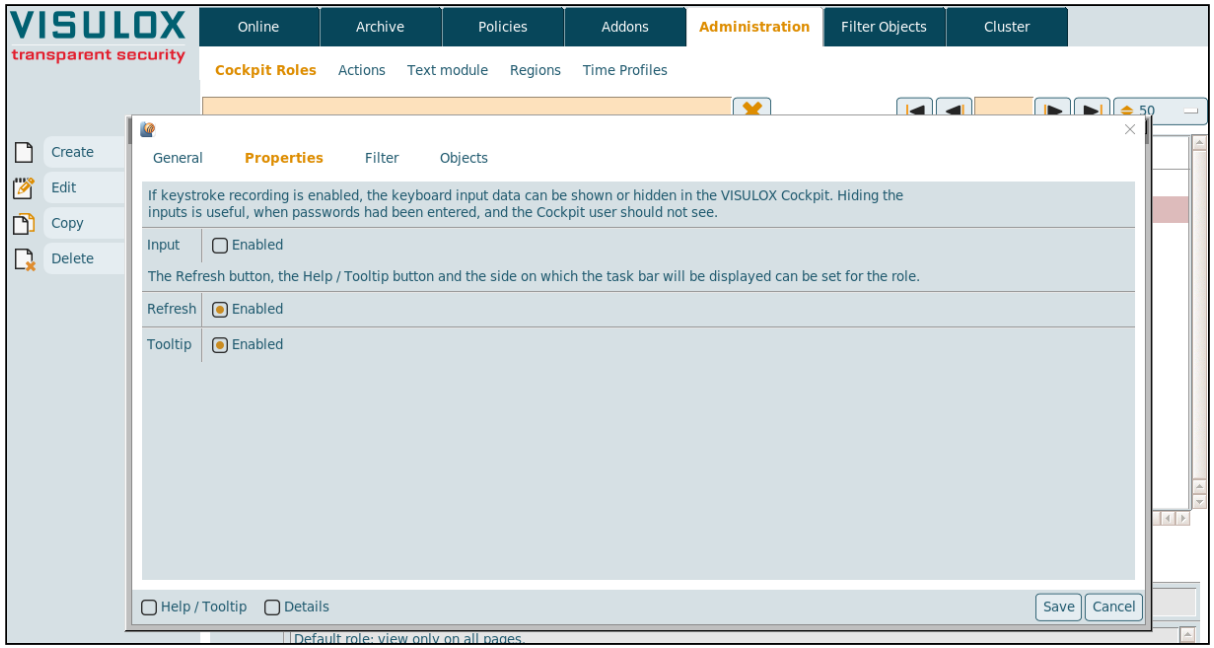


3. With the "**Create**" button, the General register tab of new Cockpit role profile is opened:



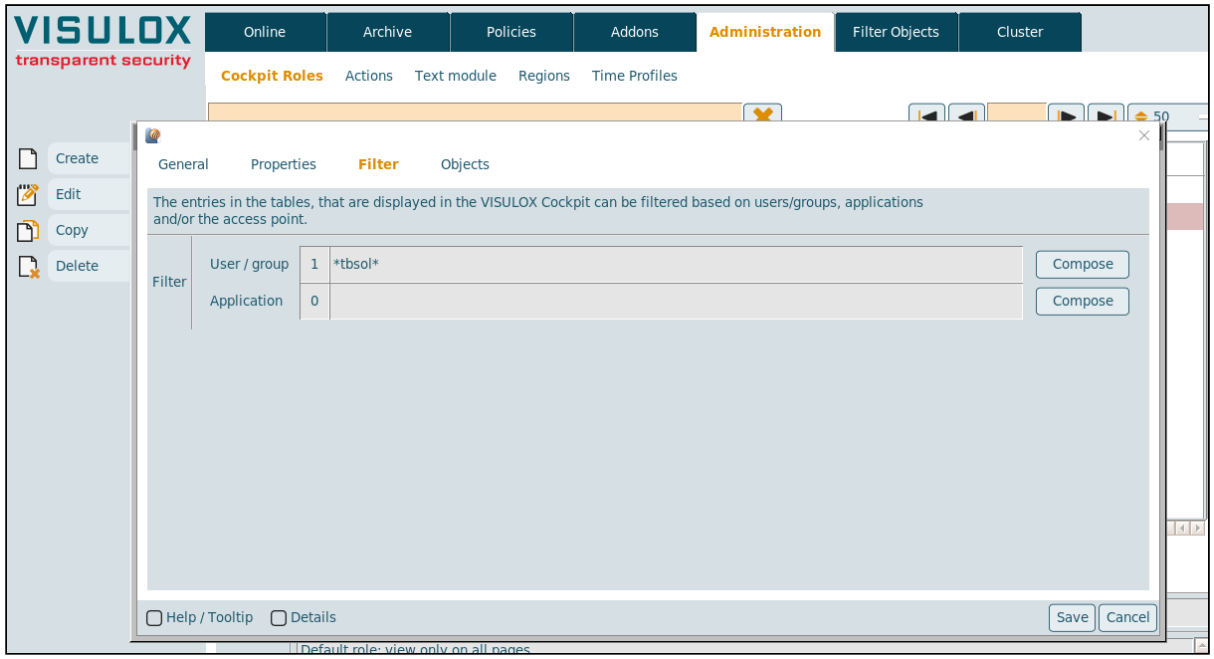
A unique name for the profile must be entered: "**POL-MC**".
A comment for the policy can be entered as well.

4. On the Proberties tab several settings can be adjusted:



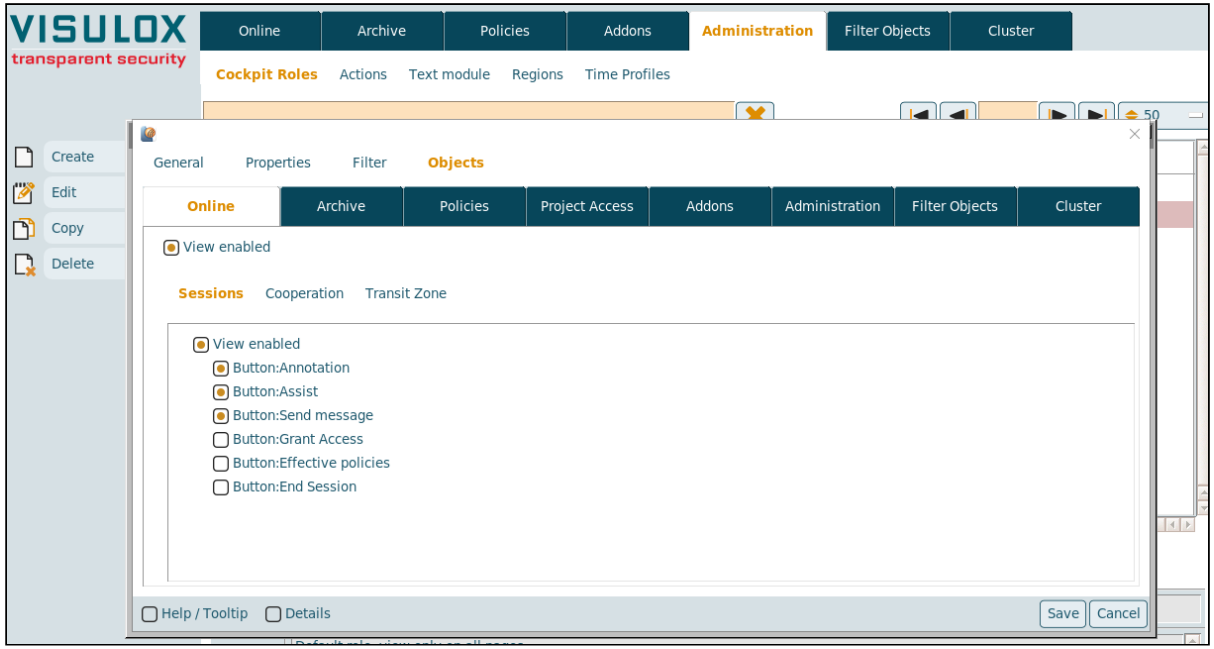
The **keyboard input data** should not be seen by user Miller, so this setting is left disabled for this user.
Refresh and **Help / Tooltip** will be available for Miller.

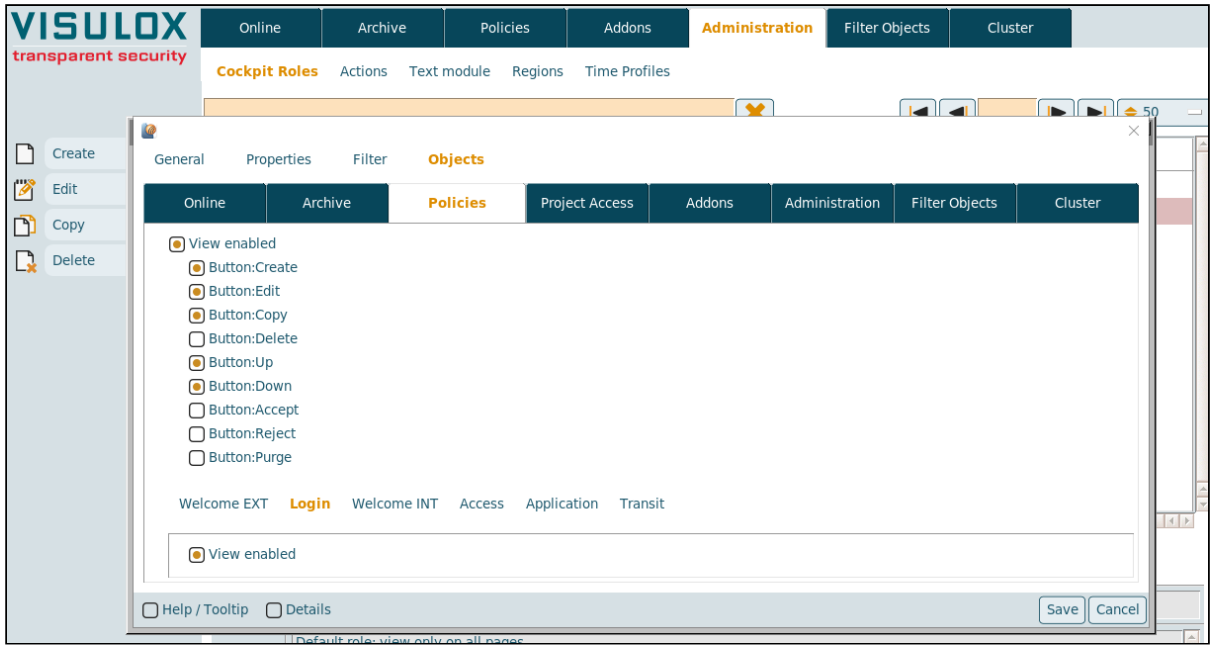
5. A filter for the displayed information in the Cockpit can be set:



The filter is set to the group "**tbsol**", so Miller can see only entries from users belonging to that group in his Cockpit.
Only the entries on the Online and Archive page are filtered.
Additional filters can be set based on the Remote IP address or on the access point (not used in this example).

6. Finally the displayed register tabs and the enabled features are set:

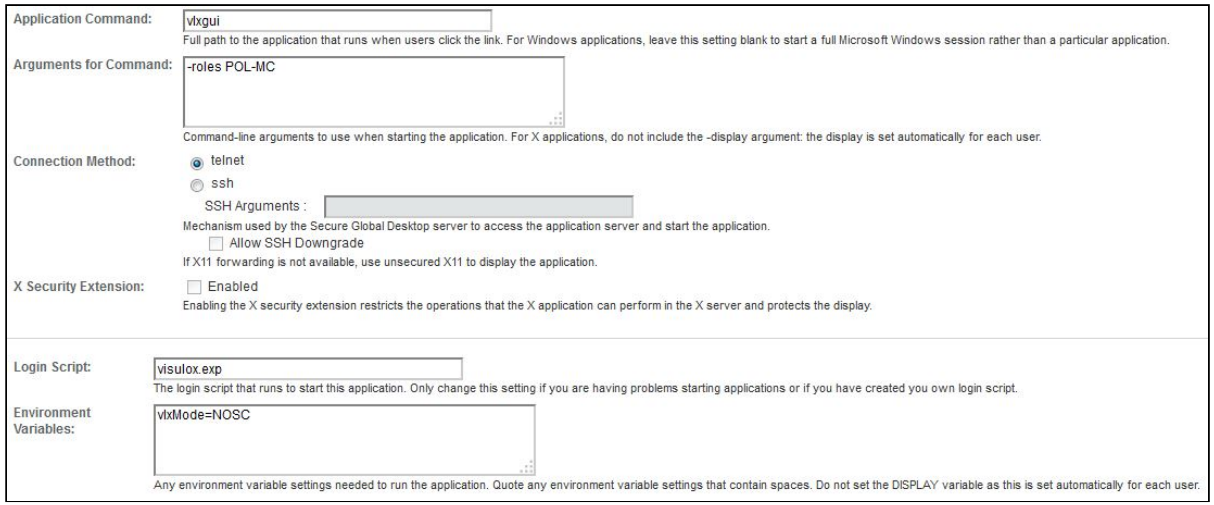

VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
Cluster
Cockpit Roles
Actions
Text module
Regions
Time Profiles
Create
Edit
Copy
Delete
General
Properties
Filter
Objects
Online
Archive
Policies
Project Access
Addons
Administration
Filter Objects
Cluster
View enabled
Sessions
Cooperation
Transit Zone
View enabled
Button:Annotation
Button:Assist
Button:Send message
Button:Grant Access
Button:Effective policies
Button:End Session
Help / Tooltip
Details
Save
Cancel



In this example user Miller will be able to see the running sessions of the users from group "**tbsol**".
He can create **annotations**, **assist** users and **send messages** to the users.
Grant Access, **Effective Policies** and **Ending Sessions** is not available for Miller.
The Policy tab will also be enabled for Miller, so that he is able to grant access to the users in the "**tbsol**" group.
He can **Create**, **Edit** and **Copy** Access Policies. **Moving** the Access Policies **Up** and **Down** is enabled as well.
Miller can not **Delete** policies. **Accept** / **Reject** and **Purge** is not enabled as well.

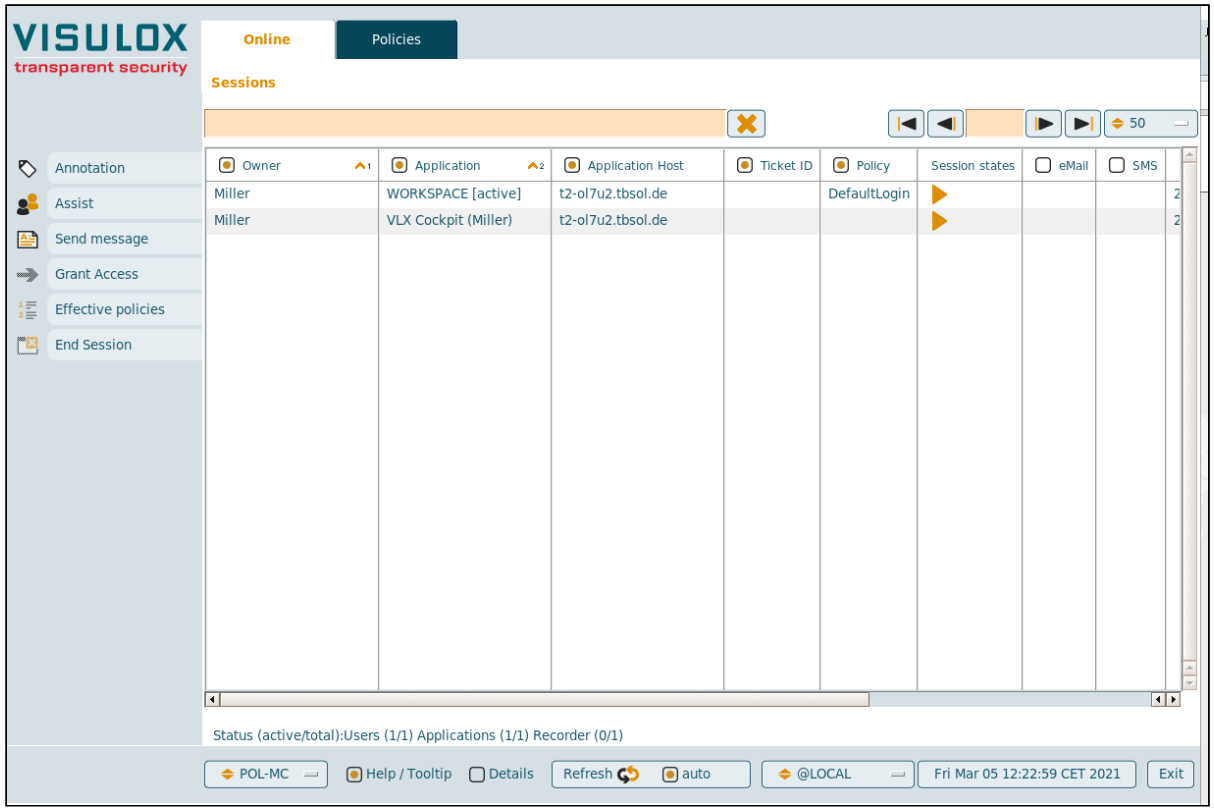
The view is enabled only for **Login Policies**.

7. The new restricted Cockpit now has to be assigned to user Miller in the **VISULOX PORTAL Console**:



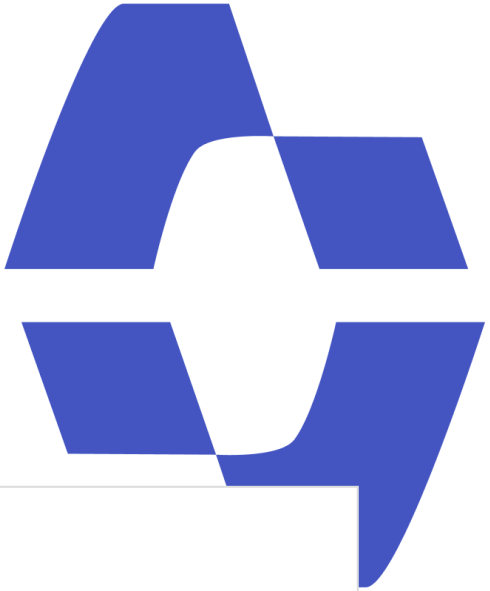
The parameters are the same as for all Cockpits, **except** the "**Arguments for Command setting**".
With "**-roles POL-MC**", the created role profile will be set for this Cockpit. More roles can be set at once separated by "**,**" and can be switched in the started Cockpit.
This Cockpit application then is **assigned** to user Miller.

8. ser Miller now can start the new assigned Cockpit from his Workspace:



Register tabs, that are not configured are not displayed.
So, In this example only the "**Online**" and the "**Policies**" tab can be seen.
Buttons that are not enabled in this role profile are grayed out.

On the bottom status line, the name of the used role profile and the configured checkboxes and buttons are displayed: **Refresh** and **Help / Tooltip** (the detail checkbox is always available).



See also:

How to control the VISULOX Cockpit

How to control VISULOX Cockpit roles from the command line

23.1.11 How to export information from VISULOX on the command line

- Overview
- Usage
- Export criteria
  - Using exportid
  - Using starttime and endtime

Overview

VISULOX Command Line Interface allows to export information.
There are three export types:

Sessions	Export session data and films including the player to a directory
Files	Export transferred files
Events	Export VISULOX Events

Usage

The data on the local node, in the cluster of the node or on the Archive Server can be exported.

The export is done in two steps:

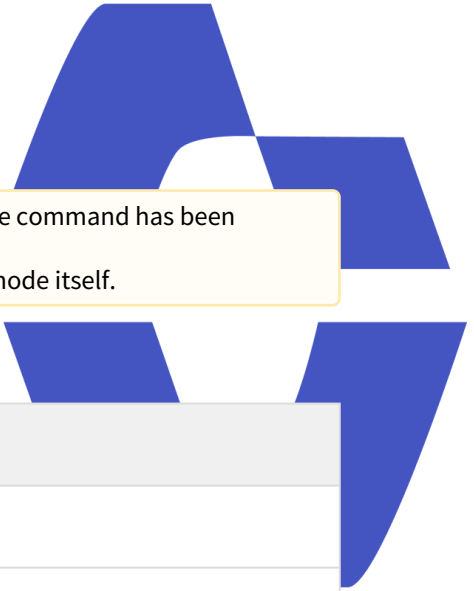
1. Find the data which fulfills the export criteria
2. Export the data into the directory

Per default, the export command does step 1. Step 2 is enabled with the **-run** option.

Options:

Parameter	Description
-directory <>	Directory for export. Default value: /tmp.
-exportid <>	Export ID of the data. Default value: std.
-object <>	Distinguished object of user or group. Object ID can be used as well!
-application <>	Export application (session only)
-starttime <>	Start time of session export. Default value: 0.
-endtime <>	End time of session export. Default value: now.
-mode <>	Mode: local, cluster or archive. Default value: cluster.
-grant <>	Set granted user in database record <>

Each time can be one of the following: the Unix epoch integer value, an interpretable time string (http://www.tcl.tk/man/tcl8.6/TclCmd/clock.htm#M80) or time arithmetic (http://www.tcl.tk/man/tcl8.6/TclCmd/clock.htm#M22).



⚠ Be careful, when setting the **-mode** variable to "**cluster**", all matching data from all VISULOX servers will be copied to the server, where the command has been started.
Make sure, that enough free disk space is available on this node or NFS share is used. The export can also be done "**local**" on every single node itself.

Export of **events** has some more options for a better presentation:

Parameter	Description
eventtypes	Present list of available events types
examples	Present some usage examples
fields	Present list of available events fields
keywords	Present list of available events keywords
-fields <>	Fields to present in the result. Default value: <*vlxowner,vlxevent,vlxeventinfo*>
-filters <>	Comma separated list of query filter <>
-orders <>	Comma separated list of fields to order <>

Export of **sessions** also has more options:

Parameter	Description
-password <>	Password for the ZIP archive. If the type is session and no password will be set, a password will be generated automatically.
-sessionid <>	Session ID <>
-kbi	Include Keyboard Inputs

Export criteria

Using exportid

Export filters can be set on objects (owner or groups) and applications. Also there is an **exportid.**

With the exportid it is possible to export only the data, which does not have that exportid already. After a successful run the exported data is marked with the exportid.

```
visulox export sessions -object cn=Group1 -directory /tmp/export -exportid "Group1" -run
```

(The directory must be readable/writeable by the vlx user.)

To restart the export from the beginning with exportid use **-force**.

Wildcards

The object parameters are always used internally with the wildcard "*" at the beginning and at the end.

Using starttime and endtime

export last week

```
visulox export sessions -object cn=Group1 -directory /tmp/export -starttime "-1 week" -endtime now -run
```

23.1.12 rrdtool error in logfile / graphical usage not displayed in VISULOX Cockpit (known issue)

If the runtime data for the graphical usage display was created on another OS / machine, the graphical usage is not displayed in the VISULOX Cockpit and the following error is shown in the log file:

```
2014-08-08 15:45:12.355:vMPOL6U3DEVEL:error:[16911]:stats:RRD::add:
err=<ERROR: This RRD was created on another architecture>
opt=<-code 1 -level 0
-errorstack {INNER invokeExpanded CALL {RRD::add 1407505512:0:0:0}}
-errorcode {CHILDSTATUS 18252 1}
-errorinfo {ERROR: This RRD was created on another architecture

 while executing

 "exec $rrdtool update $rra {*}$datapoints"} -errorline 9>
```

One possible explanation: the RRD file was created on a 32bits machine, and vMPOL6U3DEVEL is a 64bits machine.

To solve this, the runtime data for rrdtool must be deleted:

```
rm -rf /opt/visulox/data/usage/
```

23.1.13 Watching recorded films with the VISULOX player

Overview

Player

In VISULOX Cockpit / Archive / Sessions all ended recorded sessions are displayed.
Selecting a recorded session and pressing the "**Player int**" button starts the player directly in the Cockpit.

The VISULOX player has several views, controls and presents all information available for the recorded film.

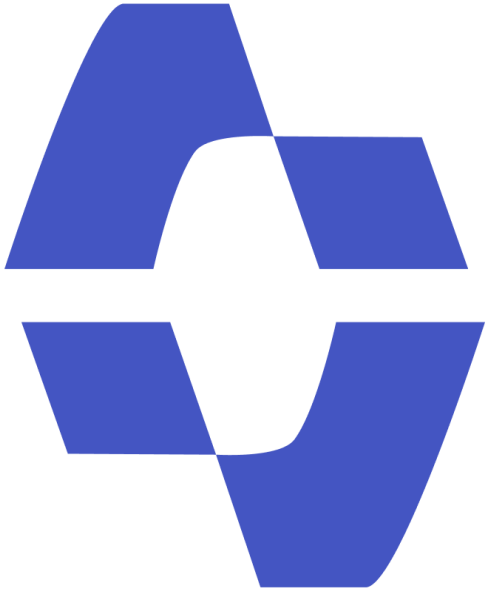
Live player

Users are able to start a live player in their recorded application session to see what has been recorded in this session so far.

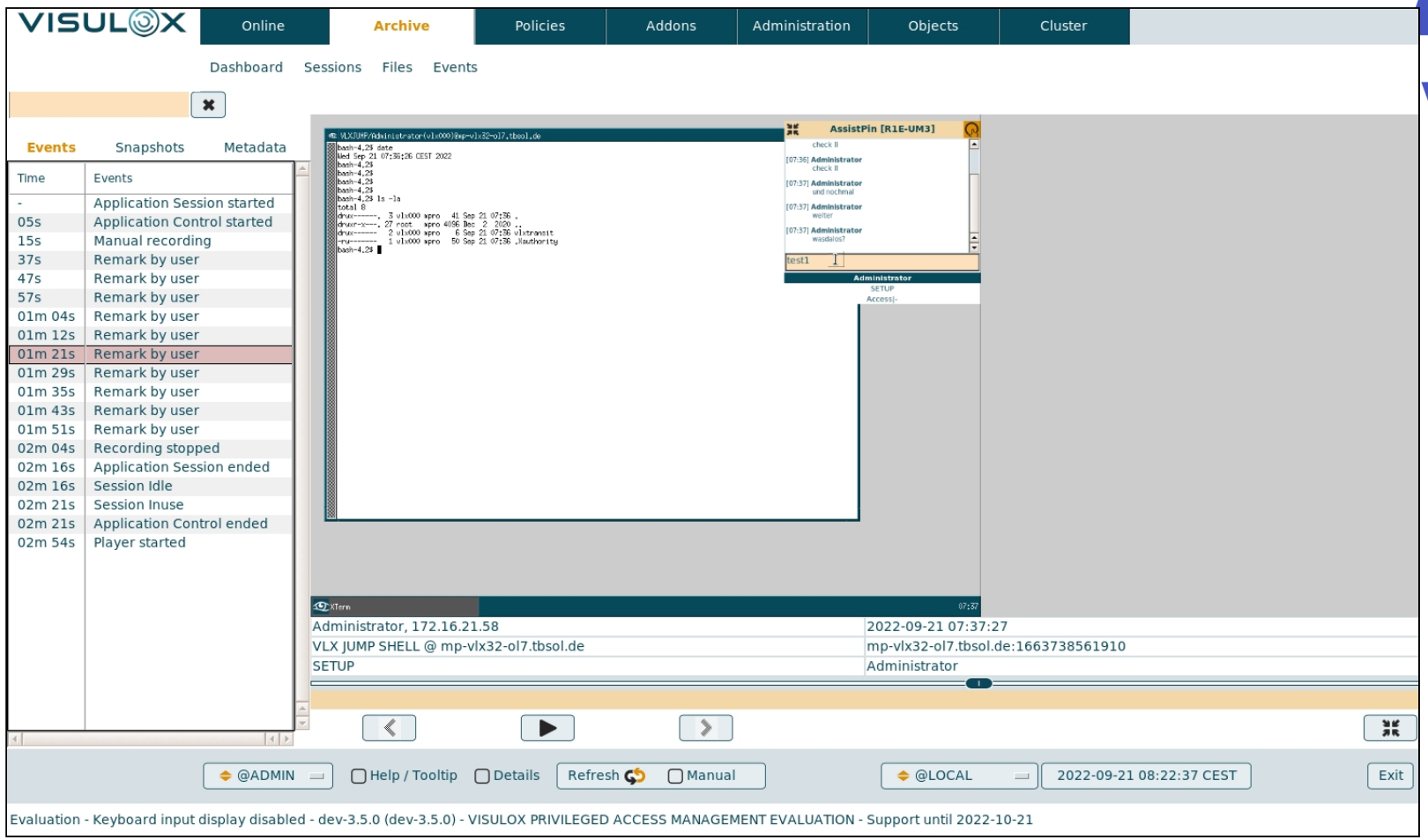
Checkout

It is also possible to checkout the recorded sessions to the Transit Zone of the user (via Checkout button in the Cockpit or CLI), where they can be downloaded to the client. Multiple checkout of recorded sessions is supported and can be configured.

- Overview
- Player elements
- Features
  - Search field
  - Player tab views
  - Main screen
  - Player controls
- Live player
- Checked out recorded films
  - Checkout via Cockpit
  - Offline player
  - Checkout via command line
  - Checkout configuration options



Player elements


VISULOX
Online
Archive
Policies
Addons
Administration
Objects
Cluster
Dashboard
Sessions
Files
Events
Events
Snapshots
Metadata
Time
Events
- Application Session started
05s Application Control started
15s Manual recording
37s Remark by user
47s Remark by user
57s Remark by user
01m 04s Remark by user
01m 12s Remark by user
01m 21s Remark by user
01m 29s Remark by user
01m 35s Remark by user
01m 43s Remark by user
01m 51s Remark by user
02m 04s Recording stopped
02m 16s Application Session ended
02m 16s Session Idle
02m 21s Session Inuse
02m 21s Application Control ended
02m 54s Player started
AssistPin [R1E-UM3]
Administrator, 172.16.21.58
2022-09-21 07:37:27
VLX JUMP SHELL @ mp-vlx32-ol7.tbsol.de
mp-vlx32-ol7.tbsol.de:1663738561910
SETUP
Administrator
@ADMIN
Help / Tooltip
Details
Refresh
Manual
@LOCAL
2022-09-21 08:22:37 CEST
Exit
Evaluation - Keyboard input display disabled - dev-3.5.0 (dev-3.5.0) - VISULOX PRIVILEGED ACCESS MANAGEMENT EVALUATION - Support until 2022-10-21

Features

Search field

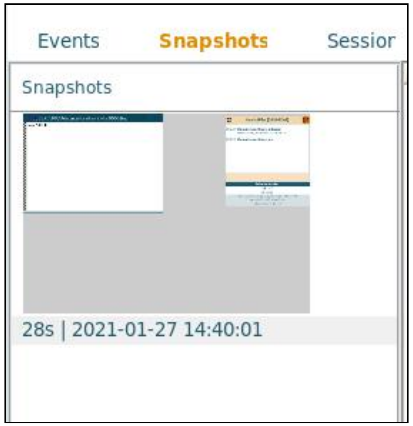
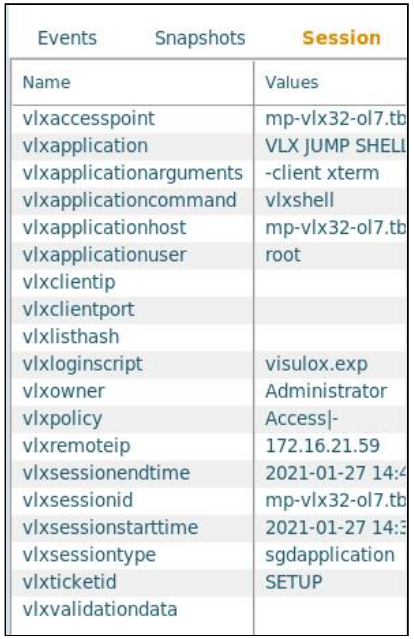
In the search field the events can be filtered:

- Search is also done in event information (keyword, info ...)
- Search is case insensitive
- Search with glob mask is possible

Player tab views

Events	Event list with all registered events is displayed, jumping to events with double click is possible
Snapshots	Snapshots of the tecorded session are displayed, jumping to snapshots with double click is possible
Session	More details can be displayed for the session (e.g. user information)

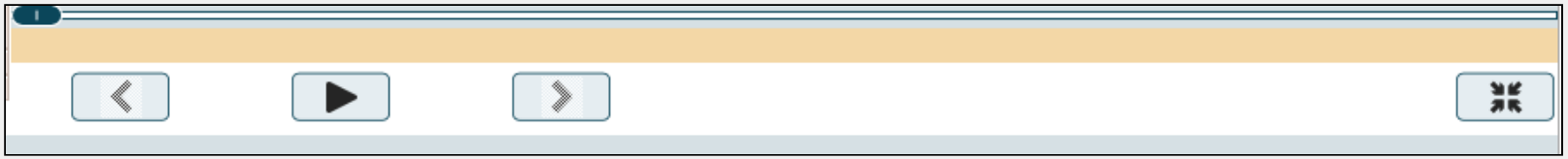
Below the sidebar the **current active user** is displayed (useful in recorded cooperation sessions with more participants).

Events	Snapshots	Session
		

Main screen

- The film is displayed in the main part of the screen. The detailed session information of the recorded film is available in the **Session** tab, showing information about the portal user name, the application name, the Application Server and the time.

Player controls



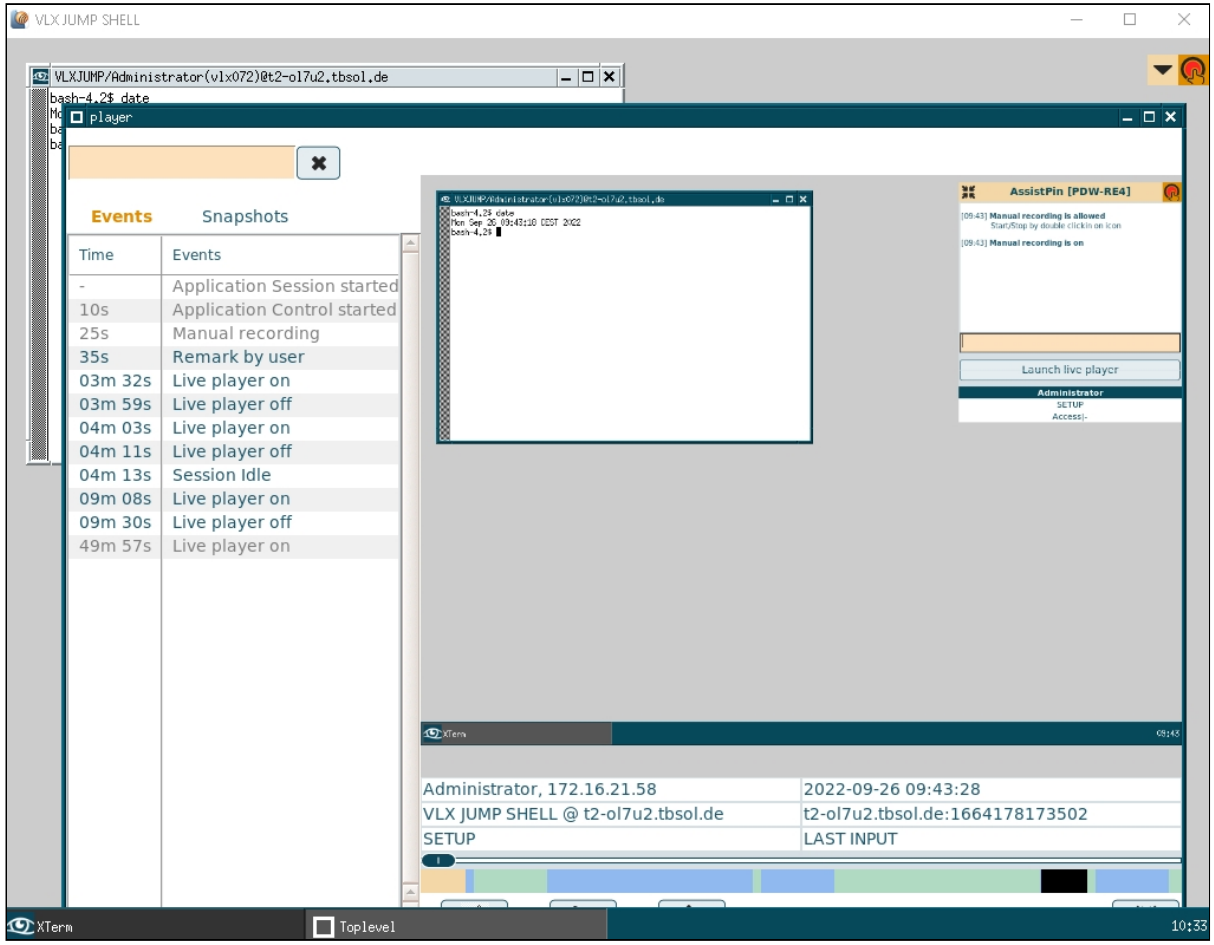
Timeline	Moveable marker for current position in the running chapter.
Chapter line	Moveable marker for current position in chapter. The current chapter and the name of the current user is displayed. The current date / time and the time remaining in the chapter is displayed.
Player controls	• **PREV Chapter:** Jump to previous chapter • **PLAY / PAUSE:** Play / pause of the chapter at this position • **NEXT Chapter:** Jump to next chapter • **SCALE:** Scale film to screen or reset

Live player

To enable the live player in recorded application sessions, use:

```
visulox config -name recorder.liveplayer=true
```

With this setting the "**Launch live player**" button is displayed in the session controller and the session can be watched from the beginning :



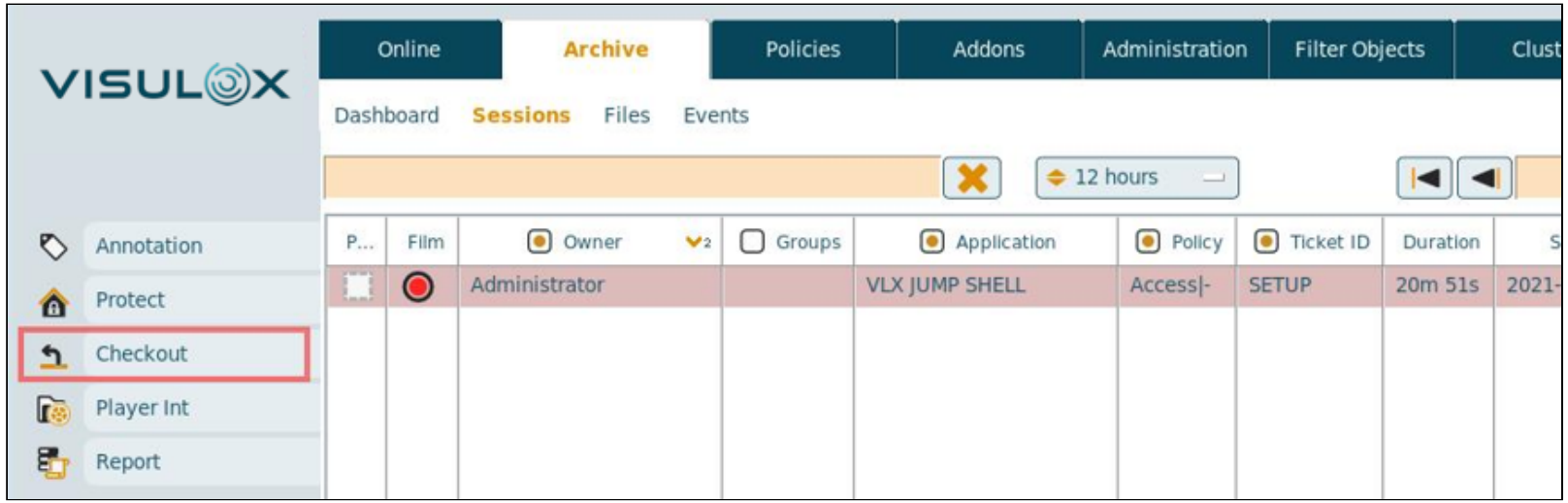
- The live player can be enabled for all types of recorded sessions, e.g manual recording, recording via poliy, etc
- The session is still recorded, when using the live player.

- Keyboard entries are not displayed in the live player

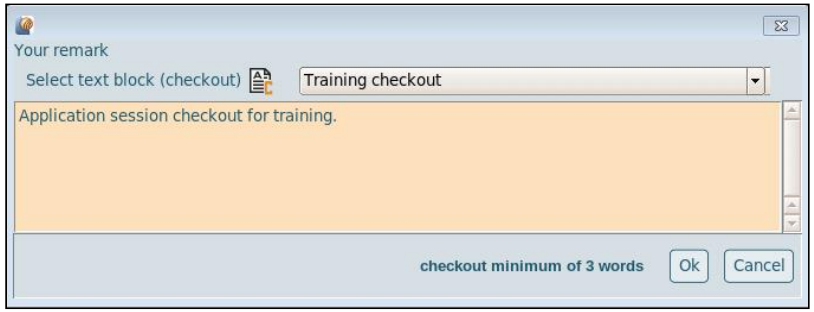
Checked out recorded films

Checkout via Cockpit

Selected recorded sessions can be checked out with the **Checkout** button on the **Archive / Session page** of the Cockpit.



- A comment has to be filled out for every checkout:

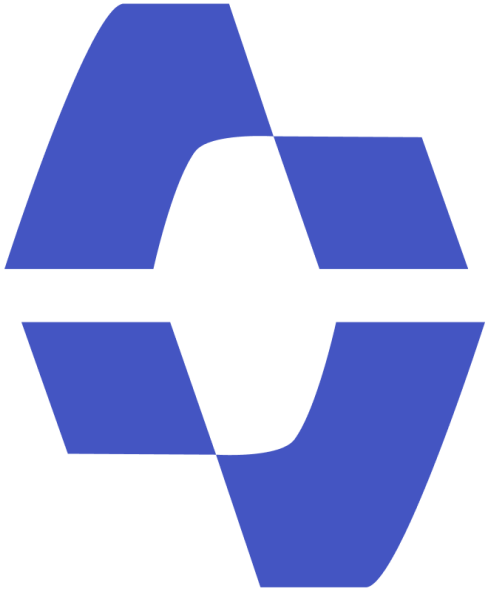


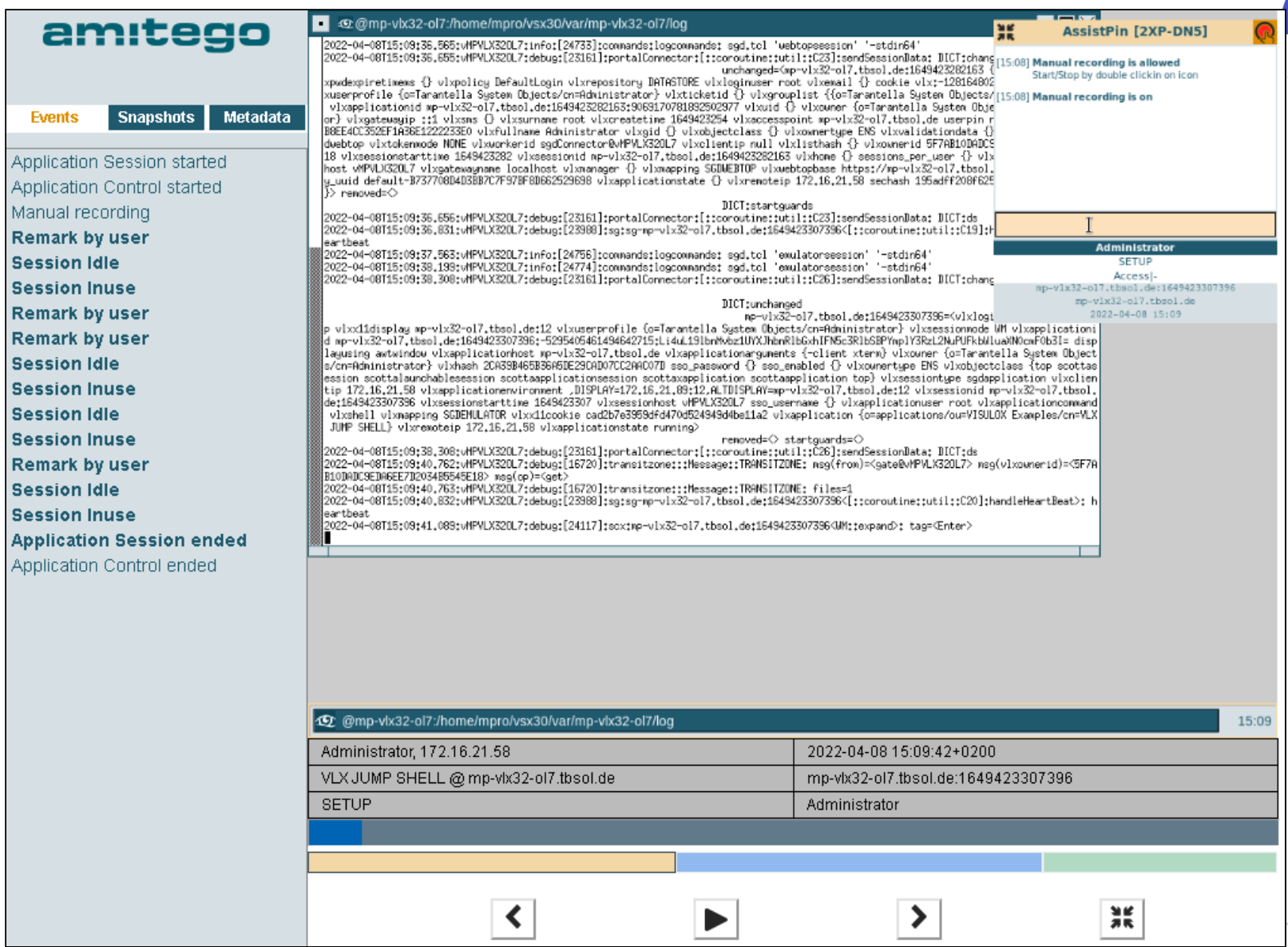
- The ZIP-Archive password is displayed and copied to clipboard:

Once the session is checked out, it is available for download in the **File Transit Zone** of the user:

The files have to be extracted from the downloaded ZIP-Archive (ZIP password is needed!).

Then the recorded chapters can be watched in the browser by opening the chapter HTML files:




amitego
Events
Snapshots
Metadata
Application Session started
Application Control started
Manual recording
Remark by user
Session Idle
Session Inuse
Remark by user
Remark by user
Session Idle
Session Inuse
Session Idle
Session Inuse
Remark by user
Session Idle
Session Inuse
Application Session ended
Application Control ended
@mp-vlx32-ol7:/home/mpro/vsx30/var/mp-vlx32-ol7/log
AssistPin [2XP-DN5]
[15:08] Manual recording is allowed
Start/Stop by double clickin on icon
[15:08] Manual recording is on
Administrator
SETUP
@mp-vlx32-ol7:/home/mpro/vsx30/var/mp-vlx32-ol7/log
15:09
Administrator, 172.16.21.58
2022-04-08 15:09:42+0200
VLX JUMP SHELL @ mp-vlx32-ol7.tbsol.de
mp-vlx32-ol7.tbsol.de:1649423307396
SETUP
Administrator

The offline player has three tabs: Events, Snapshots and Metadata.
A footnote with information about the session is attached on the bottom of the film.

Player controls	• **PREV Chapter:** Jump to previous chapter • **PLAY / PAUSE:** Play / pause of the chapter at this position • **NEXT Chapter:** Jump to next chapter • **SCALE:** Scale film to screen or reset

Checkout via command line

Recorded sessions can also be checked out with the **visulox export sessions** command.

For example:

Export all recorded sessions from Administrator in the last week

```
visulox export sessions -object Administrator -directory </tmp/export> -starttime "-1 week" -endtime now -run
```

For a detailed description of the **visulox export** command, see: How to export information interactive from VISULOX

Checkout configuration options

visulox config -name checkout.

```
-----------------------------------------
| changed | key              | value  |
-----------------------------------------
|         | checkout.disksize | 10.0GB |
```

	checkout.max	40

23.1.14 How VISULOX handles presentation roles

Overview

With the VISULOX role editor it is possible to apply one or more roles to a user, who is working with a VISULOX GUI.

A role includes beside a case sensitive role name without spaces, properties for the GUI, filter for the views and usage of register tabs.

Within the application definition in the VISULOX PORTAL, these roles can be applied with the option **-roles** and a comma separated list of roles names.

- Overview
- Role properties
- Role view filters
- Known issues and comments

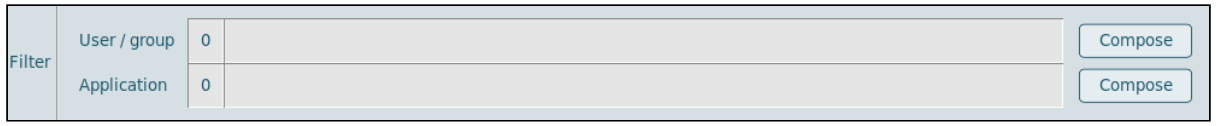
Role properties

Property	Behaviour
Keyboard input data	If enabled the user will be able to see the keyboard input events in the event log. These events include any input (including passwords) ⚠ into a session.
Refresh	If enabled, the GUI will have an automatic refresh, when the data in the current register tab has been changed. If many sessions are under VISULOX control, it is possible to disable the automatic refresh to be able to work with the GUI. New data will be signalized to the user. Pressing F5 will do an immediate update.
Help / Tooltip	If enabled, pointing to a field will present an information tooltip to the user.

Role view filters

The VISULOX views include username and groups the users belong to or the application.

The Online and Archive page view can be controlled with a role filter for user/ group or application.



If set, the supervisor will see only data matching these filters.

With "Remote IP" and "Access Point" the role can be adjusted only to apply to these criterias.

ONLY the default role can assign role mask files. A role cannot be configured to open more than the role has itself.

Known issues and comments

A role is generated for a specific application (vlxhelpdesk, vlxadmin) and can only be used for that application. Currently there is no check if a role applies to an application.

See also:

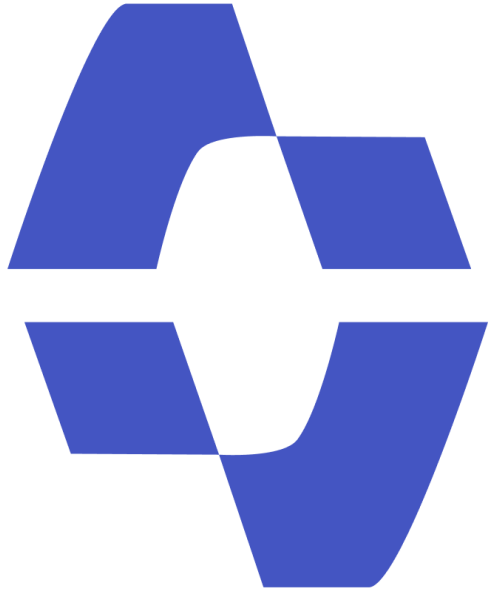
(4.2.0) How VISULOX handles presentation roles

(4.2.0) How to configure role profiles for the VISULOX Cockpit

(4.2.0) How to control Cockpit roles from the command line

(4.2.0) Restrict default VISULOX Cockpit

(4.3.2) How to control Cockpit roles from the command line



(4.3.2) How to configure role profiles for the VISULOX Cockpit
(4.3.2) How VISULOX handles presentation roles
(4.3.2) Restrict default VISULOX Cockpit
(4.1.1) How to configure role profiles for the VISULOX Cockpit
(4.1.1) How VISULOX handles presentation roles
(4.1.1) How to control Cockpit roles from the command line
(4.1.1) Restrict default VISULOX Cockpit
(4.3.1) How to configure role profiles for the VISULOX Cockpit
(4.3.1) How VISULOX handles presentation roles
(4.3.1) Restrict default VISULOX Cockpit

23.1.15 Network communication within VISULOX

Overview

There are several communication paths into, within, or out of a VISULOX environment.

This article describes the communication paths within the platform.

The article is based on the standard communication parameters within VISULOX.

- Overview
- Accessing client with VISULOX GATEWAY
- Accessing client without VISULOX GATEWAY
- VISULOX GATEWAY to VISULOX PORTAL Service
- VISULOX PORTAL Service to VISULOX PORTAL Service
- VISULOX PORTAL Service to VISULOX Service
- VISULOX Service on VISULOX ACCESS Node
- VISULOX Service on other servers to the VISULOX PORTAL Service
- VISULOX Service to VISULOX Service
- Accessing the VISULOX Transit Page
- Example configuration for firewalld (Linux 7.x)
    - VISULOX PORTAL Service
    - VISULOX Service

⚠ The VISULOX communication is dedicated to one interface.

⚠ A firewall between nodes in the cluster (VISULOX Service Nodes and VISULOX PORTAL Service Nodes) must be configured with the following setting "**session time out=never**".

Accessing client with VISULOX GATEWAY

VISULOX GATEWAY access, initiated from the client:

Port	Comment
https/443	User client communicates with HTTPS to the LoadBalancer or each VISULOX GATEWAY

Accessing client without VISULOX GATEWAY

Direct access, initiated from the client:

Port	Comment
https/443	Client communicates with HTTPS to each VISULOX PORTAL Service
AIP/5307	In VISULOX GATEWAY or in non firewall traversal mode, the client communicates to each VISULOX PORTAL Service

VISULOX GATEWAY to VISULOX PORTAL Service

Communication between VISULOX GATEWAY and VISULOX PORTAL Service, initiated from the VISULOX GATEWAY:

Port		Comment
https/443	TCP	HTTPS dialog
AIP/5307	TCP	AIP dialog

See also: How to check VISULOX PORTAL ports 443 & 5307

VISULOX PORTAL Service to VISULOX PORTAL Service

Port		Comment
PortalARRAY/5427	TCP	Communication
x11-offset/6000+	TCP	Assist, Dual Control, ttashadow

VISULOX PORTAL Service to VISULOX Service

No firewall rule needed, only loop-back communication:

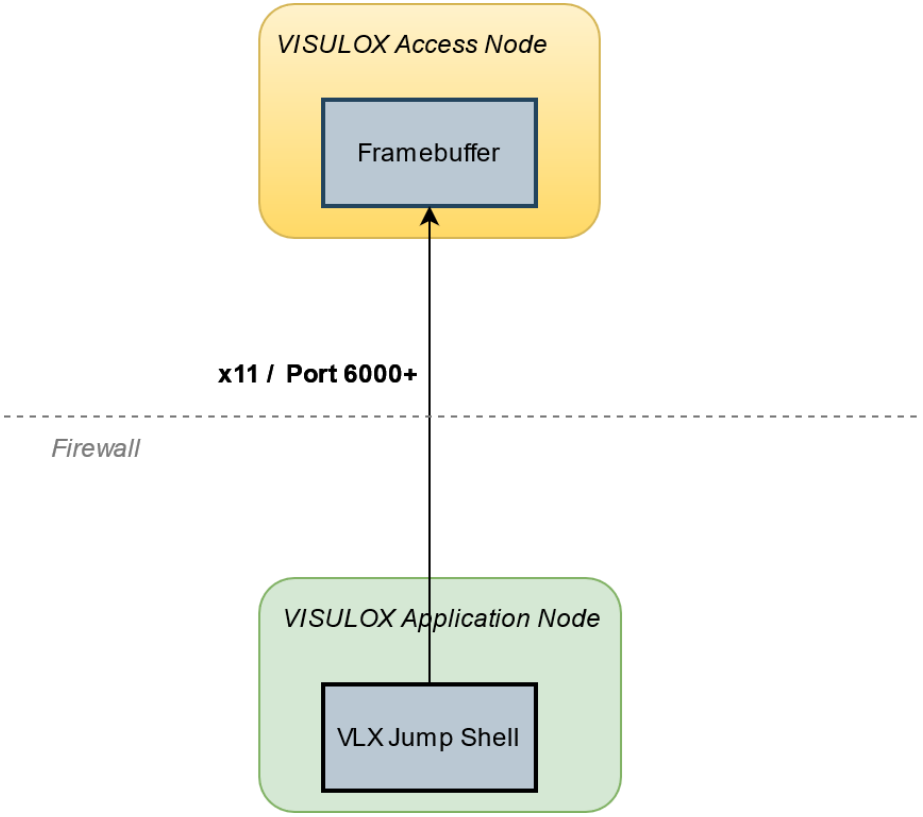
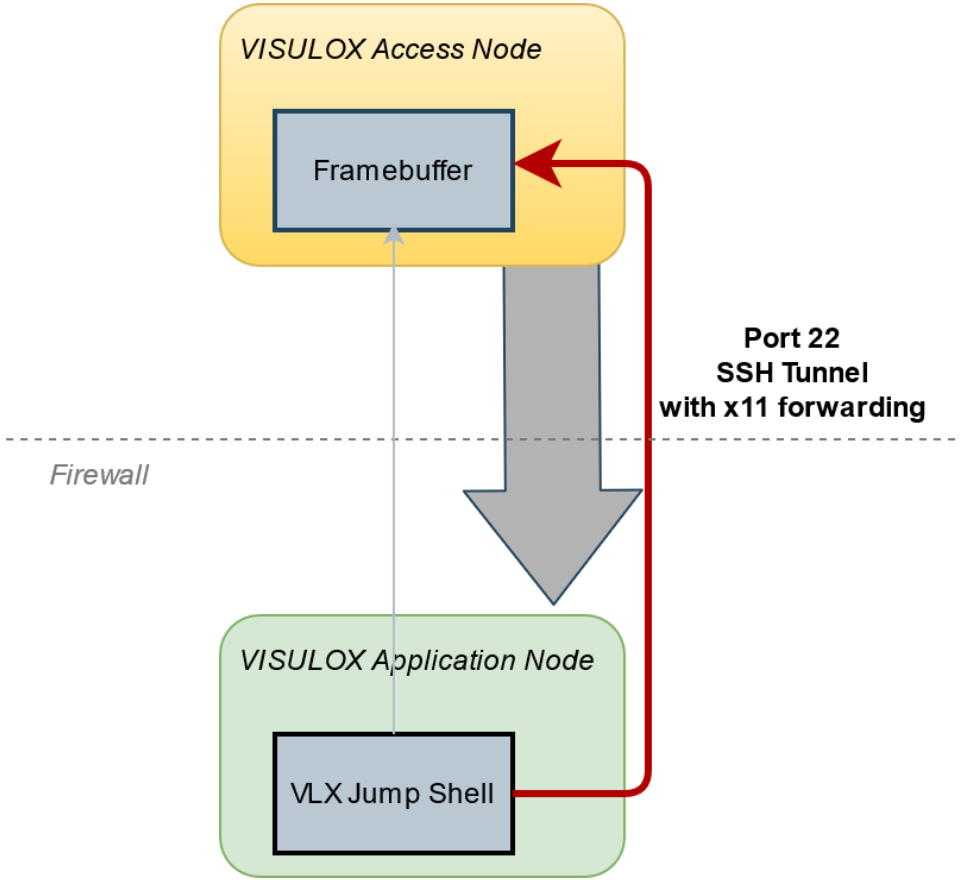
Port		Comment
9001	TCP	This will be only an internal (localhost) communication on VISULOX ACCESS Nodes, where VISULOX PORTAL Service and VISULOX Service is installed

VISULOX Service on VISULOX ACCESS Node

Port		Comment
443	TCP	VISULOX reads the VISULOX PORTAL webservice via a localhost connection (only loop-back communication:)

VISULOX Service on other servers to the VISULOX PORTAL Service

Port		Comment
x11-offset/6000+	TCP	VISULOX Cockpit, Jump Shell, Command Connect, Command Guard or FT Client always use a VLX transituser. If one of these programs is used on another server, it is necessary that this server is able to communicate via X11 native (port 6000+). ⚠ For example a VISULOX Archive Server will need this port open. See also: VISULOX SSH X11 Forwarding to VISULOX Application Nodes

Connection with port 6000+	Connection with VLX x11 forwarding
	

VISULOX Service to VISULOX Service

Communication between any VISULOX Node (including Archive Node) in a VISULOX Cluster, initiated from a VISULOX Node:

Port		Comment
7001	TCP	Send requests to the VISULOX router
7002	TCP	Status updates from other VISULOX routers
7003	TCP	File Transfer service between nodes
7004	TCP	Reserved for future communication
7005	TCP	ETCD cluster communication
7006	TCP	ETCD client to cluster communication
7007-7010	TCP	Reserved for future communication

These ports are also checked within VISULOX Integrity-Check.

Accessing the VISULOX Transit Page

Connection from a browser running on an internal application server, initiated from the application server:

Port		Comment
https/1443	TCP	User can connect to the File Transfer Transit page. This service can be configured to be available only on a specific VISULOX Node

Depending on the environment and the specific software (e.g. nagios, yum, anti-virus updates, etc) installed on the server it may become necessary to allow further ports for communication.
This weakens the security concept and has to be done very carefully for each single server.

Example configuration for firewalld (Linux 7.x)

VISULOX PORTAL Service

Create new file: **/usr/lib/firewalld/services/tta.xml**

/usr/lib/firewalld/services/tta.xml

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>Portal Firewall Rules</short>
  <description>The following rules are needed for the VISULOX PORTAL Service.</description>
  <port protocol="tcp" port="80"/>
  <port protocol="tcp" port="443"/>
  <port protocol="tcp" port="5307"/>
  <port protocol="tcp" port="5427"/>
</service>
```

VISULOX Service

Create new file: **/usr/lib/firewalld/services/vlx.xml**

/usr/lib/firewalld/services/vlx.xml

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>VISULOX Firewall Rules</short>
  <description>The following rules are needed for the VISULOX Service and the VISULOX Components.</description>
  <!-- Recorder Access on VISULOX PORTAL Nodes  -->
  <port protocol="tcp" port="6000-6500"/>
  <!-- VISULOX Communication -->
  <port protocol="tcp" port="7001-7010"/>
  <!-- Webservice, FTPD and Fileexchange  -->
  <port protocol="tcp" port="21"/>
  <port protocol="tcp" port="1443"/>
  <port protocol="tcp" port="8114"/>
  <port protocol="tcp" port="8115"/>
</service>
```

Use the following commands to permanently enable the VISULOX firewall rules:

```
firewall-cmd --permanent --zone=public --add-service=vlx
firewall-cmd --permanent --zone=public --add-service=tta

firewall-cmd --reload
success
```

23.1.16 Attaching VISULOX Service to VISULOX PORTAL Service

General

VISULOX Service connects the VISULOX PORTAL Service only locally. This means, on nodes **without** VISULOX PORTAL Service no connection is done, on nodes **with** VISULOX PORTAL Service (VISULOX ACCESS Node) the connection is done via localhost to the webservices. The connection gathers only the information from this VISULOX Access Node, so VISULOX Service must be installed on VISULOX PORTAL Service members in the array.

There is a single command interaction from VISULOX Service with VISULOX PORTAL Service:

```
visulox portal attach
```

This command has serveral arguments:

Command	Description
-all	Install all (default)
-portal	Modify VISULOX PORTAL only, write configuration
-examples	setup examples
-attach	Attach VISULOX Service to VISULOX PORTAL Service
-expect	Install expect script only

Command	Description
-webtop	Install webtop script only
-jspconfig	Create VISULOX JSP configuration file
-apacheport <*value*>	Local port to address Apache. If empty, discovered by webservice configuration <>
-externalport <*value*>	External port to address Apache. If empty, discovered by httpd.conf <>
-serviceonline <*value*>	Enable / disable Webtop Enhancements <true>
-adminuser <*value*>	UNIX user for the VISULOX webservice user in portal <vlxwebservice>
-adminuid <*value*>	User ID for the VISULOX admin user in VISULOX PORTAL <610>
-adminpwd <*value*>	Password for the VISULOX admin user in VISULOX PORTAL<generate>
-adminou <*value*>	OrgUnit for webservice user cn=<*host name*>/<adminou> <>
-version <*value*>	Force VISULOX PORTAL Service version <>

After joining the VISULOX PORTAL Array, run as root:

Attaching VISULOX

```
visulox portal attach
```

This command checks if login-ens is enabled. If this is the case a local user vlxwebservice (610) with group ttaserv (500) was added to the system. A password was also generated and stored secure.

How to use an already defined user

If the default generated user is not allowed, the user can be applied to the attach command. The user must exist and he must have a permanent password.

```
visulox portal attach -adminuser <name> -adminuid <uid> -adminpwd <pwd>
```

Testing

The connection can be tested with "**visulox integrity -portal**".

23.1.17 VISULOX PORTAL application color depth

VISULOX PORTAL can use different color depths for the sessions.

The following table shows the possible VISULOX PORTAL color definitions in the application configuration and their behaviour in VISULOX:

Color depth	**Cooperation**	
	RDP	**X11**
8 Bit	✗	⊖

Color depth	Cooperation	
	RDP	X11
16 Bit	✅	✅
24 Bit	✅	✅
8 / 16 Bit	-	⛔
8 / 24 Bit	-	⛔
16 / 8 Bit	-	✅
24 / 8 Bit	-	✅

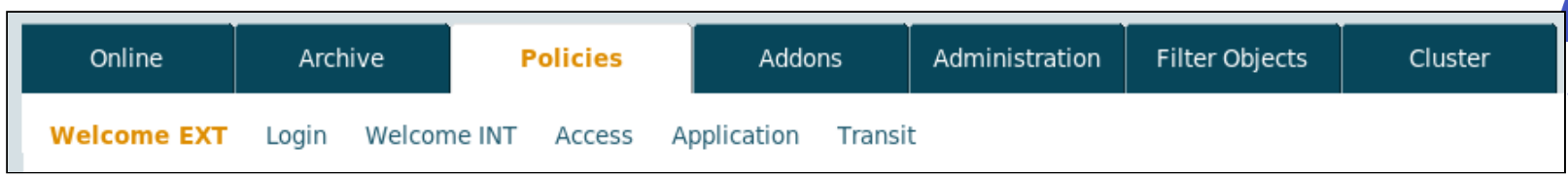
⚠ It is recommended, that all applications should use at least a color depth of **16 bit**

23.1.18 VISULOX Policies - Overview

Overview

With VISULOX everything is controlled by VISULOX policies. A VISULOX policy has a VISULOX filter and depending of the object a time, when the policy is valid.

Policies are defined in the VISULOX Cockpit.



When a user is working under VISULOX, six policies are relevant and applied in an order.

Login and Access Policies are ordered from top to down. This means, the first matching policy is applied.

A new Login or Access Policy is always placed on top of the list of policies.

Every policy takes use of VISULOX Filters.

After a policy has been changed, it may last up to 15 seconds until the adjusted policy is available on all nodes in the VISULOX Cluster.

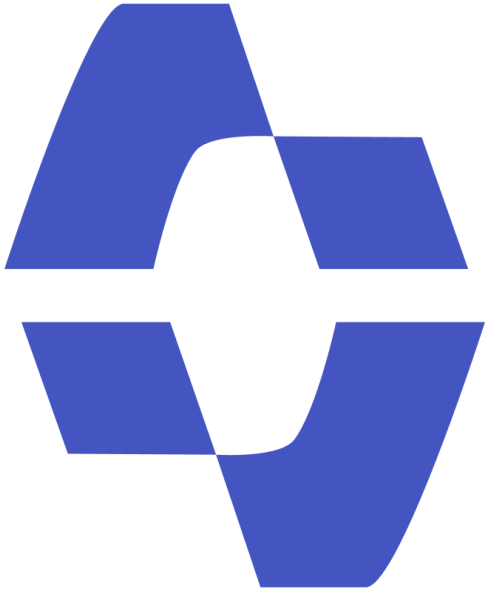
Policy	General Function	Filter Criteria	Filter Time Frame
Welcome EXT	Controls the information seen by every user on the VISULOX PORTAL login page. In this case the user is not authenticated.	Access Point	yes
Login Policy	During authentication the policy defines the behaviour in the login process, like: Login allowed, Login with 2FA, etc.	Remote IP Access Point User/Group	no

Policy	General Function	Filter Criteria	Filter Time Frame
Welcome INT	Controls the information seen by the authenticated user on his Workspace.	Access Point User/Group	yes
Access Policy	Controls if the authenticated user will have access to an application.	Remote IP Access Point User/Group Application	yes
Application Policy	Controls how VISULOX will control an application, e.g. with recording, with key stroke detection, etc.	Remote IP Access Point User/Group Application	no
Transit Policy	Controls the File Transfer into and out of the infrastructure	Remote IP Access Point User/Group	no

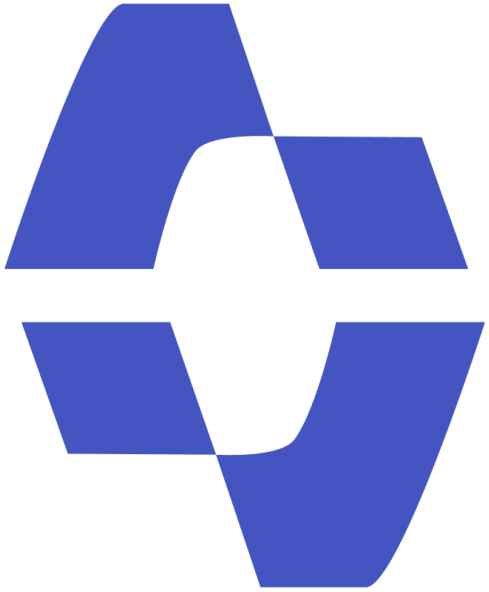
Policies via Command Line Interface

(4.2.0) How to control internal messages from the command line

(4.2.0) How to control access from the command line



(4.2.0) How to control external messages from the command line
(4.2.0) How to control applications from the command line
(4.2.0) How to control login from the command line
(4.2.0) How to control groupaccess from the command line
(4.2.0) How to control File Transit Policy from the command line
(4.3.2) How to control groupaccess from the command line
(4.3.2) How to control File Transit Policy from the command line
(4.3.2) How to control applications from the command line
(4.3.2) How to control external messages from the command line
(4.3.2) How to control access from the command line
(4.3.2) How to control login from the command line
(4.3.2) How to control internal messages from the command line
(4.1.1) How to control access from the command line
(4.1.1) How to control groupaccess from the command line
(4.1.1) How to control external messages from the command line
(4.1.1) How to control File Transit Policy from the command line
(4.1.1) How to control internal messages from the command line
(4.1.1) How to control login from the command line
(4.1.1) How to control applications from the command line
(4.3.1) How to control access from the command line
(4.3.1) How to control File Transit Policy from the command line
(4.3.1) How to control applications from the command line



(4.3.1) How to control groupaccess from the command line
(4.3.1) How to control external messages from the command line
(4.3.1) How to control login from the command line
(4.3.1) How to control internal messages from the command line
(4.3.0) How to control external messages from the command line
(4.3.0) How to control login from the command line
(4.3.0) How to control File Transit Policy from the command line
(4.3.0) How to control internal messages from the command line
(4.3.0) How to control applications from the command line
(4.3.0) How to control access from the command line
(4.3.0) How to control groupaccess from the command line
How to control File Transit Policy from the command line
How to control applications from the command line
How to control groupaccess from the command line
How to control access from the command line
How to control internal messages from the command line
How to control login from the command line
How to control external messages from the command line
How to control external messages from the command line
How to control groupaccess from the command line
How to control internal messages from the command line
How to control File Transit Policy from the command line

How to control applications from the command line
How to control access from the command line
How to control login from the command line

Welcome EXT Policy

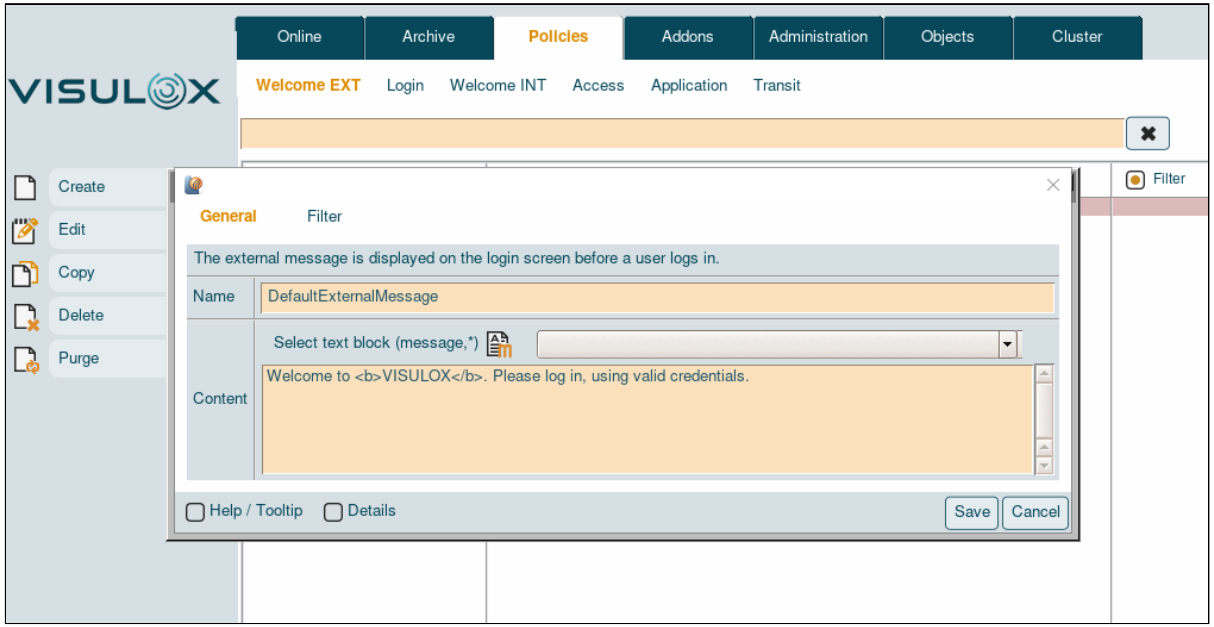
About

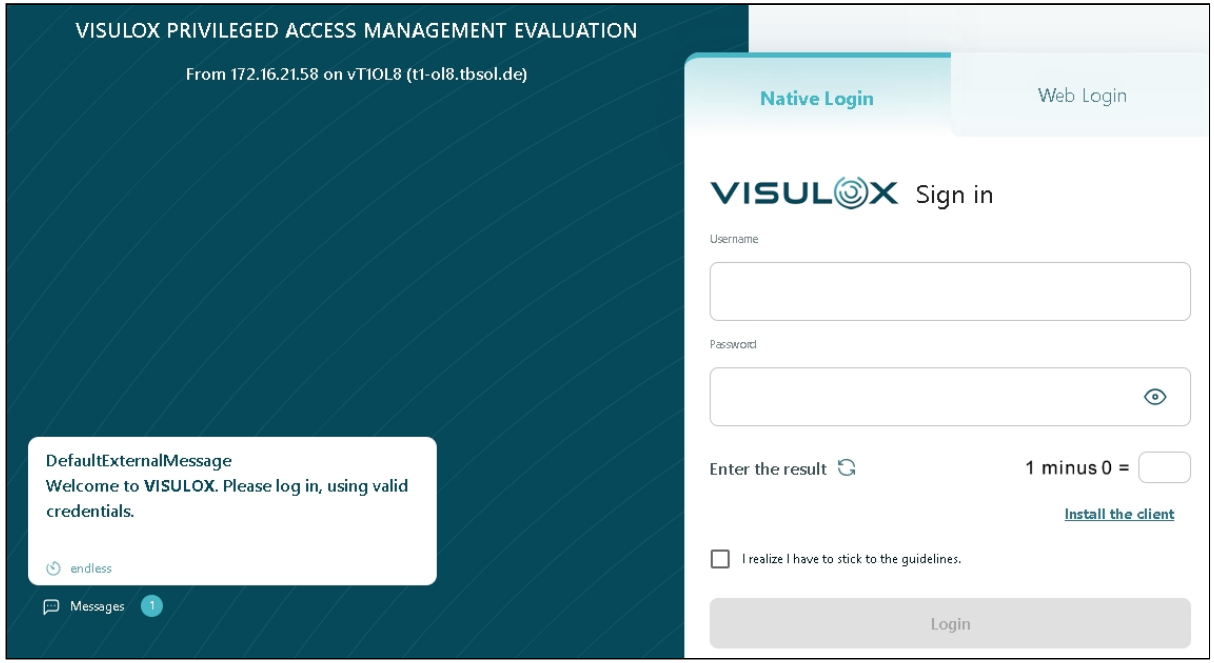
Based on the Access Point it is possible to display a message on the login page.

This piece of information has a time interval, from when and how long the information will be presented to the user before login.
To display the message a some HTML tags and placeholders are allowed.

The text can be entered manually or chosen from a text catalog (see also: Messages in VISULOX).

- About
- Definition
- Presentation
- Allowed tags in messages
- Allowed placeholders in messages
- Configuration

Definition	 Online Archive Policies Addons Administration Objects Cluster VISULOX Welcome EXT Login Welcome INT Access Application Transit Create Edit Copy Delete Purge Filter General Filter The external message is displayed on the login screen before a user logs in. Name DefaultExternalMessage Select text block (message,*) Content Welcome to VISULOX. Please log in, using valid credentials. Help / Tooltip Details Save Cancel

Presentation	

Allowed tags in messages

Modes	Tag
bold	text
center	text

Modes	Tag
italic	text
line break	
horizontal line	<hr>
link	link text (Be careful: only one link per line!)

Allowed placeholders in messages

%OWNER%	%HOST%	%NODE%	%GWIP%	%SYSTEMID%
%OWNERID%	%HOSTSHORT%	%RIP%	%GWIPLAST%	%LICENSE%
%OWNERSHORT%	%HOSTIP%	%AP%	%GWHOST%	%CUSTOMER%
%FULLNAME%	%HOSTIPLAST%	%APNODE%	%GWNODE%	

Configuration

The minimum words and the maximum length of the message can be set via a configuration parameter.

Minimum words of Welcome EXT message

```
visulox config list -name  entry.minwords.external_message_policy

    ------------------------------------------------------------
    | parameter                          |      type | value |
    ------------------------------------------------------------
    | entry.minwords.external_message_policy | OPERATION | 1     |
```

Maximum length of Welcome EXT message

```
visulox config list -name entry.maxlength.external_message_policy

    ---------------------------------------------------------------
    | parameter                           |      type | value   |
    ---------------------------------------------------------------
    | entry.maxlength.external_message_policy | OPERATION | default |
    ---------------------------------------------------------------
```

If **default** is set, the default value will be used for the message. These default values can also be adjusted:

⚠ All configuration parameters set to **default** will also have the new values after these settings are changed.

```
visulox config list -name entry.minwords.default

    ------------------------------------------
    | parameter              |      type | value |
    ------------------------------------------
    | entry.minwords.default | OPERATION | 0     |
    ------------------------------------------
```

```
visulox config list -name entry.maxlength.default

    ------------------------------------------------
    | parameter               |      type | value |
    ------------------------------------------------
    | entry.maxlength.default | OPERATION | 255   |
    ------------------------------------------------
```

All external login messages can be disabled with:

```
visulox config -name design.ui4.loginmessages=false
```

How to control external messages from the command line

Overview The command line tool "**VISULOX policy external**" allows to control external messages (Welcome EXT).	• Overview • Usage • Welcome EXT elements (edit) • Examples

Usage

The following subcommands are available:

Command	Description
list	List and print external welcome messages.
add	Add an external welcome message.
edit	Modify fields of an external welcome message.
delete	Remove an external welcome message.
purge	Remove outdated entries. Can be used via cron-job.

Welcome EXT elements (edit)

Element	Description
-name <>	Name of Policy or use AUTO <>.
-starttime <>	Starttime of the message: now or timestring. Default value: now.
-endtime <>	Endtime of the message: endless or timestring. Default value: endless.
-accesspoint <>	Policy filter: Access Point <>

Element	Description
-content <>	Content of the policy. Default value: CLI.
-grant <>	Set granted user in database record <>

Examples

List current available Welcome EXT policies

```
visulox policy external list
    --------------------------
    |              basicname |
    --------------------------
    | DefaultExternalMessage |
    --------------------------
```

Add new Welcome EXT policy

```
visulox policy external add -name MSG1 -content Server maintenance today
```

Edit policy

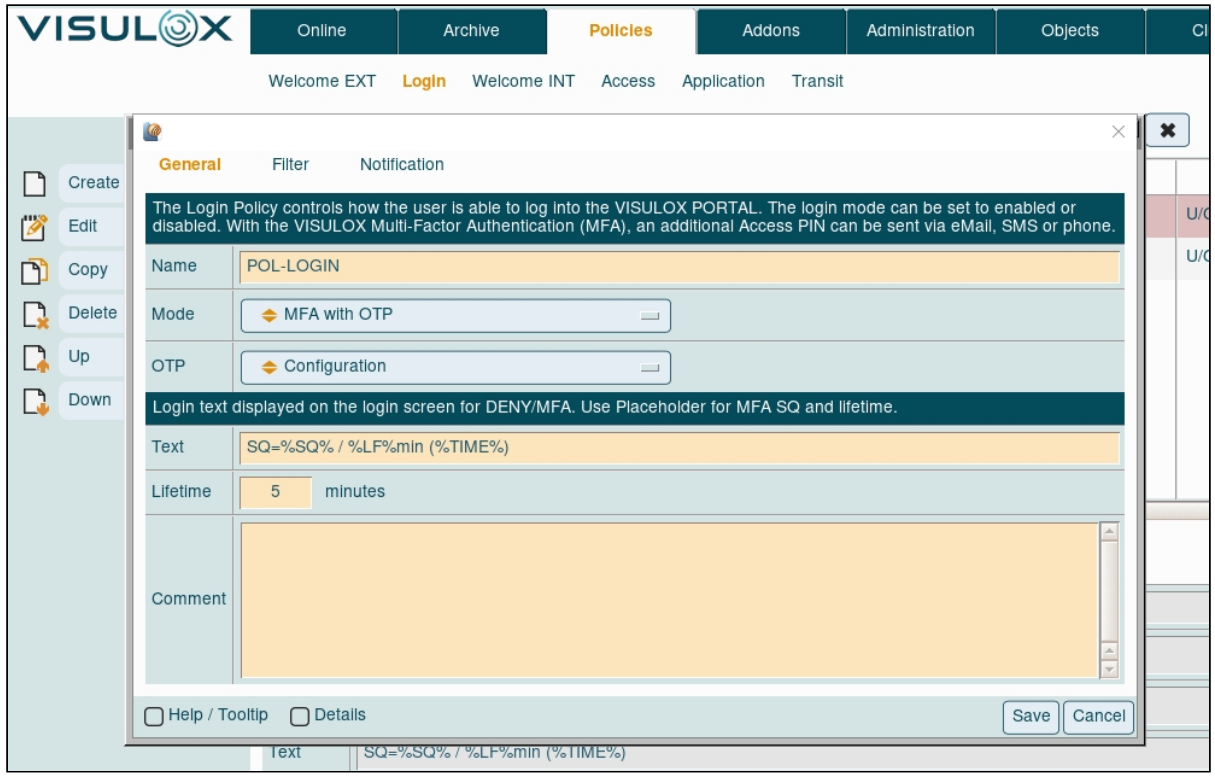
```
visulox policy external edit -name LOG1 -accesspoint test1.domain
```

Remove an entry

```
visulox policy external delete -name LOG1
```

Login Policy

General



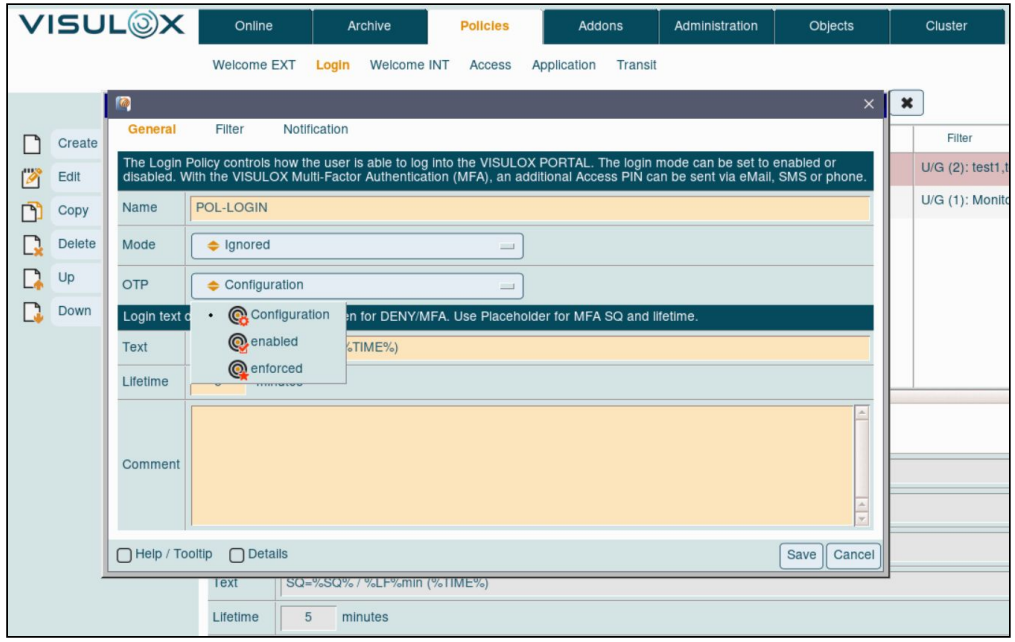
Mode

A Login Policy starts with a primary policy tag, which sets the behaviour of the policy:

Primary policy tags	Description
Ignored	Ignore this policy.
Denied	The matching user cannot use this access point.
Std Login with user name / password	The matching user can use this access point and his Workspace is started.
MFA via external Service	The matching user can use One Time Password authentication. The access code is generated via an external service.
MFA Login with OTP	The matching user can use One Time Password authentication. The access code is generated via the OTP App.
MFA Login needs verbal PIN	The matching user can use this access point. He has to request the access token verbally.
MFA Login with PIN provided via SMS	The matching user can use this access point. The access token is sent via SMS/text message.
MFA Login with PIN provided via eMail	The matching user can use this access point.The access token is sent via eMail.
MFA Login with PIN provided via eMail and/or SMS	The matching user can use this access point.The access token is sent via eMail and /or SMS
MFA Login with OTP or PIN provided via eMail and/or SMS	The matching user can use this access point.The access token is provided via OTP or PIN sent via eMail and /or SMS

MFA = Multi Factor Authentication | **OTP** = One Time Password

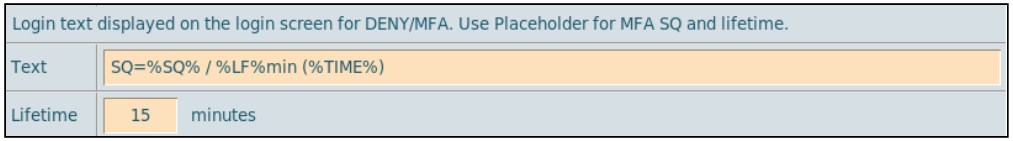
In case of an OTP Login Policy, the setup type can be chosen: Configuration, enabled or enforced:



With OTP setup type configured via Login Policy it is possible to use OTP login for selected groups / users.
Setting the OTP type via configuration parameters will be applied to all users.

PIN message definition and lifetime

Depending of the primary policy tag (DENY / MFA), the message lifetime for the PIN must be configured.



The message, that is presented to the user in the login dialog.

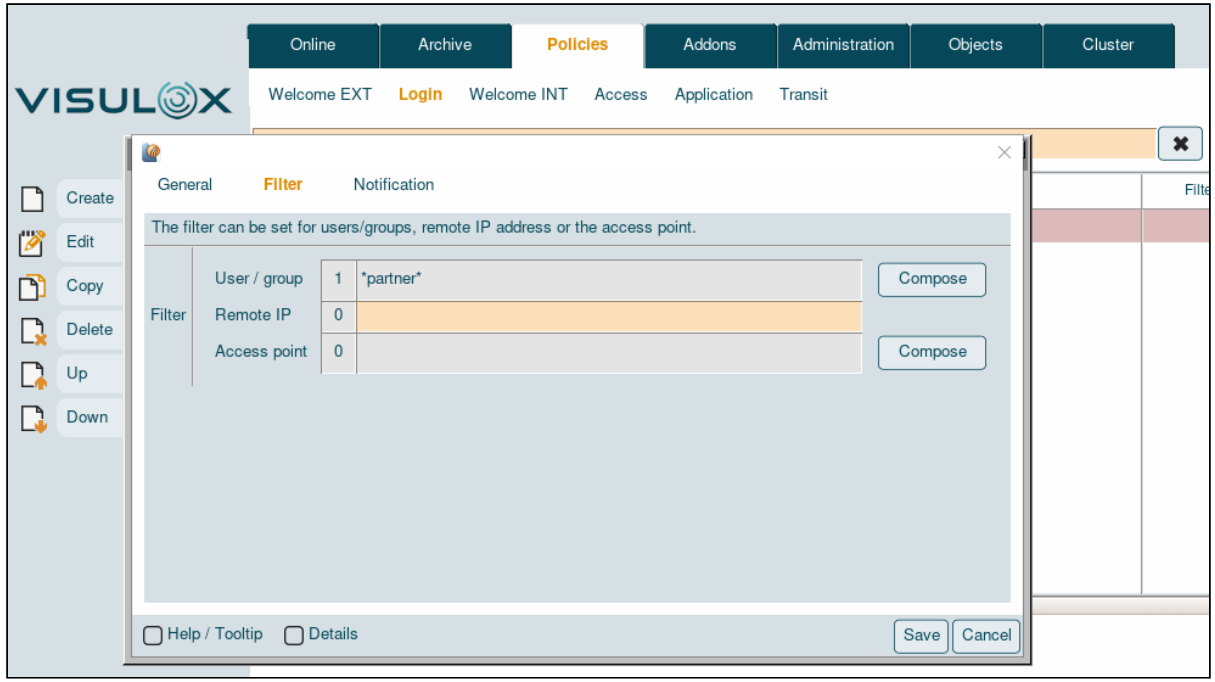
The lifetime of the access PIN.

The message has the following place holders:

#SQ#	Sequence number of the access PIN
#TIME#	The lifetime, until the access PIN gets invalid in a date format
#LF#	The lifetime in minutes, when the access PIN gets invalid

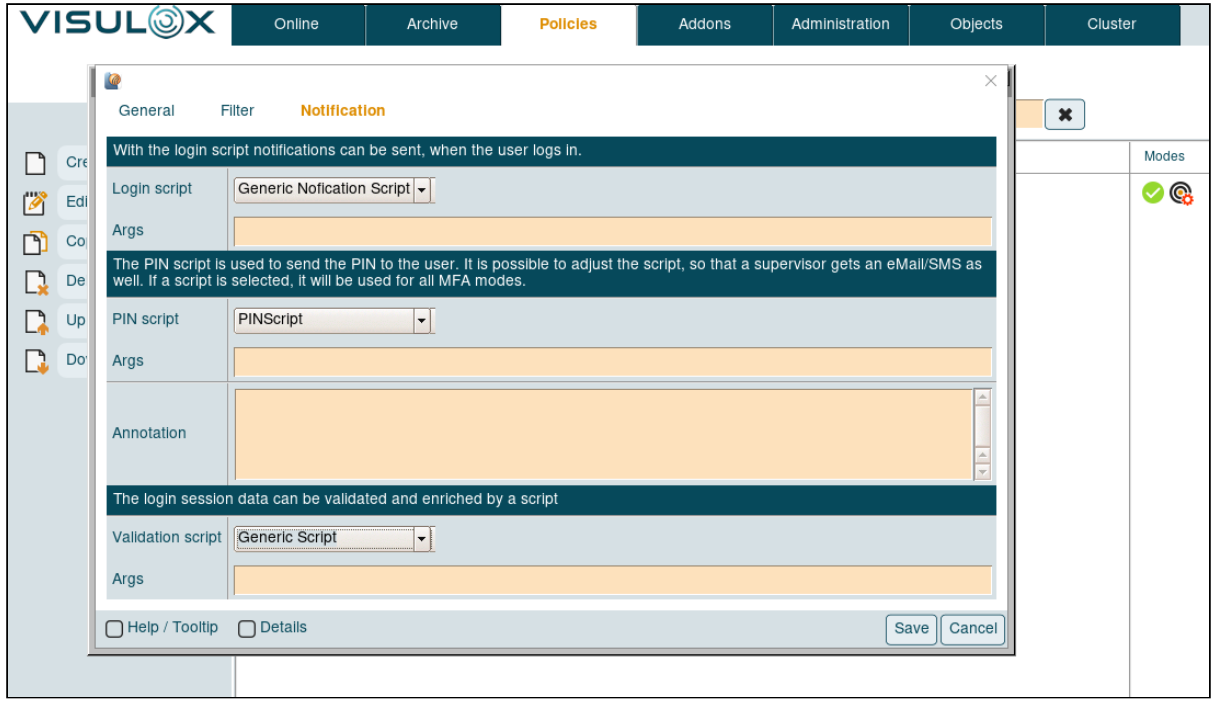
Filter

The Login Policy filter applies on a user / group the user belongs to, the remote IP of the user's connection and / or the access point, where the user wants to login.



Notification

In a Login Policy also three scripts can be defined:



A login script which is triggered after a successful login.

A script to provide the access PIN via eMail or SMS. For these scripts also a text can be entered.
The text can have several place holders (see: Variables in notifications), like the username, etc.

The login session data can be validated and enriched by a validation script.

Arguments for each script can be entered in the according **Args** field.
Depending on the underlying script, the format of the arguments can be: **-arg -arg1 -arg2 <>**

How to control login from the command line

Overview

The command line tool "**VISULOX policy login**" allows to control the Login Policy.

- Overview
- Usage
- Login Policy elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print Login Policies.
add	Add a new Login Policy.
edit	Modify fields of a Login Policy.
delete	Remove a Login Policy.
fields	List available fields in the database (**-raw** = enhanced output)

Element	Description
-name <>	Name of Policy or use AUTO <>.
-mode <>	Mode of login: off, reject, allow, otp, verbal, sms, email, both. Default value: allow
-optmode <>	Mode of OTP: config, enabled, enforced. Default value: config
-object <>	Policy filter: mask or unique distinguished object of user or group <>
-remoteip <>	Policy filter: remote IP or remote IP mask <>
-accesspoint <>	Policy filter: Access Point <>
-script <>	Trigger script. Usage: -script "<script-name>**:** args". Example with arguments: -script "Dump**:** -arg arg -arg1 <>"
-validationscript <>	Ticket script for extended Login <>
-pinscript <>	PIN script <>

Element	Description
-pinscripttext <>	Text provided to PIN script <>
-pintext <>	PIN welcome text in login dialog <>
-lifetime <>	PIN lifetime in minutes. Default value: 15
-comment <>	Comment for policy. Default value: CLI.
-grant <>	Set granted user in database record <>

Examples

List current available Login Policies

```
visulox policy login list
    ---------------------------------
    |    basicname |     policymode |
    ---------------------------------
    | DefaultLogin | allowlogin.map |
    ---------------------------------
```

List available fields

```
visulox policy login fields
```

Display selected fields

```
visulox policy login list -fields basicname,pin_script,login_script
```

Allow login for user Miller

```
visulox policy login add -mode allow -name LOG1 -object Miller
```

Edit policy

```
visulox policy login edit -name LOG1 -remoteip 172.192.15.123
```

Remove an entry

```
visulox policy login delete -name LOG1
```

Welcome INT

About

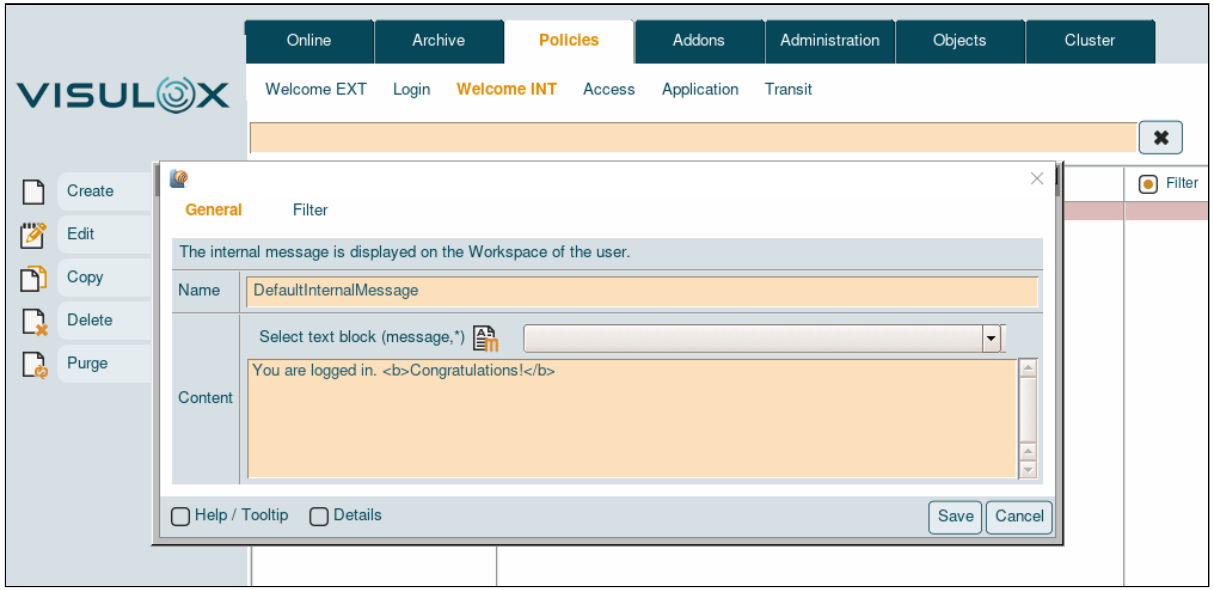
Based on the user / group and/or the Access Point it is possible to display a message on the welcome page.

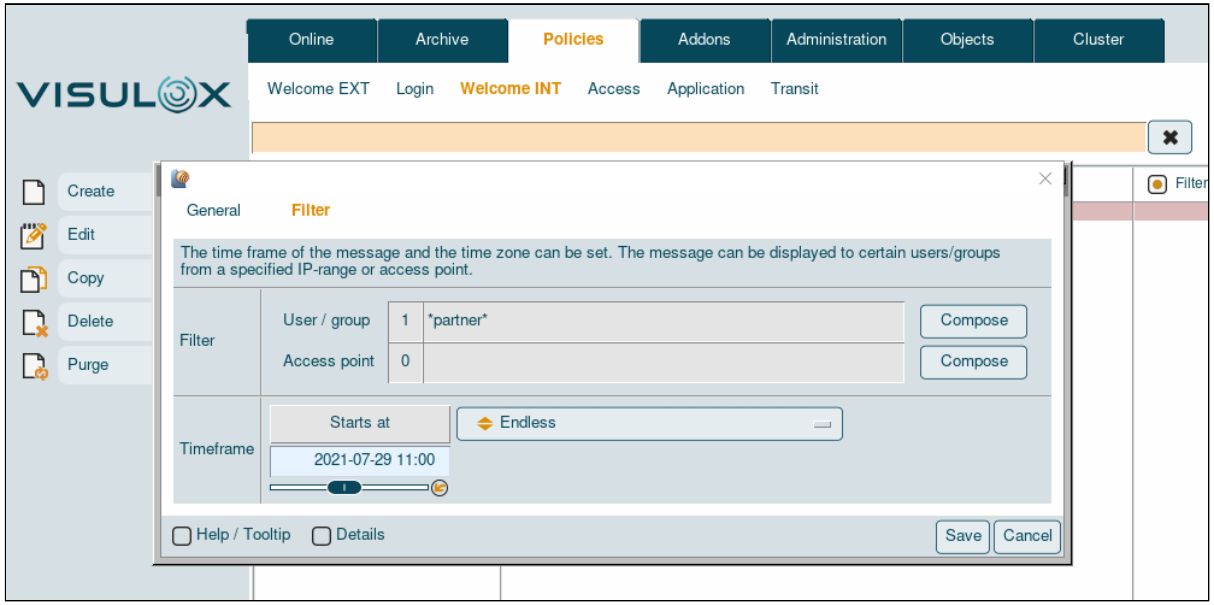
This piece of information has a time interval, from when and how long the information will be presented to the user on his Workspace. To present the message some HTML tags and placeholders are allowed.

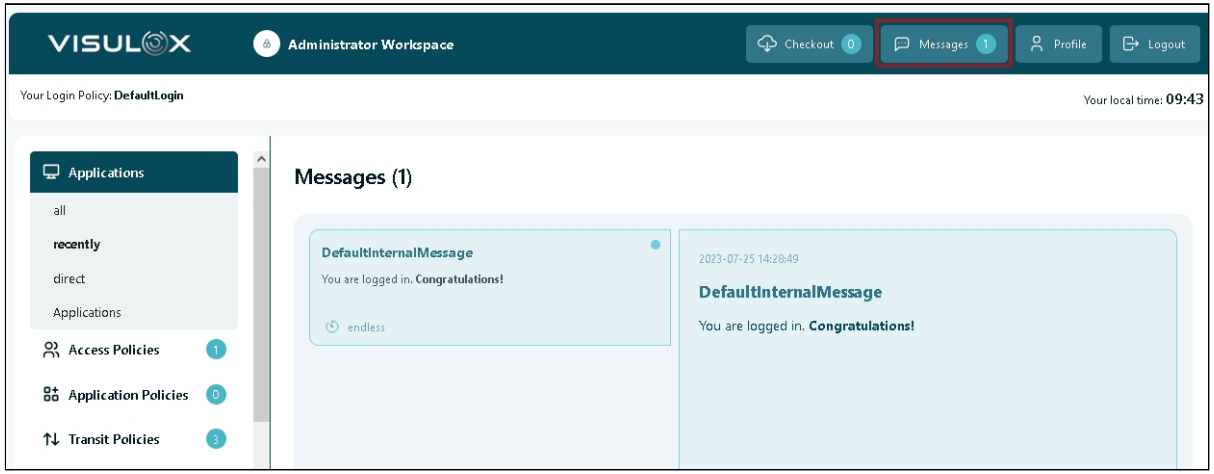
The text can be entered manually or chosen from a text catalog (see also: Messages in VISULOX v3.3).

- About
- Definition
- Presentation
- Allowed tags in messages
- Allowed placeholders in messages
- Configuration

Definition


Online
Archive
Policies
Addons
Administration
Objects
Cluster
VISULOX
Welcome EXT
Login
Welcome INT
Access
Application
Transit
Create
Edit
Copy
Delete
Purge
Filter
General
Filter
The internal message is displayed on the Workspace of the user.
Name
DefaultInternalMessage
Select text block (message,*)
Content
You are logged in. Congratulations!
Help / Tooltip
Details
Save
Cancel


Online
Archive
Policies
Addons
Administration
Objects
Cluster
VISULOX
Welcome EXT
Login
Welcome INT
Access
Application
Transit
Create
Edit
Copy
Delete
Purge
Filter
General
Filter
The time frame of the message and the time zone can be set. The message can be displayed to certain users/groups from a specified IP-range or access point.
Filter
User / group
1
partner
Compose
Access point
0
Compose
Timeframe
Starts at
Endless
2021-07-29 11:00
Help / Tooltip
Details
Save
Cancel

Presentation	

Allowed tags in messages

Modes	Tag
bold	text
center	text
italic	text
line break	
horizontal line	<hr>

Modes	Tag
link	link text (Be careful: only one link per line!)

Allowed placeholders in messages

%OWNER%	%HOST%	%NODE%	%GWIP%	%SYSTEMID%
%OWNERID%	%HOSTSHORT%	%RIP%	%GWIPLAST%	%LICENSE%
%OWNERSHORT%	%HOSTIP%	%AP%	%GWHOST%	%CUSTOMER%
%FULLNAME%	%HOSTIPLAST%	%APNODE%	%GWNODE%	

Configuration

The minimum words and the maximum length of the message can be set via a configuration parameter.

Minimum words of Welcome INT message

```
visulox config list -name  entry.minwords.internal_message_policy

    ------------------------------------------------------------
    | parameter                          |      type | value |
    ------------------------------------------------------------
```

```
    | entry.minwords.internal_message_policy | OPERATION | 1     |
```

Maximum length of Welcome INT message

```
visulox config list -name entry.maxlength.internal_message_policy

    ------------------------------------------------------------------
    | parameter                              |      type | value    |
    ------------------------------------------------------------------
    | entry.maxlength.internal_message_policy | OPERATION | default |
    ------------------------------------------------------------------
```

If **default** is set, the default value will be used for the message. These default values can also be adjusted:

⚠ All configuration parameters set to **default** will also have the new values after these settings are changed.

```
visulox config list -name entry.minwords.default

    ------------------------------------------------
    | parameter              |      type | value |
    ------------------------------------------------
    | entry.minwords.default | OPERATION | 0     |
    ------------------------------------------------

visulox config list -name entry.maxlength.default

    ------------------------------------------------
    | parameter               |      type | value |
    ------------------------------------------------
    | entry.maxlength.default | OPERATION | 255   |
```

```
-----------------------------------------------
```

How to control internal messages from the command line

Overview

The command line tool "**VISULOX policy internal**" allows to control internal messages (Welcome INT).

- Overview
- Usage
- Welcome INT elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print internal welcome messages.
add	Add an internal welcome message.
edit	Modify fields of an internal welcome message.
delete	Remove an internal welcome message.
purge	Remove outdated entries. Can be used via cron-job.

Welcome INT elements (edit)

Element	Description
-name <>	Name of Policy or use AUTO <>.
-starttime <>	Starttime of the message: now or timestring. Default value: now.
-endtime <>	Endtime of the message: endless or timestring. Default value: endless.
-object <>	Policy filter: mask or unique distinguished object of user or group <>
-accesspoint <>	Policy filter: Access Point <>
-content <>	Content of the policy. Default value: CLI.
-grant <>	Set granted user in database record <>

Examples

List current available Welcome INT policies

```
visulox policy internal list
    -------------------------
    |              basicname |
    -------------------------
    | DefaultInternalMessage |
    -------------------------
```

Add new Welcome INT Policy

```
visulox policy internal add -name MSG3 -content Meeting at 10:00
```

Edit policy

```
visulox policy internal edit -name MSG3 -object Miller
```

Remove an entry

```
visulox policy internal delete -name MSG3
```

Access Policy

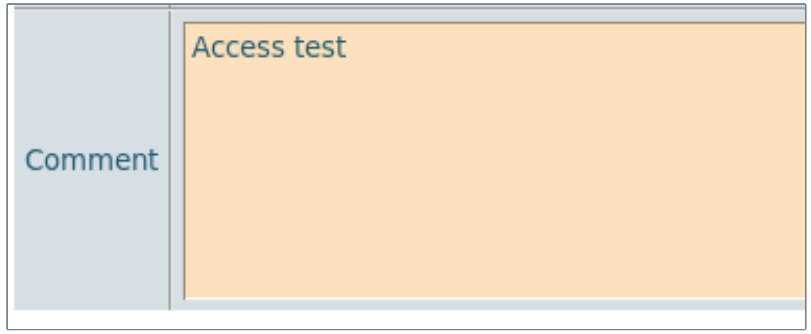
General

An Access Policy starts with a primary policy tag, which sets the behaviour of the policy:

Primary policy tags	Description
Application access is allowed	The matching user can use this access point to start the application.
Application access is denied	The matching user cannot use this access point for starting the application.
Group access	The matching user can access application based on group access
Ignored	Ignore this policy.

A valid Ticket ID for the user can be entered.

A comment for the user can be entered. This text will be shown in the locked window:

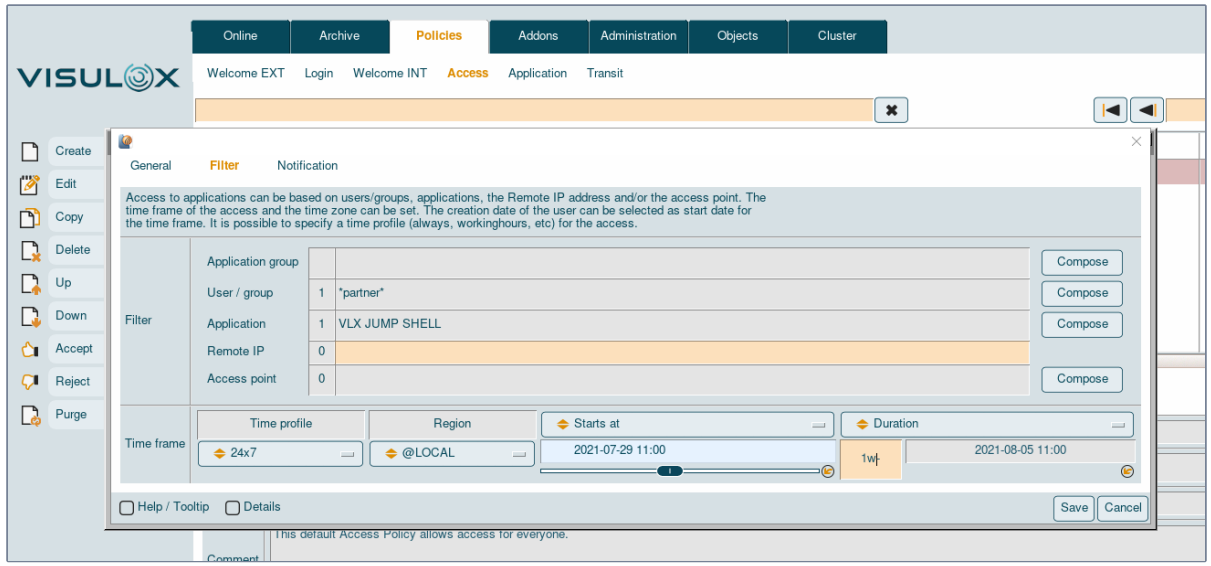


Filter

The Access Policy filter applies on a user / group the user belongs to, an application mask, the remote IP of the user's connection and / or the access point, over which the user logs in.

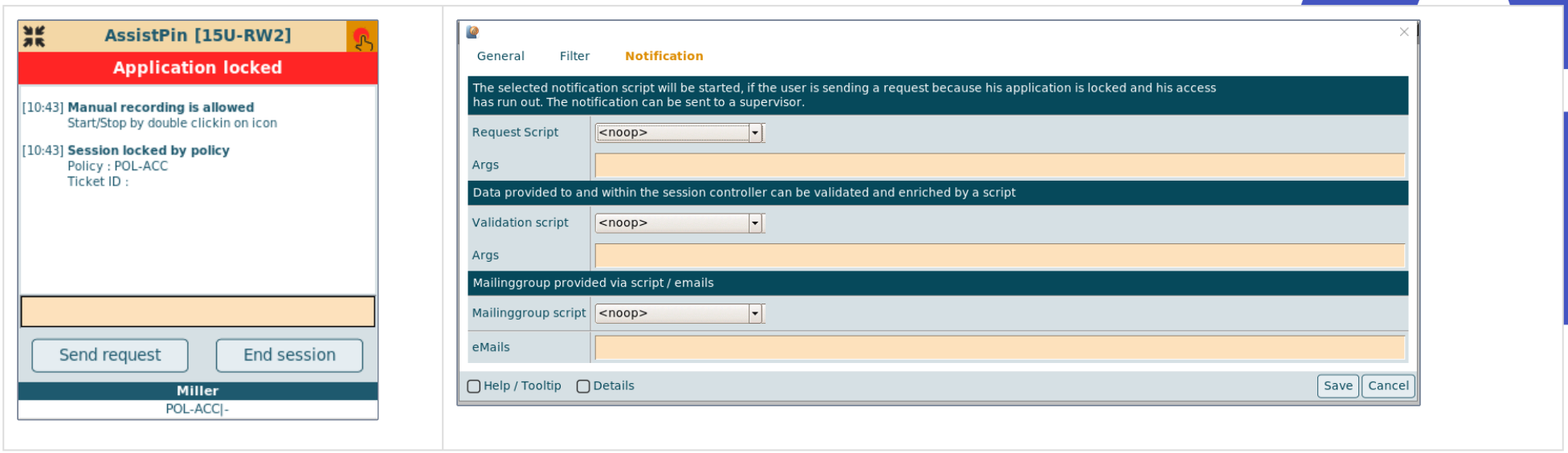
It is possible to choose a time profile and a time zone from a dropdown list of pre-configured entries.

The start and end time of the access can be chosen as well.



Notification

A notification / request script can be selected, that will be triggered, if a user presses the "**Send request**" button, because of a locked application.



This notification is sent to a supervisor / approver.
If a request script is assigned and configured, mails are sent to the requester and the approver, who is able to allow, reject the request via action link in a mail.

Arguments for the Request and Validation script can be entered in the according **Args** field.
Depending on the underlying script, the format of the arguments can be: **-arg -arg1 -arg2 <>**

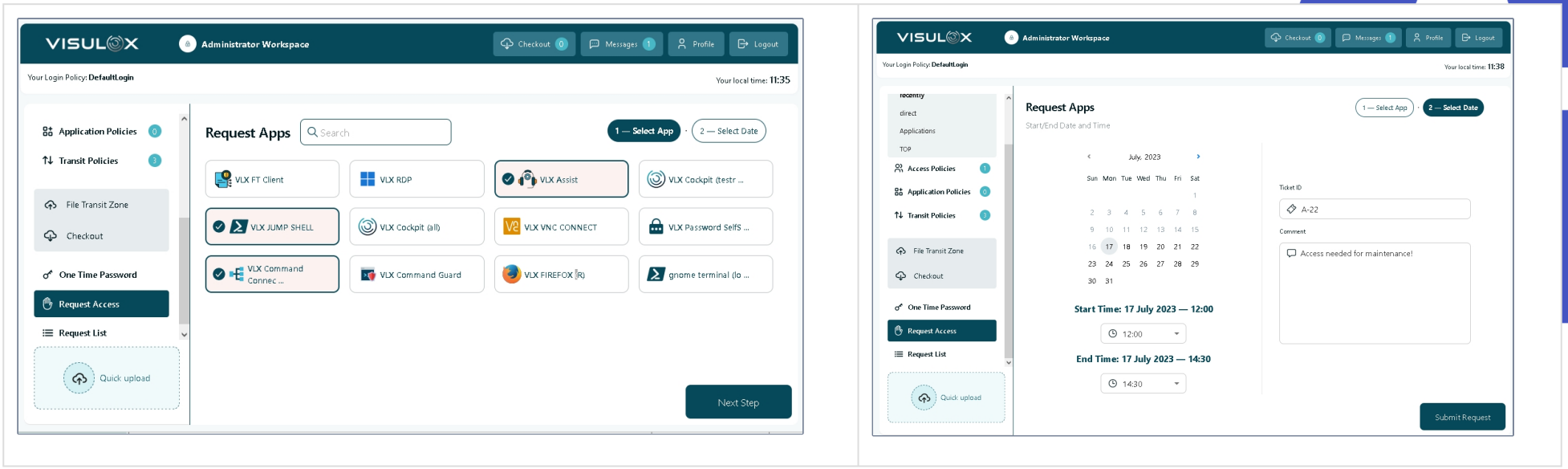
Also a preconfigured mailinggroup can be set via **Mailinggroup script** and/or single email addresses can be set via **eMails**. (See also: Mailinggroups.)

The "**Send request**" button is only displayed in the control panel, if a notification / request script is assigned.

> ⚠ Make sure that the policy is **active** for the user, so the configured script can be triggered.
> A policy where the access time has run out is no longer matching, so another (denied) policy must be created to display the "**Send request**" button.

VISULOX Access Request

Users are able to request access via the **VLX Request** application in their Workspace.



The user can request access for all selected applications. He has to enter a time frame, the ticket ID and a comment. All is checked against the configured ruleset.

The successful submit adds an access request to the Access Policies. This request is ignored and the first applying rule should be "**Deny**".

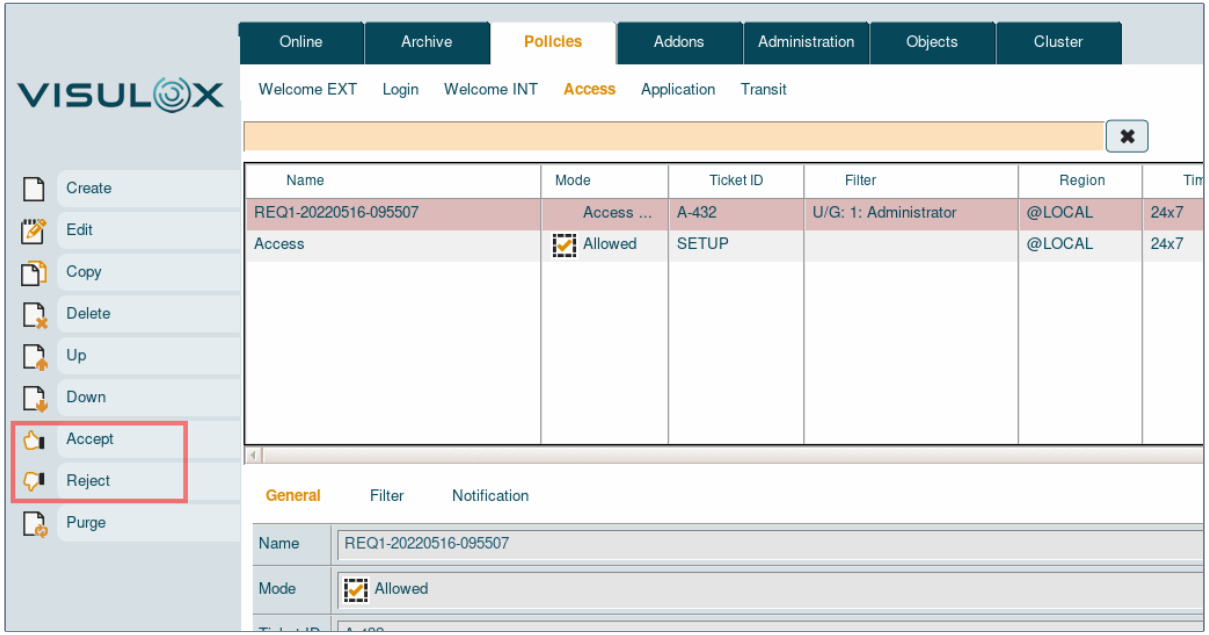
A supervisor can now modify this access request to "**Reject**" or "**Accept**". "**Reject**" is handled as "**Deny**", "**Accept**" as "**Allow**".
This can be done in the Cockpit or via action link in a mail, if a request script is used.

The script and additional parameters can be set with:

```
visulox config -name request.workspace.request=REQUEST

visulox config -name request.workspace.request
    ------------------------------------------------------------------------------------------------------------------------
    | changed | key                                    | value                                                             |
```

```
-------------------------------------------------------------------------------------------------------------------
| changed | request.workspace.request          | REQUEST                                                                |
| changed | request.workspace.request.args     | -info "A comment from the  policy   ...." -approver dev@amitego.com |
| changed | request.workspace.requestlifetime | 60                                                                     |
-------------------------------------------------------------------------------------------------------------------
```

Once an access is requested, a supervisor can see the detailed request in **Cockpit** / **Policies** / **Access Policy**.



The supervisor is able to **accept** or **reject** the access request by selecting the request and using the appropriate buttons.
When request is configured with action links via mail , the mails are sent to the requester and the approver, who is also able to to allow, reject the request via mail.

If the request is accepted, it will be changed into a valid Access Policy.

Handling ticket IDs from external systems

The TicketID is a mandatory field based on configuration coming from an external incident management system.

The format of the ticket ID can be adjusted in VISULOX configuration to meet the requirements of the existing ticket ID of the external management system.

The regular expression can be adjusted for access and spontaneous access:

```
visulox config list -name ticket
    ------------------------------------------------------------
    | changed | parameter                   |      type | value  |
    ------------------------------------------------------------
    |         | entry.ticketid.access       | OPERATION | ^A-.+$ |
    |         | entry.ticketid.spontanaccess | OPERATION | ^A-.+$ |
    ------------------------------------------------------------
```

How to control access from the command line

Overview The command line tool "**VISULOX policy access**" allows to control the Access Policy.	• Overview • Usage • Access Policy elements (edit) • Configuration of ticket ID as a regular expression • Examples

Usage

The following subcommands are available:

Command	Description
list	List and print Access Policies.
fields	List available fields in the database (**-raw** = enhanced output)
add	Add an Access Policy for a user or a group to the top of the Access Policy list. A ticket string is mandatory. The new access policy can be either "allow" or "deny"
edit	Modify fields of an Access Policy. The modification will **not** change the position in the Access Policy.
delete	Remove an Access Policy.
purge	Remove outdated entries. Can be used via cron-job.

Access Policy elements (edit)

Element	Description
-mode <>	Mode of access: allow, deny, request, group, disabled. Default value: allow.
-name <>	Name of policy or use AUTO <> If not defined during **add** within the command line, a name is generated in the form "**BATCH-yyyymmdd-hhmmss**". Compared to the GUI, no field validation is done.

Element	Description
-object <>	Policy filter: mask or unique distinguished object of user or group <> Mandatory in **add, update, remove** to identify a unique object in the datasource table (attached user repositories).
-applicationgroup <>	Policy filter: mask or applicationgroup name or applicationgroup mask <>
-application <>	Policy filter: mask or application name or application mask <>
-remoteip <>	Policy filter: remote IP or remote IP mask <>
-accesspoint <>	Policy filter: Access Point <>
-ticket <>	Assign ticket to this access <> Mandatory. In comparison to the GUI, no field validation is done.
-region <>	Name of region in the database. Default value: @LOCAL.
-timeprofile <>	Name of time profile in the database. Default value: 24x7.
-starttime <>	Start of access: now or timestring. Default value: now.
-endtime <>	End of access: endless or timestring. Default value: endless.
-script <>	Trigger script. Usage: -script "<script-name>**:** args". Example with arguments: -script "Dump**:** -arg arg -arg1 <>"

Element	Description
-mailinggroup	Name of the preconfigured mailinggroup
-mailinggroup_emails	Individual list of email addresses
-comment <>	Comment for policy. Default value: CLI. The comment can have multiple lines. "**\n**" can be used as a line separator.
-grant <>	Set granted user in database record <>

Each usage which changes the Access Policy (**add, update, remove, clean**) is running in "**dry**" mode until **-run** is applied to the command line.

Configuration of ticket ID as a regular expression

It is possible to configure the entry format of the ticket ID as a regular expression:

```
visulox config -name entry.access.ticketid

    ---------------------------------------------
    | parameter             |      type | value  |
    ---------------------------------------------
    | entry.access.ticketid | OPERATION | ^A-.+$ |
    ---------------------------------------------
```

Examples

List current available Access Policies

```
visulox policy access list
    -------------------------------
    | basicname |      policymode |
    -------------------------------
    |    Access | allowaccess.map |
    -------------------------------
```

List available fields

```
visulox policy access fields
```

Display selected fields

```
visulox policy access list -fields basicname,policymode,acc_script
```

Grant access for Miller - 1 month from now

```
visulox policy access add -name ACC1 -mode allow -object miller.si@t-online.de -ticket "TK-097612" -endtime "+ 1 month" -run
```

Deny access for every user who belongs to group CN=EXTERNAL-STAFF

```
visulox policy access add -mode deny -name ACC2 -object CN=EXTENAL -ticket "TK-1234" -endtime endless -run
```

Assign a new object to APP1

```
visulox policy access edit -name ACC1 -object cn=partner -run
```

Extend access for Miller

```
./visulox policy access edit -name ACC1 -endtime "+ 1 year" \
   -comment "Miller can have access for one year from now.\nHe is a trustfully guy." -run
```

Remove an entry

```
visulox policy access delete -name ACC1 -run
```

Disabling the "**Send request**" button for users:

```
visulox config -name scx.button.request=false -force
```

How to control groupaccess from the command line

Overview

The command line tool "**VISULOX policy groupaccess**" allows to control groupaccess.

- Overview
- Usage
- Access Policy elements (edit)
- Configuration of ticket ID as a regular expression
- Examples

Usage

The following subcommands are available:

list	List and print Group Access Policies.
fields	List available fields in the database (**-raw** = enhanced output)
add	Add a Group Access Policy.
edit	Modify fields of a Group Access Policy.
reset	Reset a Group Access Policy.
purge	Remove outdated entries. Can be used via cron-job.

Group Access Policy elements (edit)

-mode <>	Mode of access
-name <>	Name of policy or use AUTO <>
-object <>	Policy filter: mask or unique distinguished object of user or group <> Mandatory in **add, update, reset** to identify a unique object in the datasource table (attached user repositories).
-application <>	Policy filter: mask or application name or application mask <>
-ticket <>	Assign ticket to this access <>
-region <>	Name of region in the database. Default value: @LOCAL.
-timeprofile <>	Name of time profile in the database. Default value: 24x7.
-starttime <>	Start of access: now or timestring. Default value: now.
-endtime <>	End of access: endless or timestring. Default value: endless.
-comment <>	Comment for policy. Default value: CLI. The comment can have multiple lines. "**\n**" can be used as a line separator.

-grant <>	Set granted user in database record <>

Configuration of ticket ID as a regular expression

It is possible to configure the entry format of the ticket ID as a regular expression:

```
visulox config -name entry.access.ticketid

    ------------------------------------------------
    | parameter             |      type | value  |
    ------------------------------------------------
    | entry.access.ticketid | OPERATION | ^A-.+$ |
    ------------------------------------------------
```

Examples

List current available Group Access Policies

```
visulox policy groupaccess list
    ------------------------------------------------------
    | basicname |    ticketid | starttime | endtime |
    ------------------------------------------------------
    | ...
```

List members of Group Access Policy

```
 visulox policy groupaccess list -name <name>
```

List available fields

```
visulox policy groupaccess fields
```

Display selected fields

```
visulox policy groupaccess list -fields basicname,endtime,timeprofile
```

How to control OTP from the command line

Overview

The command line tool "**VISULOX otp**" allows to control the access via One Time Password.

- Overview
- Usage
- One Time Password elements
- Examples

Usage

The following subcommands are available:

Command	Description
key	Create a One Time Password key
set	Assign the key to users. Validate with current OTP token (-otp).
reset	Reset One Time Password of the user
check	Check OTP Config of user and check OTP token

One Time Password elements

Element	Description
-object <>	One Time Password user
-key	Creates a One Time Password key
-otp <>	The current token for the One Time Password key
-grant <>	Username. Default is <CLI>

With these commands and elements it is possible to create user OTP profiles with the same key for different users. For example if a group of users have the same OTP device / webpage.

Examples

Create OTP key

```
visulox otp key
44I6ZJ25DMWD2GIO
```

Assign the key to a user

```
visulox otp set -object <user> -key <otp key> -otp <current otp token>
```

Check if user has an OTP and if the OTP token is correct

```
visulox otp check -object <user> -otp <current otp token>
```

Reset OTP of a user

```
visulox otp reset -object <user>
```

Application Policy

The following features are controlled with an Application Policy: Notification, Recording, , Dual Control, Detection control and Keyword detection:

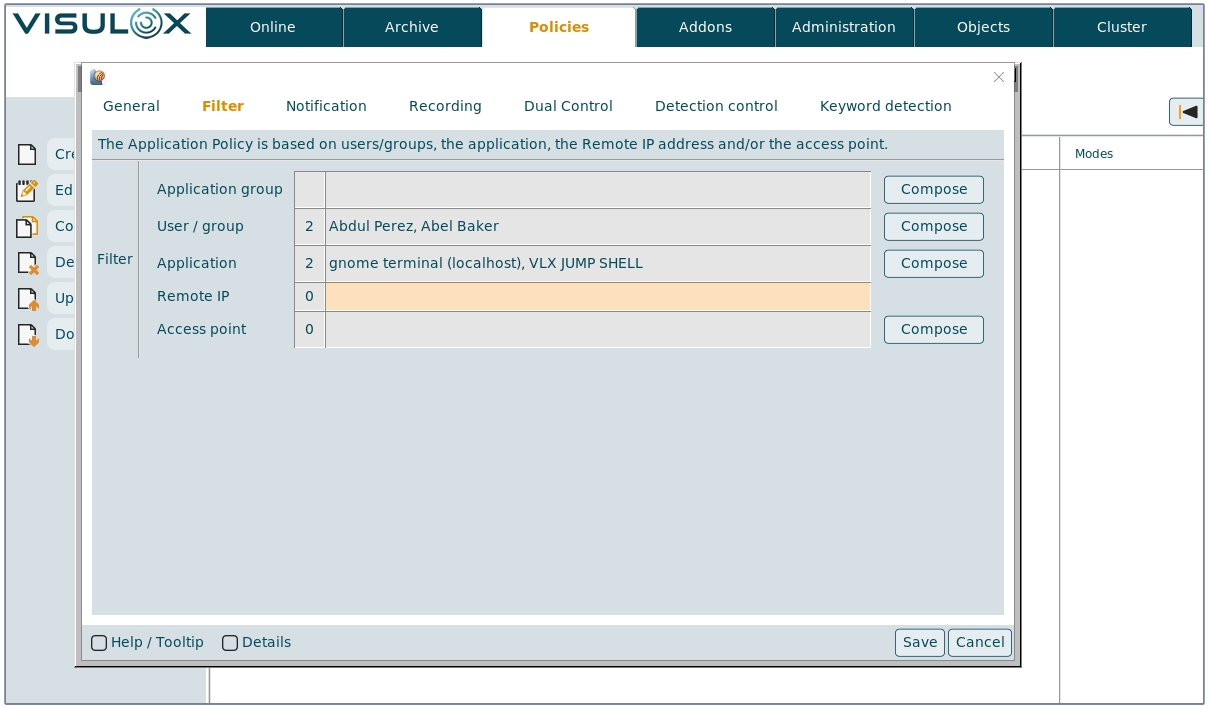
General

An Application Policy starts with a primary policy tag, which sets the behaviour of the policy:

Primary policy tags	Description
Ignored	Ignore this policy.
Enabled	The policy is active for the matching users.

Filter

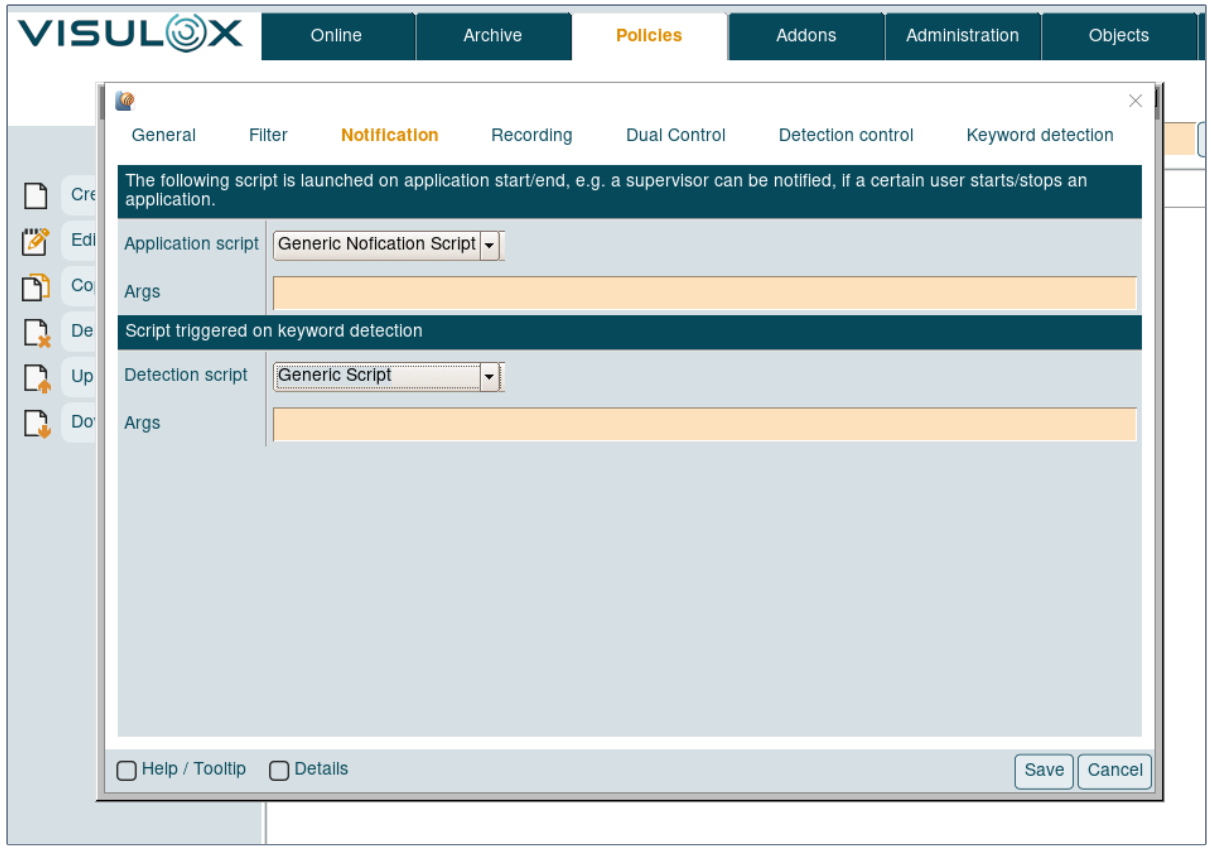
The Application Policy filter applies on a user / group the user belongs to, an application / application group, the remote IP of the user's connection and / or the access point, where the user wants to login.



Notification

A notification can be sent, when an application is started or stopped.

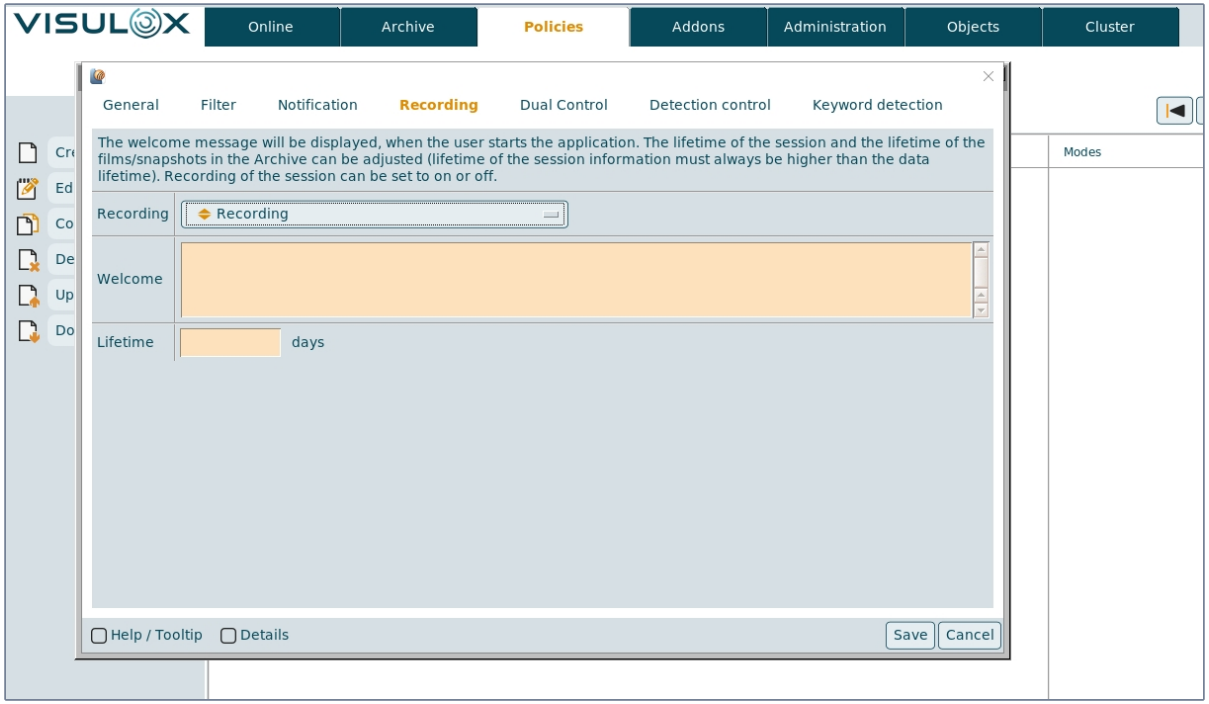
The script that will be started, when a keyword is detected can be set as well.



Arguments for the Application and Detection script can be entered in the according **Args** field.
Depending on the underlying script, the format of the arguments can be: **-arg -arg1 -arg2 <>**

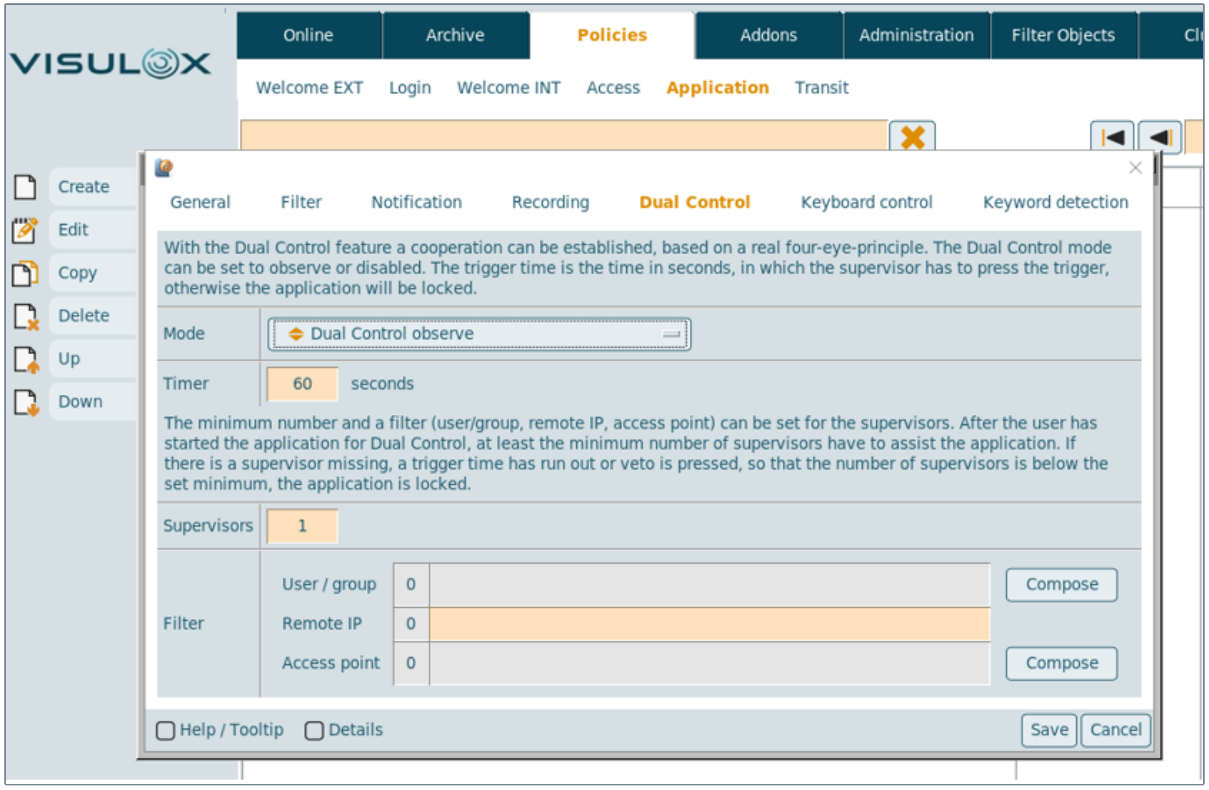
Recording

Recording can be set to "**Recording**" or "**Recording off**" and a welcome message, that will be displayed in the recorder box can be entered. The session information lifetime is set in days.



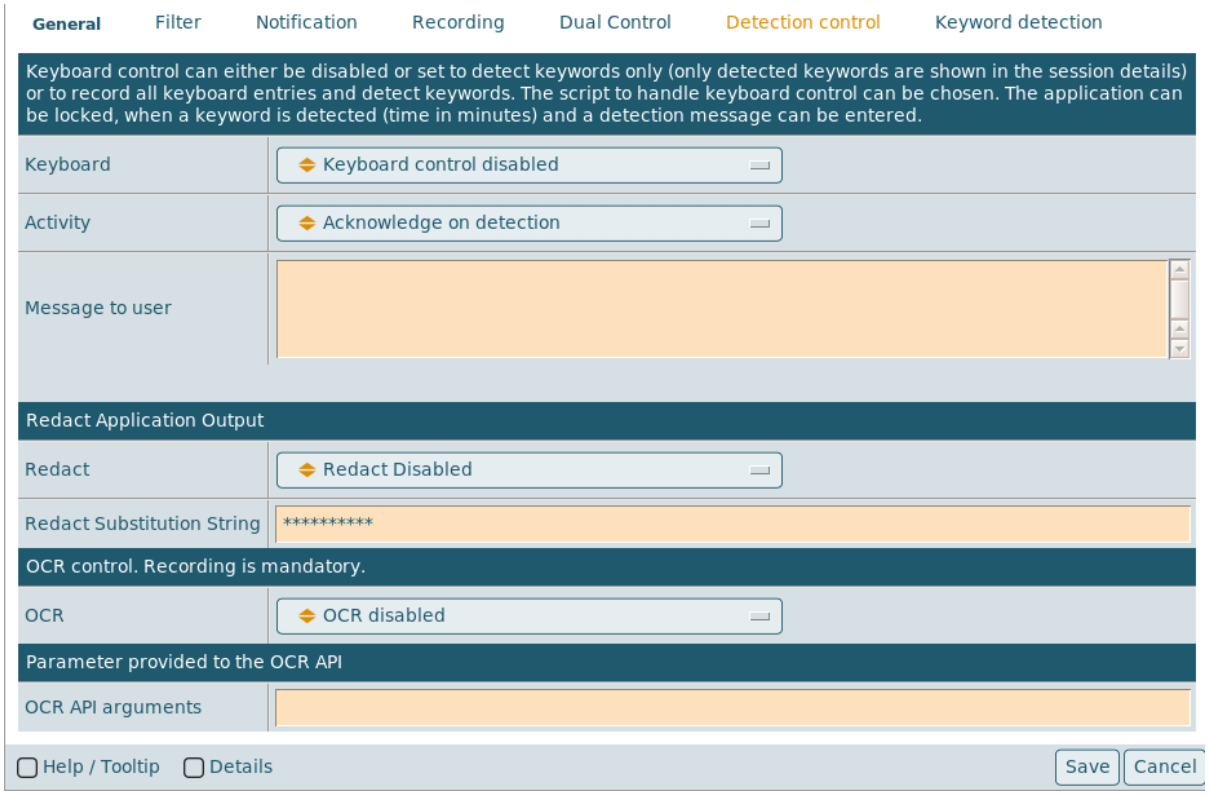
Dual Control

Primary policy tags	Description
Dual Control disabled	Dual Control will not be activated.
Dual Control observe	The supervisor is able to see the application and has a mouse pointer with his name, but can not interact.
Dual control observe and assist	The supervisor is able to see the application and has a mouse pointer with his name, but can not interact. An additional user can join the cooperation in assist observe mode.



The Dual Control timer is set in seconds. If the supervisor does not press the trigger and the timer has run out, the session is locked. The minimum number of controllers that are needed to unlock the application and the filter for the cooperation partner, who will be able to unlock the session for the user can be set based on the user / group, the remote IP address and / or the access point.

Detection control



Keyboard control mode:

Primary policy tags	Description
Keyboard control disabled	Keyboard control will not be activated.
Detect keywords only	Only keywords are detected, other keystrokes are not displayed in the Cockpit.
Record input and detect keywords	Keywords are detected, all keystrokes are recorded and can be displayed in the Cockpit.

Activity

Primary policy tags	Description
Keyword detection muted	No message or lock for the user, but detected keywords are shown in Cockpit events.
Acknowledge on detection	Screen is locked, the user has to acknowledge the "Keyword detected" box to continue working.
Lock on detection	Screen is locked, the user is able to send a request to the supervisor, screen is locked until the supervisor unlocks via Cockpit.

Redact

Similar to the keyboard recording detection it is possible to monitor and redact the input /output streams of a Command Connect session.
Using an Application Policy with keyboard recording enabled and a keyword that should trigger an event. A connection via Command Connect to a server and opening a file e.g. with cat, that contains the keyword, an event is triggered.

Primary policy tags	Description
Redact	Change mode to: Redact disabled, Redact on, Redact & close, Detect only
Redact substitution string	String for the redaction

Available event stream parameters for redact mode:

```
visulox config -name redact
    ------------------------------------------------------------------------------------------
    | changed | key                                                | value                     |
    ------------------------------------------------------------------------------------------
    |         | commandconnect.event.redact                        | default                   |
    |         | commandconnect.event.redactinfo                    | Redact %POLICY% %RMC%: %RMI%  |
    |         | guidefaults.global_application_policy.redactmode   | redactOff.map             |
    |         | guidefaults.global_application_policy.redactstring | **********                |
    ------------------------------------------------------------------------------------------
```

In the keyword detection process a script can be inserted to lock a user permanently after entering a keyword.
See: How to lock a user permanently for using an application after keyword detection

For **Acknowledge on detection** the **Detection script** has to be set on the Notification tab.

OCR control mode

⚠ Recording is mandatory for OCR

Primary policy tags	Description
OCR disabled	OCR control will not be activated.
OCR keyword detection	Only keywords are detected, other keystrokes are not displayed in the Cockpit.
OCR recording and detect keywords	Keywords are detected, OCR is recorded and can be displayed in the Cockpit.
OCR keyword detection asynchronously	Only keywords are detected asynchronously, other keystrokes are not displayed in the Cockpit.
OCR recording and detect keywords asynchronously	Keywords are detected asynchronously, OCR is recorded and can be displayed in the Cockpit.

OCR parameter

Additional arguments can be provided to the OCR API.

Parameter provided to the OCR API	
OCR API arguments	

OCR configuration parameters

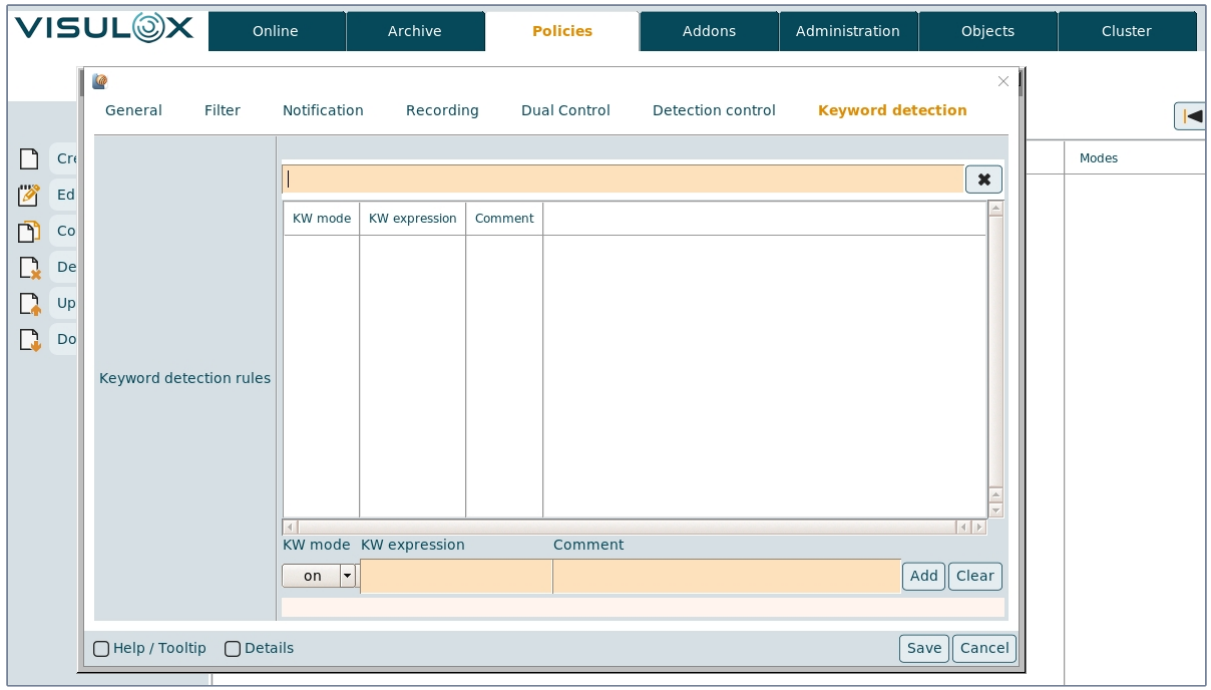
```
visulox config -name ocr
    ------------------------------------------------------------------------------------------------------
    | changed | key                                                | value                                 |
    ------------------------------------------------------------------------------------------------------
    |         | guidefaults.global_application_policy.ocr_enabled | disabled.map                          |
    |         | ocr.arguments                                      | --oem 1 --psm 11                      |
    |         | ocr.async.clients                                  | 5                                     |
    | changed | ocr.async.interval                                 | 20                                    |
    |         | ocr.async.worker                                   | 5                                     |
    |         | ocr.interval                                       | 120                                   |
    |         | ocr.length                                         | 3                                     |
    |         | ocr.pattern                                        | ^[0-9:,.]+$|^Estimating resolution as |
    |         | ocr.risk.expression                                | (%D% / %W%) * 100                     |
    |         | ocr.risk.watermark                                 | 10                                    |
    |         | ocr.statistic                                      | false                                 |
    |         | ocr.summery                                        | false                                 |
    ------------------------------------------------------------------------------------------------------
```

The underlying OCR script (ocr.sh.template) can be found in **/opt/visulox/tools/**.

The script has to be adjusted and renamed to **ocr.sh**.

In idle sessions OCR is stopped to keep the size small.

Keyword detection



The KW mode for the keyword detection must be selected: "**on**" or "**ignored**". A keyword detection comment for the keyword can be entered and the regexpression of the keyword has to be defined, e.g. "**y\badword\y**"

How to control applications from the command line

Overview

The command line tool "**VISULOX policy application**" allows to control the Application Policy.

- Overview
- Usage
- Application Policy elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print Application Policies.
add	Add an Application Policy.
edit	Modify fields of an Application Policy.
delete	Remove an Application Policy.
fields	List available fields in the database (**-raw** = enhanced output)

Element	Description
-name <>	Name of policy or use AUTO
-mode <>	Policy on or off. Default value: on.
-object <>	Policy filter: mask or unique distinguished object of user or group <>
-applicationgroup <>	Policy filter: mask or applicationgroup name or applicationgroup mask <>
-application <>	Policy filter: mask or application name or application mask <>
-remoteip <>	Policy filter: remote IP or remote IP mask <>
-accesspoint <>	Policy filter: Access Point <>
-script <>	Trigger script. Usage: -script "<script-name>**:** args". Example with arguments: -script "Dump**:** -arg arg -arg1 <>"
-recording <>	Mandatory. In comparison to the GUI no field validation is done.
-lifetime <>	Lifetime of recorder data <>
-welcome <>	Recording welcome message <>

Element	Description
-ksmode <>	KW mode: off / detect / record. Default value: off
-ksscript <>	Trigger script on detection <>
-ksaction <>	Action on detection: mute / info / lock. Default value: mute
-ksmessage <>	Message to user on detection <>
-ksrules <>	File with keystroke rules <> **Template for a ksrules file** ksmode= on ksexpr=\ybadcommand\y|\ybadword\y comment=This is badcommand or badword
-ocrmode <>	OCR mode off / detect / record. Default value: off.
-ocrargs <>	OCR API arguments <>
-dcmode <>	Dual Control on or off. Default value: off.
-dcmembers <>	Dual Control members. Default value: 1.
-dctimer <>	Dual Control timer. Default value: 30.

Element	Description
-dcobject <>	Dual Control filter: mask or unique distinguished object of user or group <>
-dcremoteip <>	Dual Control filter: mask or remote IP or remote IP mask <>
-dcaccesspoint <>	Dual Control filter: Access Point <>
-comment <>	Comment for the policy. Default value: CLI.
-grant <>	Set granted user in database record <>

Examples

List current available Application Policies

```
visulox policy application list
    --------------------------
    | basicname | policymode |
    --------------------------
    |      APP1 | active.map |
    --------------------------
```

List available fields

```
visulox policy application fields
```

List selected fields

```
visulox policy application list -fields basicname,policymode,app_script
```

Add new Application Policy

```
visulox policy application add -name APP1 -application "xterm\,xclock" -recording on
```

Edit Application Policy

```
visulox policy application edit -name APP1 -lifetime 3
```

Edit Application Policy

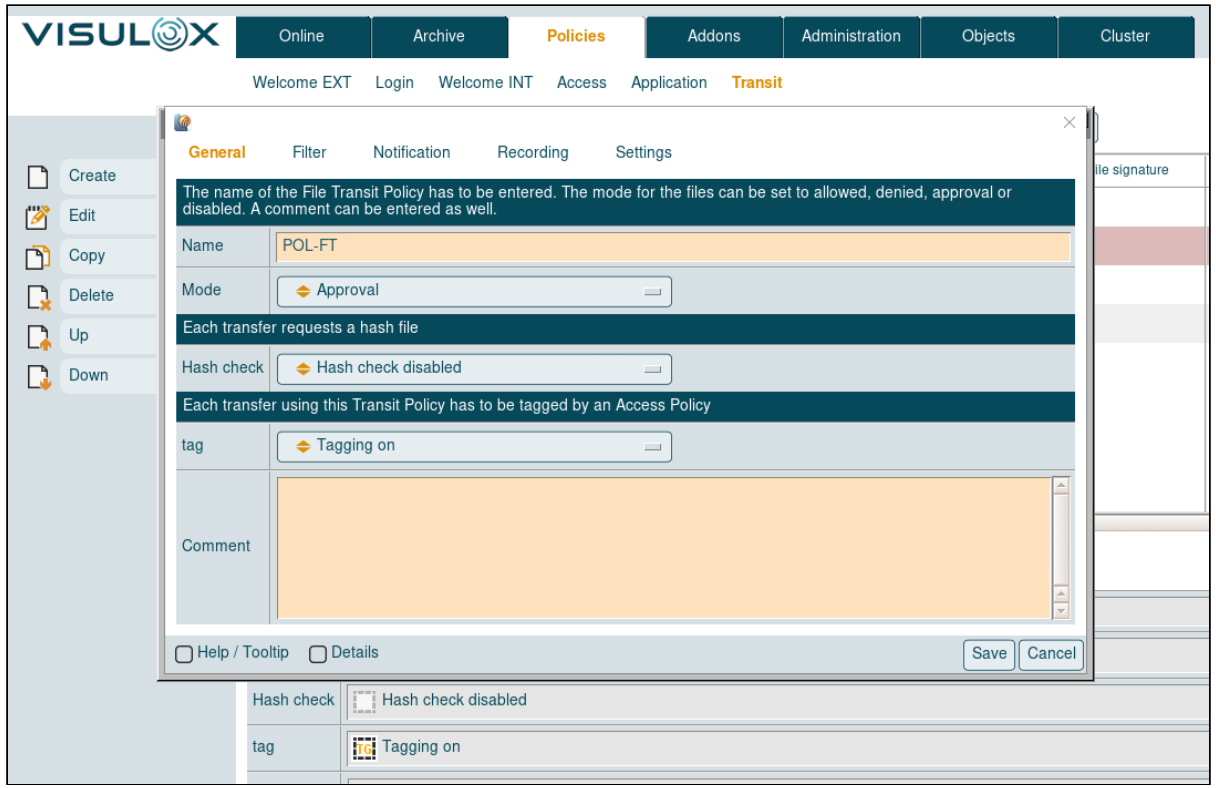
```
visulox policy application edit -name APP1 -ksmode record -ksrules /tmp/ks_rules -ksscript Dump
```

Remove an entry

```
visulox policy application delete -name APP1
```

Transit Policy

General



A Transit Policy starts with a **primary policy tag**, which sets the behaviour of the policy:

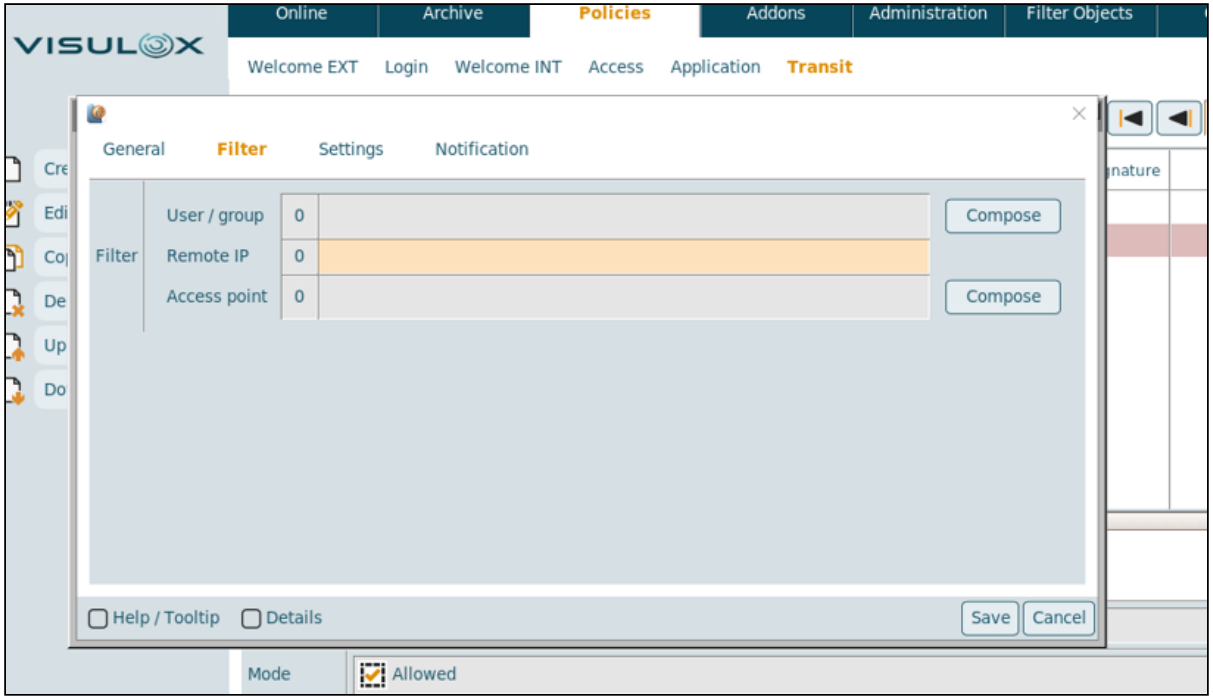
Primary policy tags	Description
Ignored	Ignore this policy.
Allowed	File transfer is allowed
Denied	File transfer is denied
Approval	File transfer needs approval
Passon	Transfer via passon script
Passon with approval	After approval file is passed on

Hash check can be enabled or disabled.
Uploaded files matching the policy with hash check enabled will get the status "**Wait for hash file**" in the Transit Zone.
Such files can only be processed, if a valid hash file is uploaded into the Transit Zone as well.

A **comment** can be entered as well.

Filter

The Transit Policy filter applies on a user / group, the remote IP of the user's connection and / or the access point, from where the user logs in.



Notification

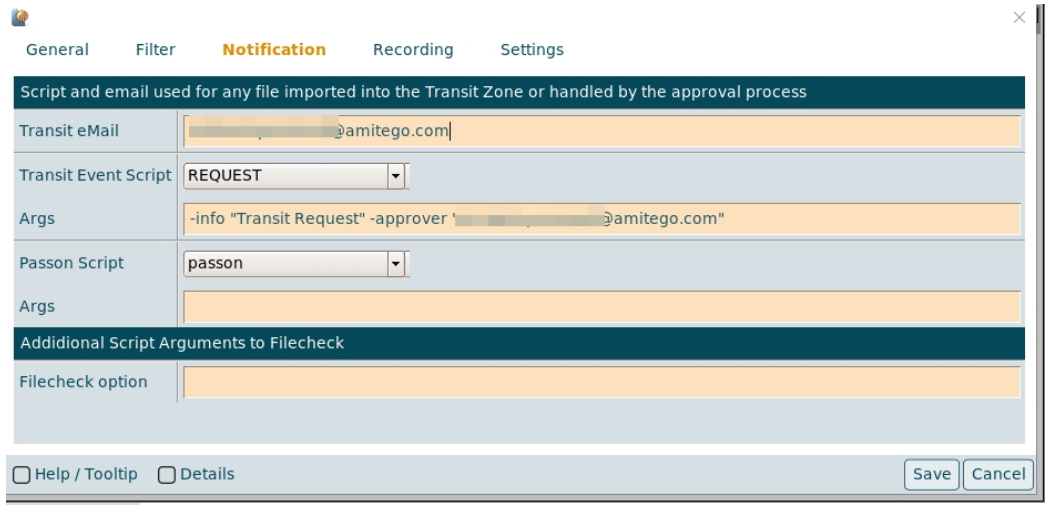
An eMail address for the notification can be set and the notification / request script can be selected, that will be triggered, if a file is imported into Transit Zone.

In the case of a passon configuration, the passon event script can be chosen as well.

Arguments for the **Transit Event** and **Passon script** can be entered in the according **Args** field.
Depending on the underlying script, the format of the arguments can be: **-arg -arg1 -arg2 <>**

The file check can be enabled/disabled for certain files / users addressed in the policy.

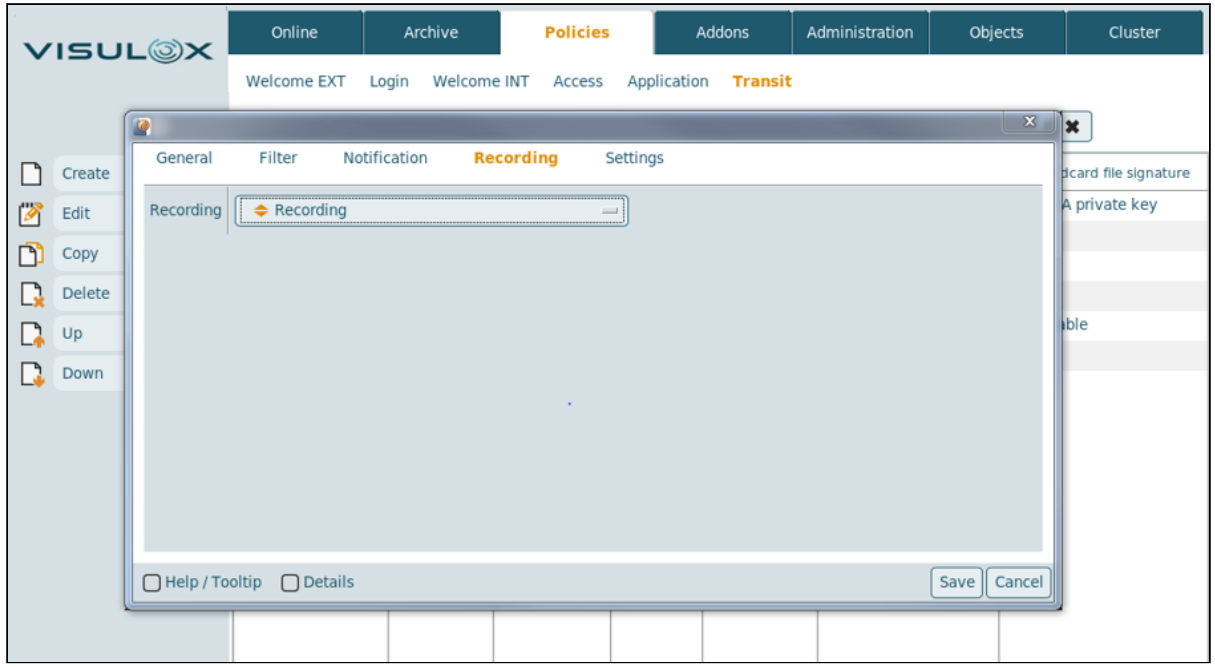
Additional script arguments can be set for the file check script.
During import of a file into the VISULOX Transit Zone the file is checked by /opt/visulox/tools/filecheck.sh.
The first argument is the file to be checked, the scripting **Filecheck option** is added (usage: arg1 arg2 ...).
Within the filecheck.sh script these parameters can be used.



Recording

Recording set to "**Recording off**" is useful for larger files.

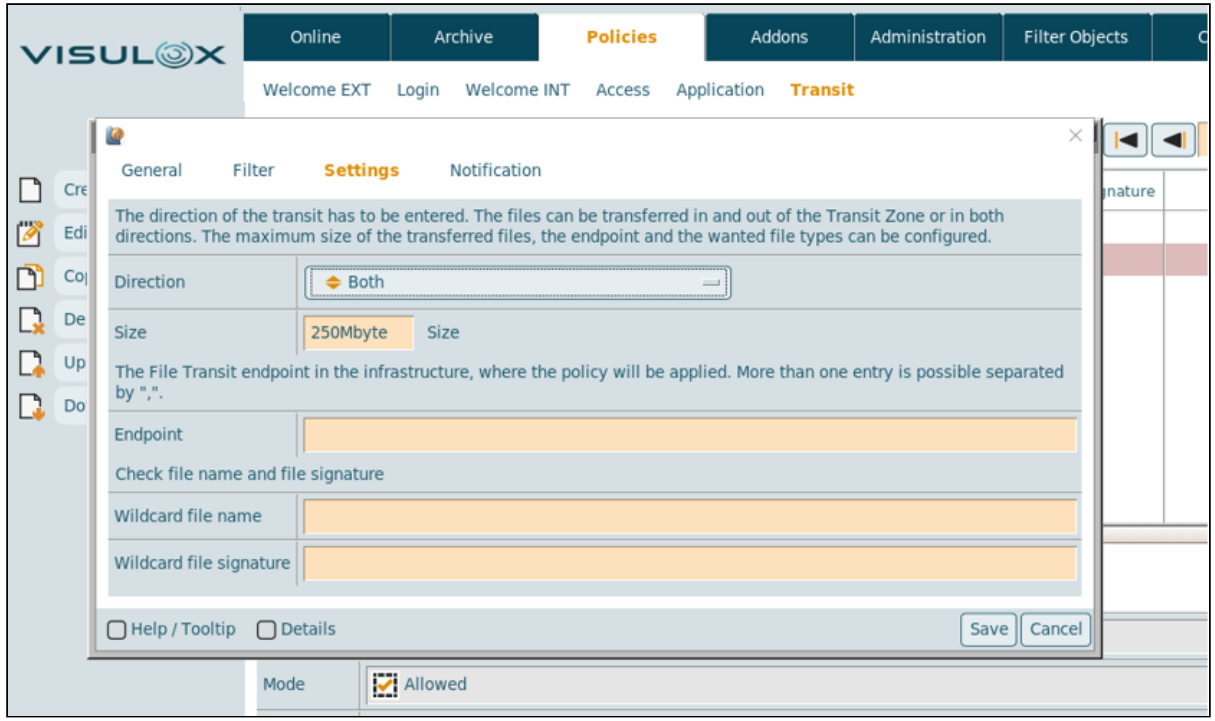
With this setting, the files will not be copied to the VISULOX File Store



Settings

The direction of the transfer has to be entered: in / out of the Transit Zone or in both directions.

The maximum size of the transferred files, the endpoint and the file type (mime type from "file") can also be configured.



If an endpoint is set, the policy takes effect immediately, if a file is transferred from the infrastructure to the Transit Zone.

If a file is transferred from a client into the Transit Zone it will be in the state "**Conditionally accepted**". Then the policy will be applied if this file is transferred to an endpoint.

For more than one endpoint "**,**" is used as a separator. The filename and/or the file signature can be set with wildcards.

How to control File Transit Policy from the command line

Overview

The command line tool "**VISULOX policy transit**" allows to control the File Transit Policy.

- Overview
- Usage
- File Transit Policy elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print File Transit Policies.
add	Add a File Transit Policy.
edit	Modify fields of a File Transit Policy.
delete	Remove a File Transit Policy.
fields	List available database fields (**-raw** = enhanced output)

Element	Description
-name <>	Name of policy or use AUTO
-mode <>	Policy off, allow, approval, deny. Default value: allow.
-hash <>	Policy hash modes: off, on. Default value: <off>
-direction <>	Policy in, out, both. Default value: both
-size <>	Filesize in Kilobytes (k), Megabytes (M), Gigabytes (G). Default value:<50M>
-namepattern <>	Wildcard on filename <>
-pattern <>	Wildcard on file signature <>
-email <>	eMail for approval <>
-endpoint <>	Mask for endpoints <>
-object <>	Policy filter: mask or unique distinguished object of user or group <>
-recording <>	Recording on/off. Default value: <off>

Element	Description
-remoteip <>	Policy filter: remote IP or remote IP mask <>
-accesspoint <>	Policy filter: Access Point <>
-script <>	Trigger script <>. Usage: -script "<script-name>**:** args". Example with arguments: -script "Dump**:** -arg arg -arg1 <>"
-passon <>	Passon script <>
-comment <>	Comment for the policy. Default value: CLI.
-grant <>	Set granted user in database record <>

Examples

List current available File Transit Policies

```
visulox policy transit list
    ---------------------------
    | basicname |  transitmode |
    ---------------------------
    |  POL-HASH | passedon.map |
    |    NOEXEC |     deny.map |
    |   TRANSIT |  allowed.map |
```

List available fields

visulox policy transit fields

List selected fields

```
visulox policy transit list -fields basicname,transitmode,ft_script
```

Add new File Transit Policy

```
visulox policy transit add -name TRANS1 -mode allow
```

Edit File Transit Policy

```
visulox policy transit edit -name TRANS1 -direction out
```

Remove an entry

```
visulox policy transit delete -name TRANS1
```

23.1.19 VISULOX Filters

Overview

With VISULOX it is possible to define filters:

- Filter for user and group
- Filter for application
- Filter for the remote access IP address
- Filter for the access point

This article explains the different filters and their usage.

- Overview
- The filter elements
  - Filter for user and group
  - Filter for application
  - Filter for the remote access IP address
  - Filter for the access point
- Wildcard filter
- VISULOX filter GUI
- Related information

The filter elements

Filter for user and group

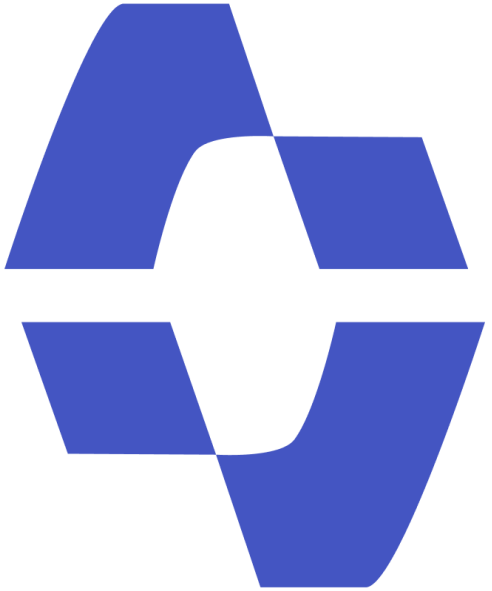
This filter is a list of users and user groups selected from the datasources. It is possible to define wild card filters as long as the filter has a result.

Filter for application

This filter is a list of applications. The applications are all listed in the datasource object of VISULOX. Wild card filters are possible as long as the filter has a result.

Filter for the remote access IP address

This filter is a list of IPv4 addresses. The element delimiter is a comma. This filter can be an IP address or IP Mask. It is possible to enter netmask like 192.168.10.0/24.



Filter for the access point

It is possible to select one ore more available acces points. An access Point is either a VISULOX Access Node or a VISULOX GATEWAY.

Wildcard filter

Wild card filters can not be used if the filter GUI is called within a role. This prevents to build filter which are too open.

Wild card filters are based on glob (http://www.tcl.tk/man/tcl8.6/TclCmd/glob.htm)

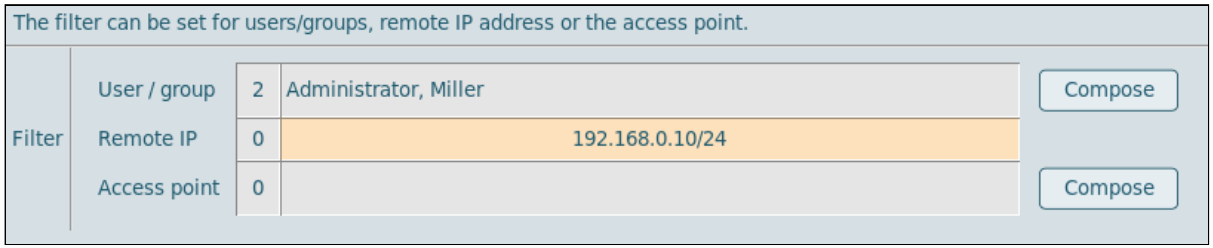
VISULOX filter GUI

The VISULOX Filter GUI has two presentations. **View** and **Edit**.

Presentations	
View	Show the lines
Edit	Strings can be entered, objects can be selected

With the **Compose** button, filters like User / group can be selected (**View**). The Remote IP filter is entered directly (**Edit**)

Filter example

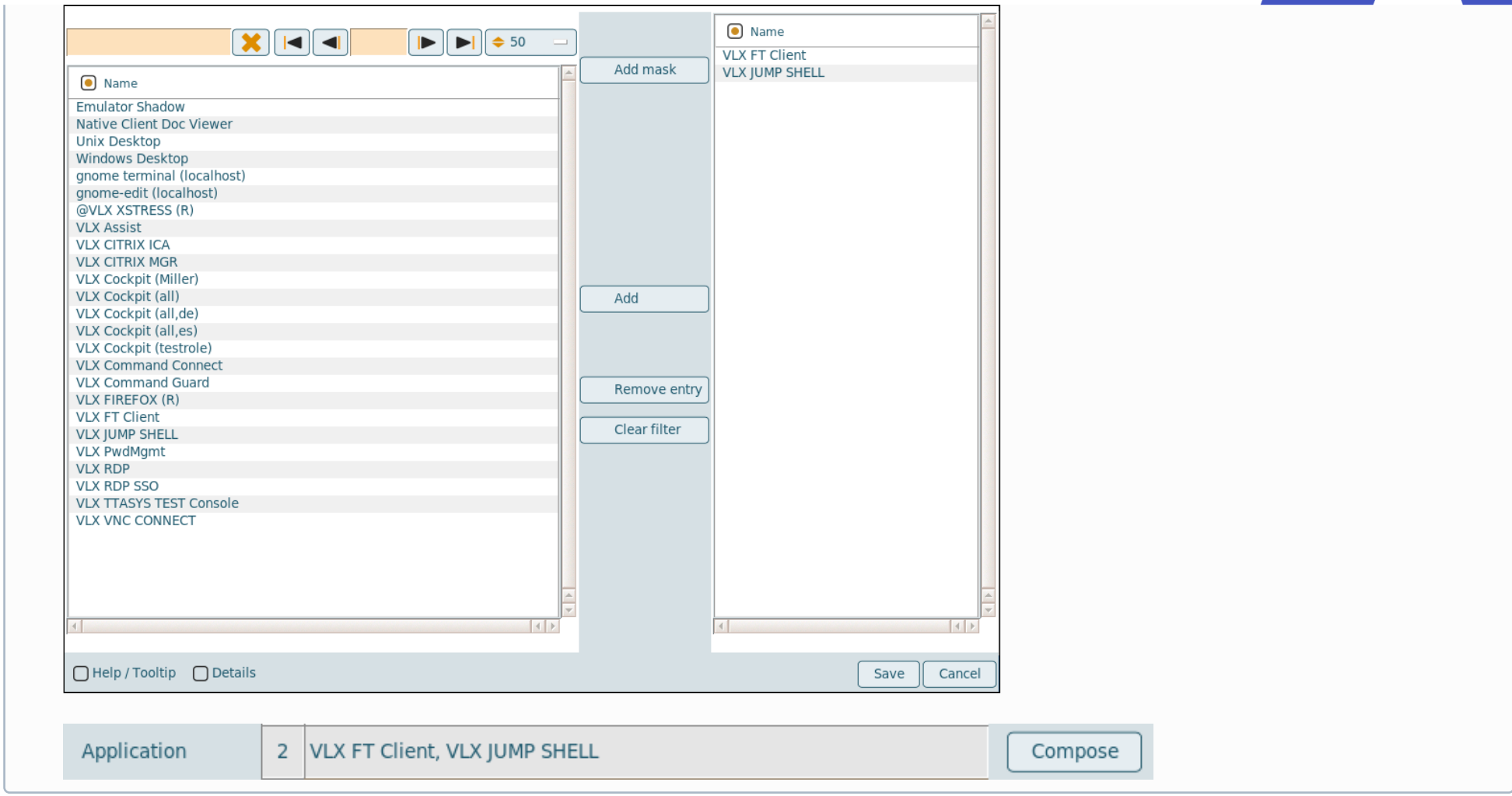


User / group is limited to 25 elements, Application to 40 per default. These values can be changed

Example to set to 10 for both, user/group and applications

```
./visulox config edit -name vlxgui.filter.maxuser=10,vlxgui.filter.maxapplication=10
```

Example: Object



Depending on the usage in the VISULOX policies, the VISULOX Filter GUI can be displayed in different presentations.

It is recommended to set the `vlxgui.usestrictfilter` parameter to 1 to prevent the configuration of a filter mask in the GUI, which will have no result.

```
visulox config edit -name vlxgui.usestrictfilter=1
```

Related information

VISULOX Policies - Overview

23.1.20 The application control variable "vlxMode"

Usage

In the application definition in the VISULOX PORTAL Datastore, the variable **vlxMode** controls some parameters for the behaviour of the application.

The variable can be set in the **Hints** field of an application object in VISULOX PORTAL Console.

The format is:

```
vlxMode=flag:flag:flag
```

The following flags are possible:

Flag	Meaning
R	Enforce recording of the application. It overrides the recording flag in the Application Policy and the welcome message in Application Policy is overwritten with the the default text.

Flag	Meaning
IU	Isolated User: Starts a **visulox.exp** application with its own transit user and Transit Zone (IU application must be started after the original app).
OCR	Enforce optical character recognition on the application.
WM	Add the VISULOX window manager with taskbar in the application. Only useful with X11 applications in **Independent Window** or **Kiosk Mode** The VISULOX window manager (default: JVM) is also used for example by VISULOX Jump Shells and can be changed with: **visulox config -name x11.windowmanager**
NOSC	No session controller. This is used, if an application should not be under control of the VISULOX Session Controller.
SYNC	The user's Transit Zone is provided into his shell or file explorer. All applications with **visulox.exp, vlxUnix.exp** and **vlxWindows.exp** (former: vlxRdp.exp**)** will get the VISULOX Transit Zone with **vlxMode=SYNC** set. On VISULOX Nodes wiithout VISULOX PORTAL Service, the replication has to be set at least to **ftonly**. **sshfs** must be installable. For OL 8 use "Oracle Linux 8 CodeReady Builder (x86_64) - Unsupported" as repository. If the user has two applications on the same server with the same shell. vlxTransit is seen in both applications, even if **vlxMODE=SYNC** is set only for one.
UPLOAD	The user's upload directory is provided into his shell or file explorer.
SCX<*pixels*>	The default value of the Session Controller GUI in Independent Windows mode is on the right hand side 10 pixel below the top. This can be not enough and covers part of the functionality in some applications (like desktops) . By adding SCX<int> via vlxMode the offset can be increased up to 200 pixels.

Flag	Meaning
ST<*in m,h,...*>	Access termination will be enforced in minutes, hours, etc
D<*delayinms*>	The SessionGuard (SG) is launched by VISULOX for any application which has to be controlled. The SG has to connect to the display after the application. The default delay value for the SG is 500ms. If application launch is slow, 500ms sometimes is not enough. **vlxMode=D<delayInMs>** can override this value. In Windows sessions, the ttaXPE should have the same color depth as the RDP session. In this case the "Delay" parameter is not needed. If different color depths are used, the color depth will be reinitialized, there are two possibilities: • The "Delay" parameter can be used • Testing different color parameters This is the preferred method because the "Delay" parameter does not lock the session until the session controller is up.

All applications with **visulox.exp** will have vlxtransit. Applications with **vlxUnix.exp** or similiar applications will have vlxtransit only, if VISULOX is running on the target system and if **vlxMode=SYNC** is set and the replication is at least **ftonly**.

Configuration for standard x11 and RDP / Windows applications

The **vlxMode** variable can be set for x11 and RDP applications in the **Hints** field on the **General** page of the application via VISULOX PORTAL Console:

For standard applications, a resource can be set as well in the hint field of the application with **vlxResource=<*resource-name*>**.

Related information

How to pass user credentials to an application - VISULOX Single Sign On - SSO

23.1.21 Access termination enforced

Enforced access termination for application sessions

Application sessions can be terminated after a configured time.
Warning messages are displayed in the session controller.

Sessioncontroller with configured session termination:

The session termination for single applications is configured via vlxMode parameter:

```
vlxMode=ST40m
```

For all applications session termination can be set via configuration parameter:

```
visulox config -name sc.forcetermination.duration=12h
```

Additional configuration parameters:

```
visulox config -name sc.
-----------------------------------------------------------------------
| changed | key                          | value                     |
-----------------------------------------------------------------------
|         | logger.sc.tracer             | false                     |
|         | sc.access.interval           | 15                        |
|         | sc.forcetermination.critical | 5                         |
|         | sc.forcetermination.duration | disabled                  |
|         | sc.forcetermination.text     | Session closing enforced  |
|         | sc.forcetermination.warning  | 30                        |
-----------------------------------------------------------------------
```

Enforced access termination for Workspace sessions

Workspace sessions termination can be enforced via a configuration parameter.
Running applications will be suspended and can be resumed after the next login.

Available parameters:

```
|         | workspace.forcetermination.duration    |
disabled                                                              ... |
|         | workspace.forcetermination.text        | Workspace closing
enforced                                                        ... |
```

23.1.22 General command line configuration

Overview

VISULOX has an internal table with many configuration parameters like:

- Layout of the node
- Default setting for new records in the GUI
- Data sources
- And others ...

- Overview
- Types
- Usage
- Common parameters
- Entering passwords via command line
- Base64 decode parameter
- Further command procession
- Ambigous values in commands
- Known issues and comments
- Related information

Types

There are three types of parameters:

- FIXED: Cannot be be changed
- SETUP: Can be changed on setup of a node
- OPERATION: Can be changed at any time

Parameters can be listed, changed and reset to their default values with the "**VISULOX config**" command.

If a parameter is changed or reset it will be replicated to other nodes.

Configuration parameters set while the node is **offline** will only be applied to the local node.
If a parameter should be changed for the whole cluster, the parameter has to be set again once the node is **online** again.

Changing can be done on any node. Last change will win.
Only parameters of the type SETUP and OPERATION can be changed.

Usage

List config parameters

```
visulox config -name <mask of parameter>
visulox config -name basicname
visulox config -name layout
```

The changed parameters can be shown with:

```
visulox config list -changed
```

With the following command the changed settings can be exported into an import script to import them on another environment:

```
visulox config export
```

Long values are truncated. This can be seen if "**...**" is presented. To get the whole value use **-raw**.

visulox config -name x11.windownames

```
-------------------------------------------------------------------------------------------------------------
| parameter       |  type | value                                                                     ... |
-------------------------------------------------------------------------------------------------------------
| x11.windownames | FIXED | Toolbar scx.tcl VLXTASKBAR metacity dtwm "TWM Icon Manager" gnome-settin ... |
-------------------------------------------------------------------------------------------------------------
```

visulox config -name x11.windownames -raw

```
-------------------------------------------------------------------------------------------------------------------------
-----
```

```
| parameter       |  type | value
|
-------------------------------------------------------------------------------------------------------------------------------
-----
| x11.windownames | FIXED | Toolbar scx.tcl VLXTASKBAR metacity dtwm "TWM Icon Manager" gnome-settings-daemon mwm FVWM |
-------------------------------------------------------------------------------------------------------------------------------
-----
```

A config parameter can be modified with "**=**" and the new value, that should be set. A validation of the value is done. The internal configuration files are written.

Changing a parameter.

```
visulox config -name guidefaults.access_policy.basicname=MYVALUE
```

Multiple parameters **and** multiple values can be modified in one statement:

Multiple parameters and values

```
visulox config -name NAME1=VALUE1:VALUE2,NAME2=VALUE1:VALUE2,NAME3=VALUE1:VALUE2
```

If a VALUE is a list, the separator is "**:**":

Separator ":"

```
visulox config -name NAME="a:b:c"
```

If a value contains a comma, which is used as separator, "\\" must be used:

Value with comma

```
visulox config -name regexp.email="[0-9]{2\\,5}"
```

A modified config parameter can be reset to his default parameter:

Reset a parameter

```
visulox config reset -name guidefaults.access_policy.basicname
```

This command rebuilds the local configuration. Under normal operation this command is not needed:

Rebuild configurations

```
visulox config rebuild
```

Tip for a better display of information greater than the terminal

visulox <command> | less -S

Common parameters

The basic admin command and subcommands have common command line options:

Command	Parameter	Description
-format	text	Default. Displays the output in a human readable format.
	csv	Output is listed in the format of comma separated values. The CSV delimiter is "**;**".
	json	Output is listed in the format of JSON.
	tcl	Output is listed in the format of a TCL array format.
	cli:var1:var2	Output is listed in the format of comma separated values of the vars listed. The delimiter is "**;**". Use full for further command execution
-force		Some commands will not run because the impact is big. With -force the command operates without comment. For addons and policy commands **-force** changes from add to edit if the object already exists.
-run		Some commands are in a dry mode and will be enabled with -run.
-stdin		This allows to pipe all parameters via stdin into the command.
-log	error,verbose,info,debug	Overrides the log level.
-verbose		Command is more chatty.

Command	Parameter	Description
-raw		Information is not formated. (unix time stamps, full user names, etc)

Usage of the **-stdin** command:

Example -stdin

```
echo "-endpoint foo1@server" | visulox addon host add -stdin
```

Spaces via **-stdin** are not allowed. If a comment with spaces should be entered, here is a possibility:

-stdin with spaces

```
echo "-name foo -endpoint foo3@server -comment64 $(echo this is the comment) " | visulox addon host add -stdin
```

Entering passwords via command line

For all configuration commands, where entering a password is necessary ((e.g. -password, adminpwd, ...), the password can be entered hidden after typing "**-**" in the console.

Base64 decode parameter

It is possible to provide any parameter in a base64 declaration. This is useful if spaces, newlines or other critical parameters have to be provided. Base64 Paramaters have the prefix 64 and is very good to use it togeter with standard in.

⚠ Characters must be in UTF-8 format.

```
 echo "-name64 dGVzdC1iYXRzLTU= -object64 bz1UYXJhbnRlbGxhIFN5c3RlbSBPYmplY3RzL2NuPUFkbWluaXN0cmF0b3I= -ticket64 QS0xMg==
-endtime64 ZW5kbGVzcw==" | visulox policy access add -stdin
```

Useful (%NODE% variable)

The following commands allow the **%NODE%** variable, which will be substituted with the local logical nodename:

```
visulox config -name "... %NODE%"
./database.tcl query -sql "... %NODE%"
```

Further command procession

The formated output is not helpful for "**grep**", "**awk**", "**sed**" etc.

Therefore use "**-format cli:var1,var2" or "-format cli:var1,var2 -raw**"

```
visulox status users -format cli:vlxowner:webtopsessionid -raw | grep Admin
```

Ambigous values in commands

Expression	Description
<value>	Will always be used as a mask
<*value*>***<*value*>	Will be used to find an unambiguous object

Expression	Description
-verbose	if object is ambiguous -verbose lists the first 10 elements which are found

This applies to the policy parameters **-application**, **-object**, **-dcobject**.

Known issues and comments

Changing of the configuration (sometimes) needs a restart of VISULOX.

On some commands the output per line is too long and so it will not be readable. Helpful is "**-format json**".

Related information

How to change the VISULOX logos and colors

How to work with VISULOX Datasources

Setting the min/max length for messages, contents and comments

23.1.23 How to adjust the Jump Shell

With the following configuration option, the focus model of the windows inside the Jump Shell can be changed.

```
visulox config -name jwm.focusmodel
    -------------------------------------
    | changed | key            | value  |
    -------------------------------------
    |         | jwm.focusmodel | sloppy |
    -------------------------------------
```

Possible values are: **sloppy** and **click**. The default setting is **sloppy**.

More parameters can be added in VISULOX to enhance / restrict the Jump Shell on request.

23.1.24 How to change the VISULOX logos and colors

Overview

On the login page, reports and recorded sessions the **customer logo** in GIF or PNG format is displayed.

Above the login mask,the **login logo** can be found. The **dashboard logo** is displayed on the Workspace.

The **product logo** is shown in the VISULOX Cockpit and the **report logo** is placed in the top right corner of reports and in recorded sessions.

With these different logos it is possible to adjust the look and the size for all places a logo can be displayed.

- Overview
- Usage
- Configuration
    - Change the current logos
- Known issues and comments

Default customer logo	Default login logo	Default dashboard logo	Default product logo	Default report logo
Login page	Login mask	Workspace	VLX Cockpit	Reports / recorded sessions

The default size of the logos is 140x50 pixels. A good width for the customer logo within the new design is 450 pixels.

It is possible to change all logos with the "**visulox config**" command.

Make sure, that the logos are not too small or large. After changing the logos, the display of the logos in reports, recorded sessions, on login page and on the Workspace should be checked.

Usage

It is always a good idea to change the logos to project or customer related logos to increase project awareness.

For individually customized **login pages** based on different access URLs, see: Access Branding

Configuration

Display the current logos names, types and design colors:

```
Logos:
    ------------------------------------------------------
    | changed | key                  | value              |
    ------------------------------------------------------
    |         | design.customerlogo  | amitego (png)      |
    |         | design.dashboardlogo | visulox-white (png)|
    |         | design.loginlogo     | visulox (png)      |
    |         | design.productlogo   | visulox (png)      |
    |         | design.reportlogo    | visulox (png)      |
    ------------------------------------------------------
 Colors:
    ------------------------------------------------------------------------------------------------------------------
    | changed | key                          | value   |                                          shortinfo | defaultvalue |
    ------------------------------------------------------------------------------------------------------------------
    |         | design.accentcolor           | #eb34c0 |                                 Separations in design |      #f3d7a6 |
    |         | design.bannercolor           | #56e820 |                Banner background color on login page |      #d6e0e4 |
    |         | design.bannertextcolor       | #eb34c0 |                     Banner text color on login page |      #1e596e |
    |         | design.basecolordark         | #eb34c0 |                                       Background color |      #06495b |
    |         | design.textcolor             | #06495b |                                             Text color |      #06495b |
```

```
|         | design.ui4.color.background | #1f1c25 | UI4: background color in left handside of login screen |      #1f1c25 |
|         | design.ui4.color.dark       | #000000 |                                          UI4: Dark color  |      #000000 |
|         | design.ui4.color.error      | #ed3131 |                                          UI4: Error Color |      #ed3131 |
|         | design.ui4.color.favorite   | #edda31 |                                       UI4: Favorit Color |      #edda31 |
|         | design.ui4.color.main       | #4455c2 |                                       UI4: General Color |      #4455c2 |
|         | design.ui4.color.success    | #5ba587 |                                       UI4: Success color |      #5ba587 |
|         | design.ui4.color.warning    | #ed7d31 |                                       UI4: Warning Color |      #ed7d31 |
-------------------------------------------------------------------------------------------------------------------
```

With the **main** color the base color for all pages is chosen and shades of this color are used as well.

design.ui4.color.background is used to change the left side of the login screen apart from the main color. This can be helpful, if the logo and the background have a similar color.

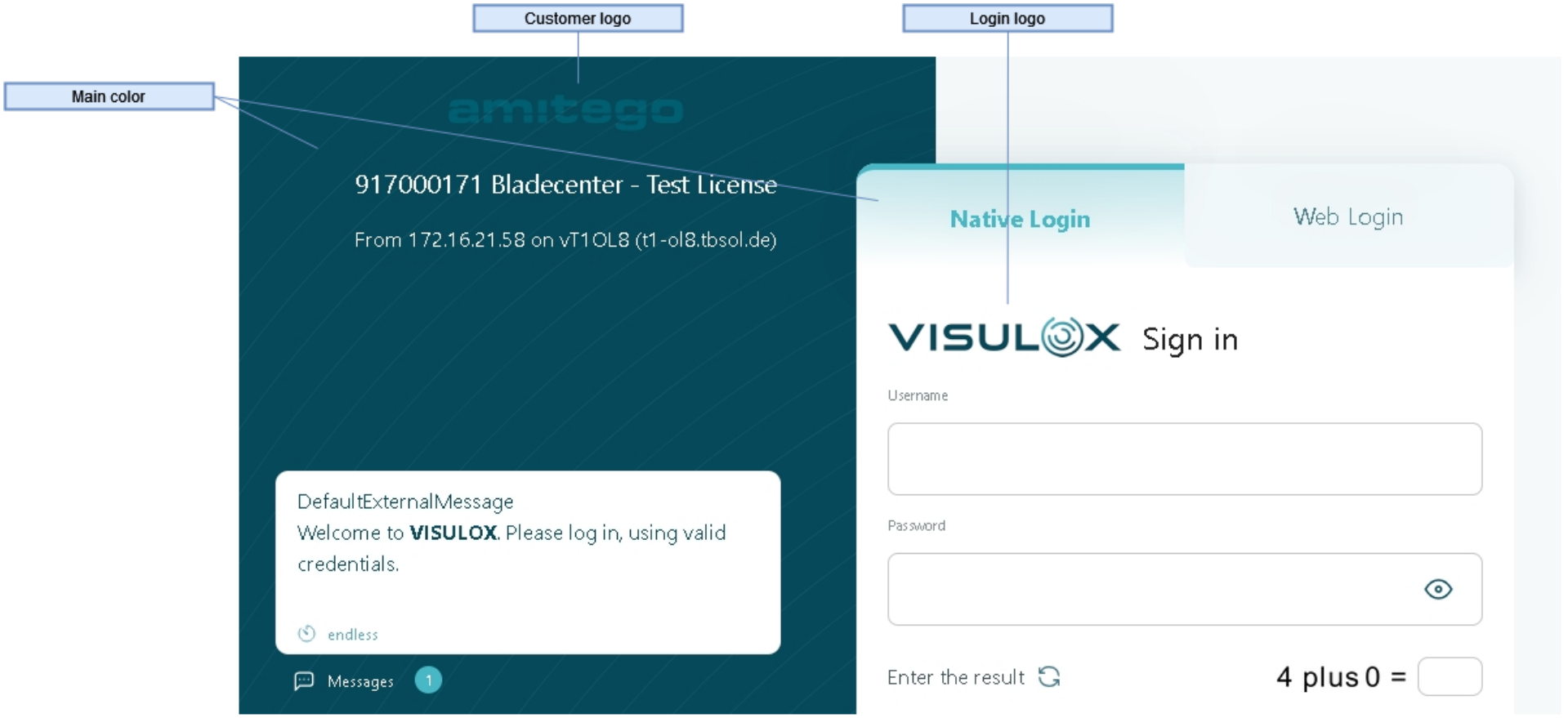
If the logo and the background have different colors (light/dark) and are well recognizable, both values can be the same.

design.ui4.color.dark is used in the Workspace for certain elements (table headers, background in tables).

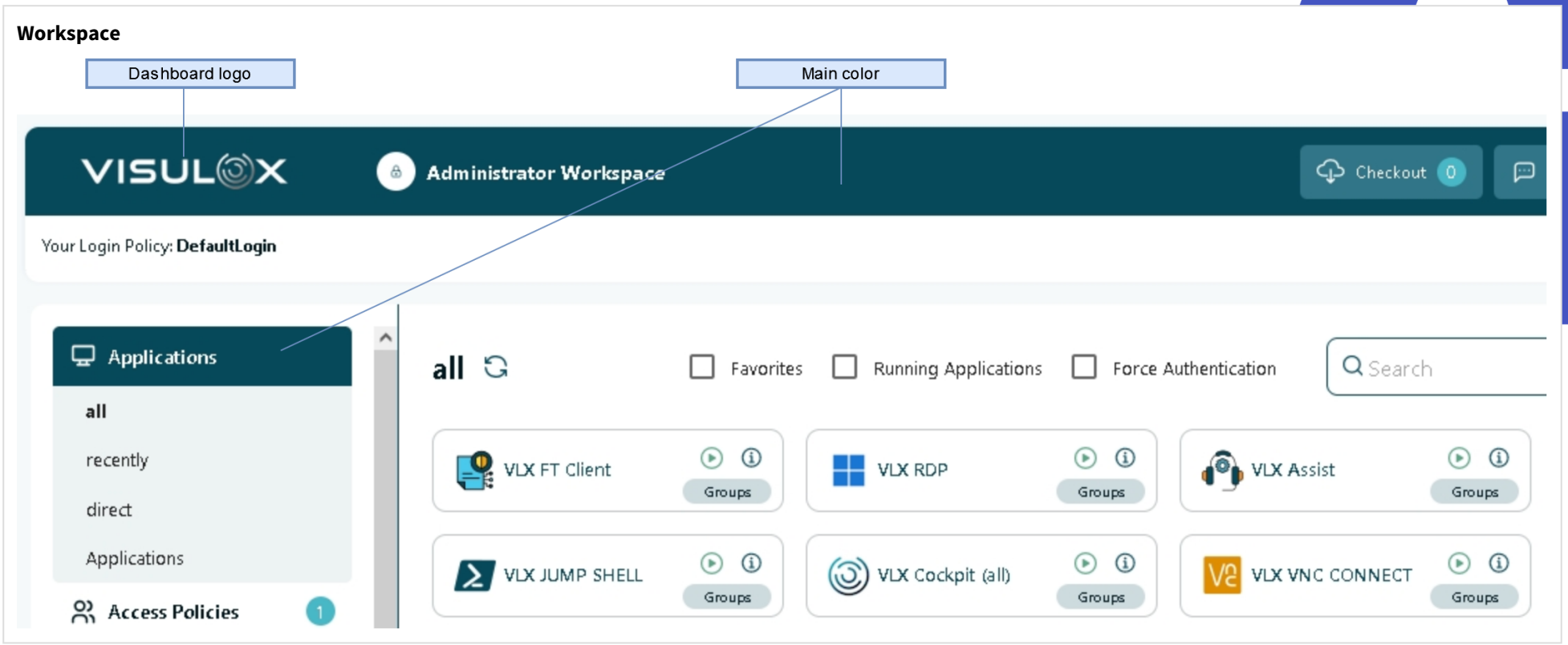
⚠ Some of the available color settings may no longer be used due to UI4 design changes.

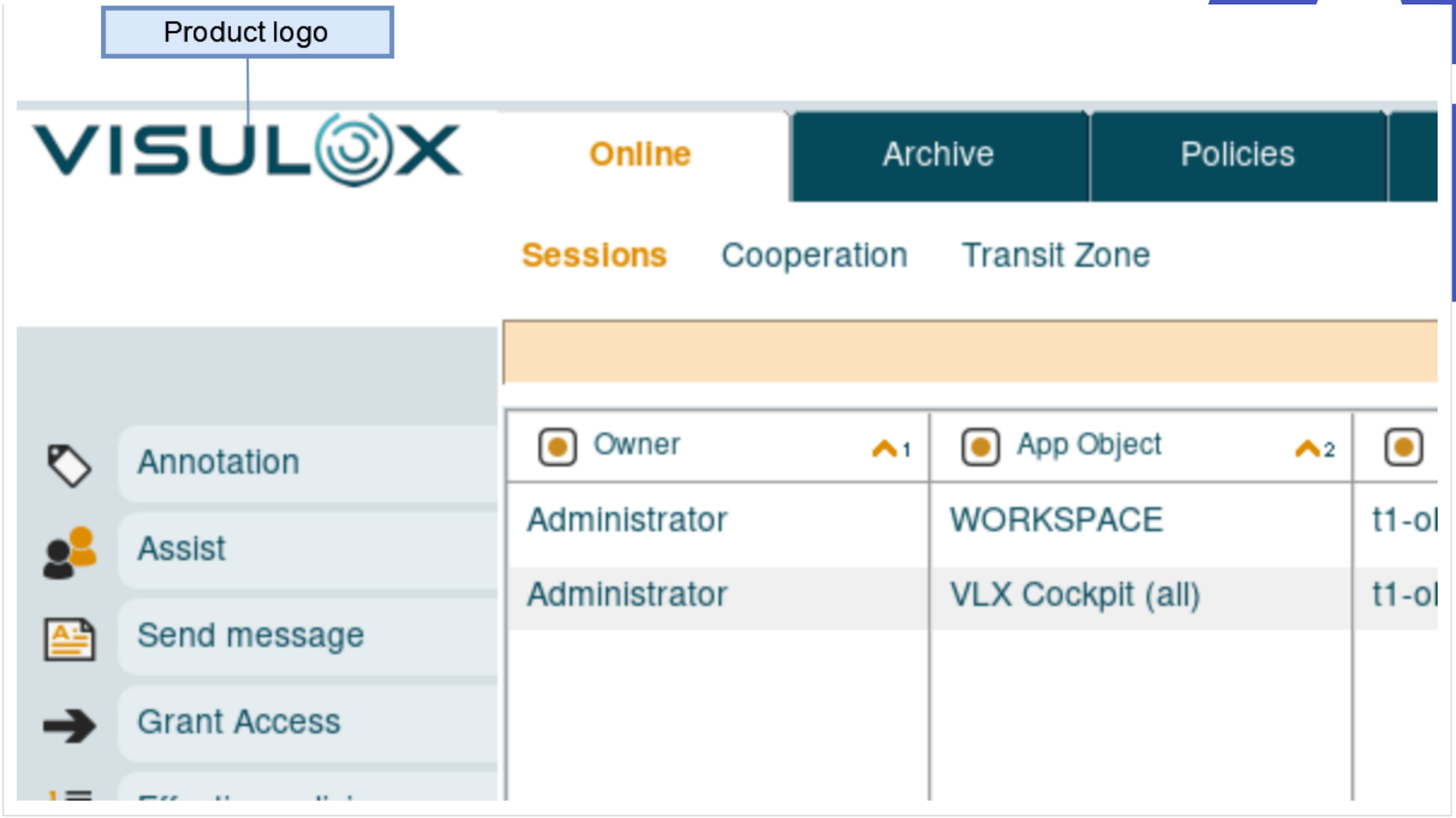
⚠ **design.advanced** should only be set to true by an integrator to adjust the available advanced color settings.
Advanced color settings can have side effects, if not used properly.

Login page


Customer logo
Login logo
Main color
amitego
917000171 Bladecenter - Test License
From 172.16.21.58 on vT1OL8 (t1-ol8.tbsol.de)
DefaultExternalMessage
Welcome to VISULOX. Please log in, using valid credentials.
endless
Messages
1
Native Login
Web Login
VISULOX Sign in
Username
Password
Enter the result
4 plus 0 =

Workspace


Dashboard logo
Main color
VISULOX
Administrator Workspace
Checkout 0
Your Login Policy: DefaultLogin
Applications
all
recently
direct
Applications
Access Policies 1
all
Favorites
Running Applications
Force Authentication
Search
VLX FT Client
Groups
VLX RDP
Groups
VLX Assist
Groups
VLX JUMP SHELL
Groups
VLX Cockpit (all)
Groups
VLX VNC CONNECT
Groups


Product logo
VISULOX
Online
Archive
Policies
Sessions
Cooperation
Transit Zone
Annotation
Assist
Send message
Grant Access
Owner
1
App Object
2
Administrator
WORKSPACE
t1-ol
Administrator
VLX Cockpit (all)
t1-ol

Available design placeholders:

```
VLXDESIGNADVANCEDERRORLIGHT VLXDESIGNUI4COLORBACKGROUND VLXDESIGNDASHBOARDLOGO VLXDESIGNADVANCEDWARNINGMAIN
VLXDESIGNUI4COLORSUCCESS
VLXPRODUCTLOGO VLXDESIGNLOGINLOGO VLXDESIGNADVANCEDERRORDARK VLXDESIGNADVANCEDINFOLIGHT VLXDESIGNUI4COLORERROR
VLXDESIGNADVANCEDINFODARK VLXREPORTLOGO VLXDESIGNADVANCEDERRORMAIN VLXDESIGNADVANCEDSECONDARYLIGHT VLXDESIGNADVANCED
VLXDESIGNUI4LOGINMESSAGES VLXDESIGNADVANCEDBACKGROUNDCOMMON VLXDESIGNADVANCEDINFOMAIN VLXDESIGNADVANCEDSECONDARYDARK
VLXDESIGNUI4COLORFAVORITE VLXDESIGNADVANCEDSUCCESSDARK VLXDESIGNBANNERTEXTCOLOR VLXDESIGNADVANCEDPRIMARYLIGHT
VLXDESIGNUI4COLORDARK VLXDESIGNPRODUCTTITLE VLXCUSTOMERLOGO VLXDESIGNADVANCEDSECONDARYMAIN VLXDESIGNADVANCEDBACKGROUNDDEFAULT
VLXDESIGNTEXTCOLOR VLXDESIGNBASECOLORDARK VLXDESIGNADVANCEDWARNINGLIGHT VLXDESIGNADVANCEDSUCCESSMAIN VLXDESIGNADVANCEDPRIMARYDARK
VLXDESIGNBANNERCOLOR VLXDESIGNACCENTCOLOR VLXDESIGNUI4COLORMAIN VLXDESIGNADVANCEDWARNINGDARK VLXDESIGNADVANCEDBACKGROUNDPAPER
VLXDESIGNUI4COLORWARNING VLXDESIGNADVANCEDSUCCESSLIGHT VLXDESIGNADVANCEDPRIMARYMAIN VLXDESIGNADVANCEDAPPNAMES
VLXBASECOLORDARK VLXACCENTCOLOR VLXTEXTCOLOR VLXBASECOLOR
```

Change the current logos

```
visulox config -name design.customerlogo=<path/filename of logo>

visulox restart
visulox portal attach
```

Known issues and comments

Changing the logo does not affect running sessions. Only new started sessions will have the changed logo applied.

It is necessary to **restart** the VISULOX service and to use the **visulox portal attach** command on the VISULOX Access Nodes to display the new design.

Clearing the browser cache on the client side can be necessary as well.

23.1.25 Custom application icons

Individual customized icons can be assigned to applications via the VISULOX Portal Console.

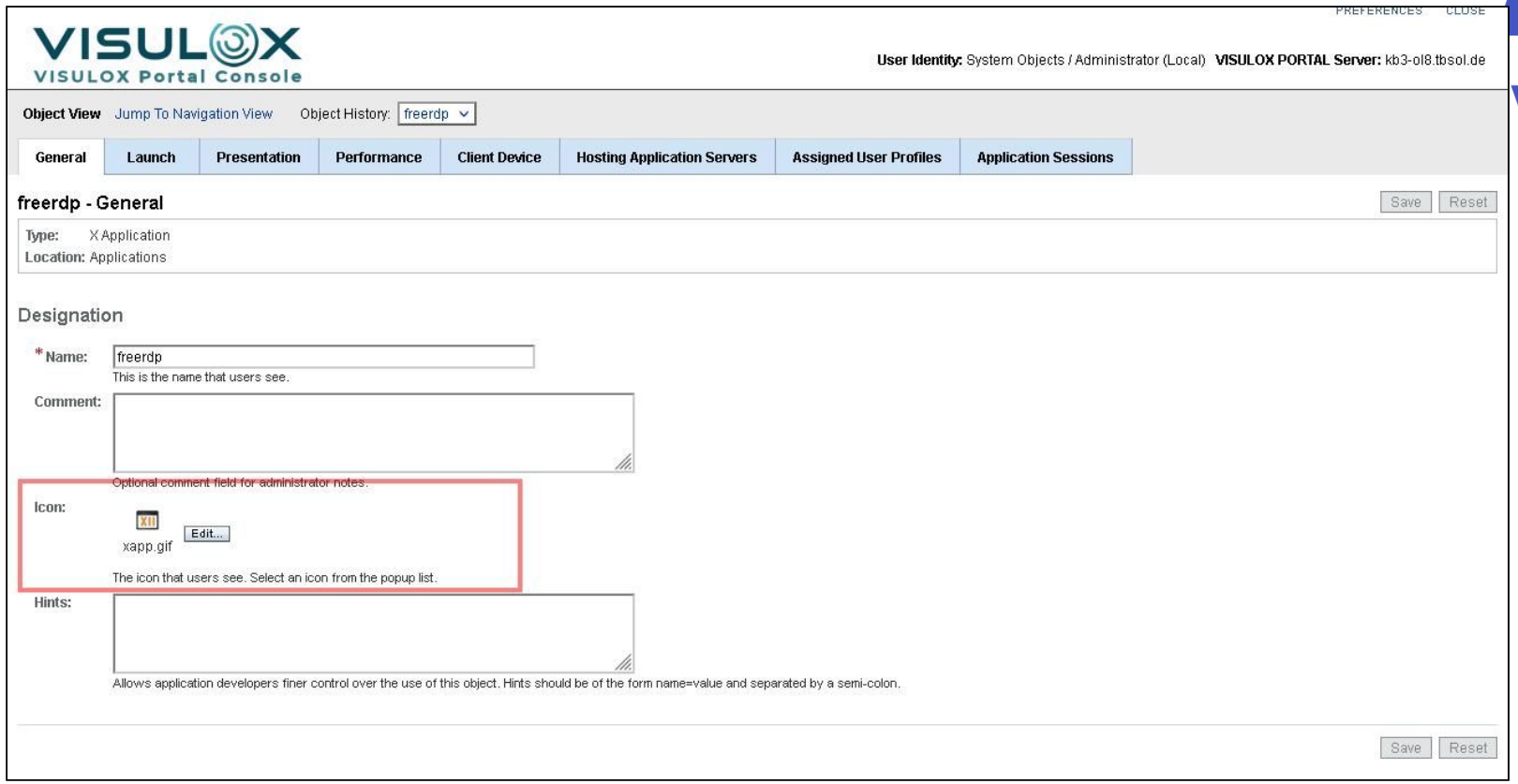
First the new custom icons have to be copied to:

```
/opt/visulox/setup/portal/icons/
```

The icons must be in **.gif** format and the size has to be not larger than **30x30 pixels**.

> ⚠ After copying the new icon, the **visulox portal attach** command must be executed once.

Than the icon has to be assigned to the application in the VISULOX Portal Console:

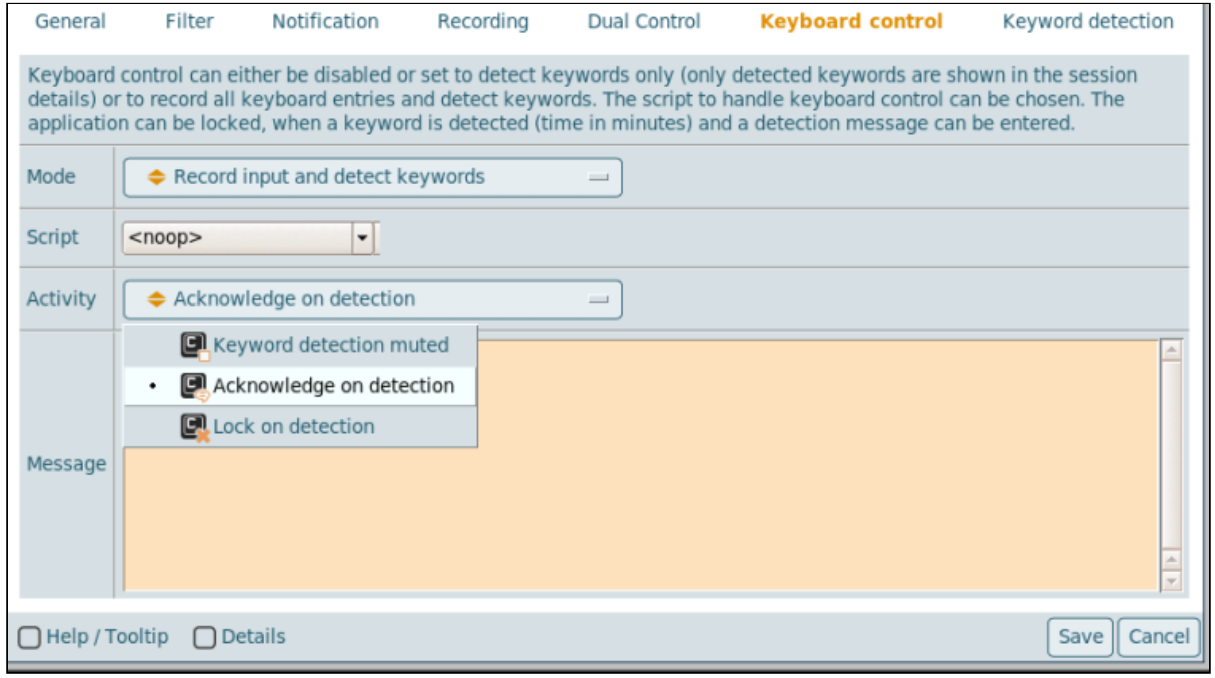


23.1.26 How to lock a user permanently for using an application after keyword detection

An Application Policy can be built to detect keywords, a user is not allowed to enter.

For the detection three modes are available:

- Keyword detection muted
- Acknowledge on detection
- Lock on detection



When the session is locked, the user can just close the application and reopen it again. This new session will be unlocked.

In the keyword detection process a script can be inserted. Within this script the user and the application is known and the following command can be issued:

```
visulox policy access add -run -mode deny \
                  -object "$VLXOWNER" \
                  -application "$VLXAPPLICATION" \
                  -ticket "Sticky lock" \
                  -endtime "+30 days"
```

This will insert a new Access Policy, which blocks the user from reusing the application again in the next 30 days.

23.1.27 How to create and use notifications

General

Notifications are used to inform supervisors and users about a variety of actions via eMail or SMS, e.g. login, application start/stop, recording start/stop, access ending, keystroke detected, etc.

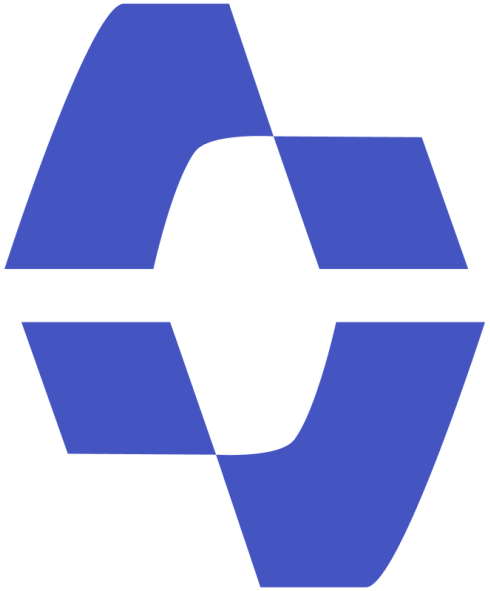
It is possible to create individual notification scripts, that can be enriched with a plenty of variables.

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

User	Role	eMail	SMS	Application	Other
Master	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	-
Miller	User	*<user>@company*.com	-	VLX Jump Shell	-

Supervisor Master creates notification scripts and configures the notifications in Cockpit / Administration / Actions.



User Miller logs into VISULOX PORTAL and starts an application.

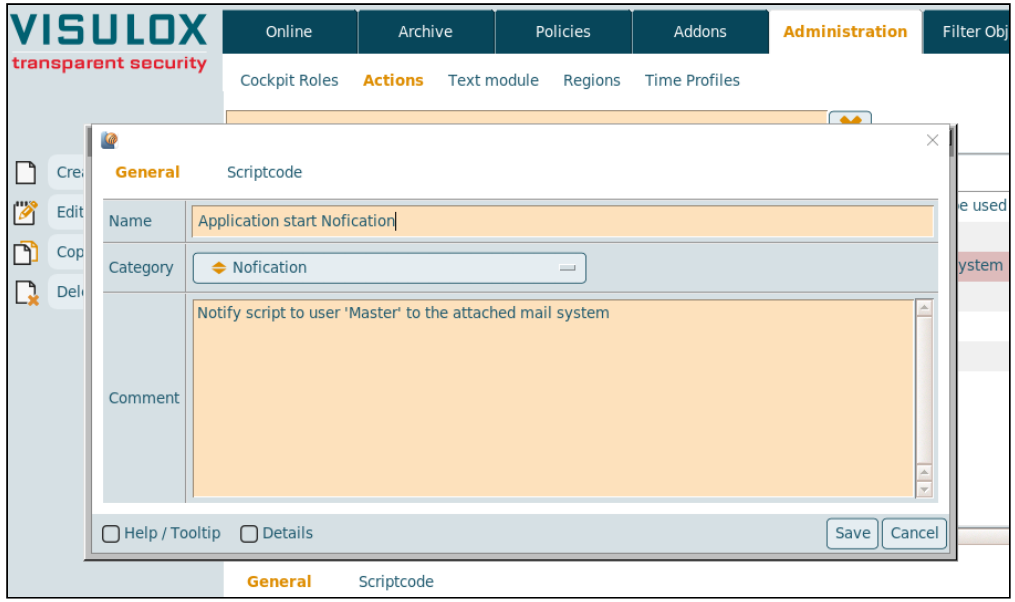
Creating a notification script

Example 1: Notification script on application start

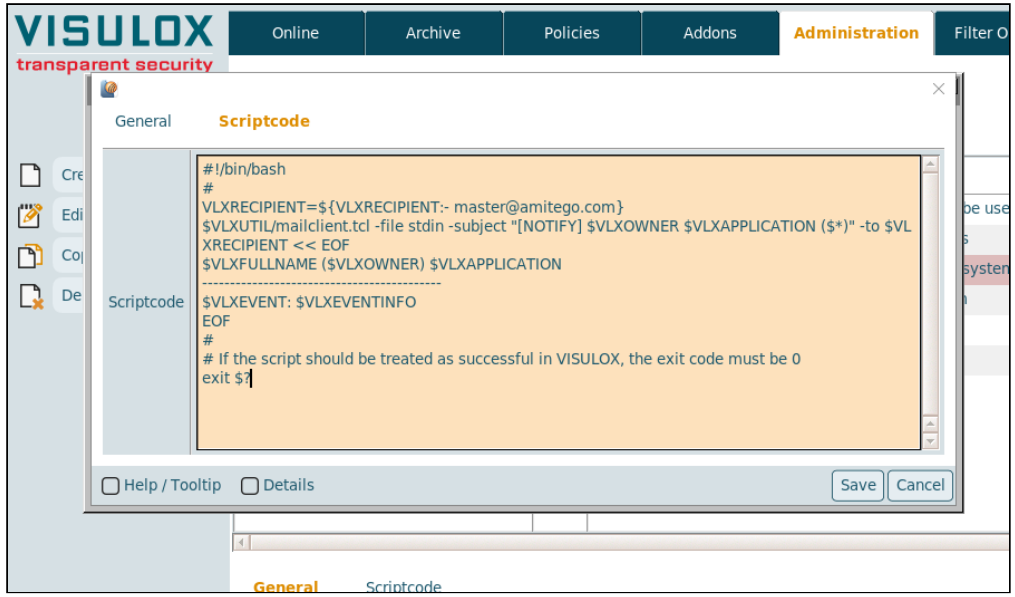
A unique name for the notification script must be entered: "**Start notification**"

The script category has to be selected: "**Notification**"

A comment can be filled out.

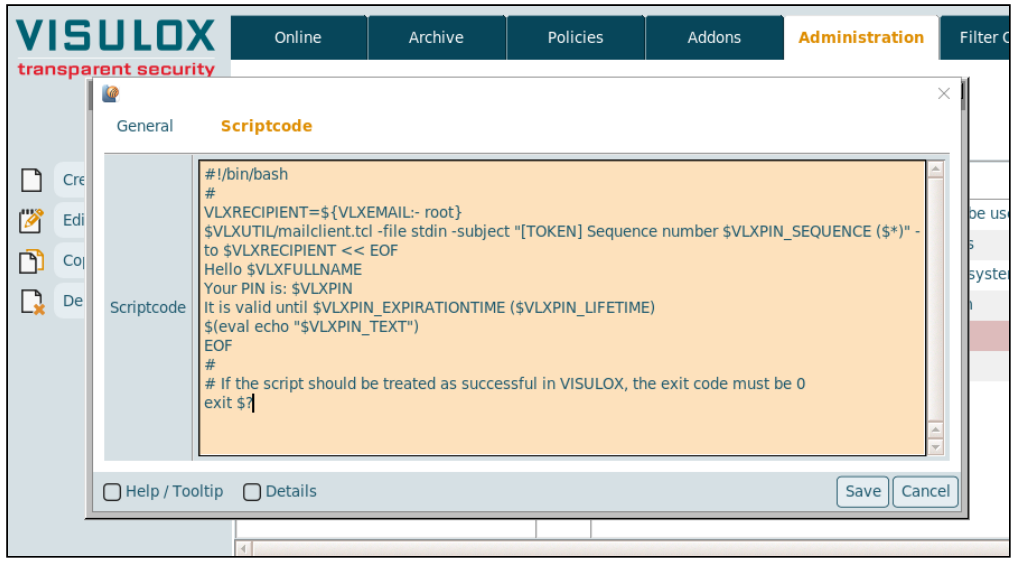


The scriptcode of the script enriched with the VISULOX variables has to be created.



As recipient, the eMail address of supervisor Master must be used in this example.

Example 2: PIN notification script to 2FA users



A unique name for the notification script must to be entered: "**PINscript**"

The script category has to be selected: "**PIN**"

A comment can be filled out.

And the content of the script enriched with the VISULOX variables has to be created.

The variable "**$VLXEMAIL**" will use the eMail address of user Miller as it is registered in the VISULOX PORTAL Datastore.

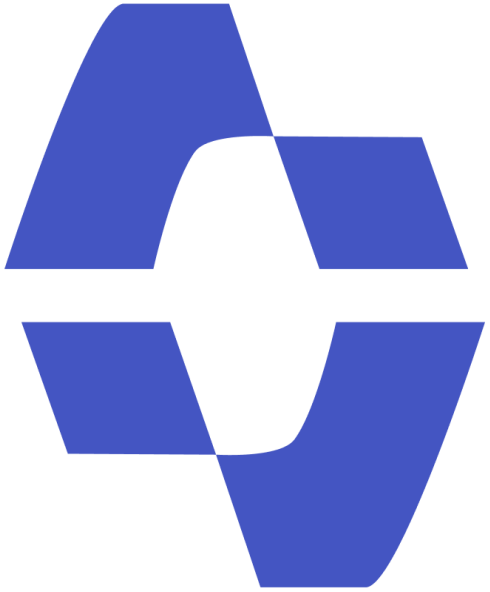
Available script categories

Category	Used as
Notification	These action scripts can be chosen, where application notifications are used (Application Policy).
Pin	These action scripts deliver information for the Multi Factor Authentication (Login Policy).
Report	These are report actions scripts.
Validate	These action scripts can be chosen for validation.
*	These action scripts are available everywhere scripts can be used. The setup provides one script in this category, which allows to dump all variables provided to an action script. This is helpful for testing.

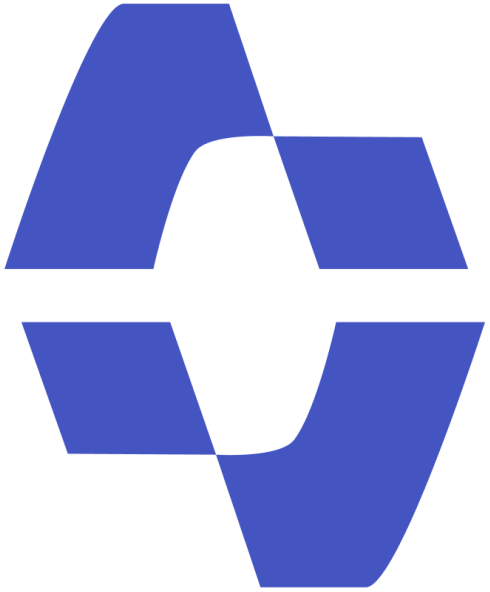
Notification script variables (examples)

The following list contains some useful examples for script variables.
To get the complete list of available variables for a certain action script, the dump script should be used.

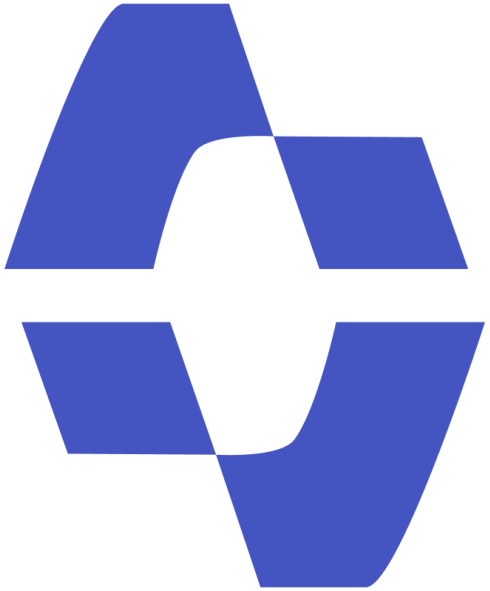
Variable	Description
VLXFULLNAME	Full name of the user
VLXSURNAME	Surname of the user



Variable	Description
VLXEMAIL	eMail address of the user
VLXSMS	SMS address of the user
VLXOWNER	Owner of the application
VLXGROUPLIST	Group list
VLXUSERPROFILE	Profile of the user
VLXPIN	PIN for Multi Factor Authentication
VLXPIN_FMT	Formatted PIN for Multi Factor Authentication
VLXPIN_SEQUENCE	Sequence number for PIN
VLXPIN_EXPIRATIONTIME	Expiration time with date for the PIN
VLXPIN_LIFETIME	Lifetime for the PIN
VLXPIN_TEXT	PIN text
VLXACCESSPOIN	Access Point



Variable	Description
VLXCREATETIME	Creation time
VLXLOG	Path to logs
VLXLOGINUSER	Logged in user
VLXMANAGER	Manager of the user
VLXOBJECT	Name of the object
VLXOWNERID	Owner ID
VLXOWNERSHORT	Short name of the owner
VLXPOLICY	VISULOX policy
VLXREMOTEIP	Remote IP
VLXSMS	SMS of the user
VLXLISTHASH	Hash
VLXCLIENTIP	Client IP address



Variable	Description
VLXLANG	Language
VLXSESSIONHOST	Host, where the session was started
VLXCREATETIME_FMT	Time of creation (readable)
VLXSESSIONSTARTTIME	Start time of the sesssion
VLXSESSIONDURATION	Duration of the session
VLXSESSIONDURATION_FMT	Duration of the session (readable)
VLXSESSIONENDTIME	Endtime of the session
VLXSESSIONENDTIME_FMT	Endtime of the session (readable)
VLXAPPLICATION	Application name
VLXRECIPENT	Recipient
VLXTICKETID	Ticket ID of the user
VLXLOGINSCRIPT	Login script

Variable	Description
VLXAPPLICATIONUSER	User of the application
VLXBADWORD	Detected keyword in Keyboard recording
VLXEVENTINFO	Event info
VLXCREATEDBY	Created by
VLXCREATEDBYSHORT	Short name of creator

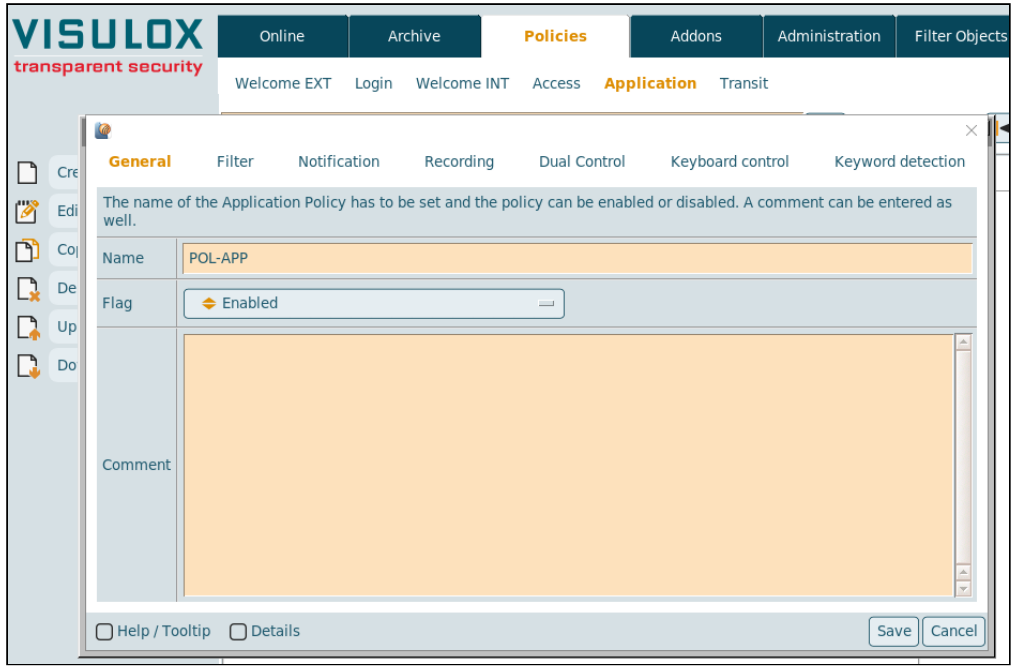
See also:

- Variables in notifications
- Transit script variables
- How to control action scripts from the command line

Configuring notifications

Example 1: Notification on application start from user Miller

Creating a new Application Policy in Cockpit:

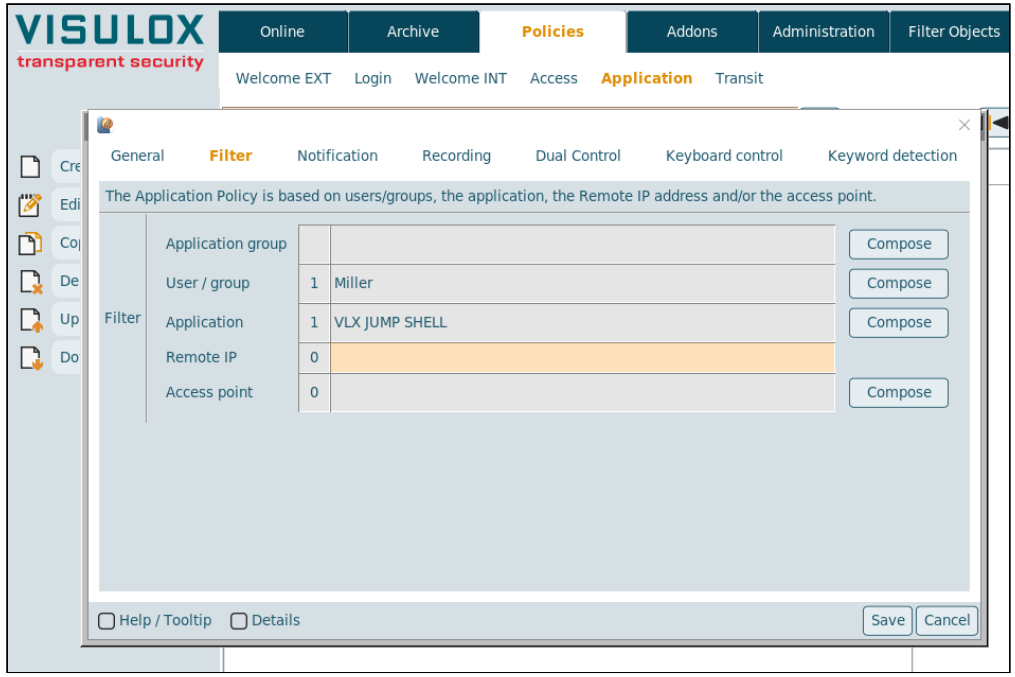


A unique name for the access Policy has to be entered: "**POL-APP**".

Policy mode is: "**Enabled**" .

A comment can be filled out as well.

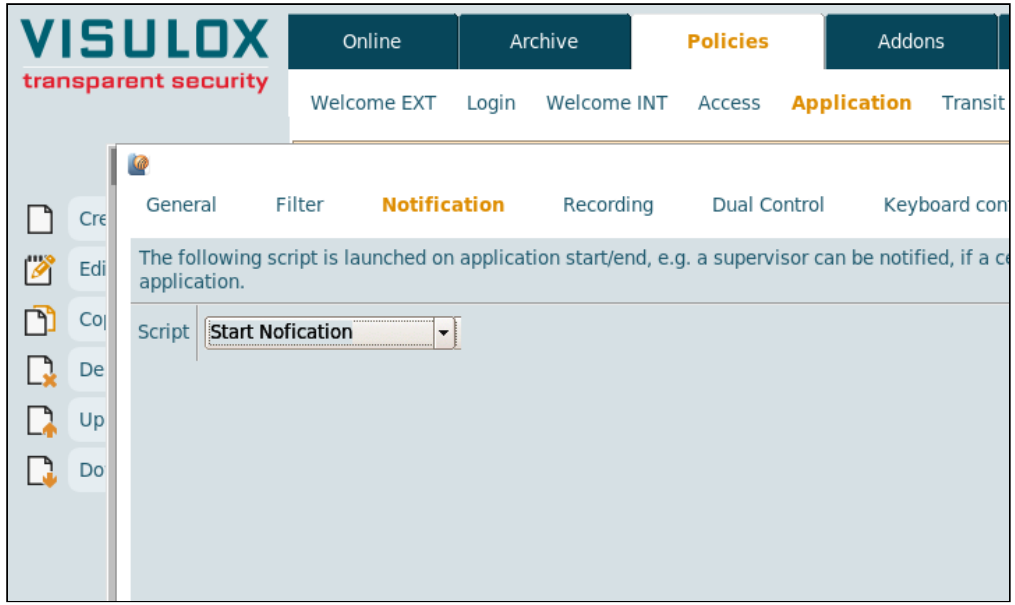
Setting the filter:



The notification will only be send for the "**VLX Jump Shell**" application from user "**Miller**" in this example.

It is also possible to set a filter for the Remote IP address or the Access point (not used in this example).

Selecting the notification script:



As notification script, the script created in the first step should be selected: "**Start Notification**".

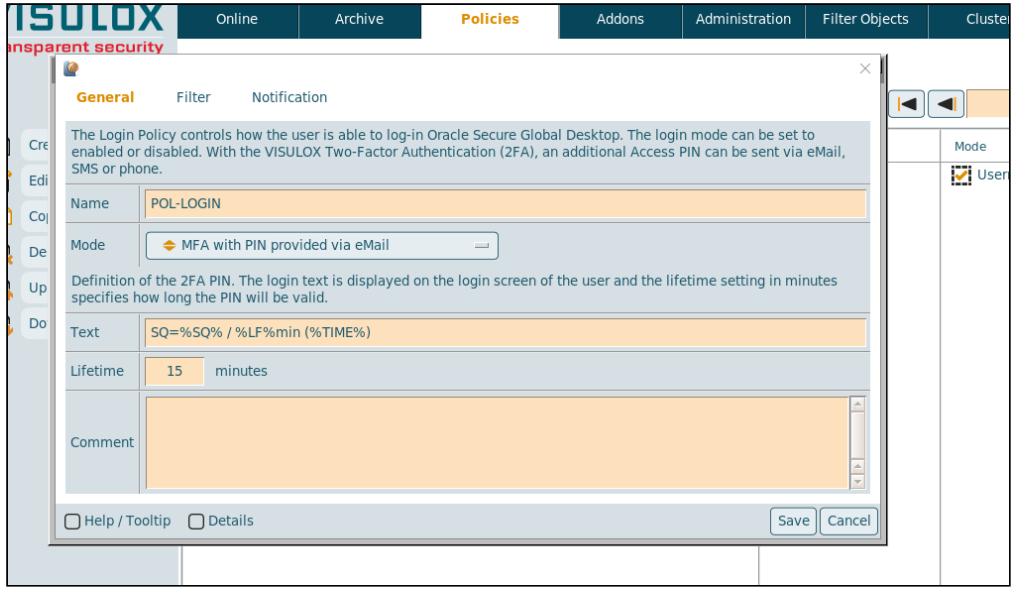
Now user Miller starts the "**VLX Jump Shell**" application from his Workspace and the notification eMail is sent to supervisor Master:

The eMail with the notification is sent to supervisor Master as registered in the script.

The displayed information is based on the created script in the first step.

Example 2: PIN notification for user Miller

Creating a new Login Policy in Cockpit:



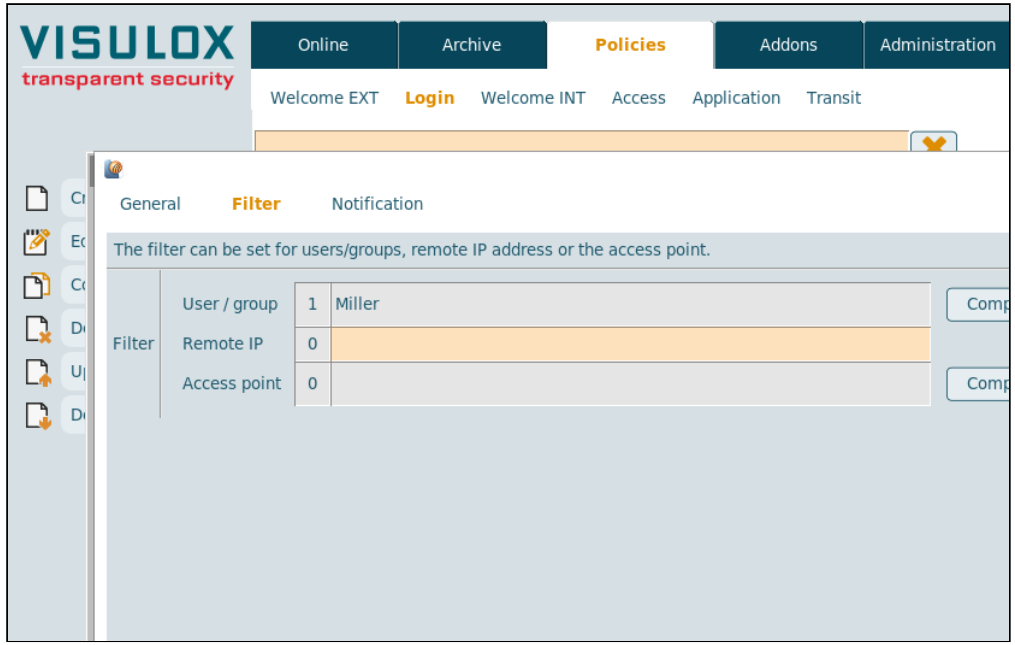
A unique name for the policy must be entered: "**POL-LOGIN**".

The Policy mode can be chosen from a dropdown list: "**MFA with PIN provided via eMail**".

The sequence number, the lifetime and the time will be displayed on the login mask of the user.

The default settings are fine for this example. A comment for the policy can be entered as well.

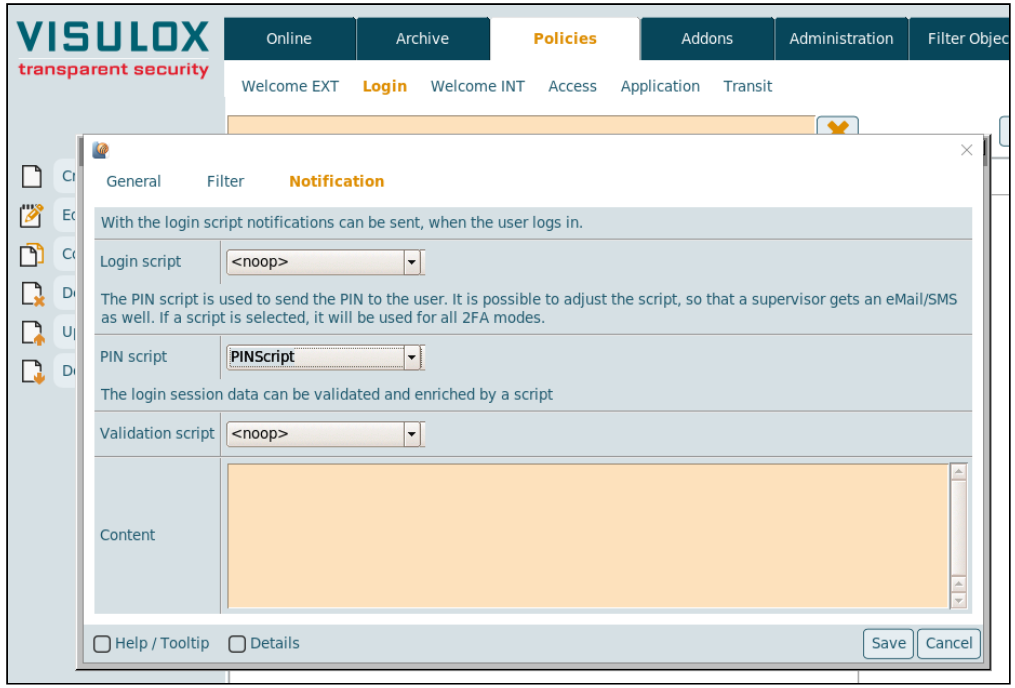
Setting the filter:



Filter is set to "**Miller**" for all examples.

Additional filters can be set based on the Remote IP address or on the access point and a login limit can be set (not used in this example).

Selecting the PIN script:



With the Login script, notifications can be sent to the supervisor (Not used in this example).

The created script ("**PINScript**") should be used to send the PIN notification to user Miller.

After saving the new Login Policy, it will be shown on top of the existing entries. The first Login Policy, that matches the filter criteria will be used.

User Miller logs into VISULOX PORTAL with 2FA active - eMail with Access PIN is sent to Miller:

[TOKEN] Sequence number 84644 (sendpin)
mpro@mp-ol6u3-devel.localdomain
Gesendet: 12:37
An: "mp@amitego.com" <mp@amitego.com> , mp@amitego.com
Hello Miller (o=VISULOX Examples/cn=Miller)
Your PIN is: [8QK-U2S-9MG]
It is valid until 12:52 (15m)

The eMail with the Access PIN is sent to the eMail address of user Miller, that is registered in VISULOX PORTAL.

The displayed information is based on the created script ("**PINScript**") in the first step.

Notifications check list and additional tests

Feature	Expected behaviour	Comment
Policy mode: disabled	• Application Policy has no effect, the next Policy, that matches will be used	
Filter settings (Depending on the notification)	• User/group mask: all registered users are recorded • Application mask: all registered applications will be recorded • Remote IP mask: all users connecting from the registered IP are recorded • Access point mask: all users connecting over the registered access point are recoded	

Feature	Expected behaviour	Comment
Notifications	• Notification sent on login / PIN sent on login • Notification sent, when access is requested • Notification sent on application start/stop • Notification sent, when keyword is detected • Report sent via eMail	
Scripts	• eMail is sent to the address used in the script • eMail is sent to the registrered address of the user in datastore, if the %VLXEMAIL% variable is used	
Script variables	• All listed variables are showing the correct values in the sent eMail • The dump script shows all available varaibles	

Variables in notifications

The following list contains some useful examples for script variables.
To get the complete list of available variables for a certain action script, the dump script should be used.

Variable	Description	Category
VLXACCESSPOINT	VISULOX Access Point used for login	ALL
VLXAPPLICATION	Workspace or application	ALL

Variable	Description	Category
VLXAPPLICATIONSHORT	Short form of the application	ALL
VLXAPPLICATIONCOMMAND	Application command	APPLICATION
VLXAPPLICATIONHOST	Application host	APPLICATION
VLXAPPLICATIONID	Workspace or application ID	ALL
VLXBADWORD	Detected keyword	APPLICATION
VLXCLIENTIP	IP address of the client	ALL
VLXCREATEDBY	Created by	ALL
VLXCREATETIMEMS	Create time	ALL
VLXCREATETIME_FMT	Create time (human readable)	ALL
VLXUPDATEDBY	Updated by	ALL

Variable	Description	Category
VLXUPDATETIMEMS	Update time	ALL
VLXUPDATETIME_FMT	Update time (human readable)	ALL
VLXEMAIL	eMail of the user	ALL
VLXEVENT	Event name	ALL
VLXEVENTINFO	Event information	ALL
VLXFULLNAME	Full name of the user	ALL
VLXGROUPLIST	Groups of the user	ALL
VLXLANG	Set language of the user	ALL
VLXLISTHASH	VISULOX session hash	ALL
VLXLOG	Log path	ALL

Variable	Description	Category
VLXLOGINSCRIPT	Login script	APPLICATION
VLXLOGINUSER	Login user	APPLICATION
VLXOWNER	Owner of the session	ALL
VLXOWNERSHORT	Short form of the owner	ALL
VLXPATH	VISULOX path	APPLICATION
VLXPOLICY	VISULOX policy	APPLICATION
VLXPIN / VLXPIN_FMT	Access PIN of the user	PIN
VLXPIN_EXPIRATIONTIME	Time until Access PIN expires	PIN
VLXPIN_LIFETIME	Lifetime of the Access PIN	PIN
VLXPIN_SEQUENCE	Sequence number of the Access PIN	PIN

Variable	Description	Category
VLXPIN_TEXT	Access PIN Text	PIN
VLXREMOTEIP	Remote IP of the user	ALL
VLXSESSIONHOST	Logical name of the host, where the session is started	ALL
VLXSESSIONID	VISULOX session ID	ALL
VLXSESSIONMODE	VISULOX session mode	ALL
VLXSESSIONSTARTTIME	Start time of the session	ALL
VLXSESSIONDURATION	Duration of the session	ALL
VLXSESSIONDURATION_FMT	Duration of the session (readable)	ALL
VLXSESSIONENDTIME	Endtime of the session	ALL
VLXSESSIONENDTIME_FMT	Endtime of the session (readable)	ALL

Variable	Description	Category
VLXSURNAME	Surname of the user	ALL
VLXTICKETID	VISULOX Ticket ID	APPLICATION
VLXUSERPROFILE	User profile	ALL
VLXUTIL	Path to VISULOX utils directory	ALL
VLXWEBTOPBASE	Workspace base URL	ALL
VLXMANAGER	Responsible manager for the user	ALL
VLXREPOSITORY	User repository	ALL
VLXFILETRANSFERINFO	File Transfer information	TRANSIT ZONE

All variables for times are displayed either as an integeger value or with the ending **_FMT** in a human readable format.

If the eMail address of the manager is needed, this can be done inside the notification script:

How to get the manager`s email address

```
$VLXUTIL/ldap.tcl -source $VLXREPOSITORY -filter $VLXMANAGER -field mail -format csv |  sed -n '2p'
```

23.1.28 How to enable, configure and use MFA

General

VISULOX MFA enriches the standard VISULOX PORTAL authentication layer to change the behaviour of the one factor authentication process (username, password) to a multi factor process (username, password / random-pin). Every time the user tries to login, a new PIN is generated. The PIN is randomly chosen and unique.

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

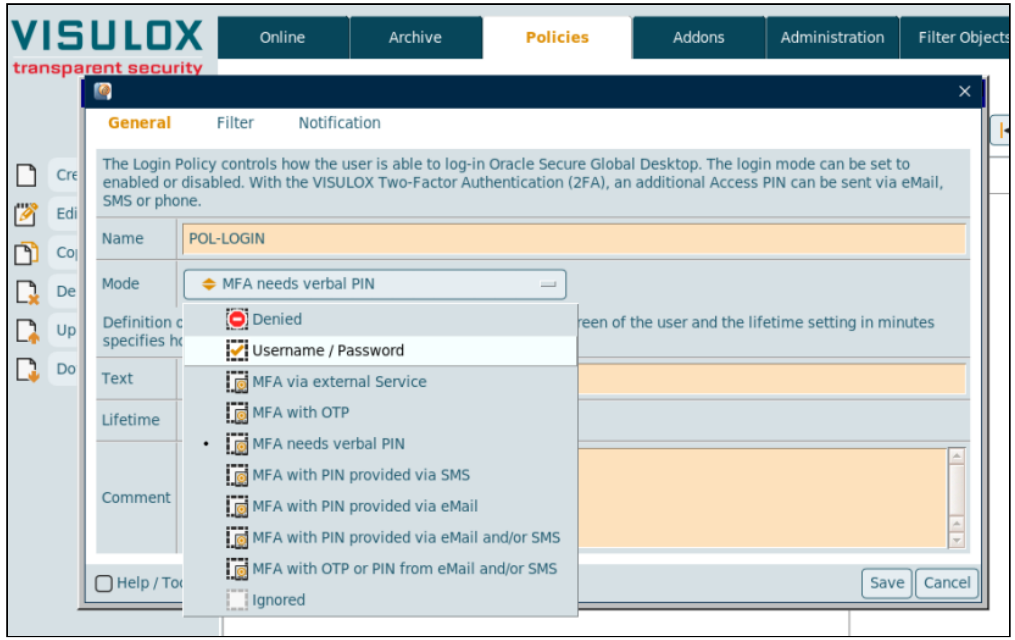
User	Role	eMail	SMS	Application
Master	Supervisor	*<supervisor>*@*company*.com	-	VISULOX Cockpit
Miller	User	*<user>*@*company*.com	*<user SMS via LDAP>*	-

Supervisor Master enables and configures the MFA login.

User Miller logs into VISULOX PORTAL with MFA authentciation enabled.

Supervisor Master: Enable MFA for Miller

Creating a new Login Policy in Cockpit:



A unique name for the policy must be entered: "**POL-LOGIN**".

The Policy mode can be chosen from a dropdown list.

The sequence number, the lifetime and the time will be displayed on the login mask of the user.

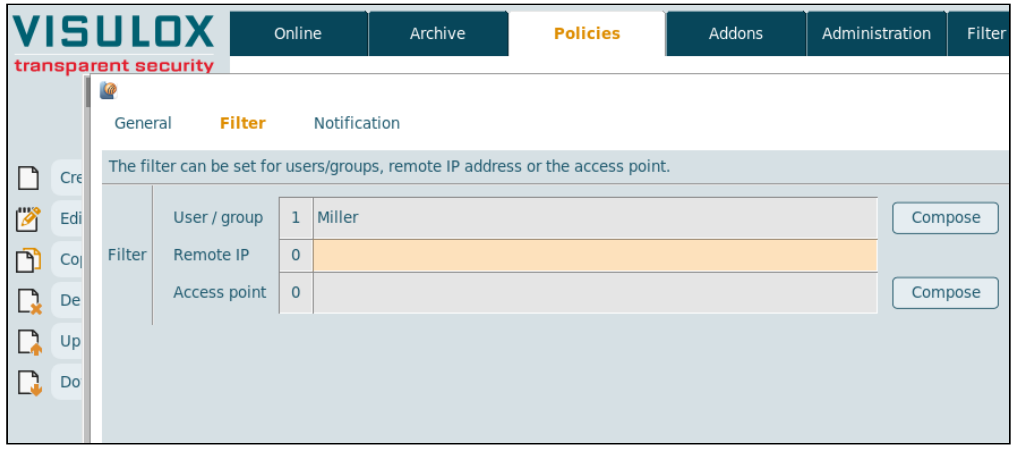
The default settings are fine for this example. A comment for the policy can be entered as well.

Selecting the policy Login mode:

- Example 1: Login is allowed with verbal token
- Example 2: Login is allowed with token provided via eMail

- Example 3: Login is allowed with token provided via SMS
  See: How to setup MFA with SMS response from the SMS Provider

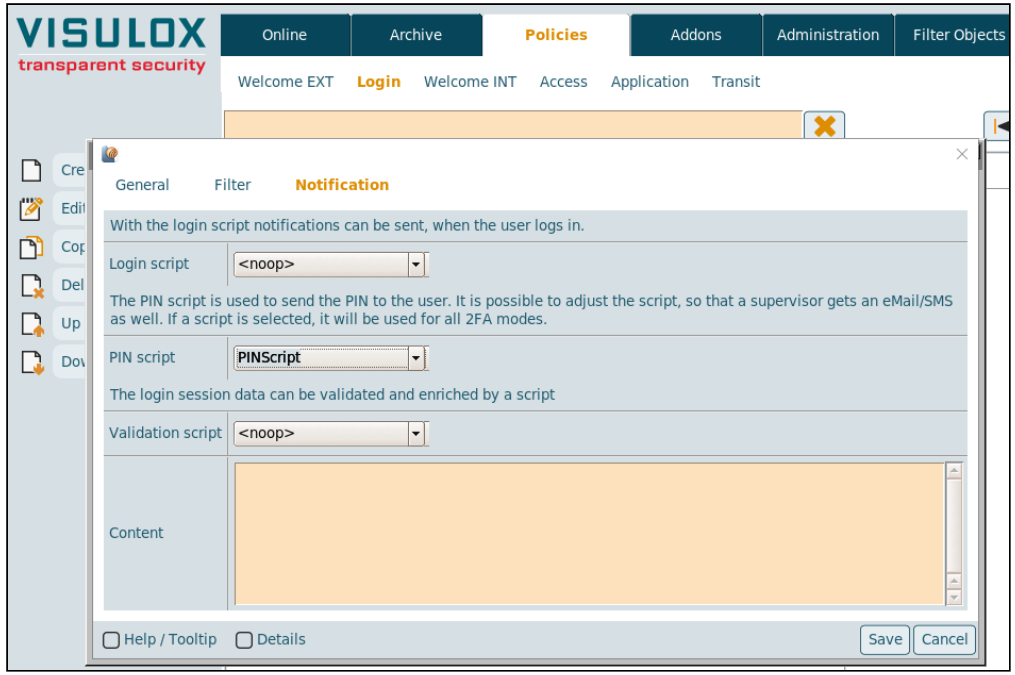
Setting the filter:



Filter is set to "**Miller**" for all examples.

Additional filters can be set based on the Remote IP address or on the access point (not used in this example).

Selecting the script:



With the Login script, notifications can be sent to the supervisor (Not used in this example).

The default "**PINScript**" can be used to send the PIN notification to user Miller.

It is also possible to adjust the PIN script, so that a supervisor gets an eMail/SMS as well (See: Action script interface & variables).

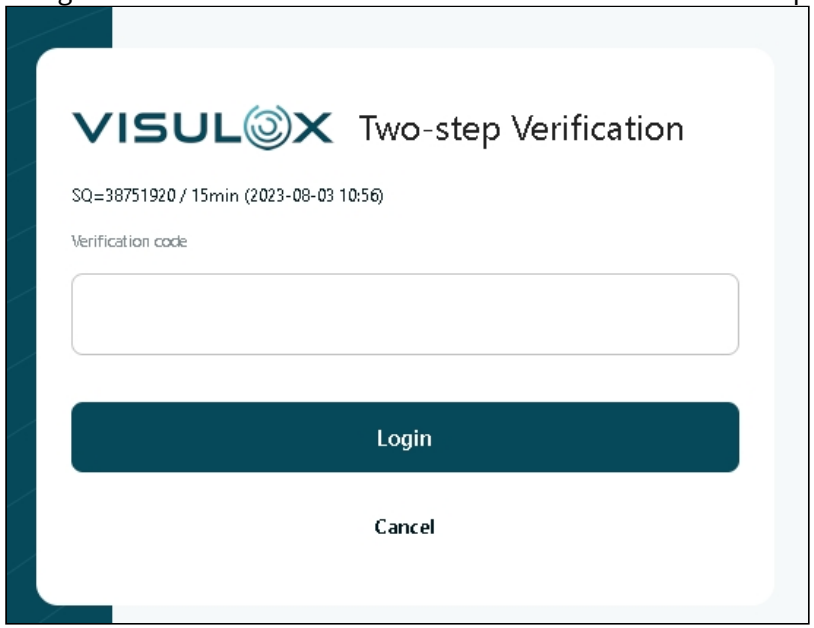
If a script is selected, it will be used for **all** MFA modes.

After saving the new Login Policy, it will be shown on top of the existing entries. The first Login Policy, that matches the filter criteria will be used.

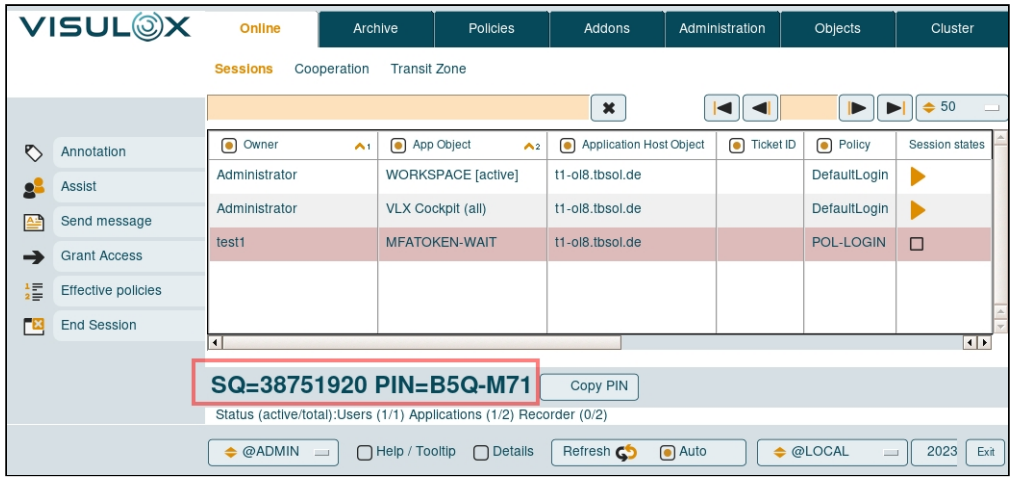
Example 1: Miller logs into VISULOX PORTAL with verbal token

1. Miller tries to login with his credentials and needs an additional PIN to login:

   The generated PIN is valid for 15 Minutes and Miller has to call supervisor Master to request the PIN for SQ=38751920.



2. Supervisor Master receives the call from Miller and opens his Cockpit:



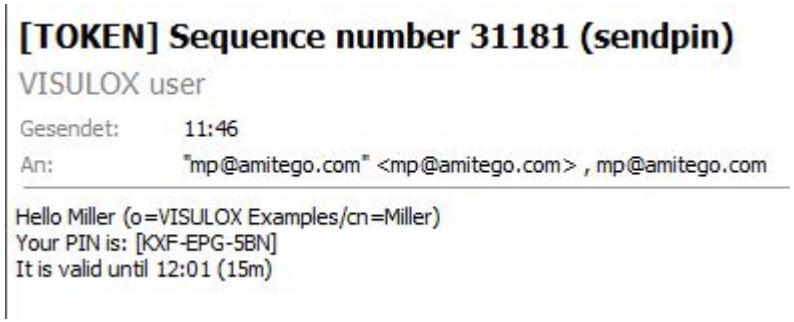
Master selects the session from Miller ("**Wait for Token**") and the sequence number with the according valid PIN is displayed.
Master provides the PIN verbally.
(With the "**Copy PIN**" button, the user and the sequence number will be copied to clipboard and can also be used in an eMail.)

3. Now Miller is able to login with his credentials and the PIN (Here: "**B5Q-M71**").

Example 2: Miller logs into VISULOX PORTAL with PIN provided via eMail

1. Miller tries to login with his credentials and needs an additional PIN to login.

2. Miller receives the eMail with his PIN shortly after he has tried to login:



The default PIN script displays the sequence number in the subject.
The name of the user, the PIN and how long the PIN is valid is shown in the eMail text.

3. Now Miller is able to login with his credentials and the PIN.

Example 3: Miller logs into VISULOX PORTAL with token provided via SMS

1. Miller tries to login with his credentials and needs an additional PIN to login.
2. Miller receives the SMS with his PIN shortly after he has tried to login.
3. Now Miller is able to login with his credentials and the PIN.

MFA check list with additional tests

Feature	Expected behaviour	Comment
Login is allowed	• User can login with his credentials, without the need of entering an additional MFA PIN	
Login allowed with verbal token	• After first login try, the login mask with PIN field and Sequence number + time is displayed • Session is displayed in Cockpit with "Wait for Token" • User is able to log in with his credentials and the valid requested PIN • User can not log in, if the PIN is no longer valid (timed out) • If the wrong or timed out PIN is entered, the correct error message is displayed • If the time of the PIN has run out, the session with "Wait for Token" disappears	
Login is allowed wiith token provided via eMail	• After first login try, the login mask with PIN field and Sequence number + time is displayed • Session is displayed in Cockpit with "Wait for Token" • User receives the eMail with the correct PIN • User is able to log in with his credentials and the valid PIN • User can not log in, if the PIN is no longer valid (timed out) • If the wrong or timed out PIN is entered, the correct error message is displayed • If the time of the PIN has run out, the session with "Wait for Token" disappears	

Feature	Expected behaviour	Comment
Login is allowed with token provided via SMS	• After first login try, the login mask with PIN field and Sequence number + time is displayed • Session is displayed in Cockpit with "Wait for Token" • User receives the SMS with the correct PIN • User is able to log in with his credentials and the valid PIN • User can not log in, if the PIN is no longer valid (timed out) • If the wrong or timed out PIN is entered, the correct error message is displayed • If the time of the PIN has run out, the session with "Wait for Token" disappears	
Login is allowed wiith token provided via eMail and/or SMS	• After first login try, the login mask with PIN field and Sequence number + time is displayed • Session is displayed in Cockpit with "Wait for Token" • User receives the SMS with the correct PIN • User receives the eMail with the correct PIN • User is able to log in with his credentials and the valid PIN • User can not log in, if the PIN is no longer valid (timed out) • If the wrong or timed out PIN is entered, the correct error message is displayed • If the time of the PIN has run out, the session with "Wait for Token" disappears	
Login is not allowed	• After first login try, not allowedmessage is displayed in the login mask	
Disabled	• Login Policy has no effect, the next Policy, that matches will be used	
Filter settings	• User/group mask: all registered users get the PIN login mask • Remote IP mask: all users connecting from the registered IP get the PIN login mask • Access point mask: all users connecting over the registered access point get the PIN login mask	

Feature	Expected behaviour	Comment
PIN definition	• Changing the login text, e.g. "PIN sent via eMail - SQ=%SQ% / %LF%min (%TIME%)" • New message is displayed in the login mask correctly • Adjusting the MFA Token lifetime	
Notification	• Selecting a notification script to inform the supervisor, when user logs in (See: How to create and use notifications) • Adjusting the PIN script, using more possible variables (See: How to create and use notifications)	
Events	• All MFA information is displayed in the Cockpit	

23.1.29 How to enable, configure and use cooperations

Overview

A cooperation is useful to work together with the same view on one application. In a cooperation is always the owner of the application and a cooperation partner. A cooperation partner is a participant, who can look at what the owner is doing (observe) or he can use keyboard and mouse as well (interact).

In observe mode the cooperation partner has a special mouse pointer with his name, which is seen by the owner. With this mouse pointer the partner can point on objects inside an application, without disturbing the application owner.

Assistance

An assisting cooperation is started by a supervisor, selecting a running session and using the "**Assist**" button in the Cockpit. The user is the owner of the application and he is able to control or close the cooperation.

Dual Control

With the Dual Control feature a cooperation can be established based on a real four-eye-principle. The supervisor has to acknowledge the cooperation within a configured period of time. If the supervisor does not acknowledge the cooperation, the cooperation window will be locked for the participant.

With Dual control it is guaranteed, that the supervisor is always in front of the screen.

In **Dual Control observe and assist** mode it is possible for an additional assisting user to join a Dual Control cooperation in observe mode.

- Example: Assistance
- Example: Dual Control

Example: Assistance

General

An assisting cooperation is started by a supervisor, selecting a running session and using the "**Assist**" button in the Cockpit.

The user is the owner of the application and he is able to control or close the cooperation.

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

User	Role	eMail	SMS	Application	Other
Master	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	-
Miller	User	*<user>@company*.com	-	VLX Jump Shell	-

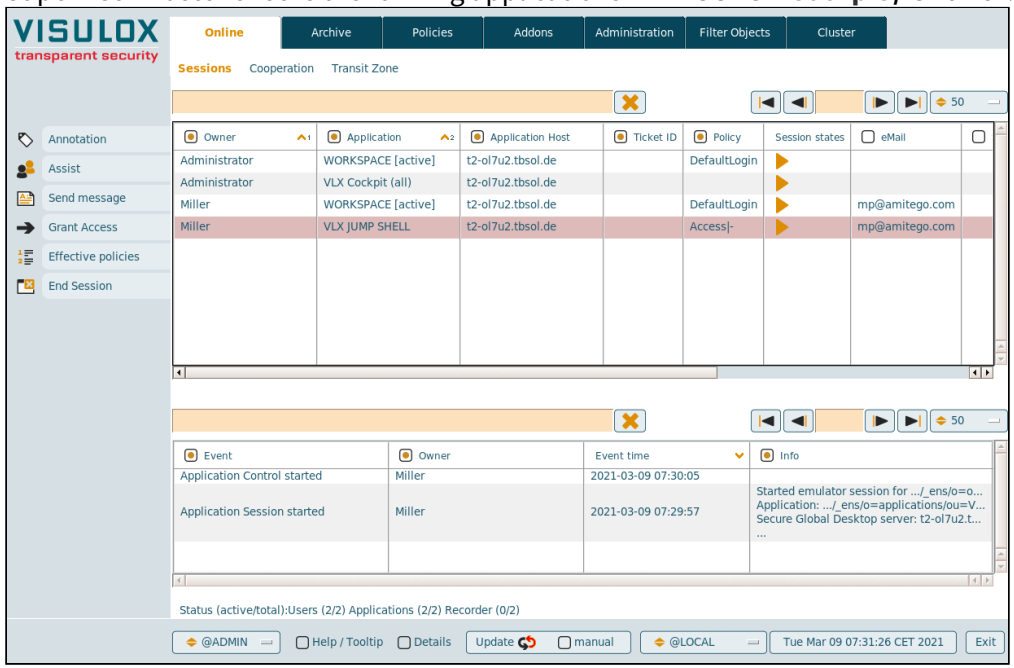
Supervisor Master initiates the Assistance.

User Miller logs into VISULOX PORTAL and starts an application for the Assistance.

Assistance on a running session in the VISULOX Cockpit

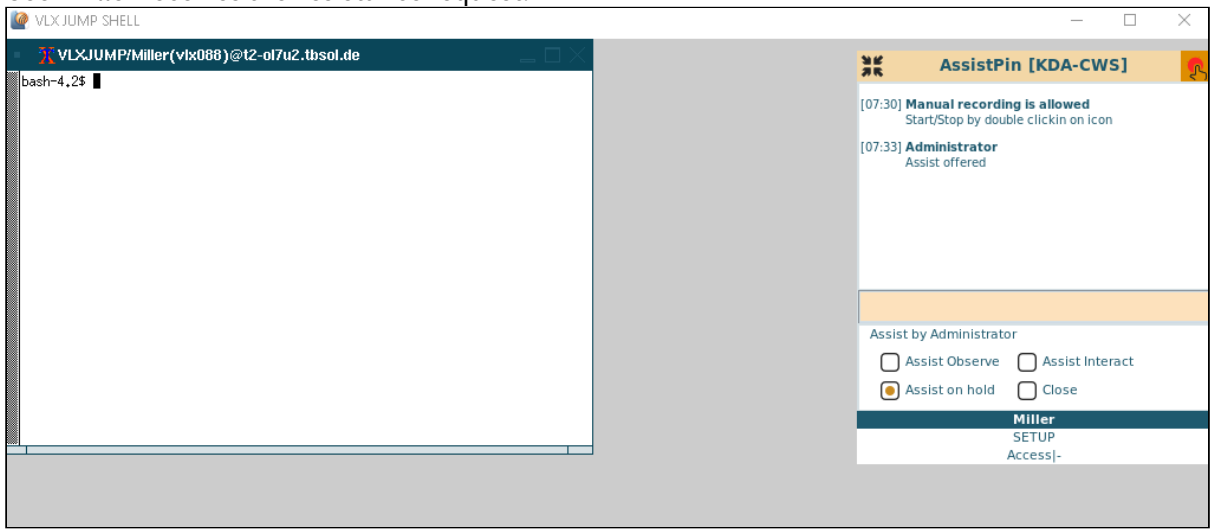
1. User Miller starts the "**VLX Jump Shell**" application from his Workspace

2. Supervisor Master checks the running applications in "**VISULOX Cockpit / Online**":



Master selects the "**VLX Jump Shell**" application from Miller.
With the "**Assist**" button, an Assistance request is sent into the selected application.
Each registered application also has an Assist PIN (4-6 digits), which is displayed in the user's session control panel. If this PIN is provided by the user, it is possible for Master to request access to the application using the "**Assist**" button on the cooperation page.

3. User Miller receives the Assistance request:

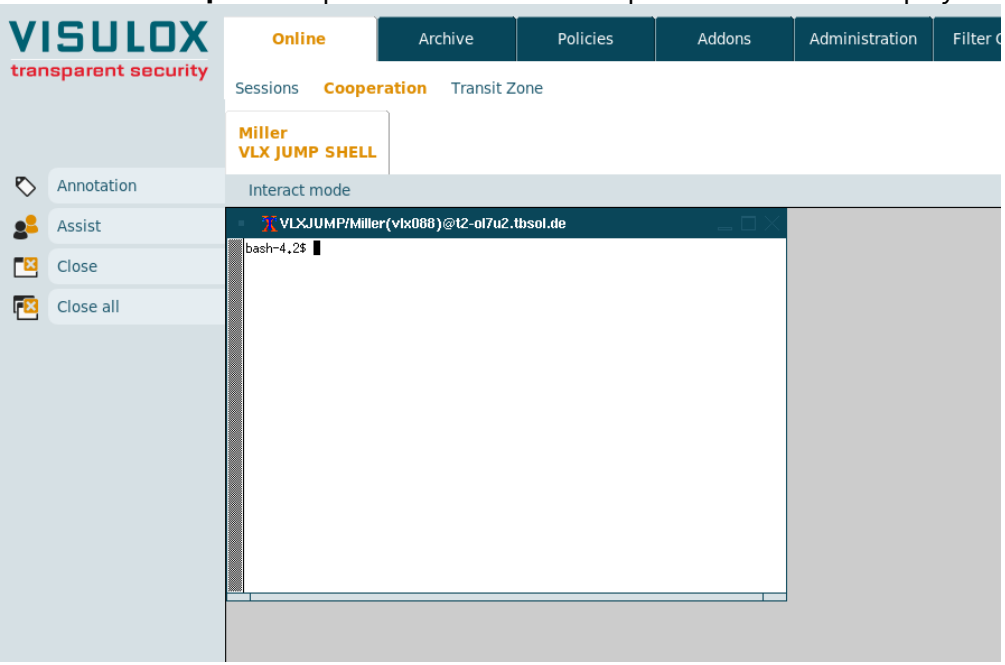


Default mode on start of a Assistance request is "**Assist on hold**".
Miller can now choose the mode for the Assistance:

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

Miller selects "**Assist Interact**" for this example Assistance.

4. In the "**VLX Cockpit**" of Supervisor Miller now a cooperation window is displayed



The mode of the Assistance is displayed above the cooperation window.
In "**Interact**" mode master has full access to the application.

Assistance check list with additional tests

Feature	Expected behaviour	Comment
Assistance	• Assist by selecting an application in VISULOX Cockpit / Online • Assist with provided PIN in VISULOX Cockpit / Online / Cooperation • Supervisor session is in "**on hold**" mode after pressing assist	

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

Events	• In the Cockpit all actions of the cooperation are displayed.	

Example: Dual Control

General

With the **Dual Control** feature a cooperation can be established based on a real four-eye-principle. The supervisor has to acknowledge the cooperation within a configured period of time. If the supervisor does not acknowledge the cooperation, the cooperation window will be locked for the participant.

With Dual Control it is guaranteed, that the supervisor is always in front of the screen.

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

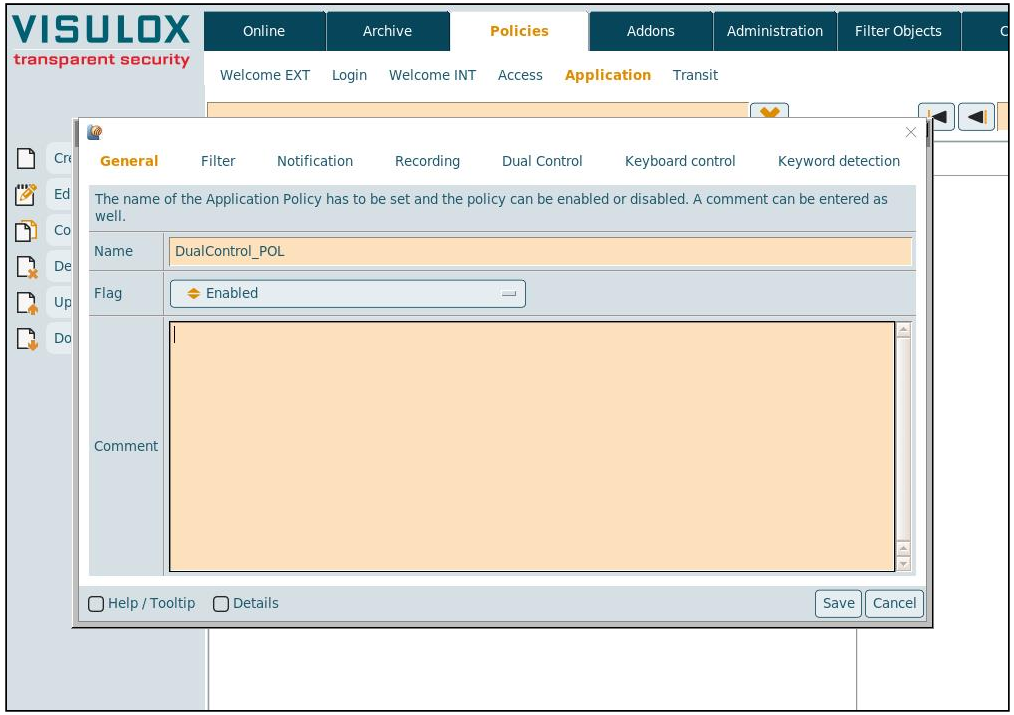
User	Role	eMail	SMS	Application	Other
Administrator	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	-
Miller	User	*<user>@company*.com	-	VLX Jump Shell	-

Supervisor Administrator initiates and configures the Dual Control cooperation.

User Miller logs into VISULOX PORTAL and starts the application for the cooperation..

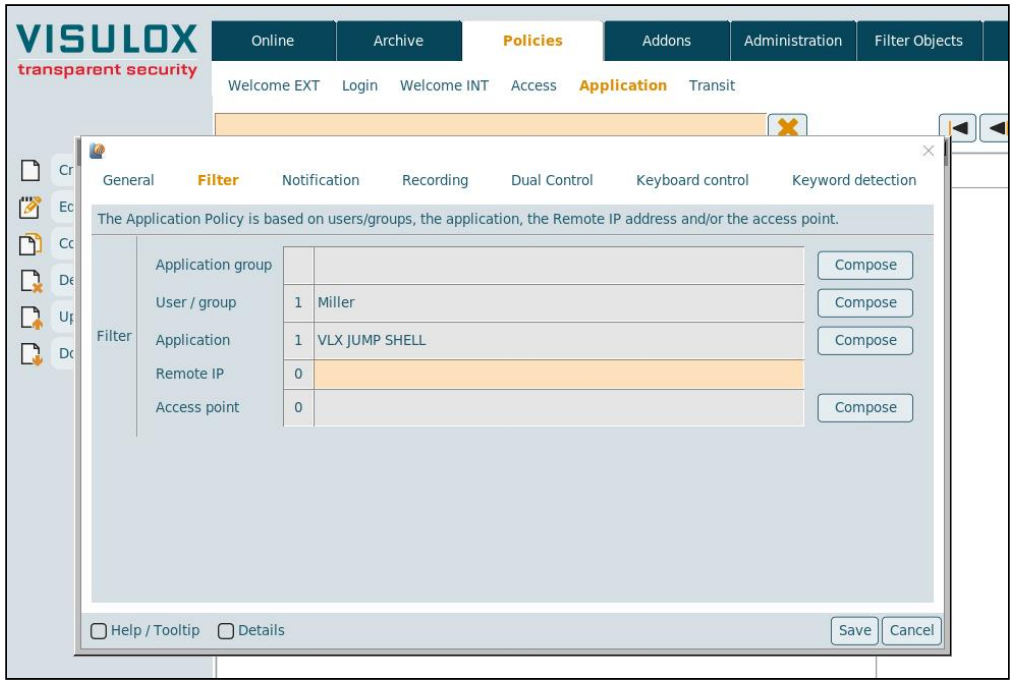
Configuration and start of a Dual Control cooperation

1. Supervisor Master creates a new Application Policy in the "**VLX Cockpit**":



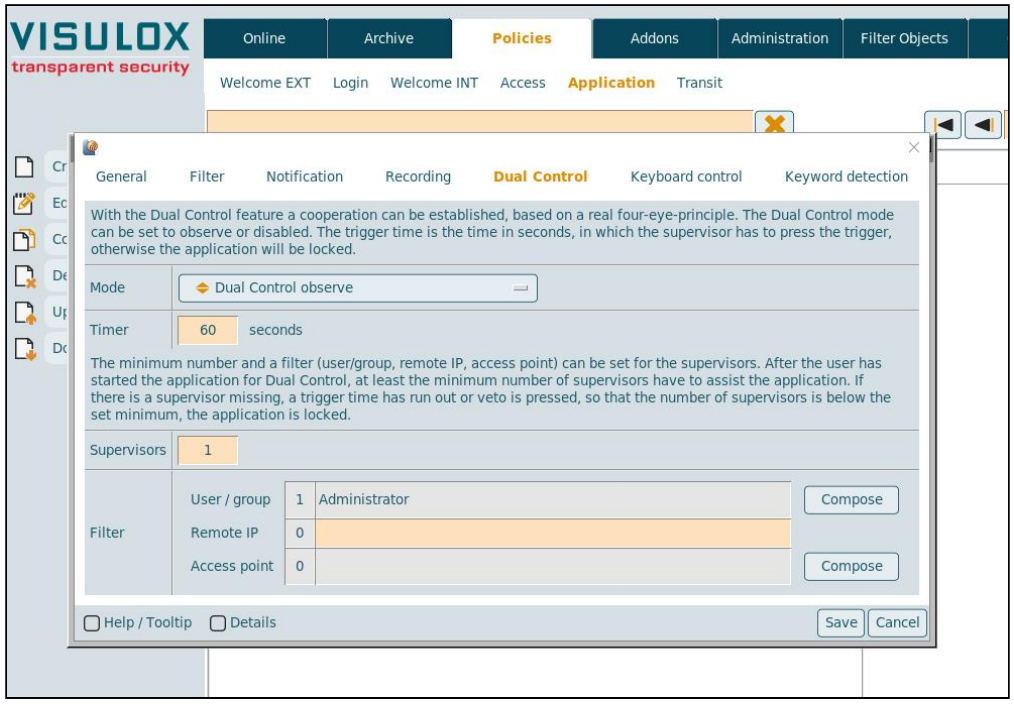
A unique name for the policy must be entered: "**DualControl_POL**".
To use the Application Policy "**Policy Enabled**" has to be selected.
A comment for the policy can be entered as well.

2. Setting the filter:



Only the "**VLX Jump Shell**" application from user "**Miller**" will be used in this example.
It is also possible to set a filter for the application group, the remote IP address or the access point (not used in this example).

3. Configuring Dual Control:



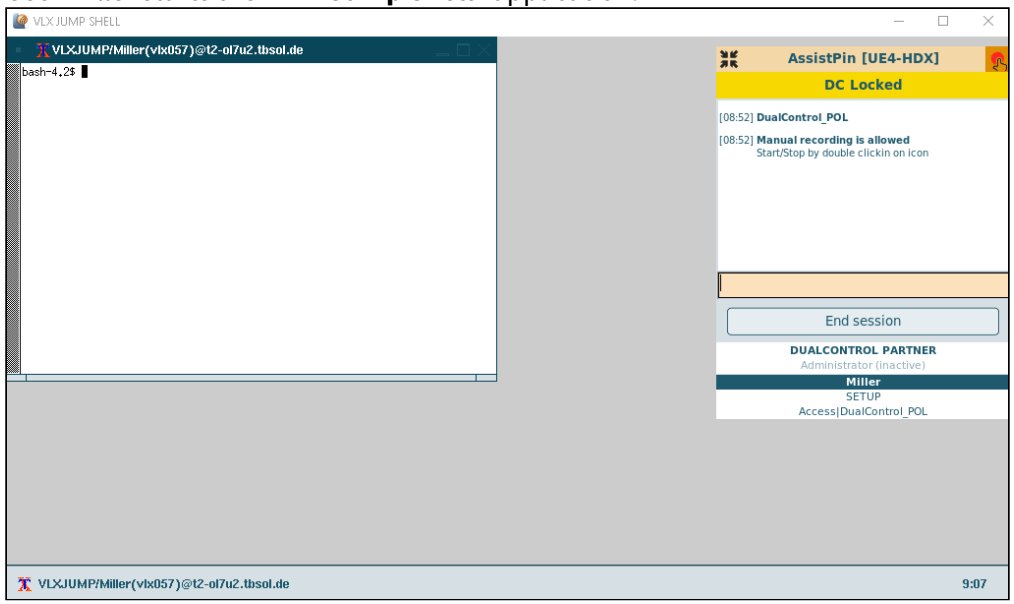
Setting the Dual Control mode:

- **Dual Control disabled**:
  No dual control cooperation possible
- **Dual Control observe**:
  The supervisor is able to see the application and has a mouse pointer with his name, but can not interact
- **Dual Control observe and assist**
  The supervisor is able to see the application and has a mouse pointer with his name, but can not interact. An additional user can be invited in assist observe mode

The supervisor selects "**Dual Control observe**" for this example.

The Dual Control timer can be set: "**60**" seconds is fine. The minimum number of controllers must be set to "**1**" and the filter for the cooperation partner is set to supervisor "**Administrator**".

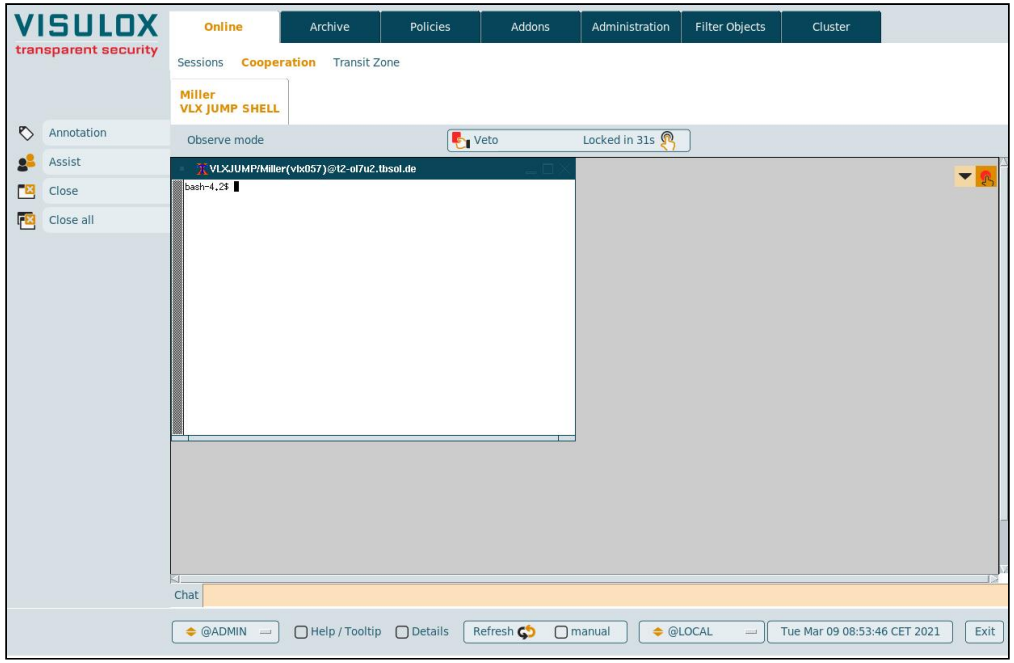
4. User Miller starts the "**VLX Jump Shell**" application:



The application is "**Locked by Dual Control**".
User Miller has to wait for the supervisor to press the trigger.

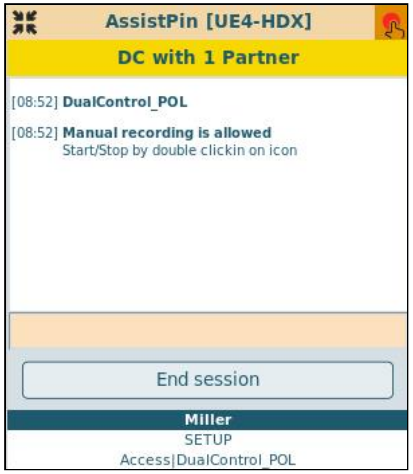
5. The supervisor opens "**VLX Cockpit**" / Online

6. The supervisor selects the "**VLX Jump Shell**" session of user Miller and presses the "**Assist**" button or he enters the provided Assist PIN on the cooperation page:

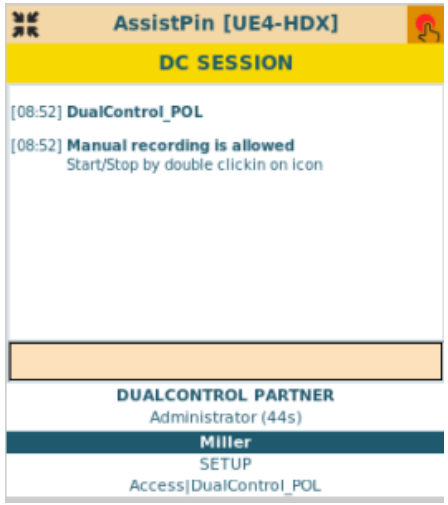


The session is unlocked, once the supervisor has joined the Dual Control cooperation.
The trigger countdown has started.
The supervisor can doubleclick on the trigger to reset the timer.
The supervisor can also use the "**Veto**" button to lock the screen immediately.

7. User Miller can now work with the application and the supervisor is watching in observe mode:

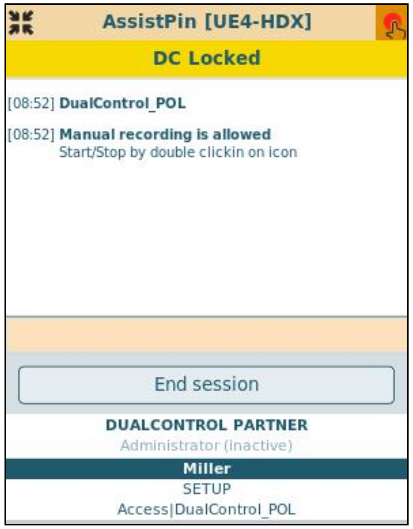


Miller is able to see the current Dual control state



If Master does not press the trigger,

the access to the application is running out.



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

Dual Control check list with additional tests

Feature	Expected behaviour	Comment
Policy mode: disabled	• Application Policy has no effect, the next Policy, that matches will be used	

Feature	Expected behaviour	Comment
Filter settings	• User/group mask: all registered users will use Dual Control • Application mask: all registered applications will be started in Dual Control mode • Remote IP mask: all users connecting from the registered IP will use Dual Control • Access point mask: all users connecting over the registered access point will use Dual Control	
Dual Control	• Dual Control disabled: No Dual Control cooperation possible • Dual Control observe and assist: Additional assisting user can be invited • Dual Control observe: The supervisor is able to see the application and has a mouse pointer with his name, but can not interact	
Dual Control timer	• The entered value is displayed in Dual Control session • Warning is shown, once the trigger time is running out • Session is locked, if the trigger is not pressed in time • Veto: the supervisor can lock the session immediately with the "**Veto**" button	
Minimum number of controllers	• If the set minimum number of controllers is not reached, the application stays locked • Once the number of controllers matches the minimum number, the application is unlocked	
Filter settings Participant	• User/group mask: all registered users are able to use Dual Control cooperations • Remote IP mask: all users connecting from the registered IP are able to use Dual Control cooperations • Access point mask: all users connecting over the registered access point are able to use Dual Control cooperations	

Feature	Expected behaviour	Comment
Dual Control Cooperation	• Supervisor joins Dual Control by using assist on a selected application in Cockpit / Online page • Supervisor joins Dual Control with provided Assist PIN by using assist in Cockpit / Online / Cooperation	
Events	• In the Cockpit all actions of the cooperation are displayed.	

23.1.30 How to enable, configure and use recording

Overview

Recording is a task that is performed in the background and does not affect the user performance. Whenever a session should be recorded (automatically or manually) VISULOX starts a task. This task records the session presentation by using the shadow command.

With applications configured in **Independent Window** mode, the best results of the recordings concerning performance and size can be achieved.

Policy based recording

Policy based recording is the recommended way to use the VISULOX recording feature.

Application based recording via vlxMode parameter

Application based recording is configured via vlxMode parameter in the Environment Variables of the application in the VISULOX PORTAL Console.

Manual recording

Manual Recording can be started by a user within an application via his control panel.

Keyboard recording

With VISULOX keyboard recording it is possible to record the keystrokes entered in an application by a user. Keywords can be defined, that will trigger several options after the keyword has been detected. It is possible to hide the recorded keystrokes in the VISULOX Cockpit, which is very useful, if the user has to enter passwords or other security related information.

- Example: Policy based recording
- Example: Application based recording via vlxMode parameter
- Example: Manual recording
- Example: Keyboard recording
- Recorder configuration

Example: Policy based recording

General

Policy based recording is the recommended way to use the VISULOX recording feature. Role based recording is possible with a variety of filters.

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

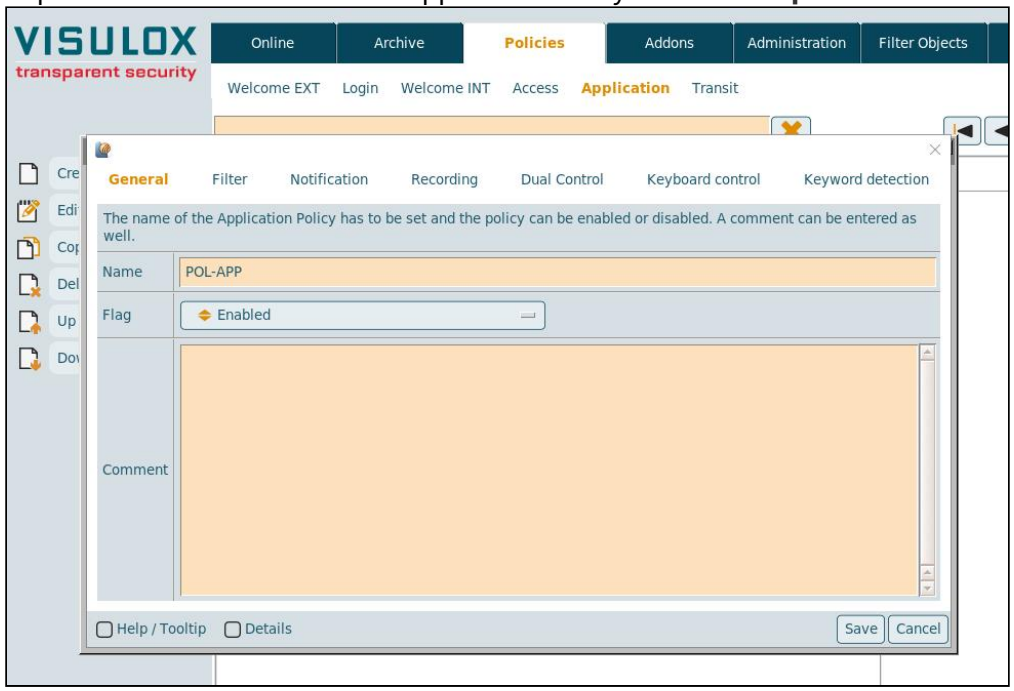
User	Role	eMail	SMS	Application	Other
Master	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	-
Miller	User	*<user>@company*.com	-	VLX Jump Shell	-

Supervisor Master enables and configures policy based recording.

User Miller logs into VISULOX PORTAL and starts the recorded application.

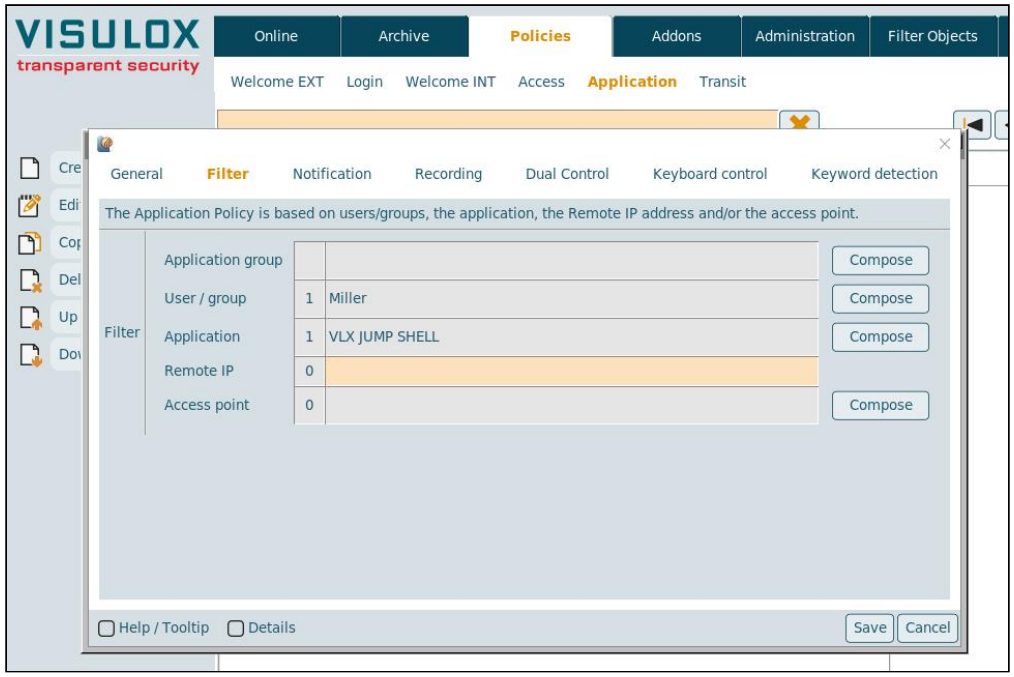
Enable role / policy based recording in the Cockpit

1. Supervisor Master creates a new Application Policy in "**VLX Cockpit**":



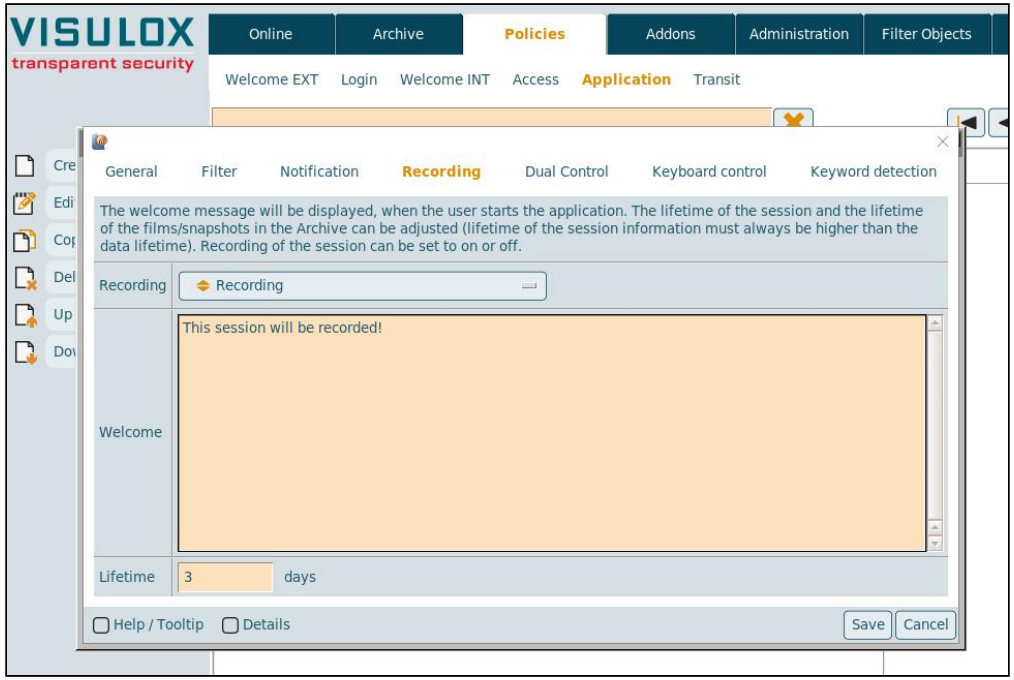
A unique name for the policy must be entered: "**POL-APP**".
To use the Application Policy "**Enabled**" has to be selected.
A comment for the policy can be entered as well.

2. Setting the filter:



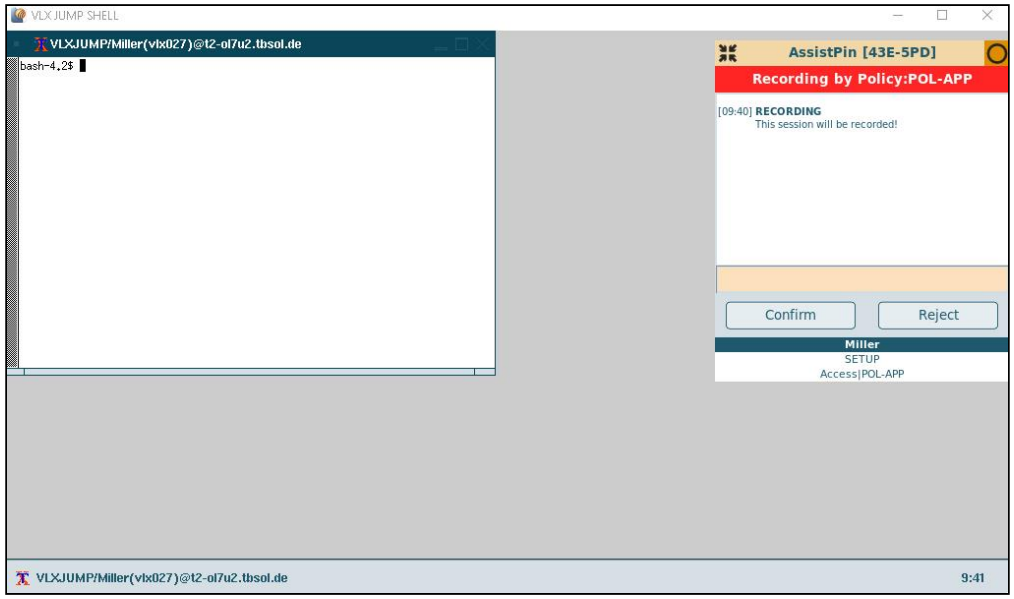
Only the "**VLX Jump Shell**" application from user "**Miller**" will be recorded in this example.
It is also possible to set a filter for the Remote IP address or the Access point (not used in this example).

3. Enable recording:



"**Recording**" must be selected and a Welcome message can be entered. The session lifetime is set to **3** days in this example. The script can be used to send a notification to the supervisor (not used in this example).

4. User Miller starts the "**VLX Jump Shell**" application from his Workspace



Once the application is started the "**Recording by Policy**" box is displayed, locking the application.
Miller can enter an annotation and must confirm the "**Recording by Policy**" box to work with the application.
If Miller rejects, the application will be closed.

Policy based recording check list with additional tests

Feature	Expected behaviour	Comment
Policy mode: disabled	• Application Policy has no effect, the next Policy, that matches will be used	

Feature	Expected behaviour	Comment
Filter settings	• User/group mask: all registered users are recorded • Application mask: all registered applications will be recorded • Remote IP mask: all users connecting from the registered IP are recorded • Access point mask: all users connecting over the registered access point are recoded	
Recording on/off	• Rec on: Recording enabled • Rec off: Recording disabled	
Session lieftime	• Session lifetime information in days. Then the session information will be deleted.	
Notification	• Send notification to supervisor (See: How to create and use notifications)	
Dual Control	• See: How to enable, configure and use cooperations	
Keyboard recording	• See: Example: Keyboard recording	
Expect scripts	• Recording with vlxWindows.exp and vlxUnix.exp (VISULOX based), recorder should start immediately • Recording with windows.exp and unix.exp (Lazy registrated), recorder needs up to 15 sec to start	
Configured recording	• Recording starts and the recorder box is displayed on the screen of the user • Recorder annotation can be entered • Screen is locked until "confirm" button is pressed • With "Reject", the session will be closed	

Feature	Expected behaviour	Comment
Events	• All actions during recording are displayed in the Cockpit.	

Example: Application based recording via vlxMode parameter

General

Application based recording can be configured via **vlxMode** parameter in the **Hints** field of the application via the VISULOX PORTAL Console.

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

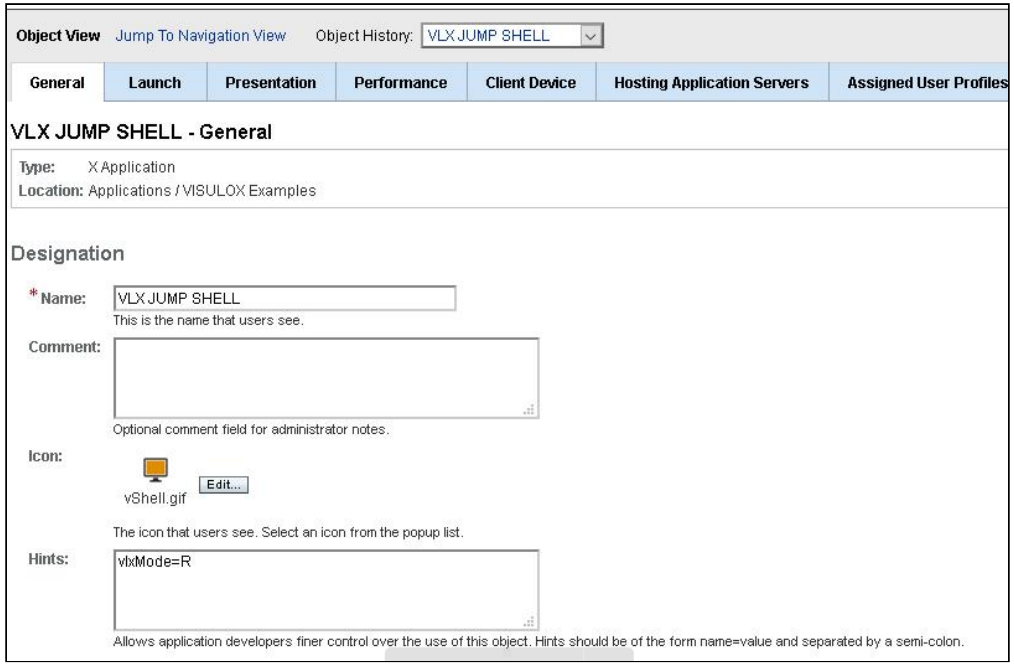
User	Role	eMail	SMS	Application	Other
Master	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	Access to VISULOX PORTAL Console
Miller	User	*<user>@company*.com	-	VLX Jump Shell	-

Supervisor Master enables and configures recording in the VISULOX PORTAL Console.

User Miller logs into VISULOX PORTAL and starts the recorded application.

Application based recording via vlxMode parameter

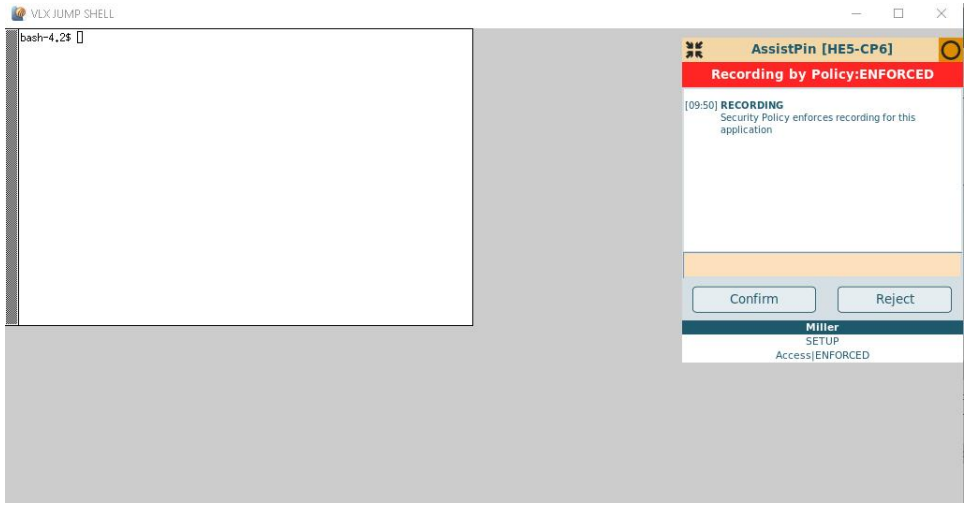
1. Supervisor Master has to adjust the launch parameter of the "**VLX Jump Shell**" application:



In the "**Hints**" field of the application, the vlxMode variable must be entered. For recording: "**vlxMode=R**".

Using the existing VISULOX PORTAL expect scripts (unix.exp, windows.exp, ...) will result in what we call "**lazy registration**".
That means, that the recorder may need up to 15 seconds to be started.

2. User Miller starts the "**VLX Jump Shell**" application from his Workspace



Once the application is started the "**Recording by Policy: Enforced**" box is displayed, locking the application.
Miller can enter an annotation and must confirm the "**Recording by Policy**" box to work with the application.
If Miller rejects, the application will be closed.

Recording check list with additional tests

Feature	Expected behaviour	Comment
Expect scripts	• Recording with vlxWindows.exp and vlxUnix.exp (VISULOX based), recorder should start immediately • Recording with windows.exp and unix.exp (Lazy registrated), recorder needs up to 15 sec to start	
vlxmode variable	• Application based recording with vlxmode=R	

Feature	Expected behaviour	Comment
Configured recording	• Recording starts and the recorder box is displayed on the screen of the user • Recorder annotation can be entered • Screen is locked until "confirm" button is pressed • With "Reject", the session will be closed	
Manual recording	• Start recording on a running application • Entering / selecting a message for the user • Recorder box with message is displayed on the screen of the user. • Recorder annotation can be entered • Screen is locked until "confirm" button is pressed	
Events	• All actions during recording are displayed in the VISULOX Cockpit.	

Example: Manual recording

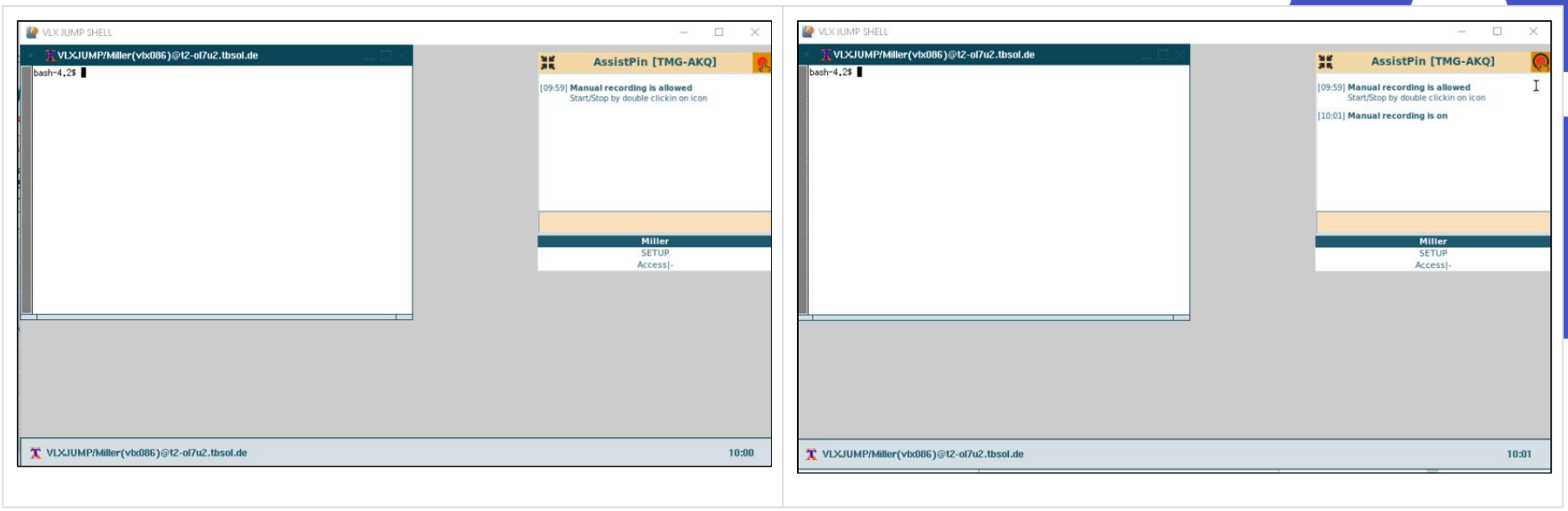
General

Manual Recording can be enabled via control panel by the application user himself.

Manual recording within the application

1. User Miller starts the "**VLX Jump Shell**" application.

2. Miller enables manual recording in his control panel with double click on the recorder icon (upper right corner):



Disable manual recording

The manual recording checkbox in the control panel can be removed to prevent users recording their own sessions.

```
visulox config -name recorder.manually=0
    ------------------------------------------------
    | changed | parameter         |      type | value |
    ------------------------------------------------
    |         | recorder.manually | OPERATION | 0     |
    ------------------------------------------------
```

Manual recording check list with additional tests

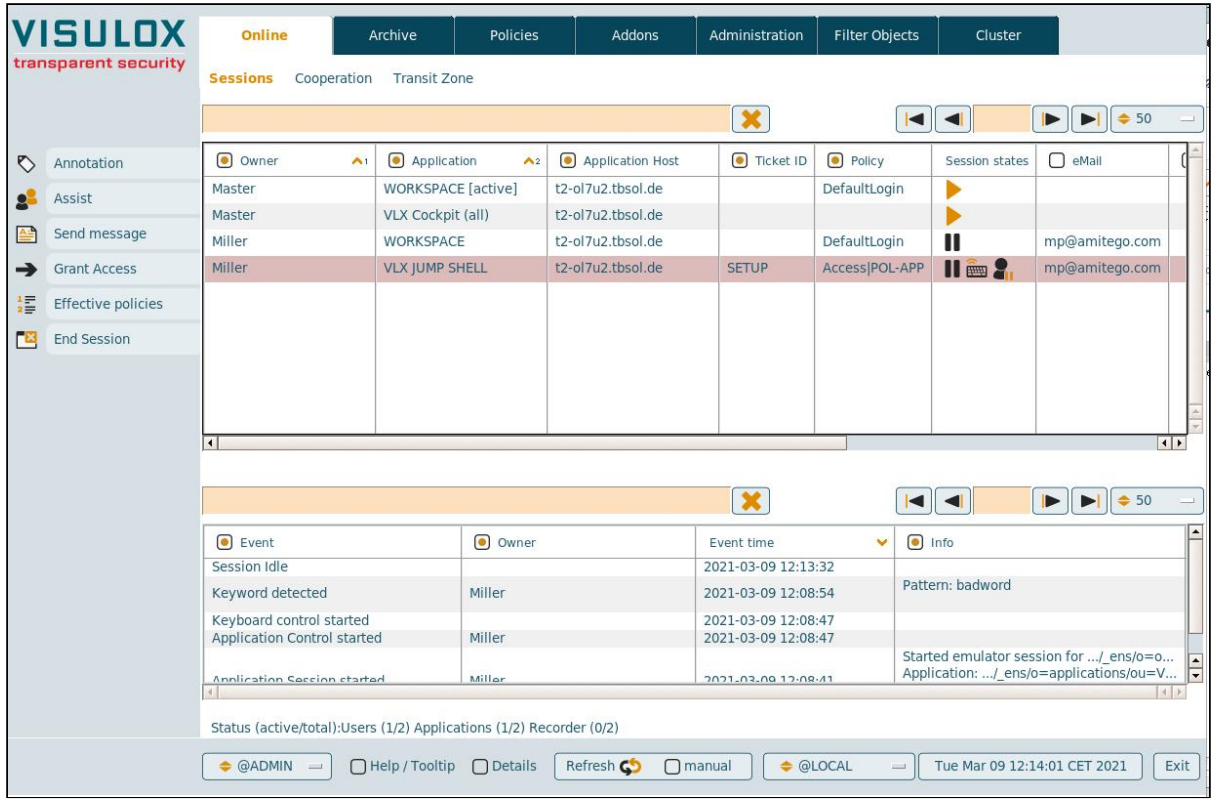
Feature	Expected behaviour	Comment
Manual recording	• Start recording in a running application • Recorder box switches to manual recording on • Annotation can be entered	
Events	• All actions during recording are displayed in the Cockpit • Film can be watched in the browser based player, once the first chapter is written	

Example: Keyboard recording

General

With VISULOX keyboard recording it is possible to record the keystrokes entered in an application by a user. Keywords can be defined, that will trigger several options after the keyword has been detected. It is possible to hide the recorded keystrokes in the VISULOX Cockpit, which is very useful, if the user has to enter passwords or other security related information.

> If recorded keystrokes are hidden in the VISULOX Cockpit, the keystrokes are hidden in reports generated with this Cockpit as well.



Keep in mind, that keyboard recording does not prevent entering certain commands. Keyboard recording detects keywords and provides some actions after the detection (nearly in real time).

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

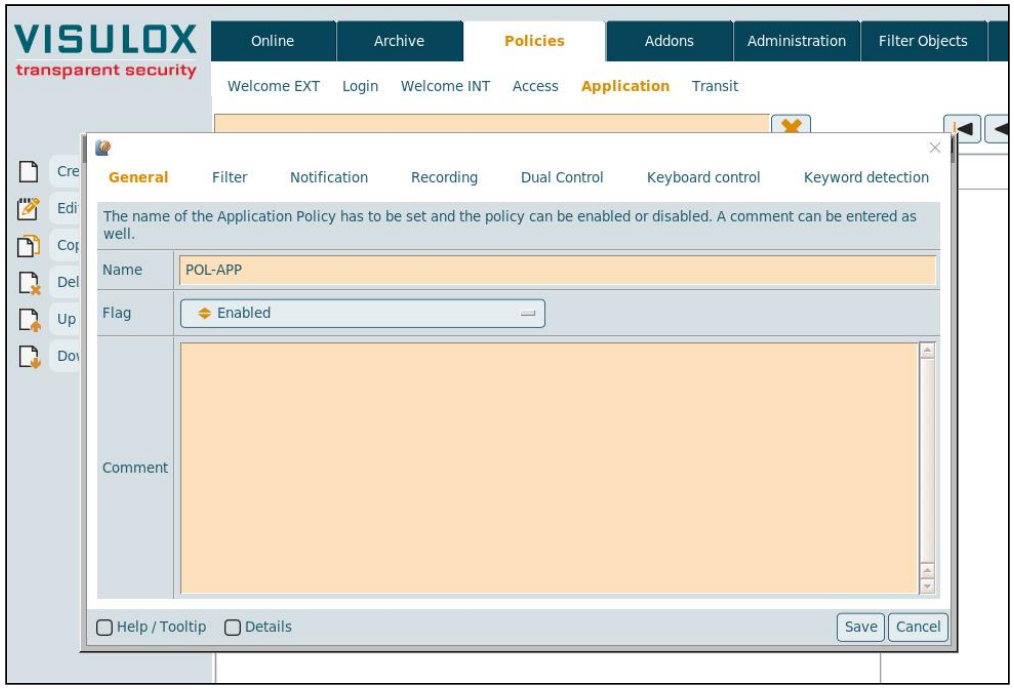
User	Role	eMail	SMS	Application	Other
Master	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	-
Miller	User	*<user>@company*.com	-	VLX Jump Shell	-

Supervisor Master enables and configures keyboard recording.

User Miller logs into VISULOX PORTAL and starts an application to enter some commands.

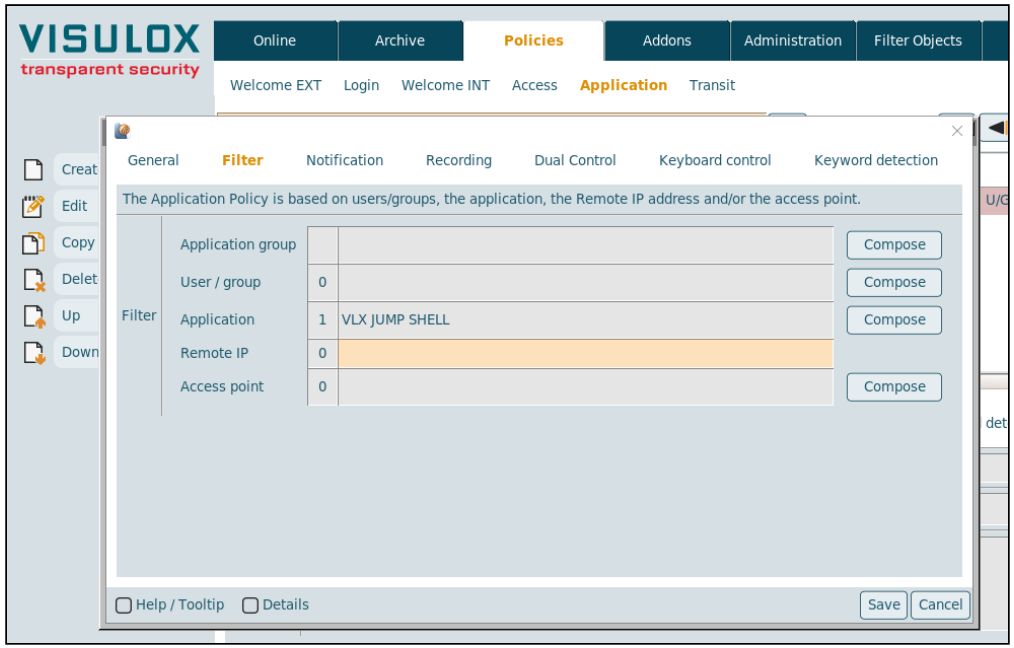
Configuration of keyboard recording

1. Supervisor Master creates a new Application Policy in "**VLX Cockpit**":



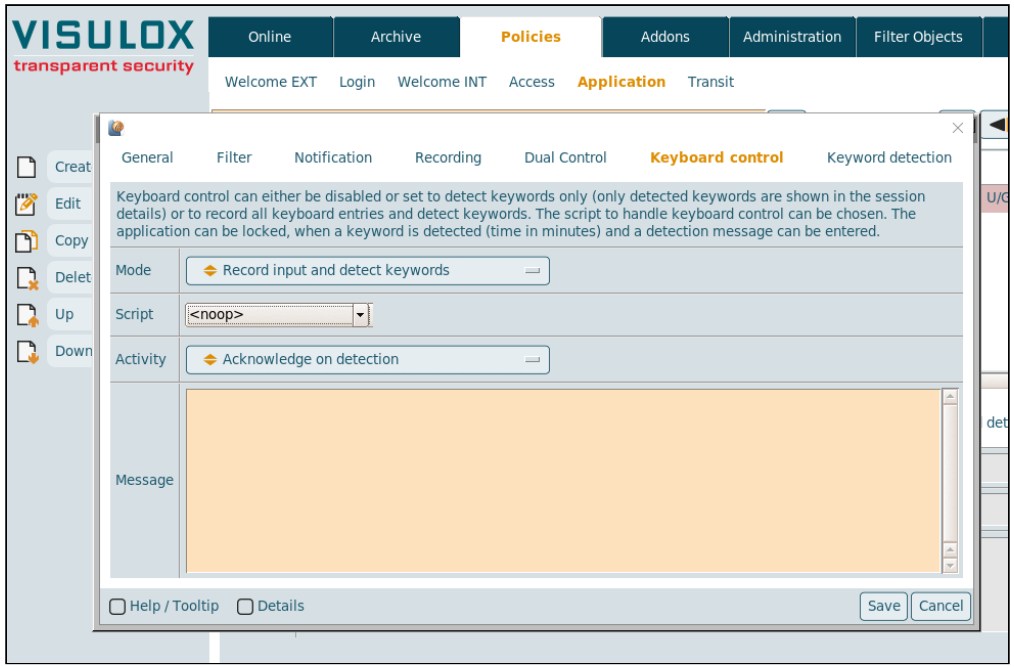
A unique name for the policy must be entered: "**POL-APP**".
To use the Application Policy "**Enabled**" has to be selected.
A comment for the policy can be entered as well.

2. Setting the filter:



Only the "**VLX Jump Shell**" application will be used for keyboard recording in this example.
It is also possible to set a filter for the application group, the remote IP address or the access point (not used in this example).

3. Configuring keyboard control:



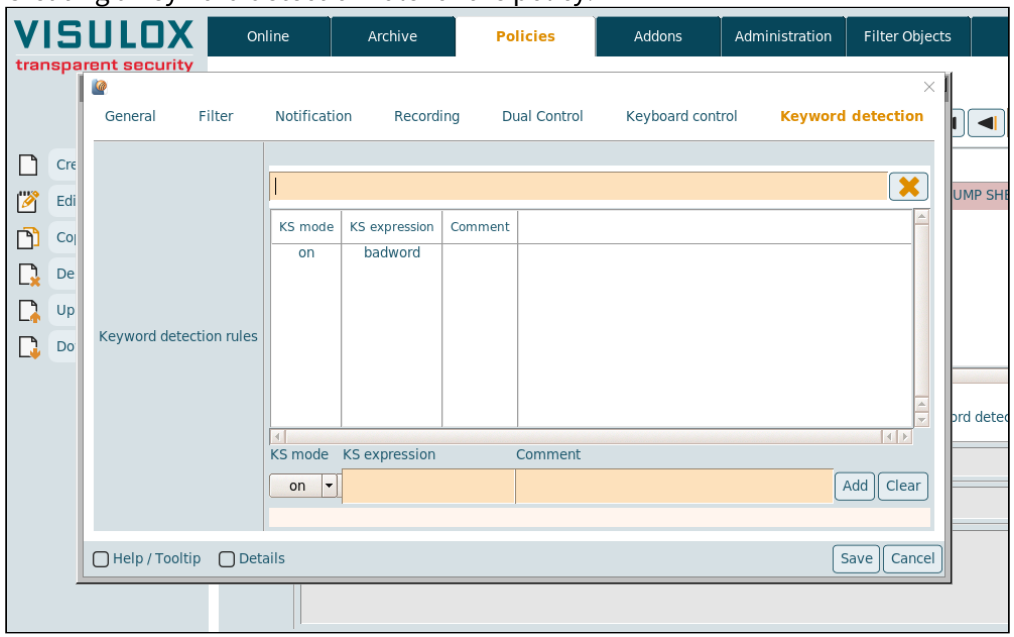
The method for keyboard recording has to be selected: "**Record input and detect keywords**".
A script can be selected, which is executed, when a keystroke is detected (not used in this example).
Activity on detection is set to "**Acknowledge on detection**".
And finally a detection message can be entered.
The Application Policy must be saved before a line item entry can be created.

There are different ways to use keyboard recording:

- Example 1: Method: "**Record input and detect keywords**" / Activity on detection: "**Acknowledge on detection"**
- Example 2: Method: "**Detect keywords only**" / Activity on detection: "**Lock on detection**"

Another possibilty for an action on detection is "**Keyword detection muted**" (not used in these examples).

4. Creating a keyword detection rule for the policy:

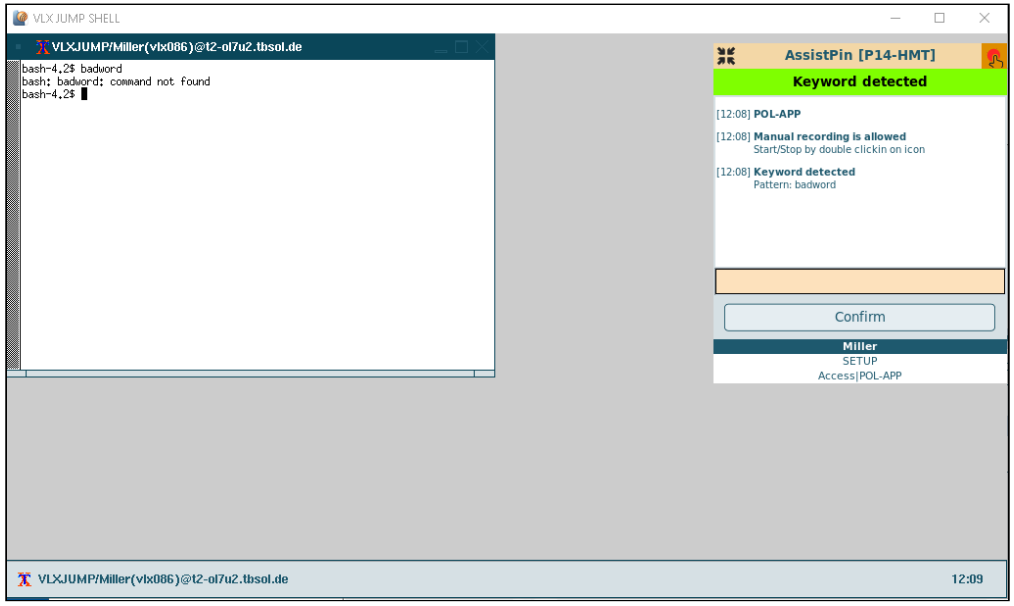


A keyword detection comment for the keyword can be entered.
The regexpression of the keyword has to be defined: "**badword**"

Example 1: Miller starts the application and enters the configured keyword

Method: "**Record input and detect keywords**" / Activity on detection: "**Acknowledge on detection"**

1. User Miller starts the "**VLX Jump Shell**" application from his Workspace:



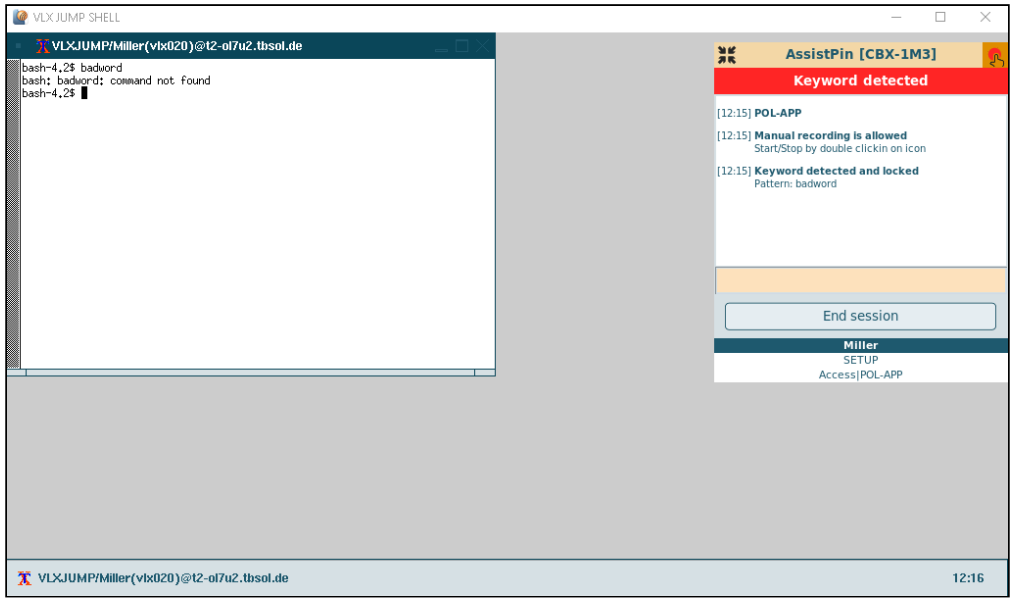
The keyword "**badword**" is detected and the application is locked.
Miller has to acknowledge the "**Keyword detected**" box to continue working.

With "**Record input and detect keywords**" all keystrokes from user Miller are displayed in the VISULOX Cockpit.

Example 2: Miller starts the application and enters the configured keyword

Method: "**Detect keywords only**" / Activity on detection: "**Lock on detection**"

1. User Miller starts the "**VLX Jump Shell**" application and enters "**badword**":



The keyword "**badword**" is detected and the application is locked.

If an denied Access Policy is configured with a request script, the "**Send Request**" button can be displayed next to the "**End session**" button.

With "**Detect keywords only**" only the entered keywords from user Miller are displayed in the Cockpit. Other keystrokes can not be seen.

Keyboard recording check list with additional tests

Feature	Expected behaviour	Comment
Policy mode: disabled	• Application Policy has no effect, the next Policy, that matches will be used	

Feature	Expected behaviour	Comment
Filter settings	• User/group mask: all registered users are recorded • Application mask: all registered applications will be recorded • Remote IP mask: all users connecting from the registered IP are recorded • Access point mask: all users connecting over the registered access point are recoded	
Recording on/off	• See: How to enable, configure and use recording	
Keystroke detection	• Keyboard control disabled: no keystrokes will be recorded • Detect keywords only: only keywords are detected, other keystrokes are not displayed in Cockpit • Record input and detect keywords: keywords are detected, all keystrokes are recorded and displayed in Cockpit	
Activity on detection	• Keyword detection muted: no message or lock for the user, keyword detection is shown in Cockpit events • Acknowledge on detection: screen is locked, the user has to acknowledge the "Keyword detected" box to continue working • Lock on detection: screen is locked, the user is able to send a request to the supervisor, screen remains locked	
Detection message	• Entered message is displayed in the user box and in VISULOX Cockpit events, if a keyword is detected	
Line items	• Active / Disabled: keyword detection is active or disabled • Regexpression: the expression for the keyword, that shoul be detected is highly configurable to match certain commands or part of commands • Script to send notification to the supervisor on keyword detection	
Events	• All actions during recording are displayed in the VISULOX Cockpit	

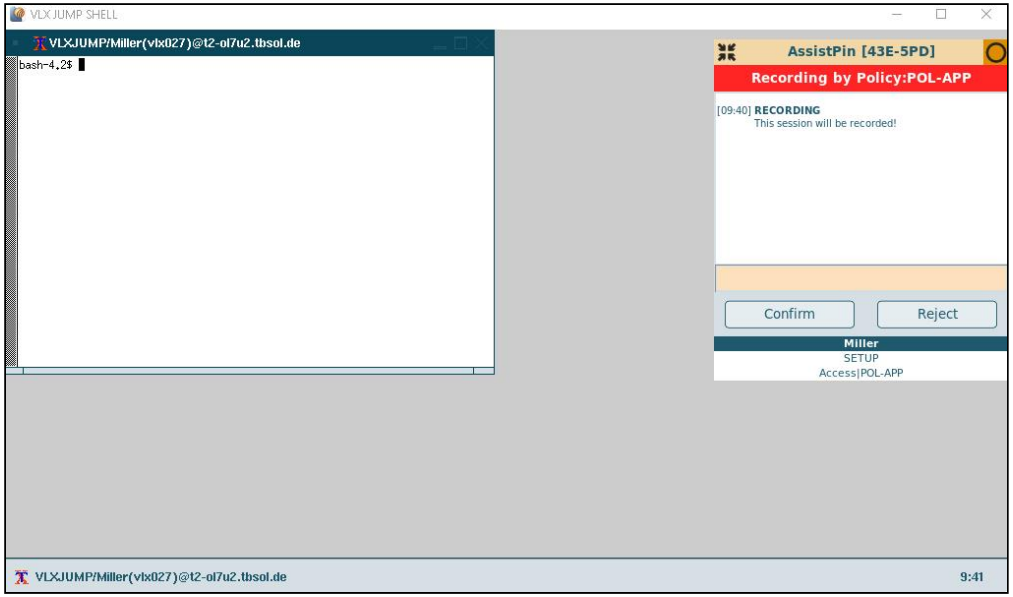
Recorder configuration

Configuration parameters

```
visulox config list -name recorder
    ---------------------------------------------------------------------------------------------
    | changed | key                        | value                                              |
    ---------------------------------------------------------------------------------------------
    |         | recorder.auto_acknowledge  | 0                                                  |
    |         | recorder.chapterinterval   | 20                                                 |
    |         | recorder.manually          | true                                               |
    |         | recorder.max               | 250                                                |
    |         | recorder.snapshotinterval  | 5                                                  |
    |         | recorder.welcome           | Security Policy enforces recording for this application |
    ---------------------------------------------------------------------------------------------
```

Auto acknowledge recording

With this setting, the behaviour of the recording box can be configured.



auto_acknowledge	Description
0	Recording dialog stays on the screen, until **confirmed** or **rejected** by the user.
1	The positive value is the time in seconds until the recording dialog is **confirmed**.
-1	The negative value is the time in seconds until the recording dialog is **rejected**.

Negative integer values are supported since version 3.1.7p2 for new installations.
Older or updated versions need a correction via database on each node:

```
visulox database query -sql "update  global_layout SET value=-5 where name='auto_acknowledge'" -force
visulox config rebuild
```

Disable manual recording

The manual recording checkbox in the control panel can be removed to prevent users recording their own sessions.

```
visulox config -name recorder.manually=0
    ------------------------------------------------
    | changed | parameter         |      type| value |
    ------------------------------------------------
    |         | recorder.manually | OPERATION | 0     |
    ------------------------------------------------
```

Chapter / frame settings

Parameter	Description
chapterinterval	Chapterinterval in minutes. The default setting is 20 min for a chapter.
framerate	Framrate in frames per second. The default framerate is set to 10 frames per seconds. Higher values will have an impact on the performance.
snapshotinterval	Snapshotinterval in minutes. Default setting: a snapshot is taken every 5 minutes.

23.1.31 How to enable access to applications

General

With VISULOX Access Management it is possible to assign controlled access to the IT infrastructure for internal and external employees, administrators and IT service providers.

This is limited to defined times or time periods and always booked under their own individual reference numbers.

Prerequisites

For this example setup two users have to be registered in VISULOX PORTAL with the following settings:

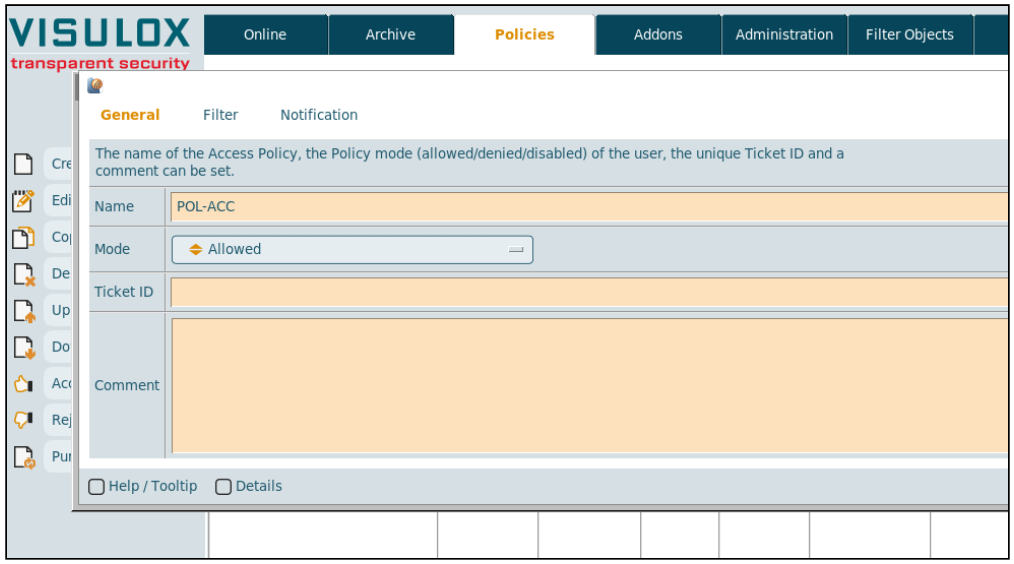
User	Role	eMail	SMS	Application	Other
Master	Supervisor	*<supervisor>@company*.com	-	VISULOX Cockpit	-
Miller	User	*<user>@company*.com	-	VLX Jump Shell	-

Supervisor Master enables and configures the access.

User Miller logs into VISULOX PORTAL and starts applications.

Supervisor Master: Enable access to applications for Miller

1. Creating a new Access Policy in the Cockpit:

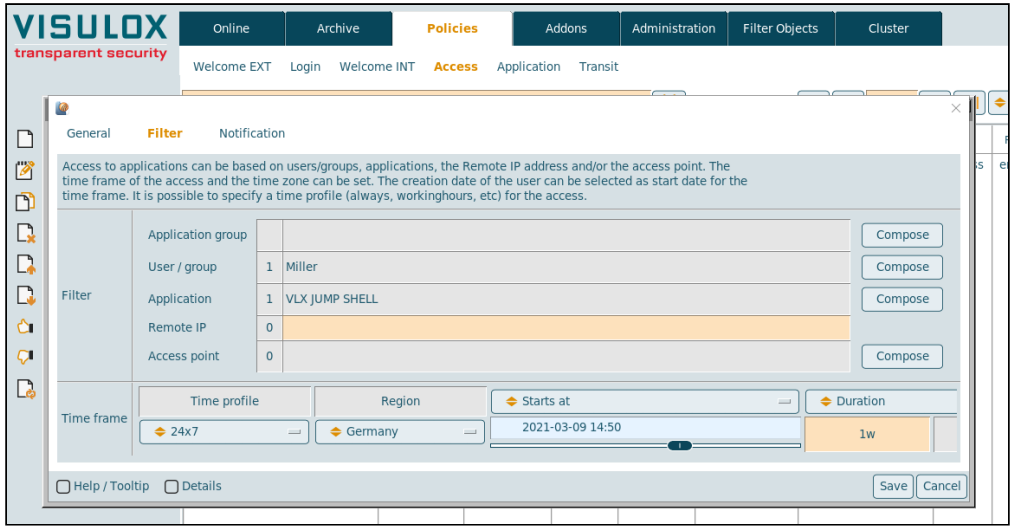


A unique name for the policy must be entered: "**POL-ACC**".
"**Allowed**" has to be selected to enable access for user Miller.
A valid Ticket ID has to be entered: "**A-1234**".
A comment for the policy can be entered as well.

Selecting the Application Policy mode:

- Example 1: Application access is allowed
- Example 2: Application access is not allowed

2. Setting the filter:



Access will only be enabled for the "**VLX Jump Shell**" application from user "**Miller**" in this example.
It is also possible to set a filter for the Remote IP address or the Access point (not used in this example).
It is possible to choose a time profile and a time zone from a dropdown list of pre-configured entries.
The start and end time of the access can be chosen as well.
The default values are fine for this example (always, Germany, 7days from now).

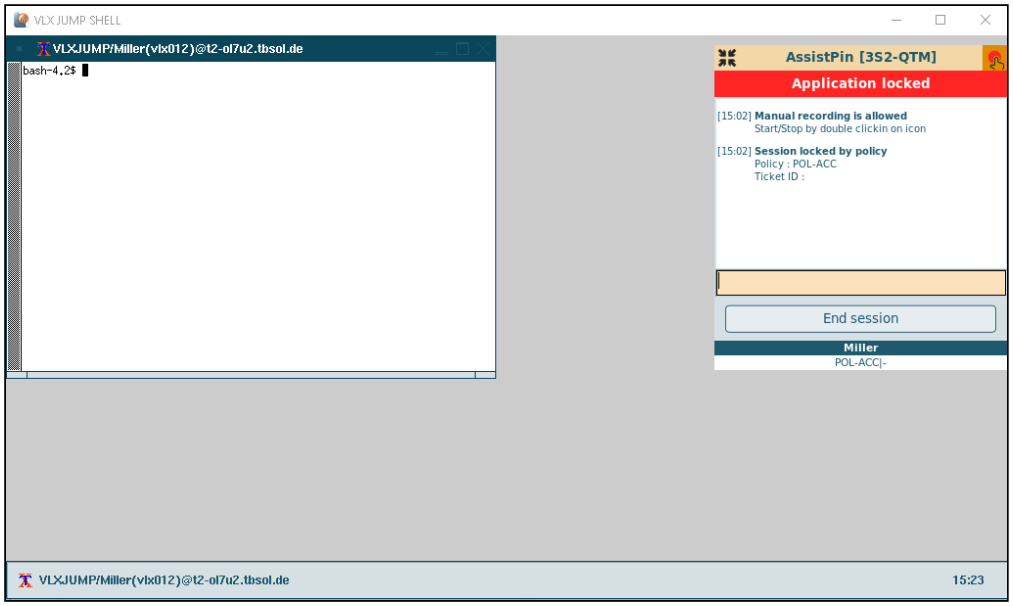
3. On the Notification page, a notification script can be selected, which displays a "**Send request**" button if the session is locked.
   This makes only sense for an additional denied policy and is not used in this example. It is also possible to setup a request script, which allows to send mails to the requester and approver, who can allow, reject the request via mail.

Example 1: Miller starts an application with access allowed

User Miller starts the "**VLX Jump Shell**" application from his Workspace.

The application is not locked, working is possible.

Example 2: Miller starts an application with access not allowed



User Miller starts the "**VLX Jump Shell**" application from his Workspace.

The application is locked.

If a denied Access Policy with a notification script matches, a notification will be sent to the supervisor by clicking the "**Send request**" button.

If a denied Access Policy with a request script matches, mails are sent to the requester and the approver, who can allow, reject this request via mail.

The session can also be ended with the "**End session**" button.

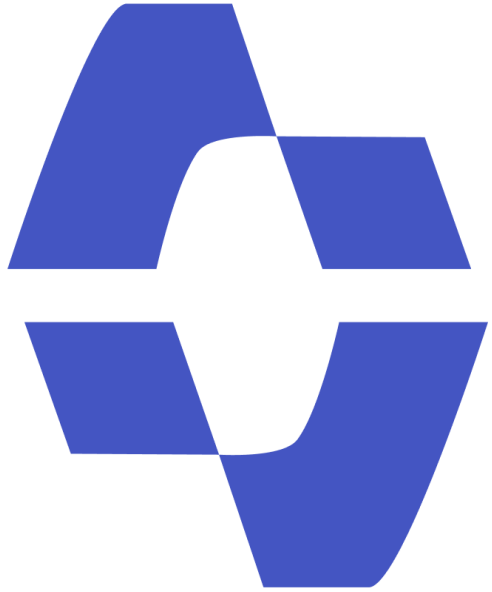
Access check list with additional tests

Feature	Expected behaviour	Comment
Application access is allowed	• User can start applications • Screen is not locked, working is possible	
Application access is not allowed	• User can start applications • Application is locked • User can enter a message for the supervisor and send it with the button "Send request"	
Disabled	• Application Policy has no effect, the next Policy, that matches will be used	
Filter settings	• User/group mask: all registered users get access to applications • Application mask: all registered applications are available for the access • Remote IP mask: all users connecting from the registered IP get access to applications • Access point mask: all users connecting over the registered access point get access to applications	
Time frame	• Time profile: different profiles are available e.g. alway, never, working hours, etc • Access is not allowed, if an application is started outside of the time profile • Time zone: different time zones can be selected for the access • Start/end time: start and end time for the access • Access is not allowed before or after the set start/end time	
Notification	• Selecting a notification script to inform the supervisor of the request (See: How to create and use notifications) • Adjusting the notification script, using more possible variables (See: How to create and use notifications)	

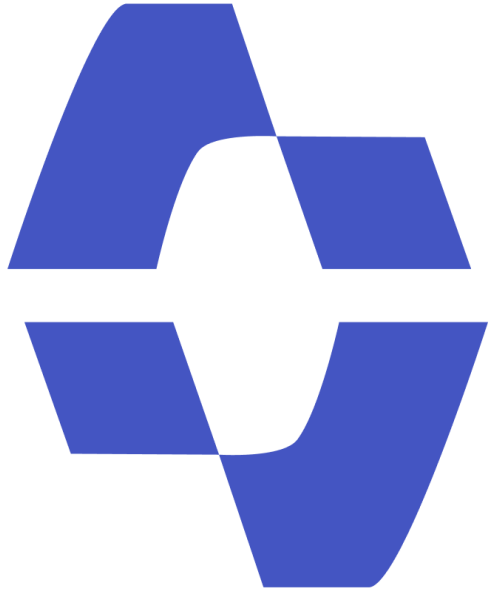
Feature	Expected behaviour	Comment
Events	• All information about the access is displayed in the Cockpit	

Related articles:

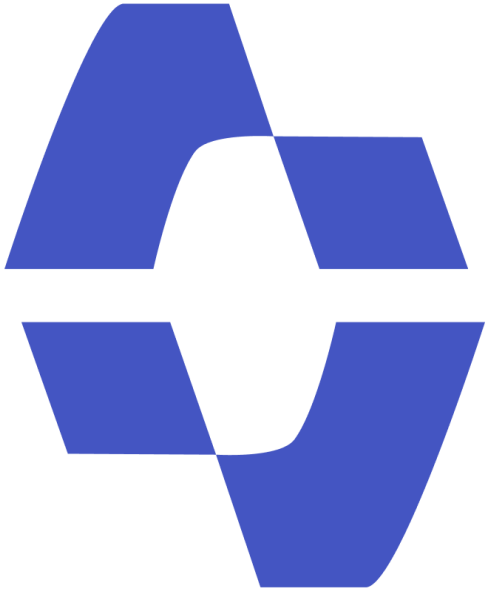
(4.1.1) Access and transit request via actionlink
(4.1.1) Access Branding
(4.1.1) Access Policy
(4.1.1) Access request and access to applications
(4.1.1) Handling ticket IDs from external systems
(4.1.1) How to control access from the command line
(4.1.1) How to control groupaccess from the command line
(4.1.1) How to enable access to applications
(4.1.1) How to handle access for groups
(4.1.1) How to lock a user permanently for using an application after keyword detection
(4.1.1) How to use the VISULOX Command Line Interface from a remote server
(4.1.1) In-time access
(4.1.1) Login and Access Management
(4.2.0) Access and transit request via actionlink
(4.2.0) Access Branding
(4.2.0) Access Policy
(4.2.0) Access request and access to applications



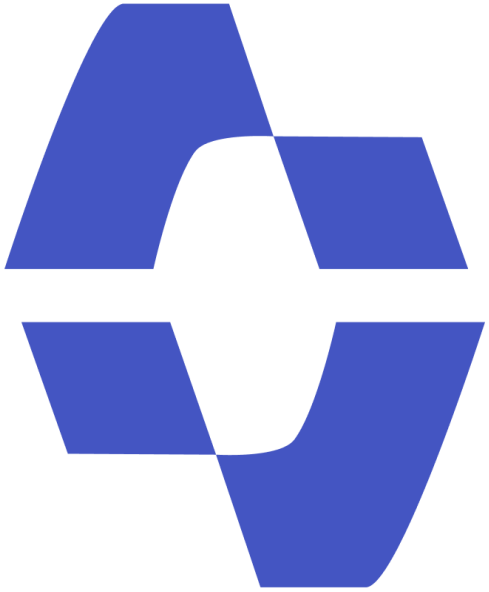
(4.2.0) Handling ticket IDs from external systems
(4.2.0) How to control access from the command line
(4.2.0) How to control groupaccess from the command line
(4.2.0) How to enable access to applications
(4.2.0) How to handle access for groups
(4.2.0) How to lock a user permanently for using an application after keyword detection
(4.2.0) How to use the VISULOX Command Line Interface from a remote server
(4.2.0) In-Time Access
(4.2.0) Login and Access Management
(4.3.0) Access and transit request via actionlink
(4.3.0) Access Branding
(4.3.0) Access Policy
(4.3.0) Access request and access to applications
(4.3.0) Handling ticket IDs from external systems
(4.3.0) How to control access from the command line
(4.3.0) How to control groupaccess from the command line
(4.3.0) How to enable access to applications
(4.3.0) How to handle access for groups
(4.3.0) How to lock a user permanently for using an application after keyword detection
(4.3.0) How to use the VISULOX Command Line Interface from a remote server
(4.3.0) In-Time Access
(4.3.0) Login and Access Management



(4.3.1) Access and transit request via actionlink
(4.3.1) Access Branding
(4.3.1) Access Policy
(4.3.1) Access request and access to applications
(4.3.1) Handling ticket IDs from external systems
(4.3.1) How to control access from the command line
(4.3.1) How to control groupaccess from the command line
(4.3.1) How to enable access to applications
(4.3.1) How to handle access for groups
(4.3.1) How to limit the granting endtime in Access Policies
(4.3.1) How to lock a user permanently for using an application after keyword detection
(4.3.1) How to use the VISULOX Command Line Interface from a remote server
(4.3.1) In-Time Access
(4.3.1) Login and Access Management
(4.3.1) Time zones, holidays and time profiles
(4.3.2) Access and transit request via actionlink
(4.3.2) Access Branding
(4.3.2) Access Policy
(4.3.2) Access request and access to applications
(4.3.2) Access termination enforced
(4.3.2) Handling ticket IDs from external systems
(4.3.2) How to control access from the command line



(4.3.2) How to control groupaccess from the command line
(4.3.2) How to enable access to applications
(4.3.2) How to handle access for groups
(4.3.2) How to limit the granting endtime in Access Policies
(4.3.2) How to lock a user permanently for using an application after keyword detection
(4.3.2) How to use the VISULOX Command Line Interface from a remote server
(4.3.2) In-Time Access
(4.3.2) Login and Access Management
(4.3.2) Time zones, holidays and time profiles
Access and transit request via actionlink
Access Branding
Access Policy
Access request and access to applications
Access termination enforced
Handling ticket IDs from external systems
How to control access from the command line
How to control groupaccess from the command line
How to enable access to applications
How to handle access for groups
How to limit the granting endtime in Access Policies
How to lock a user permanently for using an application after keyword detection
How to use the VISULOX Command Line Interface from a remote server



In-Time Access
Login and Access Management
Time zones, holidays and time profiles
(4.1.1) How to limit the granting endtime in Access Policies
(4.1.1) Time zones, holidays and time profiles
(4.2.0) How to limit the granting endtime in Access Policies
(4.2.0) Time zones, holidays and time profiles
(4.3.0) How to limit the granting endtime in Access Policies
(4.3.0) Time zones, holidays and time profiles
Access and transit request via actionlink
Access Branding
Access Policy
Access request and access to applications
Access termination enforced
Handling ticket IDs from external systems
How to control access from the command line
How to control groupaccess from the command line
How to enable access to applications
How to handle access for groups
How to limit the granting endtime in Access Policies
How to lock a user permanently for using an application after keyword detection
How to use the VISULOX Command Line Interface from a remote server

Access request and access to applications

In VISULOX a logged in user has a list of assigned applications in his Workspace. This application assignment is based on AD/LDAP groups or VISULOX PORTAL profiles.

An assigned application does not comprise, that the user can use the application. This is controlled with the VISULOX Access Policy.

A VISULOX Access Policy defines a time frame and time profiles for a user, usergroup, application or applicationgroup and the access path. If all parameters fit, the application is unlocked for user interactions.

See also: Access Policy

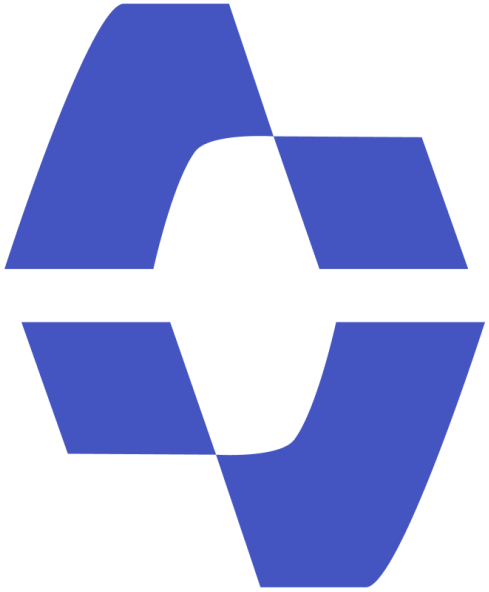
Access Policy and timeframe

Additional to timeframe and time period. the Access Poliy has a comment field, a ticket ID field and a notification script. The Access Policy state can be

- Access allowed
- Access denied
- Group access
- Access accepted
- Access rejected
- Access request
- Policy disabled

The timeframe internally is UTC times, but for better human understanding the region with its timezone is added. This means users and supervisors see the time related to their timezone.

There are different ways to define Access Policies and so to grant interaction to an application.

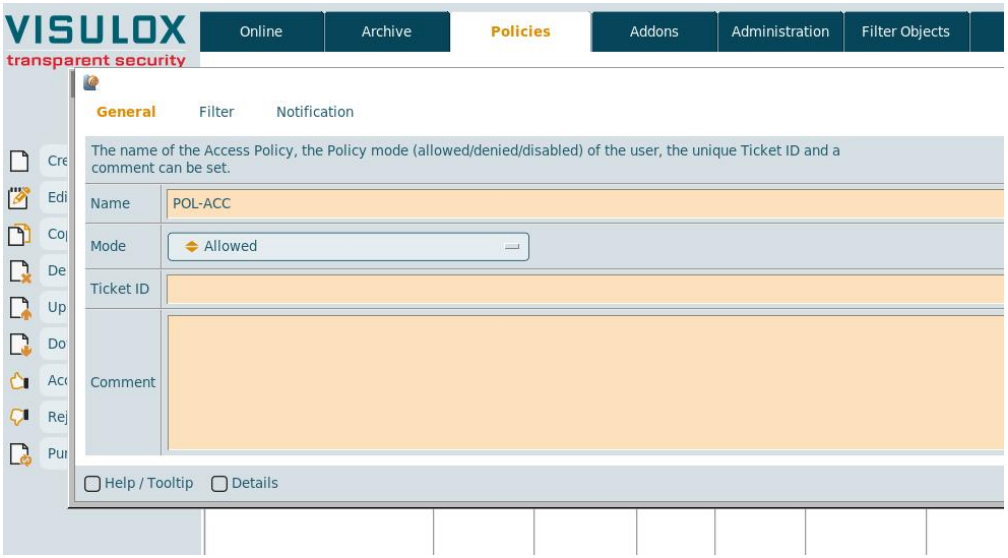


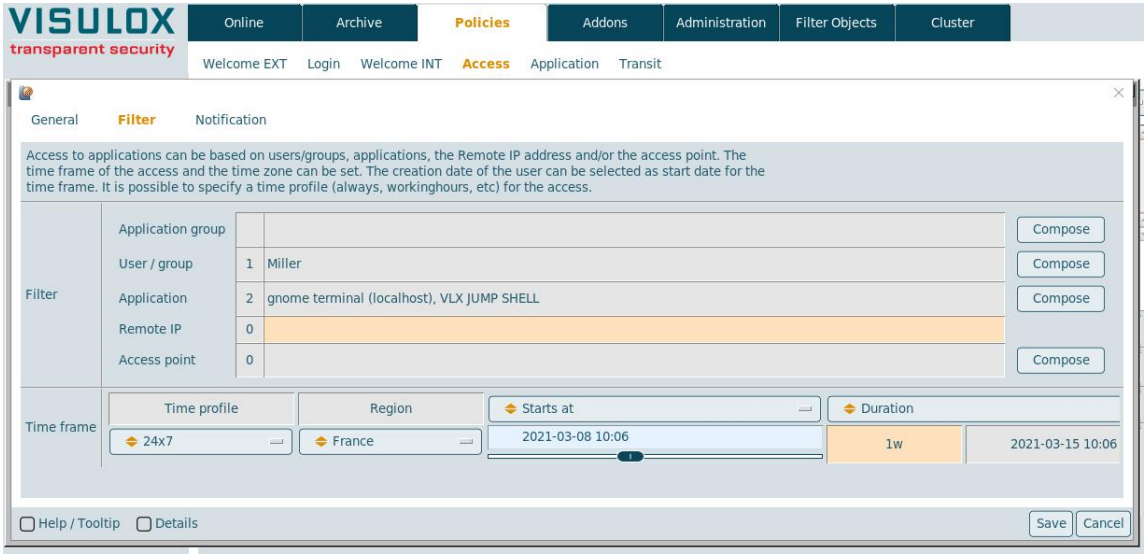
VISULOX Access Policy via VISULOX CLI

The CLI can be triggered from an external program. It needs the user, group or the application name, time period and time profile

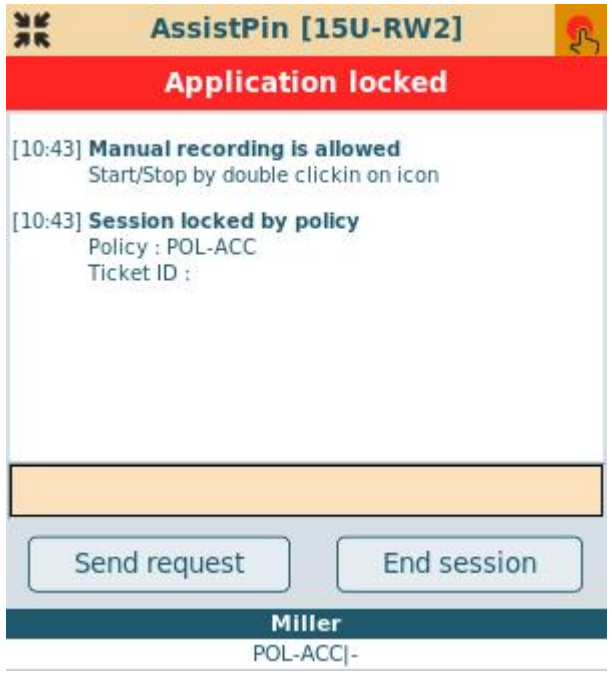
See: How to control access from the command line

Using the VISULOX Cockpit


VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
General
Filter
Notification
The name of the Access Policy, the Policy mode (allowed/denied/disabled) of the user, the unique Ticket ID and a comment can be set.
Name
POL-ACC
Mode
Allowed
Ticket ID
Comment
Help / Tooltip
Details


VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
Cluster
Welcome EXT
Login
Welcome INT
Access
Application
Transit
General
Filter
Notification
Access to applications can be based on users/groups, applications, the Remote IP address and/or the access point. The time frame of the access and the time zone can be set. The creation date of the user can be selected as start date for the time frame. It is possible to specify a time profile (always, workinghours, etc) for the access.
Filter
Application group
User / group
1
Miller
Application
2
gnome terminal (localhost), VLX JUMP SHELL
Remote IP
0
Access point
0
Compose
Time frame
Time profile
Region
Starts at
Duration
24x7
France
2021-03-08 10:06
1w
2021-03-15 10:06
Help / Tooltip
Details
Save
Cancel

User can request an access in a launched and locked application (in-time access)



The "**Send request**" button is available, once a notification / request script is configured and set in a matching denied policy.

With a request script it is possible to send a mail to the approver, who is able to grant access via an action link in the mail.
The requester also receives mails, when request is sent, approved, rejected or expired.

User can request access for a future usage of an application

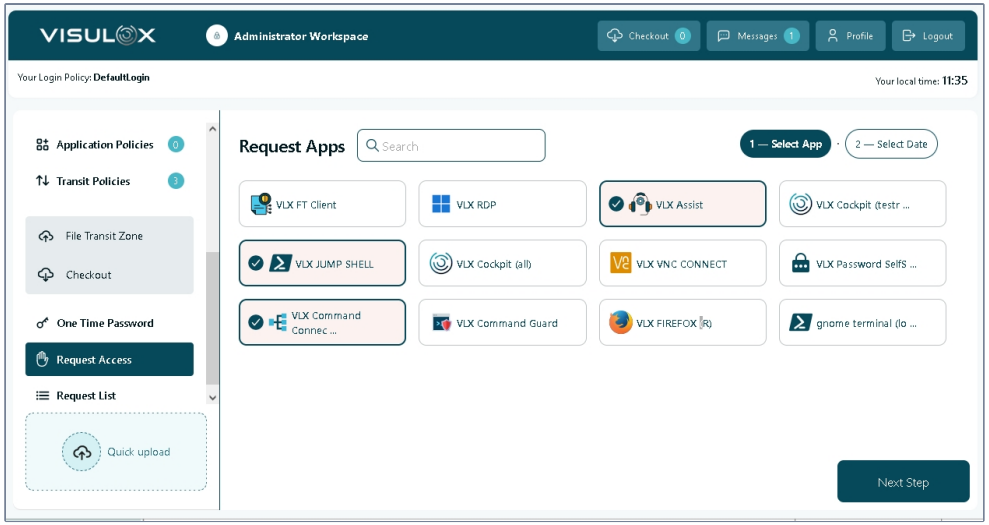
Within his Workspace, the user has a form, where he can request an access for all applications or a single one.

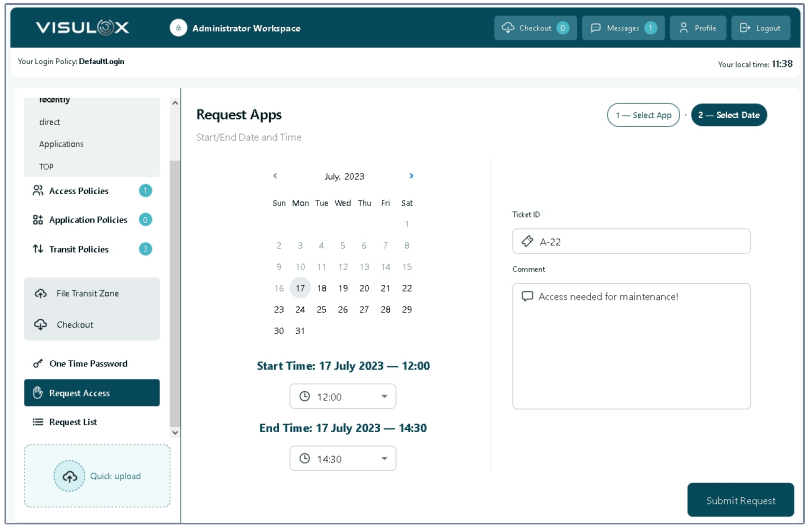
Submitting this request, creates an access request (an unconfirmed Access Policy) and an action script (Cockpit / Administration / Actions) can be triggered.
The action script includes all known data to the pending access request and the user. The script can be used to deliver this event to other services or to send an email to a supervisor.

The script is set with:

```
visulox config -name request.workspace.request="examplescript:-info Request -approver approver@visulox.com"

visulox config -name request.script
    ------------------------------------------------------------------------------------------------------
    | changed | key                   | value                                                            |
    ------------------------------------------------------------------------------------------------------
    | changed | request.workspace.request | examplescript:-info Request -approver approver@visulox.com |
    ------------------------------------------------------------------------------------------------------
```

The pending access request can be accepted or denied via the Cockpit, the VISULOX CLI or if a request script is configured via mail.

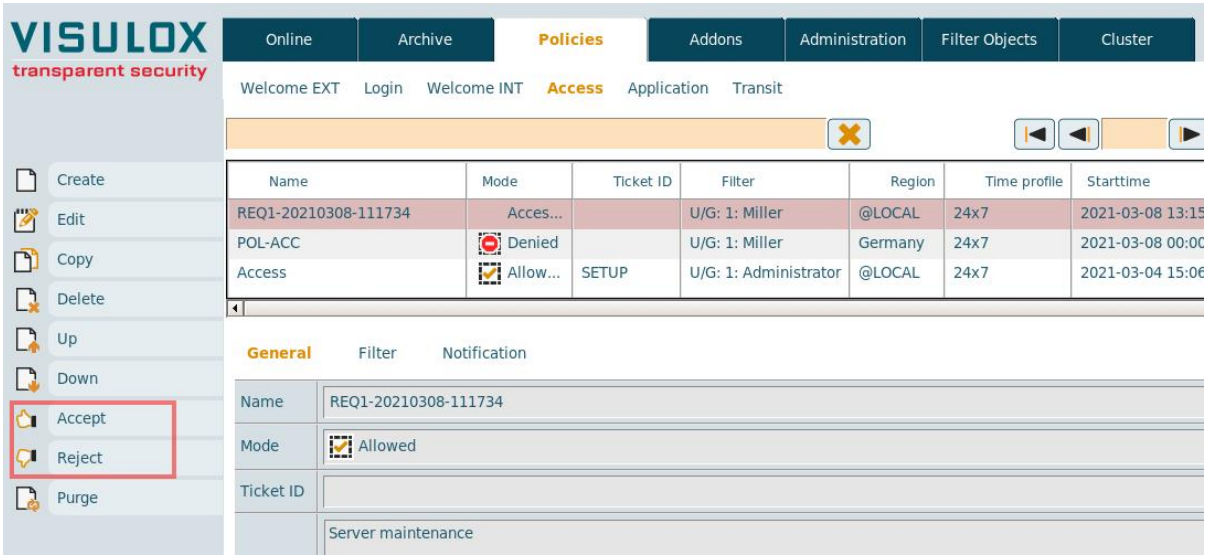




The user can request access for all selected applications. He has to enter a time frame, the ticket ID and a comment. All is checked against the configured ruleset.

The successful submit adds an access request to the Access Policies. This request is ignored and the first applying rule should be "**Deny**".

A supervisor can now modify this access request to "**Reject**" or "**Accept**". "**Reject**" is handled as "**Deny**", "**Accept**" as "**Allow**".
This can be done in the Cockpit or via action link in a mail, if a request script is used.



23.1.32 How to limit the granting endtime in Access Policies

Overview

Access to applications has to be granted by an supervisor with an Access Policy.

It can be claimed to limit the amount of time.

- Overview
- Usage
- Configuration
- Known issues and comments

Usage

The Access Policy has a filter (user/group, application) and a time frame. The time frame has a time profile (always, work hours, only Monday ..) and a start and endtime. Company Access Securitry Policy can prevent that supervisors are granting an endless access by setting a grant limitation. The parameter **vlxgui.maxgrantaccessdays** can be set.

Configuration

Show current configuration

```
visulox config list -name maxgrantaccessdays
    ------------------------------------------------------------------------------
    | parameter                 |      type | value   | validation | vlx_default |
    ------------------------------------------------------------------------------
    | vlxgui.maxgrantaccessdays | OPERATION | endless | isDay      |           1 |
    ------------------------------------------------------------------------------
```

Set to 20 days after now

```
visulox config edit  -name vlxgui.maxgrantaccessdays=20
```

Granting unlimited access

```
visulox config edit  -name vlxgui.maxgrantaccessdays=endless
```

Known issues and comments

A restart of the VISULOX Cockpit is needed to load the new parameter.

23.1.33 VISULOX Firefox integration

There are two different conceptional ways for a VISUOLX Firefox integration. With and without persistence profile.	• Non persistence and VISULOX shell • Persistent and Firefox Wrapper • Comparison • Related articles

Non persistence and VISULOX shell

The VISULOX shell provides shell enviroments to users, if no UNIX accounts are available or UNIX accounts are not needed. This is the case, if the UNIX System is used for transit to webapplications, Windows or Citrix.

If non persistence profiles are sufficient, the VISULOX vlxshell can be used:

```
vlxshell -client firefox / visulox.exp / applicationserver which is member in the visulox cluster
```

With the parameter **-P *<path to directory or .tgz file>*** a profile template can be set, which will be copied and used in firefox.

Example for Firefox started wirh a given URL:

```
vlxshell -client firefox -- "https://portal.visulox.com/wiki"
```

This command uses the platform provided Firefox. An alternate Firefox can be provided:

```
vlxshell -client firefox -clientcmd <pathToAlternateFirefox> / visulox.exp / applicationserver which in member if the visulox
cluster
```

Using the vlxshell assigns a vlxtransit user (vlx000 to vlx999) to the user. The VISULOX PORTAL login script is **visulox.exp**.

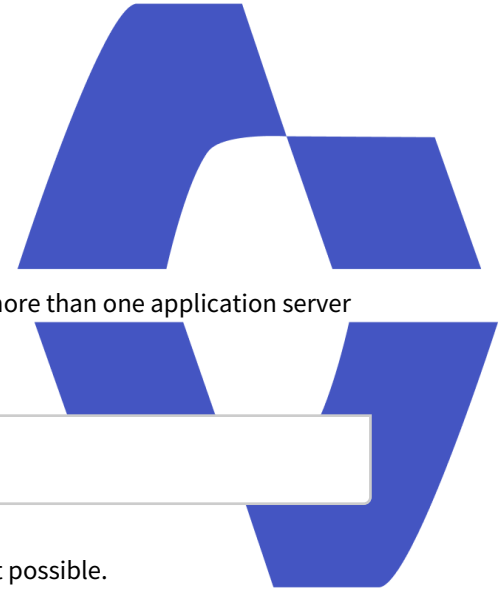
> The type (firefox, chrome, etc) can be used instead of the **vlxshell** command in the Application Command field and **-client <type>** in the Argument for Command field.

Additional plugins (like Flash, Java or Citrix) are loaded,

vlxshell.tcl parameters:

Parameter	Description
-client <*value*>	Client type. Default: xterm
-clientcmd <*value*>	Alternate path to client

Parameter	Description
-title <*value*>	Title of the GUI
-lang <*value*>	Language
-id <*value*>	Session ID
-owner <*value*>	Owner who runs this GUI
-allowedSites <*value*>	List of allowed sites in Firefox profile
-usermask <*value*>	Mask to add a prefix and/or suffix to sso_user (prefix%USER%suffix)
-E <*value*>	Extension list for Firefox
-P <*value*>	Firefox profile archive or directory
-profile <*value*>	Name of Citrix profile in database
-resource <*value*>	Name of passcache resource
-sync	Activate vlxtransit and vlxupload for the application



Persistent and Firefox Wrapper

A persistent integration needs the possibility to store the user profile. Therefore the user needs a UNIX user account and a home directory. If more than one application server is implemented, the home directory must be spanned over all servers.

The classical integration would be:

```
firefox  / unix.exp or vlxUnix.exp / applicationserver
```

The disadvantage of this integration is, that the user can use only one of the applications with Firefox. Simultaneous multiple Firefoxes are not possible.

To provide this, the VISULOX Firefox Wrapper can be used:

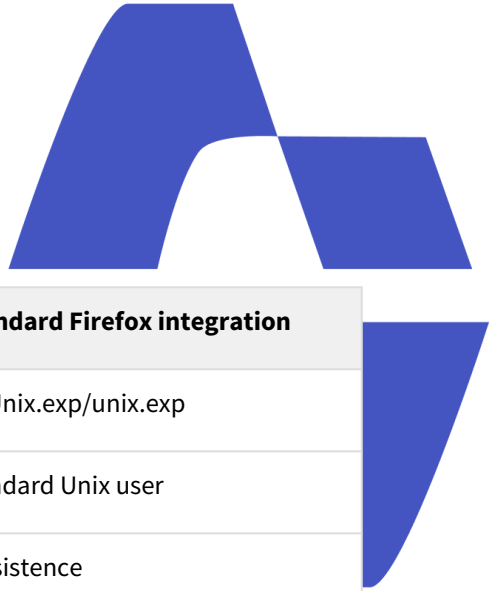
```
 VLXDIR/tools/ffw/ffwrapper.tcl / vlxUnix.exp / applicationserver which is member in the visulox cluster
```

```
vlxshell/visulox.exp  -client ffwrapper – <ffwrapper args>
```

The VISULOX Firefox Wrapper can be used only with a UNIX user account.

The VISULOX Firefox Wrapper generates the user's Firefox profile based on user name / application name and the Firefox version. The profile is stored within the user's home directory.

This integration allows different versions of Firefox and also the possibility to run multiple Firefoxes.



Comparison

	vlxshell with Firefox	Firefox wrapper	Standard Firefox integration
VISULOX PORTAL login script	visulox.exp	vlxUnix.exp	vlxUnix.exp/unix.exp
Unix user	temporary vlxtransit user	standard Unix user	standard Unix user
Profile	non persistence	persistence	persistence
Multiple instances	yes	yes	no
VISULOX File Transfer integration	yes	yes	yes
Firefox Citrix plugin	yes	yes	yes
Firefox Citrix plugin and File Transfer integration	yes	yes	no
Different Firefox versions	yes	yes	yes
Java integration	non* / platform assigned	application definition assigned different versions	non*/ platform assigned
Flash	platform assigned	part of the integration	platform assigned

	vlxshell with Firefox	Firefox wrapper	Standard Firefox integration
Handles extensions (as long as it fits to the FX version)	yes	yes	user can install

* if the Firefox Wrapper is used, the platform installed JAVA is removed and cannot be used anymore.

Related articles

VISULOX Firefox and Firefox extensions

VISULOX Firefox Wrapper setup

VISULOX Firefox CITRIX / ICA integration

How to create a persistent Firefox profile for VISULOX integration

About

This article explains how to setup a persistent Firefox profile to be used in the VISULOX Firefox integration via VLX JUMP SHELL.

There serveral steps:

- About
- Preparing a profile
- Packing and saving the profile as an archive
- Apply the profile to a Firefox application

Preparing a profile

Log into VISULOX PORTAL and start a VLX Jump Shell.

Run the following commands:

Initialize Firefox with a default profile

```
firefox -CreateProfile default
firefox -profile $HOME/.mozilla
```

You can now make customizations to your profile like visual customizations or add homepage, links etc.

A good approach is also to add profile specific certificates to the Firefox browser:

Launch Firefox and make your customizations

```
firefox -profile $HOME/.mozilla
```

Exit Firefox after customizations are done.

Test / verify youz new profile

```
firefox -profile $HOME/.mozilla
```

Packing and saving the profile as an archive

Saving the profile must be done by the administrator

```
bash-4.2$ cd  .mozilla/
bash-4.2$ tar czf $HOME/myProfile.tgz .
bash-4.2$ ls -l
total 28468
drwx------. 2 vlx000 vlxgroup        6 Feb 25 11:43 Downloads
-rw-r-----. 1 vlx000 vlxgroup 29151090 Feb 25 11:54 myProfile.tgz
drwx------. 2 vlx000 vlxgroup        6 Feb 25 10:23 vlxtransit
```

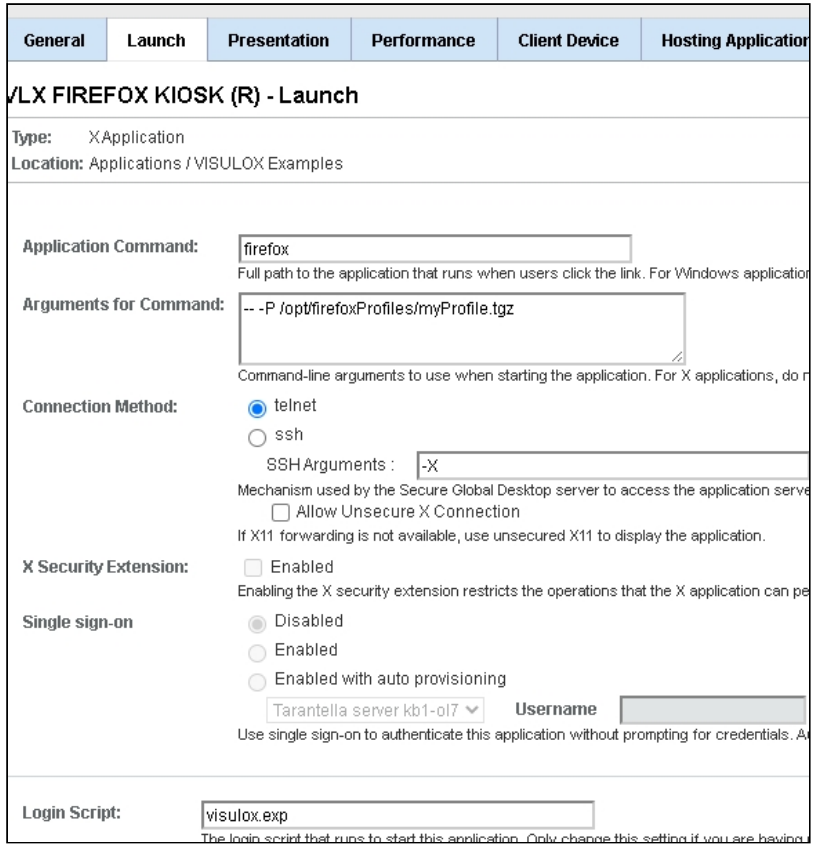
The packed Firefox profile has to be copied into a directory outside of the VLX Jump Shell environment, accessable by all VLX Jump Shells. Also the content in the folder needs to be synchronized with all nodes running the VLX Jump Shell.

Save into a folder readable for vlxgroup in a common place

```
mkdir /opt/firefoxProfiles/
cp /opt/visulox/vlxusers/vlx000/myProfile.tgz /opt/firefoxProfiles/
chgrp -R vlxgroup /opt/firefoxProfiles/
```

Apply the profile to a Firefox application

In the VISULOX PORTAL Console create a VLX Jump Shell with Firefox:



You can now launch the application and check your profile.

⚠ Please take note that the created profile must be distributed to all nodes in the VISULOX Array.

VISULOX Firefox and Firefox extensions

Keep in mind, that extensions often require a certain version of the browser.
If the used browser is updated to the latest version, please check, if the wanted extension is still available.

The Firefox integration has the ability to install Firefox extensions in this independent context. This is done within the application call.

```
vlxshell -client firefox -E extentions1,extenstion2 -- <url>
```

The extensions are provided in **./etc/firefox/extensions**. Each extension has a name, which is used as an argument. This name is a directory.

Below this direcory there are files: **user.js** file for the extension, the **.xpi** file with the extensions or the extracted extension.

It is important, that the extension file name or the exension dirname has the UUID of the extension.

The extension can be addressed via the vlxshell command with **-E <name>**. Multiple extensions can be applied: **<name1>,<name2>,..**

It is recommended to use Chromium instead of Firefox for kiosk mode.

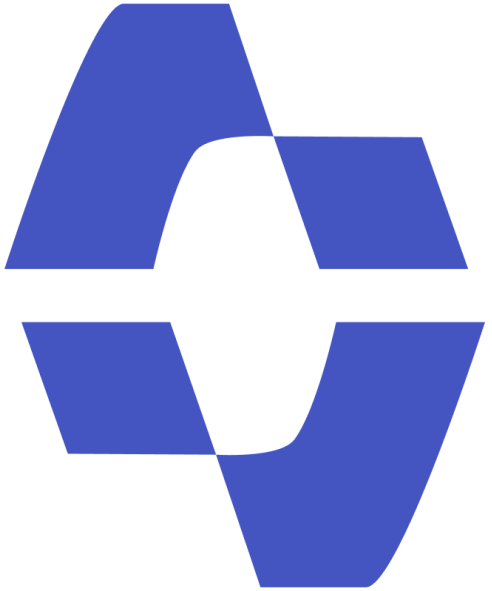
Related articles

VISULOX Firefox integration

VISULOX Firefox Wrapper setup

- Prerequisites
- Firefox Wrapper setup
  - Install Firefox Wrapper
  - Provide Firefox versions
    - The Firefox versions are stored in
  - Useful arguments

- Adding a new version
    - Adding a new Firefox version
    - Example - Firefox 45
- Provide Flash
    - Flashplugin
- Provide Java versions
    - JAVA plugins
- Firefox Wrapper sandbox
- Allowed sites for add-ons / plugins
- Update
    - Ater updating VISULOX the script has to be run manually again



Prerequisites

Installation of required libraries:

```
yum install libstdc++.i686 freetype.i686 fontconfig.i686 libXrender.i686 libXext.i686 libXdamage.i686 libXcomposite.i686 alsa-
lib.i686 dbus-glib.i686 gtk2.i686 libXt.i686 gtk2.x86_64
```

⚠ Dependencies / Packages for older versions of Firefox may not be supported.

Firefox Wrapper setup

There are several steps to get the Firefox Wrapper running.

- Provide the Firefox Wrapper library into the user context
- Provide the Firefox versions needed for the setup
- Provide Flash
- Provide JAVA

⚠ 32bit versions are needed for this setup.

A Firefox Wrapper setup package is available on request.

The package has to be extracted to **$VLXDIR/tools/ffw/**.

All setup scripts can be found in **$VLXDIR/tools/ffw/setup**.

Install Firefox Wrapper

```
sh installFirefoxWrapper.sh
```

Provide Firefox versions

The script **installFirefoxVersions.sh** will download and extract the Firefox versions (if necessary).

The Firefox versions are stored in

```
/opt/ffw/firefox
```

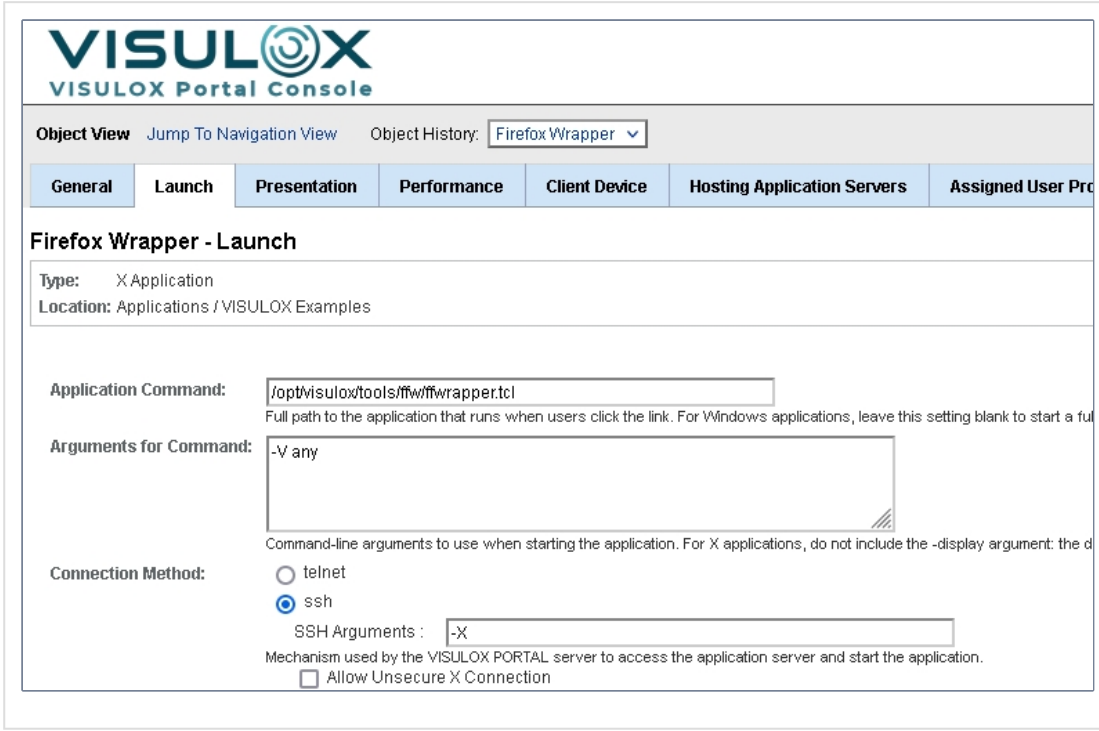
The file **pathsAndVars.sh** has the list of Firefox versions provided by the Firefox Wrapper. The list has a "name" and the URL to the Firefox versions repository.

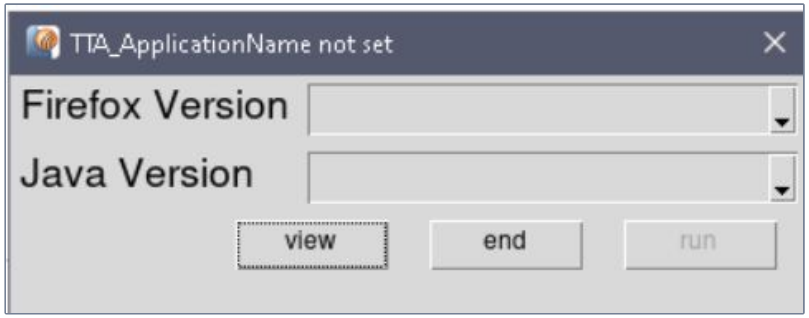
The "name" prefix is the architecture.

```
FXLIST+="36_32bit $FXRELEASE/36.0/linux-i686/en-GB/firefox-36.0.tar.bz2;"
FXLIST+="36_64bit $FXRELEASE/36.0/linux-x86_64/en-GB/firefox-36.0.tar.bz2;"
```

A selection window can be displayed on Firefox Wrapper start with the following Arguments for Command:

Configuration	Selection on application start





Useful arguments

Arguments	Description
-V <*arg*>	Select Firefox Version. If 'any', user has to select the version. OS uses the platform Firefox. Default: OS
-java <*arg*>	Requested Java Version

Arguments	Description
-drive <*arg*>	Drive name in Citrix session for vlxtransit. Default: E
-path <*arg*>	Path to Firefox Wrapper Files. Default: $FXBASE
-allowedSites <*arg*>	List of allowedSides in Firefox profile
-bwrap <*arg*>	Bubblewrap-specific options <>
-E <*arg*>	Extension list for Firefox
-debug	No auto close

Adding a new version

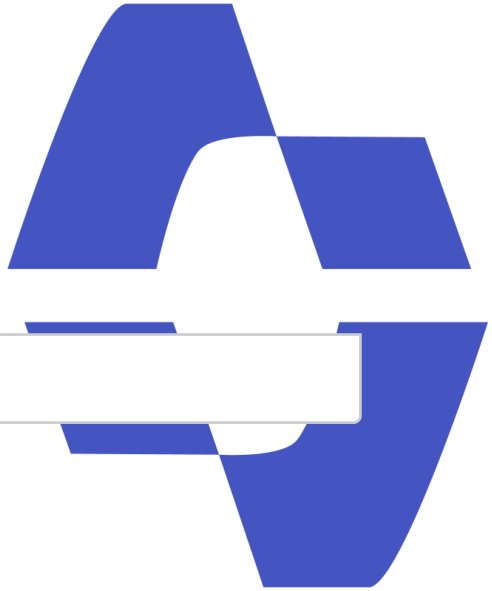
To add a new Firefox version, edit **$VLXBASEPATH/tools/ffw/pathsAndVars.sh** .

Adding a new Firefox version

```
FXLIST+="<version> $FXRELEASE/<url to version>;"
```

Example - Firefox 45

```
FXLIST+="45_64bit $FXRELEASE/45.0/linux-x86_64/en-US/firefox-45.0.tar.bz2;"
```



After adding new versions, redo the steps of the installation

If the Firefox versions can not be downloaded by the installation script, a manual download is needed from the Firefox version repository:

```
https://ftp.mozilla.org/pub/firefox/releases
```

Provide Flash

The script **installFlash.sh** puts the the flash plugin into place. The flash plugin is addressed by all Firefox versions.

Flashplugin

```
/opt/ffw/flash
```

Provide Java versions

The Firefox Wrapper can assign different Java versions as well.

The Java versions are extracted and installed as RPMS with **installJavaPlugin.sh**.

JAVA plugins

```
/opt/ffw/java
```

Previous Java versions can be downloaded from:

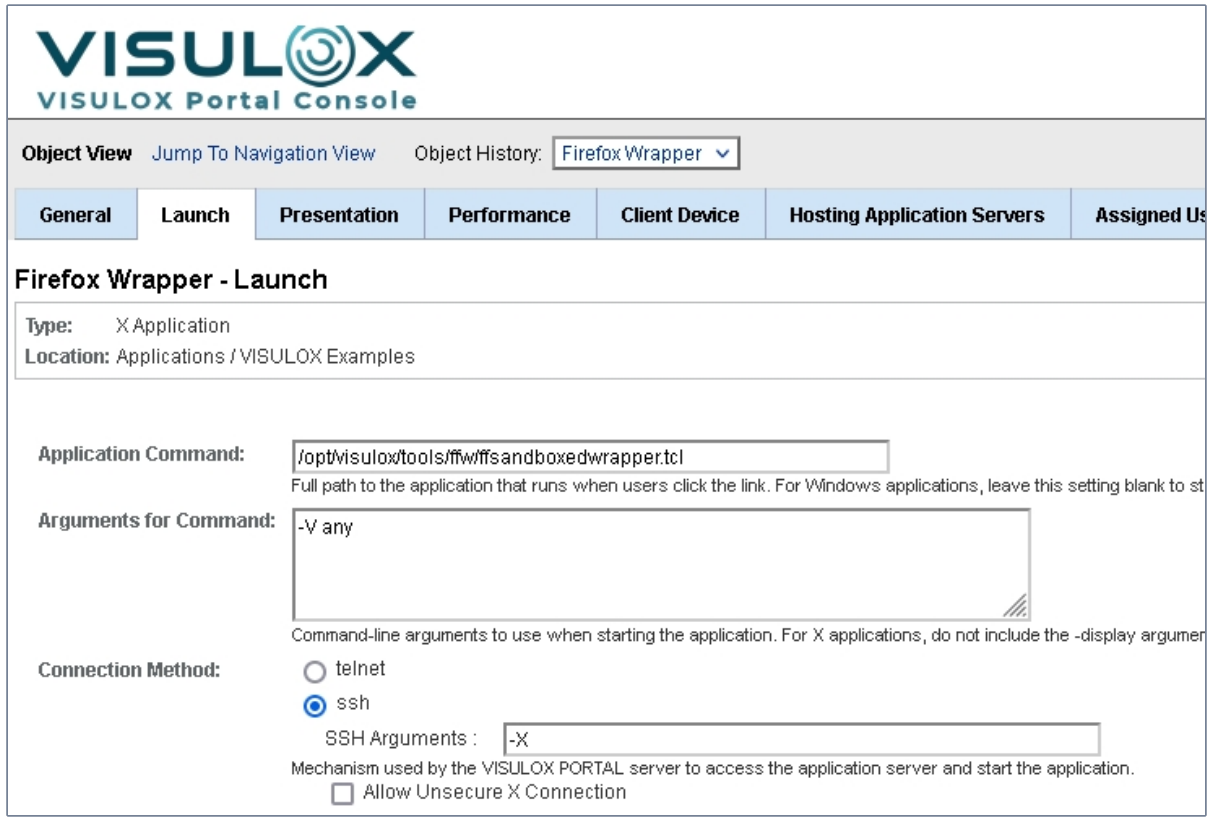
```
http://www.oracle.com/technetwork/java/archive-139210.html
```

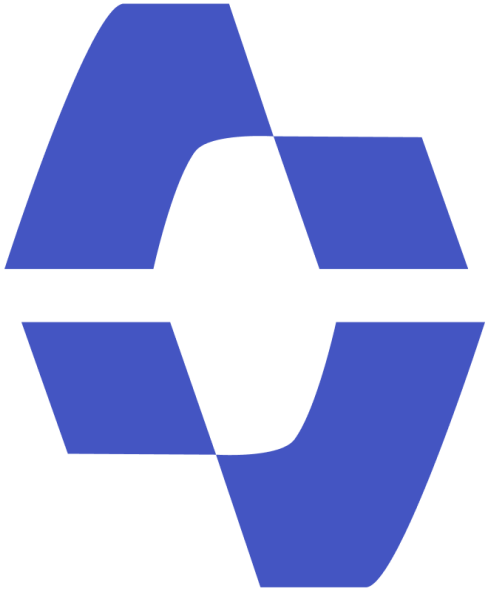
Firefox Wrapper sandbox

Firefox Wrapper can be adjusted to restrict the access of the users.

The user is able to see only his own files.

Use the following configuration for a Firefox Wrapper sandbox application:





Allowed sites for add-ons / plugins

For **vlxshell** and **ffwrapper** the Firefox allowedSite database can be preset during startup.

The parameter is **-allowedSItes**, the arguments are comma separated URLs, which will be trusted. Multiple URLs can be added.

This allows to specify websites, that are allowed to install add-ons and plugins without a warning.

Update

Ater updating VISULOX the script has to be run manually again

```
$VLXDIR/tools/ffw/setup/installFirefoxWrapper.sh
```

Check the file permissions! Files must be readable by vlx user.

VISULOX Firefox CITRIX / ICA integration

Using Firefox with Citirx Receiver (CR) plugin to address XenApp / XenDesktop.

Firefox with plugin

CITRIX Receiver 13+ has to be installed on the platform. This plugin can be used in three ways:

	CMD	Login script	User	Profile	VLX Transit Zone	Recommended
Platform Firefox	firefox	unix.exp / vlxUnix.exp	Unix user	persistence		

	CMD	Login script	User	Profile	VLX Transit Zone	Recommended
vlxshell	vlxshell -client firefox -drive E	visulox.exp	vlxtransit	non persistence	✓	✓
VISULOX Firefox Wrapper	tools/ffw/ffwrapper -drive E	vlxUnix.exp	Unix user	persistence	✓	

Because the platform does not provide the VISULOX Transit Zone integration and a persistence Firefox profile is not needed, the recommended integration is **vlxhell**.

See also: VISULOX Firefox integration

Edit ICA Client Profiles

These files can be built with the Citrix Connection Manager "**wfmgr**"

```
vlxshell -client citrixmgr -profile <name of citrix profile> Using the
```

The ICA client can be downloaded from the CITRIX homepage.

Related information:

How to pass user credentials to an application - VISULOX Single Sign On - SSO

How to assign a fixed username

23.1.34 VISULOX Chrome and Chromium integration

VISULOX provides the possibility to start the platform provided Chrome and Chromium browser in an independent context **(vlx user**).

The application is assigned in the datastore.

```
vlxshell -client chrome -- <url>
vlxshell -client chromium -- <url>
```

The type (firefox, chrome, etc) can be used instead of the **vlxshell** command in the Application Command field and **-client <type>** in the Argument for Command field.

Providing additional information to Chrome or Chromium as arguments has to be separated with "--" from the vlxshell arguments.

See also:

How to install Google Chrome

VISULOX Player: integrated or client side

How to attach Chrome/Chromium download directory to vlxtransit

23.1.35 How to work with VISULOX Datasources

Overview

VISULOX handles users, groups and applications. These are the so called datasources and they are imported by the VISULOX Importer Service.

Applications and VISULOX PORTAL user profiles are defined in the VISULOX PORTAL Datastore and are imported by default.

- Overview
- Usage datasource
  - Parameter list
    - Import only users within the LOGINGROUP
    - Import only users within the LOGINGROUP - No computer objects / only persons
    - Import only groups with VLX_ or POC-Groups in the name
  - Additional placeholders
- Configuration
  - List datasources
  - Detailed list as CSV list
  - Edit a datasource
  - Example of a fallback datasource
  - Temporarily disabling a datasource
  - Dataobjects import statistic
- Usage importer
  - ./lib/service/importer.tcl
- LDAP pagesize
- Known issues and comments
- Related information

Usage datasource

The VISULOX PORTAL authentication system can use different user repositories (UR). The URs are configured under services and with the tarantella service command.

To allow VISULOX policies on users and groups from different URs, these URs can be configured.

```
visulox datasource add | list | edit | delete | copy | check | clean | query | stat <parameters>
```

Nested groups
VISULOX does **not** support nested groups! (Using nesting, a group can be added as a member of another group).

Parameter list

Parameter	Value / example	Comment
-name	myDomain myDomain:1 myDomain:2	The name of the datasource. Without a fallback postion it is the primary datasource. :1 will be the first fallback entry.
-location	<any string>	String to identify the datastource in the GUI. Recommendation is to use a short string.
-pwdprotocol	<oud>, <ipa>, <ad>, <none>	Password protocol has to be set for password change. If **visulox datasource edit -name <> -pwdprotocol** is set to **none** and the password has to be changed, the user cannot log in and a message is displayed in the login mask, that he has to change his password.
-base		Searchbase in the LDAP tree.
-cypher	<*cipher string*>	Cipher string to use <>. For a list of available cipher strings, see: https://docs.openssl.org/3.0/man1/openssl-ciphers/#cipher-strings
-host	host/IP of the datasource	

Paramater	Value / example	Comment
-port	389 is the default LDAP port	363 is the secure LDAP port
-secure	true/false/verify	Defines unsecure (LDAP) or secure connection (LDAPS). For LDAPS also have a look at: Troubleshooting: LDAPS
-type	LDAP	Currently only LDAP connections are supported. LDAPS is controlled via **-port** and **-secure**.
-cafile	<path to cafile>	
-username	<username>	User is allowed to read the LDAP server. ⚠ The username depends on the configuration entries on the AD servers. The following fields can be used for the connection, if set: • distinguishedName • cn • userPrincipalName If a field is not set in AD, it can not be used for the connection.
-password	<passcode>	Password of the user who can access the LDAP server. STDIN input via CLI is possible as well.

Paramater	Value / example	Comment
-mapping		Mapping schema in VISULOX to map the attributes to the internal values. ⚠ Two mappings are available MSAD, LDAP. See: How to configure alternate mappings for datasources
-paging	true | false	The AD default search result is limited to 1000 objects. It can be extended, but it is a change on the AD and so this is not the best solution. This setting allows to disable the paging feature, even if the LDAP Server provides this feature.
-searchadmin	LDAP search string to get users, which are related to be admins.	The searchstring can include a place holder "%SEARCH_STRING%" to use the -filter option of the ldap.tcl test command. Internally this placeholder is not used in VISULOX. Currently there is no usecase for that!
-searchgroup	LDAP search string to get the groups	The searchstring can include a place holder "%SEARCH_STRING%" to use the -filter option of the ldap.tcl test command. Internally this placeholder is not used in VISULOX. If (distinguishedName=%SEARCH_STRING%) is in the "searchgroup", it is possible to use ldap.tcl with -filter <dn of group) to get additional data from the LDAP server in a script. Currently there is no usecase for that!
-searchuser	LDAP search string to get users, which can log into VISULOX PORTAL.	The searchstring can include a place holder "%SEARCH_STRING%" to use the -filter option of the ldap.tcl test command. Internally this placeholder is not used in VISULOX. If (distinguishedName=%SEARCH_STRING%) is in "searchuser", it is possible to use ldap.tcl with -filter $VLXOWNER to get additional data from the LDAP server in a script.
-groupfilter	<regexp on groups>	The AD provides all the groups assigned to a user and all the groups itself. This parameter allows to reduce the data from the user repository to the relevant information, i.e -groupfilter "CN=VLX" imports only groups beginning wth cn=VLX. The value is a regexp (http://www.tcl.tk/man/tcl8.6/TclCmd/re_syntax.htm). So -groupfilter "CN=VLX|CN=portal" will import two groups.

Paramater	Value / example	Comment
-dse	Disable search extensions	Disable built search extensions for searchuser / searchadmin / searchgroup. (e.g. useful for OUD) Auto-adjust will be disabled. Important is that searchuser / searchadmin / searchgroup contain "%SEARCH_STRING%", otherwise ./ldap.tcl -filter does not work.

A search query on an AD is limited to 1000. If this is the case, the MaxPageSize must be configured by the AD Administrator on the AD site (http://support.microsoft.com/kb/315071/en).
Better: Enable/disable the paging feature with the **visulox datasource -paging** command.

If too many irrelevant users or groups are imported the searchuser or searchgroup query must have an additional criteria.

Import only users within the LOGINGROUP

```
-searchuser "(&(objectClass=person)(memberOf=$LOGINGROUP)(|(distinguishedName=%SEARCH_STRING%)(cn=%SEARCH_STRING%)
(givenName=%SEARCH_STRING%)(uid=%SEARCH_STRING%)     (mail=%SEARCH_STRING%)(sAMAccountName=%SEARCH_STRING%)))"
```

Import only users within the LOGINGROUP - No computer objects / only persons

```
-searchuser "(&(objectClass=person)(!(objectclass=computer))(memberOf=$LOGINGROUP)(|(distinguishedName=%SEARCH_STRING%)
(cn=%SEARCH_STRING%)(givenName=%SEARCH_STRING%)(uid=%SEARCH_STRING%)     (mail=%SEARCH_STRING%)
(sAMAccountName=%SEARCH_STRING%)))"
```

Import only groups with VLX_ or POC-Groups in the name

```
-searchgroup "(&(objectClass=group)(|(cn=VLX_*)(cn=POC-GROUPS*))(|(distinguishedName=%SEARCH_STRING%)(cn=%SEARCH_STRING%)
(gidNumber=%SEARCH_STRING%)))"
```

Make sure that distinguished names are always used for the fields in the search string.

Additional placeholders

The default setting for the parameter **-type** is "**ldap**". LDAPS is controlled via **-port** and **-secure**.

Two placeholders are available **%isUser%** and **%isGroup%**:

```
::isUser {&(|(objectClass=user)(objectClass=person))(!(objectClass=computer))(!(userAccountControl:1.2.840.113556.1.4.803:=2))}
::isGroup {|(objectClass=group)(objectClass=posixGroup)}
```

With these placeholders a default LDAP query string is available for **searchuser** and **searchgroup**, that should work in most cases and only has to be set, if a subset of users / groups should be read out.

searchadmin is set with:

```
'(&(%isUser%)(memberOf=CN=VLX_ADMINS,DC=myDomain,DC=de))'
```

A bracket check is implemented for the LDAP strings. The number of opened brackets must match the number of closed brackets.

Configuration

List datasources

```
visulox datasource list
Datasources
    ------------------------------------------------------------
    |         name |  location |                host | disabled |
    ------------------------------------------------------------
    |    company:0 |  EMPLOYEE |      srv1.company.de |    false |
    |   myDomain:0 | Stuttgart | ur1.stgt.mydomain.de |    false |
    |   myDomain:1 |   Hamburg |  ur2.hmb.mydomain.de |    false |
    | remoteuser:0 | EXTERNALS |      srv2.company.de |    false |
```

```
    ------------------------------------------------------------
```

Detailed list as CSV list

```
visulox datasource list -name  myDomain -info -format csv

name;parameter;value
myDomain,0;location;Stuttgart
myDomain,0;host;ur1.stgt.mydomain.de
myDomain,0;type;ldap
myDomain,0;username;CN=Logon,OU=Admins,DC=myDomain,DC=de
myDomain,0;port;389
myDomain,0;password;<hidden>
myDomain,0;attributes;objectclass dn mail uid cn surname mobile member memberOf c countryCode
myDomain,0;base;OU=Users,DC=myDomain,DC=de
myDomain,0;disabled;false
myDomain,0;groupfilter;cn=
myDomain,0;mapping;MSAD
myDomain,0;searchadmin;(&(objectClass=person)(memberOf=CN=portaladmin,CN=Users,DC=test,DC=de))
myDomain,0;searchgroup;(&(objectclass=posixGroup)(|(cn=%SEARCH_STRING%)(gidNumber=%SEARCH_STRING%)))
myDomain,0;searchuser;(&(objectclass=person)(|(distinguishedName=%SEARCH_STRING%)(cn=%SEARCH_STRING%)(givenName=%SEARCH_STRING%)
(uid=%SEARCH_STRING%)(mail=%SEARCH_STRING%)(sAMAccountName=%SEARCH_STRING%)))
myDomain,0;vlx_source;vTABOL6U4SGD1510
myDomain,1;location;Hamburg
myDomain,1;host;ur2.hmb.mydomain.de
myDomain,1;type;ldap
myDomain,1;username;CN=Logon,OU=Admins,DC=myDomain,DC=de
myDomain,1;port;389
myDomain,1;password;<hidden>
myDomain,1;attributes;objectclass dn mail uid cn surname mobile member memberOf c countryCode
myDomain,1;base;OU=Users,DC=myDomain,DC=de
myDomain,1;disabled;false
myDomain,1;groupfilter;cn=
```

```
myDomain,1;mapping;MSAD
myDomain,1;searchadmin;(&(objectClass=person)(memberOf=CN=portaladmin,CN=Users,DC=test,DC=de))
myDomain,1;searchgroup;(&(objectclass=group)(|(cn=%SEARCH_STRING%)(gidNumber=%SEARCH_STRING%)))
myDomain,1;searchuser;(&(objectclass=person)(|(distinguishedName=%SEARCH_STRING%)(cn=%SEARCH_STRING%)(givenName=%SEARCH_STRING%)
(uid=%SEARCH_STRING%)(mail=%SEARCH_STRING%)(sAMAccountName=%SEARCH_STRING%)))
```

The command dumps the current configured datasources with all their values.

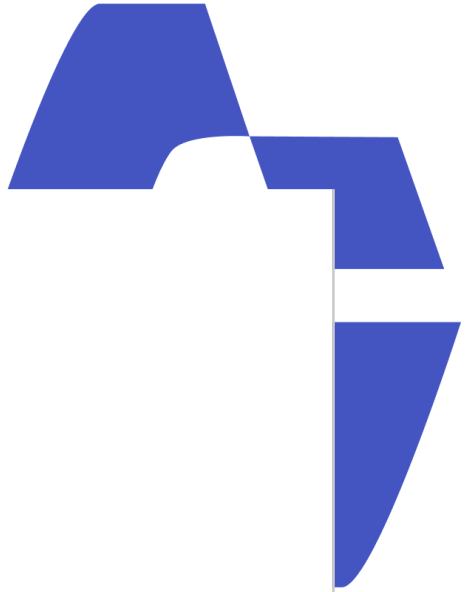
Edit a datasource

```
visulox datasource edit -name myDomain              \
  -location   Stuttgart                             \
  -type       ldap                                  \
  -host       ur1.stgt.mydomain.de                  \
  -port       389                                   \
.....
```

VISULOX supports the configuration of fallback or backup datasources. This can be done by adding additional datasources with the same name followed by the fallback position (<name>:<position>) and different physical parameters.

Example of a fallback datasource

```
visulox datasource list -name MyDomain

Datasources
    ------------------------------------------------------------------
    |       name | parameter |                                 value |
    ------------------------------------------------------------------
    | myDomain,0 |  location |                              Stuttgart |
    | myDomain,0 |      host |                 ur1.stgt.mydomain.de |
```



```
| myDomain,0 |      type |                                    ldap |
| myDomain,0 |  username | CN=Logon,OU=Admins,DC=myDomain,DC=de |
| myDomain,0 |      port |                                     389 |
| myDomain,0 |    secure |                                   false |
| myDomain,0 |  password |                                <hidden> |
| myDomain,1 |  location |                                 Hamburg |
| myDomain,1 |      host |                  ur2.hmb.mydomain.de |
| myDomain,1 |      type |                                    ldap |
| myDomain,1 |  username | CN=Logon,OU=Admins,DC=myDomain,DC=de |
| myDomain,1 |      port |                                     389 |
| myDomain,1 |  password |                                <hidden> |
-------------------------------------------------------------------
```

Temporarily disabling a datasource

```
visulox datasource edit -name  myDomain:1 -disabled true
```

Dataobjects import statistic

```
visulox datasource stat
Dataobjects import statistics
    ------------------------------------------------------------
    | datasource |            class | duration | objects | rtn |
    ------------------------------------------------------------
    |  DATASTORE |      application |    1.211 |       5 |  OK |
    |  DATASTORE | applicationgroup |    0.622 |       1 |  OK |
    |  DATASTORE |             host |    0.553 |       0 |  OK |
    |  DATASTORE |             user |    1.803 |       1 |  OK |
    |      TOTAL |                  |    4.189 |       7 |     |
    ------------------------------------------------------------
```

Datasource template
A datasource template can be found in **/opt/visulox/setup/examples**

Usage importer

The **service/importer.tcl** imports the datasources on each VISULOX Access Node. The command is run as a service, but can be called manually as well to see how the import works:

./lib/service/importer.tcl

```
/opt/visulox/lib/service/importer.tcl
Dataobjects import statistic
    ------------------------------------------------
    | datasource |       class | duration | objects |
    ------------------------------------------------
    |  DATASTORE | application |    0.386 |      23 |
    |  DATASTORE |        user |    0.314 |       1 |
    |        POC |       group |    0.222 |       5 |
    |        POC |        user |    0.218 |       1 |
    |     TESTAD |       group |    0.318 |       2 |
    |     TESTAD |        user |    0.398 |     114 |
    | TESTMASTER |       group |    0.281 |       7 |
    | TESTMASTER |        user |    1.457 |    1269 |
    |      TOTAL |             |    3.594 |    1422 |
    ------------------------------------------------
```

If the cluster key has been changed (attaching new nodes) all datasources have to be re-registered.

On all Filter Object pages a "**Reload Objects**" button is displayed. With this button the reload of LDAP import can be triggered by the user.

LDAP pagesize

If necessary, the LDAP pagesize can be adjusted. The default value is **250**.

```
visulox config -name importer.ldap.pagesize
    ------------------------------------------
    | changed | key                   | value |
    ------------------------------------------
    |         | importer.ldap.pagesize | 250   |
    ------------------------------------------
```

Known issues and comments

Import of nested groups is not supported.

Connecting to AD via LDAP or LDAPS is supported.

Related information

General command line configuration

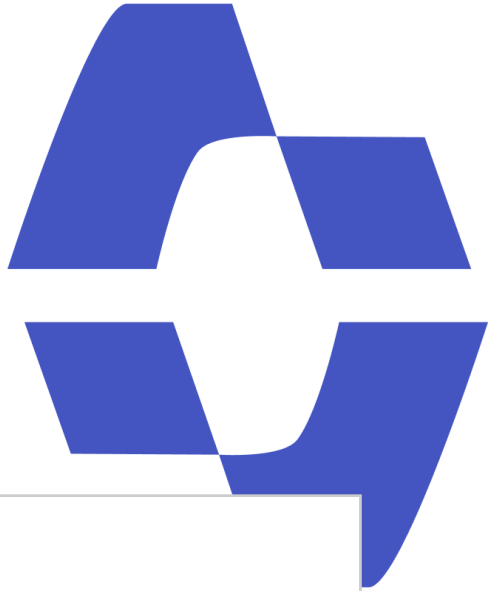
How to configure alternate mappings for datasources

Creating VISULOX user groups based on an AD/LDAP attribute

How to use Unix user profiles

How to test and check an LDAP datasource in VISULOX

Troubleshooting: LDAPS



How to check Policy, Datastore and LDAP assignments

In the datasource table all applications, users and LDAP entries can be found.

To check if there are applications assigned to users, that are not longer available in LDAP or VISULOX filters with users/applications, which do not longer exist, the following command can be used:

```
visulox assignments policy

visulox assignments datastore
```

Detailed info with **-verbose**.

The assignments are checked with Integrity-Check as well:

```
-------------------------------------------------------------------------------------
| option       | cat       | info                                           | returnCode |
-------------------------------------------------------------------------------------
| -assignments | datastore | 287 unresolveable LDAP Assignments in datastore | WARNING(2) |
| -assignments | policy    | 4 filters in policies will not match           | WARNING(2) |
-------------------------------------------------------------------------------------
```

How to test and check an LDAP datasource in VISULOX

Overview

During setup it is necessary to know, what the AD/LDAP servers offer to VISULOX.

/opt/visulox/lib/utils/ldap.tcl is a helpful tool. This article describes how to use it for testing.

- Overview
- Usage
- Related information

Usage

Command	**Prints**
./ldap.tcl	List all users
./ldap.tcl -source <name of the LDAP Datasource>	List all users (object) in the specific LDAP datasource
./ldap.tcl -source <name of the LDAP Datasource> -objectclass group	List all groups
./ldap.tcl -source <name of the LDAP Datasource> -print	List of available attributes from the specified LDAP datasource
./ldap.tcl -source <name of the LDAP Datasource> -filter Extern	List all users, which have "**Extern**" in the objectname. This works only if the datasource is configured with the %SEARCHFILTER% place holder.

Command	Prints
./ldap.tcl -source <name of the LDAP Datasource> -fields object,sn,mail	List all users (object) with **sn** and **mail**
./ldap.tcl -examples	List of examples

The output can be controlled with **-format**.

Related information

General command line configuration

How to work with VISULOX Datasources

Microsoft LAPS integration

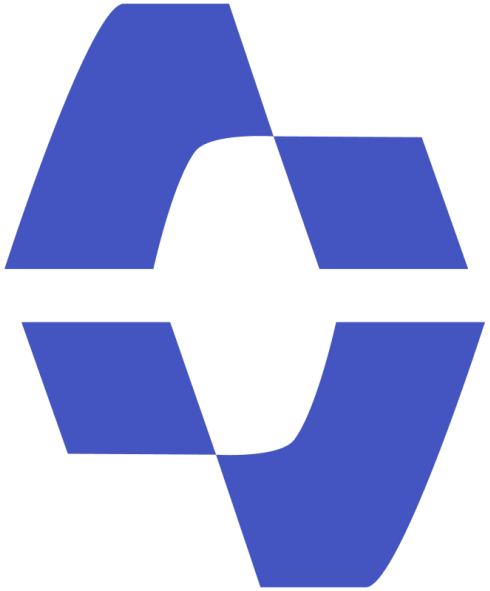
Introduction

Microsoft provides the **L**ocal **A**dministrator **P**assword **S**olution (**LAPS**).
LAPS is a solution for the problem using a shared local account on each computer in the domain with an identical password.
LAPS solves this issue by setting a randomly chosen password on each computer in the domain for the shared local administrator account.
Domain administrators using this solution are able to determine, which users are authorized to read the passwords (e.g. Helpdesk-Administrators).

The passwords are arranged and saved randomly in Active Directory protected by **A**ctive **C**ontrol **L**ists (**ACL**).
Only authorized users can read and request resetting these passwords.

Related Microsoft article: https://www.microsoft.com/en-us/download/details.aspx?id=46899

LAPS integration is also possible for Unix applications.



Implementation in VISULOX

Microsoft LAPS is addressed via **VISULOX Resources** for Windows **and** Unix applications.

Two types are available:

- vlxResource=@LAPS_GLOBAL
- vlxResource=@LAPS_USER

The resources are set via the Hints field of the application.

In case of **@LAPS_USER**, the password is querried with the user of the session.
Precondition is that the user is authorized.

In case of **@LAPS_GLOBAL** the password is querried with a VISULOX user.
This can either be the user, that is stored in the AD datasource or a user, which is depositted in an additional resource.

> In Workspace the "**Force Authentication**" check box can be used to enter a different account, that is allowed to retrieve the LAPS credentials.

Configuration

The following VISULOX configuration parameters have to be adjusted:

Parameter	Description
laps.datasource	Datasource of the LAPS Service AD (Needed to determine the LDAP server, where the LAPS passwords can be found. If different from the users, a datasource has to be created, which imports the users and groups.)

Parameter	Description

laps.adminuser	Adminuser for client access
	VISULOX Resources can be used, for example:
	`vlxResource=@LAPS_GLOBAL:root`
	or if the Windows admin user is different:
	`vlxResource=@LAPS_GLOBAL:serverAdmin`
	`vlxResource=@LAPS_GLOBAL:clientAd`

laps.audit	Successfull LAPS requests will be written to their session in VISULOX Audit
laps.filter	LDAP query string to determine the password
laps.resource	Alternate user authorized to read LAPS passwords (if not the user of the datasource)
laps.domain	Domain of the AD/LDAP server, that has the password

For access to a Windows system via LAPS, the **FQDN** of the host has to be assigned to the application.
This is the same name, that can be found in the LAPS data in Active Directory, usually in the attribute **dNSHostName**.

Hostnames longer than 15 characters
Computer objects in Microsoft Active Directory can not be longer than 15 characters.
If a computer with a longer hostname is jopined, it will be registered with a different "short name".
In this case the filter can be adjusted.

Therefore additional placeholders have been added to the **laps.filter** string:

regsub -all {%BASE%}	$filter $base
regsub -all {%HOST%}	$filter $host
regsub -all {%HOSTDOMAIN%}	$filter $hostdomain
regsub -all {%SHORTHOST%}	$filter $shorthost
regsub -all {%SHORTHOST_UPPERCASE%}	$filter $shorthost_upper
regsub -all {%NETBIOS%}	

Troubleshooting: LDAPS

If LDAPS is not working, the log file should be checked:

LDAPS error in log file

```
Protocol error: Error reading SEQUENCE response for handle <sockt> : partial
```

If this entry is shown in the log, the **ldap.secure.delay time** is set to a value, which is too fast..

To solve this, the delay time can be set to a higher value, with the following command:

```
visulox config edit -name ldap.secure.delay=<time>
```

Where ***<time>*** is the delay between each request in milliseconds.

If the check command throws the following error:

```
error: certificate verify failed
```

The CA file of the issuing authority should be added with **-cafile** or the parameter **-secure** should be changed from "**verify**" to "**true**".

23.1.36 Why is it not possible to sort some views in the GUI?

VISULOX Cockpit views can not be sorted by columns, where the postion is relevant for operation.

This effects all policies: **Login**, **Access**, **Application**, **Keystroke** and **File Transfer**.

Allowing to sort will change the view for the user and it is not clear how the real order is.

23.1.37 How to export information interactive from VISULOX

There are serveral ways to export data from the VISULOX database:

- The session as a ZIP archive
- The session into the VISULOX player
- The selected or displayed information in the views

- Session export
- Data export (Report)
- Report examples
- Related information

Session export

The export of session information includes also the events during and after the session has been terminated.

The event stream can have also keystroke information. This information is not exported by default. Export of the keystroke information can only be done if the VISULOX Cockpit is launched with the "**ksr**" tag. This tag can be set on the command line or in a Cockpit role.

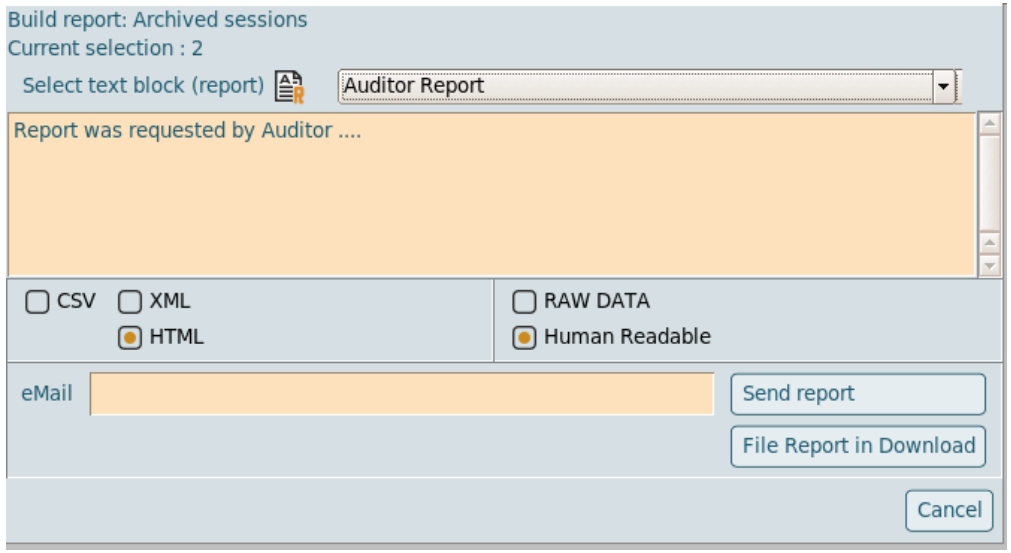
The recorded sessions are exported to the Transit Zone of the user (via Checkout button in the Cockpit or CLI), where they can be downloaded to the client.

Multiple checkout of 5 recorded sessions at once is supported.

See also: How to export information from VISULOX on the command line

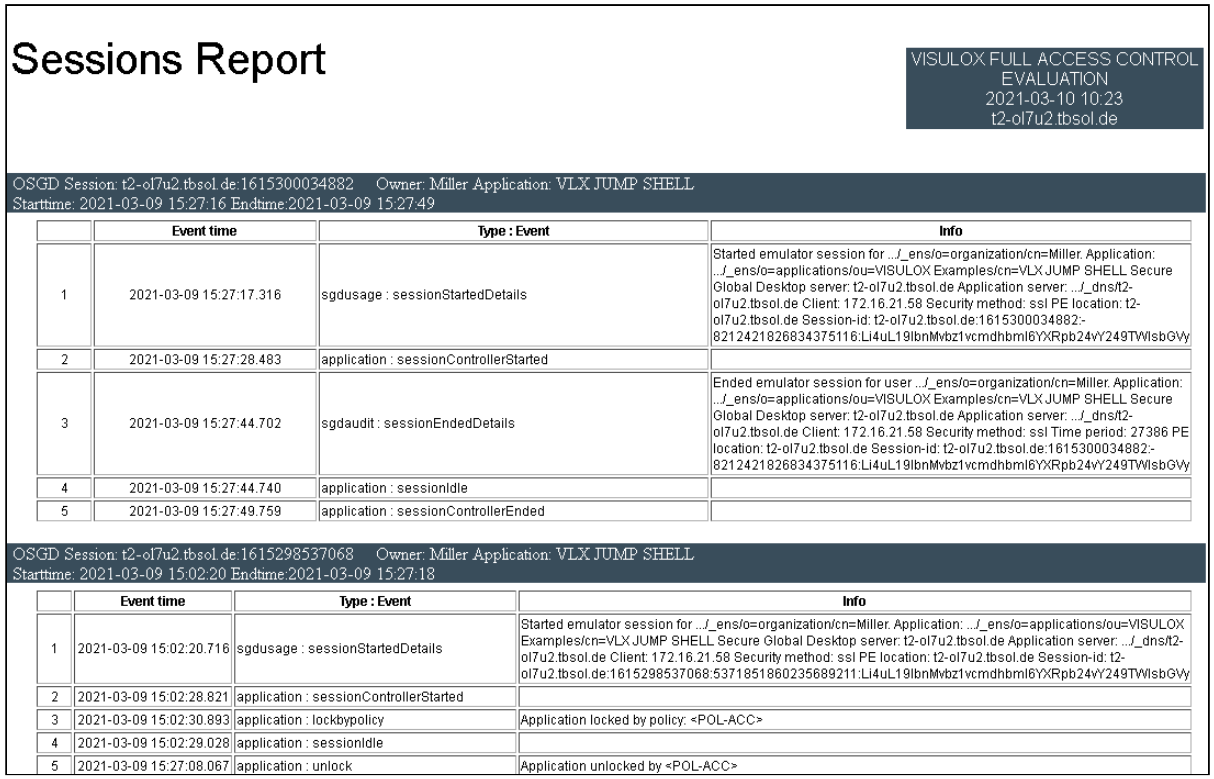
Data export (Report)

The user is able to select the export format and wether the report is sent via eMail or provided in Transit Zone.



Currently **CSV**, **XML** and **HTML** output is available and **RAW Data** or **Human Readable** can be selected as well.

- **Session report (HTML)**



Sessions Report

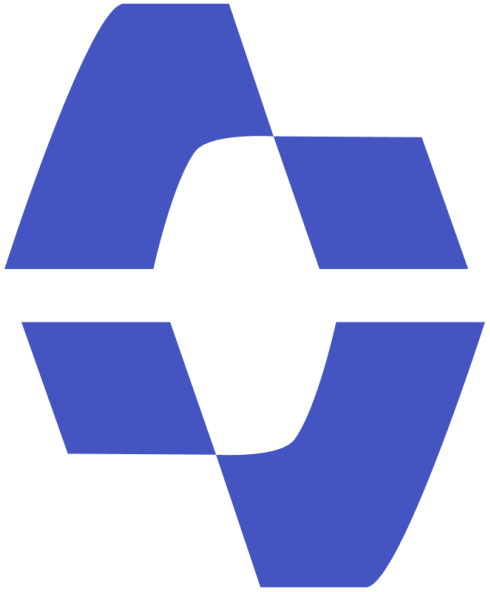
VISULOX FULL ACCESS CONTROL EVALUATION
2021-03-10 10:23
t2-ol7u2.tbsol.de

OSGD Session: t2-ol7u2.tbsol.de:1615300034882 Owner: Miller Application: VLX JUMP SHELL
Starttime: 2021-03-09 15:27:16 Endtime:2021-03-09 15:27:49

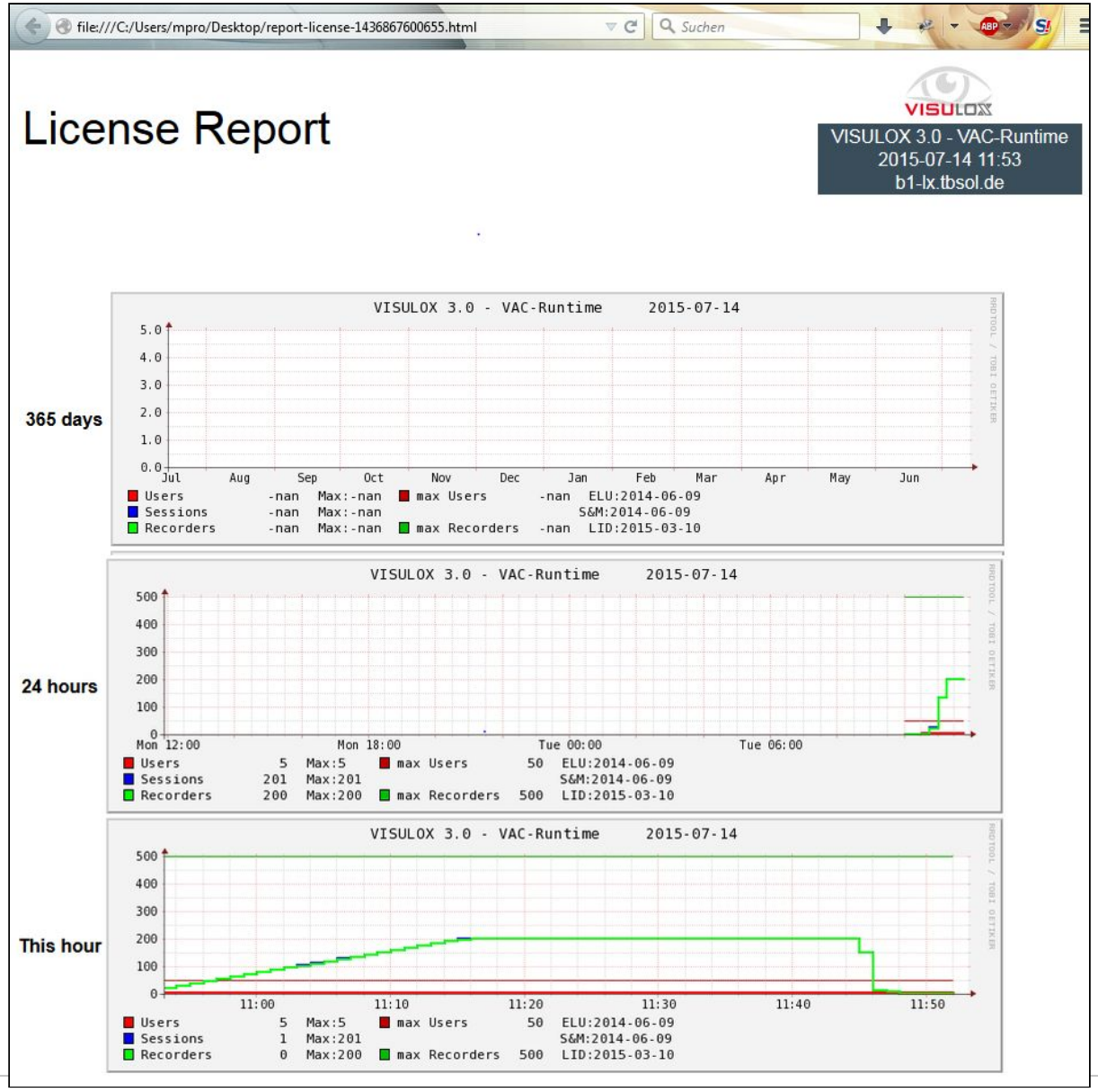
	Event time	Type : Event	Info
1	2021-03-09 15:27:17.316	sgdusage : sessionStartedDetails	Started emulator session for .../_ens/o=organization/cn=Miller. Application: .../_ens/o=applications/ou=VISULOX Examples/cn=VLX JUMP SHELL Secure Global Desktop server: t2-ol7u2.tbsol.de Application server: .../_dns/t2-ol7u2.tbsol.de Client: 172.16.21.58 Security method: ssl PE location: t2-ol7u2.tbsol.de Session-id: t2-ol7u2.tbsol.de:1615300034882:-8212421826834375116:Li4uL19lbnMvbz1vcmdhbml6YXRpb24vY249TWlsbGVy
2	2021-03-09 15:27:28.483	application : sessionControllerStarted	
3	2021-03-09 15:27:44.702	sgdaudit : sessionEndedDetails	Ended emulator session for user .../_ens/o=organization/cn=Miller. Application: .../_ens/o=applications/ou=VISULOX Examples/cn=VLX JUMP SHELL Secure Global Desktop server: t2-ol7u2.tbsol.de Application server: .../_dns/t2-ol7u2.tbsol.de Client: 172.16.21.58 Security method: ssl Time period: 27386 PE location: t2-ol7u2.tbsol.de Session-id: t2-ol7u2.tbsol.de:1615300034882:-8212421826834375116:Li4uL19lbnMvbz1vcmdhbml6YXRpb24vY249TWlsbGVy
4	2021-03-09 15:27:44.740	application : sessionIdle	
5	2021-03-09 15:27:49.759	application : sessionControllerEnded	

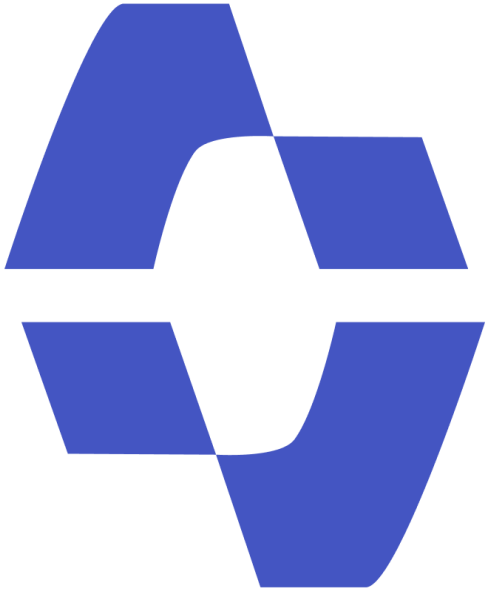
OSGD Session: t2-ol7u2.tbsol.de:1615298537068 Owner: Miller Application: VLX JUMP SHELL
Starttime: 2021-03-09 15:02:20 Endtime:2021-03-09 15:27:18

	Event time	Type : Event	Info
1	2021-03-09 15:02:20.716	sgdusage : sessionStartedDetails	Started emulator session for .../_ens/o=organization/cn=Miller. Application: .../_ens/o=applications/ou=VISULOX Examples/cn=VLX JUMP SHELL Secure Global Desktop server: t2-ol7u2.tbsol.de Application server: .../_dns/t2-ol7u2.tbsol.de Client: 172.16.21.58 Security method: ssl PE location: t2-ol7u2.tbsol.de Session-id: t2-ol7u2.tbsol.de:1615298537068:537185186023568921 1:Li4uL19lbnMvbz1vcmdhbml6YXRpb24vY249TWlsbGVy
2	2021-03-09 15:02:28.821	application : sessionControllerStarted	
3	2021-03-09 15:02:30.893	application : lockbypolicy	Application locked by policy: <POL-ACC>
4	2021-03-09 15:02:29.028	application : sessionIdle	
5	2021-03-09 15:27:08.067	application : unlock	Application unlocked by <POL-ACC>



- **License report (HTML)**


file:///C:/Users/mpro/Desktop/report-license-1436867600655.html
Suchen
License Report
VISULOX
VISULOX 3.0 - VAC-Runtime
2015-07-14 11:53
b1-lx.tbsol.de
365 days
VISULOX 3.0 - VAC-Runtime 2015-07-14
5.0
4.0
3.0
2.0
1.0
0.0
Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun
Users -nan Max:-nan
Sessions -nan Max:-nan
Recorders -nan Max:-nan
max Users -nan ELU:2014-06-09
S&M:2014-06-09
max Recorders -nan LID:2015-03-10
24 hours
VISULOX 3.0 - VAC-Runtime 2015-07-14
500
400
300
200
100
0
Mon 12:00 Mon 18:00 Tue 00:00 Tue 06:00
Users 5 Max:5
Sessions 201 Max:201
Recorders 200 Max:200
max Users 50 ELU:2014-06-09
S&M:2014-06-09
max Recorders 500 LID:2015-03-10
This hour
VISULOX 3.0 - VAC-Runtime 2015-07-14
500
400
300
200
100
0
11:00 11:10 11:20 11:30 11:40 11:50
Users 5 Max:5
Sessions 1 Max:201
Recorders 0 Max:200
max Users 50 ELU:2014-06-09
S&M:2014-06-09
max Recorders 500 LID:2015-03-10



Related information

(4.2.0) Modify VISULOX PORTAL Datastore via CLI

(4.2.0) How to export information interactive from VISULOX

(4.2.0) Reports

(4.2.0) How to export information from VISULOX on the command line

(4.2.0) Command "visulox support" - Creating a VISULOX Support Report

(4.2.0) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x

(4.2.0) Exporting / Importing Data

(4.2.0) How to control reports from the command line

(4.2.0) Migrating from VISULOX 3.x to 4.x

(4.3.2) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x

(4.3.2) Command "visulox support" - Creating a VISULOX Support Report

(4.3.2) How to control reports from the command line

(4.3.2) Modify VISULOX PORTAL Datastore via CLI

(4.3.2) How to export information interactive from VISULOX

(4.3.2) Migrating from VISULOX 3.x to 4.x

23.1.38 How to import users as VISULOX PORTAL administrators

The VISULOX PORTAL Service knows an important role: **administrator**.

Users in this role can use the VISULOX Portal Console of the VISULOX PORTAL Service.
A user can be assigned to the role with the VISULOX Portal Console or with the command line,
but only if there is an ENS profile in the datastore for this user.

This is normally not the case for users authenticated via LDAP.
To assign LDAP users to the administrator role, a LDAP mirror profile has to be configured in the datastore.

- Configuration
- Test commands
- Related articles

VISULOX provides a service to automatically create the LDAP mirror in the datastore: `alignRole`

This article explains how to configure VISULOX for automatic assignment of the VISULOX PORTAL Console to a specific group of users.

Users who are found with `searchadmin` in the datasources are created for VISULOX PORTAL administrators.

In this example it is:

```
-searchadmin '(&(objectClass=person)
                (memberOf=CN=PORTALADMIN,OU=Groups,OU=ToolBox,DC=tbsol,DC=de)
                (|(distinguishedName=%SEARCH_STRING%)
                  (cn=%SEARCH_STRING%)
                  (givenName=%SEARCH_STRING%)
                  (uid=%SEARCH_STRING%)
                  (mail=%SEARCH_STRING%)
                  (sAMAccountName=%SEARCH_STRING%)
                )
              )'
```

Configuration

`searchadmin` is configured with a datasource object within VISULOX (See: How to work with VISULOX datasources).

The `searchadmin` string should be checked. This parameter holds the search string for admin group.

```
visulox datasource list -name tbsol -info

Datasources
    ---------------------------------------------------------------------------------------------------------------------
    |    name |         parameter |                                                                                value |
    ---------------------------------------------------------------------------------------------------------------------
    | tbsol,0 |          location |                                                                            Stuttgart |
    | tbsol,0 |              host |                                                                 office-ad.tbsol.de |
    | tbsol,0 |              type |                                                                             ldap |
    | tbsol,0 |          username |                                                 CN=Logon,OU=ToolBox,DC=tbsol,DC=de |
    | tbsol,0 |              port |                                                                              389 |
    | tbsol,0 |          password |                                                                         <hidden> |
    | tbsol,0 |        attributes |                    objectclass dn mail uid cn surname mobile memberOf c countryCode |
    | tbsol,0 |              base |                                                        OU=ToolBox,DC=tbsol,DC=de |
    | tbsol,0 |          disabled |                                                                            false |
    | tbsol,0 |           mapping |                                                                             MSAD |
    | tbsol,0 |       searchadmin | (&(objectClass=person)(memberOf=CN=Admins,OU=Applikation,OU=ToolBox,DC=tbsol,DC=de)) |
    | tbsol,0 | searchapplication |                                                                                  |
    | tbsol,0 |       searchgroup |                                                                 (objectclass=group) |
    | tbsol,0 |        searchuser |                                                                (objectclass=person) |
    | tbsol,0 |        vlx_source |                                                                             vB1LX |
    ---------------------------------------------------------------------------------------------------------------------
```

List of users in the admin group

```
/opt/visulox/lib/utils/ldap.tcl -source TESTAD -objectclass admin
```

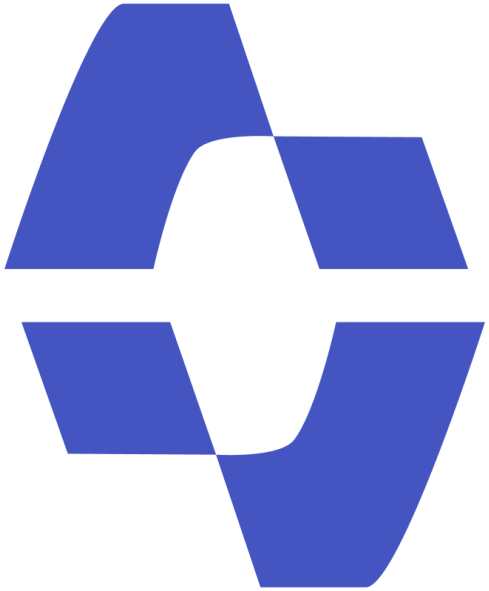
Test commands

VISULOX PORTAL command to list the admins

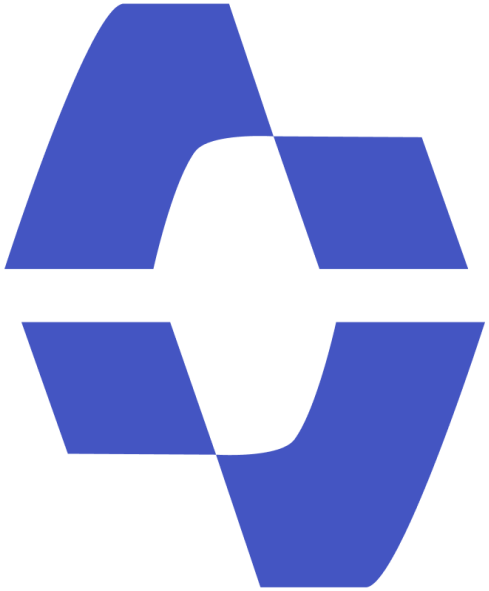
```
visulox-portal role list_members --role global
```

Related articles

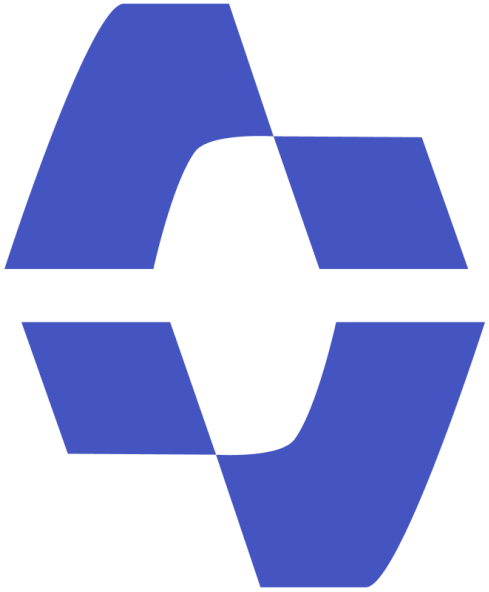
(4.2.0) VISULOX-GATEWAY Command
(4.2.0) How to exclude single datastore users from import
(4.2.0) VISULOX PORTAL Console
(4.2.0) How to configure a user account as a group account
(4.2.0) How to work with VISULOX Datasources
(4.2.0) VISULOX PORTAL Server Array
(4.2.0) VISULOX-PORTAL OBJECT Command
(4.2.0) How to use an LDAP/AD or Unix account to access the webservice
(4.2.0) VISULOX-PORTAL Command
(4.2.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.2.0) How to import users as VISULOX PORTAL administrators



(4.3.2) How to import users as VISULOX PORTAL administrators
(4.3.2) How to exclude single datastore users from import
(4.3.2) How to configure a user account as a group account
(4.3.2) How to work with VISULOX Datasources
(4.3.2) VISULOX-PORTAL Command
(4.3.2) VISULOX-PORTAL OBJECT Command
(4.3.2) VISULOX PORTAL Console
(4.3.2) VISULOX-GATEWAY Command
(4.3.2) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.2) VISULOX PORTAL Server Array
(4.3.2) How to use an LDAP/AD or Unix account to access the webservice
(4.1.1) VISULOX-GATEWAY Command
(4.1.1) How to exclude single datastore users from import
(4.1.1) How to configure a user account as a group account
(4.1.1) Attaching VISULOX Service to VISULOX PORTAL Service
(4.1.1) VISULOX-PORTAL Command
(4.1.1) How to use an LDAP/AD or a Unix account to access the Webservice
(4.1.1) VISULOX PORTAL Server Array
(4.1.1) VISULOX-PORTAL OBJECT Command
(4.1.1) How to import users as VISULOX PORTAL administrators
(4.1.1) How to work with VISULOX Datasources
(4.1.1) VISULOX PORTAL Console



(4.3.1) VISULOX-GATEWAY Command
(4.3.1) How to configure a user account as a group account
(4.3.1) How to exclude single datastore users from import
(4.3.1) How to work with VISULOX Datasources
(4.3.1) How to import users as VISULOX PORTAL administrators
(4.3.1) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.1) How to use an LDAP/AD or Unix account to access the webservice
(4.3.1) VISULOX PORTAL Server Array
(4.3.1) VISULOX-PORTAL OBJECT Command
(4.3.1) VISULOX-PORTAL Command
(4.3.1) VISULOX PORTAL Console
(4.3.0) VISULOX-PORTAL OBJECT Command
(4.3.0) How to exclude single datastore users from import
(4.3.0) How to configure a user account as a group account
(4.3.0) How to import users as VISULOX PORTAL administrators
(4.3.0) How to work with VISULOX Datasources
(4.3.0) VISULOX PORTAL Server Array
(4.3.0) VISULOX-GATEWAY Command
(4.3.0) VISULOX-PORTAL Command
(4.3.0) How to use an LDAP/AD or Unix account to access the webservice
(4.3.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.0) VISULOX PORTAL Console



VISULOX-GATEWAY Command
VISULOX-PORTAL OBJECT Command
VISULOX-PORTAL Command
VISULOX PORTAL Server Array
VISULOX PORTAL Console
How to exclude single datastore users from import
How to configure a user account as a group account
How to use an LDAP/AD or Unix account to access the webservice
How to import users as VISULOX PORTAL administrators
How to work with VISULOX Datasources
Attaching VISULOX Service to VISULOX PORTAL Service
How to use an LDAP/AD or Unix account to access the webservice
How to work with VISULOX Datasources
How to exclude single datastore users from import
(4.3.3) VISULOX-PORTAL OBJECT Command
Attaching VISULOX Service to VISULOX PORTAL Service
VISULOX PORTAL Console
(4.3.3) VISULOX-GATEWAY Command
(4.3.3) VISULOX-PORTAL Command
How to configure a user account as a group account
VISULOX PORTAL Server Array
How to import users as VISULOX PORTAL administrators

23.1.39 Security information about vlxsu and vlxchown (SUID bit)

During VISULOX installation the following binaries are set with SUID:

-r-sr-xr-x 1 root vlx 18760 Sep 17 14:14 ./lib/platform/vlxchown
-r-sr-xr-x 1 root vlx 38007 Sep 17 14:14 ./lib/platform/vlxsu

On request and NDA, amitego will provide the source code of these tools for security reviews.

- vlxchown
  - Usage
  - Command line arguments
  - Security
- vlxsu
  - Usage
  - Command line arguments
  - Optional arguments (args)
  - Security

vlxchown

vlxchown is used to chown files and/or directories to another **vlx*** user.

Usage

```
vlxchown USER PATH [PATH...]
```

Command line arguments

USER	Unix user matching vlx* in group vlx

PATH	Path to a file/directory. The ownership of those files is transferred to USER:vlx

Security

- Environment variable VLX_HOME must be set.
- Only vlx:vlx can call vlxchown.
- vlxchown must be owned by root:vlx, and setuid.
- Ownership is only transferred between members of the vlx group and from ttaserv.

vlxsu

setuid program to start specific apps as given user.

Usage

```
vlxsu [options] <user> <cmd> [<args>...]
```

Command line arguments

<user>	Name of the user of the target persona
<cmd>	Name of the command to run as persona <user>

<args>	One or more optional arguments to pass to the program

Optional arguments (args)

-h | -help | --help	Show usage and exit
-config	Show current vlxsu configuration (my_commands) and exit
-debug	Sset debug mode on
-x	Delete all files in home directory of <user>

Security

- Only vlx:vlx can call vlxsu.
- vlxsu must be owned by root:vlx, and setuid.
- The <user> must match a user prefix in my_commands.
- The <command> must match an entry in my_commands.
- Both PATH and LD_LIBRARY_PATH are preset.
- The environment of the target user is restricted.

SETUID

See the 2008 paper "Revising Setuid Demystified" at: http://code.google.com/p/change-process-identity/
In particular, the change of persona fails if the resulting persona is not the target persona.

23.1.40 How to pass user credentials to an application - VISULOX Single Sign On - SSO

- General usage
  - vlxshell connection
  - Windows connection
- Related Information

General usage

The primary login credentials of a user can be passed to the VISULOX Jump Environment for CITRIX and Windows connections.

To do this, the parameter "**vlxsso=1**" must be set in the Application Environment field in the datastore.

With this parameter a **sso_user** and **sso_password** is provided to the vlxshell system. These can be either the primary login credentials or overwritten with **vlxuser** / **vlxpwd**.
(See: How to assign a fixed username)

vlxshell connection

The vlxshell system uses these parameters to connect to the application.

Sometimes the provided user has to be mapped like "jmike" to "sys_jmike" or "jmike_adm". This can be done by using -usermask in the vlxshell call.

```
vlxshell -usermask "sys_%USER%", or vlxshell -usermask "%USER%_adm".
```

vlxshell parameters

Parameter	Description
-client <*value*>	Client type: xterm, vnx, freerdp, firefox, chrome, ... Default: <xterm>
-clientcmd <*value*>	Alternate path to client
-title <*value*>	Title of the GUI
-lang <*value*>	Language. Default <en>
-id <*value*>	Session ID
-owner <*value*>	Owner, who runs this GUI
-allowedsites <*value*>	List of allowedSites in Firefox profile
-nolang	Enforce no language
-usermask <*value*>	Mask to add a prefix and/or suffix to sso_user (prefix%USER%suffix)
-E <*value*>	Extension list for Firefox
-P <*value*>	Firefox profile archive or directory
-rdpfile <*value*>	RDP file or VISULOX Script Object

Parameter	Description
-profile <*value*>	Name of Citrix profile in database
-gateway-resource <*value*>	Name of gateway passcache resource
-resource <*value*>	Name of passcache resource
-sync	Enable vlxtransit to application
-wait <*value*>	Wait for connection in seconds. Default: <0>

Windows connection

For Windows connections **vlxWindows.exp** can be used, which is based on windows.exp with additional VISULOX entries.

With **vlxRdpNoUser.exp** the Windows login dialog will be presented to the user and no user/password will be passed through.

⚠ This works only if NLA on the Windows system is disabled. See also: Microsoft: Network Level Authentication (NLA)

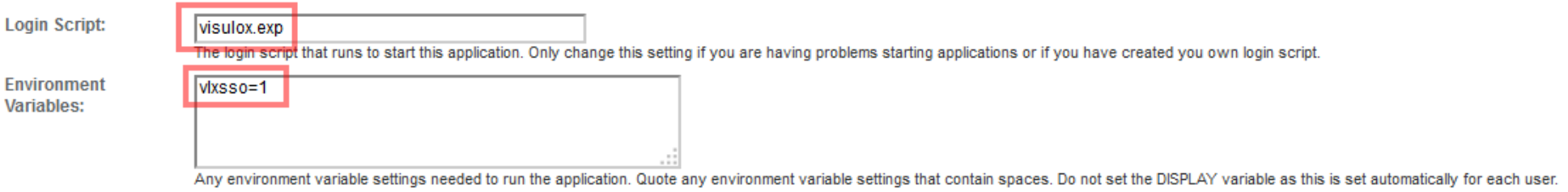
There are two possibilities to launch a Windows connection, where the login data will be entered:

- SHIFT-Click on the application link with vlxWindows.exp
- vlxShell with RDesktop / freerdp and "vlxsso=1;vlxuser="

Parameter	Description
vlxsso=0/1	If true, user and password is provided
vlxsso=1;vlxuser=<user-name>	Alternate user is provided
vlxsso=1;vlxuser=<user-name>;vlxpwd=<password>	Alternate user and password is provided
-no-nla	Allows in freeRDP the connection with/out NLA authentcation
%ANY%	Host is requested
-u xxxx	NOT ALLOWED as a parameter
-d <domain>	Can be added, if missing d "" is set. Domain can be also within the username (domain\\username)
-vlxResource <resource name>	Can be used with vlxWindows.exp and an existing resource instead of vlxuser/vlxpwd.

The following example shows a configuration of an RDP connection via **visulox.exp**, using the same credentials for login as provided to the VISULOX PORTAL:

Former **Environment Variables** setting (outdated):



Related Information

The application control variable "vlxMode"

VISULOX Firefox integration

Passcache

23.1.41 How to configure input idle detection

Sessions can be used over a long time and sometimes the question is, if the session is still in use. With input idle detection an event is triggered if the user is not interacting with the session within a configurable time window.

The input idle detection is enabled in general for any recorded session, independent of keystroke recording.

The configuration parameter **inputdetection.idle** controls the time in seconds for the event **inputFocusIdle**.
If the value is set to "**0**" the input idle detection is **disabled**.

inputdetection.idle

```
visulox config list -name inputdetection.idle
    ------------------------------------------
    | parameter           |      type | value |
    ------------------------------------------
    | inputdetection.idle | OPERATION | 300   |
    ------------------------------------------
```

Fire event when user is idle for 10 minutes

```
visulox config edit -name inputdetection.idle=600
```

23.1.42 VISULOX VNC integration

VISULOX provides the possibility to start the platform provided VNC viewer in an independent context (vlx user).

The application is assigned in the datastore.

```
vlxshell -client vnc -- <host>:<display>
```

Providing additional information with arguments is possible and has to be separated with "--" from the vlxshell arguments.

vlxResource in the Hints field of the application and the **-resource** parameter via CLI can be used (not allowed as transit user in a jump shell).

Requirements

The VNC viewer must be installed:

```
yum install tigervnc
```

See also:

How to install Google Chrome

VISULOX Player: integrated or client side

How to assign a fixed username

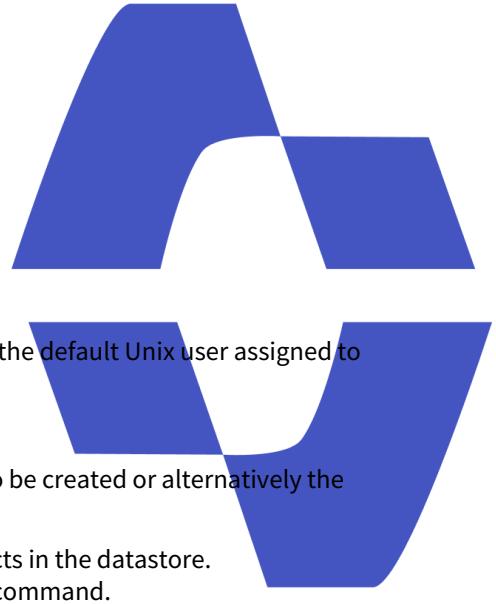
23.1.43 How to use an LDAP/AD or Unix account to access the webservice

Purpose

For platform security reasons in projects, it makes sense to disable the login of native Unix users into the VISULOX PORTAL. This can be done with the VISULOX PORTAL Console or via Command Line Interface.

If this is done the VISULOX user can no longer login. Therefore an LDAP account can be used as VISULOX Webservice User.

- Purpose
- Abstract
- Creating the LDAP user
- Disable Unix login
- Related information



Abstract

One of the VISULOX login authorities is the PAM stack. This allows any user listed in the Unix user repository to login into his account.

For security reason VISULOX PORTAL is limited to allow access only to those users, which have a VISULOX PORTAL profile in the datastore, i.e.. the default Unix user assigned to the user profile "o=Tarantella System Objects/cn=Administrator" is the unix user "root" (this can be changed).

With the VISULOX datasource distinguished LDAP name in searchadmin any LDAP user can be lifted to be a VISULOX PORTAL administrator.

In the latest VISULOX version (VLX 4.1.1) PAM is used for local users as well. **/etc/pam.d/visulox** can be adjusted. Profiles for local users have to be created or alternatively the Unix profile has to be activated again.

Each VISULOX PORTAL node needs a VISULOX webservice to retrieve information about other users, their sessions, the configuration and objects in the datastore. This VISULOX webservice user is created as Unix user (hidden unexpireable password) during VISULOX portal attach or can be assigned to the command.

If PAM authority has to be disabled fully, a special LDAP user can take the role of the VISULOX webservice.

The webservice user is always the node name. This name must exists in the user repository.

```
cn=<node>,OU=org2,OU=org1,DC=domain,DC=top
```

It is important, that this LDAP user has a password, that never expires.

Creating the LDAP user

Create a user for each VISULOX Access Node in one of the LDAP/AD servers. The name of the user must be the short name of the VISULOX Access Node. Every user must have a valid password with unlimited lifetime.

Attach with LDAP user

```
visulox portal attach -adminou <oupathtouser> -adminpwd <pwd>
```

Example

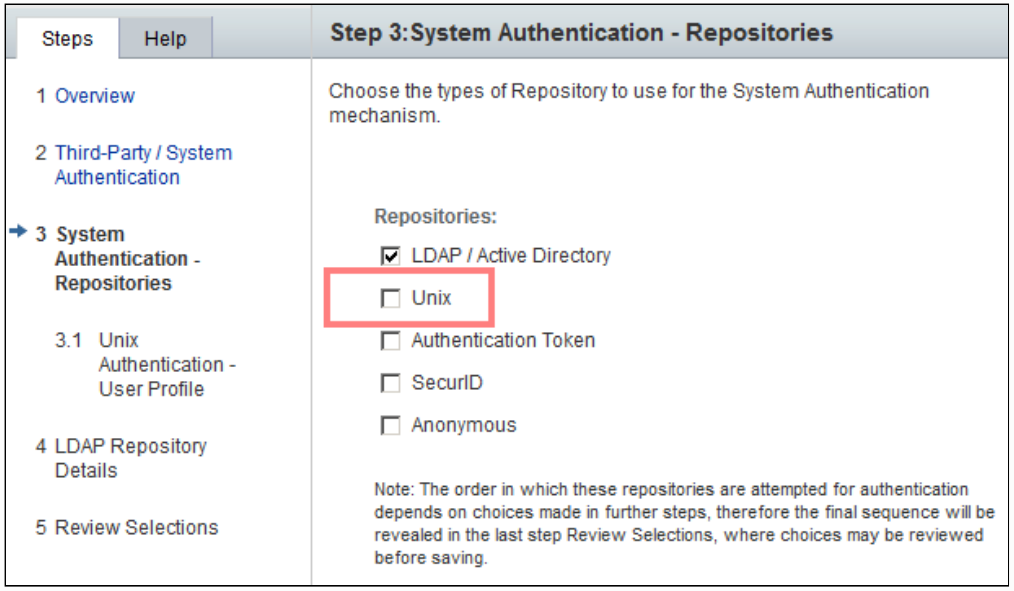
```
visulox portal attach -adminou "ou=Group1,ou=Org a,dc=domain,dc=com" -adminpwd <pwd>
```

The command creates the necessary LDAP mirroring in the VISUOX PORTAL datastore.

Disable Unix login

This will disable the local webservice user login.

./tarantella config edit --login-ens 0



Or disable Unix user login via command line

```
visulox-portal config edit --login-ens 0
```

Related information

(4.2.0) VISULOX-GATEWAY Command
(4.2.0) How to exclude single datastore users from import
(4.2.0) VISULOX PORTAL Console
(4.2.0) How to configure a user account as a group account
(4.2.0) How to work with VISULOX Datasources
(4.2.0) VISULOX PORTAL Server Array
(4.2.0) VISULOX-PORTAL OBJECT Command
(4.2.0) How to use an LDAP/AD or Unix account to access the webservice
(4.2.0) VISULOX-PORTAL Command
(4.2.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.2.0) How to import users as VISULOX PORTAL administrators
(4.3.2) How to import users as VISULOX PORTAL administrators
(4.3.2) How to exclude single datastore users from import
(4.3.2) How to configure a user account as a group account
(4.3.2) How to work with VISULOX Datasources

23.1.44 VISULOX Filestore

The files, films and snapshots created during recording or File Transfer by VISULOX are stored on the disk attached to the VISULOX Filestore.

These files are stored with an unique ID in a two-layer directory hierarchy. All files are encrypted and tagged with the creation time of 1.1.1970.

A file is always written to the filestore slot with the largest available capacity. There are two types of filestore slots. The default store and links to extra file system partitions to extend the file store.

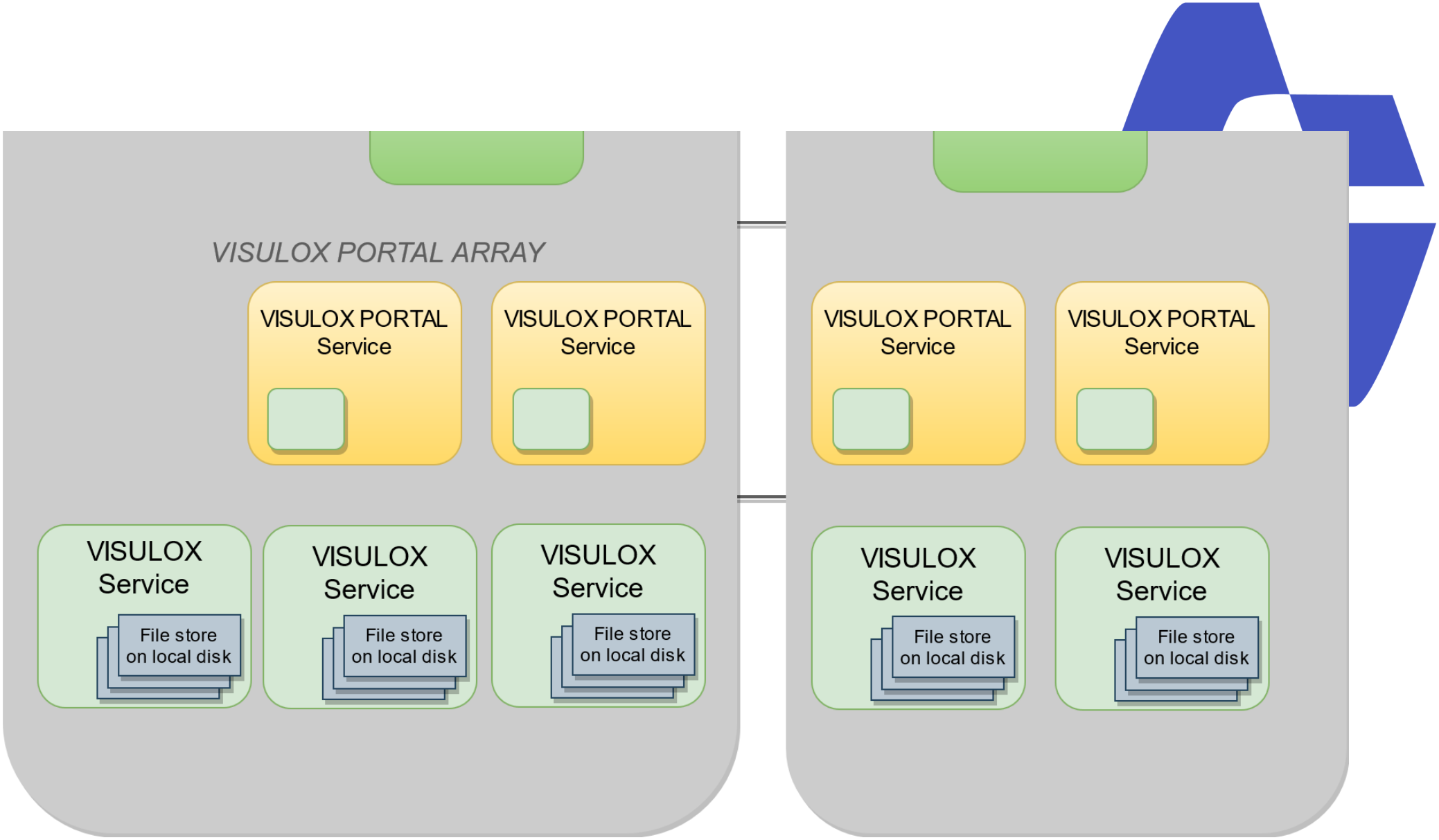
The default filestore is always a sym link to slot 0.

Filestore anchor

```
Jan  1  1970 d1/76/d1769ac2-99b7-48c5-bf77-ea2ad4dda44b
Jan  1  1970 12/26/12268c3f-3d97-437b-aa99-ee182bb47cfe
Jan  1  1970 a2/12/a212a0c3-5f18-4d56-a70e-5c6d6baff692
Jan  1  1970 52/b2/52b2e02e-7aab-430f-b37e-bf85284b3cb1
Jan  1  1970 8a/be/8abe83bc-9ffc-405e-9073-ed9dd452d48a
```

A slot is a mount point to a disk or NFS share. The slot 0 represents the local disk and is used as long as no other slot is enabled.

⚠ If there is a problem with an enabled slot, this slot will be disabled and the next available slot will be used. If no other slots are available, the default slot 0 will be used as fallback.


VISULOX PORTAL ARRAY
VISULOX PORTAL Service
VISULOX PORTAL Service
VISULOX PORTAL Service
VISULOX PORTAL Service
VISULOX Service
File store on local disk
VISULOX Service
File store on local disk
VISULOX Service
File store on local disk
VISULOX Service
File store on local disk
VISULOX Service
File store on local disk

To extend the filestore an extra disk or NFS share must be attached. Important are the permissions. They must be **vlx:vlxgroup** and are checked by integrity.

After attaching and enabling a slot, the default slot is disabled automatically.

Status

```
visulox store

File store status
    ------------------------------------------------------------------------------
    | slot | attached | enabled |    total |     used | available | capacity | files |
    ------------------------------------------------------------------------------
    |    0 |     true |   false |  98.43GB | 62.82GB |   30.61GB |      68% |     0 |
    |    1 |     true |    true | 978.52MB |  1.88MB |  909.30MB |       1% |     6 |
    |    2 |     true |    true | 978.55MB | 42.64MB |  868.57MB |       5% |     4 |
    |    3 |     true |    true | 978.55MB |  1.30MB |  909.91MB |       1% |     1 |
    ------------------------------------------------------------------------------
```

Using **-verbose** will also present the physical device of the file store slot.

Managing

There are two steps to activate slots by VISULOX:

```
visulox store attach -path <path to mount point>
visulox store enable -slot #
```

Attaching is always done to the next free slot.

Once a slot is enabled, it is used when new files are stored on the disk.

For example

```
mkdir /store1
mount /dev/sdb1 /store1
chmod -R 777 /store1
chown -R vlx: /store1
visulox store attach -path /store1
visulox store enable -slot 1
```

To stop storing files on a slot, the following command can be used:

```
visulox store disable -slot #
```

After a slot has been disabled, files can still be read from this slot.

To release a disk, the files on the disk must be moved to another disk:

```
visulox store migrate -from # -to #
```

Only a disabled slot can be used as a source.

Migrate only moves files that are relevant for the node, where the command is executed. The files remain where they were. This is important for sessionstores on NFS shares. With the parameter **-global** files will be moved regardless of their owner.

```
visulox store migrate -from # -to # -global
```

The **-global** parameter is set on Archive Nodes per default.

In case of a NFS share as destination, it may happen that not all files are migrated in the first run. Try to run the command again with **-force** option several times. The amount of files that were not copied should decrease with every run.

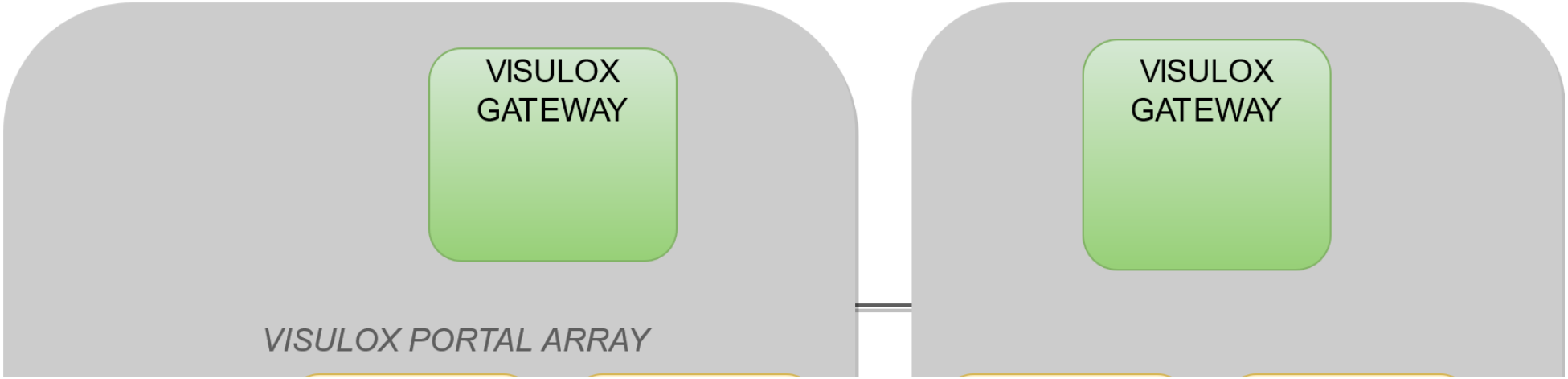
The managing of the filestore can be done when the VISULOX Service is online. This allows to add additional disks, if they are needed or to merge disks onto a disk with larger capacity.

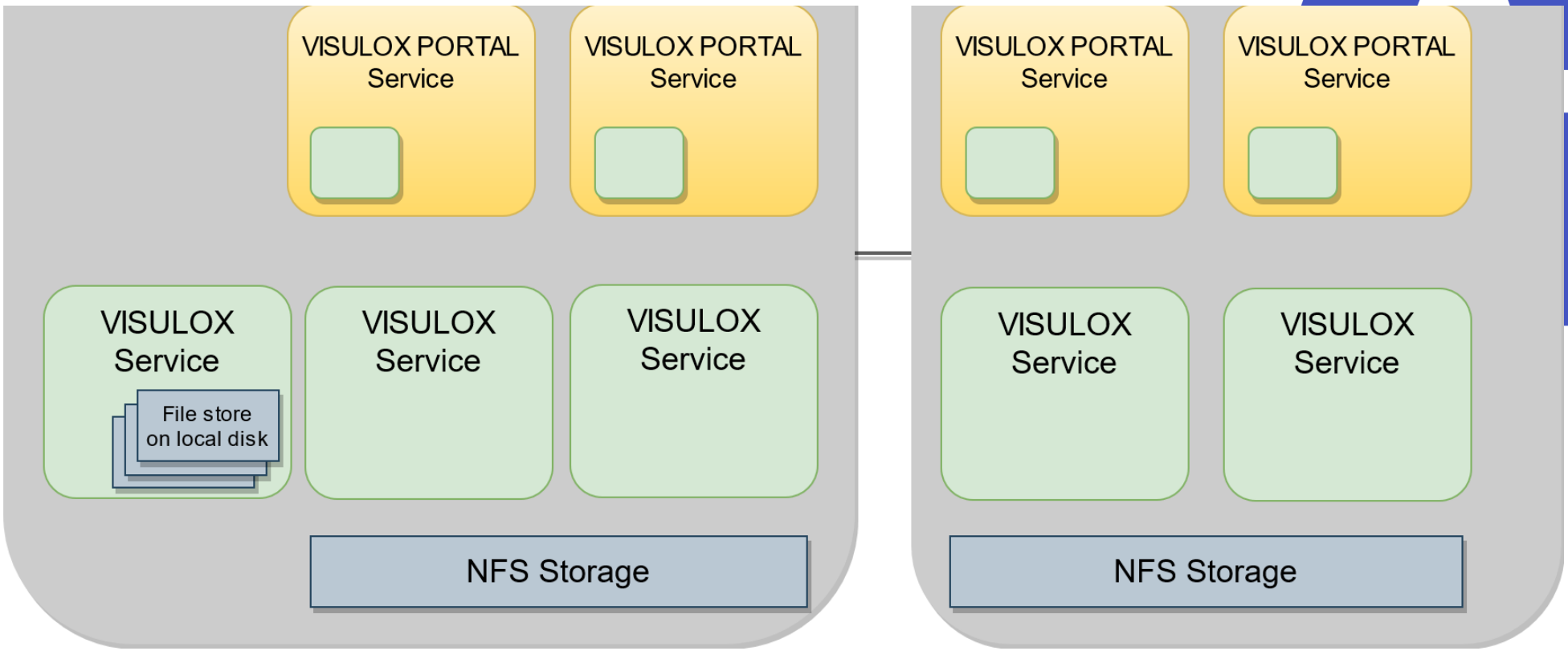
There are additional commands to check the integrity of the filestore.

Using NFS

A slot can be mounted on a NFS share. This has the advantage, that all files are seen across the cluster. It is recommended to have an **independent** NFS share for each location.

Do **not** use any purgeing of files if the Filestore was provided via NFS across **multiple Nodes**.





The outcome of using VISULOX Filestore via NFS is also an improved performance.

The Archive Server cannot be connected to the NFS share, because node and Archive life times are different. The node would delete the files in the Archive.

Make sure the mount points are available after reboot.

Make sure the mount points have the right permissions.
If there are many files in the filestore, operations like **status / migrate** will take a long time.

Filestore parameters

Parameter	Description
attach	Attach path to slot of filestore
changed	List files that do not match their records
detach	Detach slot from filestore
disable	Disable an attached slot
enable	Enable an attached slot
extras	List files present on disk, but not listed in the database Do not use this command on nodes, where replication is off and a shared NFS Filestore is used! The information will be wrong.
files	List files in filestore
get	Get file from filestore
migrate	Move files from source to destination slot

Parameter	Description
missing	List files registered in the database, but missing on disk **- details** More info regarding missing files
purge	Delete files, that do not match the database **-slot <*value*>** Slot to purge **-backup <*value*>** Directory collecting the purged files **-nonlocal** Also purge all non-local files **-dryrun** Show purge files only, do not actually purge
put	Put file into filestore
status	Filestore status
survey	Survey cluster for a given file

Using a commands like **"missing"** requires the VISULOX Services running.

On VISULOX Access Nodes in a cluster, that are used often for checkout or viewing films, the **purge -nonlocal** command should be used to get more free disk space again.
In case of large files this command will take some time.

This command should not be used if the Filestore was provided via NFS across **multiple Nodes**.

23.1.45 Adding a VISULOX Revision Server

Overview

In a VISULOX Cluster **one** node can be enabled/promoted to be a Revision / Archive Server.

The Revision Server is disabled for VISULOX application loadbalancing (no session controllers, no recorders).

> ⚠ VISULOX supports **one** Revision Server to guarantee 100% of the audit data from all production servers.

- Overview
- Requirement
- Configuration
  - Enable Archive mode on the node which will be promoted to be an Archive Node
  - Forced enabling of the Archive mode without prompting
- Setting the Archive lifetimes
  - Archive lifetimes
- X11 native port
- Accessing the information
- Troubleshooting
  - Is the Archive mode enabled?
  - Relevant services

Requirement

- All nodes must be joined in one cluster before Archive mode is enabled
- Archive retention times **must** be defined before setting the node tag "**archive**"
- Configuration of nodes must be in sync (**visulox config list -name layout**)
- If the node runs the VISULOX Cockpit (and is not on the VISULOX Access Node), the replication mode has to be set to **all**

Configuration

Enable Archive mode on the node which will be promoted to be an Archive Node

```
visulox archive -set
```

```
(From another node: visulox archive -set -node <archive-nodename>)
```

Forced enabling of the Archive mode without prompting

```
visulox archive -set -force
(From another node: visulox archive -set -force -node <archive-nodename>)
```

Archive mode cannot be disabled!

Setting the Archive lifetimes

Archive lifetimes are separated from the lifetimes in the production environment:

Archive lifetimes

```
visulox config list -name lifetime.archive

    ------------------------------------------------------
    | parameter                       |      type | value |
    ------------------------------------------------------
    | lifetime.archive.application    | OPERATION | 180   |
    | lifetime.archive.bigfiletransfer | OPERATION | 180   |
    | lifetime.archive.default        | OPERATION | 180   |
    | lifetime.archive.filetransfer   | OPERATION | 180   |
    | lifetime.archive.input          | OPERATION | 180   |
    | lifetime.archive.login          | OPERATION | 180   |
    | lifetime.archive.script         | OPERATION | 180   |
    | lifetime.archive.sgdaudit       | OPERATION | 180   |
    | lifetime.archive.system         | OPERATION | 180   |
    ------------------------------------------------------
```

The lifetimes (in days) are adjusted with:

```
visulox config edit -name lifetime.archive.filetransfer=360
```

During replication of the data on the Revision Server, the new retention time is set, if is is greater than the time in the production environment.
Standard retention data is 90 days, on the Revision Server it is 180 days. If an application enforces 500 days, this will not be overwritten.

X11 native port

The Revision Server must be able to communicate via X11 native (port 6000+).

See also: VISULOX SSH X11 Forwarding to VISULOX Application Nodes

Accessing the information

To access the data on the Revision Server a VISULOX Cockpit has to be configured in the VISULOX PORTAL Datastore with the assigned Revision Server.

It is helpful to use **-name vlxarchive** in the "**Arguments of Command**" field of the Archive Cockpit to display only the relevant pages.

Troubleshooting

Is the Archive mode enabled?

```
visulox archive
```

Relevant services

```
vlxService replication.tcl
vlxService archive.tcl
```

23.1.46 How to route a VISULOX application to other nodes

A VISULOX application could be the VISULOX GUI framework (VISULOX Cockpit,, File Transfer ...) or a VISULOX Transit Shell (shell, Firefox, Chrome, Chromium, VNC, etc).
All these applications have in common, that the login script is ***visulox.exp***.

During application definition in the VISULOX PORTAL datastore one or more hosts can be assigned to an application (tier3 load balancing).
If no host is assigned, the VISULOX PORTAL Server where the XPE is running (tier2 load balancing) is used.

The VISULOX session controller is balanced within a location and always assigned to the node with the fewest recorders.
The recorder per node is limited.

List of features

```
 ------------------------------------------------------------------------------------
| parameter                                 |  type | value | validation | vlx_default |
 ------------------------------------------------------------------------------------
| layout.vTABOL5U7DEVEL.feature.sc          | SETUP | 400   | isInteger  |         400 |
 ------------------------------------------------------------------------------------
```

The amount of recorders can be limited:

```
visulox config -name layout.<node>.feature.sc=200
```

This can be helpful, if this node will have additional tasks like the VISULOX GUI framework or VISULOX Transit Shell.

23.1.47 VISULOX Cluster

Usage

```
visulox cluster <options>
```

Option	Description
data	Displays cluster data
layout	Displays layout as known from router
build	-template creates template -f <file> build cluster from file

For example:

Displays VISULOX Cluster data (router working data - should be the same on each router):

```
visulox cluster data
```

Displays the layout as known by router:

```
Visulox cluster layout
```

A cluster with several nodes can be built automatically.

A template can be created that can be redirected to a file and processed:

```
visulox cluster build -template
```

Example template:

```
# CLUSTER BUILD FILE:
#
# to use with:
#
#       visulox cluster build -file FILE
#
# 1. Comment lines and blank lines are ignored.
# 2. A non-commented line stands for a node of the cluster.
# 3. A node is defined by the three fields hostname, location, zone
#    in that order, separated by blanks.
#
#       HOSTNAME1  LOCATION1  ZONE1
#       HOSTNAME2  LOCATION2  ZONE2
#       ...
#
# or with default zone (STANDARD)
#
#       HOSTNAME3  LOCATION3
#
# or with default location (STANDARD) and zone (STANDARD)
#
#       HOSTNAME4
```

```
#
# 4. Each listed node must have
#    - VISULOX installed,
#    - VISULOX running,
#    - the correct location and zone set.
# 5. If a node is already member of the cluster, it will be ignored.
#
# -> add your entries below:
#
```

A file that fulfills the template requirements can be used to build the VISULOX Cluster:

```
visulox cluster build -f <file>
```

Related articles

VISULOX Node hierarchy

VISULOX layout of a node

Network communication within VISULOX

23.1.48 VISULOX layout of a node

Overview

A VISULOX Node owns a layout. The layout has serveral fields.

Some of the fields are for information, some of them are controlling the behaviour of the node.

- Overview
- Usage
- Replication mode
    - Setting
- Example: disabling session controllers on a node
- Related articles

Usage

Fields	Description	Comment
layout.<*node*>.feature.sc	Each node can handle VISULOX Session Controller (recorder). This parameter defines how many can be provided by this node.	Can be configured to adapt the node to customer needs.
layout.<*node*>.fileexchange	Enable / disable File Echange (true, false)	Default setting is false
layout.<*node*>.ftpd	Enable / disable FTP Service (true, false)	Default setting is false
layout.<*node*>.location	This is a name tag for the location. Nodes with the same location are grouped. This field has the same meaning as in the VISULOX PORTAL.	Can be configured to adapt the node to customer needs.
layout.<*node*>.logname	Logical name of the node.	Set during installation, fixed,

Fields	Description	Comment
layout.<*node*>.replication	Replication mode of the node.(default, all, ftonly, false)	Replication service has special replication behavior on tables "session,files,events".
layout.<*node*>.runlevel	The current runlevel of the node.	Operation.
layout.<*node*>.shortinfo	A description field.	Information, can be configured to adapt the node to customer needs. The shortinfo is displayed with visulox status and on the cluster page in the Cockpit.
layout.<*node*>.webservice	Enable / disable webservice (true, false)	Default setting is false
layout.<*node*>.zone	This is a name tag for the zone. Nodes with the same zone are grouped.	Firewall ports must be configured between nodes in the same zone.

Replication mode

The replcation mode after setup is default, witch means, that each node with a VISULOX PORTAL Service and VISULOX Archive has all data, any other node has no session, files, events from other nodes.

There are different reasons to have more data:

- If the node is envolved with VISULOX File Transfer, the replication mode has to be to **ftonly**
- If the node runs the VISULOX Cockpit (and is not on the VISULOX Access Node), the repication mode has to be set to **all**

Setting

Setting	Description
default	If the node is a VISULOX PORTAL or VISULOX Archive - sessions, files, events are replicated from other nodes. On standalone servers default will lead to a warning in integrity. On standalone servers the replication mode can be set to false.
all	Independent wether VISULOX PORTAL or other node - session, files, events are replicated from other nodes.
ftonly	Only the File Transfer entries are replicated from other node. **ftonly** is necessary for VISULOX PORTAL Nodes and application nodes, if no other information is needed and Cockpit is on an extra server.
false	Replication service is disabled (recommended setting for standalone servers). If there is more than one node, this setting will lead to an error.

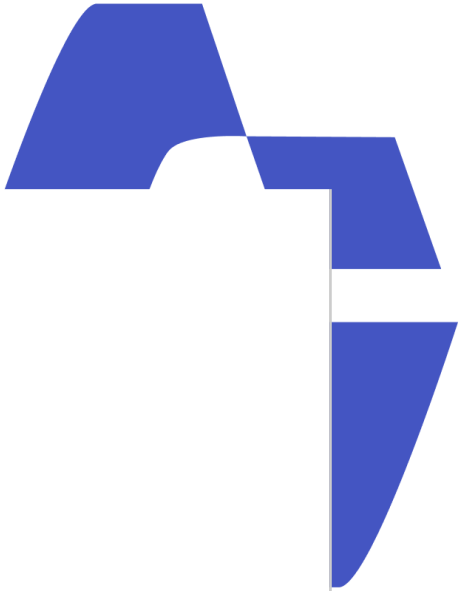
When an application is started on a node without replication, the files in the vlxtransit directory can't be seen.
If the assigned host is in the VISULOX PORTAL Array, then everything is fine (**default** replication is ok!).
If the assigned host is **not** in the VISULOX PORTAL Array, then **ftonly** or **all** has to be used.

Example: disabling session controllers on a node

The following example shows how the session controller feature on a VISULOX Access Node set to 0. This node the will not provide any session controller and so it will not be used for recording.

Displaying the layout entries

```
visulox config -name layout
    ------------------------------------------------------------------
    | changed | key                                    | value        |
    ------------------------------------------------------------------
```



```
    |         | layout.<logical server name>.banner       |           |
    |         | layout.<logical server name>.connection   |           |
    |         | layout.<logical server name>.feature.sc   | 400       |
    | changed | layout.<logical server name>.fileexchange | true      |
    |         | layout.<logical server name>.ftpd         | false     |
    |         | layout.<logical server name>.location     | STANDARD  |
    |         | layout.<logical server name>.replication  | default   |
    |         | layout.<logical server name>.runlevel     | accepting |
    |         | layout.<logical server name>.shortinfo    | STANDARD  |
    |         | layout.<logical server name>.webservice   | false     |
    |         | layout.<logical server name>.zone         | STANDARD  |
    ---------------------------------------------------------------
```

Setting session controller to 0

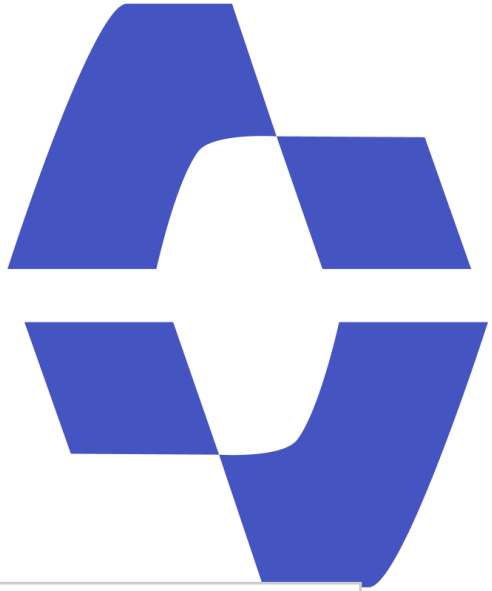
```
visulox config edit -name layout.<logical server name>.feature.sc=0

    ------------------------------------------------------------
    | parameter                                |  type | value |
    ------------------------------------------------------------
    | layout.<logical server name>.feature.sc | SETUP | 0     |
    ------------------------------------------------------------
```

Related articles

VISULOX Cluster

VISULOX Node Hierarchy

Network communication within VISULOX



23.1.49 VISULOX Node hierarchy

In some environments it makes sense to setup VISULOX Nodes in different locations and zones.

Therefore the location has to be set, once a node is created and the zone is specified, when the node is attached to the VISULOX Cluster.

The location is set with the following command:

Example: Setting location A

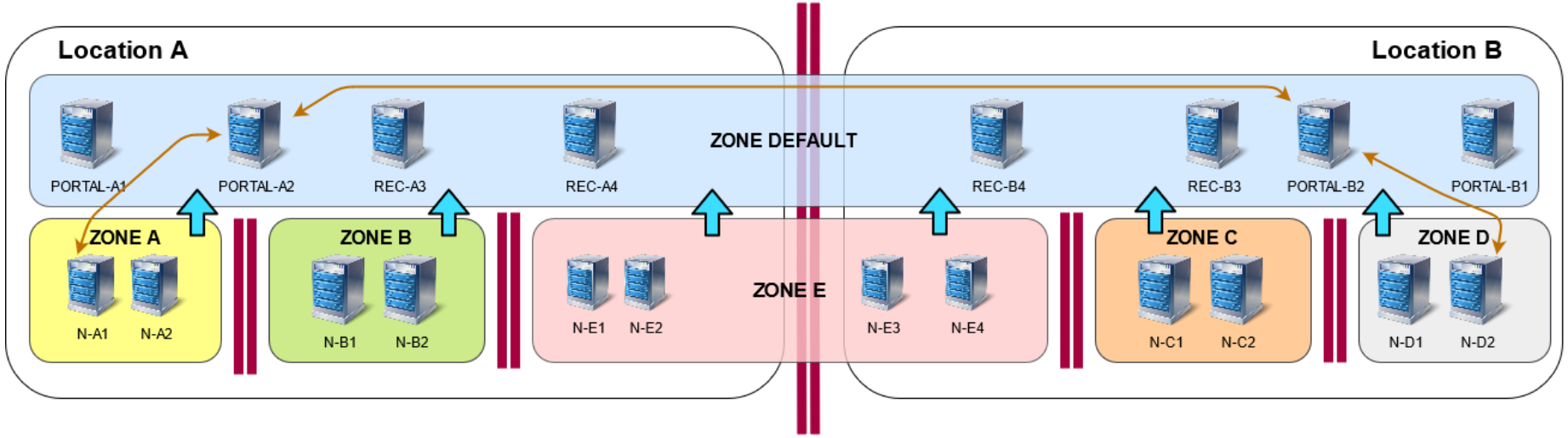
```
visulox config -name layout.<nodename>.location=A
```

When the node is attached to the VISULOX Cluster, the location and the zone must be specified:

Example: Attaching a node location A, zone B

```
visulox attach -location A -zone B
```

Example setup



Nodes within the same zone are communicating with each other and need all related ports open.
Nodes within the same location need all VISULOX related ports open subject to the layout of the node.
Therefore the firewall rules must be set accordingly (see: Network communication within VISULOX).

In an environment with different locations and zones, the nodes in different Zones communicate only via the default zone and not directly with each other.

The Zones can be setup in various network segments with firewalls between them.

Related articles

VISULOX Cluster

VISULOX layout of a node

Network communication within VISULOX

23.1.50 How to assign a fixed username

Overview

Depending on the setup, sometimes an automatic access with a fixed username is needed.

This article explains different methods to achieve this. A fixed user is **not** the Unix username or Windows username of the logged-in user.

Depending on the setup a password is needed for that fixed user.

The user credentials to the application server can be controlled with **vlxuser** / **vlxpwd** in the application definition.

If no user should be set, so that the login mask is always shown, this can also be achieved with the vlxRdpNoUser.exp expect script.

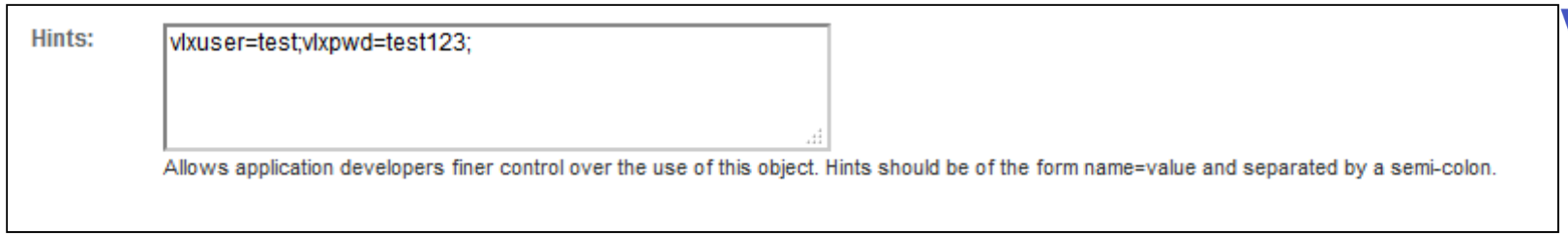
For the VISULOX Addons the **vlxSSO=1** enables using the users login credentials or override these with **vlxuser** / **vlxpwd**.

See: How to pass user credentials to an application - VISULOX Single Sign On - SSO

- Overview
- Using vlxuser / vlxpwd in standard application configuration
    - Former way of using vlxuser / vlxpwd in standard application configuration (outdated)
- VISULOX VNC with a fixed username
- Related information:

Using vlxuser / vlxpwd in standard application configuration

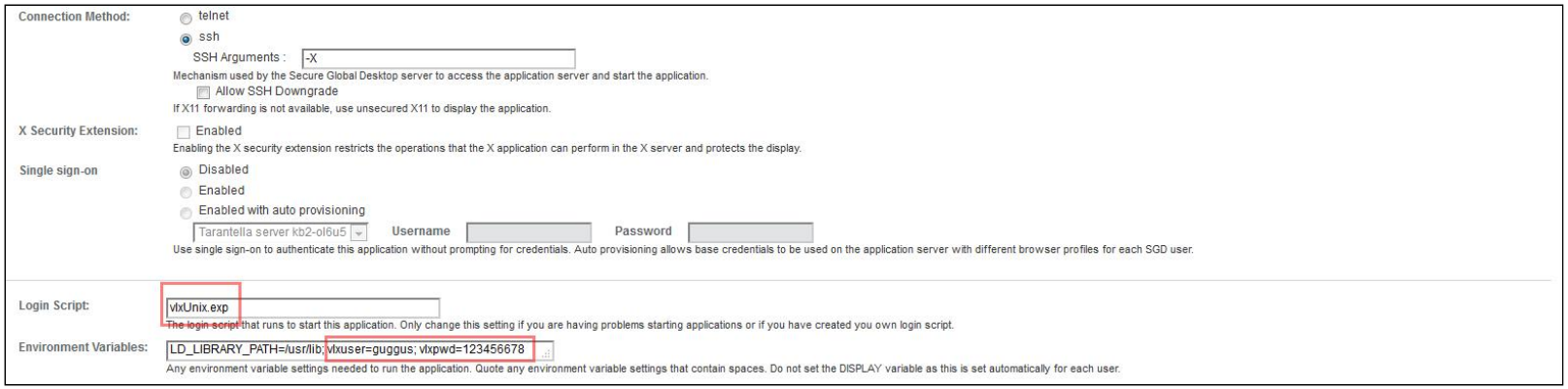
For a standard VISULOX PORTAL integration with **vlxUnix.exp** or **vlxWindows.exp** (former: vlxRdp.exp) it is possible to assign a fixed user and password for the connection in the **Hints** field on the **General** page of the application.



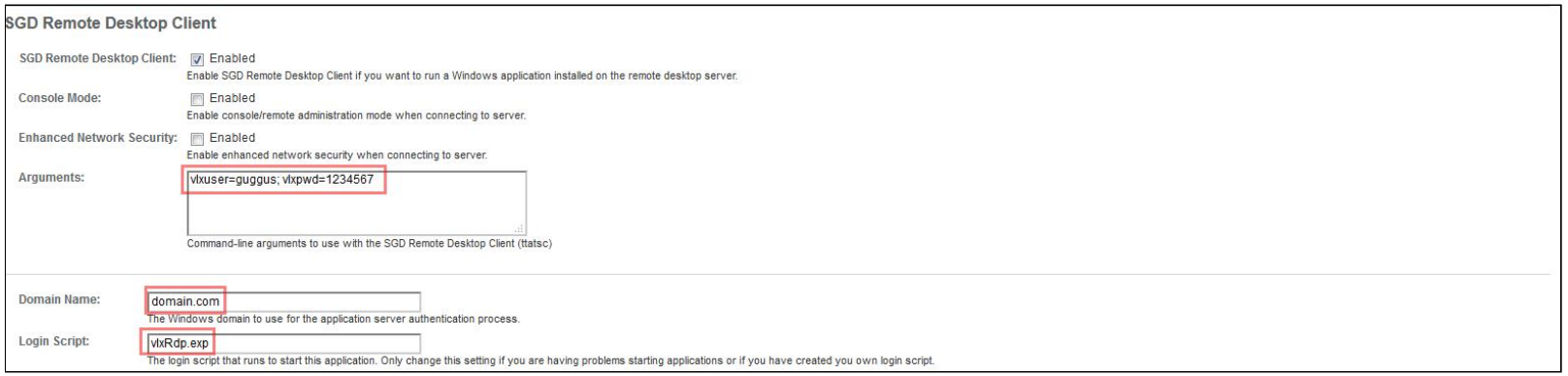
⚠ For RDP applications, the domain field has to be filled out.

Former way of using vlxuser / vlxpwd in standard application configuration (outdated)

Applications using vlxUnix.exp (SSH or Telnet applications)



Applications using vlxRdp.exp (Windows Applications)



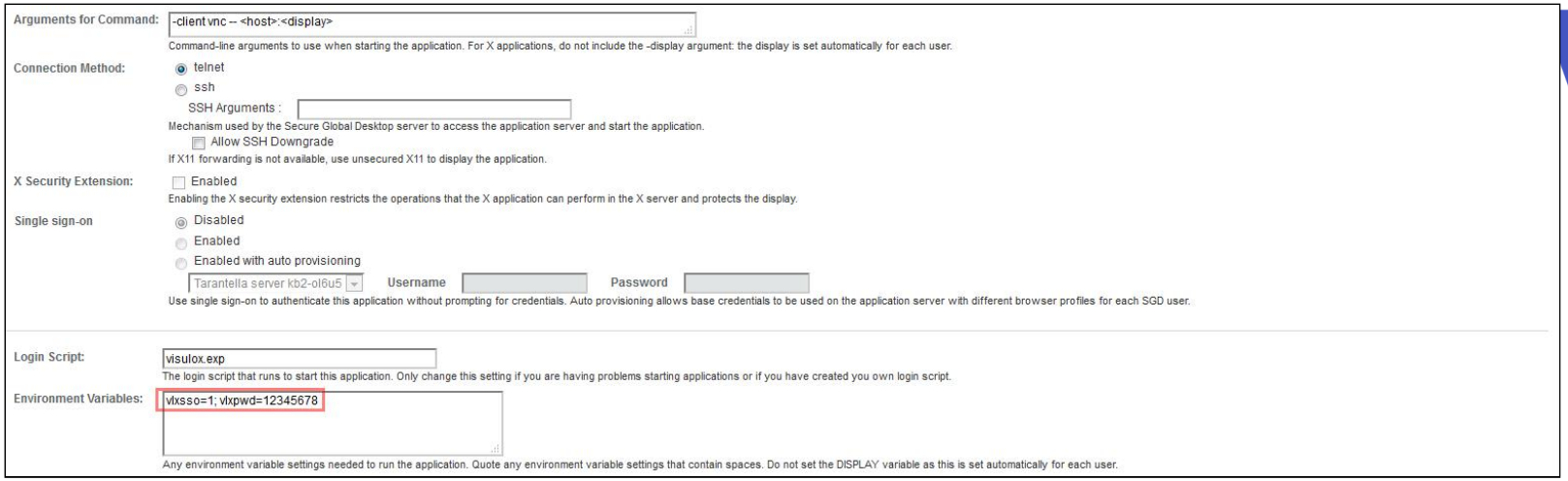
vlxRdp.exp is still usable, but **vlxWindows.exp** should be used for new configurations.

Arguments and Environment Variables must be seperated by a space. e.g. like shown in the example: vlxuser=guggus; vlxpwd=12345678

As login script **vlxWindows.exp** (new) or vlxRdp.exp (old) can be used for Windows applications.

The **Hint** field on the **General** page of the application should be used instead of the "Environment Variables" field, which is outdated.

VISULOX VNC with a fixed username



Related information:

How to pass user credentials to an application - VISULOX Single Sign On - SSO

How to use SSH-Keys within Command Connect / Guard and FT Client

Passcache

23.1.51 VISULOX Lifetimes

With the VISULOX housekeeping mechanism the lifetimes can be adapted to customer specific requirements.

Whenever an information is stored, it is tagged with a lifetime. Only films can have an individual lifetime, specified in the according Application Policy (Recording / Lifetime in days or endless). The Application Policy setting of the lifetime will overwrite the default lifetime of the recorded film.

If an information is transferred to the Archive, the lifetimes are reset to Archive specific lifetimes. The new Archive lifetimes of webtopsessions, emulatorsessions, chapters and File Transfer are set during the Archive process.

If the Archive life times are modified, it will affect only new archived data.

All lifetimes can be seen and edited with the **visulox config** command.

⚠ Lifetimes should not be set lower than 7 days!

Displaying the lifetimes:

visulox config list -name lifetime -info

```
------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------
| changed | key                              | value   |
shortinfo ... | defaultvalue |
------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------
|         | filecache.lifetime               | 3600    |                 If a file in file cache is older in secondes, it will be
removed ... |         3600 |
|         | lifetime.application             | default |                        the lifetime of session data including films and
chapters ... |      default |
|         | lifetime.archive.application     | default |                                                the session,film and chapters in
archive ... |      default |
|         | lifetime.archive.bigfiletransfer | default |                                                     the bigfiletransfer data in
archive ... |      default |
|         | lifetime.archive.commandconnect  | default |                          default lifetime for any archived commandconnect
events ... |      default |
```

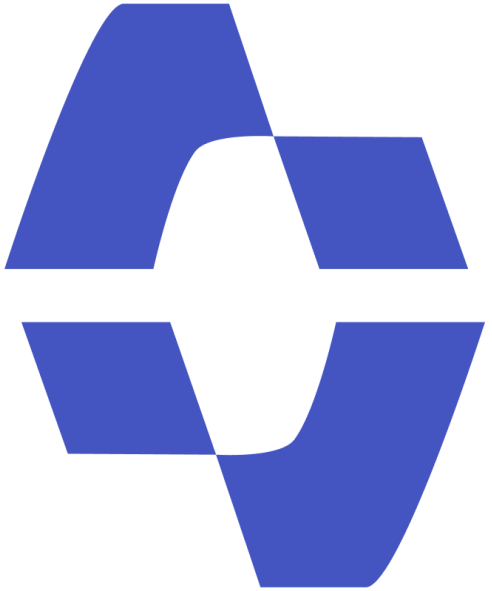
```
|         | lifetime.archive.commandguard    | default |                    default lifetime for any archived commandguard
events ... |      default |
|         | lifetime.archive.default         | 365     |                                                  Default value in
archive ... |          365 |
|         | lifetime.archive.filetransfer    | default |                                        the filetransfer data in
archive ... |      default |
|         | lifetime.archive.input           | default |                                         keyboard input lines in
archive ... |      default |
|         | lifetime.archive.login           | default |                                                       Login event
Events ... |      default |
|         | lifetime.archive.script          | default |                                                  script events in
archive ... |      default |
|         | lifetime.archive.sgdaudit        | default |                                        events from SGD AUDIT in
archive ... |      default |
|         | lifetime.archive.sgdusage        | default |                                        events from SGD Usage in
archive ... |      default |
|         | lifetime.archive.system          | default |                                                         GUI Edit
Events ... |      default |
|         | lifetime.archive.vlxshell        | default |                       default lifetime for any archived vlxshell
events ... |      default |
|         | lifetime.bigfiletransfer         | default |                                                  the
bigfiletransfer data ... |      default |
|         | lifetime.commandconnect          | default |                          default lifetime for any commandconnect
events ... |      default |
|         | lifetime.commandguard            | default |                            default lifetime for any commandguard
events ... |      default |
|         | lifetime.default                 | 90      |                                                           default
 lifetime ... |          90 |
|         | lifetime.filetransfer            | default |                                          the lifetime of
transfer files ... |      default |
|         | lifetime.input                   | default |                    the lifetome of keyboard input lines in the event
tables ... |      default |
|         | lifetime.login                   | default |                                                              Login
Events ... |      default |
```

```
|         | lifetime.scale                | 86400   | Do not change. For testing only, scaling factor for the lieftimes 3600 =
hour 86 ... |        86400 |
|         | lifetime.script               | default |                                                                    script
events ... |      default |
|         | lifetime.sgdaudit             | default |                                                                Events from
SGD AUDIT ... |      default |
|         | lifetime.sgdusage             | default |                                        Events from SGD for login and
application start ... |      default |
|         | lifetime.system               | default |                                                                GUI Edit
Events ... |      default |
|         | lifetime.vlxshell             | default |                                    default lifetime for any vlxshell
events ... |      default |
|         | lifetime.warningthreshold     | 5       |                                    warning threshold for experation
in days ... |            5 |

-------------------------------------------------------------------------------------------------------------------------------
----------------------------
```

For example:

Examples

```
Setting application lifetime
visulox config edit -name lifetime.application=10

Setting lifetime of archived applications
visulox config edit -name lifetime.archive.application=100

Setting filetransfer lifetime
visulox config edit -name lifetime.filetransfer=10
```



23.1.52 VISULOX Webservice

General behaviour

VISULOX includes a webservice interface for different kind of purposes:

- Register external events
- Register feedback from other services (SMS)
- Retrieve information

This service has fixed behaviours and will be extended on project request.

Configure webservice

Example

./visulox config edit -name webservice.sslport=8114
./visulox config edit -name webservice.certfile=portalcert.pem,webservice.keyfile=portalkey.pem

The files for SSL must exist.

./visulox config edit -name webservice.allowedip=ip1:ip2

Do not forget to **restart** VISULOX after this adjustment!

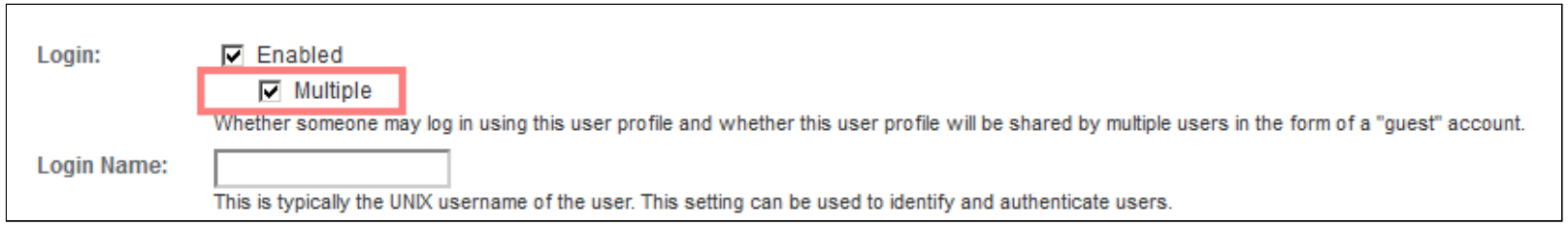
Configure layout

```
visulox config -name layout.%NODE%.webservice=true
```

23.1.53 How to configure a user account as a group account

In the VISULOX PORTAL Service a user is an ambiguous object. If the user logs in, he has an unique session. If he logs in again from another client, his session will be transferred. This is the standard VISULOX PORTAL Service behaviour.

If there is a necessity to allow the usage of an account by more than one person, the according setting in the VISULOX PORTAL Service profile has to be marked.



.

If VISULOX PORTAL Service is connected to an LDAP server, the user who logs in will have the `"o=Tarantella System Objects/cn=LDAP Profile"` profile.

To make it possible for LDAP users to be group users, a LDAP mirroring profile has to be configured.

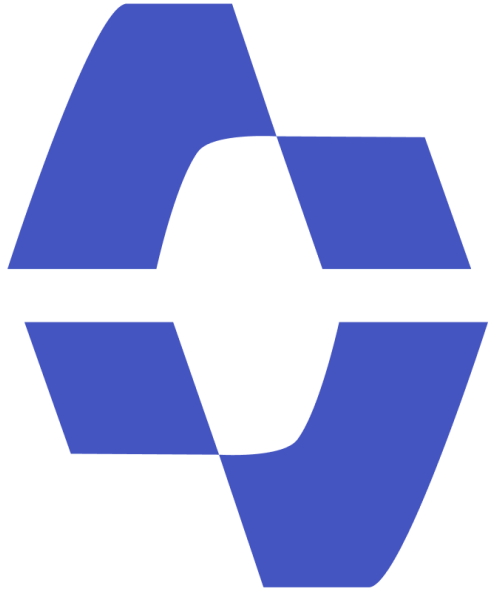
Important is to consider How to exclude single datastore users from import.

Group accounts can be used within the policies including MFA Login Policy.

Related articles:

(4.2.0) VISULOX-GATEWAY Command

(4.2.0) How to setup MFA with SMS response from the SMS Provider



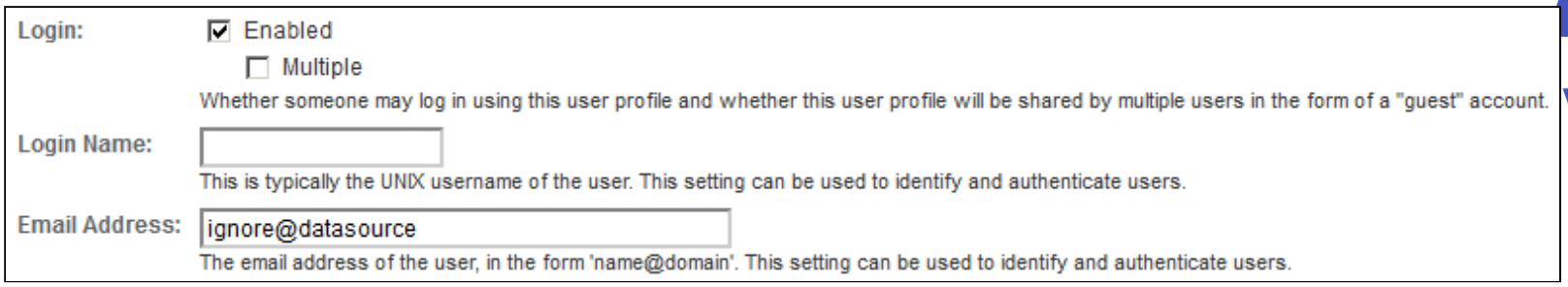
(4.2.0) How to exclude single datastore users from import
(4.2.0) VISULOX PORTAL Console
(4.2.0) How to configure a user account as a group account
(4.2.0) How to work with VISULOX Datasources
(4.2.0) VISULOX PORTAL Server Array
(4.2.0) RSA SecureID Implementation via RSA API
(4.2.0) VISULOX-PORTAL OBJECT Command
(4.2.0) VISULOX Webservice
(4.2.0) How to use an LDAP/AD or Unix account to access the webservice
(4.2.0) Migrating to One Time Password Authentication
(4.2.0) The VISULOX PIN Service
(4.2.0) VISULOX-PORTAL Command
(4.2.0) Attaching VISULOX Service to VISULOX PORTAL Service

23.1.54 How to exclude single datastore users from import

Every user in the VISULOX PORTAL Datastore is imported into the VISULOX Datasource.

If one of these users is a LDAP Mirroring profile, this will end in having two entries, one from datastore and one from the LDAP server.

To eliminate this ambiguous situation, the datastore profile has to be marked to be ignored. This is done by inserting `"ignore@datasource"` in the email field.



This is automatically done, when users are imported as administrators or integrated as a VISULOX webservice user.

This will be needed, if LDAP accounts are used as group accounts.

Related articles:

(4.2.0) VISULOX-GATEWAY Command

(4.2.0) How to exclude single datastore users from import

(4.2.0) VISULOX PORTAL Console

(4.2.0) How to configure a user account as a group account

(4.2.0) How to work with VISULOX Datasources

(4.2.0) VISULOX PORTAL Server Array

(4.2.0) VISULOX-PORTAL OBJECT Command

(4.2.0) How to use an LDAP/AD or Unix account to access the webservice

(4.2.0) VISULOX-PORTAL Command

(4.2.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.2.0) How to import users as VISULOX PORTAL administrators
(4.3.2) How to import users as VISULOX PORTAL administrators
(4.3.2) How to exclude single datastore users from import
(4.3.2) How to configure a user account as a group account
(4.3.2) How to work with VISULOX Datasources

23.1.55 VISULOX database backup, restore and performance

Backup and restore

The database backup is always encrypted. The key is the VISULOX cluster key.

This means, that a new environment, where the backup should be restored needs the same cluster key.

Available commands of database.tcl:

Command	Description
backup	Backup database to file (possible during operation)
compare	Compare table between nodes
fields	Display name of columns in table
integrity	Clean database

Command	Description
list	Stats about the database
query	Direct database query
restore	Restore file to database (VISULOX service has to be stopped)
-name <*value*>	A mask for the matching tables <*****>
-info	Shows column names in tables
-node <*value*>	Node to connect database<>
-timeout <*value*>	Timeout <10>

For example:

Backup

```
visulox database backup
```

The file will be extended with the time stamp and copied to the **/tmp** directory.

Restore

```
visulox database restore -path <path to file>
```

It is possible to do the backup on node1 and restore the database on node2. All host related references will be converted to the new host. After restore the configuration is reloaded automatically (loadconfig).

If **-force** has to be used to backup and restore a database, the VISULOX Support should be involved.

Restore will overwrite the existing database.

Running (recorded) sessions will not be available in the VISULOX Cockpit after the database has been restored.

For restoring the database, VISULOX must be offline.

Database performance

The database status of a node or all nodes can be checked with:

```
visulox database integrity (only status)
visulox database integrity -repair (with confirmation)
visulox database integrity -repair -force (without confirmation)
```

23.1.56 Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x

Since VISULOX 3.3 environments Oracle Secure Gobal Desktop and its components are embedded.

A VISULOX installation now consists of three major components: VISULOX, VISULOX PORTAL and VISULOX GATEWAY.

VISULOX PORTAL cannot be installed upon existing Oracle Secure Global Desktop environments.

This article shows the steps to migrate the SGD 5.40 (or later) datastore, password cache and user preferences and the VISULOX 3.x Database and Keys.

⚠ In case of a redundant environment with more servers, that are updated in several steps, make sure not to have servers running in the cluster with different VISULOX versions at the same time,

- Starting point
- Gateway on separate node
  - Gateway certificates
  - Remove the OSGD Gateway
  - Install VISULOX Gateway
  - Import Gateway certificates
- VISULOX PORTAL with and without Gateway
  - Install and run OSGD Backup and Restore Tool
  - Remove current OSGD fully (if new environment will be installed here)
- VISULOX 3.x
  - Copy VISULOX Database and Key
  - Remove VISULOX 3.x (if new environment will be installed here)
- Install VISULOX Components on VISULOX Access Node
  - Restore previous SGD configuration to VISULOX PORTAL
  - Restore previous VISULOX 3.x configuration
- Starting / Attaching VISULOX PORTAL and VISULOX
  - Starting the VISULOX Components
  - Attaching VISULOX Service to VISULOX PORTAL
  - Attaching VISULOX Cluster
- Finishing work
  - Check status
  - VISULOX PORTAL Console
  - VISULOX Cockpit
  - Check configuration parameters
- Related articles

Starting point

SGD 5.40 (or later) can be installed with several SGD Array members and SGD Gateways in front.

VISULOX 3.x is installed on the OSGD Nodes (such a node is called VISULOX Access Node). On pure VLX Nodes, follow the steps for VLX only.

Gateway on separate node

Gateway certificates

Make sure the Gateway certificates and keys are available, otherwise export the certificates from the existing Gateway installation. (See: How to export Gateway frontend certificate including key)

Remove the OSGD Gateway

```
yum erase oracle-sgd-gateway
```

Check and delete **/opt/SUNWsgdg/** if it still exists after removing the Gateway.

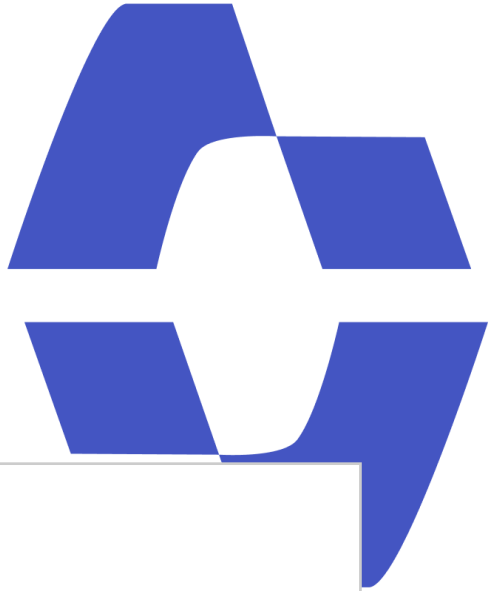
Install VISULOX Gateway

```
yum install <visulox-gateway-4.x-<version>
```

Import Gateway certificates

With existing certiificates

```
visulox-gateway sslkey import --keyfile <filename> --certfile <filename> [--cacertfile <filename>]
```



VISULOX PORTAL with and without Gateway

In this case the VISULOX PORTAL Node has a previous version of Oracle Secure Global Desktop: 5.40 (or later).

A backup of the configuration also has to be made with the Oracle Secure Global Desktop Backup and Restore Tool.

Install and run OSGD Backup and Restore Tool

```
yum install oracle-sgd-backup-5.60.550-1.noarch.rpm

/opt/sgd-backup/bin/backup.sh (note the needed temporary password)
```

⚠ Always the latest version of the OSGD Backup and Restore Tool should be used.

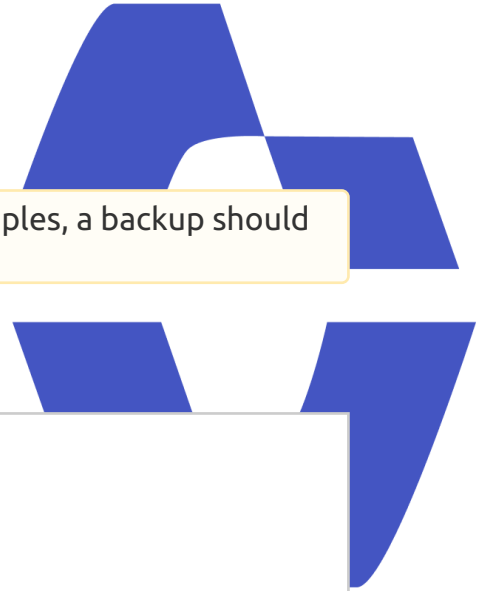
⚠ If **use visulox-portal <command>** is displayed, the following steps are necessary:

```
cat /sbin/visulox-portal
#!/bin/sh
#########################################################################
# Copyright (c) amitego engineering GmbH, www.amitego.com
#########################################################################
export VLX_EMBEDDED=true
export LD_LIBRARY_PATH=/opt/tarantella/lib
exec /opt/tarantella/bin/tarantella "$@"
```

In this case insert the line **export VLX_EMBEDDED=true** into **/opt/sgd-backup/bin/backup-utils.sh**.

This backup includes the Gateway configuration, if a local Gateway is installed on this server.

⛔ Remember the password or run tool without encryption!



⚠ If there are customized files, e.g. **expect scripts** or customized **OSGD applications** under VISULOX Examples, a backup should be made as well.

Remove current OSGD fully (if new environment will be installed here)

Erase all OSGD related packages like **oracle-sgd-server**, **oracle-sgd-gateway**, **oracle-sgd-webclient**:

```
yum list installed | grep oracle-sgd | cut -f 1 -d " "

yum erase oracle-sgd-server
yum erase oracle-sgd-webclient
yum erase ...
```

Check and delete remaining folders in **/opt** after yum erase.

VISULOX 3.x

Copy VISULOX Database and Key

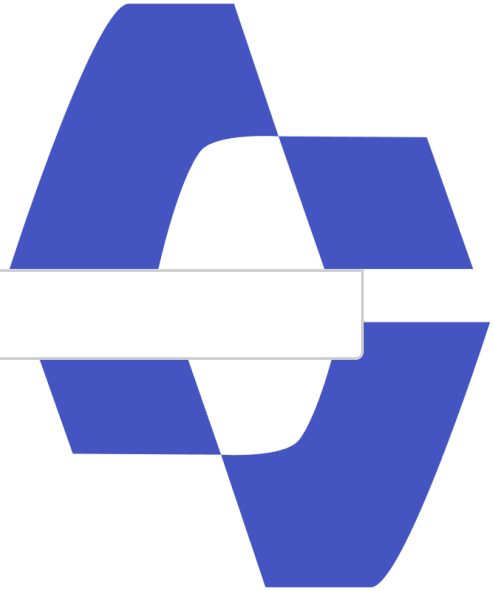
Copy the VISULOX Database and the VISULOX Key to a temporary folder:

```
mkdir /tmp/update
./visulox database clean
cp /opt/visulox/data/database/* /tmp/update/
cp /opt/visulox/etc/key /tmp/update/
cp /opt/visulox/etc/key.node /tmp/update/
```

Check for other customized files, that should be saved before VISULOX will be uninstalled, eg **event.sh**, customized **reports**, **filecheck.sh**, etc

Configurations in **pam.d** must be saved as well and manually added in the new environmenmt after installation.

It is also necessary to make a copy of the files in the VISULOX Filestore. Have a look at the VISULOX Administration Guide: VISULOX Filestore



Remove VISULOX 3.x (if new environment will be installed here)

```
/opt/visulox/setup/uninstall.sh -a
```

Check and delete remaining folders in **/opt** after uninstall.

Check and delete SGD users (ttasys, ttaserv) and group (ttasys), if they are not removed during uninstall.

Install VISULOX Components on VISULOX Access Node

Install the VISULOX Components, also have a look at the Installation Guide for VISULOX 4.x:

```
yum install visulox-rte-1.2-<version>.rpm
yum install visulox-4.x-<version>.rpm
yum install visulox-portal-4.x-<version>.rpm
```

On pure VISULOX Nodes the visulox-portal package is **not** needed.

On VISULOX PORTAL with local Gateways, the visulox-gateway package has to be installed as well.

Restore previous SGD configuration to VISULOX PORTAL

The sgd-restore tool has to take care about the VISULOX PORTAL version. Therefore "**VLX_EMBEDDED=true**" is added in front of the command or in the shell.

Announce VISULOX PORTAL to the restore tool.

```
export VLXEMBEDDED=true
```

Run the restore command:

VISULOX PORTAL with VISULOX Gateway

```
/opt/sgd-backup/bin/restore.sh --serverfile /opt/sgd-backup/data/sgd-backup-encrypted-<date>.tar.gz --gatewayfile /opt/sgd-backup/
data/sgdg-backup-encrypted-<date>.tar.gz
```

VISULOX Portal only

```
/opt/sgd-backup/bin/restore.sh --serverfile /opt/sgd-backup/data/sgd-backup-encrypted-<date>.tar.gz
```

On separate Gateway

```
visulox-gateway server add-array --name sgd --serverurl https://<sgd-hostname.domain>
```

⚠ In case of a new installtion of the Gateways with imported certificates, the old entries of the Gateways have to be removed on the VISULOX Portal Servers before the add-array command.

Restore previous VISULOX 3.x configuration

Restore VLX database:

```
chown vlx: /tmp/update/

Dry run / check:
/opt/visulox/setup/update/migrate.tcl all -source /tmp/update/

Migrate / run:
/opt/visulox/setup/update/migrate.tcl all -source /tmp/update/ -run
```

Check/ adjust previous saved customized files, eg **event.sh**, customized **reports**, **filecheck.sh**, **pam.d** etc

Copy the previous saved files from Filestore back into the related Filestore directory.

Starting / Attaching VISULOX PORTAL and VISULOX

Starting the VISULOX Components

```
visulox-gateway start
visulox-portal start
visulox start
```

Attaching VISULOX Service to VISULOX PORTAL

```
visulox portal attach
```

Attaching VISULOX Cluster

```
visulox attach <FQDN vlx node 2>
...
visulox attach <FQDN vlx node n>
```

If nodes are in different locations and/or zones, have a look at VISULOX Node hierarchy.
Depending on the VISULOX Setup, it can be necessary to adjust the layout of the VISULOX Nodes in the cluster and to start needed VISULOX Services, e.g. FTP, File Exchange, etc.

When finished a **COMPLETE RESTART** of **all** services on **all** nodes is recommended.

Finishing work

Check status

```
visulox-gateway status
visulox-portal status
visulox status

visulox integrity
```

VISULOX PORTAL Console

- Adjust the Workspace application icons
- Remove TransitWeb application from Workspace (Transfer from/to the client is now done in the File Transit Area in Workspace)

VISULOX Cockpit

- Assign a category to action scripts manually, where the category is missing and assign these scripts again to the according policies
- Check configured VISULOX Policies, Command Connetcs, Hosts, etc

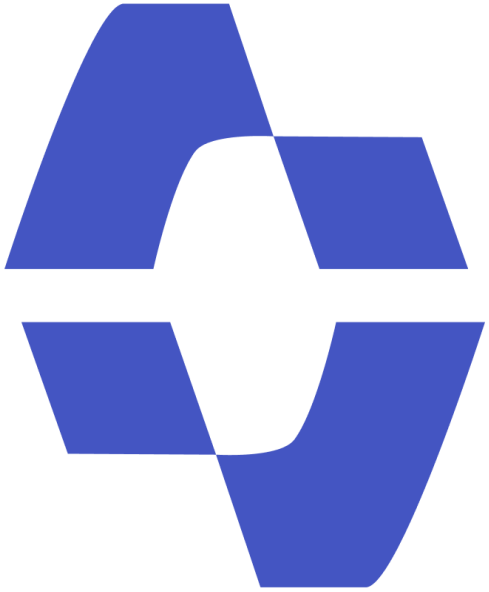
Check configuration parameters

Check the changend configuration parameters, special sizes are now stored in a different format and have to be set again, even if the presentation is the same.
Use **visulox config edit** for all parameters with size, that have been changed (visulox config list -changed), e.g. transit.maxuploadsize, transit.quota, etc

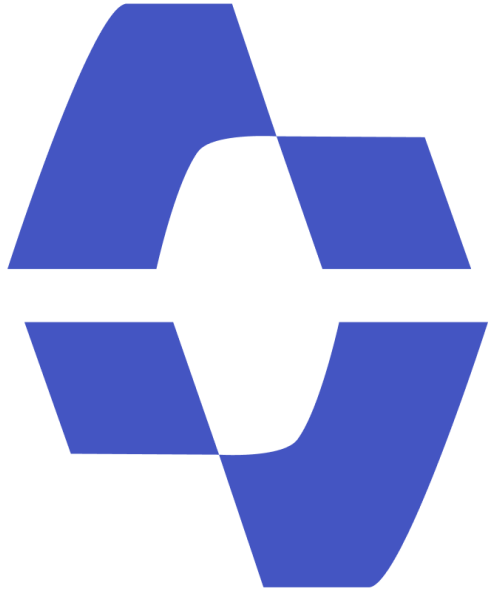
Related articles

(4.2.0) How to route a VISULOX application to other nodes

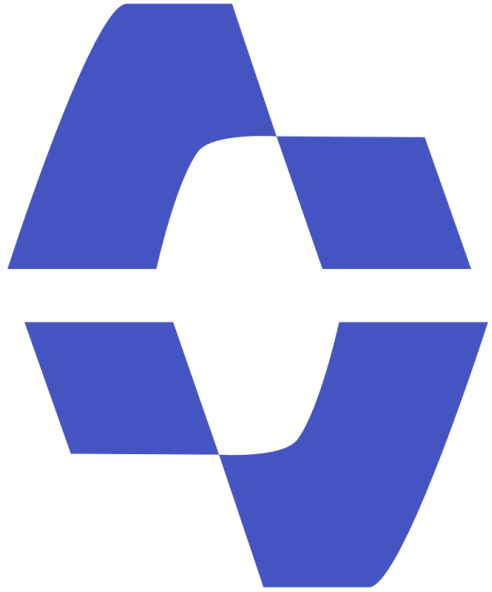
(4.2.0) Modify VISULOX PORTAL Datastore via CLI



(4.2.0) Gateway Session Balancing
(4.2.0) VISULOX Filestore
(4.2.0) VISULOX layout of a node
(4.2.0) How to export Gateway frontend certificate including key
(4.2.0) VISULOX PORTAL Server Array
(4.2.0) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.2.0) Adding a VISULOX Revision Server
(4.2.0) Setup architecture
(4.2.0) VISULOX Cluster
(4.2.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.2.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.2.0) Migrating from VISULOX 3.x to 4.x
(4.2.0) VISULOX Node hierarchy
(4.2.0) VISULOX Architecture
(4.2.0) Security information about vlxsu and vlxchown (SUID bit)
(4.3.2) VISULOX Architecture
(4.3.2) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.2) Setup architecture
(4.3.2) VISULOX Portal maintenance mode
(4.3.2) Modify VISULOX PORTAL Datastore via CLI
(4.3.2) VISULOX Cluster
(4.3.2) Migrating from VISULOX 3.x to 4.x



(4.3.2) VISULOX layout of a node
(4.3.2) VISULOX Node hierarchy
(4.3.2) How to route a VISULOX application to other nodes
(4.3.2) Adding a VISULOX Revision Server
(4.3.2) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.2) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.2) How to export Gateway frontend certificate including key
(4.3.2) Security information about vlxsu and vlxchown (SUID bit)
(4.3.2) VISULOX PORTAL Server Array
(4.3.2) VISULOX Filestore
(4.1.1) VISULOX Node hierarchy
(4.1.1) VISULOX Cluster
(4.1.1) Migrating from VISULOX 3.x to 4.x
(4.1.1) VISULOX layout of a node
(4.1.1) Attaching VISULOX Service to VISULOX PORTAL Service
(4.1.1) Modify VISULOX PORTAL Datastore via CLI
(4.1.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.1.1) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.1.1) How to route a VISULOX application to other nodes
(4.1.1) Setup architecture
(4.1.1) How to export Gateway frontend certificate including key
(4.1.1) Gateway Session Balancing



(4.1.1) VISULOX Filestore

(4.1.1) Adding a VISULOX Revision Server

(4.1.1) Security information about vlxsu and vlxchown (SUID bit)

(4.1.1) VISULOX PORTAL Server Array

(4.1.1) VISULOX Architecture

(4.3.1) Setup architecture

(4.3.1) How to export Gateway frontend certificate including key

(4.3.1) Modify VISULOX PORTAL Datastore via CLI

(4.3.1) VISULOX Portal maintenance mode

(4.3.1) VISULOX layout of a node

(4.3.1) Migrating from VISULOX 3.x to 4.x

(4.3.1) How to route a VISULOX application to other nodes

(4.3.1) Adding a VISULOX Revision Server

(4.3.1) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x

(4.3.1) VISULOX Node hierarchy

(4.3.1) Attaching VISULOX Service to VISULOX PORTAL Service

(4.3.1) VISULOX Architecture

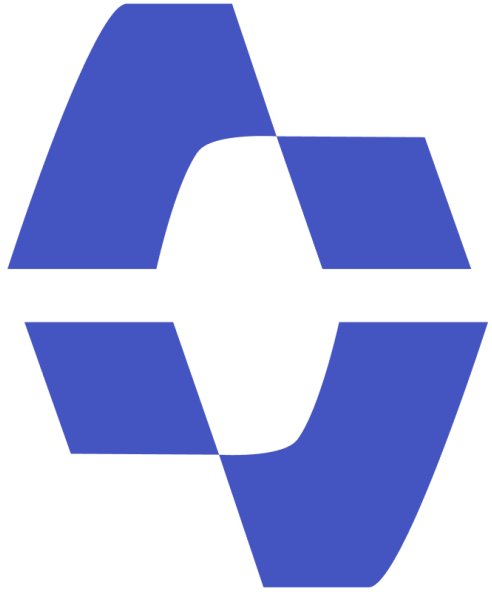
(4.3.1) Security information about vlxsu and vlxchown (SUID bit)

(4.3.1) VISULOX PORTAL Server Array

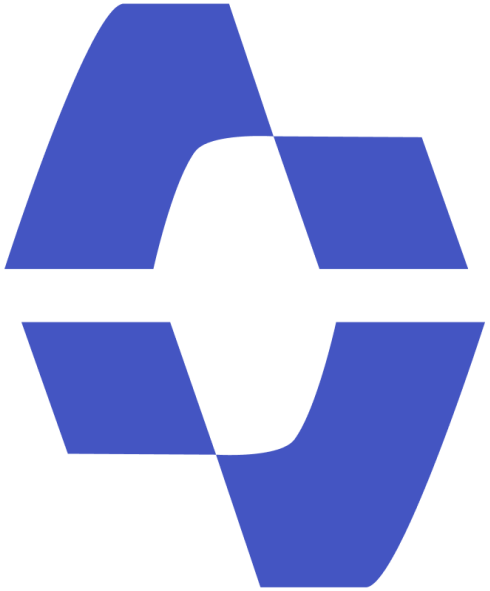
(4.3.1) VISULOX Cluster

(4.3.1) VISULOX Filestore

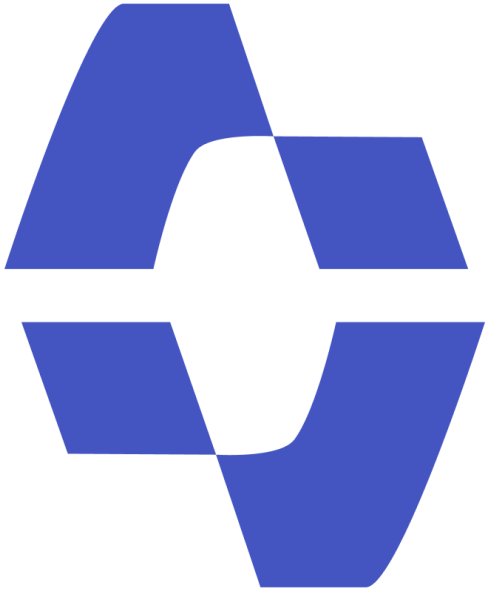
(4.3.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration



(4.3.0) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.0) Migrating from VISULOX 3.x to 4.x
(4.3.0) VISULOX Cluster
(4.3.0) VISULOX Node hierarchy
(4.3.0) VISULOX Filestore
(4.3.0) Security information about vlxsu and vlxchown (SUID bit)
(4.3.0) VISULOX PORTAL Server Array
(4.3.0) How to export Gateway frontend certificate including key
(4.3.0) Modify VISULOX PORTAL Datastore via CLI
(4.3.0) VISULOX layout of a node
(4.3.0) How to route a VISULOX application to other nodes
(4.3.0) VISULOX Architecture
(4.3.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.0) Setup architecture
(4.3.0) VISULOX Portal maintenance mode
(4.3.0) Attaching VISULOX Service to VISULOX PORTAL Service
(4.3.0) Adding a VISULOX Revision Server
Setup architecture
How to export Gateway frontend certificate including key
VISULOX PORTAL Server Array
Modify VISULOX PORTAL Datastore via CLI
VISULOX Portal maintenance mode



How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
Migrating from VISULOX 3.x to 4.x
Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
VISULOX Node hierarchy
VISULOX layout of a node
VISULOX Cluster
How to route a VISULOX application to other nodes
Adding a VISULOX Revision Server
VISULOX Filestore
Security information about vlxsu and vlxchown (SUID bit)
Attaching VISULOX Service to VISULOX PORTAL Service
VISULOX Architecture
VISULOX layout of a node
Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
VISULOX Node hierarchy
Modify VISULOX PORTAL Datastore via CLI
VISULOX Cluster
VISULOX Filestore
Migrating from VISULOX 3.x to 4.x
How to export Gateway frontend certificate including key
How to route a VISULOX application to other nodes
Attaching VISULOX Service to VISULOX PORTAL Service



(4.3.3) Setup architecture
VISULOX Architecture
Adding a VISULOX Revision Server
How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
VISULOX PORTAL Server Array
Security information about vlxsu and vlxchown (SUID bit)
VISULOX Portal maintenance mode

23.1.57 Migrating from VISULOX 3.x to 4.x

The following steps can be used to migrate from VISULOX 3.x to VISULOX 4.x .

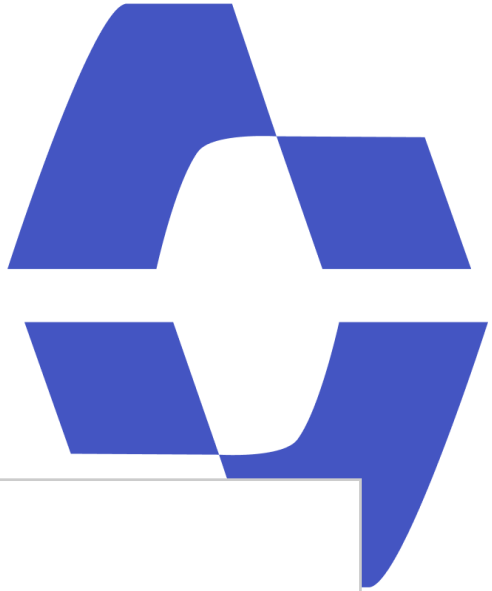
> ⚠ In case of a redundant environment with more servers, that are updated in several steps, make sure not to have servers running in the cluster with different VISULOX versions at the same time,

- Preparation: Exporting data on the old servers
- Installation on new servers / running servers in parallel
- Update same VISULOX Node
- Finishing work
    - Check for errors / warnings

Preparation: Exporting data on the old servers

- Export the database (use database clean command before), the cluster key and scripts in the tools directory.
  Copy these files to another directory outside of VISULOX (/tmp/update is possibly too small). It is a good idea to use one folder for each server for the backup files.

```
mkdir /tmp/update
cp /opt/visulox/data/database/database.db /tmp/update
cp /opt/visulox/etc/key /tmp/update
cp /opt/visulox/etc/key.node /tmp/update
```



- Backup or providing the files in the VISULOX Filestore
- Backup customized files, e.g. event.sh, filecheck.sh, customized reports, pam.d, etc

Installation on new servers / running servers in parallel

- Install new nodes with VISULOX 4.x and complete the setup (build cluster / standalone database and configuration)
- Migration can be done online (makes sense for the audit data)
- Copy the backup files to the node:

```
chown -R vlx: /tmp/update/

Dry run / check:
/opt/visulox/setup/update/migrate.tcl all -source /tmp/update/ -nodemap <old logical nodename>=<new logical nodename>

Migrate / run:
/opt/visulox/setup/update/migrate.tcl all -source /tmp/update/ -nodemap <old logical nodename>=<new logical nodename> -run
```

- Getting the files and copy them to the new filestore with rsync (be aware of enough diskspace)
- Migration detects if the database belongs to an Archive Server
- Check / adjust previous saved customized files (event.sh, filecheck.sh, pam.d, etc)

migrate.tcl

- The script executes a 1on1 migration of the complete audit data from all nodes
- With the parameter **-nodemap** a mapping of the nodea name from OLD=NEW can be done
  The switch allows to use either a mapstring or a file, that contains lines with a mapstring
  OLD and NEW must be a logical nodename

Update same VISULOX Node

- umount store and remove VISULOX 3.x
- Install VISULOX 4.x and complete the setup (build cluster / standalone database and configuration)
- Getting the backup to the node:

```
chown vlx: /tmp/update/
/opt/visulox/setup/update/migrate.tcl all -source /tmp/update/
/opt/visulox/setup/update/migrate.tcl all -source /tmp/update/ -run
```

migrate.tcl
The script executes a 1on1 migration of the complete audit data from all nodes
With the parameter **-nodemap** a mapping of the nodea name from OLD=NEW can be done
The switch allows to use either a mapstring or a file, that contains lines with a mapstring
OLD and NEW can be a hostname or a nodename
For example **-nodemap vAAAA=vNEW1,vBBBB=vNEW2,server1.dom=server-new1.dom**

- Getting the files and copy them to the new filestore with rsync (be aware of enough diskspace)
- Attach slot in store
- Check / adjust previous saved customized files (event.sh, filecheck.sh, etc)

Finishing work

Check for errors / warnings

```
visulox-gateway status
visulox-portal status
visulox status

visulox integrity
```

VISULOX PORTAL Console

- Adjust the Workspace application icons
- Remove TransitWeb application from Workspace (Transfer from/to the client is now done in the File Transit Area in Workspace)

- Assign a category to action scripts manually, where the category is missing and assign these scripts again to the according policies
- Check configured VISULOX Policies, Command Connetcs, Hosts, etc

23.1.58 Restrict default VISULOX Cockpit

Overview

The default VISULOX Cockpit without a role has no resitriction.
To build a restricted view, a role for the VISULOX Cockpit must be defined.

- Overview
- View restrictions of a Cockpit without a role
- Keyboard input line restriction without a role
- Restriction within a role

A role can have a filter for users / usergroups, applications and information for the input lines.

In a process driven environment it is expected, that the Cockpit can only be used in a Dual Control cooperation or by a special group.

Because the VISULOX PORTAL admin can assign a Cockpit without a role, it is not fulfilled, that this view is restricted.

Another fact is, that the eventstream may contain, based on policies, the keyboard input lines a user entered in the application. Per default, these events are hidden and can be presented in the Cockpit by setting the option **-ksr**. If the companies process policy requests, that the keyboard input lines should only be seen by a special group of persons, the VISULOX PORTAL admin has to define a Cockpit with **-ksr** and assign the group. This implies, that he can assign this application to himself.

This article describes, how to setup a default Cockpit with view restrictions.

View restrictions of a Cockpit without a role

On the command line, two casesensitive glob filters can be defined:

```
vlxgui.default.view_filter_application
vlxgui.default.view_filter_user_group
```

To restrict the Cockpit in its default behaviour, set:

```
visulox config edit -name vlxgui.default.view_filter_user_group=<user/group glob>
visulox config edit -name vlxgui.default.view_filter_application=<application glob>
```

Example:

This defines a Cockpit without a role, presenting only logged in users. No infomation about the applications they are running.

```
visulox config edit -name vlxgui.default.view_filter_application="WORKSPACE"
```

Keyboard input line restriction without a role

This defines a Cockpit without a role, presenting only logged in users. No information about the applications they are running.

```
visulox config edit -name vlxgui.ksrgroup=<user/group glob>
```

If the user belongs to *<user/group glob>*, he will see the keyboard inputlines.

Restriction within a role

For restrictions within a role and a configuration example have a look at: How to configure role profiles for thr VISULOX Cockpit

23.1.59 VISULOX Mail Client and Send PIN

Overview

The VISULOX utilities include a small mail client to transport mails: **mailclient.tcl**.

Another useful script for sending SMS and mails in VISULOX utilities is **sendPIN.tcl**.

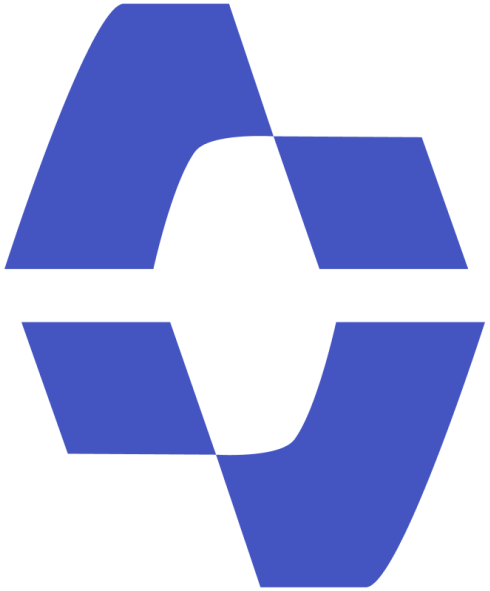
- Overview
- mailclient.tcl
  - Configuration parameters
  - Configuration in database
  - How to test the functionality of the VISULOX Mail Client
- sendPIN.tcl
  - Configuration parameters
- Related articles

mailclient.tcl

```
/opt/visulox/lib/utils/mailclient.tcl
```

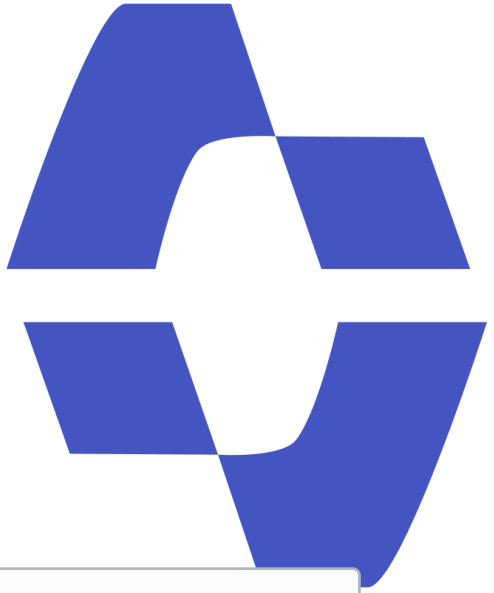
Configuration parameters

Command	Description
-from <*value*>	Sender (originator) email, default: <**visulox**>
-to <*value*>	Comma or space separated list of recipients email, default: <**root**>



Command	Description
-mg <*value*>	The mailinggroup and an individual email list can be provided: VLXMAILINGGROUP_UUID, VLXMAILINGGROUP_EMAILS
-server <*value*>	SMTP server, default: <**localhost**>
-port <*value*>	SMTP server port, default: <**25**>
-secure <*value*>	SMTP Securing mode: none, startTLS, TLS/SSL <**none**>
-subject <*value*>	Subject, default: <**Visulox Mail Client**>
-html <*value*>	-html <path to HTML file> -html <templatename> in /etc/html/template/
-file <*value*>	Text file <**stdin**>
-user <*value*>	SMTP user (overwritten by resource) <>
-password <*value*>	SMTP password (overwritten by resource) <>
-bodymime <*value*>	Mime type of mail body, default: <**text/plain**>
-attachements <*value*>	Attachments <>

Command	Description
-timeout <*value*>	Timeout in seconds, default: <**10**>
-test	Full test of the configuration
-helo	Small Helo test to mail server



After reading of **stdin**, **-file** or **-html** all variables like **%VLX<xxx>%** are substituted.
All style sheets in **/opt/visulox/etc/css/** are read and they are ready for substitution:
%VLXINCLUDE:visulox.css% is **/etc/css/visulox.css**

Configuration in database

visulox config list -name mail -force

```
-------------------------------------------------------------------------------
| parameter           |  type | value                                         |
-------------------------------------------------------------------------------
| mail.port           | SETUP | 25                                            |
| mail.recipient      | SETUP | root                                          |
| mail.resource       | SETUP |                                               |
| mail.secure         | SETUP | none                                          |
| mail.sender         | SETUP | visulox                                       |
| mail.server         | SETUP | localhost                                     |
| regexp.email        | FIXED | ^[A-Za-z0-9._-]+@[A-Za-z0-9.-]+\.[A-Za-z0-9-]{2,4}$    |
| regexp.report.email | FIXED | ^$|^[A-Za-z0-9._-]+@[A-Za-z0-9.-]+\.[A-Za-z0-9-]{2,4}$ |
```

```
-------------------------------------------------------------------------------
```

The mail client can be under control of the VISULOX configuration. So it is not needed to set the mail server in each script for example.

```
visulox config edit -name mail.server=relay.domain.com
```

How to test the functionality of the VISULOX Mail Client

In the **mail.sender** field the SMTP-server is configured. The desired setup has to be entered if localhost should not be used.

Modifications to the setup are done e.g.

```
visulox config edit -name mail.server=relay.domain.dom
visulox config edit -name mail.sender=noreply@domain.dom
```

Testing the functionality

```
/opt/visulox/lib/utils/mailclient.tcl -to user@domain.dom -file <testfile> -subject test
```

If the mail is received, the setup is good. If no mail is delivered most likely the SMTP-server needs some configuration (check log files).

Make sure the VISULOX user has a valid eMail address configured.

Requirement for the functionality is a local or an external SMTP server.

sendPIN.tcl

```
/opt/visulox/lib/utils/sendPIN.tcl
```

The Multi Factor Authentication has to provide a PIN to the user. The PIN is sent via a PIN Script.

In some cases, the user has both, an eMail address and a text message number in the datasource and the PIN has to be be sent via one of the channels.

Here the script sendPIN.tcl is helpful. sendPIN.tcl sends the eMail and/or textmessage via SMTP.

VISULOX provides the text message number, the mail address, the PIN text in the configured PIN script. sendPIN.tcl takes care on sending.

sendPIN.tcl sends the text via eMail and/or SMS. Minimum is SMS **or** eMail, maximum is both.

Configuration parameters

Commandline value	**Alternate value**	**Description**
-domain <*value*>		The text message will be sent via SMTP to <*textmessagenumber*>@domain. This parameter configures the SMS domain.
-smsvia <*value*>		SMTP server to send <*textmessagenumbe*r>@domain. This is needed, if the SMS should not use the eMail server. If not set, the configured SMTP server is used
-emailvia <*value*>		SMTP server to send the PIN text via eMail. If not set, the configured SMTP server is used

Commandline value	Alternate value	Description
-sms <*value*>	VLXSMS	Text number of user
-email <*value*>	VLXEMAIL	eMail of user
-text <*value*>	VLXPIN_TEXT	Text to send (160 characters)
-subject <*value*>		Subject of the eMail / text message
-local <*value*>		Replaces local number with leading 0 to suffix <>
-00		Replaces leading + to 00
-trim		Trims leading 0

Related articles

(4.2.0) How to setup MFA with SMS response from the SMS Provider

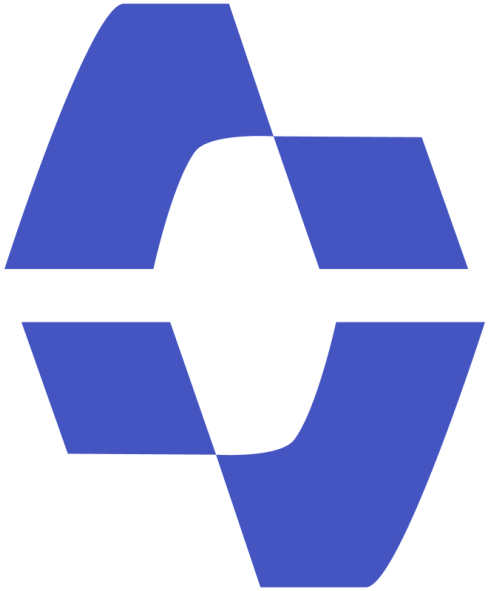
(4.2.0) How to configure a user account as a group account

(4.2.0) Variables in notifications

(4.2.0) How to create and use notifications

(4.2.0) RSA SecureID Implementation via RSA API

(4.2.0) VISULOX Webservice



(4.2.0) Transit script variables

(4.2.0) Migrating to One Time Password Authentication

(4.2.0) The VISULOX PIN Service

(4.2.0) How to control action scripts from the command line

(4.2.0) Notifications

(4.2.0) MFA via external service

(4.2.0) VISULOX Mail Client and Send PIN

(4.2.0) How to enable, configure and use MFA

(4.3.2) How to configure a user account as a group account

23.1.60 Monitoring VISULOX

The following VISULOX Commands can be used to monitor the VISULOX Services. In case of the Integrity-Check commands, the return values are: **Success** (stdout: 0)**, Warning** (stdout: 0) **and Failure** (stdout: 1)	• Commands to check the functionality of the VISULOX Services • Monitoring VISULOX base service • Command to check the connection to VISULOX PORTAL Service • Command to check the datasources • Related articles

visulox status

```
visulox status

Cluster status
    ------------------------------------------------------------------------------------------------
    |   node | location | status | archive |  uptime |  runlevel |        hostname |          started |
    ------------------------------------------------------------------------------------------------
    |  vB1LX |      DC1 |     up |         | 03m 39s | accepting |  b1-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB2LX |      DC1 |     up |         | 03m 49s | accepting |  b2-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB3LX |      DC1 |     up |         | 02m 54s | accepting |  b3-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB4LX |      DC1 |     up |         | 02m 58s | accepting |  b4-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB5LX |      DC1 |     up |         | 02m 49s | accepting |  b5-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB6LX |  ARCHIVE |     up |         | 02m 53s | accepting |  b6-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB7LX |      DC2 |     up |         | 03m 41s | accepting |  b7-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB8LX |      DC2 |     up |         | 03m 37s | accepting |  b8-lx.tbsol.de | 2015-06-10 14:23 |
    |  vB9LX |      DC2 |     up |         | 02m 57s | accepting |  b9-lx.tbsol.de | 2015-06-10 14:23 |
    | vB10LX |      DC2 |     up |         | 03m 00s | accepting | b10-lx.tbsol.de | 2015-06-10 14:24 |
    | vB11LX |      DC2 |     up |         | 02m 54s | accepting | b11-lx.tbsol.de | 2015-06-10 14:23 |
    ------------------------------------------------------------------------------------------------
```

Only certain fields can be selected with the **-fields <>** parameter. A list of the fields is displayed with **-print**.

Other output formats are available and can be used with the **-format** parameter:

```
visulox status -format json
```

```
visulox status -format csv
```

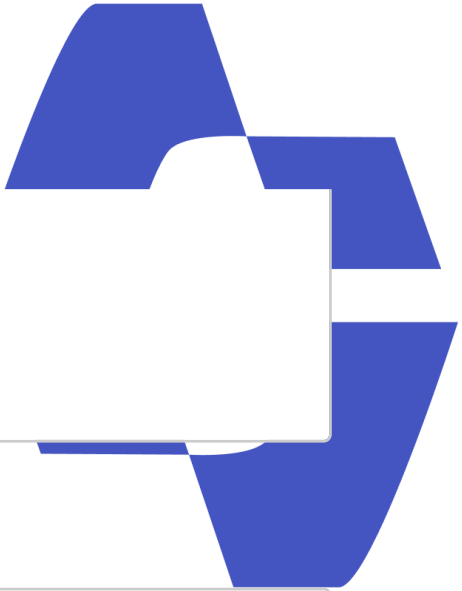
Current usage via status command:

```
visulox status usage
```

Monitoring VISULOX base service

visulox integrity -vlx

```
visulox integrity -vlx

    ------------------------------------------------------------------------------
    | option | cat             | info                                  | returnCode |
    ------------------------------------------------------------------------------
    | -vlx   | Install Base    | ok                                    | SUCCESS(0) |
    | -vlx   | monitor         | online                                | SUCCESS(0) |
    | -vlx   | router          | online                                | SUCCESS(0) |
    | -vlx   | dict            | online                                | SUCCESS(0) |
    | -vlx   | database        | online                                | SUCCESS(0) |
    | -vlx   | store           | online                                | SUCCESS(0) |
    | -vlx   | filecopy        | online                                | SUCCESS(0) |
    | -vlx   | filecache       | online                                | SUCCESS(0) |
    | -vlx   | pin             | online                                | SUCCESS(0) |
    | -vlx   | config          | online                                | SUCCESS(0) |
    | -vlx   | scripts         | online                                | SUCCESS(0) |
    | -vlx   | policy          | online                                | SUCCESS(0) |
    | -vlx   | publish         | online                                | SUCCESS(0) |
```



```
    | -vlx   | importer        | online                                | SUCCESS(0) |
    | -vlx   | portalConnector | online                                | SUCCESS(0) |
    | -vlx   | gate            | online                                | SUCCESS(0) |
    | -vlx   | object2Portal   | online                                | SUCCESS(0) |
    | -vlx   | replication     | Standalone node: can be disabled      |       INFO |
    | -vlx   | vT2OL7U2        | all ports to t2-ol7u2.tbsol.de are ok | SUCCESS(0) |
    ---------------------------------------------------------------------------
```

Command to check the connection to VISULOX PORTAL Service

visulox integrity -portal

```
visulox integrity -portal
    ---------------------------------------------------------------------------
    | option  | cat              | info                          | returnCode |
    ---------------------------------------------------------------------------
    | -portal | core             | PORTAL 5.60                   | SUCCESS(0) |
    | -portal | connect          | yes                           | SUCCESS(0) |
    | -portal | webtop           | ok                            | SUCCESS(0) |
    | -portal | var              | security-xsecurity ok         | SUCCESS(0) |
    | -portal | var              | xpe-maxsessions ok            | SUCCESS(0) |
    | -portal | var              | xpe-maxusers ok               | SUCCESS(0) |
    | -portal | role             | administrator is root         | WARNING(2) |
    | -portal | array            | P: mp-vlx32-ol7.tbsol.de      | SUCCESS(0) |
    | -portal | security-gateway | mp-vlx32-ol7.tbsol.de is good | SUCCESS(0) |
    ---------------------------------------------------------------------------
```

Command to check the datasources

```
visulox integrity -datasources
Please wait ...
Integrity-Check: VISULOX EVALUATION / development / development
    ------------------------------------------------------------------------
    | option       | cat         | info                    | returnCode |
    ------------------------------------------------------------------------
    | -datasources | TESTLDAPS,0 | ok                      | SUCCESS(0) |
    | -datasources | TESTAD,0    | TESTAD:0 not reachable | FAILURE(1) |
    | -datasources | TESTAD,1    | ok                      | SUCCESS(0) |
    ------------------------------------------------------------------------

ExitCode: FAILURE
One or more tests failed! For more information see /tmp/visulox-integrity.log
```

Related articles

Interface for current usage - stats.sh

How to send VISULOX Events to external services

Interface for current usage - stats.sh

Overview

VISULOX usage stats are generated via rrd tool and can be seen in VISULOX Cockpit / Cluster status.

With the stats service it is possible to trigger a script each time a new entry is written into the rrd.

An example script is available: **/opt/visulox/tools/stats.sh.template**. This script has to be renamed to **stats.sh** and the file permissions must be **vlx/vlxgroup/0550**.

Usage

Example of a simple dump script for testing:

Dump

```
#!/bin/bash
dump () {
 (
  echo "----------------------------------------"
  date
  env | lsort | egrep -e ^VLX[A-Z]
 ) >> $1
  # generated file must have group write permissions for other vlxusers
  chmod -f g+w $1
}
dump /tmp/stats.visulox
exit 0
```

Environment variables

The following environment variables are available:

Variable	Description
VLXUSAGE_SESSIONS	Current running sessions
VLXUSAGE_COMMANDCONNECTS	Current running Command Connects
VLXUSAGE_USERS	Current working users
VLXUSAGE_RECORDERS	Current running recorders
VLXUSAGE_TIME	Usage time

Related articles

How to send VISULOX Events to external services

Monitoring VISULOX

23.1.61 How to setup VISULOX end2end monitoring

About

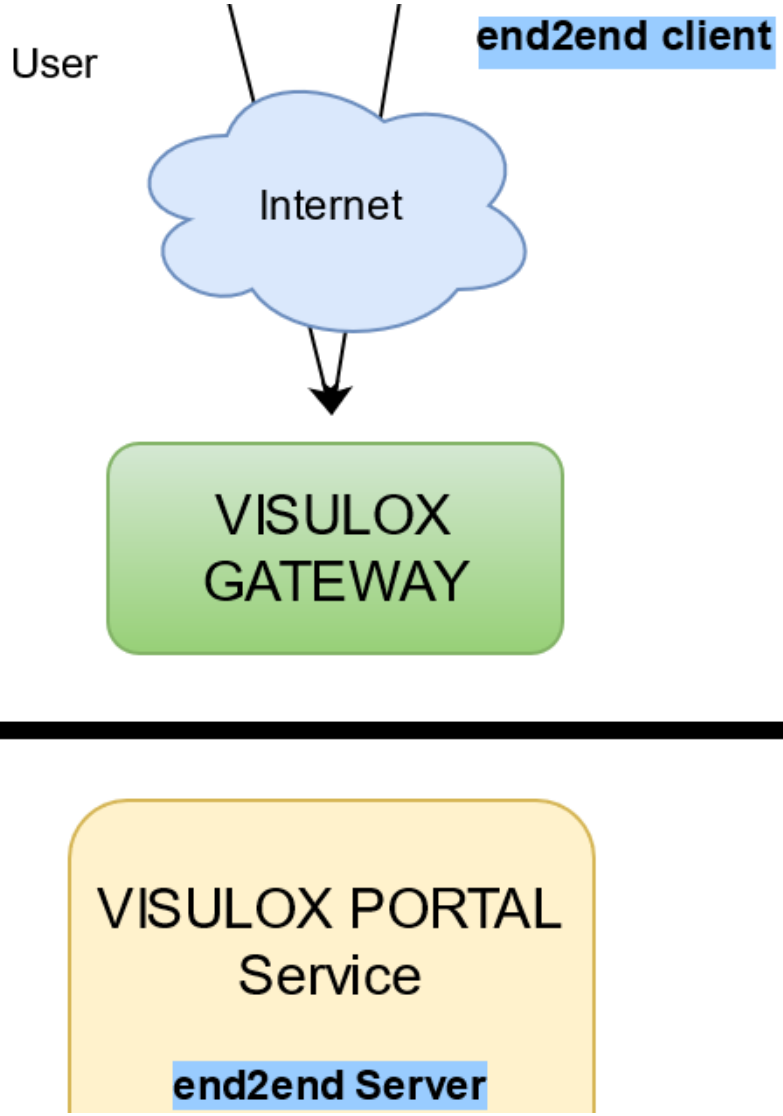
VISULOX end2end has a **server** and a **client** side component.

On the **server side** the end2end server component has to be installed on the VISULOX Access Nodes via a script.

For the **client side** two RPM packages have to be installed on an **external** Linux server. The check on the client side can be triggered by cron. The tool simulates a user and checks the reachability of the VISULOX Access Nodes.

Login into the VISULOX PORTAL and launching an application will be executed automatically.

- About
- Setup on the VISULOX Access Nodes
- Installing the end2end client


User
end2end client
Internet
VISULOX
GATEWAY
VISULOX PORTAL
Service
end2end Server

Setup on the VISULOX Access Nodes

The following setup script has to be launched on **all** VISULOX Access Nodes:

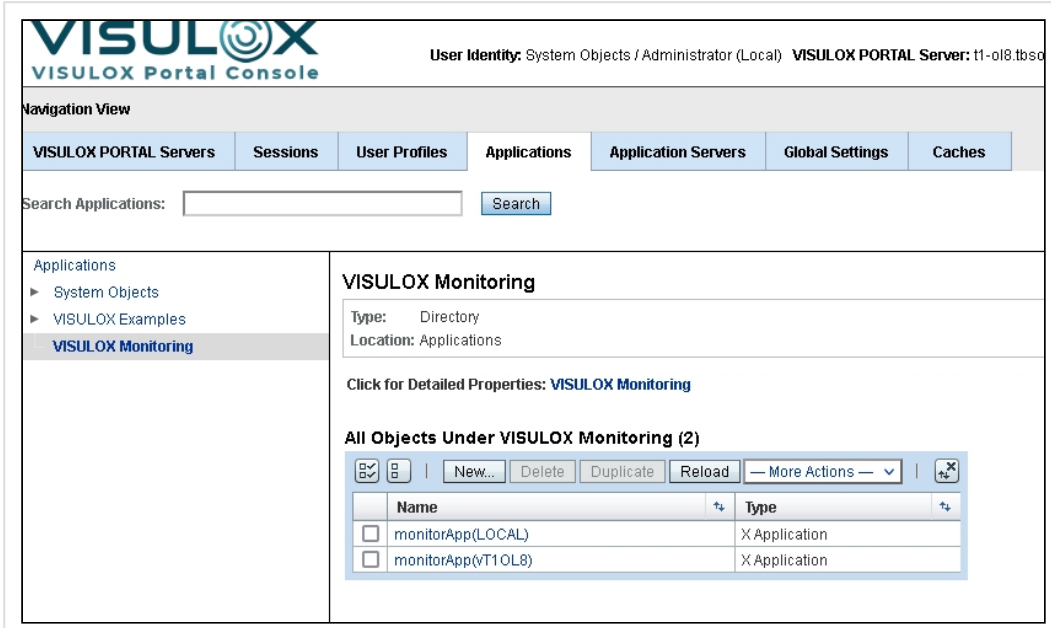
setupEnd2End.sh on the server side
`/opt/visulox/setup/monitoring/setupEnd2End.sh`

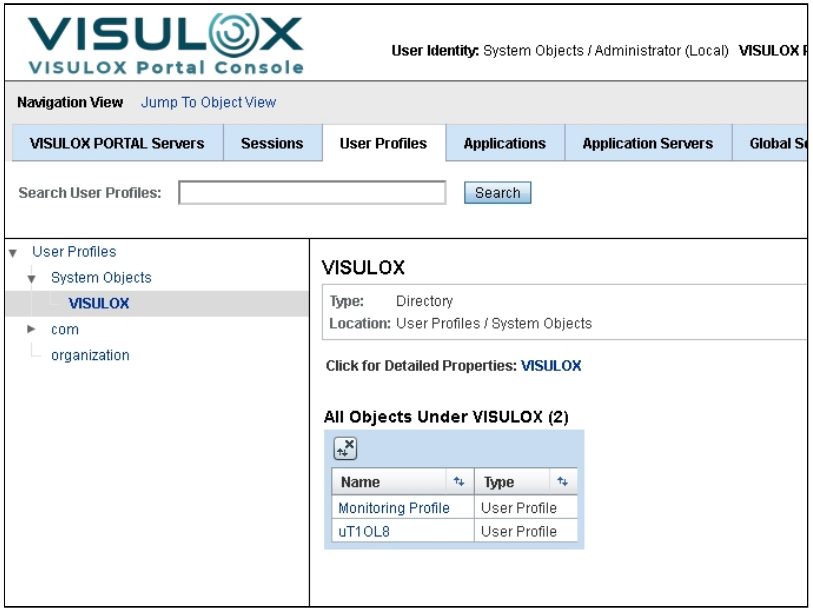
With this script a configuration file is created that has to be copied to the end2end client.

The setup creates 1+**n** applications, **n** is the number of nodes in the cluster.
With the parameter **-id <*nodename*>** the availability of a certain node can be tested.

> ⚠ In an environment with more VISULOX Access Nodes, run the script on **all** VISULOX Access Nodes.

Added end2end default applications and user profile:





Own monitoring applications can be added manually as well, for example:

```
o=applications/ou=VISULOX Monitoring/cn=monitorApp(XSTRESS)
```

Then this application can be addressed with **-id XSTRESS**.

Installing the end2end client

To install the end2end client, the VISULOX RTE package and the VISULOX End2End package is needed.

```
yum update
```

```
yum install visulox-rte-1.2.0-1.el8.x86_64.rpm
yum install visulox-end2end-4.0.0-1.rpm
```

Copy the created configuration file from the VISULOX Portal Server to the **/opt/visulox-end2end/** directory.

Basic example for running the end2end client from CLI:

Example with no cert check

```
visulox-end2end -nocheck -clientname T1-TEST -secretfile  end2end-client.conf  https://<host.domain>

2023-07-20 09:57:24.413 :   CERT :Verification error: self signed certificate
2023-07-20 09:57:24.451 :   INFO :login
2023-07-20 09:57:25.561 :   INFO :startClient
2023-07-20 09:57:31.810 :   INFO :startApp
2023-07-20 09:57:41.380 :   INFO :done (2)
2023-07-20 09:57:41.380 :   INFO :logout
Duration : 17s
```

end2end client parameters:

```
visulox-end2end options:

 -headless            run in  headless mode
 -clientname value    Alternate Clientname <>
 -secretfile value    Alternate Secretfile <>
 -id value            App ID <LOCAL>
 -startport value     Xvfb Port <100>
 -timeout value       maximum time to start application  <15>
```

```
-nocheck            no cert check
-quiet              only the duration result
-debug              debugging
-curl               print CURL Calls
--                  Forcibly stop option processing
-help               Print this message
-?                  Print this message
```

Use the parameter **-nocheck** with care. The monitoring only works with root certificates known by the client.
With **-headless** the test can be done via X11 (important for the Cron implementation)
With **-clientname** an information can be added to the end2end.sh record to see the different clients, if more than one portals are tested.

If **/opt/visulox/tools/end2end.sh** exists on the server, the monitoring tests will be logged by this script.

23.1.62 Integrity-Check

The Integrity-Check is started automatically during installation of VISULOX to make sure, that all requirements are met for a properly running system.

However Integrity-Check can also be used in an already running environment for diagnose purpose.

Integrity-Check can be started via the visulox command:

```
visulox integrity
```

In the quiet mode no shell output and no log entries in **/tmp/visulox-integrity.log** are written.

Only the Integrity-Check exit code will be returned:

```
visulox integrity -quiet
```

Available Integrity-Check commands

Command	Description
-sw	Check of online software status
-vlx	Check the VLX Services and cluster ports
-sys	Check the system environment
-lib	Check for missing libs
-cmd	Check command for missing libraries
-disk	Check disk
-users	Check VISULOX transit users
-portal	Check the VISULOX PORTAL Service
-cert	Check certificates within VISULOX and VISULOX PORTAL

Command	Description
-store	Check store
-recorder	Check recorder
-datasources	Check datasources
-assignments	Check datastore assignments and dynamic applications
-license	Check license
-policies	Check policies (VISULOX must be online)
-index	Check index
-scripts	Check scripts
-x11forward	Check x11forward
-gate	Check gate config
-mail	Check mail configuration

General commands

Command	Description
-format <*value*>	Format of output (text,xml,csv,json,tcl) <*text*>
-verbose	More messages on stdout
--	Forcibly stop option processing
-help	Print this message
-?	Print this message

Usage

```
visulox integrity

Please wait ....
Integrity-Check: amitego engineering  - in house license / beta2-3.1.1 / 2016-07-12 12:46:32 UTC
    ------------------------------------------------------------------------------
    | option   | cat                                    | info          | returnCode |
    ------------------------------------------------------------------------------
    | -license | check                                  | Evaluation    | WARNING(2) |
```

```
    | -sys     | Script /opt/visulox/tools/filecheck.sh | not configured | WARNING(2) |
    | -sys     | Script /opt/visulox/tools/event.sh     | not configured | WARNING(2) |
    | -portal  | 5.60 Warnings                          | see logfile    | WARNING(2) |
    ------------------------------------------------------------------------------

ExitCode: WARNING
Check the warnings. For more information see /tmp/visulox-integrity.log
```

Only warnings and errors are displayed by default. All Integrity checks can be shown with the **-verbose** parameter.

visulox integrity -portal

```
    ------------------------------------------------------------------------
    | option   | cat              | info                          | returnCode |
    ------------------------------------------------------------------------
    | -portal | core              | PORTAL 5.60                   | SUCCESS(0) |
    | -portal | connect           | yes                           | SUCCESS(0) |
    | -portal | webtop            | ok                            | SUCCESS(0) |
    | -portal | var               | security-xsecurity ok         | SUCCESS(0) |
    | -portal | var               | xpe-maxsessions ok            | SUCCESS(0) |
    | -portal | var               | xpe-maxusers ok               | SUCCESS(0) |
    | -portal | role              | administrator is root         | WARNING(2) |
    | -portal | array             | P: mp-vlx32-ol7.tbsol.de      | SUCCESS(0) |
    | -portal | security-gateway  | mp-vlx32-ol7.tbsol.de is good | SUCCESS(0) |
    ------------------------------------------------------------------------
```

visulox integrity -cert

```
   ------------------------------------------------------------------------------------------------
    | option | cat       | info                                                          | returnCode |
    ------------------------------------------------------------------------------------------------
```

```
    | -cert  | SSL-CERT  | issuer  =  /C=de/ST=de/O=amitego/CN=test.tbsol.de          | SUCCESS(0) |
    | -cert  | SSL-CERT  | subject = test.tbsol.de                                   | SUCCESS(0) |
    | -cert  | SSL-CERT  | serial  = EA8628EF3B3A7F44                                | SUCCESS(0) |
    | -cert  | SSL-CERT  | from    = 2016-12-16 09:12                                | SUCCESS(0) |
    | -cert  | SSL-CERT  | until   = 2017-12-16 09:12                                | SUCCESS(0) |
    | -cert  | SSL-CERT  | remain  = 360d 21h                                        | SUCCESS(0) |
    | -cert  | PEER-CERT | issuer  =  /CN=mp-ol6u3-devel.tbsol.de CA Cert            | SUCCESS(0) |
    | -cert  | PEER-CERT | subject = test.tbsol.de CA Cert                           | SUCCESS(0) |
    | -cert  | PEER-CERT | serial  = 9F3D8E05D8800F22                                | SUCCESS(0) |
    | -cert  | PEER-CERT | from    = 2013-07-15 12:20                                | SUCCESS(0) |
    | -cert  | PEER-CERT | until   = 2023-07-13 12:20                                | SUCCESS(0) |
    | -cert  | PEER-CERT | remain  = 2395d 23h                                       | SUCCESS(0) |
    | -cert  | SSL-CA    | issuer  =  /C=de/ST=de/O=amitego/CN=test.tbsol.de          | SUCCESS(0) |
    | -cert  | SSL-CA    | subject = test.tbsol.de                                   | SUCCESS(0) |
    | -cert  | SSL-CA    | serial  = EA8628EF3B3A7F44                                | SUCCESS(0) |
    | -cert  | SSL-CA    | from    = 2016-12-16 09:12                                | SUCCESS(0) |
    | -cert  | SSL-CA    | until   = 2017-12-16 09:12                                | SUCCESS(0) |
    | -cert  | SSL-CA    | remain  = 360d 21h                                        | SUCCESS(0) |
    ------------------------------------------------------------------------------------------------
```

Integrity check with the parameter **-cert** shows the status of the both VISULOX PORTAL certificates. PEER-CERT and SSL-CERT.

The serials can be displayed on the local VISULOX GATEWAY with the command **visulox-gateway server list** and have to match with the serials of the VISULOX PORTAL certificates.

Integrity check shows a warning, when the lifetime is lower than 30 days or an error when the lifetime is expired.

visulox integrity -disk

```
Please wait ...Integrity-Check: VISULOX EVALUATION / xdevelopment / development
    ------------------------------------------------------------------------------------
    | option | cat          | info                                          | returnCode |
    ------------------------------------------------------------------------------------
    | -disk  | Diskspace    | ok in base (base threshold at 2.0GB has 39.67GB)  | SUCCESS(0) |
```

```
    | -disk  | Diskspace    | ok in var (var threshold at 5.0GB has 39.67GB)    | SUCCESS(0) |
    | -disk  | Diskspace    | ok in data (data threshold at 20.0GB has 39.67GB) | SUCCESS(0) |
    | -disk  | Diskspace    | ok                                                | SUCCESS(0) |
    | -disk  | DB Partition | ok fileserver.tbsol.de:/home/users/xxx            | SUCCESS(0) |
    | -disk  | DB Partition | needs atleast 157.30MB - has 39.67GB              | SUCCESS(0) |
    ------------------------------------------------------------------------------------------
ExitCode: SUCCESS
```

Among the checks also the diskspace for the database is checked. 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 integriy check.

Troubleshooting

- **VISULOX PORTAL connect failure**

  On servers, where VISULOX Service is installed together with VISULOX PORTAL Service, the connection to the VISULOX PORTAL Service can be checked with a small tool:

```
/opt/visulox/lib/utils/sgd.tcl check

Check connections

-------------------------------------------------------------------------------------------------------------------------
    |                                        scottasessionid |                                        scottasessionowner
|

-------------------------------------------------------------------------------------------------------------------------
    | test-ol6u5.tbsol.de:1434362892796:1108252004568201775 | {.../_ens/o=Tarantella System Objects/ou=Visulox/cn=test-ol6u5}
|
```

```
-------------------------------------------------------------------------------------------------------------------------
```

The following command reinstalls the necessary VISULOX PORTAL Service components on the server and mostly fixes connection errors:

```
visulox portal attach
```

- **VISULOX PORTAL Service warnings**

  More details can be found in visulox-integrity.log. The Java tuning values should be adjusted for the environment.
  Mostly, the following settings will be adequate:
  - tuning-jvm-initial: 1024
  - tuning-jvm-max: 2048
  - tuning-jvm-scale: 150

Adjust the values, with:

```
visulox-portal config edit --tuning-jvm-initial 2048
visulox-portal config edit --tuning-jvm-max 2048
visulox-portal config edit --tuning-jvm-scale 150
```

The following VISULOX PORTAL Service default values should also be checked:

- sessions-timeout-always
- sessions-timeout-session
- webtop-session-idle-timeout

Changes of VISULOX PORTAL Service configurations is known to VISULOX after "**visulox portal attach -portal**".

- **"Administrator is root" warning**

  The warning can be disabled by adding a new administrator to VISULOX PORTAL:

  Add a user

  ```
  useradd <name of the new portal administrator>
  passwd <name of the new portal administrator>
  ```

  Add the new administrator to the VISULOX PORTAL administrators

  ```
  visulox-portal object edit --name "/o=tarantella system objects/cn=administrator" --user admin
  ```

  After changes to the VISULOX PORTAL, VISULOX needs to be reregistered

  ```
  visulox portal attach
  ```

  Doing a VISULOX Integrity-Check again, the warning has disappeared. root can be removed from the administrators list.

- **event.sh and filecheck.sh missing**

  The files event.sh.template and filecheck.sh.template in **/opt/visulox/tools/** must be copied to event.sh and filecheck.sh, if needed.
  The correct permission (**0550 / vlx:vlxgroup**) has to be set as well for these files.

  ```
  cd /opt/visulox/tools
  cp events.sh.tmplate events.sh
  cp filecheck.sh.template filecheck.sh
  chown vlx: events.sh filecheck.sh
  ```

```
chmod 0550 events.sh filecheck.sh
```

23.1.63 How to increase the log level

VISULOX has several log levels:

error	In a production environment, the log level is set to error and should only be changed by the support
warning	Also displays warnings
info	Also displays info entries
debug	Displays all available information

The log level is a general parameter for the whole cluster and for all programs.

Set log level to debug

```
visulox config edit -name logger.level=debug
```

Some commands can be started with an explicit log level:

```
<command> -log debug ...
```

Enabling logging in a running production environment for a service:

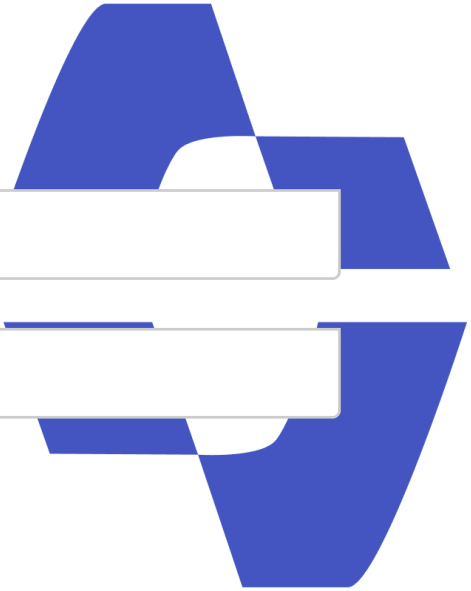
```
/opt/visulox/bin/cmd/msg.tcl -to <service> -command LOGLEVEL -loglevel debug
```

It is also possible to reset the loglevel after a period of time automatically:

```
/opt/visulox/bin/cmd/msg.tcl -to <service> -command LOGLEVEL -loglevel debug -resetafter "1 hour"
```

Possible values:

- -resetafter "60 seconds"
- -resetafter "1 minute"
- -resetafter "2 hours 30 minutes"



⚠ Always remember to set the log level back to error after debugging (if **resetafter** is not set).

⚠ Configuration parameters set while the node is **offline** will only be applied to the **local node**.
If a parameter should be changed for the whole cluster, the parameter has to be set **again** once the node is **online** again.

23.1.64 Command "visulox support" - Creating a VISULOX Support Report

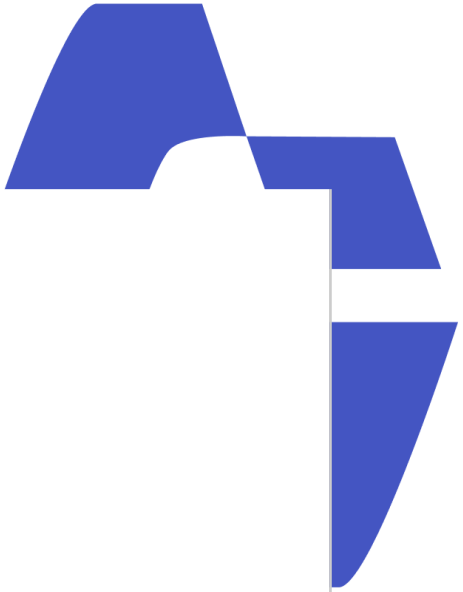
- VISULOX Support Report
- VISULOX Short Support Report
- Related information

VISULOX Support Report

With the **visulox support** command an overview of the installed components, the configuration and the logfiles is created as a ZIP archive.This archive is password protected.

If the command is executed with root permissions, the VISULOX PORTAL Service log files will be collected as well.

```
visulox support

config ...
    get cluster using </globalhome/mpro/vsx30/bin/visulox status -verbose -format csv> ...
    get license using </globalhome/mpro/vsx30/bin/visulox license> ...
    get config using </globalhome/mpro/vsx30/bin/visulox config list -format csv> ...
    get archive using </globalhome/mpro/vsx30/bin/visulox archive> ...
dbstat ...
    get dbstat using </globalhome/mpro/vsx30/bin/visulox database  backup -path /tmp/vlxdb.25780 -stat> ...
dump ...
etc ...
integrity ...
    get integrity using </globalhome/mpro/vsx30/bin/visulox integrity -verbose -format csv> ...
logs ...
net ...
    get iptable using </sbin/iptables --list> ...
    get ifconfig using </sbin/ifconfig> ...
platform ...
    get hosts using <cat /etc/hosts> ...
    get resolve.conf using <cat /etc/resolv.conf> ...
    get platform using <uname -a> ...
    get processtable using <ps -aef> ...
    get memory using <free> ...
    get selinux using <cat /etc/selinux/config> ...
    get ntp using <ntpq -p> ...
    get date using <date> ...
    get df using </bin/df> ...
    get mount using </bin/mount> ...
runtime ...
tta ...
    get version using </opt/tarantella/bin/tarantella version> ...
    get patch using </opt/tarantella/bin/tarantella patch list> ...
```



```
    get array using </opt/tarantella/bin/tarantella array list> ...
    get gateway using </opt/tarantella/bin/tarantella gateway list> ...
    get config using </opt/tarantella/bin/tarantella config list> ...
    get service using </opt/tarantella/bin/tarantella service list> ...
    get tarantella logs ...
    get apache logs ...
    get tomcat logs ...
userlogs ...
    get user logs ...
var ...
Result in /tmp/visulox-support-vMPOL6U3DEVEL.zip
Passcode is HVCyv7M3
```

The result is copied to a password protected ZIP file: **/tmp/visulox-support-<*host*>.zip**

The generated archive (and the passcode) is useful to request support from the hotline and should be sent to amitego engineering in case of a support request.

The Support Report passcode is shown at the end of the output and it is also stored in a file: **/tmp/.vlx.supportid**.

The option "**-unprotect**" allows to generate an unprotected ZIP archive.

VISULOX Short Support Report

A Short Support Report to send via eMail can be created as well:

visulox support -info

```
visulox support -info

Get Support Header ...
   done
```

```
---------------------- snip -----------------
     Datum : 2017-08-30 07:18:59
  SystemId : Evaluation
  Platform : Linux mp-ol6u3-devel 3.8.13-118.4.2.el6uek.x86_64
   VISULOX : xdevelopment (development)
     Nodes : VISULOX is not running!
     Nodes : vMPOL6U3DEVEL
      OSGD : 5.30.914 (Patch_53p1, JVM_1.8.0_131, apache-2.2.32_openssl-1.0.2k_jk1.2.42_64, tomcat-7.0.75, Patch_53p1hf1)
     ARRAY : mp-ol6u3-devel.tbsol.de
---------------------- snip -----------------
```

To get the complete information, the Short Support Report should be started as root user.

The Short Support Report should be sent to the **VISULOX Support Team** every time a new Support Request is opened.

Related information

Command "visulox log" - Analyzing log files

VISULOX Service command

How to control reports from the command line

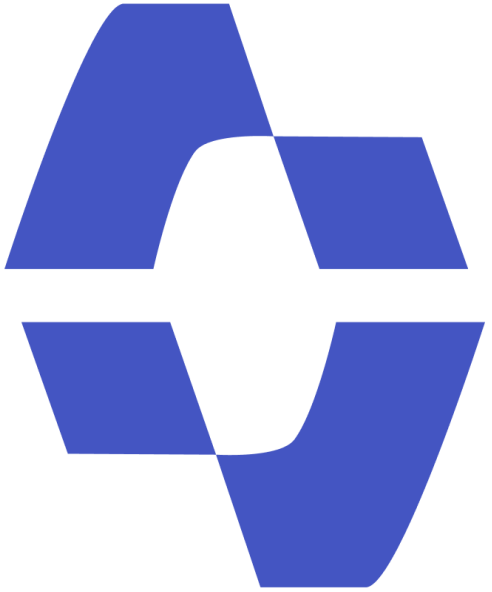
23.1.65 Messages in VISULOX

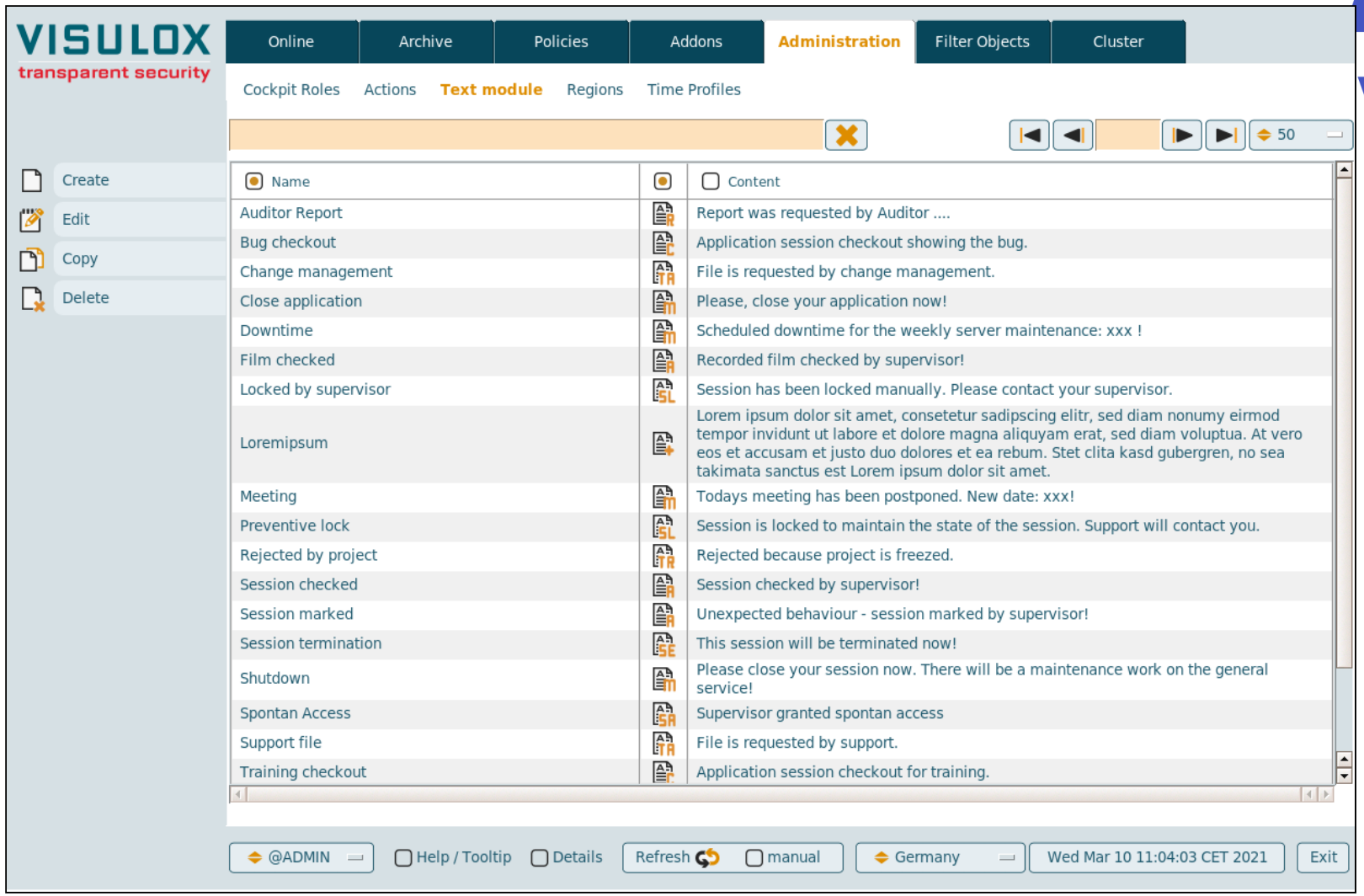
In VISULOX a text can be sent to users, appended to sessions or needed in workflows.

These texts can be composed using the message feature in VISULOX Cockpit / Administration / Text module.

A message in VISULOX is a piece of text, which is often used. Each message has a category, where it can be used.

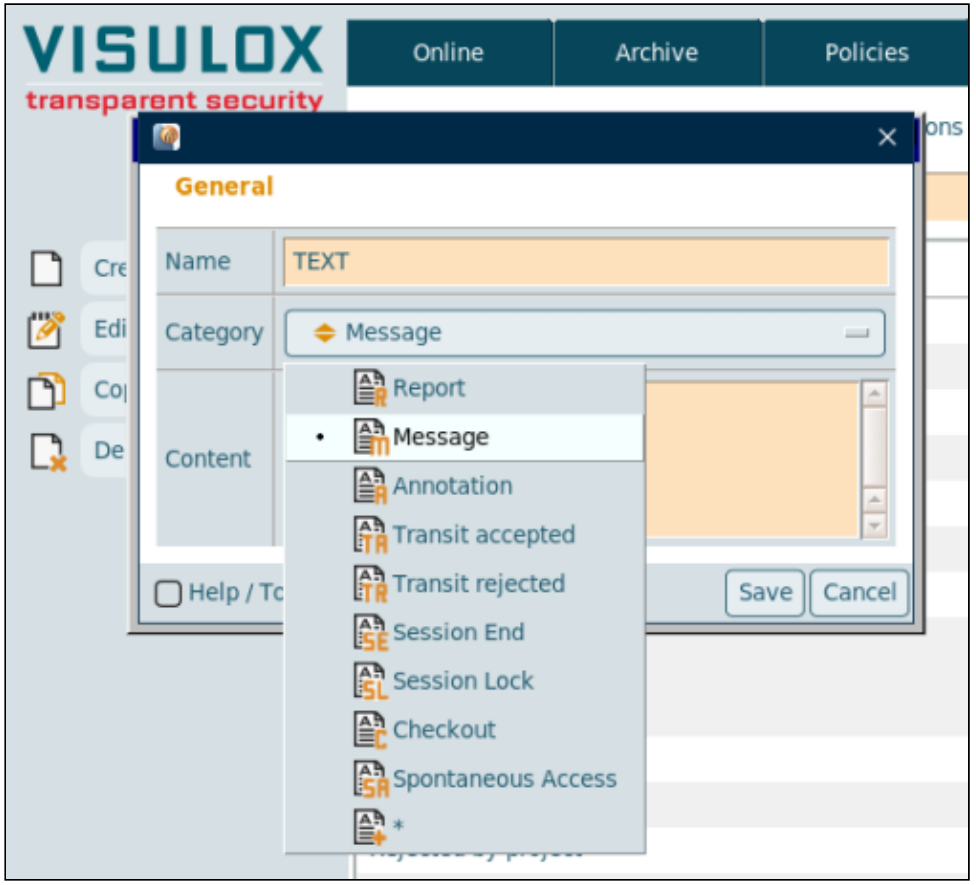
- VISULOX Cockpit / Administration / Text module
- Categories
- Allowed tags in messages
- Configuration parameters
- Related information




VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
Cluster
Cockpit Roles
Actions
Text module
Regions
Time Profiles
50
Create
Edit
Copy
Delete
Name
Content
Auditor Report
Report was requested by Auditor ....
Bug checkout
Application session checkout showing the bug.
Change management
File is requested by change management.
Close application
Please, close your application now!
Downtime
Scheduled downtime for the weekly server maintenance: xxx !
Film checked
Recorded film checked by supervisor!
Locked by supervisor
Session has been locked manually. Please contact your supervisor.
Loremipsum
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.
Meeting
Todays meeting has been postponed. New date: xxx!
Preventive lock
Session is locked to maintain the state of the session. Support will contact you.
Rejected by project
Rejected because project is freezed.
Session checked
Session checked by supervisor!
Session marked
Unexpected behaviour - session marked by supervisor!
Session termination
This session will be terminated now!
Shutdown
Please close your session now. There will be a maintenance work on the general service!
Spontan Access
Supervisor granted spontan access
Support file
File is requested by support.
Training checkout
Application session checkout for training.
@ADMIN
Help / Tooltip
Details
Refresh
manual
Germany
Wed Mar 10 11:04:03 CET 2021
Exit

Categories

Category	Used
Message	to send to a session, e.g. Online / Message
Annotation	to make an annotation for a session
Spontaneous access	when temporary access is granted
Transit accepted	to accept a pending File Transfer file
Transit rejected	to reject a pending File Transfer file
Session end	to end a session
Session lock	to lock a session
Report	for reporting
Checkout	when a checkout is done
*	these messages are available everywhere they can be used



Available predefined messages can be selected via a drop down list.

Allowed tags in messages

Modes	Tag
bold	text
large	<l1>text</l1>, <l2>text</l2>, <l3>text</l3>
center	text
italic	text
line break	
horizontal line	<hr>
link	link text (Be careful: only one link per line!)

Configuration parameters

It is possible to configure the minium amount of words and the maximum length of a text for the different messages.

List of entries with minimum words setting

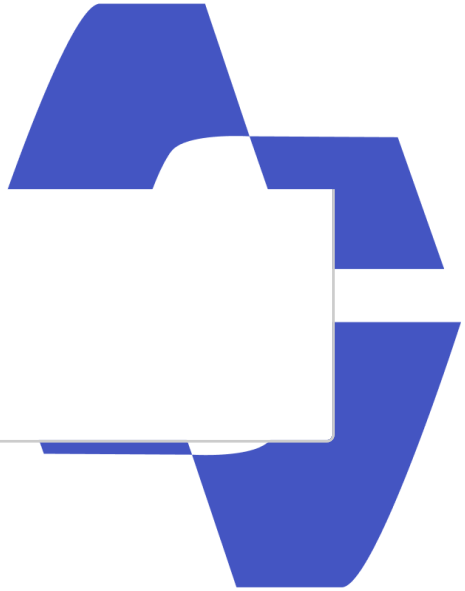
```
visulox config list -name entry.minwords

    ------------------------------------------------------------
    | changed | key                                    | value   |
    ------------------------------------------------------------
    |         | entry.minwords.access_policy           | default |
    |         | entry.minwords.annotation              | 3       |
    |         | entry.minwords.application_policy      | default |
    |         | entry.minwords.checkout                | 3       |
    |         | entry.minwords.citrixobject_form       | 0       |
    |         | entry.minwords.commandconnect          | default |
    |         | entry.minwords.commandguard            | default |
    |         | entry.minwords.default                 | 0       |
    |         | entry.minwords.external_message_policy | 1       |
    |         | entry.minwords.filetransit             | default |
    |         | entry.minwords.ftapproved              | 3       |
    |         | entry.minwords.ftreject                | 3       |
    |         | entry.minwords.host_object             | default |
    |         | entry.minwords.internal_message_policy | 1       |
    |         | entry.minwords.login_policy            | default |
    |         | entry.minwords.cockpit                 | default |
    |         | entry.minwords.message                 | 3       |
    |         | entry.minwords.region                  | default |
    |         | entry.minwords.resource                | default |
    |         | entry.minwords.script                  | default |
    |         | entry.minwords.script_object           | 1       |
    |         | entry.minwords.sessionend              | default |
    |         | entry.minwords.sessionlock             | default |
    |         | entry.minwords.spontanaccess           | 3       |
    |         | entry.minwords.textblocks              | 3       |
    |         | entry.minwords.timeprofile             | default |
```

```
    |         | entry.minwords.transit_policy          | default |
    ------------------------------------------------------------
```

List of entries with maximum length setting

```
visulox config list -name  entry.maxlength

    ------------------------------------------------------------
    | changed | key                                    | value   |
    ------------------------------------------------------------
    |         | entry.maxlength.access                 | default |
    |         | entry.maxlength.access_policy          | default |
    |         | entry.maxlength.annotation             | default |
    |         | entry.maxlength.application_policy     | default |
    |         | entry.maxlength.checkout               | default |
    |         | entry.maxlength.citrixobject_form      | 2048    |
    |         | entry.maxlength.commandconnect         | default |
    |         | entry.maxlength.commandguard           | default |
    |         | entry.maxlength.default                | 255     |
    |         | entry.maxlength.external_message_policy | default |
    |         | entry.maxlength.filetransit            | default |
    |         | entry.maxlength.ftapproved             | default |
    |         | entry.maxlength.ftreject               | default |
    |         | entry.maxlength.host_object            | default |
    |         | entry.maxlength.internal_message_policy | default |
    |         | entry.maxlength.login_policy           | default |
    |         | entry.maxlength.cockpit                | default |
    |         | entry.maxlength.message                | default |
    |         | entry.maxlength.region                 | default |
    |         | entry.maxlength.resource               | default |
    |         | entry.maxlength.script                 | default |
```

```
|         | entry.maxlength.script_object          | default |
|         | entry.maxlength.sessionend             | default |
|         | entry.maxlength.sessionlock            | default |
|         | entry.maxlength.textblocks             | default |
|         | entry.maxlength.timeprofile            | default |
|         | entry.maxlength.transit_policy         | default |
-----------------------------------------------------------------
```



Related information

Setting the min/max length for messages, contents and comments

How to control messages from the command line

How to control messages from the command line

Overview The command line tool "**VISULOX admin message**" allows to control messages.	• Overview • Usage • Message elements (edit) • Examples

Usage

The following subcommands are available:

Command	Description
list	List and print messages.
add	Add a message.
edit	Modify fields of a message.
delete	Remove a message.
categories	Show all available message categories
fields	List available database fields (**-raw** = enhanced output)

Message elements (edit)

Element	Description
-name <>	Name of the message or use AUTO <> (mandatory)
-category <>	Message category <> (mandatory!)
-content <>	Content of the message <>
-grant <>	Set granted user in database record <>

Examples

List current available messages

```
visulox admin message list
    ----------------------------------------
    |            basicname |      category |
    ----------------------------------------
    |             Downtime |          info |
    |              Meeting |          info |
    |              Welcome |          info |
    |      Session checked |    annotation |
    |         Film checked |    annotation |
    |       Session marked |    annotation |
    |             Shutdown |       message |
    |  Session termination |    sessionend |
    |       Spontan Access | spontanaccess |
    |      Preventive lock |   sessionlock |
    | Locked by supervisor |   sessionlock |
    |    Close application |       message |
    |      Unknown content |      ftreject |
    |  Rejected by project |      ftreject |
    |    Change management |    ftapproved |
    |         Support file |    ftapproved |
    |         Bug checkout |      checkout |
    |    Training checkout |      checkout |
    ----------------------------------------
```

Add new message

```
visulox admin message add -name Test -category info -content "Adding a new test message"
```

Edit message

```
visulox admin action edit -name Test -grant Supervisor
```

Display available categories

```
visulox admin message categories
info,message,annotation,ftapproved,ftreject,sessionend,sessionlock,sessionrecmanually,checkout,spontanaccess
```

Remove an entry

```
visulox admin message delete -name Test
```

23.1.66 Useful database queries: Size of film chapters, snapshots, files, usage

Overview

- Overview
- Report queries
  - Recorded films
    - Average size of film chapters

        - Show total film size
    - Usage
        - List unused applications via report command
        - Top used applications
        - Login failures
- Database queries
    - Recorded films
        - Size of all files (chapters, snapshots, transferred files)
        - Size of film chapters only
        - Size of snapshots only
        - Size of transferred files only
        - Average chapter size
    - Usage
        - Most used application
        - Most active user

Report queries

Recorded films

Average size of film chapters

Average size of film chapters

```
visulox report -query averageFilm -tframe CURRMONTH -raw

Average size of film chapters (in KB)
```

```
221.52
```

Show total film size

Total film size of the day

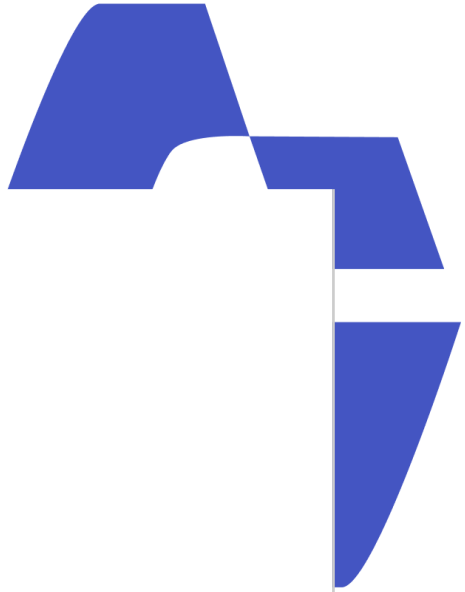
```
visulox report -query totalFilmSize -tframe CURRDAY -raw

Size of all files (in KB)
1046
```

Usage

List unused applications via report command

Unused applications of the current month

```
visulox report -query unusedApplications -tframe CURRMONTH -raw

APPLICATION
o=applications/cn=3270
o=applications/cn=5250
o=applications/cn=Unix Desktop
o=applications/cn=Windows Desktop
o=applications/cn=gnome-edit (mp-ol6u3-devel)
o=applications/cn=xclock (mp-ol6u3-devel)
o=applications/ou=VISULOX Examples/cn=@VLX XSTRESS (R)
o=applications/ou=VISULOX Examples/cn=VLX Assist
o=applications/ou=VISULOX Examples/cn=VLX CITRIX ICA
o=applications/ou=VISULOX Examples/cn=VLX CITRIX MGR
```



```
o=applications/ou=VISULOX Examples/cn=VLX Command Connect
o=applications/ou=VISULOX Examples/cn=VLX Command Guard
o=applications/ou=VISULOX Examples/cn=VLX Devel GUI ()
o=applications/ou=VISULOX Examples/cn=VLX FT Client
o=applications/ou=VISULOX Examples/cn=VLX Management (all,de)
o=applications/ou=VISULOX Examples/cn=VLX Management (all,es)
o=applications/ou=VISULOX Examples/cn=VLX Management (all,pt)
o=applications/ou=VISULOX Examples/cn=VLX Management (testrole)
o=applications/ou=VISULOX Examples/cn=VLX RDP
o=applications/ou=VISULOX Examples/cn=VLX RDP SSO
o=applications/ou=VISULOX Examples/cn=VLX TTASYS TEST Console
o=applications/ou=VISULOX Examples/cn=VLX VNC CONNECT
```

Top used applications

Top applications of the day

```
visulox report -query topApplication -tframe CURRDAY -raw

vlxapplication;count
o=applications/ou=VISULOX Examples/cn=VLX JUMP SHELL;2
o=applications/cn=gnome terminal (mp-ol6u3-devel);1
o=applications/cn=xterm;1
o=applications/ou=VISULOX Examples/cn=VLX FIREFOX KIOSK (R);1
```

Login failures

Show login failures this month

```
visulox report -query loginFailure -tframe CURRMONTH -raw
```

```
User;Fail login current month
root;1
miller;1
roberts;1
```

Database queries

Recorded films

Size of all files (chapters, snapshots, transferred files)

```
visulox database query -sql "
    SELECT (SUM(postsize) /1024) AS 'Size of all files in the last 7 days (in KB)'
    FROM files WHERE 'createtime' > 'DATE_SUB(CURDATE(),INTERVAL 7 DAY)'
"

Database Query 152ms

    ------------------------------------------------------
    | Size of all files in the last 7 days (in KB)       |
    ------------------------------------------------------
    |                                                524 |
    ------------------------------------------------------
```

Size of film chapters only

```
visulox database query -sql "
    SELECT (SUM(postsize) /1024) AS 'Size of all films in the last 7 days (in KB)'
    FROM files WHERE filetype LIKE 'chapter' AND 'createtime' > 'DATE_SUB(CURDATE(),INTERVAL 7 DAY)'
```

```
"

Database Query 149ms

    ------------------------------------------------
    | Size of all films in the last 7 days (in KB) |
    ------------------------------------------------
    |                                          398 |
    ------------------------------------------------
```

Size of snapshots only

```
visulox database query -sql "
    SELECT (SUM(postsize) /1024) AS 'Size of all snapshots in the last 7 days (in KB)'
    FROM files WHERE filetype LIKE '%-snapshot' AND 'createtime' > 'DATE_SUB(CURDATE(),INTERVAL 7 DAY)'
"

Database Query 148ms

    ------------------------------------------------------
    | Size of all Snapshots in the last 7 days (in KB) |
    ------------------------------------------------------
    |                                               48 |
    ------------------------------------------------------
```

Size of transferred files only

```
visulox database query -sql "
    SELECT (SUM(postsize) /1024) AS 'Size of all transferred files in the last 7 days (in KB)'
    FROM files WHERE filetype LIKE 'file' AND 'createtime' > 'DATE_SUB(CURDATE(),INTERVAL 7 DAY)'
"
```

```
Database Query 153ms

    ------------------------------------------------------------
    | Size of all transferred files in the last 7 days (in KB) |
    ------------------------------------------------------------
    |                                                       77 |
    ------------------------------------------------------------
```

Average chapter size

```
visulox database query -sql "
    SELECT ROUND((AVG(postsize) /1024),2) AS 'Average size of film chapters (in KB)'
    FROM files WHERE filetype LIKE 'chapter'
"

Database Query 149ms

    ----------------------------------------
    | Average size of film chapters (in KB) |
    ----------------------------------------
    |                                199.06 |
    ----------------------------------------
```

Usage

Most used application

```
 visulox database query -sql "select vlxapplication,count(*) AS c from sessions GROUP BY vlxapplication ORDER BY C DESC" -raw

Database Query 107ms
    ------------------------------------------------------------
```

```
    |                                    vlxapplication | c |
    ------------------------------------------------------------
    |                      o=applications/cn=xterm (TEST2) | 1 |
    | o=applications/ou=VISULOX Examples/cn=VLX JUMP SHELL | 1 |
    ------------------------------------------------------------
```

Most active user

```
visulox database query -sql "select vlxowner,count(*) AS c from sessions GROUP BY vlxowner ORDER BY C DESC" -raw

Database Query 76ms
    ----------------------------------------------------
    |                                   vlxowner | c |
    ----------------------------------------------------
    | o=Tarantella System Objects/cn=Administrator | 2 |
    ----------------------------------------------------
Columns: vlxowner c
```

23.1.67 How to disable/modify the presentation of the remote IP address on the login page

On the login page information about the license and the remote IP address is presented.

To **hide** this information one easy step is necessary:

```
visulox config edit -name portal.connection=""
```

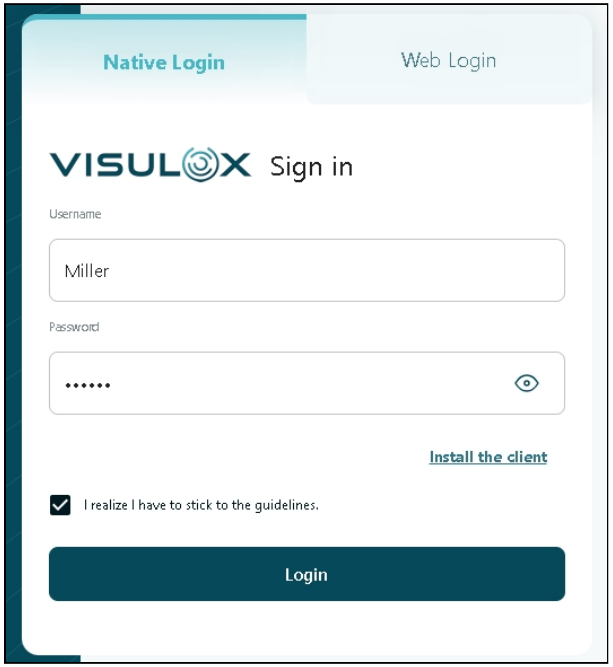
Example for displaying the VISULOX GATEWAY:

```
visulox config -name portal.connection="From %RIP% via GW%GWIPLAST% to %NODE%"
```

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

A standard form contract can be displayed within the login mask of the VISULOX PORTAL.

The contract can be viewed via a link and must be checked before a user is able to log into the VISULOX PORTAL.



Turning the login consent on / off

```
visulox config -name consent.enable=true
visulox config -name consent.enable=false
```

With Access Branding it is possible to display different login page designs for different users according to their access point.
It is possible to overwrite the global consent setting for the different accesspoints:

Example for setting captcha and consent

```
visulox config accesspoint edit -name customera.tbsol.de -consent true
```

Possible values for -consent are: **true** / **false** / **config**
With the value config, the **consent.enable** from the global configuration will be used.

Changing the consent text

```
visulox config edit -name consent.en="<b>I realize</b> I have to <i>stick</i> to the <a href='https://xxx.com'> guidelines.</a>"
```

Formatting the text with stylesheet commands

```
visulox config edit -name consent.style=<css commands>
```

Available languages

```
consent.de
consent.en
consent.es
consent.sv
```

visulox portal attach must be used after changing the values.

23.1.69 Access Branding

About

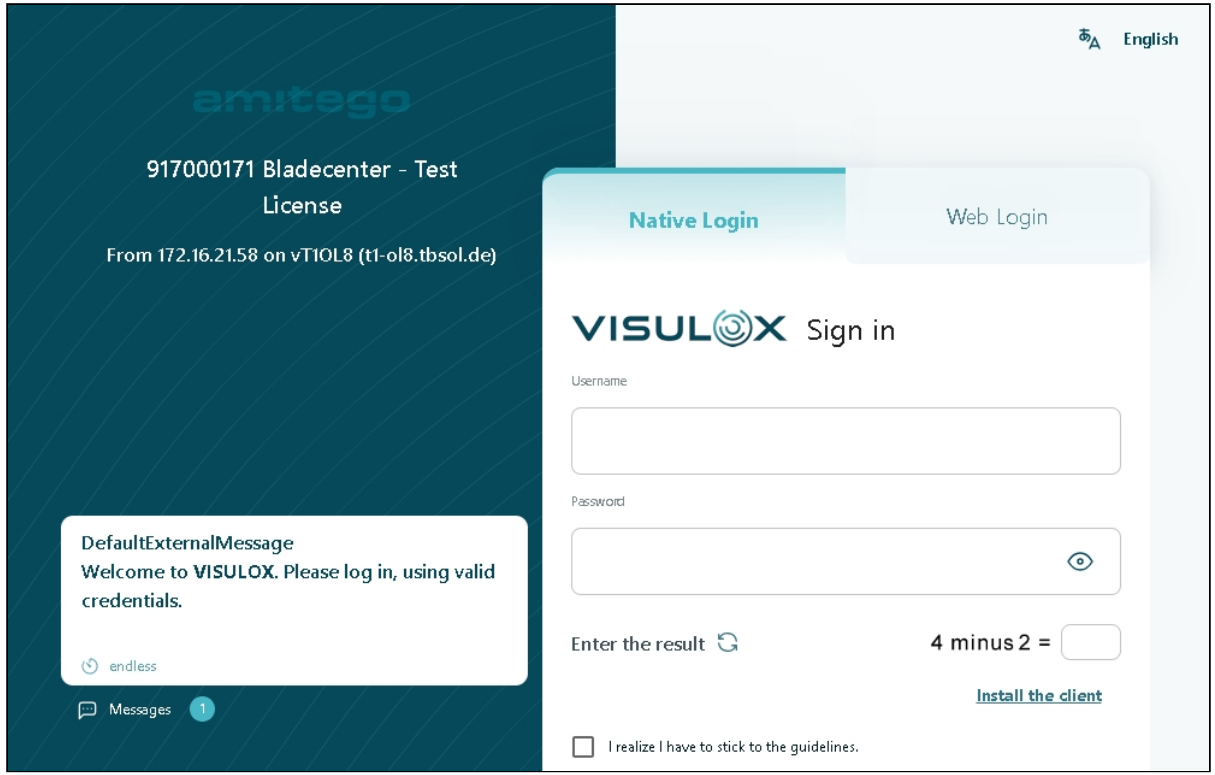
With **default settings** all users get the same design of the VISULOX PORTAL login page (aka landing page),
with the customized logo on the left and the banner / connection information on the right side.

With **Access Branding** it is possible to display different login page designs for
different users according to their access point.

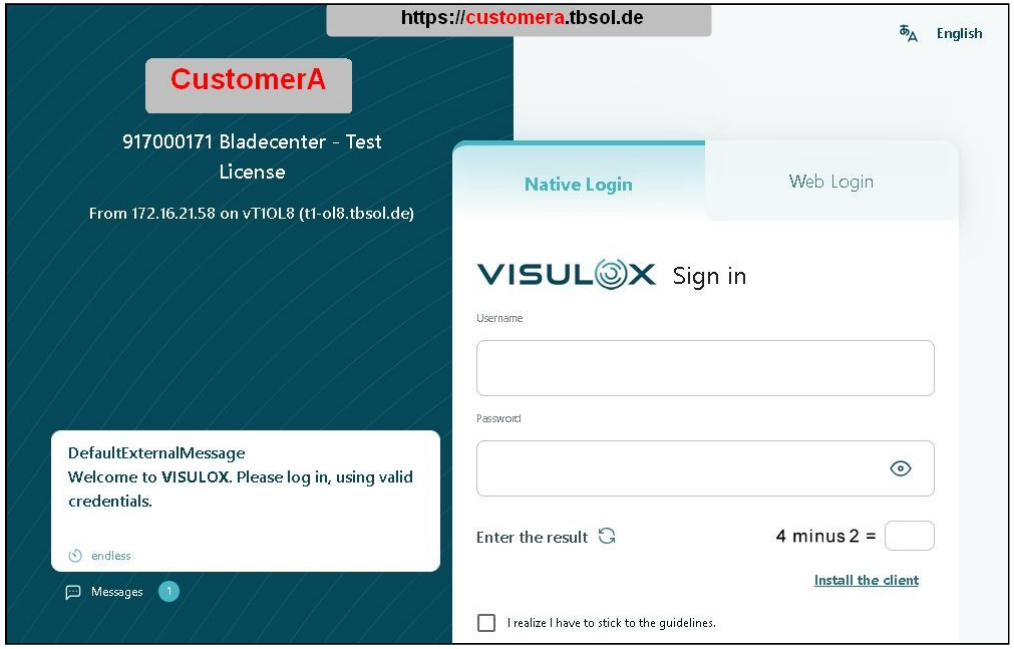
- About
- Implementation
- CLI command
  - Usage
  - Access Branding elements (edit)
  - Placeholders for banner and connection information
  - Command to setup Access Branding
- Workspace
- VISULOX Cockpit
- Related articles

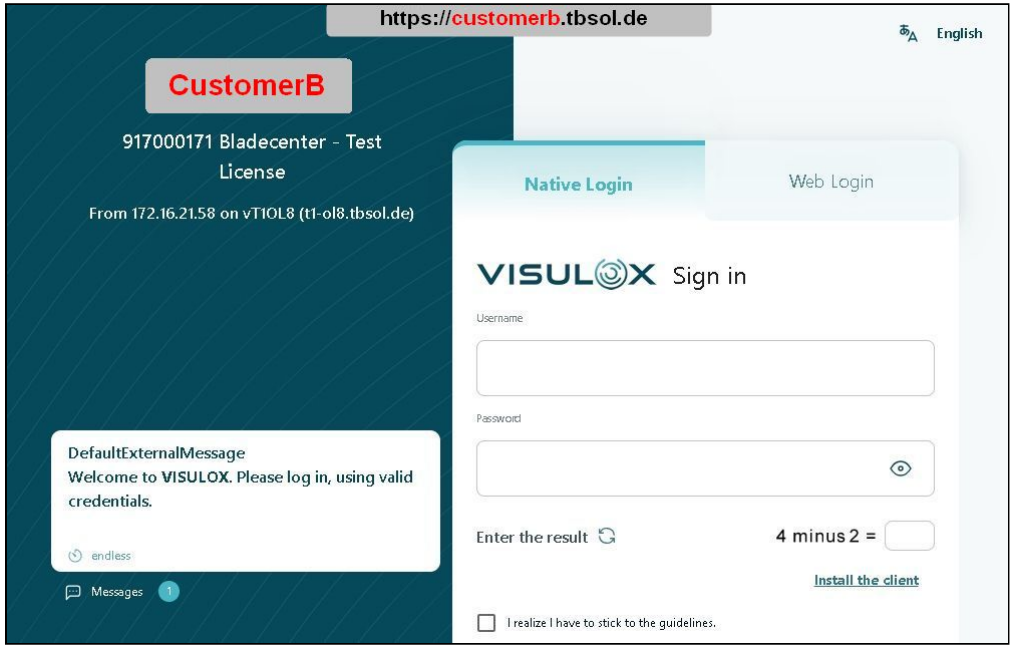
Implementation

Since VISULOX 3.2 the design of the VISULOX PORTAL login page has been reworked completely to get a neutral view.



To achieve the display of different designs on the login page, various access URLs are needed.
In the following example each customer will get his own access URL:

Customer	Access URL
Customer A	

Customer	Access URL
Customer B	
Customer C	https://customerc.<domain>.com (other domains are possible as well).

All this access URLs end on the same IP address. The certificates deposited on the VISULOX Gateways have to be issued again and enhanced with the names of the customers (alternate DNS names).

Command to import new key and certificate

```
visulox-gateway sslkey import --keyfile /tmp/<key>.pem --certfile /tmp/<cert>.crt --cacertfile /<cacert>.crt --keyalg RSA
```

It can be necessary to restart the VISULOX Service after importing new certificates for the VISULOX GATEWAY.

CLI command

Depending on the access URL a dedicated logo and the banner / connection information can be presented individually customized on the login page.

Usage

```
visulox config accesspoint
```

The following subcommands are available:

Command	Description
list	List all Access Brandings
add	Create an Access Branding configuration
edit	Edit an Access Branding configuration
delete	Delete an Access Branding configuration

Access Branding elements (edit)

Element	Description
-name <*value*>	FQDN of the used access point of the users <>

Element	Description
-gatewayip <*value*>	List of Gateway IP or mask - for any, use: "ANY"
-logo <*value*>	File name of logo presented the login page <>
-banner <*value*>	Banner text on the login page <> (placeholders are possible)
-color <*value*>	Main color of design <>
-background <*value*>	Background color of design (lhs loginpage) <>
-connection <*value*>	Connection text on the login page <> (placeholders are possible)
-human <*value*>	Enable/disable/config captcha request on login page <>
-consent <*value*>	Enable/disable/config consent request on login page <>
-clients <*value*>	Enable/disable/config download of clients on login page <>
-entra <*value*>	Enable/disable Entra authentication <>
-pwdlogin <*value*>	Enable/disable PWD authentication <>

Login is not possible if the entered hostname and the used VISULOX Gateway does not match the access point name and the configured Gateway IP.

On VISULOX local Gateways, the gatewayip must be set to "ANY".

Placeholders for banner and connection information

Variable	Description
%SYSTEMID%	Unique system ID
%LICENSE%	License name
%CUSTOMER%	Name of the customer
%HOST%	Hostname
%HOSTSHORT%	Short name of the host
%HOSTIP%	IP of the host
%HOSTIPLAST%	Last IP of the host
%NODE%	Logical name of the node
%RIP%	Remote IP address
%GWIP%	Gateway IP address
%GWIPLAST%	Last Gateway IP address

Variable	Description
%GWHOST%	Gateway hostname
%GWNODE%	Gateway nodename
%AP%	Access Point
%APNODE%	Access Point node

Command to setup Access Branding

Access Branding setup

```
visulox config accesspoint add -name <Access URL> -logo <file of the logos> -banner <text string banner> -connection <text string connection info> -gatewayip <ip>
```

For example:

Examples for customera and customerb

```
visulox config accesspoint add -name customera.tbsol.de -logo "/tmp/custa.png" -banner %LICENSE% -connection "From %RIP% on %NODE% (%HOST%)" -gatewayip 0.0.0.0/0
visulox config accesspoint add -name customerb.tbsol.de -logo "/tmp/custb.png" -banner "Unique System ID: %SYSTEMID%" -connection "Host: %HOST% - Host IP: %HOSTIP%" -gatewayip 192.168.0.123
```

Example for setting captcha and consent

```
visulox config accesspoint edit -name customera.tbsol.de -consent true -human true
visulox config accesspoint edit -name customerb.tbsol.de -consent config -human false
```

Possible values for -consent and -human are: **true** / **false** / **config**

With the value config, the **login.human.check** and/or **consent.enable** from the global configuration will be used.

Check Access Branding entries

```
visulox config accesspoint list -verbose
    ------------------------------------------------------------------------------------------------
    |        accesspoint |                       banner |      logo |                       connection |
    ------------------------------------------------------------------------------------------------
    | customera.tbsol.de |                    %LICENSE% | custa.png |    From %RIP% on %NODE% (%HOST%) |
    | customerb.tbsol.de | Unique System ID: %SYSTEMID% | custb.png | Host: %HOST% - Host IP: %HOSTIP% |
    ------------------------------------------------------------------------------------------------
```

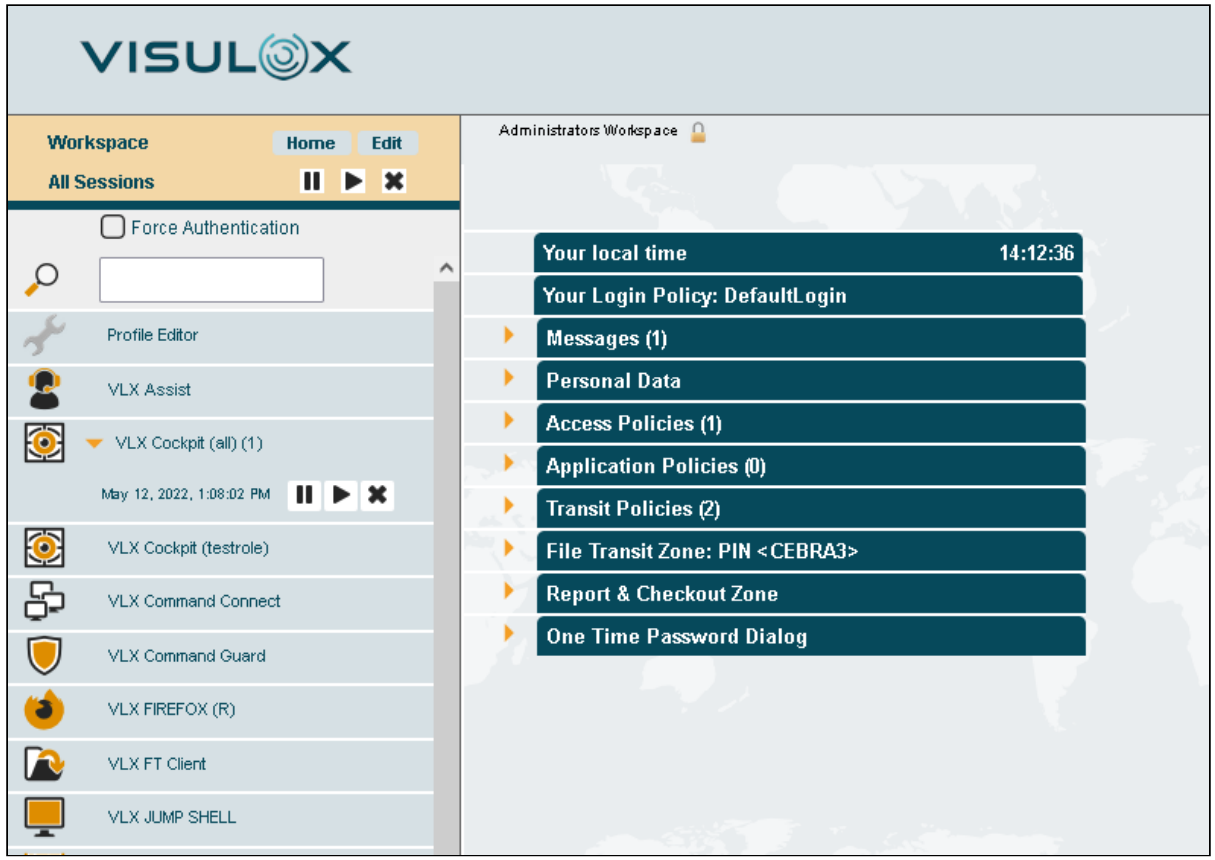
Use portal attach -webtop after changes

```
visulox portal attach -webtop
```

The logo for access branding should not be too small or too large, the format can be a GIF or PNG file and will only be displayed on the login page.

Workspace

After login all users of all customers will still get the same Workspace design.

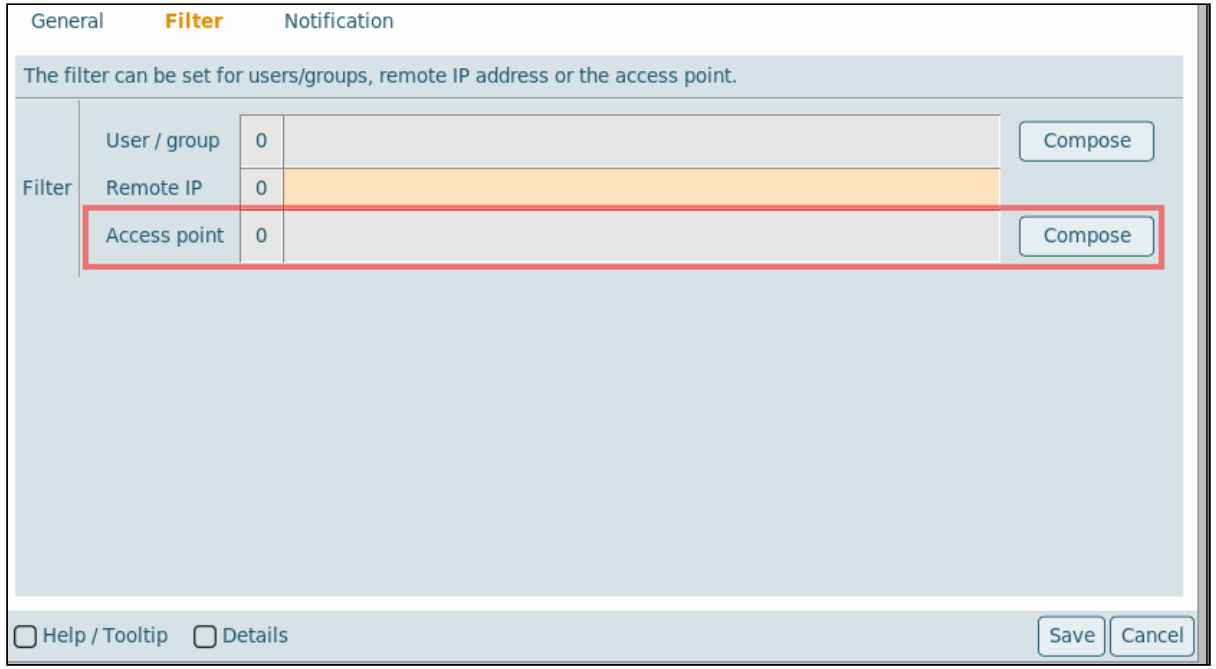


The different logos and the customized banner / connection information are only displayed to the according users on the login page.
In the Workspace, VISULOX Cockpit, etc potentially customized settings will be the same for all users, once logged in.

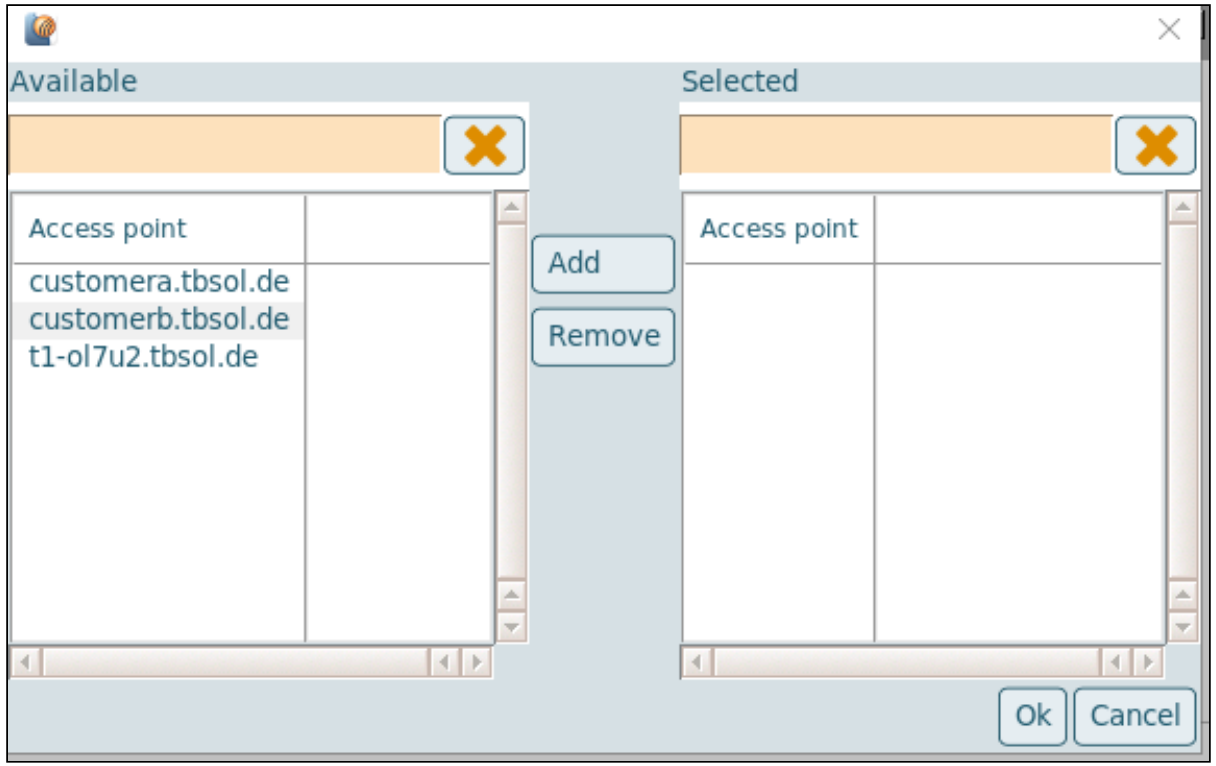
VISULOX Cockpit

VISULOX Administrators with access to the VISULOX Cockpit can use the different access points of the users for the VISULOX Policies as well.

For example: VISULOX Cockpit / Policies / Login Policy / Filter

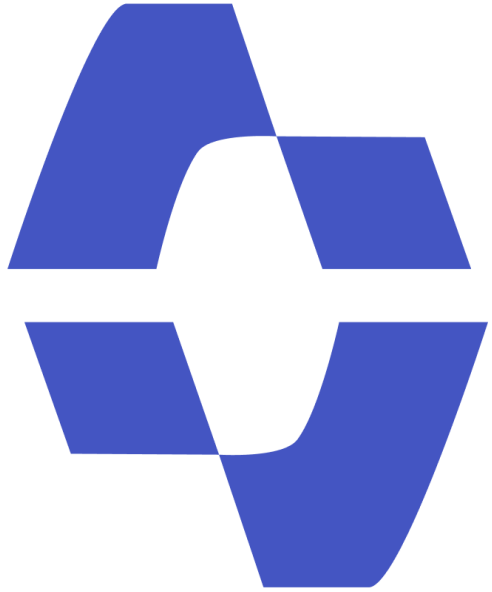


With a click on the **compose** button, a list of the available access points is displayed and can be selected for the filter.



The access point filter is only availble for policies, where access points make sense.

Related articles



(4.2.0) Access Branding
(4.2.0) How to change the VISULOX logos and colors
(4.2.0) How to change the license name / banner
(4.3.2) How to change the VISULOX logos and colors
(4.3.2) Access Branding
(4.3.2) How to change the license name / banner
(4.1.1) Access Branding
(4.1.1) How to change the VISULOX logos and colors
(4.1.1) How to change the license name / banner
(4.3.1) How to change the VISULOX logos and colors
(4.3.1) How to change the license name / banner
(4.3.1) Access Branding
(4.3.0) How to change the VISULOX logos and colors
(4.3.0) Access Branding
(4.3.0) How to change the license name / banner
How to change the license name / banner
Access Branding
How to change the VISULOX logos and colors
How to change the VISULOX logos and colors
Access Branding
How to change the license name / banner

23.1.70 Login page configuration options

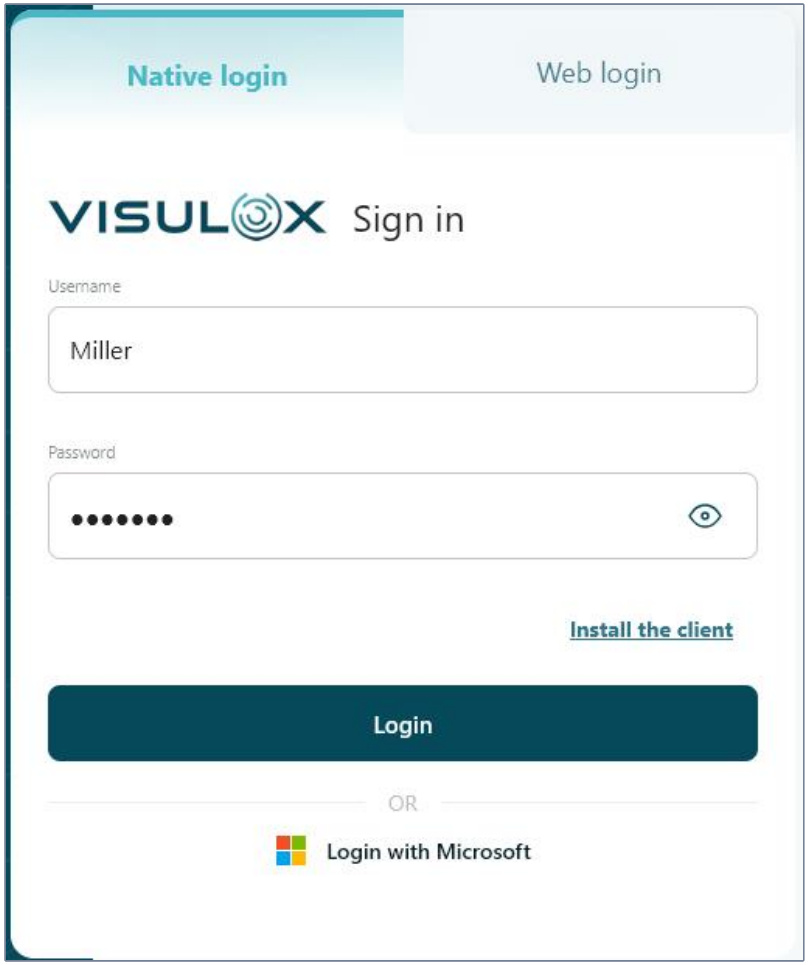
- Authentication
    - Example: Entra enabled / PWD enabled
- Enable captcha
    - Example for setting captcha and consent
- In use check
- Turning the login consent on / off
- Disable install the client option
- Setting the default login method
- Disable external messages
- Setting the language
- Hide PIN
- Login issue wit two detected Remote IP's
- Examples
- Related articles

Authentication

The following authentication methods can be enabled/disabled on the login page:

Example: Entra enabled / PWD enabled

```
visulox config -name portal.entra.enabled=true
visulox config -name portal.pwdlogin.enabled=true
```

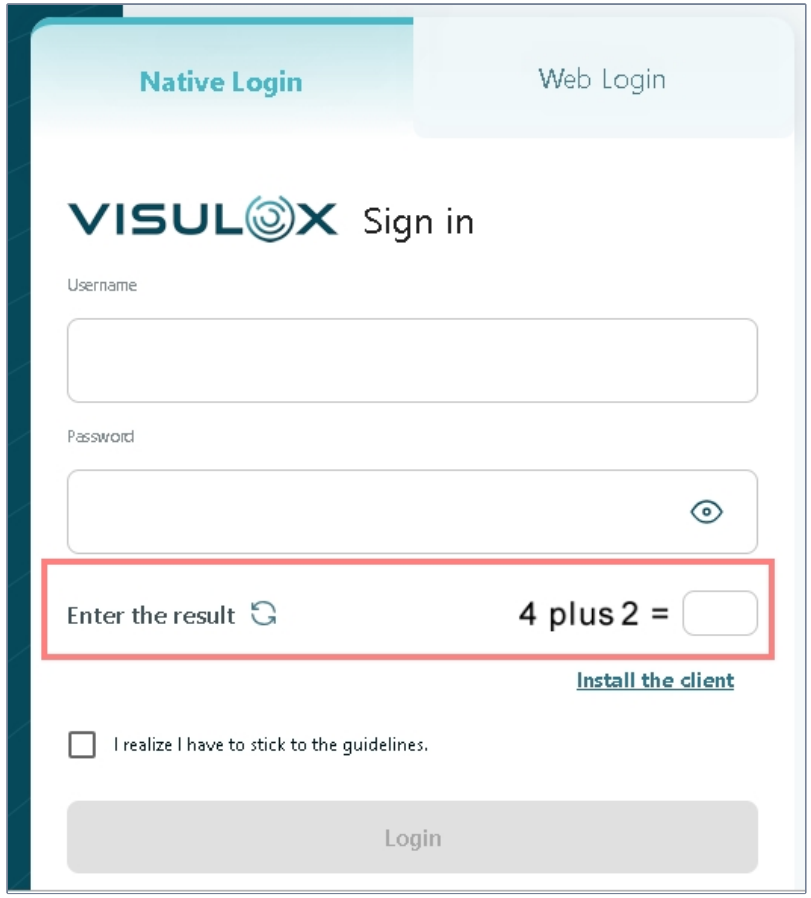

Native login
Web login
VISULOX Sign in
Username
Miller
Password
Install the client
Login
OR
Login with Microsoft

Enable captcha

A captcha can be displayed on the login page, that has to be entered by the user before login:

To enable the human check, use:

```
visulox config -name login.human.check=true
```



With **Access Branding** it is possible to display different login page designs for different users according to their access point.
It is possible to overwrite the global login.human.check setting for the different accesspoints:

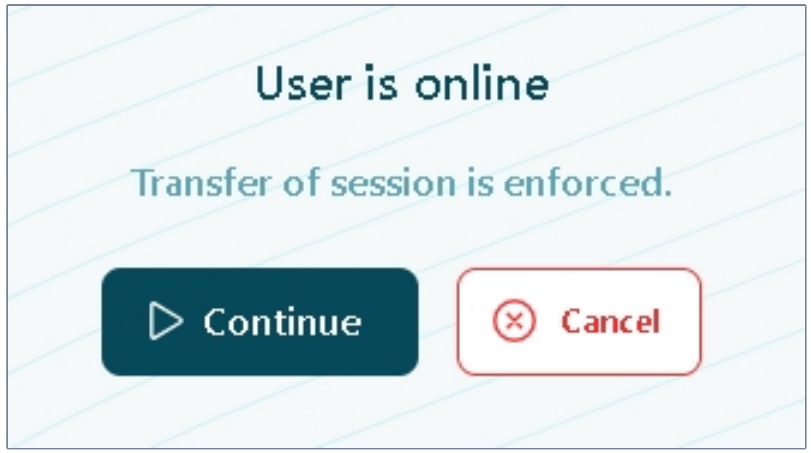
Example for setting captcha and consent

```
visulox config accesspoint edit -name customera.tbsol.de -human true
```

Possible values for -human are: **true** / **false** / **config**
With the value config, the **login.human.check** from the global configuration will be used.

In use check

A message can be displayed, where the user is able to continue and transfer the running session or to cancel the login.



This message is enabled and the according text / tooltip is configured with:

```
visulox config -name loginextend.inusecheck
```

```
-------------------------------------------------------------------------------
| changed | key                              | value                            |
-------------------------------------------------------------------------------
| changed | loginextend.inusecheck           | true                             |
|         | loginextend.inusecheck.comment   | User is online                   |
|         | loginextend.inusecheck.usertip   | Transfer of session is enforced. |
-------------------------------------------------------------------------------
```

Turning the login consent on / off

```
visulox config -name consent.enable=true
visulox config -name consent.enable=false
```

With **Access Branding** it is possible to display different login page designs for different users according to their access point.
It is possible to overwrite the global consent setting for the different accesspoints:

Example for setting captcha and consent

```
visulox config accesspoint edit -name customera.tbsol.de -consent true
```

Possible values for -consent are: **true** / **false** / **config**
With the value config, the **consent.enable** from the global configuration will be used.

Changing the consent text

```
visulox config edit -name consent.en="<b>I realize</b> I have to <i>stick</i> to the <a href='https://xxx.com'> guidelines.</a>"
```

Formatting the text with stylesheet commands

```
visulox config edit -name consent.style=<css commands>
```

Available languages

- `consent.de`
- `consent.en`
- `consent.es`
- `consent.sv`

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

Disable install the client option

```
visulox config -name portal.clients.download=false

    ---------------------------------------------
    | changed | key                     | value |
    ---------------------------------------------
    |         | portal.clients.download | false |
    ---------------------------------------------
```

Setting the default login method

```
visulox config -name portal.clients
    ---------------------------------------------
```

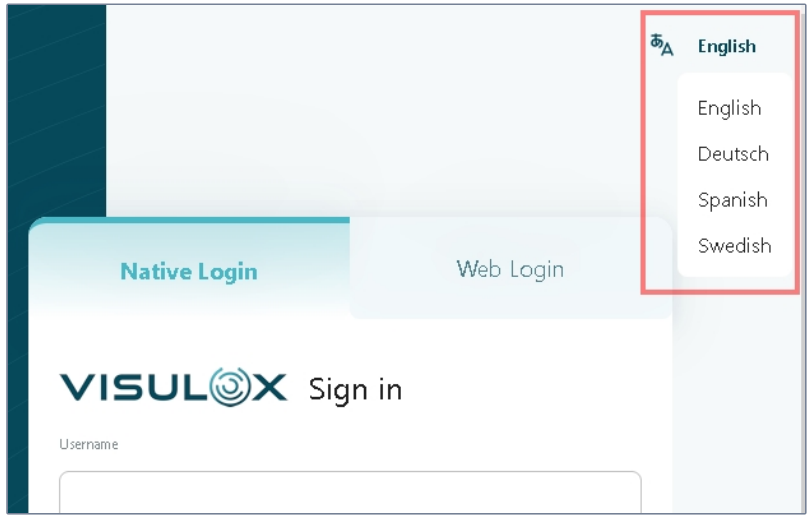
```
| changed | key                          | value   |
-----------------------------------------------
|         | portal.clients               | tcc:hc5 |
...
```

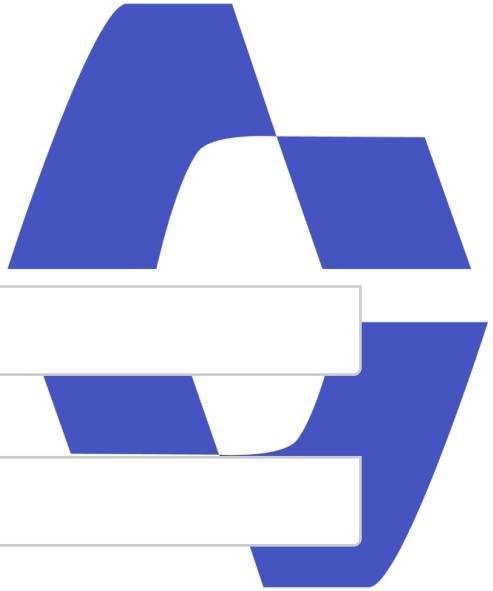
Disable external messages

```
visulox config -name design.ui4.loginmessages=false
```

Setting the language

On the login page, the language used in the VISULOX Portal can be selected:





The displayed languages and can be changed with:

```
visulox config -name portal.language=de:en:es
```

To use the language setting from the client, the following parameter has to be set:

```
visulox config -name portal.language.useclient=true
```

If the client language is not available, english will be used.

Hide PIN

If a second factor has to be entered by the user, the PIN entry can be hidden with:

```
visulox  config -name pin.hide -info
    ------------------------------------------------------------------------------------------------------------
    | changed | key      | value |                                                    shortinfo | defaultvalue |
    ------------------------------------------------------------------------------------------------------------
    |         | pin.hide | false | if true the frontend will hide the entry of the PIN using *  |        false |
    ------------------------------------------------------------------------------------------------------------
```

Login issue wit two detected Remote IP's

In some rare cases the login page may open an empty login page after login.
If there are two Remote IP's shown in the log entries, the following setting is needed:

```
visulox config -name portal.mobile=true
```

Examples

```
visulox config -name loginextend.override.ticketid=true
visulox config -name loginextend.inusecheck=true,loginextend.inusecheck.comment="In use",loginextend.inusecheck.usertip="User
already in use"

visulox config -name extendsession.login.entry1="Ticket<br>(Valid Ticket Number)"
visulox config -name extendsession.login.entry1.usertip="Registered users have to provide a valid ticket number."

visulox config -name extendsession.login.entry2="Phone<br>(Valid Phone Number)"
visulox config -name extendsession.login.entry2.usertip="Users can leave this empty."

visulox config -name extendsession.login.entry3=""

visulox portal attach -jspconf
```

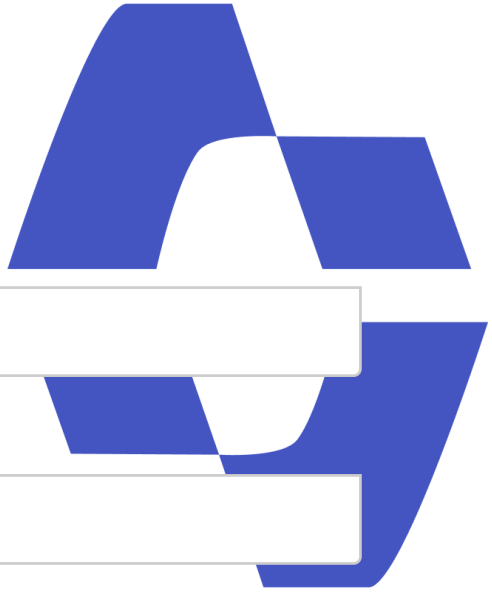
Related articles

How to disable/modify the presentation of the remote IP address on the login page

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

23.1.71 Disable Workspace elements

The following Workspace elements can be disabled:



Access Policy

```
visulox config -name workspace.showAccessPolicy.expand=disable
```

Application Policy

```
visulox config -name workspace.showApplicationPolicy.expand=disable
```

Checkout Zone

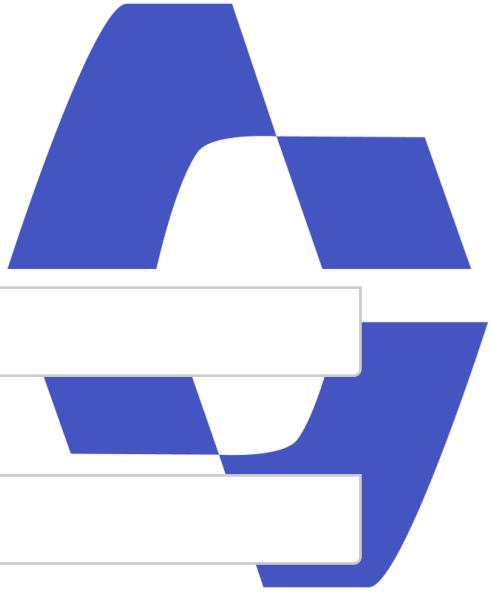
```
visulox config -name workspace.showCheckoutZone.expand=disable
```

Client time

```
visulox config -name workspace.showClientTime.expand=disable
```

Login Policy

```
visulox config -name workspace.showLoginPolicy.expand=disable
```



Messages

```
visulox config -name workspace.showMessages.expand=disable
```

Profile

```
visulox config -name workspace.showPersona.expand=disable
```

Printer

```
visulox config -name workspace.showPrinting.expand=disable
```

Request

```
visulox config -name workspace.showRequestZone.expand=disable
```

Disabling / enabling Request needs a logout and login again.

Transit Policy

```
visulox config -name workspace.showTransitPolicy.expand=disable
```

Transit Zone

```
visulox config -name workspace.showTransitZone.expand=disable
```

OTP setup

```
visulox config -name otp.setupmode=disabled
```

23.1.72 How to disable indexing by search engines

To prevent Google and other search engines of indexing Gateway / portal. the **robots.txt** on the server has to be adjusted or created.

```
   /opt/tarantella/webserver/apache/2.2.25_openssl-1.0.0k_jk1.2.37/htdocs/robots.txt
```

With the following setting, the site will be excluded from indexing:

```
# Exclude site from all robots
User-agent: *
Disallow: /
```

See also: http://www.bjoernsworld.de/suchmaschinen/robots-txt.html

23.1.73 Command "visulox log" - Analyzing log files

Overview

Log files can grow, log files are in different places, log files contain previous errors.

Therefore VISULOX log entries are provided via **systemd / journalctl**.

The "**visulox log**" command allows to get all VISULOX related information in one place.

- Overview
- Usage
- For example

Usage

```
./visulox log <options>
```

The default behaviour is analyzing from last VISULOX service restart.

Option	Description
-S | --since	Start date / time for logging If **-S** is used without the **-U** parameter: **-<*int*>** seconds, minutes, hours, days, weeks, months, or years
-U | --until	End date / time for logging
-l | --loglevel	Loglevel: error, notice, info, debug (Default: **info**). This setting depends on the configured global logger.level setting (Default: **error**).

Option	Description
-f | --follow	Tailing log information on stdout
-t | --identifier	Show entries with the specified syslog identifier, e.g. transitzone, webservice, ... As root, use "journalctl SYSLOG_IDENTIFIER=" & press "*TAB*" to display a list o f all identifiers.

For example

The default setting of the system logger is **error**. To display debug information within the **visulox log** command, the logger has to be set to **debug**.

Setting the logger to debug

```
visulox config -name logger.level
    ----------------------------------------
    | changed | key              | value    |
    ----------------------------------------
    |         | logger.level     | error    |
    ----------------------------------------


visulox config -name logger.level=debug
```

Show log entries on stdout

```
 visulox log -loglevel debug -follow
```

If log level of the system has not been set to debug, the visulox log command can not display debug information regardless of -loglevel setting.

Show error log entries for a given timeframe

```
visuloxlog-S "-10 minutes" -loglevel error
```

```
visulox log -S "-2 days" -loglevel error
```

```
 visulox log -since "08:00" -until "12:00" -loglevel debug
```

```
 visulox log -S "Tue Jul 12 10:00:15 CEST 2022" -until "Fri Jul 15 10:42:15 CEST 2022" -loglevel error
```

Format of log entries (examples)

Date / Time	Node	Loglevel	Process	Log entry information
2022-07-27 10:21:06.951562	vT2OL7U2	debug	stats.tcl(12146)	::dataChanged tables=<global_vlxconfig>
2022-07-27 10:23:33.878061	vT2OL7U2	debug	stats.tcl(12146)	<::coroutine::util::C772>::LicenseCount::create e=<No DataDict from dict>
2022-07-27 10:27:56.987730	vT2OL7U2	info	objects2Portal.tcl(14374)	<::coroutine::util::C27>::AdminsToDatastore::runSingle e=<no datasources found,terminating secure Global Desktop>
...				

If more detailed logs are needed, this can be done with journal.ctl commands directly.
In this case, please contact the VISULOX Support Team for more information.

23.1.74 VISULOX disk space protection

- Overview
- Usage
- Configuration

Overview

During operation the disk space is growing and if there is no platform monitoring configured, this will end in uncontrolled situations.

The VISULOX disk space protection detects low disk space and a warning will be displayed. Once a critical value is reached, the service will be shutdown.

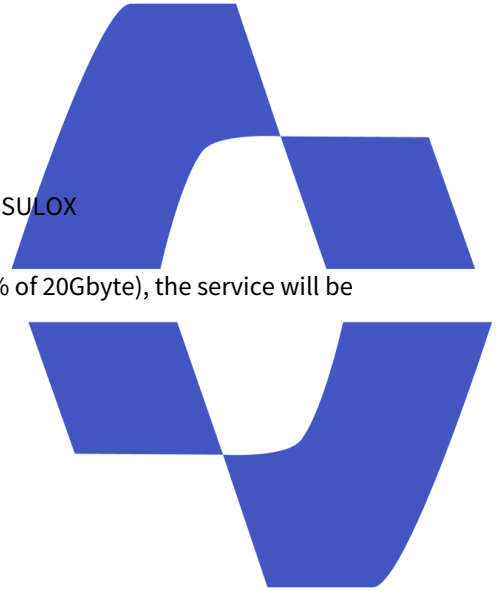
An entry is written into the log. Integrity-Check is also checking the disk quotas, independent of enabled or disabled disk space protection.

Usage

The default configuration is:

```
-------------------------------------------
| changed | key                   | value  |
-------------------------------------------
|         | diskprotect.base      | 2.0GB  |
|         | diskprotect.data      | 20.0GB |
|         | diskprotect.filestore | 50.0GB |
| changed | diskprotect.shutdown  | false  |
|         | diskprotect.threshold | 50     |
|         | diskprotect.var       | 5.0GB  |
-------------------------------------------
```

Disk space protection is on (diskprotect.shutdown=1). For the base path of VISULOX a minimum of 2Gbyte is needed, for var 5Gbyte and for the data 20Gbyte.



The threshold represents a value in percent. If the requested disk space is less than this perentage, the disk protection service will shutdown VISULOX (diskprotect.shutdown=1).

Data needs at least 20Gbyte. If this space is not available, a warning is displayed in the VISULOX Cockpit. If space for the data is at 10Gbyte (50% of 20Gbyte), the service will be shutdown.

- Base : /opt/visulox
- Data: /opt/visulox/data
- Filestore: /opt/visulox/data/filestore/... (each single slot / disk)
- Var: /opt/visulox/var

Configuration

Disabling the disk protection

```
visulox config edit -name diskprotect.shutdown=0
```

Data must have at least 100Gbyte free

```
visulox config edit -name diskprotect.data=100Gbyte
```

Changing these parameters will take effect immediately.

The Disk Protection parameters are global parameters and will be set for all nodes in the cluster.
If one node is shutdown, because of low disk space, no more sessions will be distributed to this node.

23.1.75 VISULOX addon command line interface (CMD Connect / Guard, etc)

Overview

The VISULOX addons are Command Connect, Command Guard and FT Client. These addons have assigned hosts and scripts.

The VISULOX addon command line interface allows to create entries for Command Connnect, Command Guard, FT Client, hosts and scripts.

- Overview
- Usage
- Assignments
- Configuration
- Known issues and comments
- Related Information

Usage

The primary command is:

```
visulox addon <subcommand> <subcommand> <options>
```

The addon has subcommands:

```
   cmdconnect           Handle cmdconnect
   cmdguard             Handle cmdguard
   export               Handle export
   ftclient             Handle ftclient
   host                 Handle host
   privathost           Handle privathost
   purge                Handle purge
   script               Handle script
   template             Handle template
```

Each subcommand has additional subcommands:

```
visulox addon (cmdconnect|cmdguard|export|ftclient|host|privathost|purge|script|template) (list|add|edit|delete|export|import|
fields)
visulox addon template (host|guard)
```

The options are related to usage:

```
visulox addon <subcommand> <subcomand> -?
```

Available fields in the database can be displayed with:

```
visulox addon cmdconnect fields
visulox addon cmdconnect fields -raw
```

Assigned hosts for Command Connect:

```
visulox addon cmdconnect listhosts
```

Assigned private hosts for Command Connect:

```
visulox addon cmdconnect listprivatehosts
```

Assigned scripts for Command Guard:

```
visulox addon cmdguard listscripts
```

Export into a script:

```
visulox addon export
visulox addon privathost export
```

Available options:

Option	Description
-grant <*value*>	Add -grant <*value*> in import script
-addcomment <*value*>	Add an import comment <>
-overwrite <*value*>	Add -force to import script

- **visulox addon export** to export all data into a script
- **visulox addon <*segment*> export** to export a single segment into a script, e.g. privathost

For importing this data, the same users must be available on the system.

Assignments

The subcommand cmdconnect and ftclient need assigned endpoints (hosts), additionally the server side scripts to cmdguard.

The assignment is a list of endpoints / scripts. The assignment is not done additional, it is done fully. Already assigned elements are removed if they are not on the request.

Create a Group with two servers

```
visulox addon host add -name "server1" -endpoint sysadm@server1 -mode on -comment "ADMIN SERVER1"
visulox addon host add -name "server2" -endpoint sysadm@server2 -mode on -comment "ADMIN SERVER2"
visulox addon cmdconnect add -name adminServer -mode on -comment "group of admin Server" \
        -hosts server1,server2
```

Configuration

For Command Connect and Command Guard, the user can add private hosts, if hostrules are provided. Command Guard needs also the guardrules. These rules can be applied by the command line.

```
visulox addon cmdconnect edit -name adminServer -hostrules <path to defintion>
visulox addon cmdguard edit -name adminServer -hostrules <path to defintion> -guardrules <path to defintion>
```

```
visulox addon template hosts|guard provides a template for these configuration files
```

List of available Command Connect / Guard parameters

Parameter	Description
-name <*value*>	Name of this definition <>
-comment <*value*>	Comment for this definition <>
-mode <*value*>	Enable/disable the definition <*on*>
-color <*value*>	Frame color for all session within this definition <*white*>
-term <*value*>	TERM to shell <>
-resource <*value*>	Resource in passcache <> If an owner is set for the ressource, the owner must be set also for Command Connect in the ressorce name field: **<ressource-name>%OWNER%**
-sshkeymask <*value*>	Filtermask for SSH-keys provided in the sessions <>
-hostrules <*value*>	File with rules to set private hosts <> Rules that can be set: rulemode, rulematchtype, userexpr, hostexpr, protocol, port
-ftmode <*value*>	File Transfer with Command Guard <*on*>
-object <*value*>	User/group filter allowed to use this definition <>

Parameter	Description
-remoteip <*value*>	Remote IP from where this definition can be used <>
-accesspoint <*value*>	Access Point over which this definition can be used <>
-hosts <*value*>	List of hosts assigned to this definition <>
-grant <*value*>	Set granted user in database record <>

Known issues and comments

Any option except **-script <path>**, **-hostrules <path>** and **-guardrules <path>** can be provided via stdin from a remote host.

Related Information

- General command line configuration
- How to control FT Client from the command line
- How to control script objects from the command line
- How to control host objects from the command line
- VISULOX Command Line Interface (CLI)

23.1.76 Host Control (Command Connect / Guard)

Host Connect, consist of two applications named **Command Connect** and **Command Guard** that provide a more flexible way to
access endpoints using a shell interface. Command Connect and Command Guard handle flexible groups and allows the user to send commands to multiple endpoints simultaneously.

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

Remaining faithful to the whole VISULOX concept, no agents are needed on the endpoints to achieve this.

- Overview
  - Command Connect / Guard features
- Command Connect / Guard GUI
  - Unmanaged sessions (CMD Connect only)
  - Temporary hosts group
  - Own hosts
- File Transfer
- Configuration parameters
- Related information

Overview

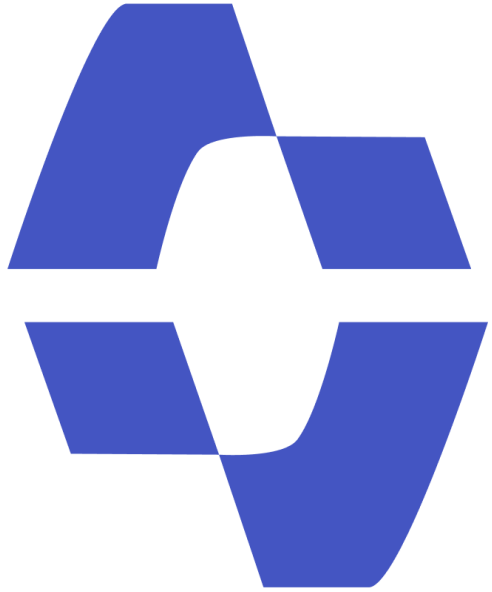
VISULOX Command Connect / Guard is a multi functional shell connect client.

Command Connect / Guard has a list of groups containing several host objects, the user can connect to. The connection method can be Telnet, SSH or SSH Keys.

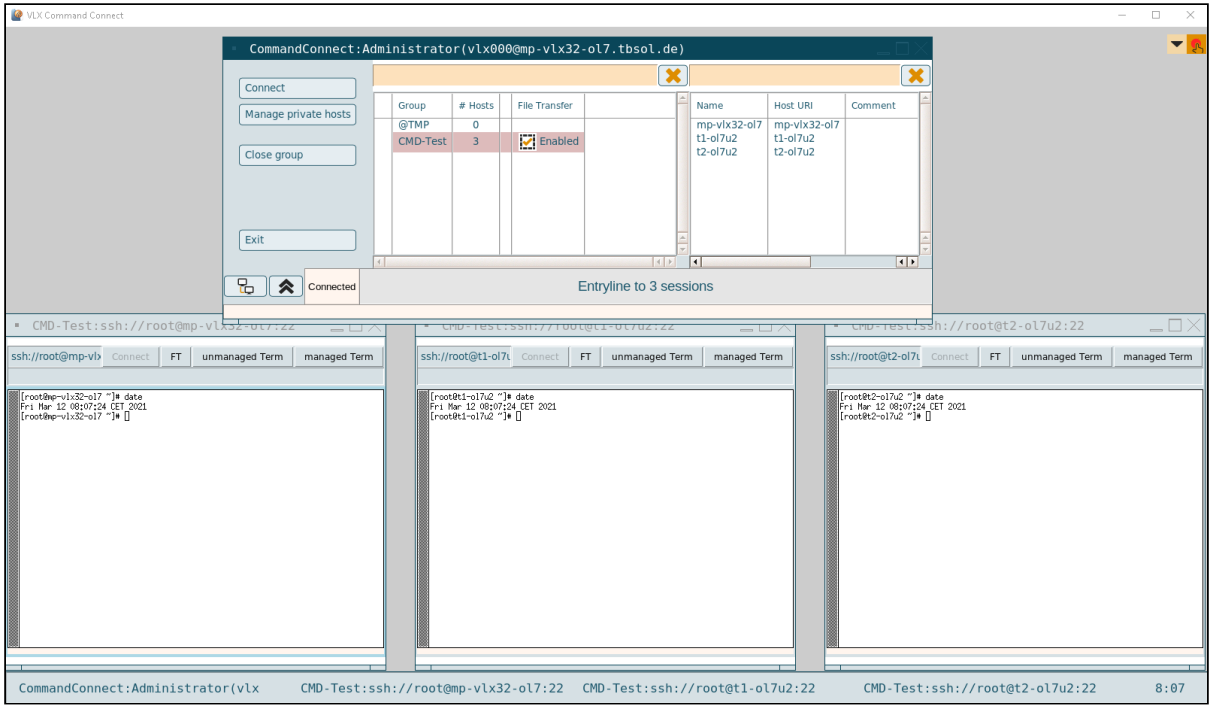
The connection port is configurable via the Host Object addon.

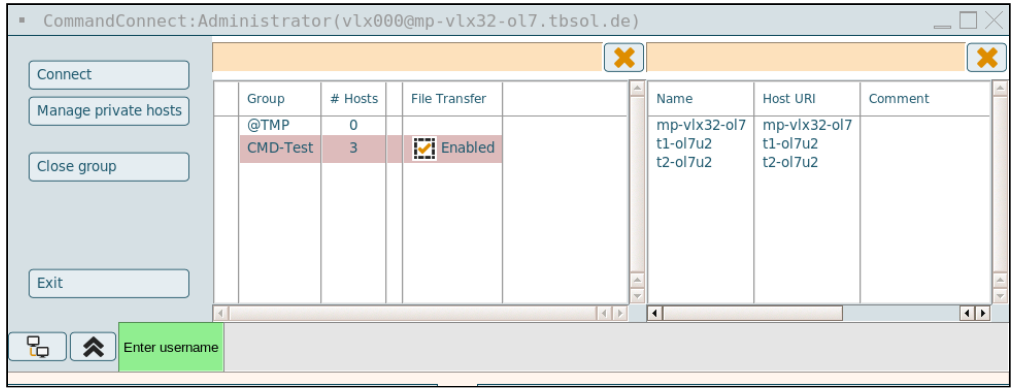
Command Connect / Guard features

- Multiple groups
- Multiple endpoints per group
- Colorized grouping of hosts
- Auto arrange of the connection windows
- Single entry line for selected hosts or a host group
- Black and white command list (CMD Guard only)



- File Transfer to the hosts can be enabled
- User can add hosts by himself (depending on rules)
- Assigned hosts can be combined in a temporary group
- Scripts can be assigned for Command Guard (server-side) (CMD Guard only)
- Additional managed and unmanaged sessions can be started (CMD Connect only)
- Client side SSH Key handling


VLX Command Connect
CommandConnect:Administrator(vlx000@mp-vlx32-ol7.tbsol.de)
Connect
Manage private hosts
Close group
Exit
Group
Hosts
File Transfer
@TMP
0
CMD-Test
3
Enabled
Name
Host URI
Comment
mp-vlx32-ol7
t1-ol7u2
t2-ol7u2
Connected
Entryline to 3 sessions
CMD-Test:ssh://root@t2-ol7u2:22
unmanaged Term
managed Term
CommandConnect:Administrator(vlx
CMD-Test:ssh://root@mp-vlx32-ol7:22
CMD-Test:ssh://root@t1-ol7u2:22
CMD-Test:ssh://root@t2-ol7u2:22
8:07



- **Connect:** Opens a shell to all hosts in the selected group
- **Manage private hosts:** A user can manage his own hosts
- **Close group:** All sessions of the selected group will be closed
- **Exit:** Command Connect / Guard application and all open sessions are closed
- **Arrange:** Connected session windows will be rearranged based on the first window marked with the colored frame
- **Collapse:** Collapse Command Connect / Guard Console
- **Scripts:** Shows all available scripts for this group, a selected script can be applied on all open shells (CMD Guard only). (See also: Script objects)

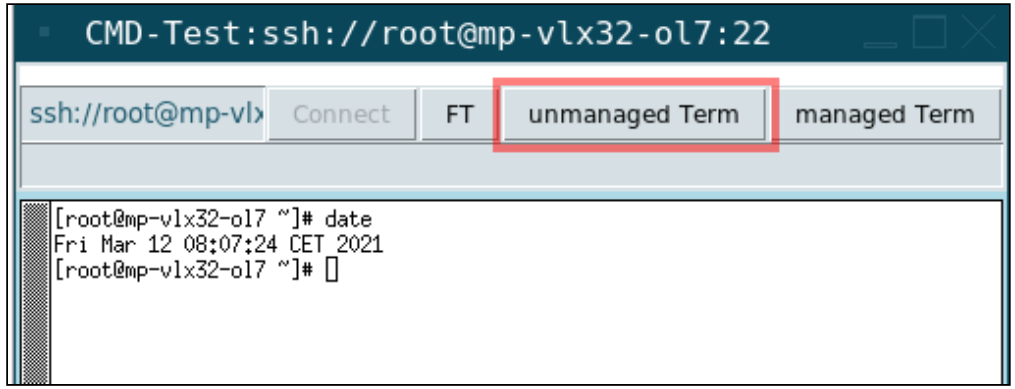
To send a command to all connected shells, the input field of the Command Connect / Guard application can be used: The status of the connected terminals is also shown.

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

Unmanaged sessions (CMD Connect only)

In Command Connect the user has a managed session per host assigned to his Command Connect groups. Additionally the user can open one or more extra managed and unmanaged sessions to this host via the "**unmanaged Term**" and the "**managed Term**" button.

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



Temporary hosts group

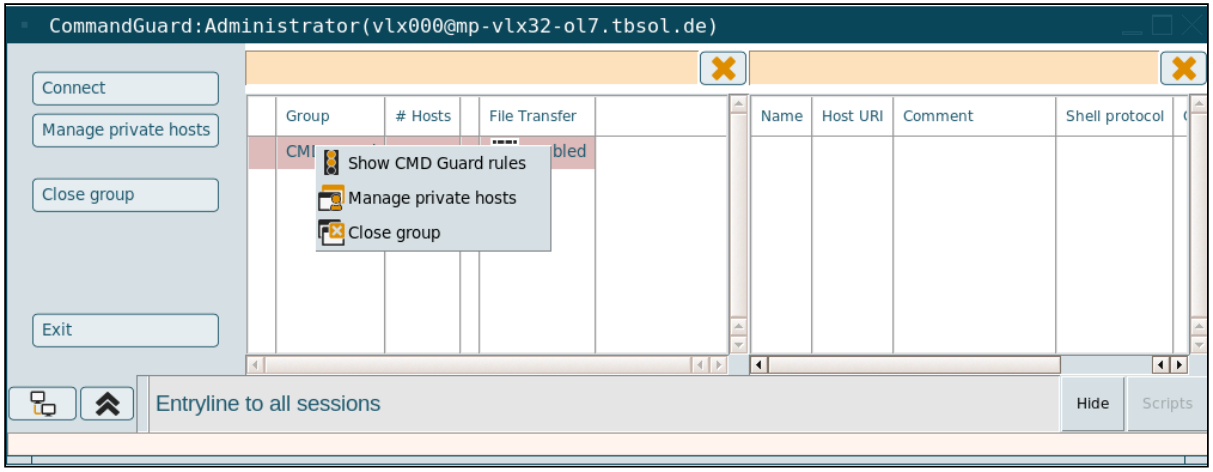
With a right click on an assigned host, the host can be added to a temporary group (@TMP).

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

Own hosts

Command Connect / Guard has the ability, that a user can manage his own hosts.

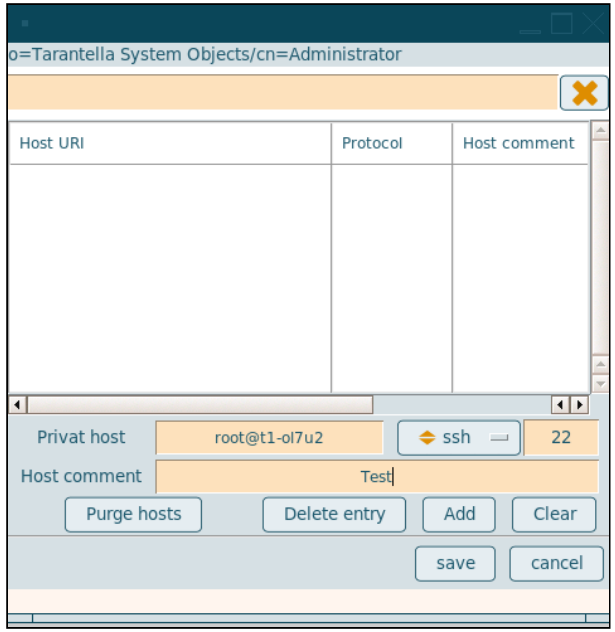
To keep this under control, the admin has to define a ruleset, what kind of hosts a user can add. The ruleset is part of the Command Connect / Guard group.



With a right click on a group in Command Connect / Guard, the user can view the Guard rules (Guard only), manage own private hosts (depending on the rules) or close the group.

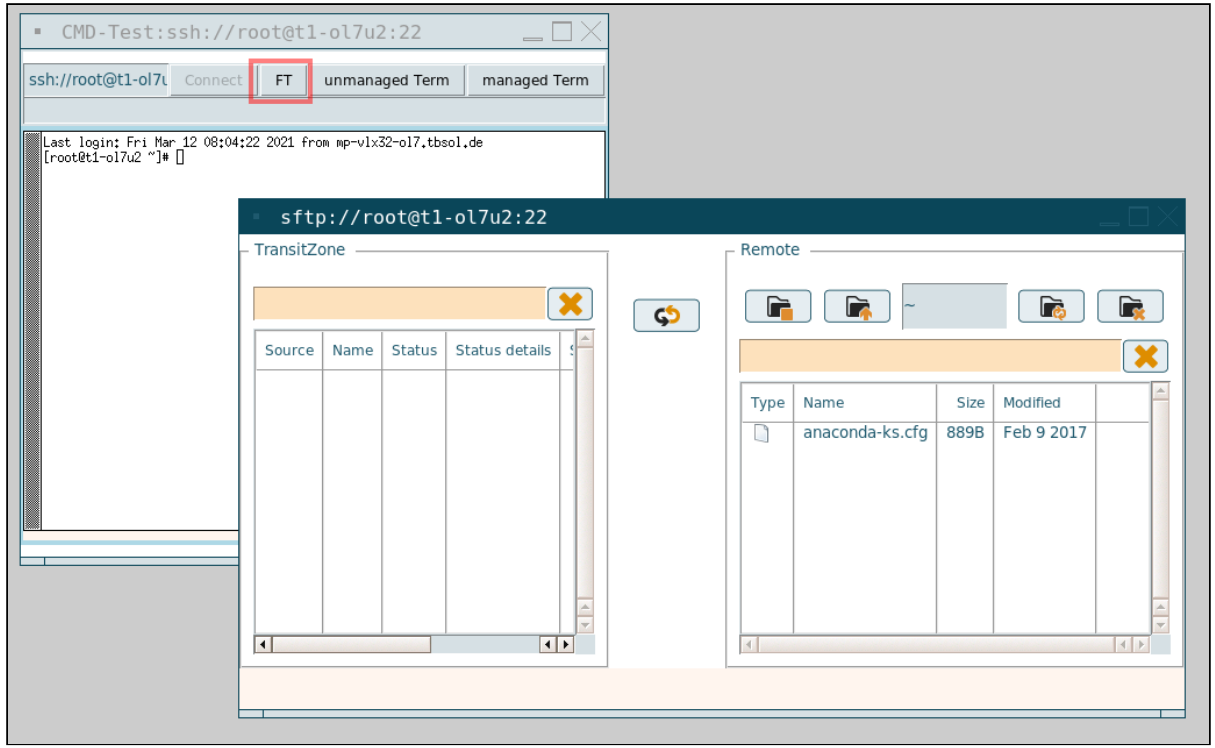
The private hosts are based on rules, the user is a string and the host is a string or an IP address.

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



File Transfer

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



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

> ⚠ For File Transfer within Command Connect MaxSessions in sshd_config on the destination server has to be set at least to 2. With a MaxSession setting of 1 only the FT Client can be used without Command Connect.

⚠ Take care, when allowing File Transfer to application servers - scripts can be uploaded, which contain commands, that are not wanted.

Configuration parameters

Application	Application command	Login script
Command Connect	vlxcmdconnect	visulox.exp
Command Guard	vlxcmdguard	visulox.exp

The following parameters can be used with Command Connect / Guard:

Parameter	Description
-title <*value*>	Application title <> (Placeholders are possible[1])
-groups <*value*>	Comma seperated list of groups <>
-lang <*value*>	Language <>
-scripts <*value*>	Path to scripts <>
-cdm	CDM: mount client drives in home directory for scripts and SSH-keys

Parameter	Description
-guard	Enable to use Command Guard
-sshkeymask <*value*>	SSH-key: mask to select SSH-keyfiles %HOST%, %USER%, %LOGINUSER%,%LOGINUSERID%,%OWNERID%,%GROUP%
-sshoptions <*value*>	SSH: extra options (like -X,-Y). See documentation for more
-termoptions <*value*>	TERM: extra options (like: -termoptions "-fn: 10x20"), more examples[2]
-resource <*value*>	Name of passcache resource
-files <*value*>	Comma seperated list of definition files <>
-hosts <*value*>	Comma seperated list of hosts <>, e.g. ssh://user@host
-autoconnect	Auto connect, if there is only one host
-ftoff	Disable usage of FT Client in Term
-cmoff	Disable usage of Control Master
-prompt <*value*>	Regexpression for prompt detection. Default: <^.+\$ |^.+#>
-arranging <*value*>	Arrangment mode (classic,on,off,fixon,fixoff). Default: <classic> (With fixon/fixoff the user is not able to change the mode.)

Parameter	Description
-iconify <*value*>	Iconfy mode (classic,on,off,fixon,fixoff). Default: <classic> (With fixon/fixoff the user is not able to change the mode.)
-sshpassprompt <*value*>	Override default sshpass password prompt. See: "man sshpass -P"
-doubleclickoff	Disable double click action on host group selection

[1] Placeholders for the title can also be set with the configuration parameter: **guidefaults.title**

[2] More examples for the -termoptions parameter: "-fg <color>", "-bg <color>", "-leftbar", "-rightbar", "-title", "-/+fullscreen", etc

Command Connect / Guard can be controlled from the command line or the database.
If no option is set, the groups are assigned by the database definition. See also: Command Connect / Guard and FT Client with empty filters

Command Connect / Guard support **-hosts** / **-files** / **-groups**. Each parameter is a comma separated list.

If one is set, the groups are not taken from the database.

- **-hosts** allows to specify a list of hosts. A single group is generated named **CLI**
- **-files** allows to read groups and hosts from a file. The file must be readable by **vlxgroup** on all VISULOX Access Nodes.
  If the files are not found, they will be searched in the directory assigned via **general.hostfileslookuppath**.
  File example:

```
[Access external:light_slate_gray]
root@GW1/Gateway1
root@GW2/Gateway2
root@GW3/Gateway3

[Access internal:light_slate_blue]
root@portal1:22/portal1
```

```
root@portal2:23/portal2
root@portal3:22/portal3
```

As long as no [...] defines the group name, the name of the group will be the name of the file. Custom **ports** can be declared with "**:**" and **comments** can be added with "**/**".

- **-groups** requests the group and assigned hosts from the database.

With **-autoconnect** always the first group will be activated. If there is only one group with one host and **-autoconnect** is set, the panel will be hidden and if the window is closed, vlxcmdconnec will be closed as well.
For Command Connect the command input line is also disabled.

With **-ftoff** the FT Client can be disabled.

Command Connect / Guard / FT Client use the Control Master. Some ILO SSH implementations can not handle Control Master sessions.
Therefore Command Connect / Guard can be used without Control Master with the parameter **-cmoff** set (if this is the case, **-prompt** can be adjusted if necessary)**.**

If needed "**cmoff**" can be implemented also into the Command Connect / Guard objects (not for FT Client) as a database field on customer request.
The current implementation is done to allow access to ILOs. Four sessions per host connection are allowed with Control Master.
With **-sshpassprompt** an alternate ssh password prompt can be set.

Command line parameter **-X** is needed to allow X11 forwarding, if Command Connect / Guard is started with command line parameters.

Related information

(4.1.1) Additional events for Command Connect / Guard

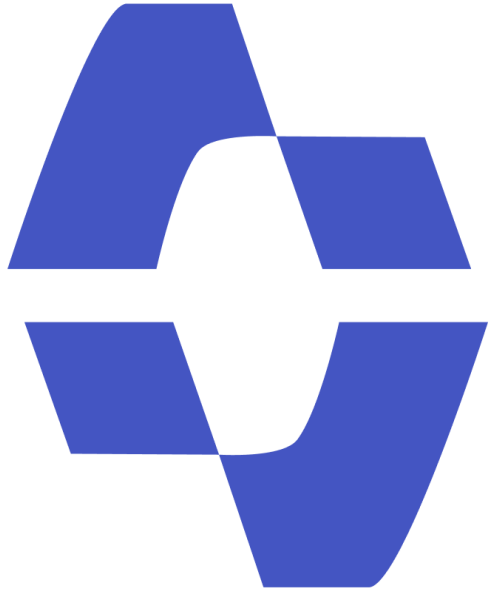
(4.1.1) Command Connect / Guard and FT Client with empty filters

(4.1.1) Configuration of Host Control in the VISULOX Cockpit

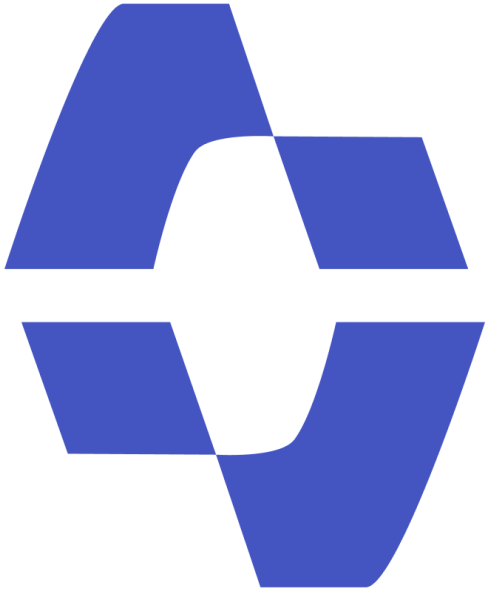
(4.1.1) Host Control (Command Connect / Guard)

(4.1.1) Host objects

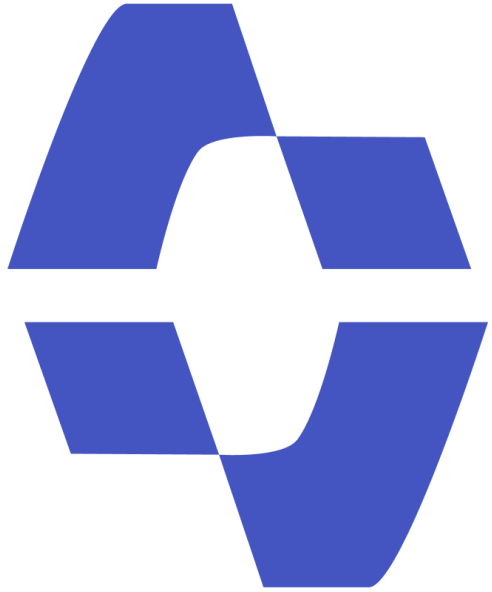
(4.1.1) How to control host objects from the command line



(4.1.1) How to control script objects from the command line
(4.1.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.1.1) Private host tool
(4.1.1) Script objects
(4.1.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.2.0) Command Connect / Guard and FT Client with empty filters
(4.2.0) Configuration of Host Control in the VISULOX Cockpit
(4.2.0) Host Control (Command Connect / Guard)
(4.2.0) Host objects
(4.2.0) How to control host objects from the command line
(4.2.0) How to control script objects from the command line
(4.2.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.2.0) Private host tool
(4.2.0) Script objects
(4.2.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.0) Command Connect / Guard and FT Client with empty filters
(4.3.0) Configuration of Host Control in the VISULOX Cockpit
(4.3.0) Host Control (Command Connect / Guard)
(4.3.0) Host objects
(4.3.0) How to control host objects from the command line
(4.3.0) How to control script objects from the command line
(4.3.0) How to use SSH-Keys within Command Connect / Guard and FT Client



(4.3.0) Private host tool
(4.3.0) Script objects
(4.3.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.1) Additional events for Command Connect / Guard
(4.3.1) Command Connect / Guard - X11 statement
(4.3.1) Command Connect / Guard and FT Client with empty filters
(4.3.1) Command Guard limitations
(4.3.1) Configuration of Host Control in the VISULOX Cockpit
(4.3.1) Host Control (Command Connect / Guard)
(4.3.1) Host objects
(4.3.1) How to control host objects from the command line
(4.3.1) How to control script objects from the command line
(4.3.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.1) Private host tool
(4.3.1) Script objects
(4.3.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.2) Additional events for Command Connect / Guard
(4.3.2) Command Connect / Guard - X11 statement
(4.3.2) Command Connect / Guard and FT Client with empty filters
(4.3.2) Command Guard limitations
(4.3.2) Configuration of Host Control in the VISULOX Cockpit
(4.3.2) Host Control (Command Connect / Guard)



(4.3.2) Host objects
(4.3.2) How to control host objects from the command line
(4.3.2) How to control script objects from the command line
(4.3.2) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.2) Private host tool
(4.3.2) Script objects
(4.3.2) VISULOX addon command line interface (CMD Connect / Guard, etc)
Additional events for Command Connect / Guard
Command Connect / Guard - X11 statement
Command Connect / Guard and FT Client with empty filters
Command Guard limitations
Configuration of Host Control in the VISULOX Cockpit
Host Control (Command Connect / Guard)
Host objects
How to control host objects from the command line
How to control script objects from the command line
How to use SSH-Keys within Command Connect / Guard and FT Client
Private host tool
Script objects
VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.1.1) Command Connect / Guard - X11 statement
(4.1.1) Command Guard limitations

(4.2.0) Additional events for Command Connect / Guard
(4.2.0) Command Connect / Guard - X11 statement
(4.2.0) Command Guard limitations
(4.3.0) Additional events for Command Connect / Guard
(4.3.0) Command Connect / Guard - X11 statement
(4.3.0) Command Guard limitations
Additional events for Command Connect / Guard
Command Connect / Guard - X11 statement
Command Connect / Guard and FT Client with empty filters
Command Guard limitations
Configuration of Host Control in the VISULOX Cockpit
Host Control (Command Connect / Guard)
Host objects
How to control host objects from the command line
How to control script objects from the command line
How to use SSH-Keys within Command Connect / Guard and FT Client
Private host tool
Script objects
VISULOX addon command line interface (CMD Connect / Guard, etc)

How to use SSH-Keys within Command Connect / Guard and FT Client

Command Connect / Guard has the ability to launch an Xterm via SSH and File Transfer has the ability to use SSH for transferring files.

It allows SSH connections with SSH-Keys for an automatic login or with passcode protected keys.

The sshkey can either be provided from the node or from the user.

The SSH Key

The key pair generation can be done anywhere using the command ssh-keygen. The result is a private and public key. The public key part is appended to **$HOME/ssh/authorized_keys** on the destination server.

The private key is stored on any VISULOX Node in a directory readable by the VISULOX Group. Each key must be readable by the group.

```
ls -al /opt/vlxkeys/*
-r--r-----. 1 root vlxgroup 1671 Dec 21 09:27 /opt/vlxkeys/key1
-r--r-----. 1 root vlxgroup  414 Dec 21 09:27 /opt/vlxkeys/key1.pub
-r--r-----. 1 root vlxgroup 1671 Dec 21 09:27 /opt/vlxkeys/key2
-r--r-----. 1 root vlxgroup  414 Dec 21 09:27 /opt/vlxkeys/key2.pub
-r--r-----. 1 root vlxgroup 1675 Dec 21 09:27 /opt/vlxkeys/key3
-r--r-----. 1 root vlxgroup  414 Dec 21 09:27 /opt/vlxkeys/key3.pub
```

When CommandConnect or File Transfer requests an SSH key, the key is copied temporarily into the VISULOX Transit environment and the permission are corrected to the SSH standards (readonly by user).

To allow a more organized addressing of SSH keys, the sshkey mask can be configured.

Command Connect / Guard and FT-Client present the keys, which are found with this mask to the user. Then the user can select the correct key. A pattern matching with placeholders (e.g. %USER%, %HOST%) is possible.

Available placeholders:

Placeholder	Description
%HOST%	Target host

Placeholder	Description
%USER%	Target user
%GROUP%	Group
%LOGINAME%	Login name
%LOGINAMEID%	md5 of the login name
%OWNERID%	md5 TFN (can be seen on Welcome page of the user)

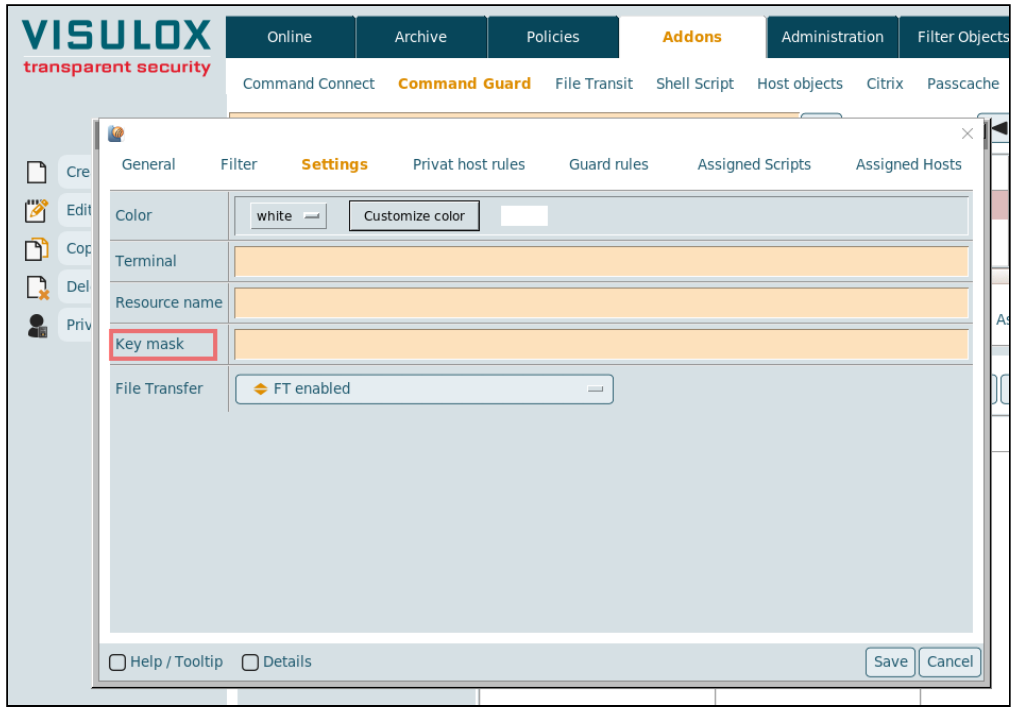
CLI examples

```
/opt/visulox/bin/apps/vlxftclient.tcl -sshkeymask %LOGINUSER%  -hosts root@s1
/opt/visulox/bin/apps/vlxcmdconnect.tcl -sshkeymask %LOGINUSER%  -hosts root@s1
```

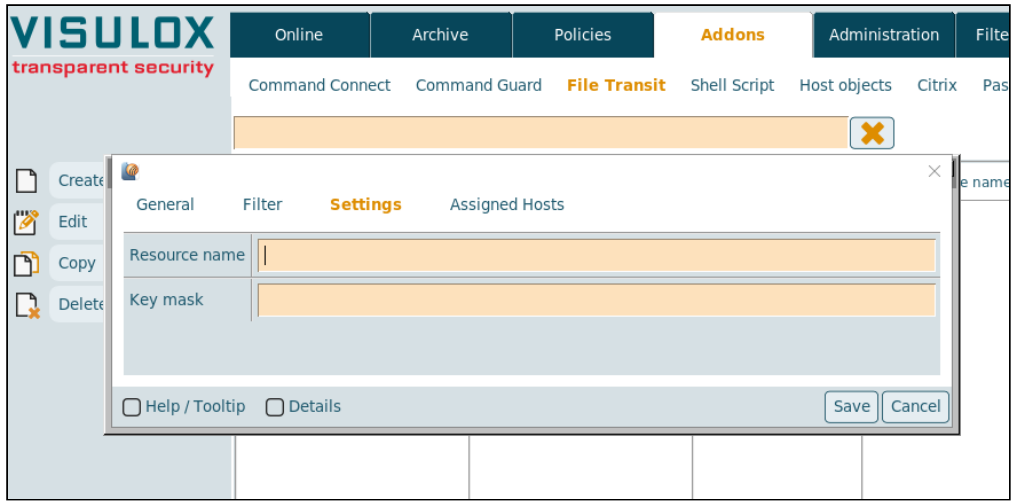
Option -sshkey

Host Connect and File Transfer need to know, where the private key can be found.
This is handled with the option **-sshkey *<path1 to keyfile>*, *<path2 to keyfile>*** (Additional paths are separated via comma).

Command Connect / Guard:



File Transit Console:



Command Connect / Guard - X11 statement

The access to an endpoint can be either **SSH** or **Telnet**.

Telnet does not have an automatic X11 forwarding mechanism.

SSH allows to forward an X11 environment to the endpoint.

- In Command Guard X11 forwarding is disabled hard-coded. This is done for security reasons.

- In Command Connect, the X11 policy on the client (See: **/etc/ssh/ssh_config** on the VISULOX Node) and the endpoint (See: **/etc/ssh/sshd_config** on the endpoint) are considered.

/etc/ssh/ssh_config and /etc/ssh/sshd_conf

```
ssh_config:     ForwardX11 yes
sshd_config:    X11Forwarding yes
```

This allows to open additional xterms in Command Connect. These xterms are not taken into account for **Close**, **Arrange** and **Exit**. They are independent.

To enable X11 forwarding in Command Connect it is also possible to use the **-sshoptions -X** parameter of the Command Connect application to use regular SSH commands.

Command Guard limitations

- The solution does not allow the use VI or other interactive tools.
- The user has to build the command line fully and when he is done, the command line is sent to the server (no auto-completion is possible).
- Process control keys like **^C** and **^D** are provided.
- Any denied or allowed command is logged in the event table.
- This solution is alligned with our philosophy not to change anything on the destination server.

Command Connect / Guard and FT Client with empty filters

It is possible to adjust the behaviour of Command Connect / Guard and FT Client group definitions in case of empfy filters.

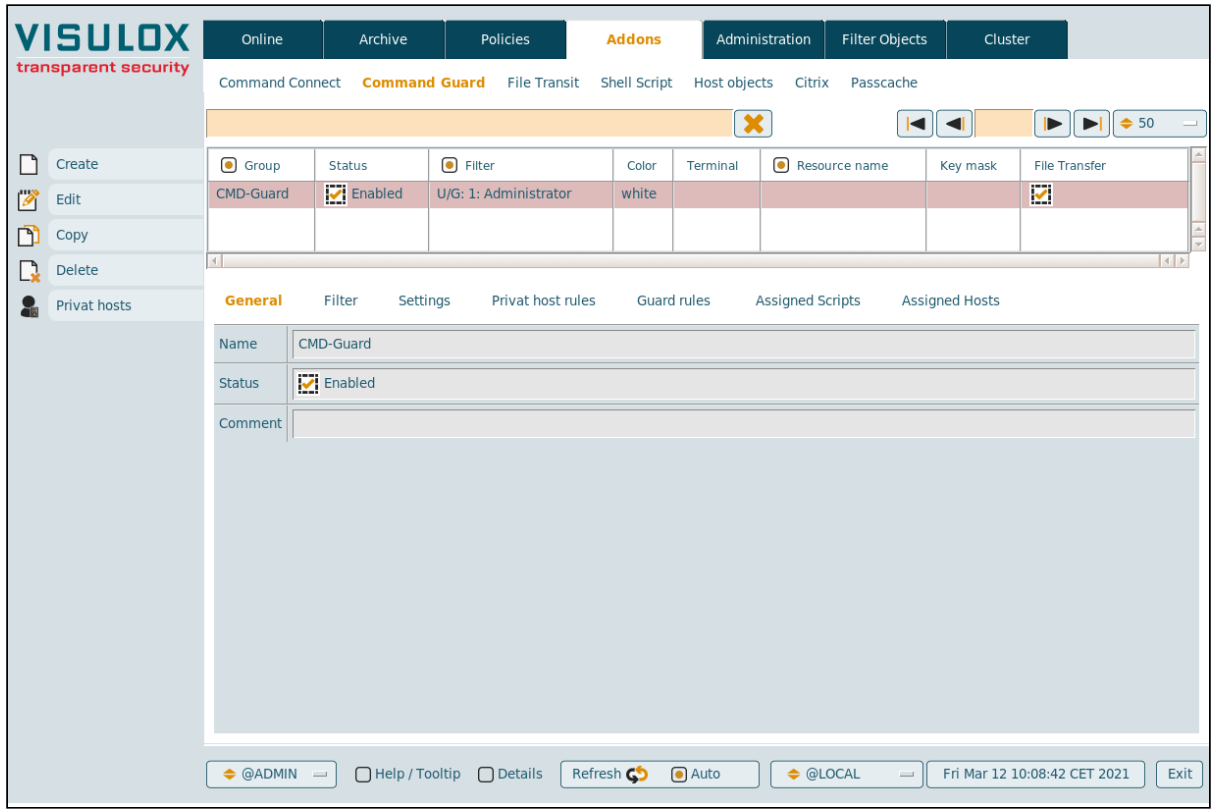
The default setting is, that no groups are displayed when the filter is empty.

```
visulox config edit -name general.allowemptyfilter=0
```

To enable displaying of groups in Command Connect / Guard and FT Client without a filter definition.(definition with no filter (user/group, remoteip, accesspoint) is assigned to all users) set:

```
visulox config edit -name general.allowemptyfilter=1
```

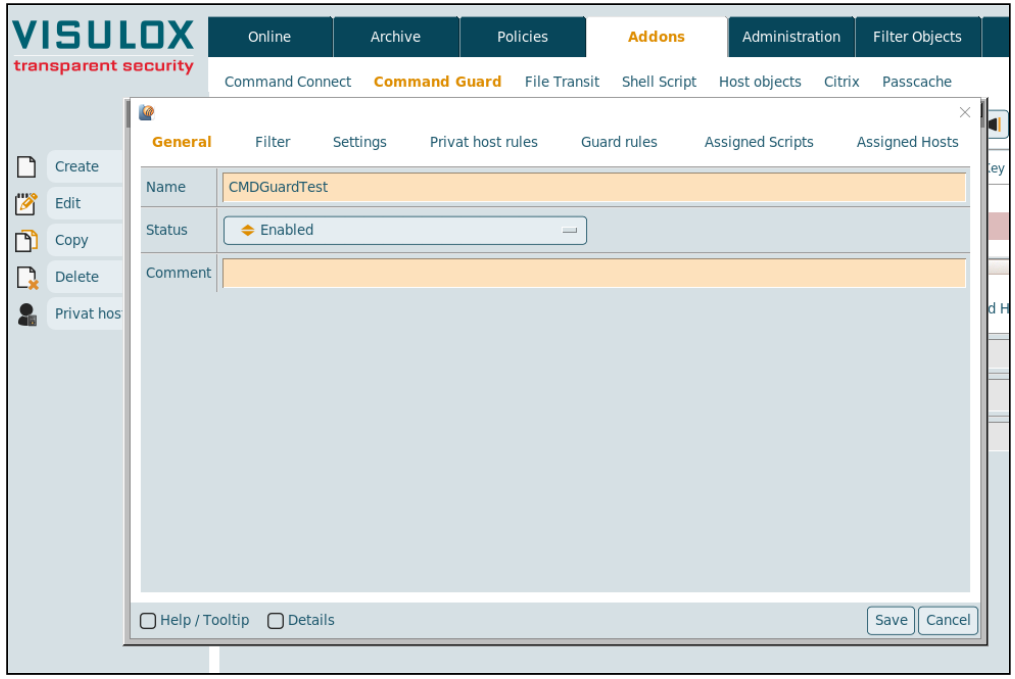
Available Command Guard groups



New Command Connect / Guard groups can be created and existing groups can be edited, copied or deleted.

If users have added private hosts, they can be displayed for the selected group with the **Private hosts** button.

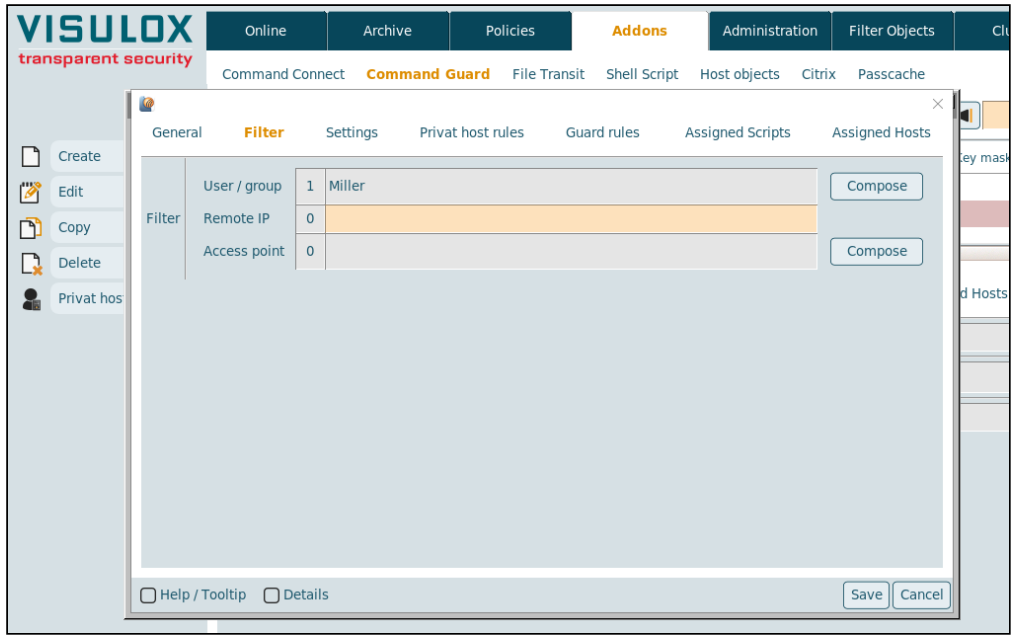
General



The name of the group and the status (enabled or disabled) has to be entered.

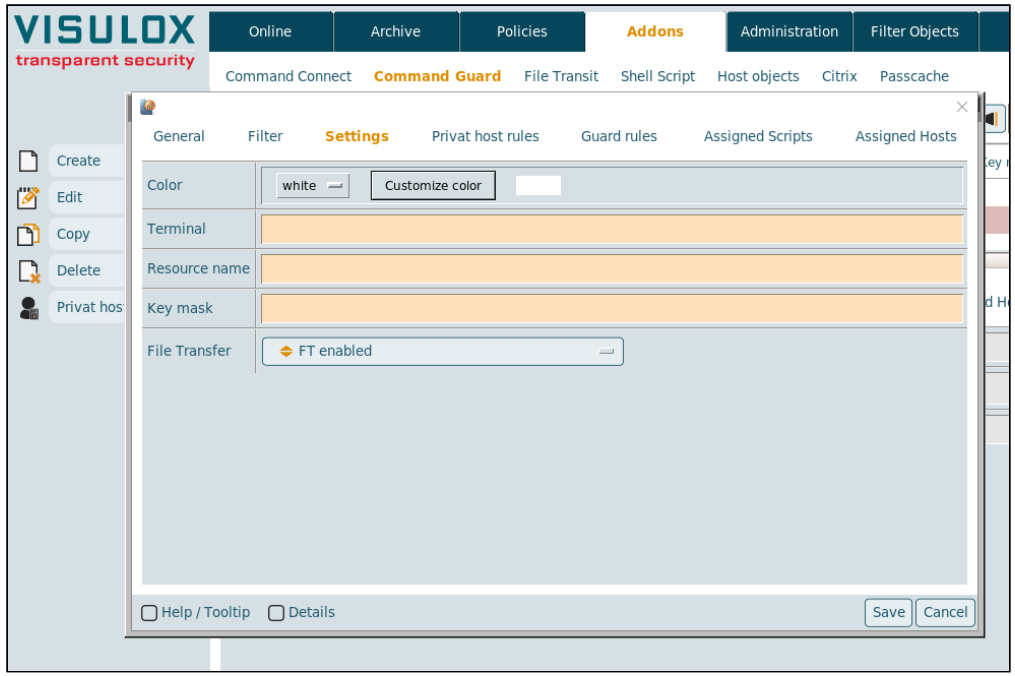
A comment for the group can be added as well.

Filter



The filter for Command Connect / Guard groups can be set on user/groups, the remote IP or the access point.

Settings

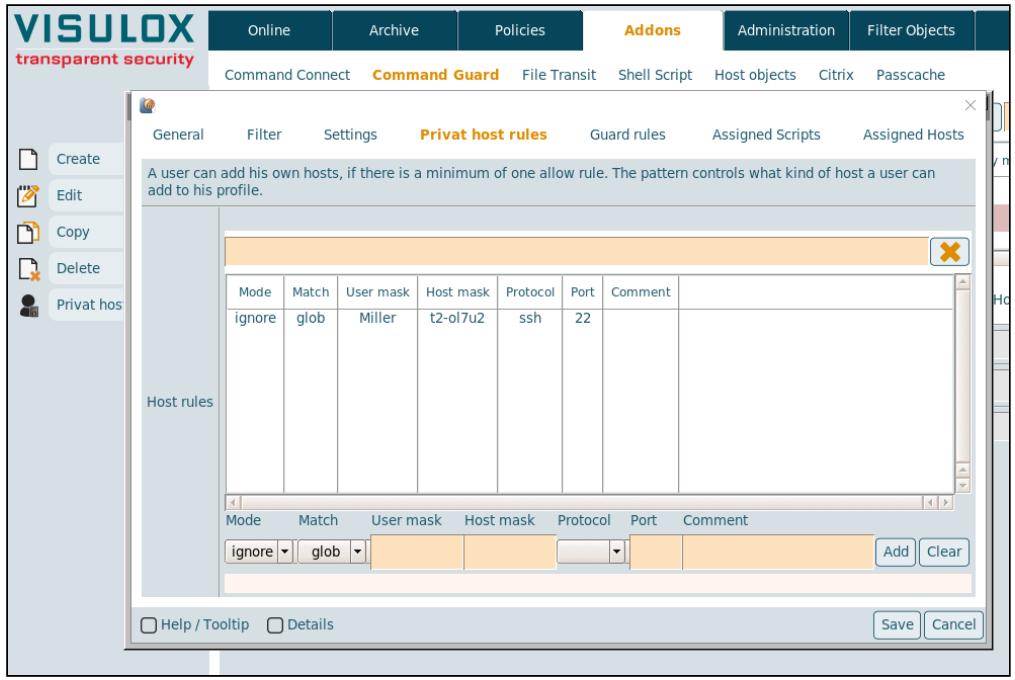


The color for the shells can be chosen and the term variable can be set. If term is set, it is provided via SSH to the remote host session. The default terminal is **xterm** in Telnet and SSH sessions. If the remote host does not support this terminal type in the xterm, the terminal can be overwritten with the Terminal setting.

The resource and the keymask for connections via SSH Key can be set and File Transfer can be enabled or disabled for this group.

If an owner is set for the resource, the owner must be set also for Command Connect in the ressource name field: **<resource-name>%OWNER%**

Private host rules

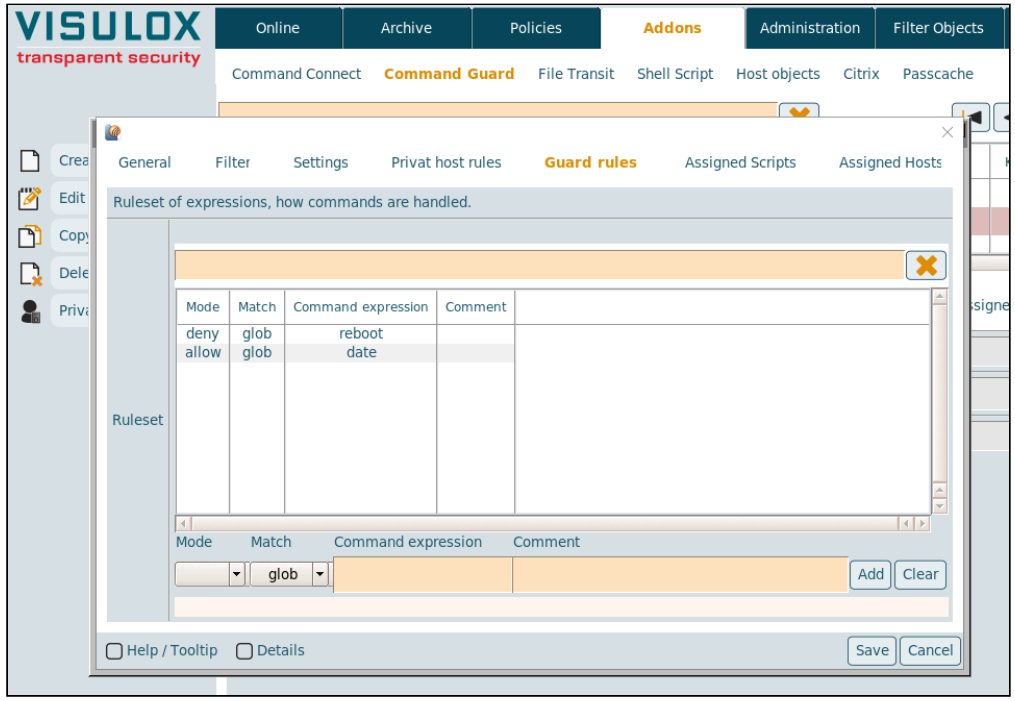


If at least one allow rule is configured, the user can add hosts by himself based on the rules entered here.

- **Mode:** The mode of the rule can be chosen: ignore, allow or deny
- **Match:** The matching mode of the rule: glob or regexpr
- **User mask:** User mask for the connection
- **Host mask:** Host mask for the connection
- **Protocol:** SSH or Telnet

- **Port:** The port for the connection
- **Comment:** Optional comment

Guard rules (Command Guard only)



Guard rules are available only in Command Guard. with these rules commands in the shells can be allowed or denied.

- **Mode:** The mode of the rule can be chosen: ignore, allow or deny
- **Match:** The matching mode of the rule: glob, regline or regexpr

- **Command expression:** The command itself
- **Comment:** Optional comment

Rule / pattern definition

The allow / deny rules are based on a regular expression. Applied line by line, exit on first match.

Regular expressions are helpful for complex pattern recognition. If the expressions are getting too complex, eventually they will not be easy to understand (in this case a human expert is a better solution). Therefore an interface is provided to select server side scripts, which can be executed without passing through Command Guard.

Policy definition
deny:cat /etc/hosts: Viewing this file is not allowed
allow:cat [a-z09^.]+: Any other file can be viewed

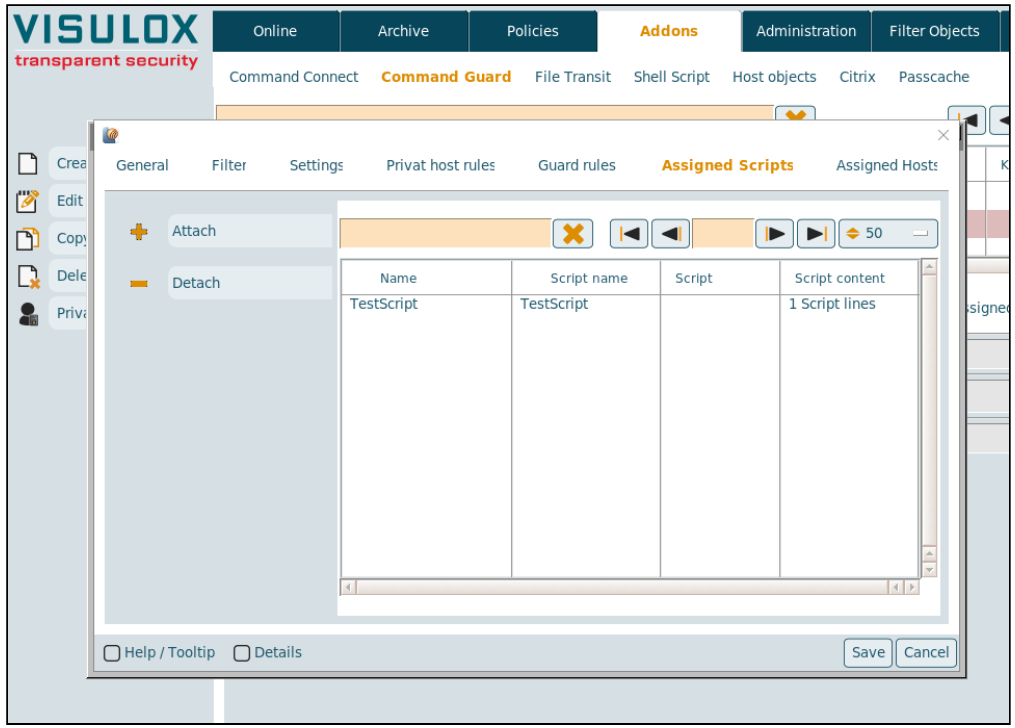
- User can view any file, but not /etc/hosts
- If no rule matches the command is denied
- A rule can control Unix pipes as well

Format syntax for rules (private host rules, Guard rules):

regexp: http://www.tcl.tk/man/tcl8.6/TclCmd/re_syntax.htm

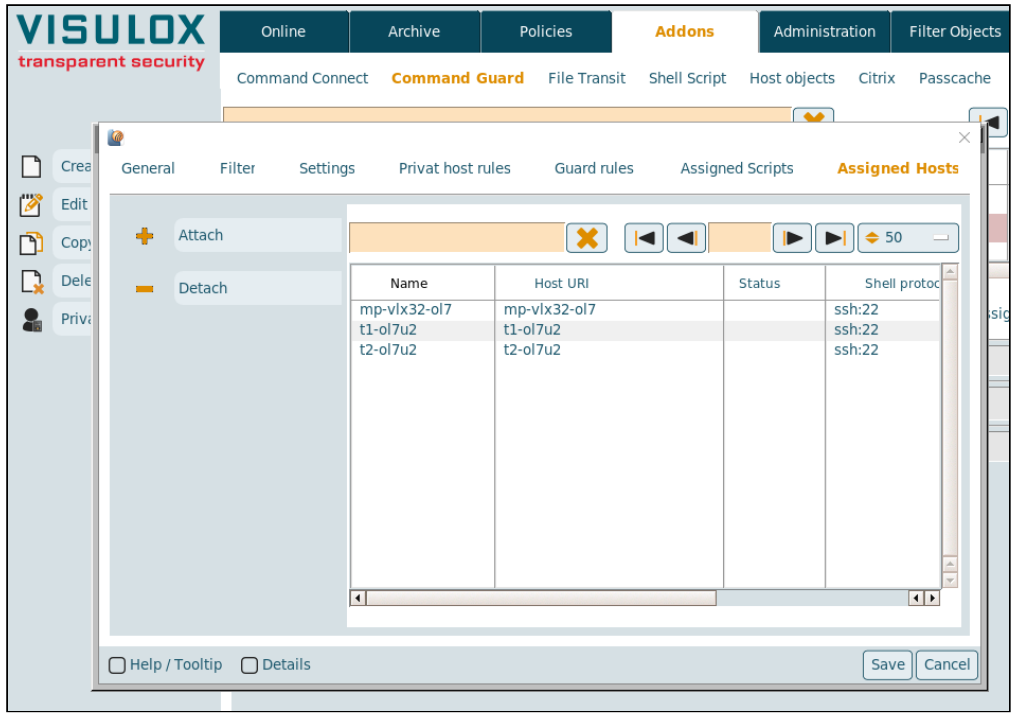
glob: http://www.tcl.tk/man/tcl8.6/TclCmd/glob.htm

Assigned scripts (Command Guard only)



Available scripts can be attached / detached from the Command Guard group. (See also: Script objects)

Assigned hosts



Host objects can be attached / detached from the Command Connect / Guard group. (See also: Host objects)

Before hosts can be added to a new created group, the group must be saved once.

Additional events for Command Connect / Guard

Additional events can be enabled for Command Connect / Guard.

An event can be triggered for Command Connect / Guard sessions, when connecting, disconnecting, getting a shell prompt, redact mode, command not allowed and starting an unmanaged terminal.

> These events are disabled by default

All events can be enabled with:

All events at once

```
visulox config -name commandconnect.event.default=true
```

Single events can be enabled with the according entry:

```
    ------------------------------------------------------------------
    | changed | parameter                        |      type | value   |
    ------------------------------------------------------------------
    |         | commandconnect.event.alert       | OPERATION | default |
    |         | commandconnect.event.connect     | OPERATION | default |
    |         | commandconnect.event.default     | OPERATION | false   |
    |         | commandconnect.event.disconnect  | OPERATION | default |
    |         | commandconnect.event.shellprompt | OPERATION | default |
    |         | commandconnect.event.unmanaged   | OPERATION | default |
    ------------------------------------------------------------------
```

Additional events for redact mode:

```
visulox config -name redact
    ------------------------------------------------------------------------------------------------
    | changed | key                                                  | value                       |
```

```
-------------------------------------------------------------------------------------------
|         | commandconnect.event.redact                          | default                    |
|         | commandconnect.event.redactinfo                      | Redact %POLICY% %RMC%: %RMI%  |
|         | guidefaults.global_application_policy.redactmode     | redactOff.map              |
|         | guidefaults.global_application_policy.redactstring | **********                 |
-------------------------------------------------------------------------------------------
```

23.1.77 File Transfer

VISULOX File Transfer guarantees that security zones are not connected and remain separate.
In contrast to other solutions this is a true logical split of secure protocols.

Multiple transfer policies to different endpoints can be defined. (direction, content, size).

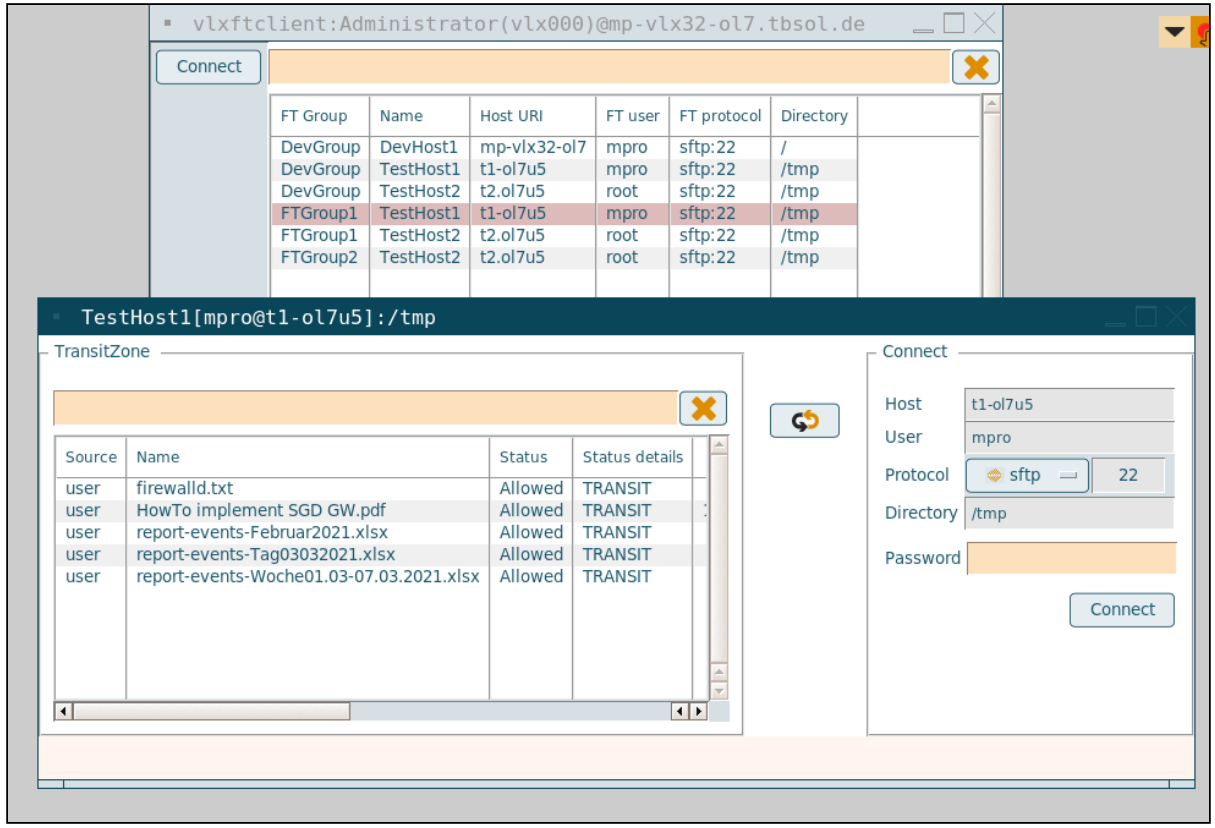
Also, the transferred files are provided to the users through their home directory
or via a FTP server in a controlled manner.

- Overview
  - Configuration options
- Transit Zone in VISULOX Cockpit
- FT Client application
  - FT Client connection
  - Transfer
  - Configuration parameters
- Connect to Bitvise SFTP server
- Related information

Overview

The File Transit Console is an interface to interact between the Transit Zone and an SFTP/FTP endpoint.

This allows to connect to a server using **SFTP**, **FTP passive** or **FTP active** protocol.



Depending on the underlying policies, the user can transfer files between the Transit Zone and the available application servers.

Configuration options

Changing the name of the files in Transit Zone

transit.naming

```
./visulox config list -name transit.naming
    ------------------------------------------------
    | changed | key            | value               |
    ------------------------------------------------
    |         | transit.naming | %NAME%-%HOST%-%USER% |
    ------------------------------------------------
```

```
./visulox config list -name transit.filename
    ------------------------------------------------------------
    | changed | key              | value                      |
    ------------------------------------------------------------
    |         | transit.filename | [0-9a-zA-Z \.\-_@=#:+~%()] |
    ------------------------------------------------------------
```

Regexpression with **^**and **+$** is possible.

Adjusting retention times for the Transit Zone

Retension times

```
visulox config -name retentiontime -info

------------------------------------------------------------------------------------------------------------------------------------------------------
------------------
    | changed | key                                      | value |
 shortinfo | defaultvalue |
```

```
------------------------------------------------------------------------------------------------------------------------------------------
------------------
    |         | transit.retentiontime                  | 3600  |                retention time of files in the transit zone in
seconds  |         3600 |
    |         | transit.retentiontime.approved         | 7200  | retention time of files in the transit zone after approved in
seconds  |         7200 |
    |         | transit.retentiontime.pending          | 7200  |   retention time of files in pending state in transit zone in
seconds  |         7200 |
    |         | transit.retentiontime.warningthreshold | 300   |               warning befor file is removed from transizone in
seconds |          300 |

------------------------------------------------------------------------------------------------------------------------------------------
------------------
```

Adjusting maxuploadsize and Transit quota

transit.maxuploadsize & transit.quota

```
visulox config edit -name transit.maxuploadsize=1Gbyte (Default: 20Gbyte)
visulox config edit -name transit.quota=30Gbyte (Default: 50Gbyte)
```

Possible units: k(kbyte, m (mbyte) g (gbyte).

Modifing **maxuploadsize** needs to register VISULOX at the VISULOX Access Node.

```
visulox portal attach -jspconf
```

See also: Attaching VISULOX Service to VISULOX PORTAL Service

Default temporary Transit directory

The default temporary Transit directory (general.filearea) is **/opt/visulox/var/filearea/**. All temporary files during transit, ftclient and fileexchange are stored temporarily in this directory.
Integrity Check displays a warning, if **general.filearea** is smaller than four times of the **transit.maxuploadsize**.

Depending on the usage, **general.filearea** has to be configured.

> size = transit.maxuploadsize * concurrent users using File Transfer.

The path of the filearea folder can be changed with:

```
visulox config -name general.filearea
    ---------------------------------------
    | changed | key              | value |
    ---------------------------------------
    |         | general.filearea |       |
    ---------------------------------------
```

> With an NFS Share the **%NODE%** variable has to be used for the nodes.

Time in seconds, how long files remain in the Transit Zone

transit.retentiontime

```
visulox config edit -name transit.retentiontime=1800 (Default: 3600)
```

The Transit Zone has to be used by the user to transfer files from A to B. It should not be abused as a "store". This is not the service of the Transit Zone.

Checkout of rejected File Transfer files

With the following configuration parameter rejected File Transfer files will be stored in the filestore and are available for checkout:

```
visulox config -name transit.storerejectedfiles=true
```

Enable File Exchange service

```
visulox config -name layout.<logical server name>.fileexchange=true
visulox restart -service monitor
```

File Exchange certificate configuration

```
-------------------------------------------------------------------------
| changed | key                       | value                           |
-------------------------------------------------------------------------
|         | fileexchange.banner       | %LICENSE%                       |
|         | fileexchange.cafile       |                                 |
|         | fileexchange.certfile     | visulox.self.pem                |
|         | fileexchange.connection   | From %RIP% on %NODE% (%HOST%)   |
|         | fileexchange.keyfile      | visulox.self.key                |
|         | fileexchange.port         |                                 |
|         | fileexchange.sslport      | 1443                            |
-------------------------------------------------------------------------
```

Files need to be placed in **/opt/visulox/etc/ssl/**.

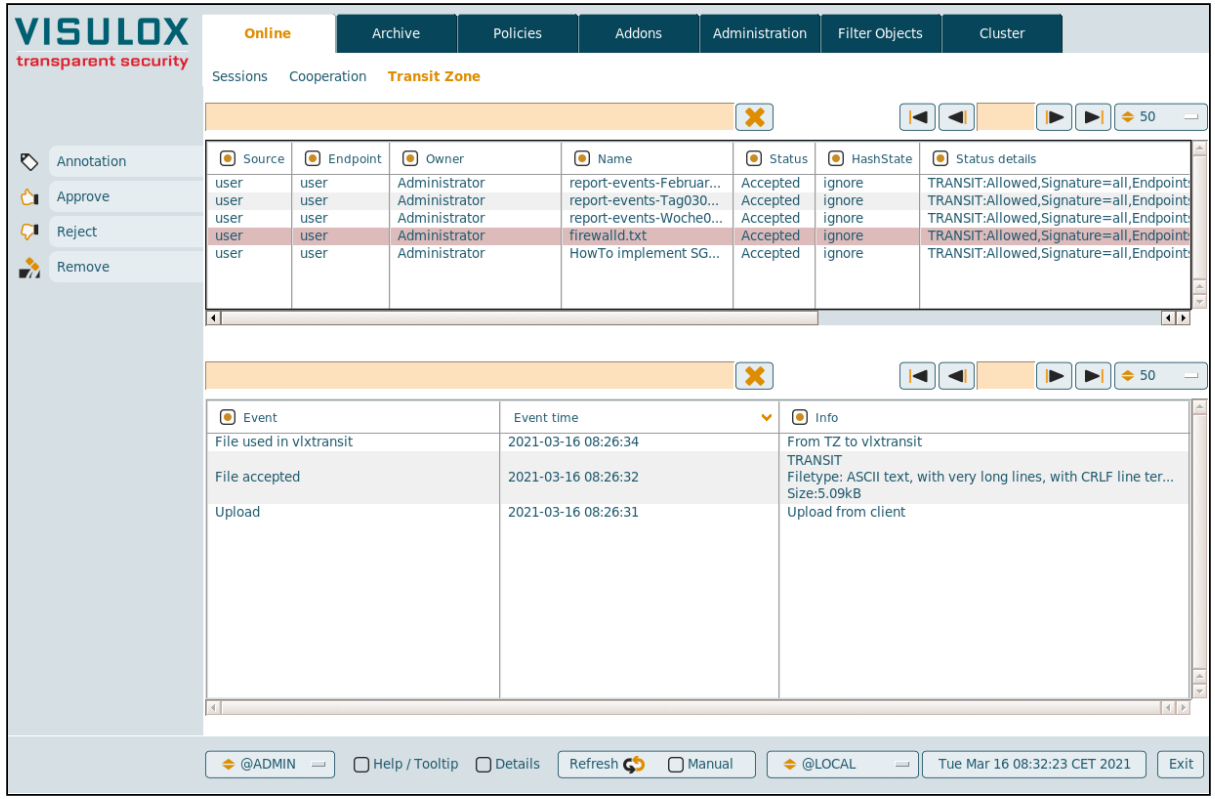
Isolated transit user

The **vlxMode** parameter **IU** starts a **visulox.exp** application with its own transit user and Transit Zone.

The IU application must be started after the original application.

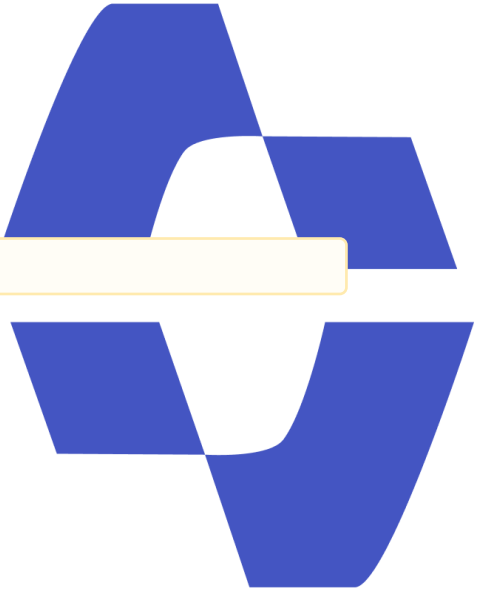
Transit Zone in VISULOX Cockpit

The current files in Transit Zone are displayed in the Cockpit.



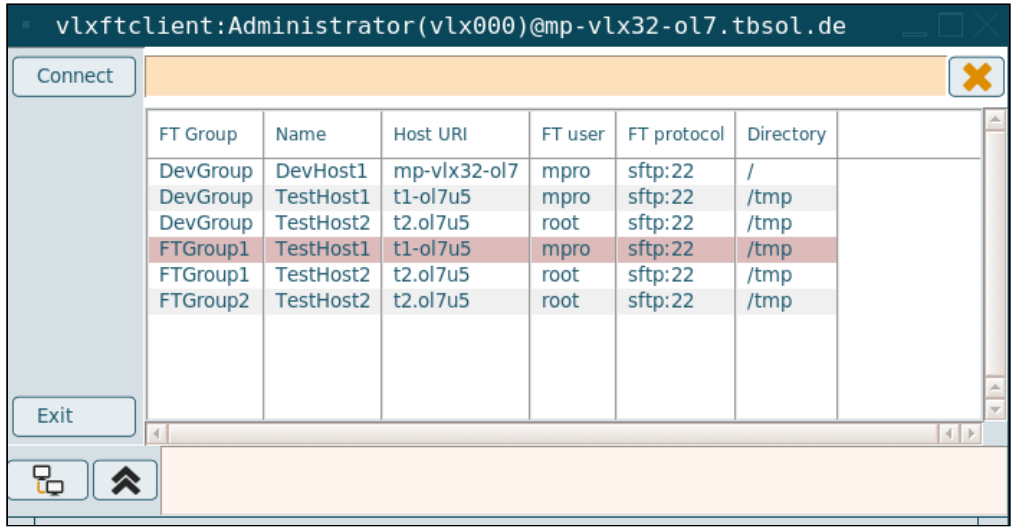
- **Annotation:** A remark for the selected record can be added
- **Approve:** The selected file will be approved. (⚠ A user can not approve his own files!)
- **Reject:** The selected file will be rejected
- **Remove:** Selected files are removed from the Transit Zone

With a right-click on an entry, it is possible to jump to the file entry in Cockpit / Archive.



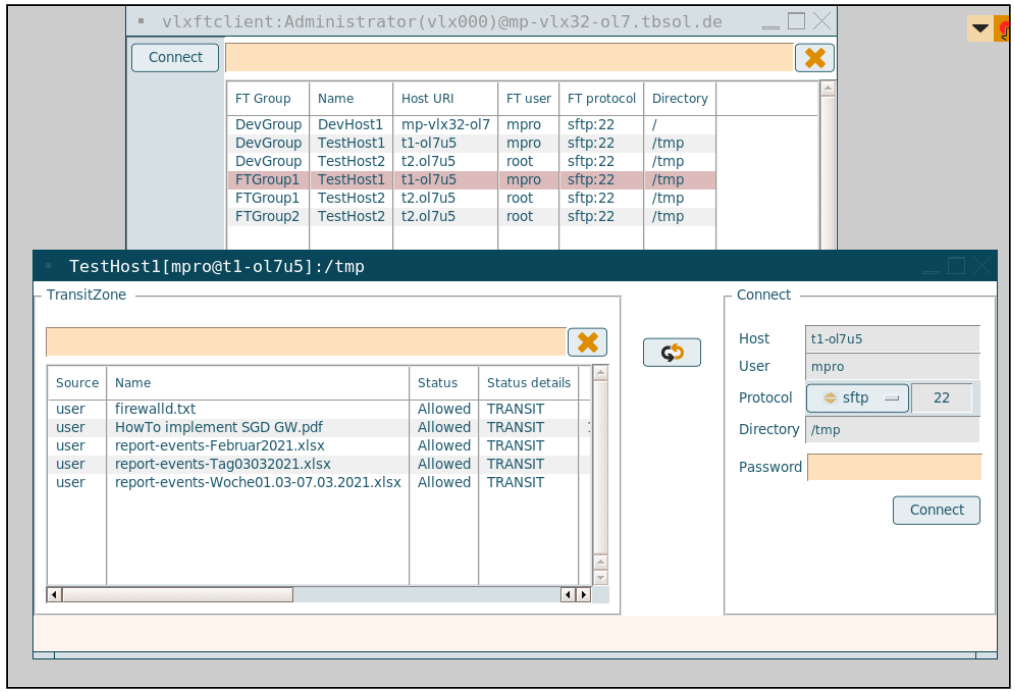
⚠ Guest users with multiple login enabled have no access to uploaded files after re-login.

FT Client application



- **Connect:** Opens FT Client to all selected hosts
- **Exit:** FT Client application and all open sessions are closed
- **Arrange:** FT Client connections will be rearranged
- **Collapse:** Collapse Console

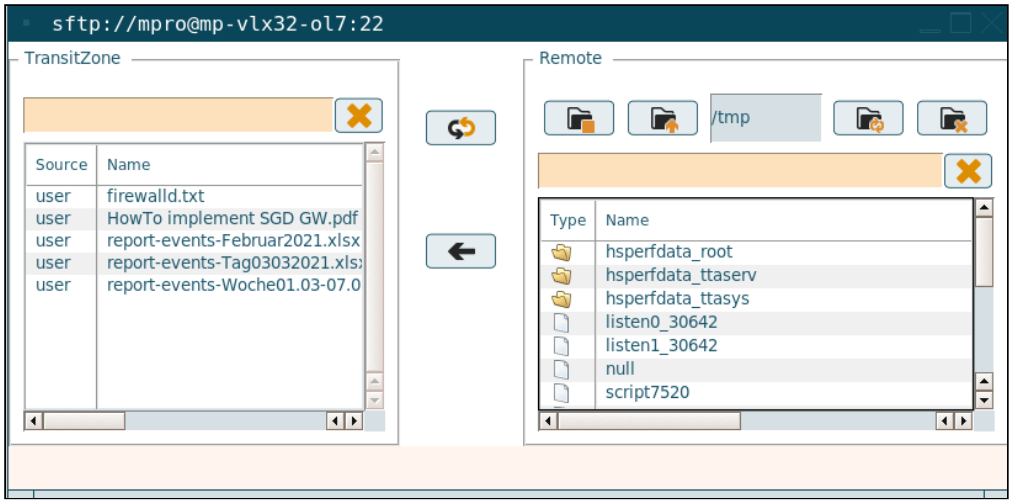
FT Client connection



Depending on the configuration, the user has to enter the credentials for the selected connection.

An FT Client Group has endpoints assigned. No user in the endpoint allows to enter a free user.

Transfer



Depending on the underlying policies, the user can transfer files between the Transit Zone and the available application servers.

Configuration parameters

Application	Application command	Login script
FT Client	vlxftclient	visulox.exp

The following parameters can be used with the FT Client:

Parameter	Description
-title <*value*>	Application title <>
-groups <*value*>	Comma seperated list of groups <>
-lang <*value*>	Language <>
-hosts <*value*>	Comma separated list of hosts (sftp://user@host) <>
-sshkey <*value*>	SSH-key: path to SSH-keyfiles <>
-sshkeymask <*value*>	SSH-key: mask to select SSH-keyfiles %HOST%, %USER%, %LOGINUSER%,%OWNERID%,%GROUP%
-files <*value*>	Comma seperated list of definition files <>
-autoconnect	Auto connect, if there is only one host
-resource <*value*>	Name of passcache resource
-sshpassprompt <*value*>	Override default sshpass password prompt. See: "man sshpass -P"

FT Client supports **-hosts** / **-files** / **-groups**. Each parameter is a comma separated list.

If one is set, the groups are not taken from the database.

- **-hosts** allows to specify a list of hosts. A single group is generated named **CLI**

- **-files** allows to read groups and hosts from a file. The file must be readable by **vlxgroup** on all VISULOX Access Nodes. If the files are not found, they will be searched in the directory assigned via **general.hostfileslookuppath**.

  File example:

```
[GRP1]
sftp://root@GW1//tmp
sftp://root@GW2

[GRP2]
sftp://root@portal1:22//tmp
sftp://root@portal2:23
```

  Custom **ports** can be declared with "**:**" and **directories** can be added with "**/**".

- **-groups** requests the group and assigned hosts from the database.

With **-autoconnect** always the first group will be activated. If there is only one group with one host and **-autoconnect** is set, it wil be opened directly (in fullscreen).

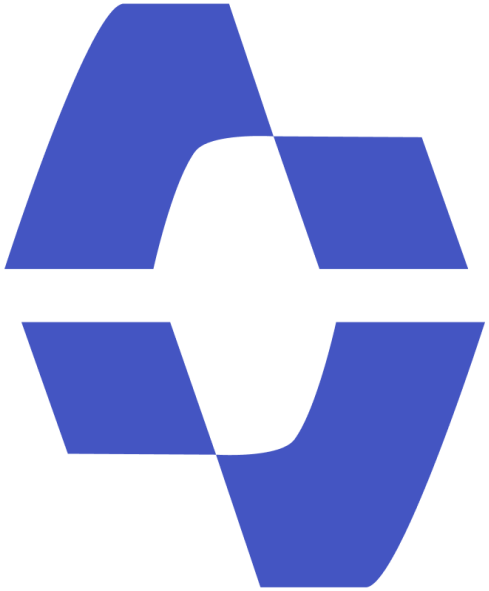
This allows to have ftclient with ANY/ANY or a single host in an independent window w/out windowmanager.

Connect to Bitvise SFTP server

Connection to a Bitvise SFTP server on Windows servers is supported with all FT modules.

In this case, there are two possible options:

- command shell mode full access
- bvshell with full access and limit to root directory



Related information

(4.1.1) Accessing the File Exchange web page

(4.1.1) Allowing File Transfer from internal to internal

(4.1.1) Automated transfer of files into Transit Zone (Passon)

(4.1.1) Command Connect / Guard and FT Client with empty filters

(4.1.1) Configuration of File Transfer in the VISULOX Cockpit

(4.1.1) Custom vlxuser ID for transit users

(4.1.1) Extended Transit Policy with hash check by provided hash file

(4.1.1) File Transfer

(4.1.1) File Transfer features

(4.1.1) File Transfer modules

(4.1.1) File Transfer recommendations

(4.1.1) File Transit with approval

(4.1.1) How to attach Chrome/Chromium download directory to vlxtransit

(4.1.1) How to configure File Transfer content check

(4.1.1) How to control FT Client from the command line

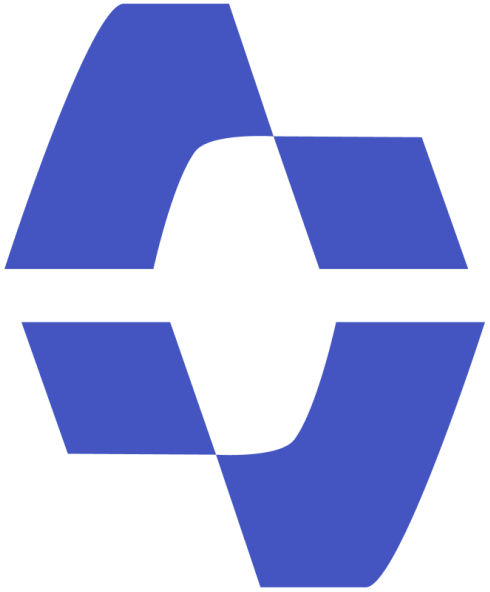
(4.1.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service

(4.1.1) How to use SSH-Keys within Command Connect / Guard and FT Client

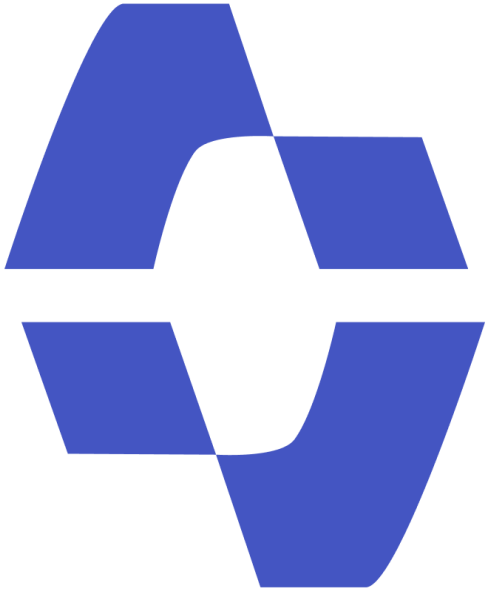
(4.1.1) Transit Policy

(4.1.1) Transit script variables

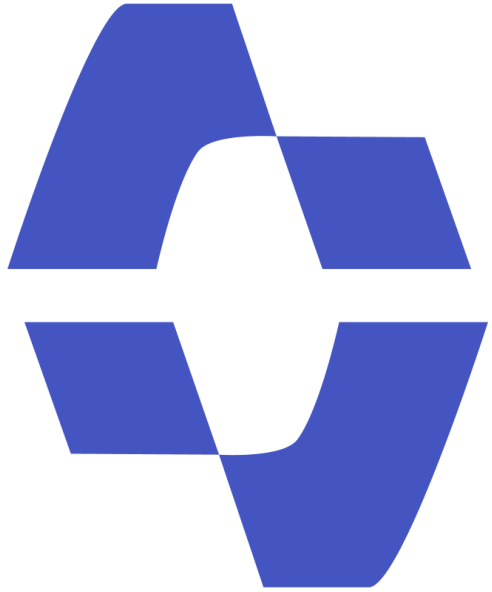
(4.1.1) VISULOX addon command line interface (CMD Connect / Guard, etc)



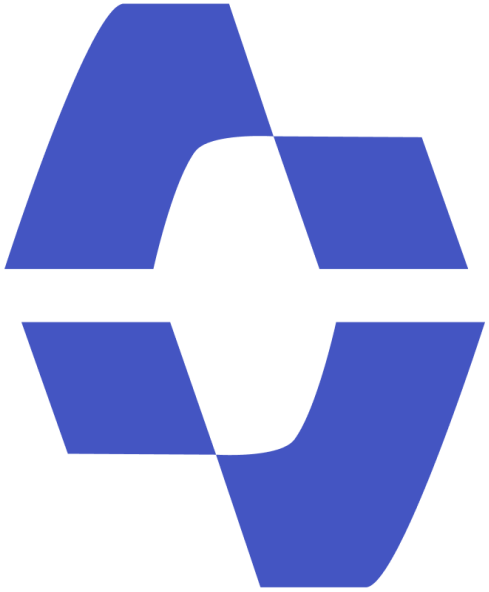
(4.1.1) VISULOX Transit mapping
(4.1.1) VISULOX Transit Mapping and Ubuntu application servers
(4.1.1) VISULOX4_FileTransfer_(VFT)
(4.2.0) Accessing the File Exchange web page
(4.2.0) Automated transfer of files into Transit Zone (Passon)
(4.2.0) Command Connect / Guard and FT Client with empty filters
(4.2.0) Configuration of File Transfer in the VISULOX Cockpit
(4.2.0) Extended Transit Policy with hash check by provided hash file
(4.2.0) File Transfer
(4.2.0) File Transfer features
(4.2.0) File Transfer modules
(4.2.0) File Transit with approval
(4.2.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.2.0) How to configure File Transfer content check
(4.2.0) How to control File Transit Policy from the command line
(4.2.0) How to control FT Client from the command line
(4.2.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.2.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.2.0) Transit Policy
(4.2.0) Transit script variables
(4.2.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.2.0) VISULOX Transit mapping



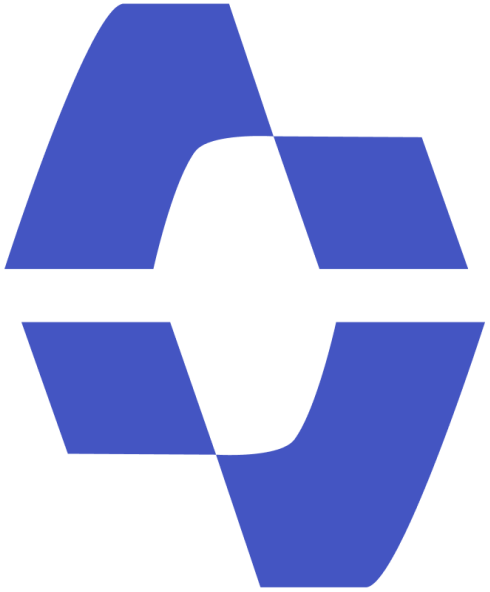
(4.2.0) VISULOX Transit Mapping and Ubuntu application servers
(4.2.0) VISULOX4_FileTransfer_(VFT)
(4.3.0) Accessing the File Exchange web page
(4.3.0) Automated transfer of files into Transit Zone (Passon)
(4.3.0) Command Connect / Guard and FT Client with empty filters
(4.3.0) Configuration of File Transfer in the VISULOX Cockpit
(4.3.0) Extended Transit Policy with hash check by provided hash file
(4.3.0) File Transfer
(4.3.0) File Transfer features
(4.3.0) File Transfer modules
(4.3.0) File Transit with approval
(4.3.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.0) How to configure File Transfer content check
(4.3.0) How to control FT Client from the command line
(4.3.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.0) Object ID
(4.3.0) Transit Policy
(4.3.0) Transit script variables
(4.3.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.0) VISULOX FTP Service
(4.3.0) VISULOX Transit mapping



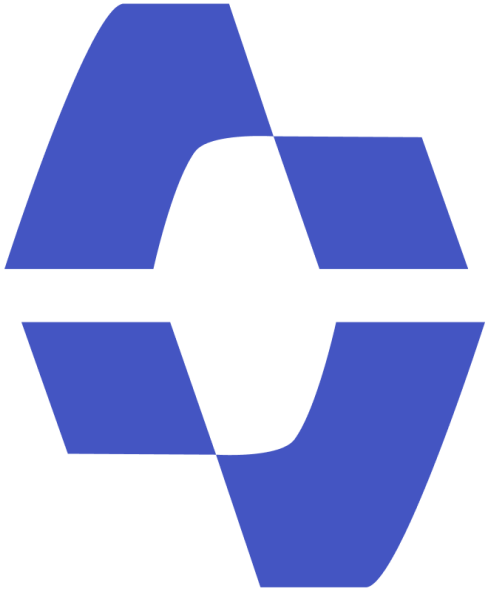
(4.3.0) VISULOX Transit Mapping and Ubuntu application servers
(4.3.0) VISULOX4_FileTransfer_(VFT)
(4.3.1) Accessing the File Exchange web page
(4.3.1) Allowing File Transfer from internal to internal
(4.3.1) Automated transfer of files into Transit Zone (Passon)
(4.3.1) Command Connect / Guard and FT Client with empty filters
(4.3.1) Configuration of File Transfer in the VISULOX Cockpit
(4.3.1) Custom vlxuser ID for transit users
(4.3.1) Extended Transit Policy with hash check by provided hash file
(4.3.1) File Transfer
(4.3.1) File Transfer features
(4.3.1) File Transfer modules
(4.3.1) File Transfer recommendations
(4.3.1) File Transfer via command line
(4.3.1) File Transit with approval
(4.3.1) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.1) How to configure File Transfer content check
(4.3.1) How to control File Transit Policy from the command line
(4.3.1) How to control FT Client from the command line
(4.3.1) How to discard filetypes from the Transit Zone synchronisation
(4.3.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.1) How to use SSH-Keys within Command Connect / Guard and FT Client



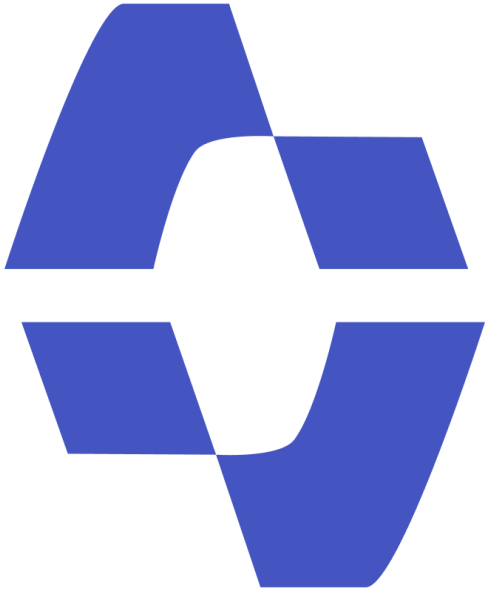
(4.3.1) Object ID
(4.3.1) Transit Policy
(4.3.1) Transit script variables
(4.3.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.1) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.1) VISULOX FTP Service
(4.3.1) VISULOX Transit mapping
(4.3.1) VISULOX Transit Mapping and Ubuntu application servers
(4.3.1) VISULOX4_FileTransfer_(VFT)
(4.3.2) Accessing the File Exchange web page
(4.3.2) Allowing File Transfer from internal to internal
(4.3.2) Automated transfer of files into Transit Zone (Passon)
(4.3.2) Command Connect / Guard and FT Client with empty filters
(4.3.2) Configuration of File Transfer in the VISULOX Cockpit
(4.3.2) Custom vlxuser ID for transit users
(4.3.2) Extended Transit Policy with hash check by provided hash file
(4.3.2) File Transfer
(4.3.2) File Transfer features
(4.3.2) File Transfer modules
(4.3.2) File Transfer recommendations
(4.3.2) File Transfer via command line
(4.3.2) File Transit with approval



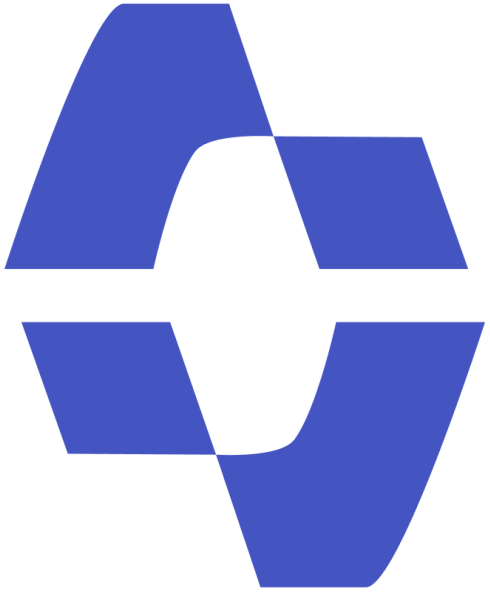
(4.3.2) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.2) How to configure File Transfer content check
(4.3.2) How to control File Transit Policy from the command line
(4.3.2) How to control FT Client from the command line
(4.3.2) How to discard filetypes from the Transit Zone synchronisation
(4.3.2) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.2) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.2) Object ID
(4.3.2) Transit Policy
(4.3.2) Transit script variables
(4.3.2) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.2) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.2) VISULOX FTP Service
(4.3.2) VISULOX Transit mapping
(4.3.2) VISULOX Transit Mapping and Ubuntu application servers
(4.3.2) VISULOX4_FileTransfer_(VFT)
Accessing the File Exchange web page
Allowing File Transfer from internal to internal
Automated transfer of files into Transit Zone (Passon)
Command Connect / Guard and FT Client with empty filters
Configuration of File Transfer in the VISULOX Cockpit
Custom vlxuser ID for transit users



Extended Transit Policy with hash check by provided hash file
File Transfer
File Transfer features
(4.3.3) File Transfer modules
File Transfer recommendations
File Transfer via command line
File Transit with approval
How to attach Chrome/Chromium download directory to vlxtransit
How to configure File Transfer content check
How to control File Transit Policy from the command line
How to control FT Client from the command line
How to discard filetypes from the Transit Zone synchronisation
How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
How to use SSH-Keys within Command Connect / Guard and FT Client
Object ID
Transit Policy
Transit script variables
VISULOX addon command line interface (CMD Connect / Guard, etc)
VISULOX File Transit and Sophos Endpoint Security and Control
VISULOX FTP Service
VISULOX Transit mapping
VISULOX Transit Mapping and Ubuntu application servers



(4.3.3) VISULOX4_FileTransfer_(VFT)
(4.1.1) File Transfer via command line
(4.1.1) How to control File Transit Policy from the command line
(4.1.1) How to discard filetypes from the Transit Zone synchronisation
(4.1.1) Object ID
(4.1.1) VISULOX File Transit and Sophos Endpoint Security and Control
(4.1.1) VISULOX FTP Service
(4.2.0) Allowing File Transfer from internal to internal
(4.2.0) Custom vlxuser ID for transit users
(4.2.0) File Transfer recommendations
(4.2.0) File Transfer via command line
(4.2.0) How to discard filetypes from the Transit Zone synchronisation
(4.2.0) Object ID
(4.2.0) VISULOX File Transit and Sophos Endpoint Security and Control
(4.2.0) VISULOX FTP Service
(4.3.0) Allowing File Transfer from internal to internal
(4.3.0) Custom vlxuser ID for transit users
(4.3.0) File Transfer recommendations
(4.3.0) File Transfer via command line
(4.3.0) How to control File Transit Policy from the command line
(4.3.0) How to discard filetypes from the Transit Zone synchronisation
(4.3.0) VISULOX File Transit and Sophos Endpoint Security and Control



Accessing the File Exchange web page

Allowing File Transfer from internal to internal

Automated transfer of files into Transit Zone (Passon)

Command Connect / Guard and FT Client with empty filters

Configuration of File Transfer in the VISULOX Cockpit

Custom vlxuser ID for transit users

Extended Transit Policy with hash check by provided hash file

File Transfer

File Transfer features

File Transfer modules

File Transfer recommendations

File Transfer via command line

File Transit with approval

How to attach Chrome/Chromium download directory to vlxtransit

How to configure File Transfer content check

How to control File Transit Policy from the command line

How to control FT Client from the command line

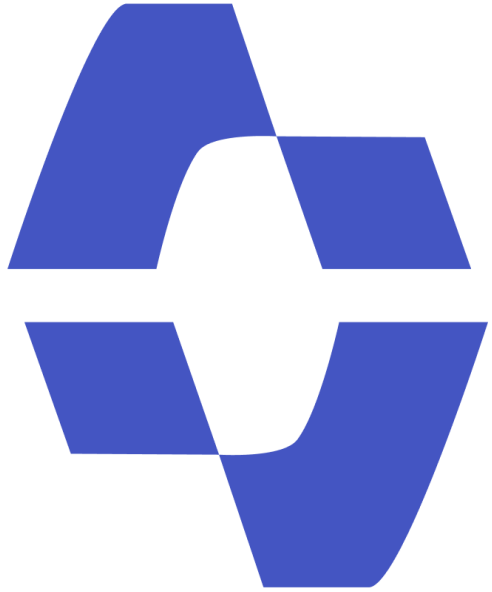
How to discard filetypes from the Transit Zone synchronisation

How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service

How to use SSH-Keys within Command Connect / Guard and FT Client

Object ID

Transit Policy



Transit script variables
VISULOX addon command line interface (CMD Connect / Guard, etc)
VISULOX File Transit and Sophos Endpoint Security and Control
VISULOX FTP Service
VISULOX Transit mapping
VISULOX Transit Mapping and Ubuntu application servers
VISULOX4_FileTransfer_(VFT)

Accessing the File Exchange web page

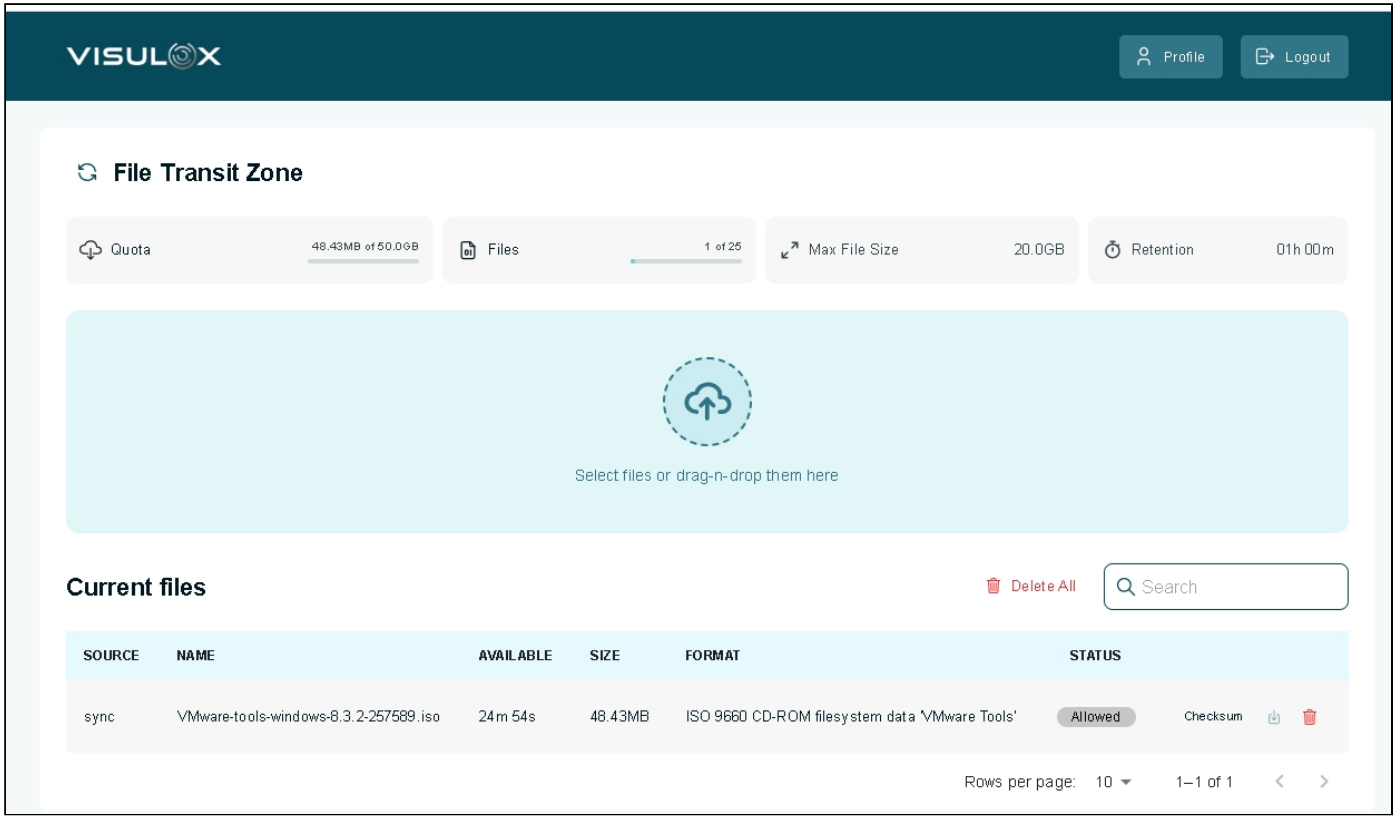
- Overview
- Configuration
  - Enable the File Exchange service
  - File Exchange URL
  - Format of the configuration value
  - More configuration options

Overview

The VISULOX File Exchange frontend can be reached via web access from an internal server using a browser.

The user can connect to every VISULOX node, using the internal WEB browser and a known URL. The WEB Access PIN is needed to see the Transit Zone.
Now the user is able to upload and download files from the Transit Zone. (⚠ The File Exchange service has to be enabled by the administrator).

ℹ It may be necessary to add the URL for File Exchange to the trusted sites in the browser.


VISULOX
Profile
Logout
File Transit Zone
Quota
48.43MB of 50.0GB
Files
1 of 25
Max File Size
20.0GB
Retention
01h 00m
Select files or drag-n-drop them here
Current files
Delete All
Search
SOURCE
NAME
AVAILABLE
SIZE
FORMAT
STATUS
sync
VMware-tools-windows-8.3.2-257589.iso
24m 54s
48.43MB
ISO 9660 CD-ROM filesystem data 'VMware Tools'
Allowed
Checksum
Rows per page:
10
1–1 of 1

Configuration

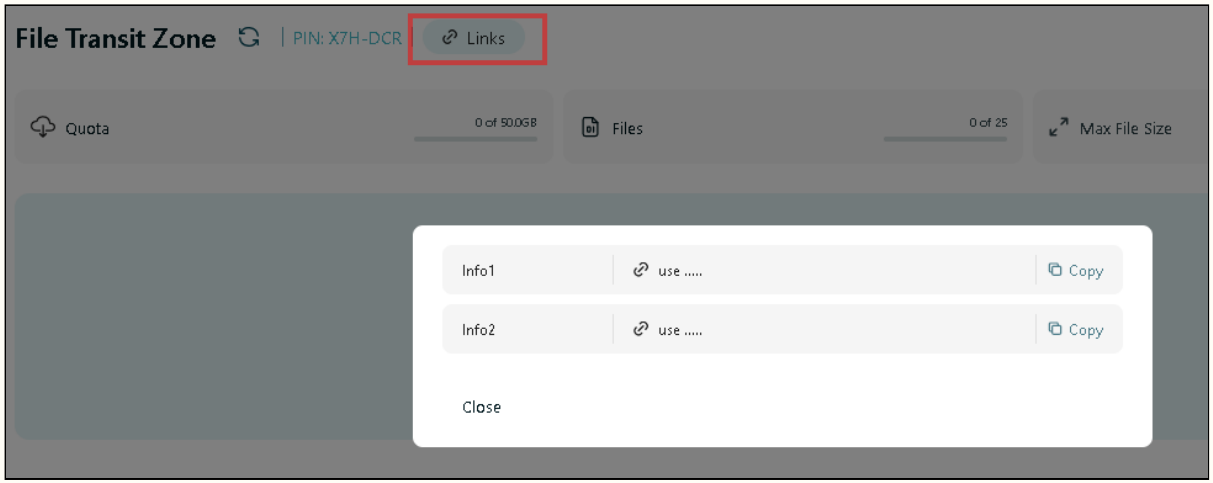
Enable the File Exchange service

```
visulox config -name layout.<logical server name>.fileexchange=true
visulox restart -service monitor
```

File Exchange URL

The transit URL must be known by the File Exchange users and is displayed via the **Links** button in Workspace / Transit Zone.
The transit URLs can be entered with the following configuration parameter:

```
visulox config -name transit.info.0="File Exchange URL:https\://%HOST%\:%SSLPORT%/transitloginpage?fxpin=%PIN%"
```



To change the **transit.url.info.x** entry it is necessary to use a **backslash** "\" before the "**:**" **within the URL,** because "**:**" is used as delimiter.

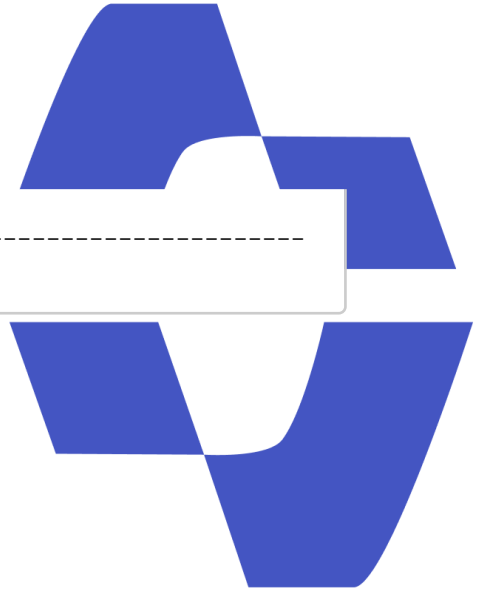
Format of the configuration value

The value has two elements: the name, which is displayed in the selection dialog and the value of the clipboard. Both elements can have place holders.

Placeholders	Used in	Description
%NODE%	name	Name of the node, where the File Transfer GUI is running
%HOST%	value	Physical FQDN hostname
%HOSTSHORT%	value	Short hostname
%PINFMT$	value	Formated PIN
%PIN%	value	RAW format of the PIN
%PORT%	value	The unsecure port (if used)
%SSLPORT%	value	The SSL port
%OWNER%	value	Owner of the session
%OWNERID%	value	Owner ID
%OWNERSHORT%	value	Short form of the owner

More configuration options

```
visulox config -name fileexchange. -info


--------------------------------------------------------------------------------------------------------------------------------
----------
    | changed | key                     | value                         |                            shortinfo |
 defaultvalue |

--------------------------------------------------------------------------------------------------------------------------------
----------
    |         | fileexchange.accesslog  |                               |                            accesslog |
            |
    |         | fileexchange.banner     | %LICENSE%                     |     Banner line on fileexchange page |
  %LICENSE% |
    |         | fileexchange.cafile     |                               |               CA for transit service |
            |
    |         | fileexchange.certfile   | visulox.self.pem              |     ssl certfile for transit service |
 visulox.self.pem |
    |         | fileexchange.connection | From %RIP% on %NODE% (%HOST%) | Connection line on fileexchange page | From %RIP% on
%NODE% (%HOST%) |
    |         | fileexchange.interface  | 0.0.0.0                       |    interface for incomming requestes |
    0.0.0.0 |
    |         | fileexchange.keyfile    | visulox.self.key              |      ssl keyfile for transit service |
 visulox.self.key |
    |         | fileexchange.port       |                               |                  the listening ports |
            |
    |         | fileexchange.sslport    | 1443                          |                  the listening ports |
       1443 |
```



File Transfer features

Overview

- Overview
- The File Transfer modules
- Status of the transferred files
- Related articles

The File Transfer modules

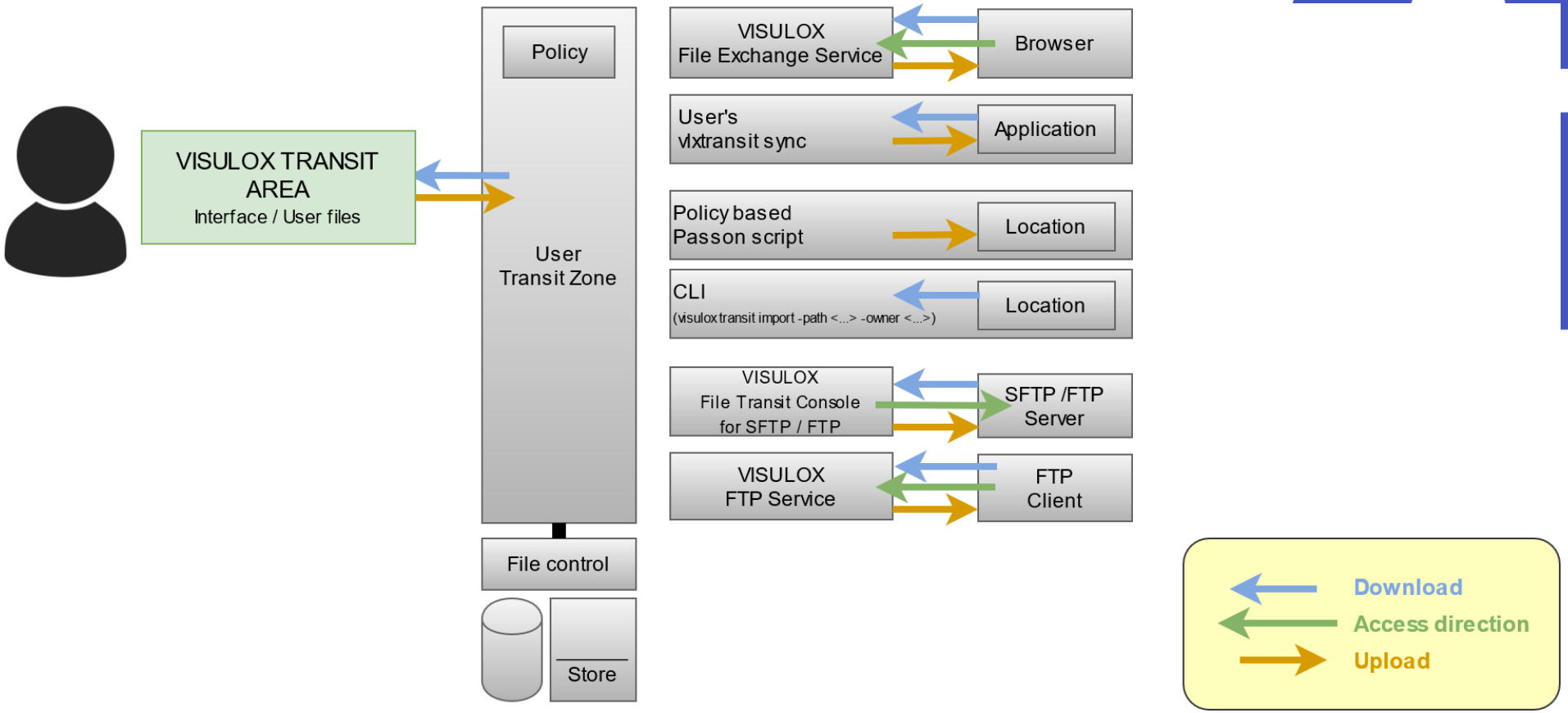
The modules provide access to the Transit Zone. There are several File Transfer modules, each providing a connection to the Transit Zone:

Module	Description
Transit Web in Workspace	File Transfer interface is presented in the user`s Workspace. The user can upload or download files from his client into the Transit Zone
File Exchange	The user can connect to every VISULOX Node, using the internal WEB browser and a known URL. The WEB Access PIN is needed to see the Transit Zone. Now the user is able to upload and download files from the Transit Zone. (⚠ The File Exchange service has to be enabled by the administrator).

Module	Description
Sync	Depending on the configuration, the user has a local directory, where he has direct access to the Transit Zone. All applications with **visulox.exp, vlxUnix.exp** and **vlxWindows.exp** (former: vlxRdp.exp**)** will get the VISULOX Transit Zone with **vlxMode=SYNC** set. On VISULOX Nodes wiithout VISULOX PORTAL Service, the replication has to be set at least to **ftonly**. **sshfs** must be installable. For OL 8 use "Oracle Linux 8 CodeReady Builder (x86_64) - Unsupported" as repository.
Passon script / CLI (automated transfer)	Users are able to upload into the Transit Zone. Depending on the user, file name or file type these files can be passed on automatically to another location via script. It is also possible to copy a file into the Transit Zone of another user via VISULOX transit command line interface. (See also: Automated transfer of files into Transit Zone (Passon))
File Transit Client SFTP/FTP	Interface to interact between the Transit Zone and an SFTP/FTP endpoint. This allows to connect to a server using SFTP, FTP passive or FTP active protocol. Depending on the policy, the user gets a list of hosts he can connect to or he is able to configure his own host list for File Transfer.
FTP Service	Interface to interact between a application server side FTP client with the Transit Zone. (⚠ The FTP service has to be enabled , before FTP Service can be used).

Also have a look at the User Guide: (4.3.3) File Transfer modules

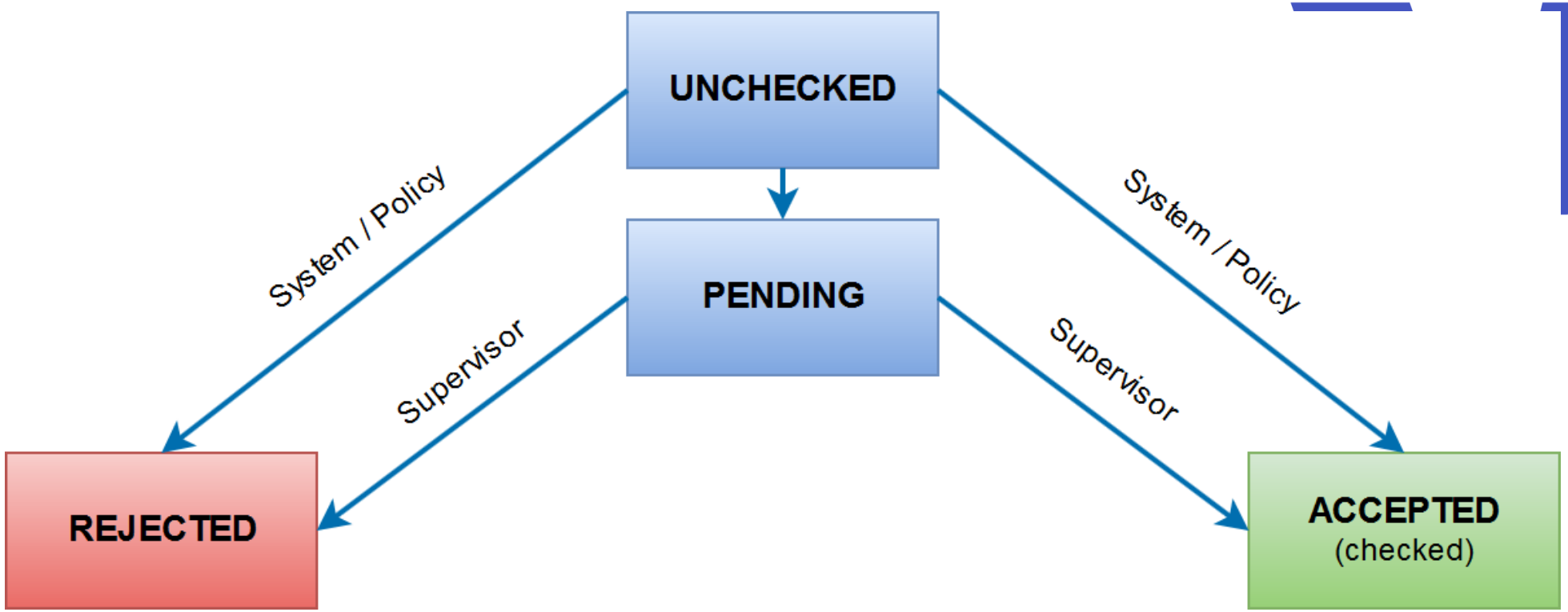
⚠ To display the checksum of transferred files in the File Transfer interface in the user's Workspace it is necessary to install rhash, which is available in the Epel repository.



Status of the transferred files

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

A file in the Transit Zone can have several states:



State	Description
unchecked	If a file is inserted into the file store, it is set to unchecked and the background task is informed to check the file
pending	If the File Transfer Policy detects a file pattern, where the file type needs approval, the file is marked as "Needs approval". Using the Cockpit a supervisor can "approve" or "reject" this file for the user.
rejected	If the system rejects the file, there are several reasons: ▪ File is too big ▪ Quota of the Transit Zone is reached ▪ The file contains a virus ▪ File pattern rule rejects the file, e.g. it is not allowed to handle executable files
checked or approved	The file is checked and can be used by the user internally or externally

A file can be deleted manually by the user to gain more free diskspace, when his quota is reached. Also the files will be deleted automatically, if the lifetime in the Transit Zone is reached.

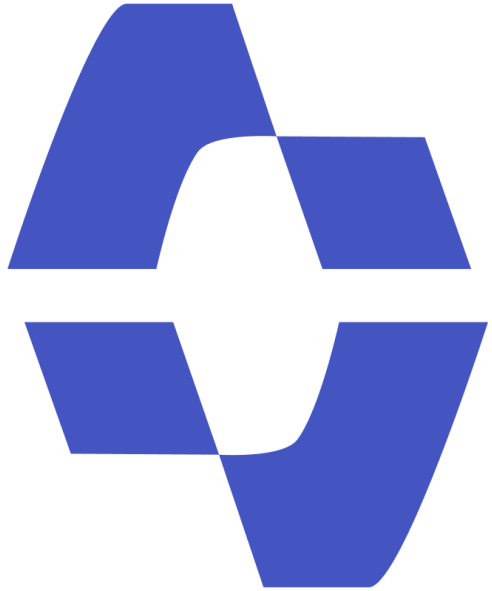
Related articles

(4.2.0) VISULOX File Transit and Sophos Endpoint Security and Control

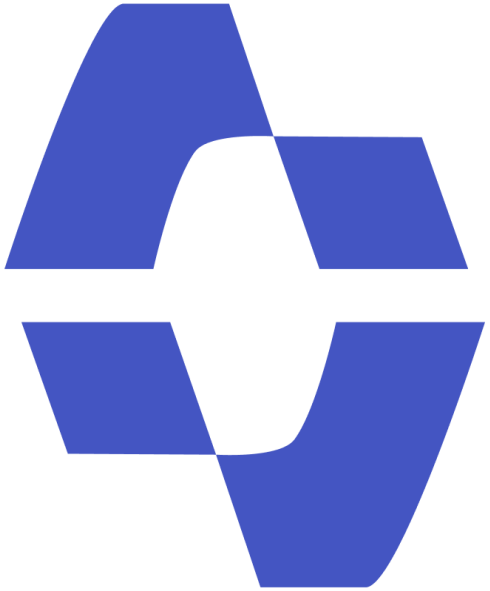
(4.2.0) How to discard filetypes from the Transit Zone synchronisation

(4.2.0) Configuration of File Transfer in the VISULOX Cockpit

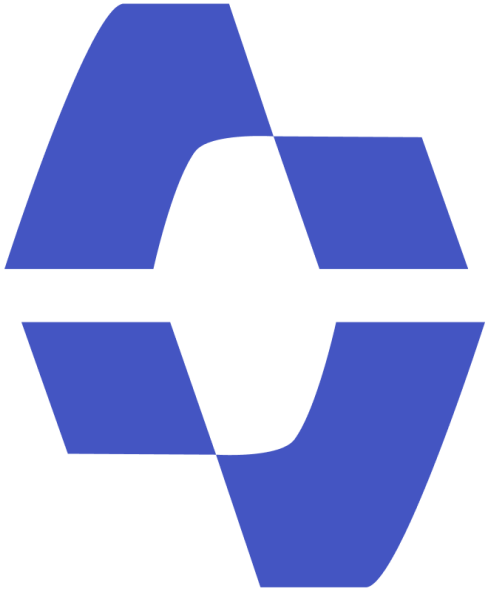
(4.2.0) File Transfer



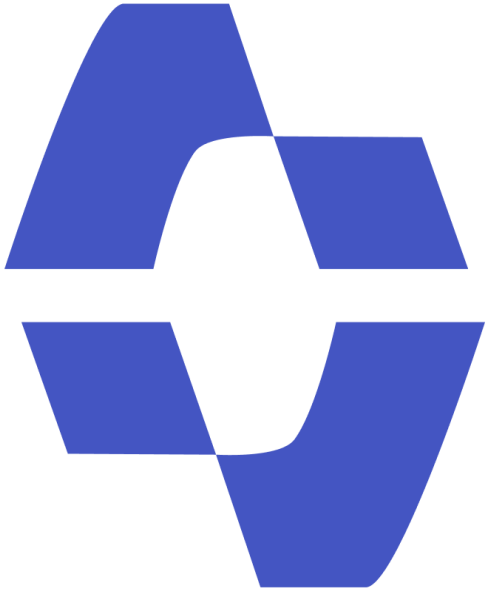
(4.2.0) File Transfer modules
(4.2.0) Command Connect / Guard and FT Client with empty filters
(4.2.0) VISULOX4_FileTransfer_(VFT)
(4.2.0) Accessing the File Exchange web page
(4.2.0) VISULOX Transit Mapping and Ubuntu application servers
(4.2.0) Automated transfer of files into Transit Zone (Passon)
(4.2.0) VISULOX FTP Service
(4.2.0) File Transfer recommendations
(4.2.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.2.0) How to control FT Client from the command line
(4.2.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.2.0) How to configure File Transfer content check
(4.2.0) Object ID
(4.2.0) Transit Policy
(4.2.0) Allowing File Transfer from internal to internal
(4.2.0) Transit script variables
(4.2.0) File Transfer features
(4.2.0) Custom vlxuser ID for transit users
(4.2.0) File Transfer via command line
(4.2.0) File Transit with approval
(4.2.0) How to control File Transit Policy from the command line
(4.2.0) Extended Transit Policy with hash check by provided hash file



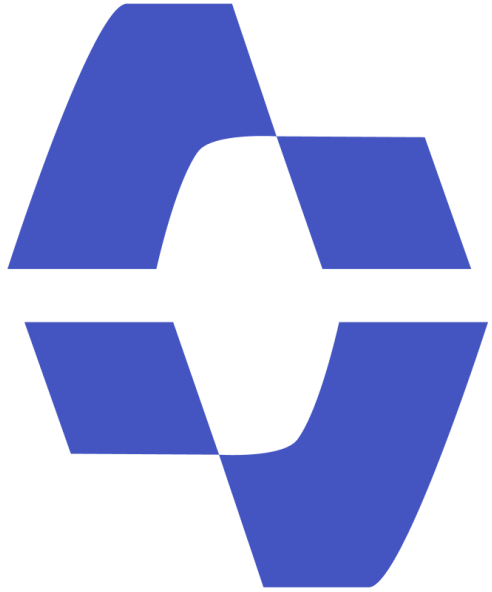
(4.2.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.2.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.2.0) VISULOX Transit mapping
(4.3.2) VISULOX FTP Service
(4.3.2) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.2) Command Connect / Guard and FT Client with empty filters
(4.3.2) Custom vlxuser ID for transit users
(4.3.2) Transit Policy
(4.3.2) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.2) How to control File Transit Policy from the command line
(4.3.2) File Transfer via command line
(4.3.2) File Transfer
(4.3.2) Object ID
(4.3.2) VISULOX4_FileTransfer_(VFT)
(4.3.2) How to control FT Client from the command line
(4.3.2) Accessing the File Exchange web page
(4.3.2) Configuration of File Transfer in the VISULOX Cockpit
(4.3.2) File Transfer recommendations
(4.3.2) Automated transfer of files into Transit Zone (Passon)
(4.3.2) File Transit with approval
(4.3.2) VISULOX Transit Mapping and Ubuntu application servers
(4.3.2) How to attach Chrome/Chromium download directory to vlxtransit



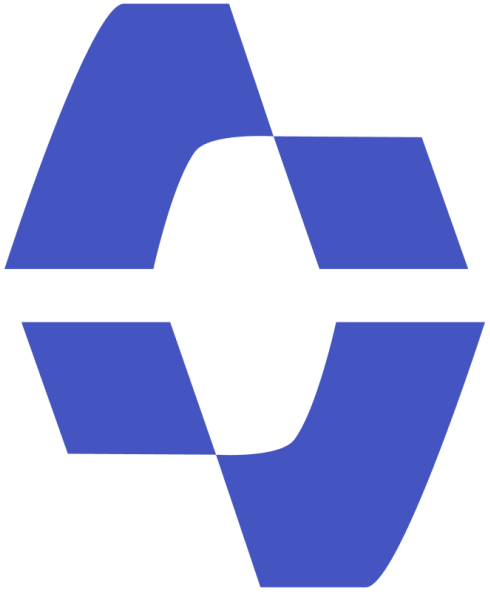
(4.3.2) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.2) File Transfer features
(4.3.2) Transit script variables
(4.3.2) Extended Transit Policy with hash check by provided hash file
(4.3.2) How to discard filetypes from the Transit Zone synchronisation
(4.3.2) File Transfer modules
(4.3.2) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.2) How to configure File Transfer content check
(4.3.2) Allowing File Transfer from internal to internal
(4.3.2) VISULOX Transit mapping
(4.1.1) VISULOX File Transit and Sophos Endpoint Security and Control
(4.1.1) Transit script variables
(4.1.1) VISULOX FTP Service
(4.1.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.1.1) Object ID
(4.1.1) Automated transfer of files into Transit Zone (Passon)
(4.1.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.1.1) How to control FT Client from the command line
(4.1.1) How to configure File Transfer content check
(4.1.1) File Transit with approval
(4.1.1) VISULOX Transit mapping
(4.1.1) Extended Transit Policy with hash check by provided hash file



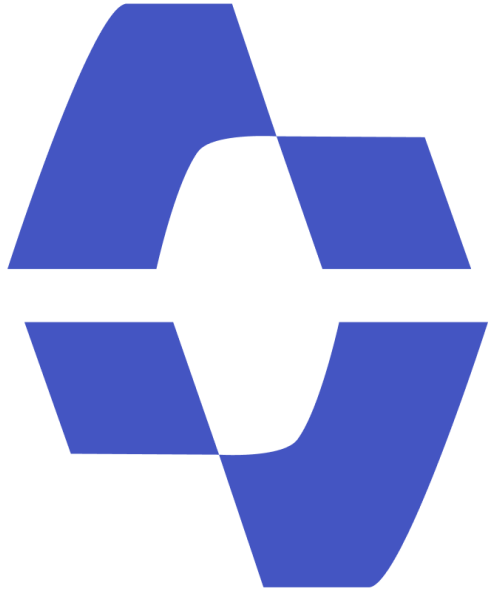
(4.1.1) Allowing File Transfer from internal to internal
(4.1.1) File Transfer modules
(4.1.1) File Transfer recommendations
(4.1.1) File Transfer features
(4.1.1) How to attach Chrome/Chromium download directory to vlxtransit
(4.1.1) How to control File Transit Policy from the command line
(4.1.1) Configuration of File Transfer in the VISULOX Cockpit
(4.1.1) File Transfer via command line
(4.1.1) File Transfer
(4.1.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.1.1) Command Connect / Guard and FT Client with empty filters
(4.1.1) VISULOX4_FileTransfer_(VFT)
(4.1.1) Accessing the File Exchange web page
(4.1.1) Custom vlxuser ID for transit users
(4.1.1) VISULOX Transit Mapping and Ubuntu application servers
(4.1.1) Transit Policy
(4.1.1) How to discard filetypes from the Transit Zone synchronisation
(4.3.1) File Transfer features
(4.3.1) File Transit with approval
(4.3.1) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.1) Configuration of File Transfer in the VISULOX Cockpit
(4.3.1) VISULOX FTP Service



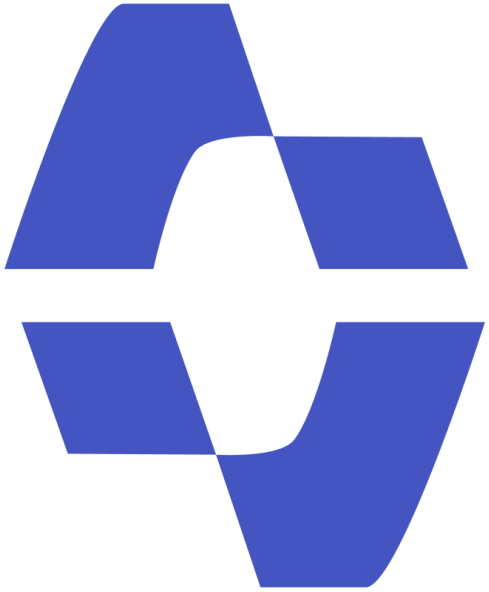
(4.3.1) Command Connect / Guard and FT Client with empty filters
(4.3.1) Extended Transit Policy with hash check by provided hash file
(4.3.1) How to control File Transit Policy from the command line
(4.3.1) File Transfer via command line
(4.3.1) Automated transfer of files into Transit Zone (Passon)
(4.3.1) Transit Policy
(4.3.1) How to discard filetypes from the Transit Zone synchronisation
(4.3.1) File Transfer
(4.3.1) How to configure File Transfer content check
(4.3.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.1) VISULOX4_FileTransfer_(VFT)
(4.3.1) Custom vlxuser ID for transit users
(4.3.1) Transit script variables
(4.3.1) File Transfer modules
(4.3.1) File Transfer recommendations
(4.3.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.1) Accessing the File Exchange web page
(4.3.1) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.1) Object ID
(4.3.1) VISULOX Transit Mapping and Ubuntu application servers
(4.3.1) VISULOX Transit mapping
(4.3.1) How to control FT Client from the command line



(4.3.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.1) Allowing File Transfer from internal to internal
(4.3.0) How to control File Transit Policy from the command line
(4.3.0) Automated transfer of files into Transit Zone (Passon)
(4.3.0) VISULOX FTP Service
(4.3.0) Accessing the File Exchange web page
(4.3.0) File Transit with approval
(4.3.0) Allowing File Transfer from internal to internal
(4.3.0) How to control FT Client from the command line
(4.3.0) VISULOX Transit Mapping and Ubuntu application servers
(4.3.0) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.0) File Transfer modules
(4.3.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.0) How to configure File Transfer content check
(4.3.0) Extended Transit Policy with hash check by provided hash file
(4.3.0) Transit script variables
(4.3.0) Command Connect / Guard and FT Client with empty filters
(4.3.0) File Transfer features
(4.3.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.0) VISULOX4_FileTransfer_(VFT)
(4.3.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.0) Custom vlxuser ID for transit users



(4.3.0) Object ID
(4.3.0) Configuration of File Transfer in the VISULOX Cockpit
(4.3.0) File Transfer via command line
(4.3.0) How to discard filetypes from the Transit Zone synchronisation
(4.3.0) File Transfer
(4.3.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.0) Transit Policy
(4.3.0) File Transfer recommendations
(4.3.0) VISULOX Transit mapping
VISULOX4_FileTransfer_(VFT)
File Transfer modules
How to attach Chrome/Chromium download directory to vlxtransit
Custom vlxuser ID for transit users
Object ID
File Transit with approval
Extended Transit Policy with hash check by provided hash file
VISULOX Transit Mapping and Ubuntu application servers
VISULOX Transit mapping
File Transfer via command line
Automated transfer of files into Transit Zone (Passon)
Allowing File Transfer from internal to internal
How to discard filetypes from the Transit Zone synchronisation



How to control FT Client from the command line

Configuration of File Transfer in the VISULOX Cockpit

How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service

VISULOX File Transit and Sophos Endpoint Security and Control

Transit script variables

VISULOX FTP Service

How to configure File Transfer content check

File Transfer recommendations

File Transfer features

Accessing the File Exchange web page

File Transfer

Command Connect / Guard and FT Client with empty filters

How to use SSH-Keys within Command Connect / Guard and FT Client

VISULOX addon command line interface (CMD Connect / Guard, etc)

How to control File Transit Policy from the command line

Transit Policy

VISULOX Transit mapping

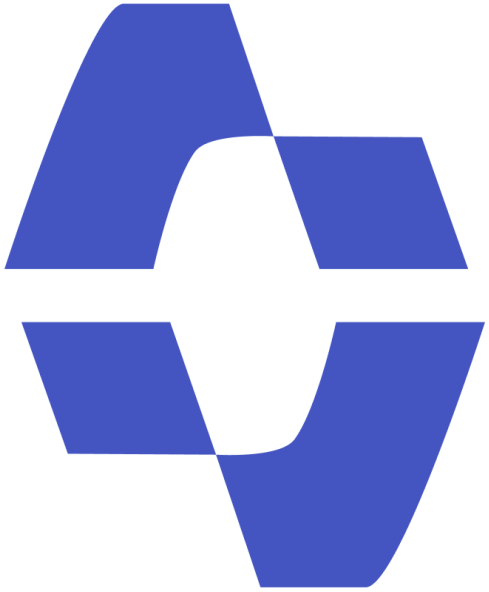
VISULOX File Transit and Sophos Endpoint Security and Control

Transit Policy

Transit script variables

File Transfer features

How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service



How to use SSH-Keys within Command Connect / Guard and FT Client
Extended Transit Policy with hash check by provided hash file
(4.3.3) File Transfer modules
VISULOX FTP Service
Configuration of File Transfer in the VISULOX Cockpit
Custom vlxuser ID for transit users
VISULOX addon command line interface (CMD Connect / Guard, etc)
File Transit with approval
Command Connect / Guard and FT Client with empty filters
How to control File Transit Policy from the command line
How to control FT Client from the command line
How to configure File Transfer content check
Object ID
File Transfer via command line
How to discard filetypes from the Transit Zone synchronisation
File Transfer
Allowing File Transfer from internal to internal
(4.3.3) VISULOX4_FileTransfer_(VFT)
Accessing the File Exchange web page
VISULOX Transit Mapping and Ubuntu application servers
Automated transfer of files into Transit Zone (Passon)
File Transfer recommendations

File Transfer recommendations

- Keep provided quota low
- Keep size per file low
- Keep life time per file low in the Transit Zone

The Transit Zone has to be used by the user to transfer files from A to B. It should not be abused as a "store". This is not the service of the Transit Zone.

Housekeeping in the Transit Zone is not done by users. Users will keep anything as long as possible. Many files and directories or huge files will have an impact on the usability for the users and the whole VISULOX Node.

⚠ Symbolic links are displayed in FT Client but cannot be processed any further.

⚠ If **autofs** is used wiith **transit mapping**, Selinux has to be disabled

How to configure File Transfer content check

Introduction

Path to the content check script: **/opt/visulox/tools/filecheck.sh**

After installation there is no filecheck.sh file available.
There is a template file: **/opt/visulox/tools/filecheck.sh.template**

This script has to be adjusted and can be used together with an external command line virus scanner.

Permission of this file must be **vlx/vlxgroup/0550**.

Possible products for Linux are **F-Secure Command Line Scanner, F-Prot Antivirus, ClamAV,** etc.
(no warranty for operation by amitego engineering).

> In the Transit Policy file check can be enabled/disabled for certain files/users and additional script arguments can be set for the file check script.

- Introduction
- File Transfer content check template
  - filecheck.sh.template
- Example for F-Secure
  - F-Secure
- Example for F-Prot Antivirus
  - F-Prot
- Example for Microsoft Defender

File Transfer content check template

filecheck.sh.template

```
#!/bin/bash
#########################################################################
#  Copyright (c) amitego engineering GmbH, www.amitego.com
#########################################################################
#
# Copy this file to filecheck.sh, set permission to vlx:vlxgroup:440
# modify for your purpose
#
```

```
# This is the content filtering script for File Transfer by VISULOX.
#
# This script is used for the connection to a virus-scanner to scan the file.
#
# On stdout a text can be displayed, which is used as the "description text".
# Return code: OK == 0 /  ERROR CODE

# If the file contains "THIS IS A VISULOX TEST" the script is triggered (for testing purpos)

# Echo of result on stdout
grep "THIS IS A VISULOX TEST" $1 && echo ": VIRUS TEST"  && exit 1

echo "Check on $*"
true
exit $?
```

⚠ Splitted archives are not supported in Sophos AntiVirus!

Example for F-Secure

F-Secure

```
 #!/bin/bash
#########################################################################
#  Copyright (c) amitego engineering GmbH, www.amitego.com
#########################################################################
#
# Copy this file to filecheck.sh, set permission to vlx:vlxgroup:440
# modify for your purpuse
#
# This is the content filtering script for File Transfer by VISULOX.
#
# This script is used for the connection to a virus-scanner to scan the file.
```

```
#
# On stdout a text can be displayed, which is used as the "description text".
# Return code: OK == 0 /  ERROR CODE

# if the file contains "THIS IS A VISULOX TEST" the script trigger (for testing purpos)

# Echo of result on stdout
#grep "THIS IS A VISULOX TEST" $1 && echo ": VIRUS TEST"  && exit 1

#echo "Check on $*"
of1=/tmp/ana1-$$
of2=/tmp/ana2_$$

IFS="
"
fsav $* 2>/dev/null > $of1
return=$?

# Analyse the output
grep  "file i" $of1 > $of2
egrep -o '.+' $of2 || cat $of2

rm $of1 $of2

exit $return
```

Example for F-Prot Antivirus

F-Prot

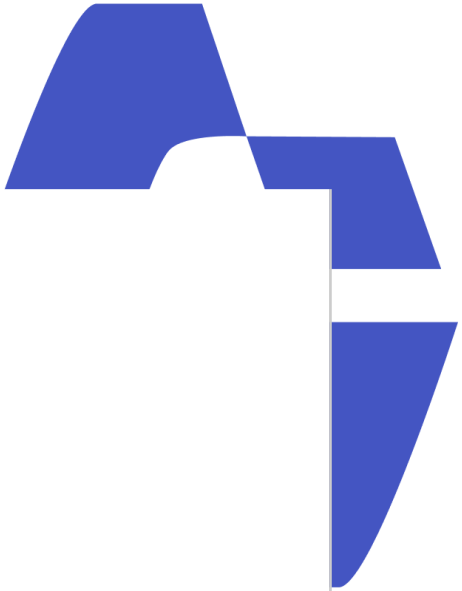
```
#!/bin/bash
```

```
#########################################################################
#  Copyright (c) amitego engineering GmbH, www.amitego.com
#########################################################################
#
# Copy this file to filecheck.sh, set permission to vlx:vlxgroup:440
# modify for your purpuse
#
# This is the content filtering script for File Transfer by VISULOX.
#
# This script is used for the connection to a virus-scanner to scan the file.
#
# On stdout a text can be displayed, which is used as the "description text".
# Return code: OK == 0 /  ERROR CODE

# if the file contains "THIS IS A VISULOX TEST" the script trigger (for testing purpos)

# Echo of result on stdout

# echo "Check on $*"
of1=/tmp/ana1-$$
of2=/tmp/ana2_$$

IFS="
"
/opt/f-prot/fpscan --report $* 2>/dev/null > $of1
return=$?

# Analyse the output
grep  "Found virus" $of1 > $of2
egrep -o '<.+>' $of2 || cat $of2

rm $of1 $of2
```

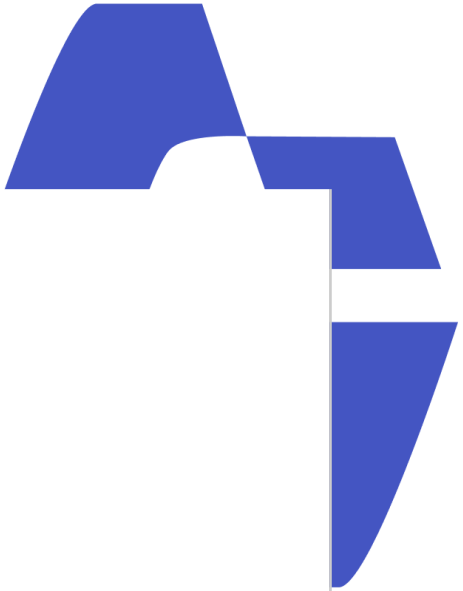
```
exit $return
```

Example for Microsoft Defender

```
##########################################################################
#  Copyright (c) amitego engineering GmbH, www.amitego.com
##########################################################################
#

# ###############################################
# Microsoft Defender for Endpoint on Linux
# ###############################################

# \
        .  $(dirname $0)/../etc/vlx.profile
# \
        exec tclsh "$0" "$@"

package require Command
package require Tclx

set ::SCANNER /usr/bin/mdatp
set ::SCANOPTION {scan custom --path}

#set ::SCANNER /usr/bin/cat
#set ::SCANOPTION {}

############################
proc main {} {
    set rtn $::ExitCode::SOFTWARE
    Logger::install virsuscheck
    set file [lindex $::argv 0]
    log::debug start $file
```



```
    try {
        check $file beforscan
        scanner
        set answer [scan $file]
        if {$answer ne ""} {
            # remove provided file pattern from answer
            regsub -- $file $answer "CONTENT:" answer
            puts $answer
            set rtn $::ExitCode::DENYVIRUS
        } else {
            set rtn $::ExitCode::SUCCESS
        }

        check $file afterscan

    } trap {CLI} {e} {
        log:::error "SOFTWARE" e
        puts $e
        set rtn $::ExitCode::FAILURE
    } on error {e o} {
        puts "General error"
        log:::error "SOFTWARE" e o
    }
    return $rtn
}
############################
proc scanner {} {
    if {![file executable $::SCANNER]} {
        return -code error -errorcode {CLI} "$::SCANNER not found"
    }
}
############################
proc check {file text } {
    if {![file exists $file]} {
```



```
        return -code error -errorcode {CLI} "Scanfile not found $text"
    }
    if {![file readable $file]} {
        return -code error -errorcode {CLI} "Scanfile not readable $text"
    }
}
############################
proc scan {file} {
    set answer ""

    catch { exec $::SCANNER {*}$::SCANOPTION $file } scanData

    foreach line [split $scanData \n] {
        if {[regexp -nocase --  {Password} $line ]} {
            lappend viruslist "Password protected"
        }
        if {[regexp -nocase -- {Name: (.*)} $line dy virusname]} {
            lappend viruslist [string trim $virusname \']
        }
    }
    if {[info exists viruslist]} {
        set answer [join [lrmdups $viruslist] ,]
    }

    return $answer
}
############################
exit [main]
```

VISULOX FTP Service

Overview

VISULOX provides a classic FTP server, which is connected to the File Transit Zone.

- Overview
- Usage
- Configuration
- Connection with an FTP client
    - List of tested FTP clients

Usage

If users have to use an FTP client to up- and download files via the application service, this service has to be enabled.

If enabled, the user can connect the VISULOX Node with an FTP client, where the VISULOX FTP Service is enabled.

The user is prompted for his username and a password.

The password is always the user's Transit PIN, which is provided to him either on the Transit Web Page or in the Transit Console.

The username can be <loginuser> <email> <mobile> <surname> <common name>.

Configuration

Enabling the FTP Service:

```
visulox config -name layout.<logical server name>.ftpd=true
visulox restart -service monitor
```

Adjusting the scanning definition of the file list command in **/opt/visulox/lib/ft/ftregex.tcl:**

```
# This file holds the scanning definition from the file list command.
# Each server has a different way to present filename, filetime and filesize
```

```
# via a curl.
# 1: scanning result
# 2: regex for scaning
# 3: order of the resulting elements size,date,name
#
################ STANDARD LINUX ######################
lappend ::curl::regdef {isdirectory
                {^d.{9} +[0-9]+ +[^ ]+ +[^ ]+ +([0-9]+) +([A-z]{3} [ 0-9]{2} [0-9]{2}:[0-9]{2}|[A-z]{3} [ 0-9]{2}  [0-9]{4}) (.+)
$}
                {size date name}
}
# standard linux file
lappend ::curl::regdef {isfile
                {^-.{9} +[0-9]+ +[^ ]+ +[^ ]+ +([0-9]+) +([A-z]{3} [ 0-9]{2} [0-9]{2}:[0-9]{2}|[A-z]{3} [ 0-9]{2}  [0-9]{4}) (.+)
$}
                {size date name}
}
# standard linux symlink
lappend ::curl::regdef {islink
                {^l.{9} +[0-9]+ +[^ ]+ +[^ ]+ +([0-9]+) +([A-z]{3} [ 0-9]{2} [0-9]{2}:[0-9]{2}|[A-z]{3} [ 0-9]{2}  [0-9]{4}) (.+)
$}
                {size date name}
}
################ STANDARD WINDOWS ######################
lappend ::curl::regdef {isdirectory
                {^([0-9]{2}-[0-9]{2}-[0-9]{2}  [0-9]{2}:[0-9]{2}..) +(<DIR>) +(.+)$}
                {date size name}
}
lappend ::curl::regdef {isfile
                {^([0-9]{2}-[0-9]{2}-[0-9]{2}  [0-9]{2}:[0-9]{2}..) +([0-9]+) +(.+)$}
                {date size name}
}
```

```
visulox config list -name ftp
```

```
| ftpd.banner  | OPERATION | VISULOX FTP Server: to login with username/pin. You will find your pin in your T ... |
| ftpd.servers | OPERATION | .+                                                                                   ... |
-----------------------------------------------------------------------------------------------------------------------
```

The VISULOX FTP Service will be started, if the server is in the list of **ftpd.servers**. This field is a regular expression.

.+	On any VISULOX node
<server1>|<server2>	On server 1 and server 2
<server>[1-5]+ftp	On server1ftp to server5ftp

Connection with an FTP client

List of tested FTP clients

- Command line client
- MobaXterm

After connecting with a FTP client, only a view commands are available or making sense:

```
dir / nlist / ascii / binary / passive / get / mget / put / mput
```

In the directory list additionally the filename, filesize, filetime, file source and the file type is displayed.

File source is from where the file in the Transit Zone was transferred (via Workspace (user), File Exchange, FTP, ...). The file status can be unchecked, checked, pending, rejected or approved.

The FTP server takes care about the File Transfer Policy. This means the direction and the parameters of the files are under control.

Transit script variables

On each import into the Transit Zone, the event script assigned to the matching policy is triggered.
On import from the user side into the Transit Zone more than one policy can match.
Then the assigned script is triggered for each policy.

The following script variables are available in all scripts related to File Transit:

```
File:  %VLXFILENAME%
Sign:  %VLXFILETYPE%
Size:  %VLXFILESIZE_FMT%
Hashs: %VLXFILEHASHS%
```

Event script variables

Script variables

```
 VLXACCESSPOINT  = <Access-URL>
   VLXCREATETIME = 1298913407
        VLXEMAIL = <User-eMail-address>
    VLXEVENTINFO = tzimport
     VLXFULLNAME = <Username>
    VLXGROUPLIST = {DC=de/DC=tbsol/OU=ToolBox/OU=Worker/CN=<Username>} CN=Office-IAS,OU=Applikation,OU=ToolBox,DC=tbsol,DC=de
CN=Office-WTS,OU=Applikation,OU=ToolBox,DC=tbsol,DC=de
```

```
          VLXLANG = en
      VLXLISTHASH = 437EE5E4387545EA96C1D053FE463298
           VLXLOG = /vsx30/var/log
     VLXLOGINUSER = <Loginname>
       VLXMANAGER = CN=<Supervisor-name>,OU=Worker,OU=ToolBox,DC=tbsol,DC=de
        VLXOBJECT = cfossil.sh
         VLXOWNER = CN=<Username>,OU=Worker,OU=ToolBox,DC=tbsol,DC=de
       VLXOWNERID = A11E4B272716B5EB14632E86B1184BF1
    VLXOWNERSHORT = <Username>
          VLXPATH = /vsx30
         VLXPOLICY = AAP12
VLXPOLICYCOMMENT = This is the Policy Comment. edittest
     VLXRECIPIENT = <eMail-address>
      VLXREMOTEIP = 172.16.21.33
    VLXREPOSITORY = TESTAD
   VLXSESSIONHOST = vTABOL6U4SGD1510
           VLXSMS = <SMS-number>
       VLXSURNAME = <User-surname>
   VLXUSERPROFILE = DC=de/DC=tbsol/OU=ToolBox/OU=Worker/CN=<Username>
          VLXUTIL = /vsx30/lib/utils
    VLXWEBTOPBASE = https://<hostname>.tbsol.de:443/sgd
```

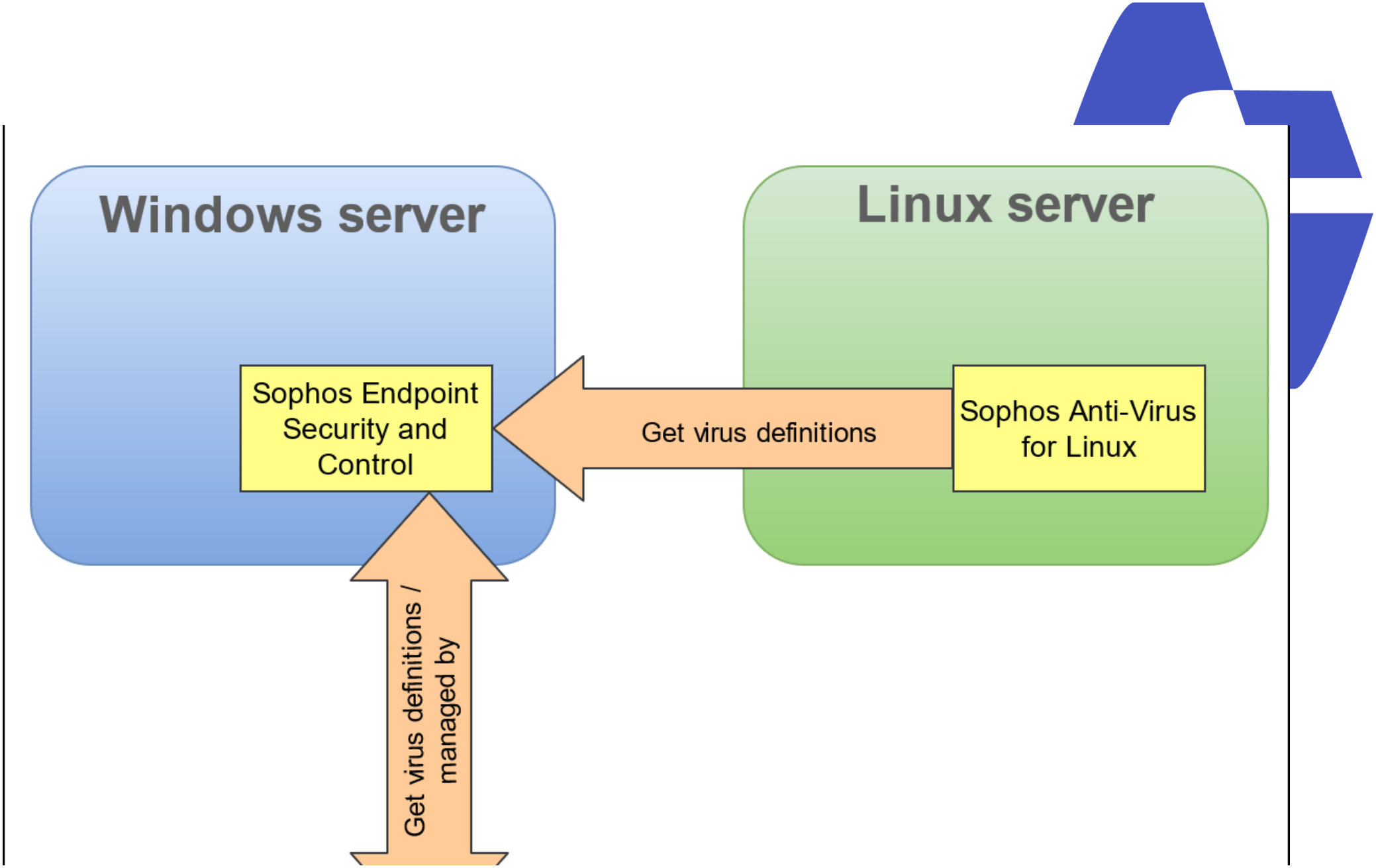
Approval: accept or reject

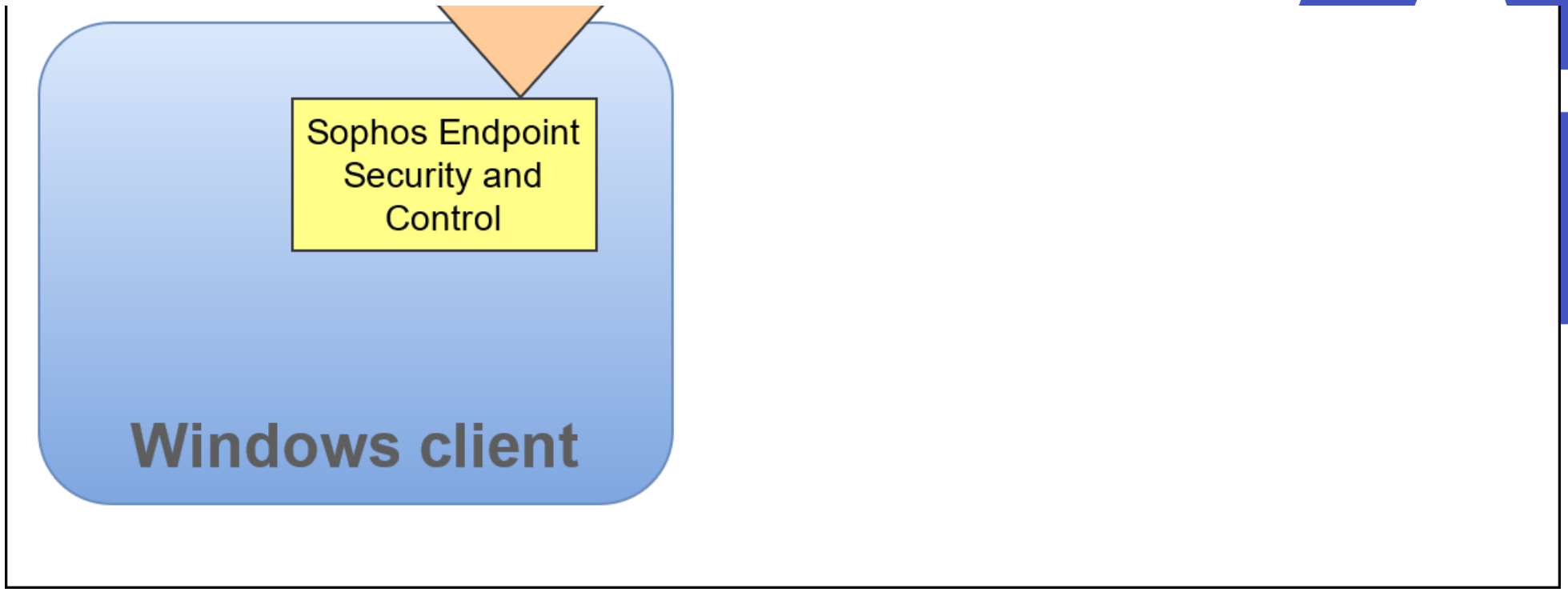
```
    VLXAPPROVALMODE = approved
      VLXAPPROVEDBY = CN=<Username>,OU=Worker,OU=ToolBox,DC=tbsol,DC=de
VLXAPPROVEDBYEMAIL = <eMail-address>
   VLXAPPROVEDBYSMS = <SMS-number>
      VLXCREATETIME = 1459843544
           VLXEMAIL = <eMail-address>
           VLXEVENT = approved
       VLXEVENTINFO = asdAASAS
```

```
      VLXGROUPLIST = {DC=de/DC=tbsol/OU=ToolBox/OU=Worker/CN=<Username>} CN=Office-IAS,OU=Applikation,OU=ToolBox,DC=tbsol,DC=de
CN=Office-WTS,OU=Applikation,OU=ToolBox,DC=tbsol,DC=de
            VLXLOG = /vsx30/var/log
        VLXMANAGER = CN=<Supervisor-name>,OU=Worker,OU=ToolBox,DC=tbsol,DC=de
         VLXOBJECT = cfossil.sh
          VLXOWNER = CN=<Username>,OU=Worker,OU=ToolBox,DC=tbsol,DC=de
     VLXOWNERSHORT = <Username>
           VLXPATH = /vsx30
         VLXPOLICY = AAP12
  VLXPOLICYCOMMENT = This is the Policy Comment. edittest
      VLXRECIPIENT = <eMail-address>
       VLXREMOTEIP = <IP-address>
            VLXSMS = <SMS-number>
           VLXUTIL = /vsx30/lib/utils
```

VISULOX File Transit and Sophos Endpoint Security and Control

Overview


Windows server
Linux server
Sophos Endpoint Security and Control
Get virus definitions
Sophos Anti-Virus for Linux
Get virus definitions / managed by



The Sophos Endpoint Security and Control product can be Installed on a Windows server. On a Linux server Sophos Anti-Virus for Linux (SAVL) is needed.

SAVL can now use the Windows server to update the local virus definitions. If no Windows server should be used, SAVL can get the definitions directly from Sophos itself.

To check a file the local SAVL check program is called. Based on the return code, the file is released or in quarantine.

Installation

If the product is bought or a trial version is connected to the MySophos account, the installation guide for Sophos Anti-Virus for Linux can be found on the MySophos website.

tbsSophos.sh

```
#!/bin/bash
name=`basename "$1"`
# Return value
rtn=0

scanresult=`/opt/sophos-av/bin/savscan -ss -archive $1`
# catch the error NOW !!
if [ "$?" != "0" ]; then
    rtn=1
fi
out=$(echo $scanresult | sed "s/.*Virus '\([^']*\)'.*/\1/")
echo "Virus $out"
exit $rtn
```

How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service

The File Exchange service is enabled by setting the layout in configuration**:**

```
visulox config -name layout*fileexchange
    ------------------------------------------------------
    | changed | key                                | value |
    ------------------------------------------------------
    |         | layout.<log_nodename>.fileexchange | false |
    ------------------------------------------------------
```

This service needs SSL certifcates, which are available on VISULOX Nodes. These certificates are copied during installation into **/opt/visulox/etc/ssl**.

The certifcate names can be configured:

visulox config list -name cert

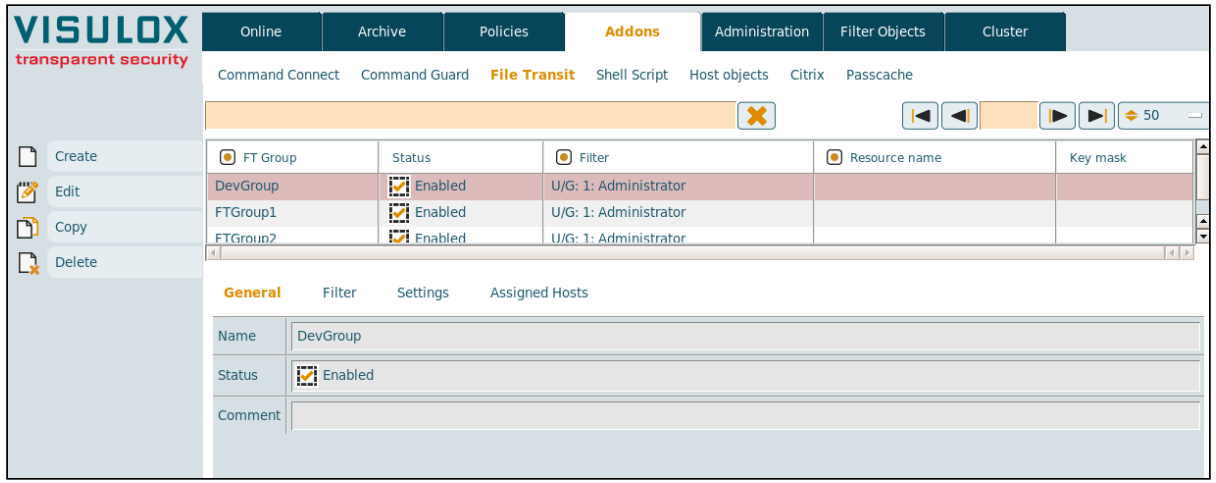
```
-------------------------------------------------------
| changed | key                   | value            |
-------------------------------------------------------
|         | fileexchange.certfile | visulox.self.pem |
|         | webservice.certfile   | visulox.self.pem |
-------------------------------------------------------
```

Related articles

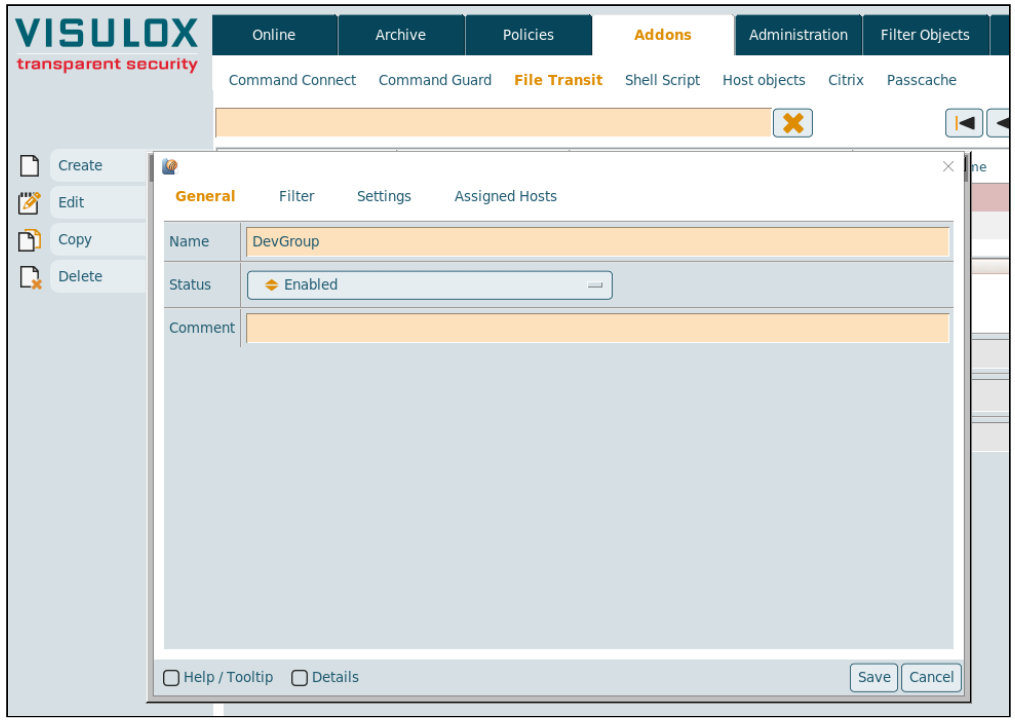
Accessing the File Exchange web page

File Transfer

Available File Transfer groups



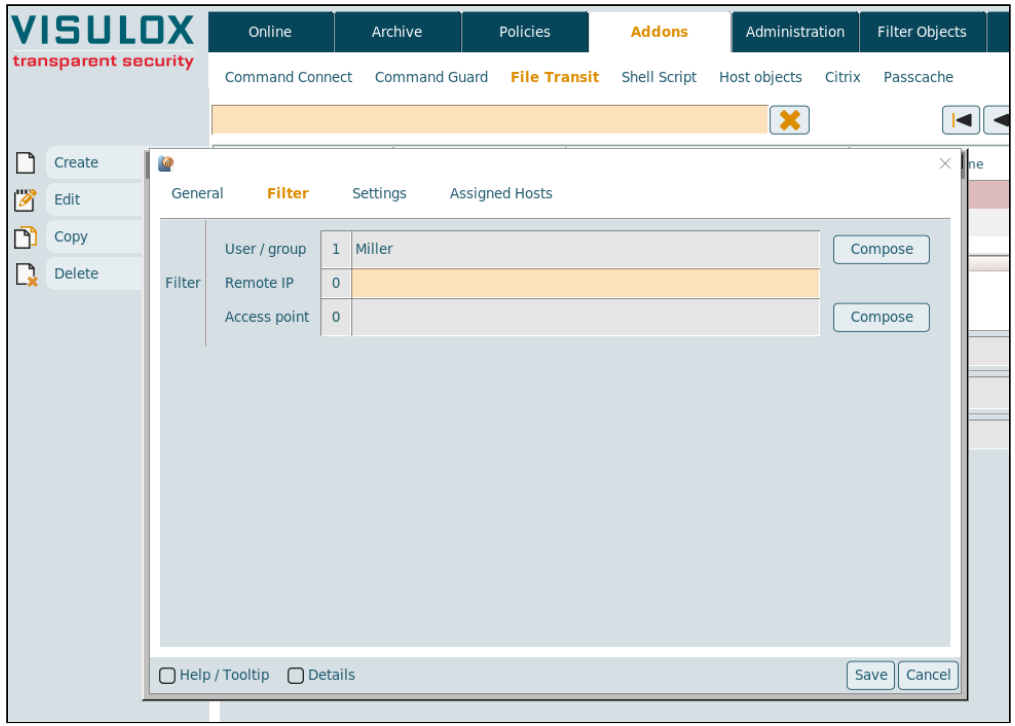
New File Transfer groups can be created and existing groups can be edited, copied or deleted.



The name of the group and the status (enabled or disabled) has to be entered.

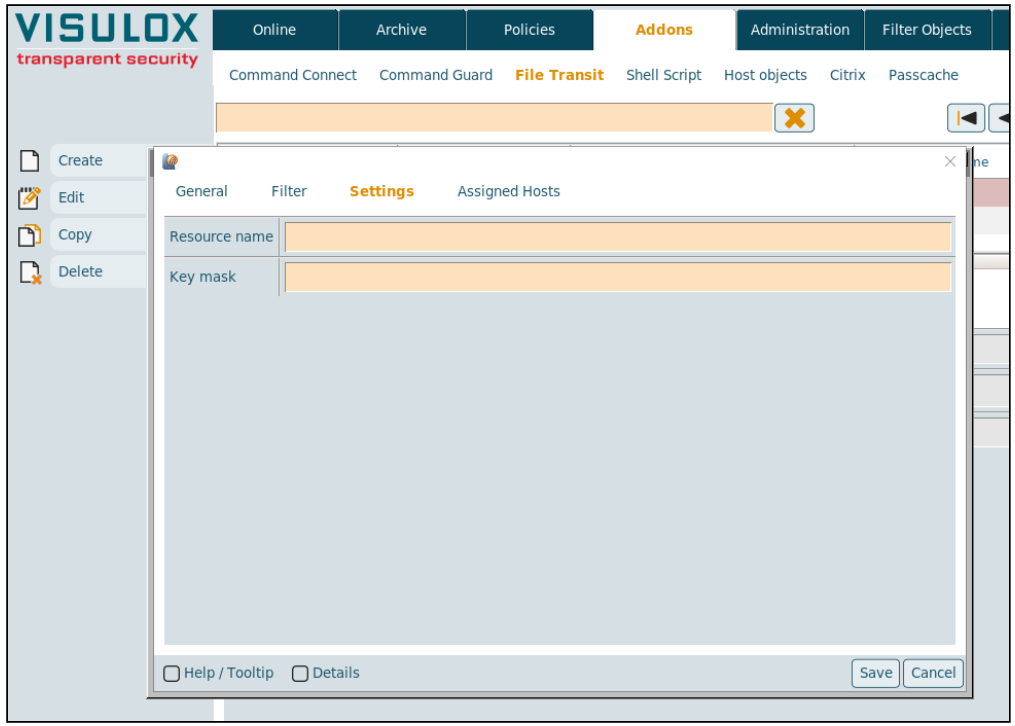
A comment for the group can be added as well.

Filter



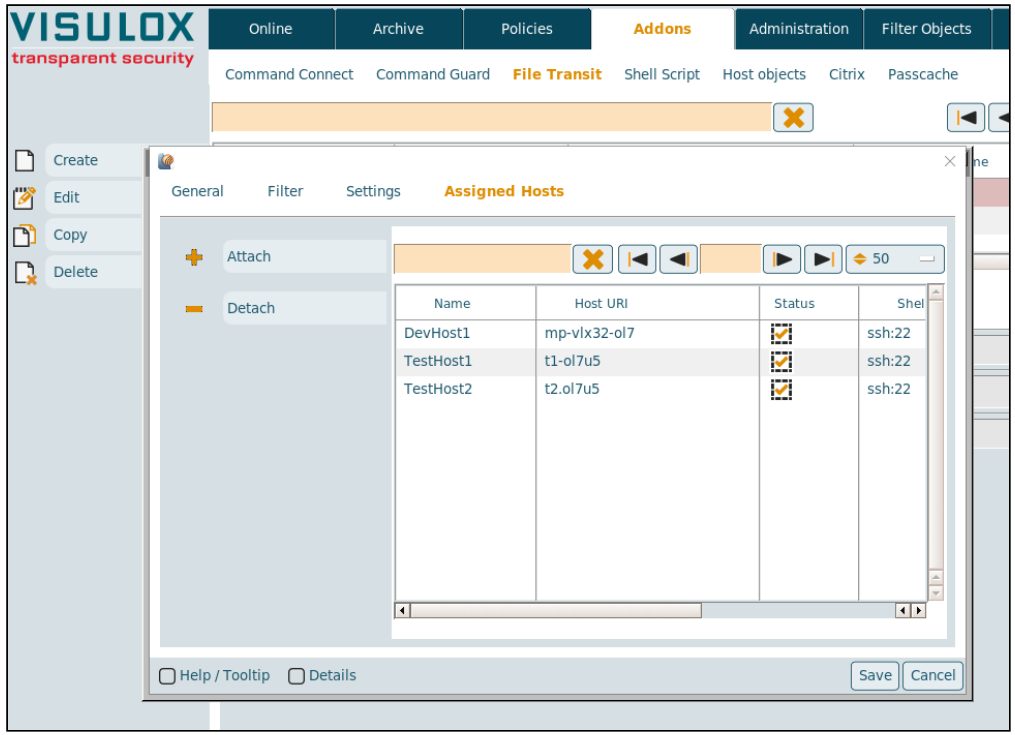
The filter for File Transfer groups can be set on user / group, the remote IP or the access point.

Settings



The resource name or a key mask for connections via SSH Key can be set.

Assigned hosts



Host objects can be attached / detached from the File Transit group. (See also: Host objects)

Before hosts can be added to a new created group, the group must be saved once.

How to control FT Client from the command line

Overview

The command line tool "**VISULOX addon ftclient**" allows to control the VISULOX FT Client application.

- Overview
- Usage
- FT Client elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print FT Client objects.
add	Add a FT Client object.
edit	Modify fields of a FT Client object.
delete	Remove a FT Client object.
fields	List available fields in the database
listhosts	List assigned hosts

FT Client elements (edit)

Element	Description
-name <>	Name of this definition <>
-comment <>	Comment for this definition <>
-mode <>	Enable / disable this definition. Default value: on.
-resource <>	Resource in passcache
-sshkeymask <>	Filtermask for SSH-keys provided in the sessions <>
-object <>	User/group filter allowed to use this definition <>
-remoteip <>	Remote IP from where this definition can be used <>
-accesspoint <>	Filter: Access Point <>
-hosts <>	List of hosts assigned to this definition <>
-grant <>	Set granted user in database record <>

Examples

List current available FT Client objects

```
visulox addon ftclient list

    ----------------------------
    | basicname |   recordmode |
    ----------------------------
    |  ft1-test |  enabled.map |
    |  ft2-test | disabled.map |
    ----------------------------
```

List available database fields

```
visulox addon ftclient fields
```

Display selected fields

```
visulox addon ftclient list -fields basicname,ft_assign_host,ft_comment
```

Add FT Client object

```
visulox addon ftclient add -name ft3-test
```

Edit FT Client object

```
visulox addon ftclient edit -name ft3-test -mode off
```

Remove an entry

```
visulox addon ftclient delete -name ft3-test
```

How to discard filetypes from the Transit Zone synchronisation

- Introduction
- Show filetypes on the Transit Zone synchronisation ignore list
- Add filetypes to the Transit Zone synchronisation ignore list

Introduction

In some cases certain filetypes are unwanted and are generated automatically in conjunction with other filetypes e.g. Thumbs.db, .identifier and others.

This article explains how to ignore such filetypes in the Transit Zone.

Show filetypes on the Transit Zone synchronisation ignore list

List all files on the ignore list

```
visulox config list -name transitsync.ignore.globs
```

VISULOX default configuration will show:

```
-------------------------------------------------------------------------------------------
| changed | parameter                |  type | value                                        |
-------------------------------------------------------------------------------------------
|         | transitsync.ignore.globs | FIXED | *.tmp *.swp *.bak *.part Thumbs.db           |
-------------------------------------------------------------------------------------------
```

Add filetypes to the Transit Zone synchronisation ignore list

As seen above, there are already filetypes on the list. Filetypes that should be ignored can be added to this default list. In this example we add ".identifier" to the list.

Add filetypes to the ignore list

```
visulox config edit -name transitsync.ignore.globs="*.tmp *.swp *.bak *.part Thumbs.db *.identifier" -force
```

VISULOX confirms changes to the ignore list by showing the new value

New ignore list

```
-------------------------------------------------------------------------------------------
| changed | parameter                |  type | value                                        |
-------------------------------------------------------------------------------------------
| changed | transitsync.ignore.globs | FIXED | *.tmp *.swp *.bak *.part Thumbs.db *.identifier  |
-------------------------------------------------------------------------------------------
```

From now on files with the extension ".identifier" will be ignored by the Transit Zone synchronisation

The Transit Zone ignore list can also be configured with regular expressions.

```
visulox config list -name transitsync.ignore.regexps
    ---------------------------------------------------------
    | changed | parameter                  |  type | value |
    ---------------------------------------------------------
    |         | transitsync.ignore.regexps | FIXED |       |
    ---------------------------------------------------------
```

Allowing File Transfer from internal to internal

File Transfer is designed to allow transfers from a client into the infrastructure (external → internal) **and** from the infrastructure to a client via the Transit Zone (internal → external).

If users want to move a file from an application server in the infrastructure to another via the Transit Zone, File Transit from **internal to internal** has to be enabled.

```
visulox config -name transit.inside=true
```

With this setting enabled, users can transfer files to the Transit Zone and from there to each application server, where they have access and are allowed to transfer files.

visulox restart is necessary after changing this setting!

Automated transfer of files into Transit Zone (Passon)

Overview

Users are able to upload into the Transit Zone. Depending on the user, file name or file type these files can be passed on automatically to another location via script with or without approval.

It is also possible to copy a file into the Transit Zone of another user via VISULOX Transit Command Line Interface.

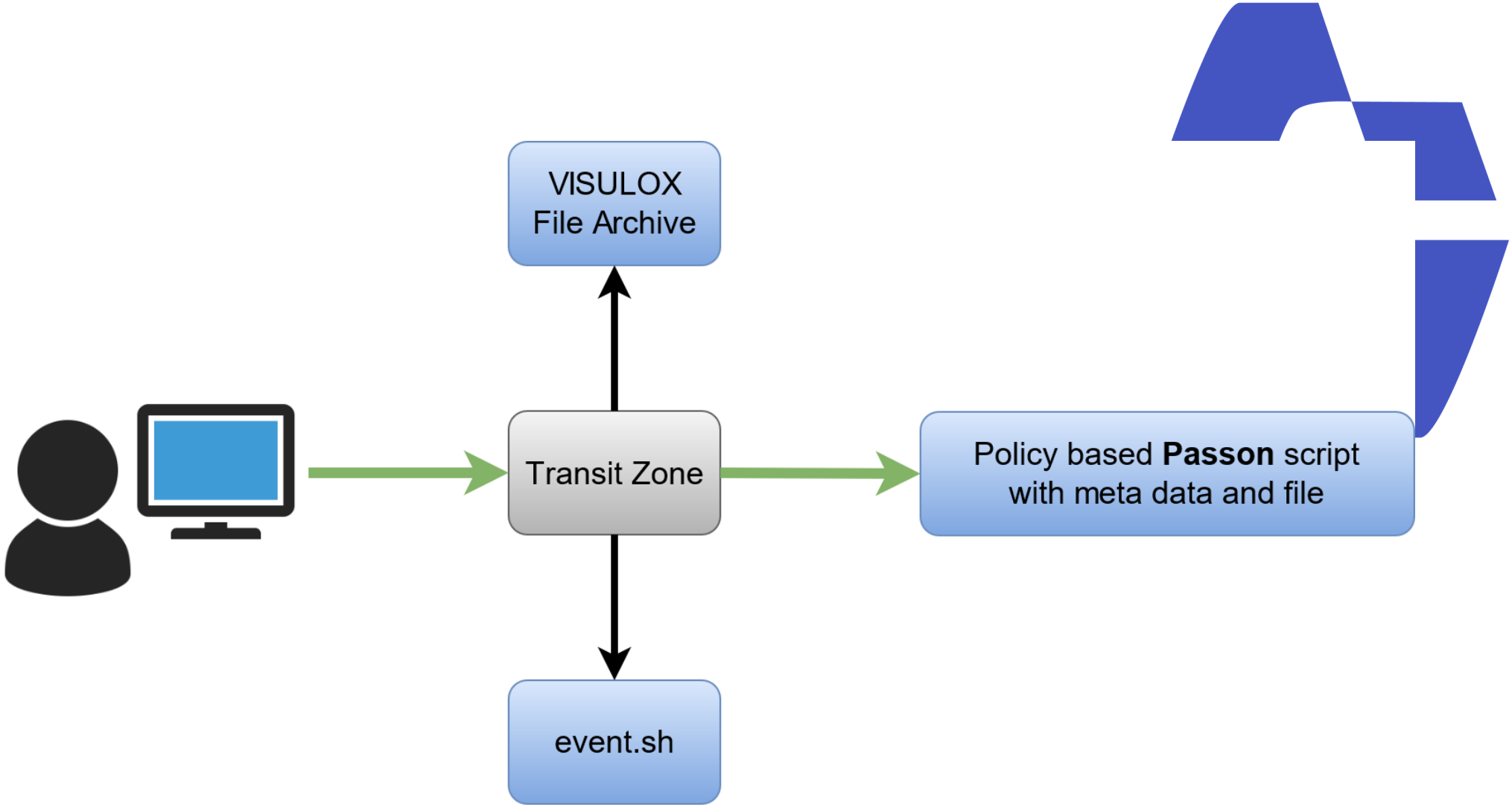
The configuration is easily done in VISULOX Cockpit / Policies / Transit Policy.

The passon script used for the automated transfer can be created or adjusted in VISULOX Cockpit / Administration / Actions as well.

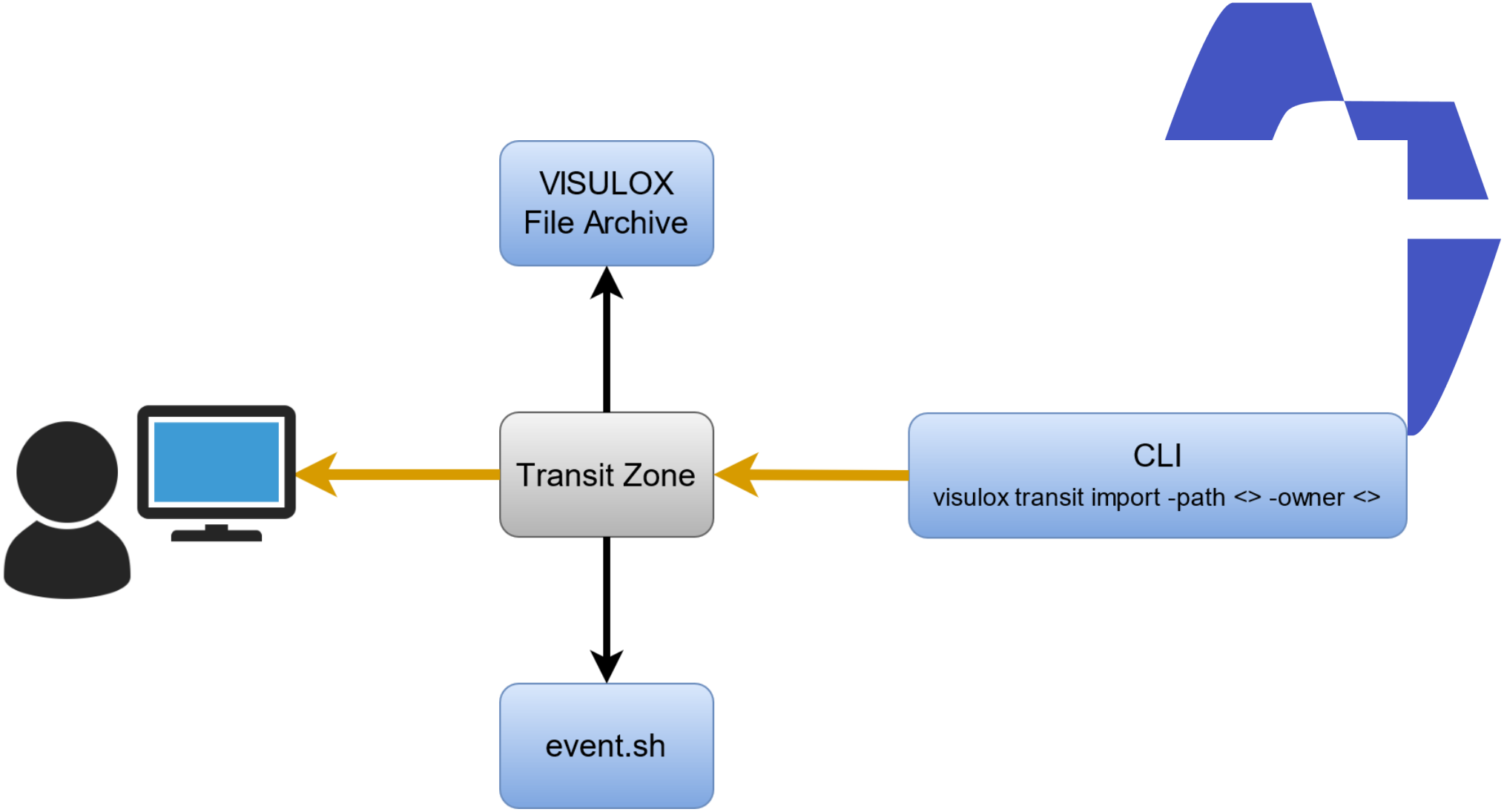
- Overview
  - Upload
  - Download
- Create a passon example script
  - Example script: passon.sh
  - Most important variables within the script
  - Additional variables that can be used in the script
  - Passon approved variables
  - Passon rejected variables
- Configuration of a passon Transit Policy

Important: Files **must not** be deleted or renamed in the Transit Zone during the transfer process..

Upload


VISULOX
File Archive
Transit Zone
Policy based **Passon** script
with meta data and file
event.sh

Download


VISULOX
File Archive
Transit Zone
CLI
visulox transit import -path <> -owner <>
event.sh

Create a passon example script

Using the CLI a passon example script can be implemented with the following steps.

1. Create a file with the example script (see below)
2. Use the following command to implement the script for the Transit Policies:

Setup script

```
visulox admin action add -name passon -category validate -scriptfile /tmp/passon.sh
```

3. The passon script now is displayed in VISULOX Cockpit / Administration / Actions and can be used in the Transit Policies

Example script: **passon.sh**

```
#!/bin/bash
# VLXOBJECT = Originale filename
# VLXFILEPATH = Path to file on disk (no not delete within script)
$VLXPATH/bin/cmd/config.tcl env > /tmp/passon.$$
cp $VLXFILEPATH /tmp/${VLXLOGINUSER}-${VLXCREATETIME}-$VLXOBJECT
echo "done with $VLXOBJECT"
# If the script should be treated as successful in VISULOX, the exit code must be 0
true
exit $?
```

In this example script the file will be copied to **/tmp** (the available variables will be dumped to a file in **/tmp** as well).

The login user name and the timestamp will be added to the filename.

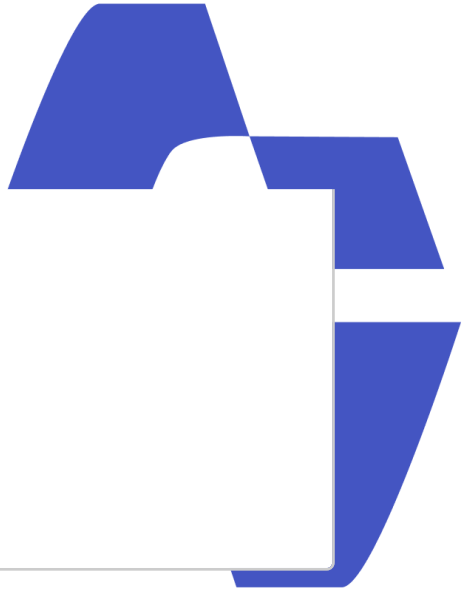
Most important variables within the script

```
        VLXFILEPATH = /opt/visulox/var/filearea/upload/81e77f1e-b8d1-4004-96dd-f87d85b18b32
          VLXOBJECT = Hydrangeas.jpg
           VLXOWNER = o=Tarantella System Objects/cn=Miller
```

```
File:  %VLXFILENAME%
Sign:  %VLXFILETYPE%
Size:  %VLXFILESIZE_FMT%
Hashs: %VLXFILEHASHS%
```

Additional variables that can be used in the script

```
     VLXACCESSPOINT = example.domain.com
        VLXCLIENTIP = 192.168.1.123
      VLXCREATETIME = 1538735003
    VLXCREATETIMEMS = 1538735003717
VLXCREATETIMEMS_FMT = 2018-10-05 12:23:23.717
  VLXCREATETIME_FMT = 2018-10-05 12:23:23
       VLXEVENTINFO = POL-FT Filetype: JPEG image data, JFIF standard 1.02 Size:581.33kB
        VLXFULLNAME = Miller
       VLXGROUPLIST = {o=Tarantella System Objects/cn=Miller}
   VLXGROUPLIST_FMT = Worker
           VLXLANG = en
            VLXLOG = /opt/visulox/var/log
       VLXLOGINUSER = Miller
         VLXOWNERID = 6F69AFA4EFD0B379724F330FCB81A65C
      VLXOWNERSHORT = Miller
            VLXPATH = /opt/visulox
```



```
          VLXPOLICY = POL-FT
       VLXPOLICYMODE = passedon
         VLXREMOTEIP = 192.168.1.123
       VLXREPOSITORY = DATASTORE
      VLXSESSIONHOST = vEXAMPLE
          VLXSURNAME = Miller
        VLXTOKENMODE = NONE
      VLXUSERPROFILE = o=Tarantella System Objects/cn=Miller
VLXUSERPROFILESHORT = Miller
             VLXUTIL = /opt/visulox/lib/utils
       VLXWEBTOPBASE = https://example.domain.com:443/sgd
```

Passon approved variables

```
       VLXACCESSPOINT  = t1-ol9.tbsol.de
       VLXAPPROVALMODE = approved
  VLXAPPROVEDBYEMAIL   = xxx
VLXAPPROVEDBY_FMT_FMT = test
VLXAPPROVEDBY_FMT     = o=organization/cn=test
         VLXAPPROVEDBY = o=organization/cn=test
         VLXCREATETIME = 1758172170
     VLXCREATETIME_FMT = 2025-09-18 07:09:30
          VLXEVENTINFO = File is requested by change management.
              VLXEVENT = tzapproved
          VLXFILEHASHS = sha256 25e70697b2ed05bd5e14057b6b450868deffd26be525b49a1d81d257b7c02205 md5
d0ab9f7d4c1d286cad20deaa8c638669
           VLXFILENAME = cust.png
           VLXFILESIZE = 876
       VLXFILESIZE_FMT = 876B
           VLXFULLNAME = Administrator
          VLXGATEWAYIP = ::1
        VLXGATEWAYNAME = localhost
              VLX_HOME = /opt/visulox
```

```
             VLXLANG = en
          VLXLOGINUSER = root
             VLXOBJECT = cust.png
            VLXOWNERID = 5F7AB10DADC9EDA6EE7D2034B5545E18
              VLXOWNER = o=Tarantella System Objects/cn=Administrator
         VLXOWNERSHORT = Administrator
               VLXPATH = /opt/visulox
             VLXPOLICY = POL-FT-Passon
           VLXREMOTEIP = 172.17.5.1
          VLXREPOSITORY = DATASTORE
              VLXSCRIPT = SCRIPT.1758172170411.log
        VLXSESSIONHOST = vT1OL9
             VLXSURNAME = root
        VLXUSERPROFILE = o=Tarantella System Objects/cn=Administrator
   VLXUSERPROFILESHORT = Administrator
              VLXUTIL = /opt/visulox/lib/utils
```

Passon rejected variables

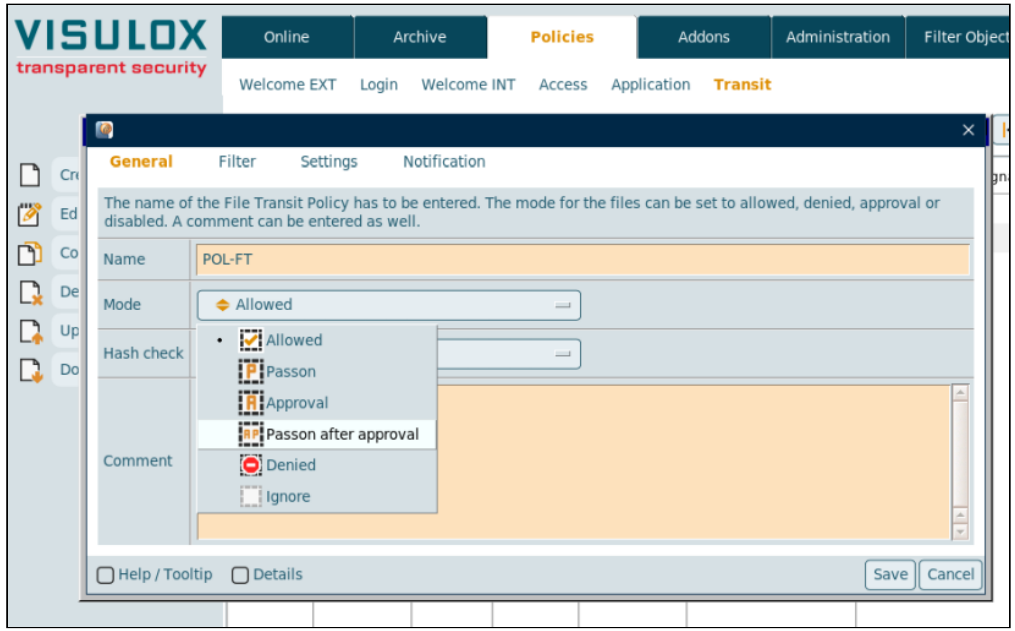
```
   VLXAPPROVALMODE = rejected
     VLXAPPROVEDBY = CN=Tom Meyer,OU=Mitarbeiter,OU=ToolBox,DC=tbsol,DC=de
 VLXAPPROVEDBY_FMT = Tom Meyer
     VLXCREATETIME = 1591725924
 VLXCREATETIME_FMT = 2020-06-09 20:05:24
          VLXEVENT = rejected
      VLXEVENTINFO = Rejected because project is freezed.
       VLXFILEPATH = /tmp/vlx.dump
      VLXGROUPLIST = o=organization/cn=foo
  VLXGROUPLIST_FMT = foo
            VLXLOG = /globalhome/tbasien/vsx30/var/tab-dev1/log
         VLXOBJECT = data_ok.png
          VLXOWNER = o=organization/cn=foo
     VLXOWNERSHORT = foo
```

```
      VLXPATH = /globalhome/tbasien/vsx30
    VLXPOLICY = PASSON
 VLXREMOTEIP = 192.168.3.166
     VLXUTIL = /globalhome/tmeyer/vsx30/lib/utils
```

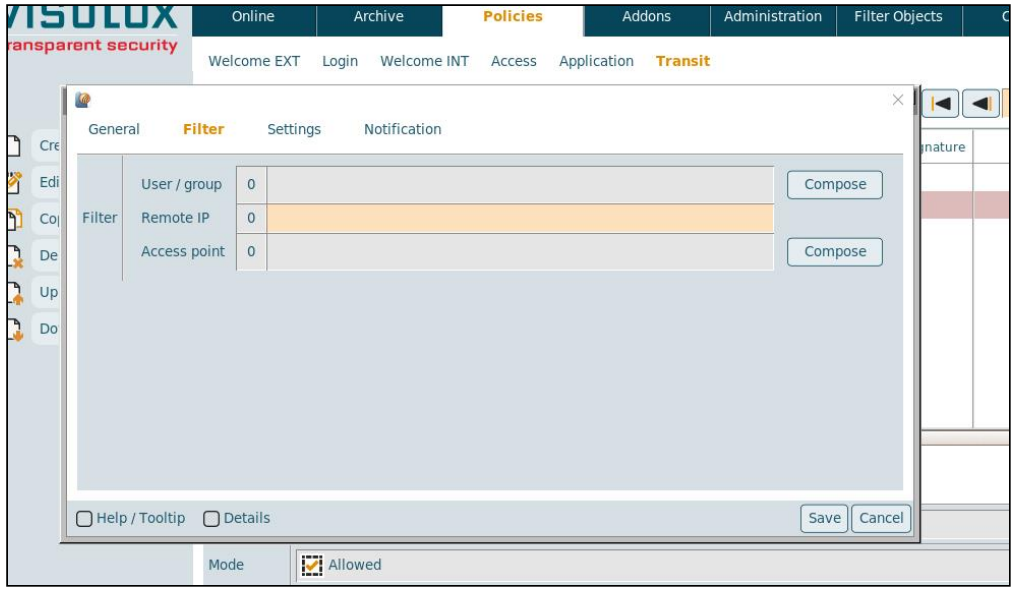
Configuration of a passon Transit Policy

In VISULOX Cockpit / Policies / Transit Policy a new policy has to be created.

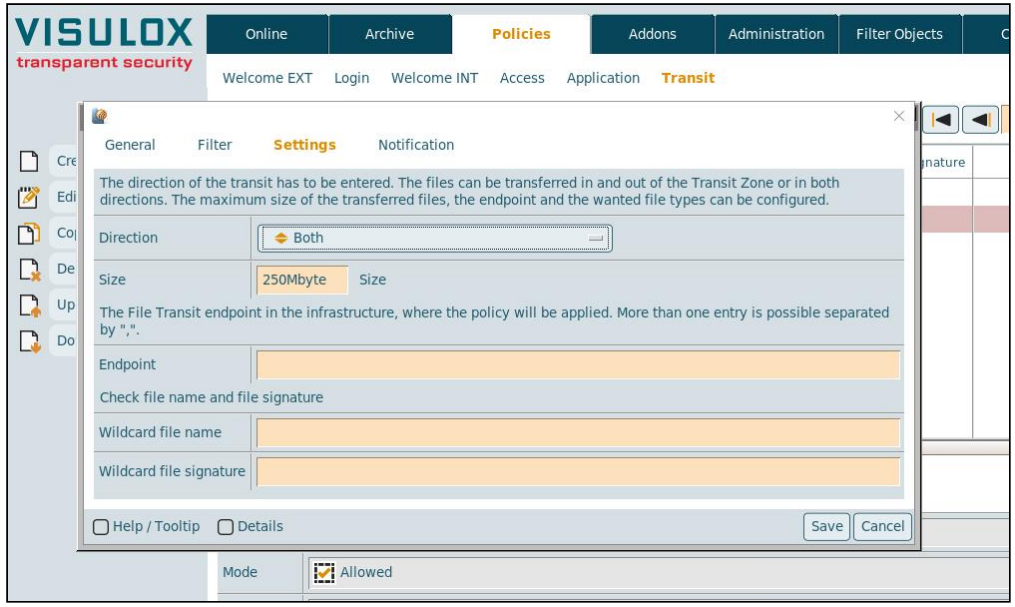
Select policy mode **Passon or Passed on after approval:**



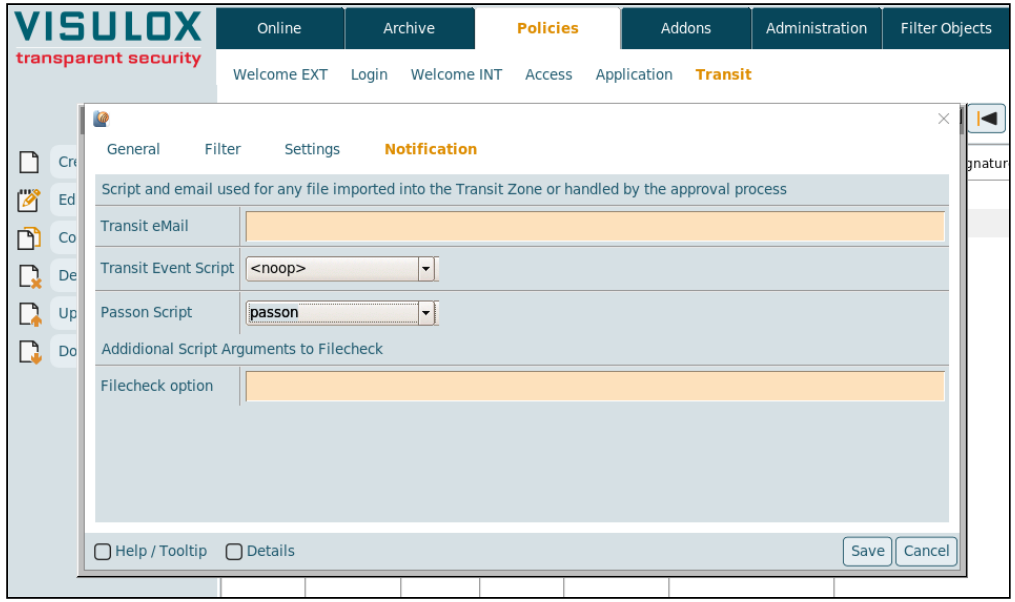
Set the Transit Policy filter for **user / group** and/or **access point:**



Enter **filename** and/or **filetype** of the files, that will be passed on (wildcards are possible):



Select the **Passon** event script:



A file that is uploaded via Passon Policy is shown in the Transit Zone. It can not be downloaded with VLX Transit Web or VISULOX File Exchange.
→ passon enforces direction: **in**

Files transferred via **Passed on with approval** have to be approved or rejected by a supervisor in VISULOX Cockpit / Online / Transit Zone.
⚠ Approval is done and processed on the server of the supervisor!

Command Line Interface

The **visulox transit** command can be used to copy files into the Transit Zone of another user. A standard Transit Policy is applied.

Available commands and their options

approval	Approve or reject pending files in Transit Zone • -state <*value*> Approve / true / 1 Reject / false / 0
import	Import file into a users Transit Zone • -owner <*value*> Unique owner <> • -path <*value*> Path to readable file <> • -asreport Allows to inject a file as a report file for the user For example a report can be created via cron and sent to the Checkout Zone of the user automatically • -rtime <*value*> Retention time in Transit Zone in seconds <*default*>
list	List user's with files in the Transit Zones
delete	Delete files in Transit Zone • -owner <*value*> Unique owner <> • -file <*value*> File in Transit Zone <> • -all All files in Transit Zone

Example to import a file for download into the Transit Zone

```
visulox transit import -path <path to file> -owner <unique owner> -rtime <retention time in sec>
```

- Import command needs a standard Transit Policiy with the direction both or out, size, pattern, etc.

- The retention time maximum is limited to the lifetime in archive

File Transfer via command line

Command Line Interface

The **visulox transit** command can be used to copy files into the Transit Zone of another user. A standard Transit Policy is applied.

Available commands and their options

approval	Approve or reject pending files in Transit Zone • -state <*value*> Approve / true / 1 Reject / false / 0
import	Import file into a users Transit Zone • -owner <*value*> Unique owner <> • -path <*value*> Path to readable file <> • -asreport Allows to inject a file as a report file for the user For example a report can be created via cron and sent to the Checkout Zone of the user automatically • -rtime <*value*> Retention time in Transit Zone in seconds <*default*>
list	List user's with files in the Transit Zones
delete	Delete files in Transit Zone • -owner <*value*> Unique owner <> • -file <*value*> File in Transit Zone <> • -all All files in Transit Zone

Example to import a file for download into the Transit Zone

```
visulox transit import -path <path to file> -owner <unique owner> -rtime <retention time in sec>
```

- Import command needs a standard Transit Policiy with the direction both or out, size, pattern, etc.
- The retention time maximum is limited to the lifetime in archive

VISULOX Transit mapping

All applications with **visulox.exp, vlxUnix.exp** and **vlxWindows.exp** (former: vlxRdp.exp**)** will get the VISULOX Transit Zone with **vlxMode=SYNC** set.

On VISULOX Nodes wiithout VISULOX PORTAL Service, the replication has to be set at least to **ftonly**.

sshfs must be installable. For OL 8 use "Oracle Linux 8 CodeReady Builder (x86_64) - Unsupported" as repository.

To setup the VISULOX Transit Zone on **Unix application servers**, that are not a VISULOX Node an RPM file is available for installation:

```
visulox-transitmapping-4.1.0-1-el8.x86_64.rpm
```

To enable transit mapping after installation, use:

```
/opt/visulox-transit/bin/transitmapping.sh enable
```

The connection user has to be in the group: **fuse**:

```
usermod -G fuse <user>
```

If the transit users have been customized with **/opt/visulox/setup/vlxuser/mgmt.tcl** and visulox-transitmapping is installed, then the mapping has to be adjusted too:

```
/opt/visulox/setup/vlxusers/mgmt.tcl add -# 10
/opt/visulox-transit/bin/transitmapping.sh enable
```

If **autofs** is used wiith **transit mapping**, Selinux has to be disabled

See also: VISULOX Transit Mapping and Ubuntu application servers

VISULOX Transit Mapping and Ubuntu application servers

Abstract

This article explains how to deploy the VISULOX Transit Zone into a user shell on an Ubuntu application server.

Application setup in VISULOX

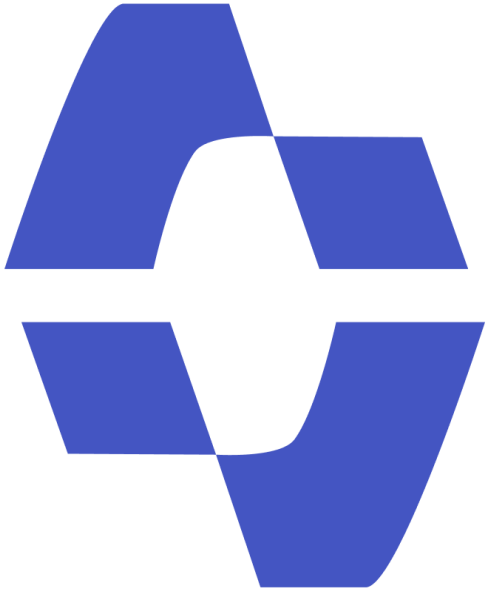
Standard Unix aplication interaction using **vlxUnix.exp** with **vlxMode=SYNC**.

Setup steps on the Ubuntu application server

- CLI: **apt-get install sshfs**
- Add the line "**session required pam_namespace.so**" (*without double quotes*) at the end of the file **/etc/pam.d/common-session**
- Create the file **/etc/security/namespace.d/visulox.conf** (chmod 644) with the line "**$HOME/vlxtransit $HOME/.vlxtransit.inst/ level:create=0775**" (*without double quotes*):

/etc/security/namespace.d/visulox.conf

```
$HOME/vlxtransit $HOME/.vlxtransit.inst/ level:create=0775
```



See also: VISULOX Transit mapping

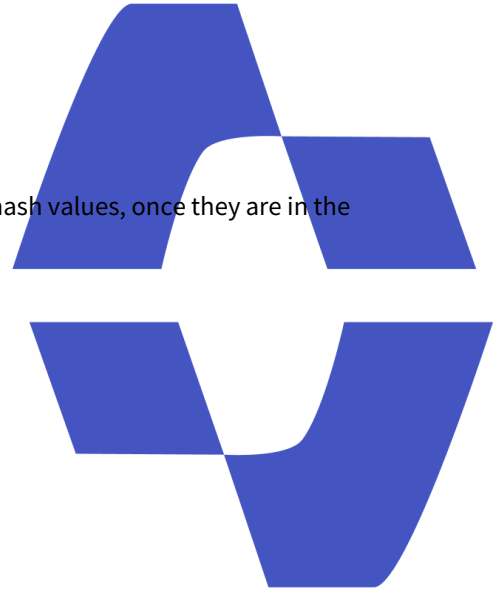
Extended Transit Policy with hash check by provided hash file

- About
- Features
- Configuration
    - Enabling hash check for a Transit Policy
    - More policy modes (Approval and Passon)
- Using hash check / Workspace view
    - Transit policies
    - Uploading files
    - Transit Zone
    - Policy mode: Approval
    - Policy mode: Passon
    - Policy mode: Passon with approval
    - Hash information
- Command line interface
    - VISULOX policy transit command
    - VISULOX transit command
- Related articles in documentation

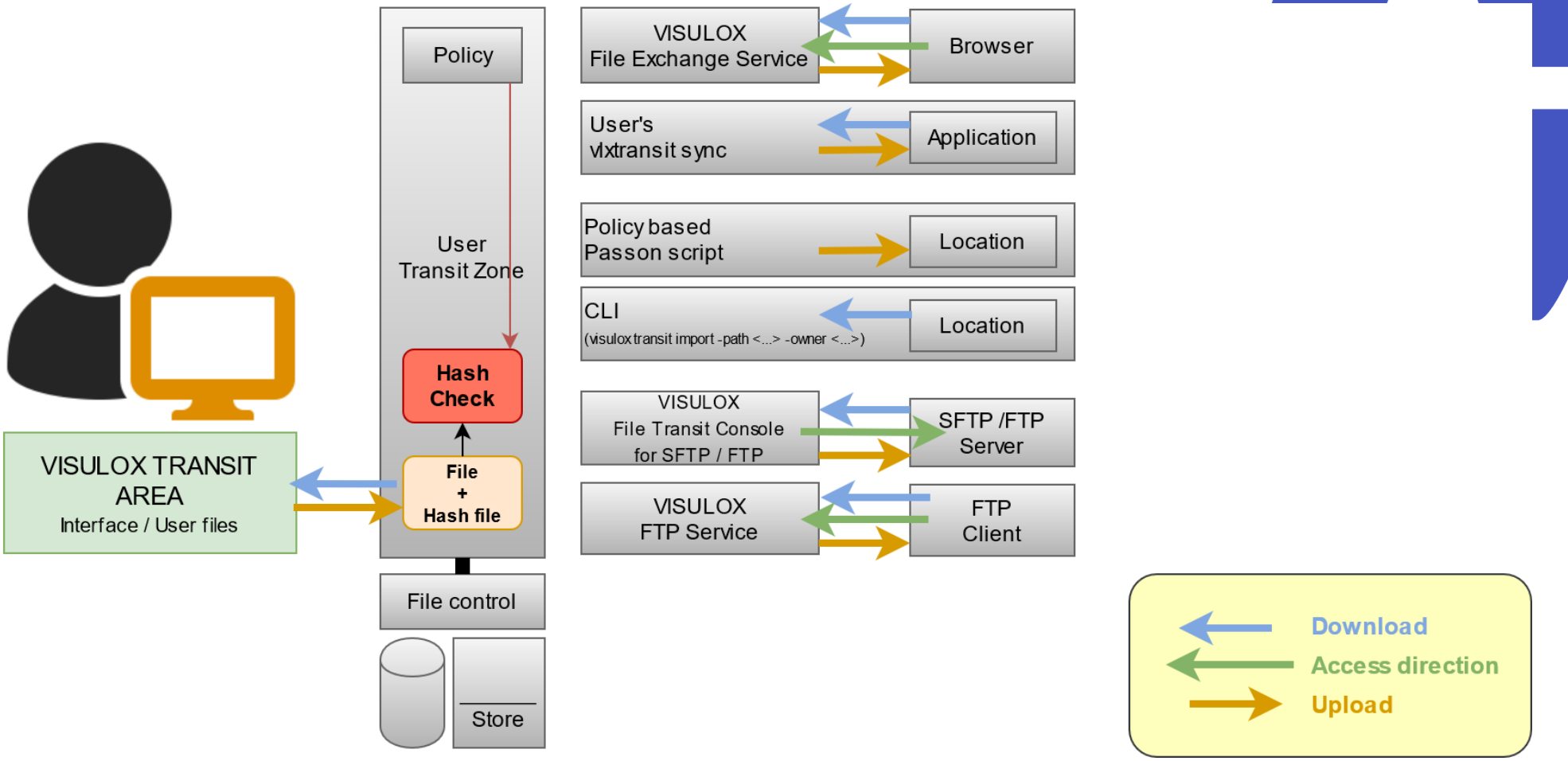
About

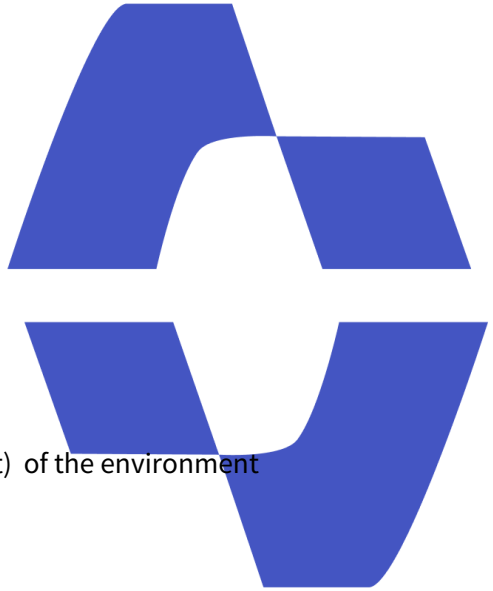
File Transit has been enhanced to check the hash values of uploaded files against a created hash file.

If the Transit Policy is set to "**Hash check enabled**", files can be uploaded into Transit Zone as usual.
The files matching the policy with hash check enabled will get the status "**pending**" in the Transit Zone.
Such files can only be processed, if a valid hash file is uploaded into the Transit Zone as well.



The hash file containing **one** or **more** hash values can be uploaded **before** or **after** the actual files. Files and hash files are always checked for hash values, once they are in the Transit Zone.
Files that have a matching hash value in a hash file will be processed depending on the configured policy mode.


Policy
User
Transit Zone
Hash
Check
File
+
Hash file
File control
Store
VISULOX TRANSIT
AREA
Interface / User files
VISULOX
File Exchange Service
Browser
User's
vlxtransit sync
Application
Policy based
Passon script
Location
CLI
(visulox transit import -path <...> -owner <...>)
Location
VISULOX
File Transit Console
for SFTP / FTP
SFTP /FTP
Server
VISULOX
FTP Service
FTP
Client
Download
Access direction
Upload



Features

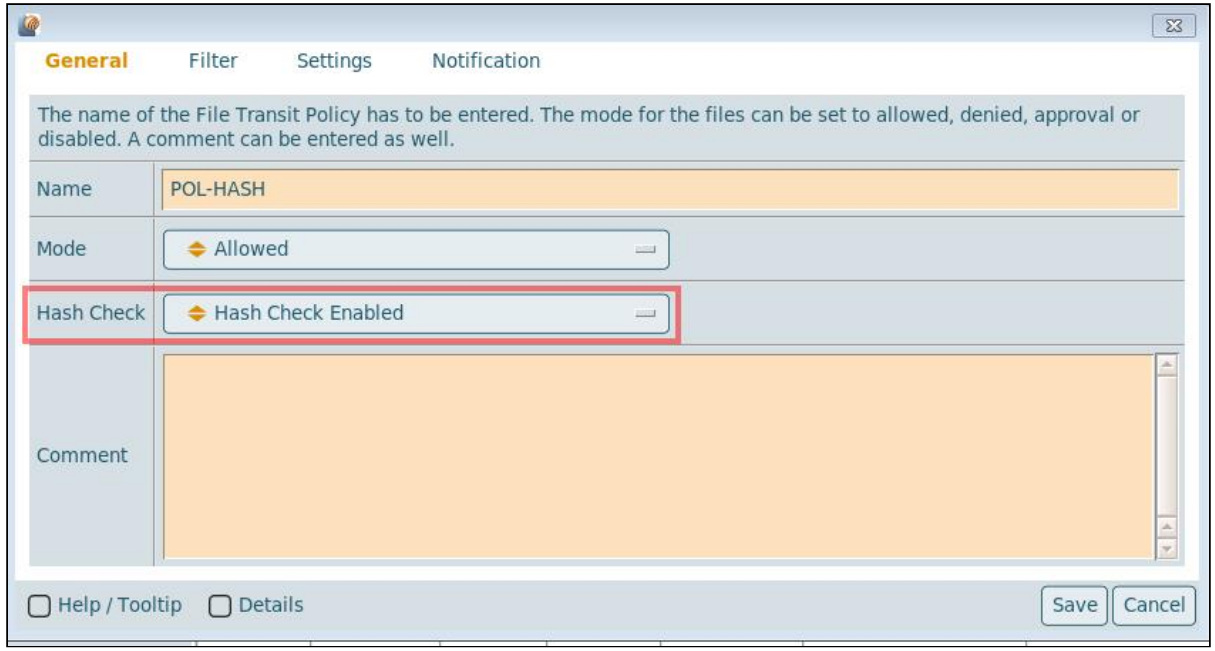
- One or **more** hash values are possible in a single hash file
- Files can be processed as long as the files and their corresponding hash file are available in the Transit Zone
  ⚠ Default lifetime of files in the Transit Zone is set to two hours!
- Hash check is available for all policy modes: Allowed, Approval, Passon and Passon with Approval
- The hash file itself is passed on like regular files to check the hash values of the files on the endpoint as well
- Hash check ban be enabled for files transferred in (client → Transit Zone → server) and out (server → Transit Zone → client) of the environment

Configuration

Enabling hash check for a Transit Policy

Hash check can be enabled in VISULOX Cockpit / Policies / Transit within a Transit Policy.

It is also possible to create or adjust Transit Policies via the command line (see: **Command Line Interface**).

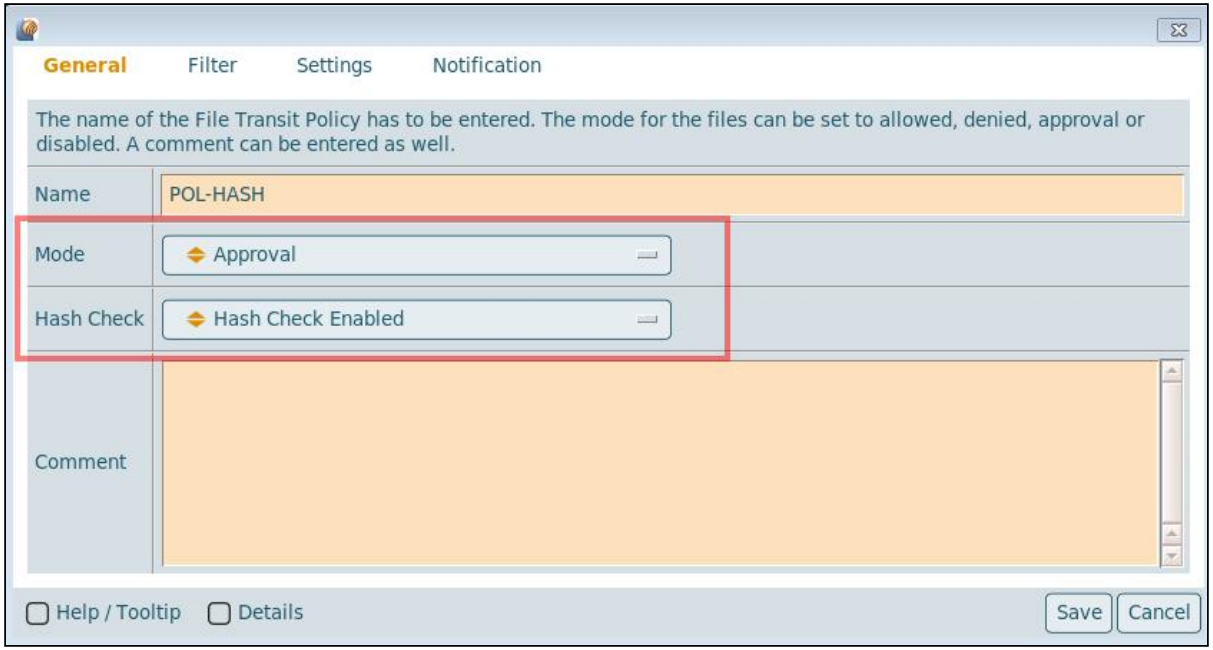


Hash check has to be set to enabled for the Transit Policy.
The Transit Policy has to be configured as usual (filter, settings, notifications) to match the wanted files uploaded into Transit Zone.

In this case policy mode "**Allowed**" is selected.
Files matching this policy will be available for further processing, once a file and a hash file with matching hash values are uploaded into the Transit Zone.

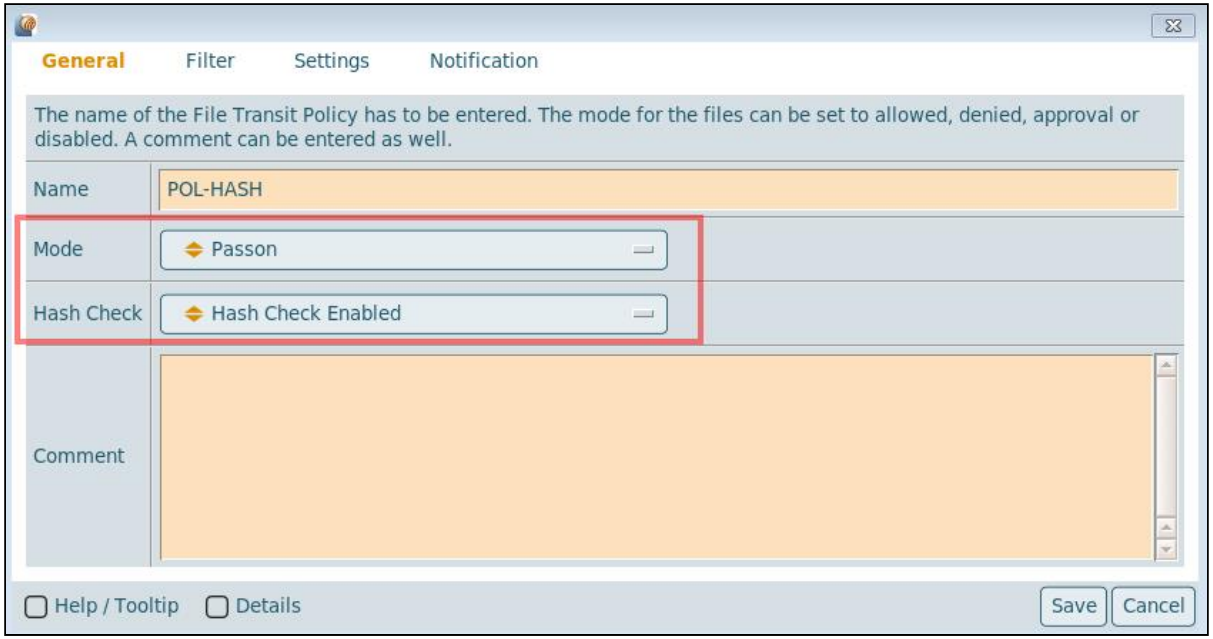
More policy modes (Approval and Passon)

Transit Policy with policy mode set to "**Approval**":



Files matching this policy will be available for further processing, once a file and a hash file with matching hash values are uploaded into the Transit Zone **and** approval has been done.

Transit Policy with policy mode set to "**Passon**":



The passon script has to be adjusted and selected in Notification / Passon Script.
Files matching this policy are passed on, once a file and a hash file with matching hash values are uploaded into the Transit Zone.

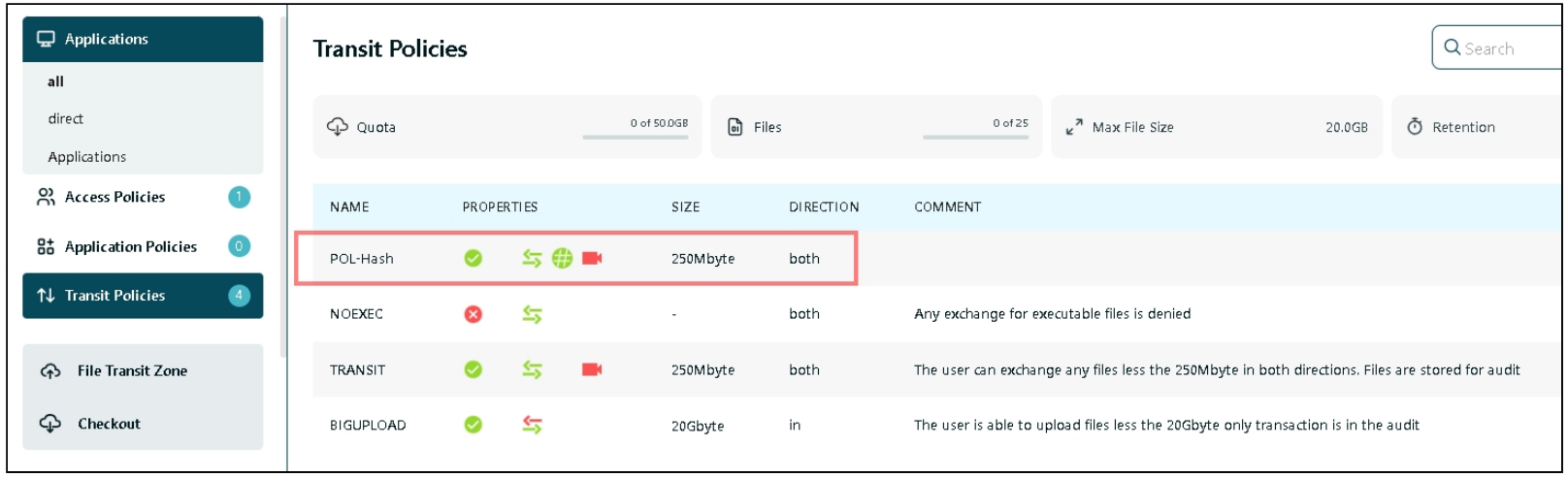
The policy mode "**Passon with approval**", which is a combination of passon and approval can also be used with hash check enabled.

Using hash check / Workspace view

In the Workspace of the users all necessary information regarding File Transit are diplayed.

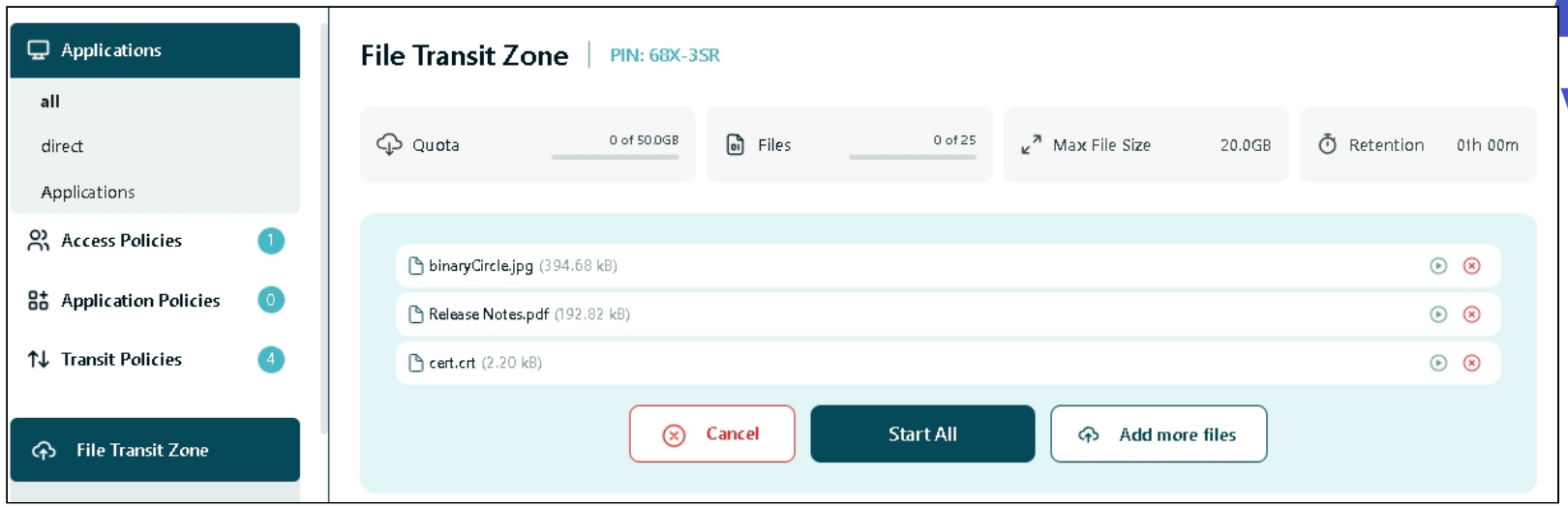
Transit policies

In the "**Transit Policies**" section all policies of the current user and details about file transit are listed:



Uploading files

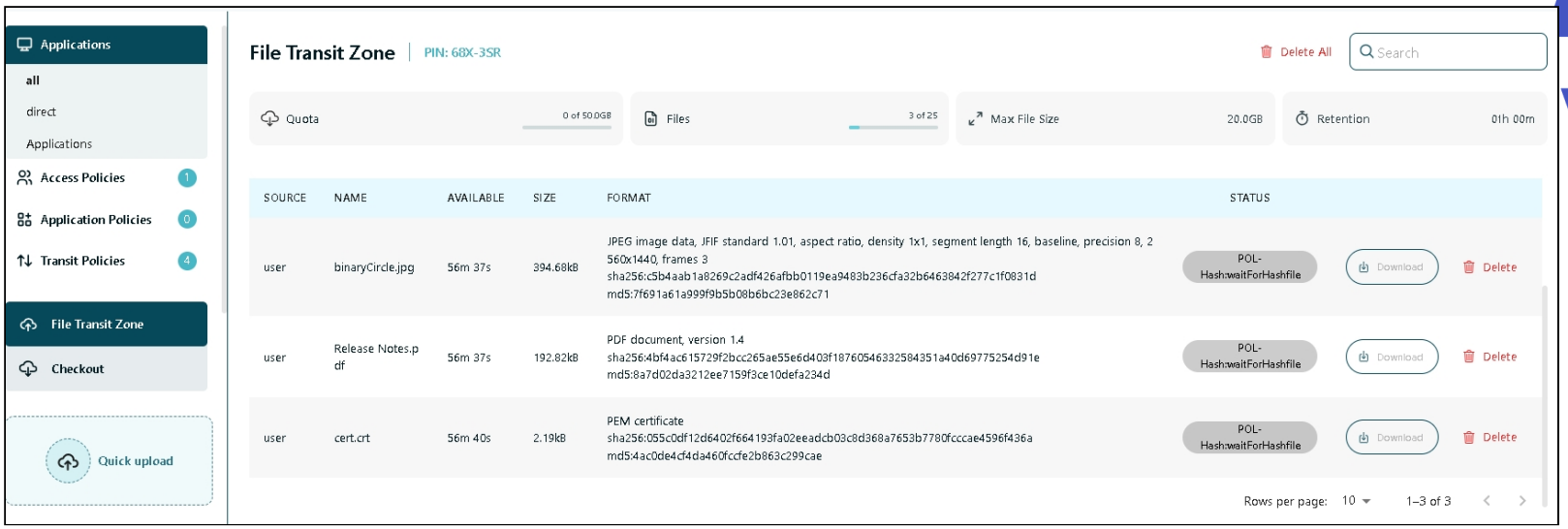
In the **VISULOX Transit Area** of the Workspace the files can be uploaded from the client to the Transit Zone:



Files can be uploaded one by one or numerous files can be added and uploaded at once, depending on the configured restrictions of the File Transit Zone.

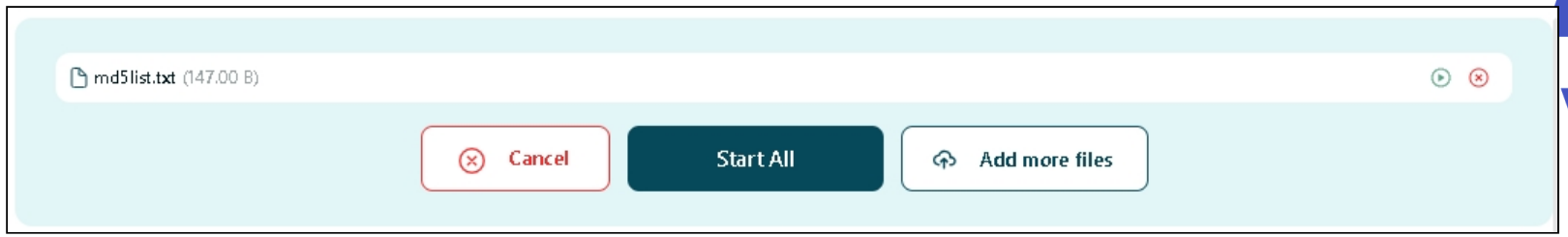
Transit Zone

Once the files are uploaded, they are displayed in the "**Transit Zone**":



The files matching the hash check policy are set to the status "**Wait for hash file**" and can not be processed further without the hash file containing the correct hash values.

The **hash file** including the hash values for the files must uploaded to the Transit Zone as well:



Example: md5 hash file with three hash values:

File: md5list.md5

```
7f691a61a999f9b5b08b6bc23e862c71  binaryCircle.jpg
4ac0de4cf4da460fccfe2b863c299cae  cert.crt
8a7d02da3212ee7159f3ce10defa234d  Release Notes.pdf
```

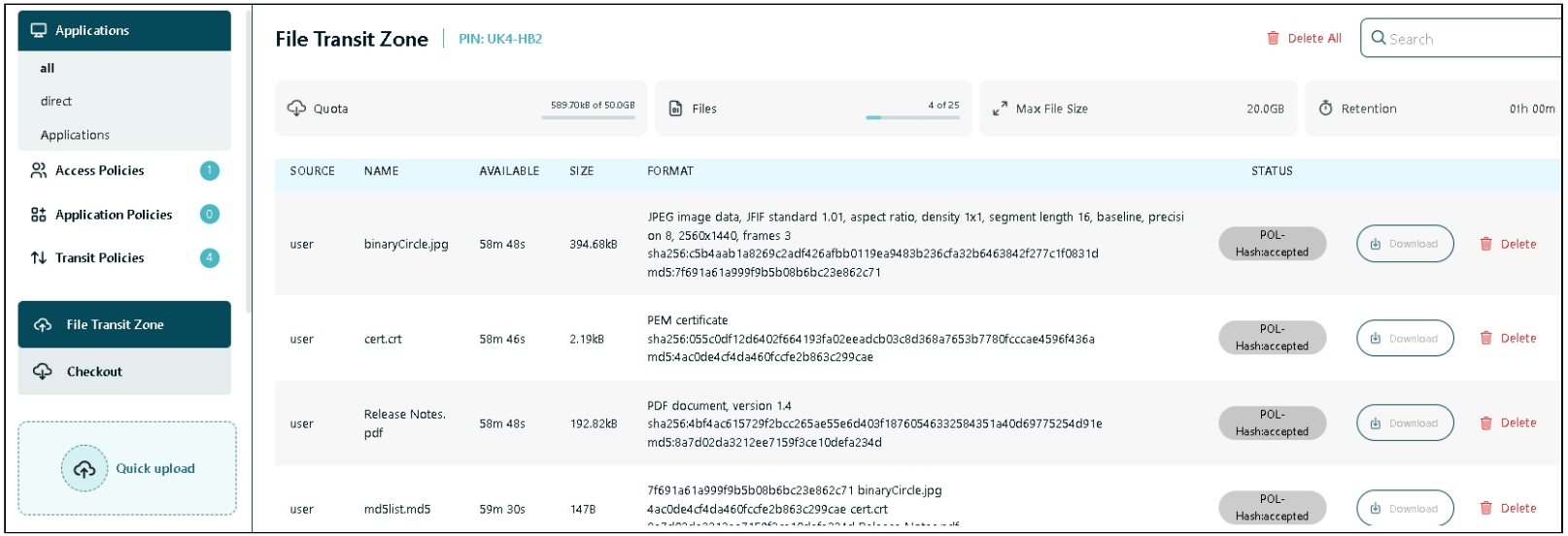
The default hash check is done with **sha256** / **md5** for files ending with **.md5** and **.sha256**,

The configuration parameters for the checksum and the recognized hash files are set with:

```
visulox config -name transit.checksums
    ------------------------------------------
    | changed | key              | value      |
    ------------------------------------------
    |         | transit.checksums | sha256:md5 |
    ------------------------------------------

visulox config -name transit.hashfile
    ----------------------------------------------
```

```
| changed | key              | value          |
-------------------------------------------------
|         | transit.hashfile | *.md5:*.sha256 |
-------------------------------------------------
```

Once the hash file is uploaded to the Transit Zone, the previous uploaded files change their status to "**accepted**":



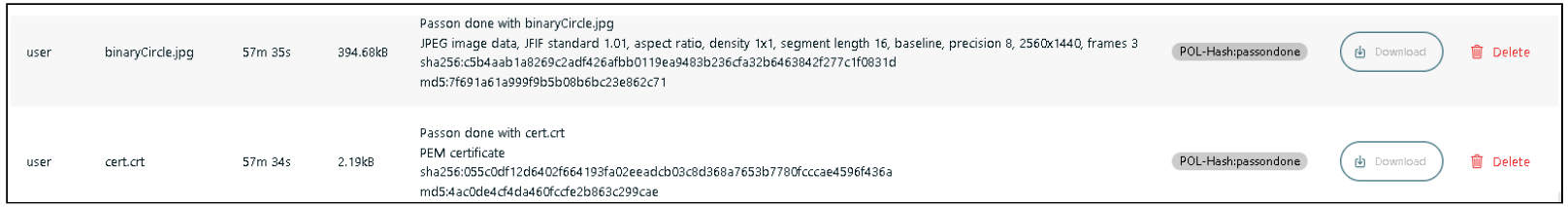
Depending on the policy mode (here policy mode: Allowed), the files are now available for further processing in this case.

> The hash file containing **one** or **more** hash values can be uploaded **before** or **after** the actual files.

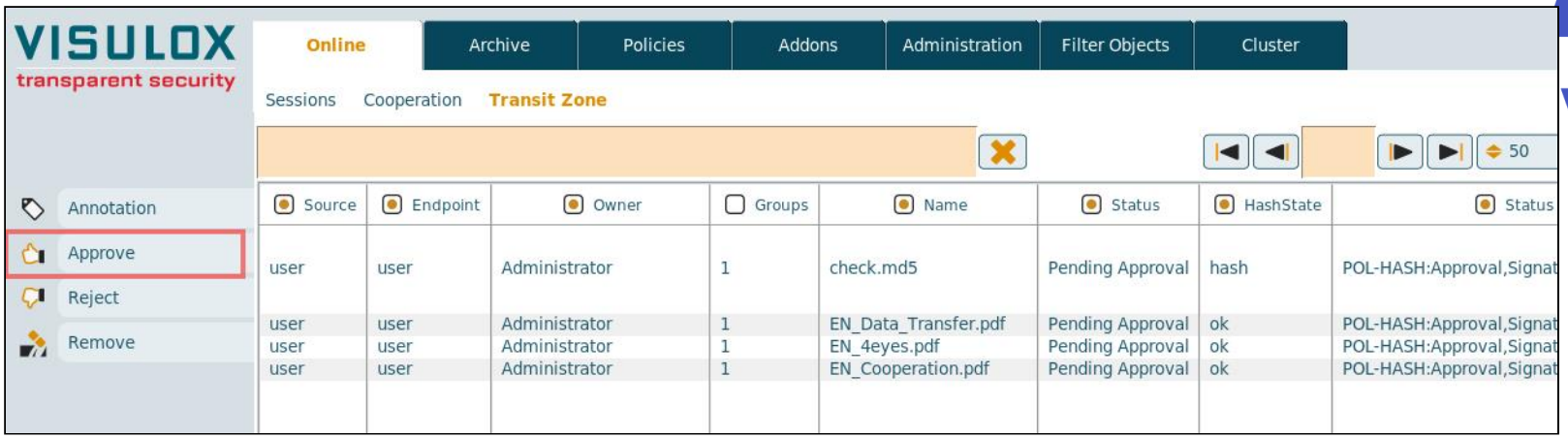
Policy mode: Approval

With the policy mode set to "**Approval**" and hash check enabled, the status is set to status "**Wait for hash file**":

Uploading the hash file changes the status to "**pending**":



Approval is done by a supervisor in VISULOX Cockpit / Online / Transit Zone or via mail with an assigned request script:



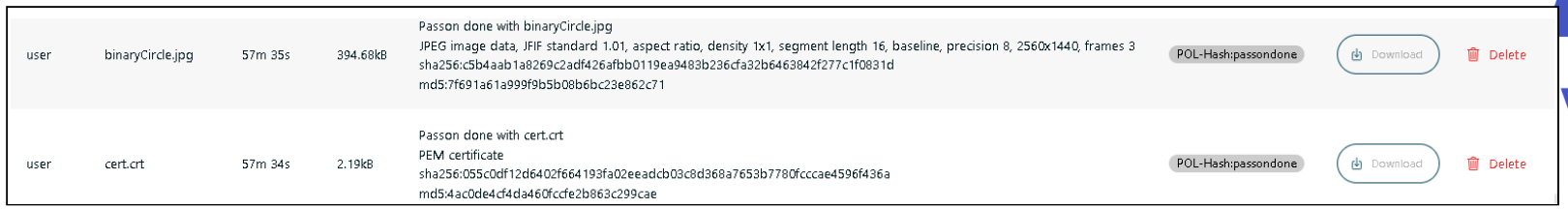
The supervisor is able to approve, reject and remove files. An annotation for a file can also be set.

Approving and rejecting files can also be done via command line interface (see: **VISULOX transit command**) or via mail with assigned request script..

Policy mode: Passon

With the policy mode set to "**Passon**" and hash check enabled, the status is set to status "**Wait for hash file**".

Uploading the hash file changes the status to "**Passon Done**":



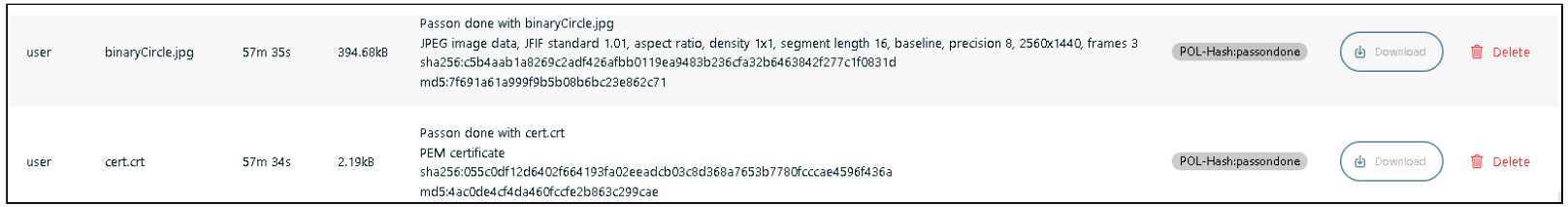
Policy mode: Passon with approval

"**Passon with approval**" is a combined mode of "**Passon**" and "**Approval**".

If the policy mode "**Passon with approval**" is set, the files have to be approved by a supervisor before they are passed on.

Hash information

The hash value of each file is displayed and the hash values included in the hash file are displayed as well in the format column.



VISULOX policy transit command

The command line tool "**VISULOX policy transit**" allows to control the File Transit Policy.

The following subcommands are available:

Command	Description
list	List and print File Transit Policies.
add	Add a File Transit Policy.
edit	Modify fields of a File Transit Policy.
delete	Remove a File Transit Policy.
fields	List available database fields (**-raw** = enhanced output)

File Transit Policy elements (edit):

Element	Description
-name <>	Name of policy or use AUTO

Element	Description
-mode <>	Policy off, allow, approval, deny. Default value: allow.
-hash <>	**Policy hash modes: off, on. Default value: off**
-direction <>	Policy in, out, both. Default value: both
-size <>	Filesize in Kilobytes (k), Megabytes (M), Gigabytes (G). Default value:<50M>
-namepattern <>	Wildcard on filename <>
-pattern <>	Wildcard on file signature <>
-email <>	eMail for approval <>
-endpoint <>	Mask for endpoints <>
-object <>	Policy filter: mask or unique distinguished object of user or group <>
-remoteip <>	Policy filter: remote IP or remote IP mask <>
-accesspoint <>	Policy filter: Access Point <>

Element	Description
-script <>	Trigger script <>
-passon <>	Passon script <>
-comment <>	Comment for the policy. Default value: CLI.
-grant <>	Set granted user in database record <>

Examples

List current available File Transit Policies

```
visulox policy transit list
    ----------------------------
    | basicname |  transitmode |
    ----------------------------
    |  POL-HASH | passedon.map |
    |    NOEXEC |     deny.map |
    |   TRANSIT |  allowed.map |
    ----------------------------
```

List available fields

```
visulox policy transit fields
```

List selected fields

```
visulox policy transit list -fields basicname,transitmode,ft_script,hash
```

Add new File Transit Policy

```
visulox policy transit add -name TRANS1 -mode allow -hash on
```

Edit File Transit Policy

```
visulox policy transit edit -name TRANS1 -direction in
```

Remove an entry

```
visulox policy transit delete -name TRANS1
```

VISULOX transit command

The **visulox transit** command can be used to copy files into the Transit Zone of another user. A standard Transit Policy is applied.

Available commands and their options

approval	Approve or reject pending files in Transit Zone • -state <*value*> Approve / true / 1 Reject / false / 0
import	Import file into a users Transit Zone • -owner <*value*> Unique owner <> • -path <*value*> Path to readable file <> • -rtime <*value*> Retention time in Transit Zone in seconds <*default*>
list	List user's with files in the Transit Zones

Example to import a file for download into the Transit Zone

```
visulox transit import -path <path to file> -owner <unique owner> -rtime <retention time in sec>
```

- Import command needs a standard Transit Policiy with the direction **both** or **out**, **size**, **pattern**, etc.
- The retention time maximum is limited to the lifetime in archive

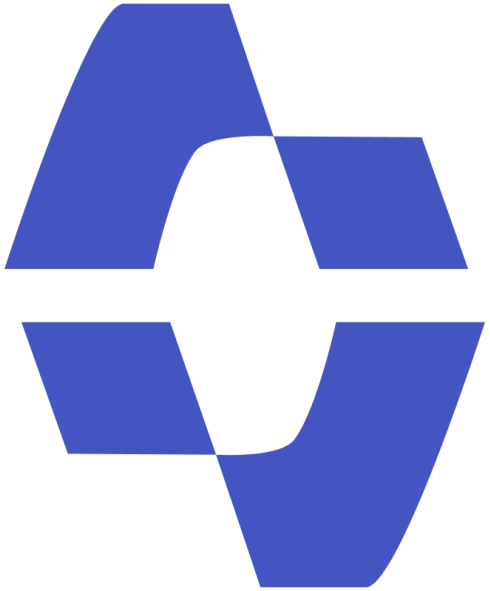
Related articles in documentation

(4.1.1) Accessing the File Exchange web page

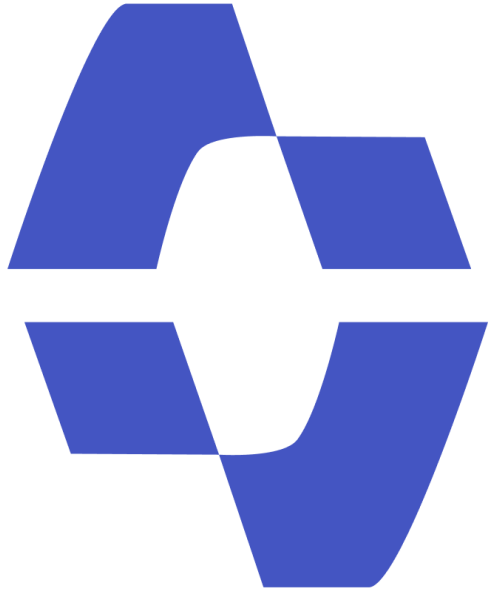
(4.1.1) Allowing File Transfer from internal to internal

(4.1.1) Automated transfer of files into Transit Zone (Passon)

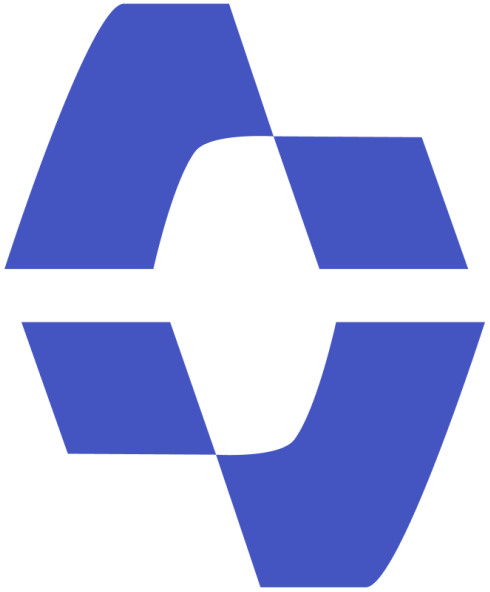
(4.1.1) Command Connect / Guard and FT Client with empty filters



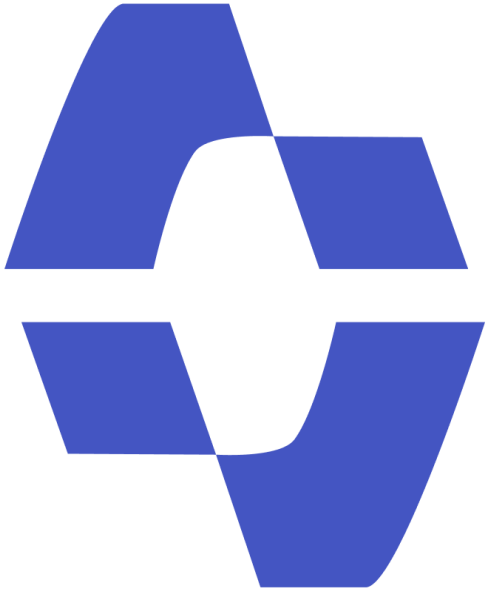
(4.1.1) Configuration of File Transfer in the VISULOX Cockpit
(4.1.1) Custom vlxuser ID for transit users
(4.1.1) Extended Transit Policy with hash check by provided hash file
(4.1.1) File Transfer
(4.1.1) File Transfer features
(4.1.1) File Transfer modules
(4.1.1) File Transfer recommendations
(4.1.1) File Transit with approval
(4.1.1) How to attach Chrome/Chromium download directory to vlxtransit
(4.1.1) How to configure File Transfer content check
(4.1.1) How to control FT Client from the command line
(4.1.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.1.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.1.1) Transit Policy
(4.1.1) Transit script variables
(4.1.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.1.1) VISULOX Transit mapping
(4.1.1) VISULOX Transit Mapping and Ubuntu application servers
(4.1.1) VISULOX4_FileTransfer_(VFT)
(4.2.0) Accessing the File Exchange web page
(4.2.0) Automated transfer of files into Transit Zone (Passon)
(4.2.0) Command Connect / Guard and FT Client with empty filters



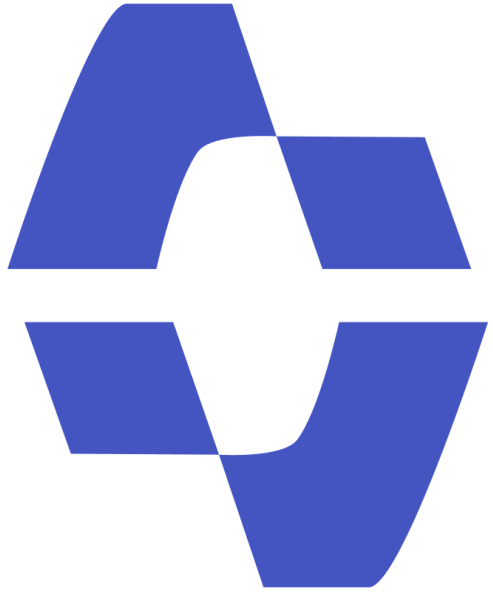
(4.2.0) Configuration of File Transfer in the VISULOX Cockpit
(4.2.0) Extended Transit Policy with hash check by provided hash file
(4.2.0) File Transfer
(4.2.0) File Transfer features
(4.2.0) File Transfer modules
(4.2.0) File Transit with approval
(4.2.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.2.0) How to configure File Transfer content check
(4.2.0) How to control File Transit Policy from the command line
(4.2.0) How to control FT Client from the command line
(4.2.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.2.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.2.0) Transit Policy
(4.2.0) Transit script variables
(4.2.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.2.0) VISULOX Transit mapping
(4.2.0) VISULOX Transit Mapping and Ubuntu application servers
(4.2.0) VISULOX4_FileTransfer_(VFT)
(4.3.0) Accessing the File Exchange web page
(4.3.0) Automated transfer of files into Transit Zone (Passon)
(4.3.0) Command Connect / Guard and FT Client with empty filters
(4.3.0) Configuration of File Transfer in the VISULOX Cockpit



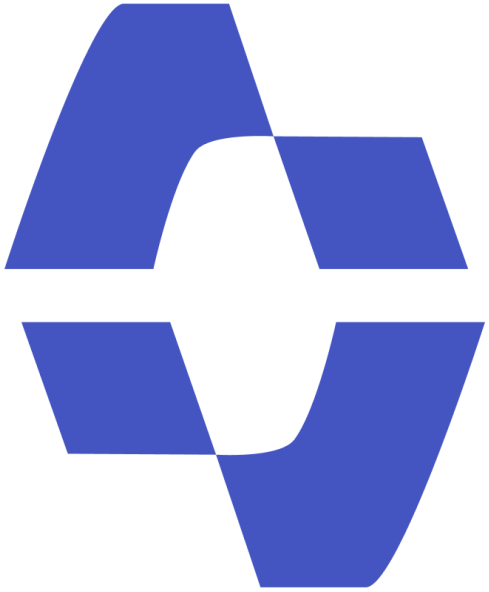
(4.3.0) Extended Transit Policy with hash check by provided hash file
(4.3.0) File Transfer
(4.3.0) File Transfer features
(4.3.0) File Transfer modules
(4.3.0) File Transit with approval
(4.3.0) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.0) How to configure File Transfer content check
(4.3.0) How to control FT Client from the command line
(4.3.0) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.0) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.0) Object ID
(4.3.0) Transit Policy
(4.3.0) Transit script variables
(4.3.0) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.0) VISULOX FTP Service
(4.3.0) VISULOX Transit mapping
(4.3.0) VISULOX Transit Mapping and Ubuntu application servers
(4.3.0) VISULOX4_FileTransfer_(VFT)
(4.3.1) Accessing the File Exchange web page
(4.3.1) Allowing File Transfer from internal to internal
(4.3.1) Automated transfer of files into Transit Zone (Passon)
(4.3.1) Command Connect / Guard and FT Client with empty filters



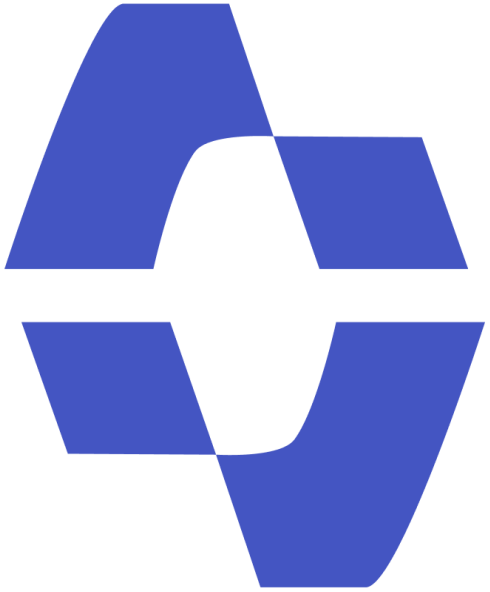
(4.3.1) Configuration of File Transfer in the VISULOX Cockpit
(4.3.1) Custom vlxuser ID for transit users
(4.3.1) Extended Transit Policy with hash check by provided hash file
(4.3.1) File Transfer
(4.3.1) File Transfer features
(4.3.1) File Transfer modules
(4.3.1) File Transfer recommendations
(4.3.1) File Transfer via command line
(4.3.1) File Transit with approval
(4.3.1) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.1) How to configure File Transfer content check
(4.3.1) How to control File Transit Policy from the command line
(4.3.1) How to control FT Client from the command line
(4.3.1) How to discard filetypes from the Transit Zone synchronisation
(4.3.1) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
(4.3.1) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.1) Object ID
(4.3.1) Transit Policy
(4.3.1) Transit script variables
(4.3.1) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.1) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.1) VISULOX FTP Service



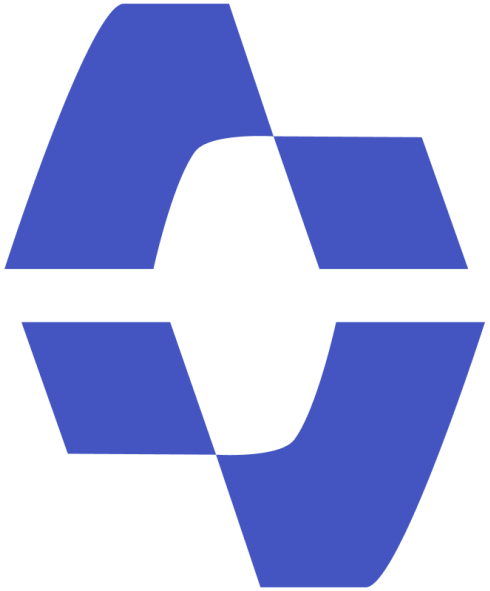
(4.3.1) VISULOX Transit mapping
(4.3.1) VISULOX Transit Mapping and Ubuntu application servers
(4.3.1) VISULOX4_FileTransfer_(VFT)
(4.3.2) Accessing the File Exchange web page
(4.3.2) Allowing File Transfer from internal to internal
(4.3.2) Automated transfer of files into Transit Zone (Passon)
(4.3.2) Command Connect / Guard and FT Client with empty filters
(4.3.2) Configuration of File Transfer in the VISULOX Cockpit
(4.3.2) Custom vlxuser ID for transit users
(4.3.2) Extended Transit Policy with hash check by provided hash file
(4.3.2) File Transfer
(4.3.2) File Transfer features
(4.3.2) File Transfer modules
(4.3.2) File Transfer recommendations
(4.3.2) File Transfer via command line
(4.3.2) File Transit with approval
(4.3.2) How to attach Chrome/Chromium download directory to vlxtransit
(4.3.2) How to configure File Transfer content check
(4.3.2) How to control File Transit Policy from the command line
(4.3.2) How to control FT Client from the command line
(4.3.2) How to discard filetypes from the Transit Zone synchronisation
(4.3.2) How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service



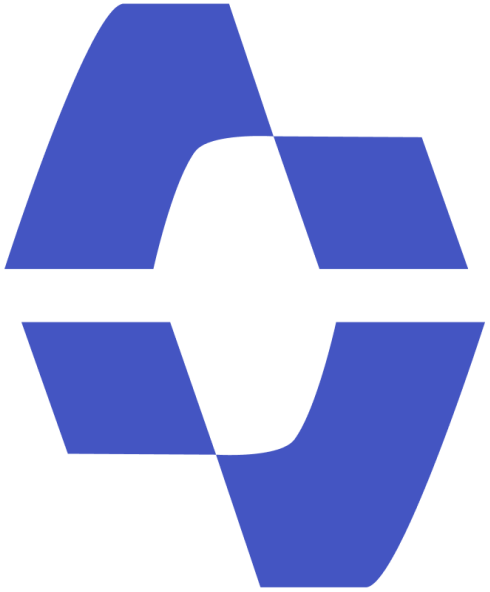
(4.3.2) How to use SSH-Keys within Command Connect / Guard and FT Client
(4.3.2) Object ID
(4.3.2) Transit Policy
(4.3.2) Transit script variables
(4.3.2) VISULOX addon command line interface (CMD Connect / Guard, etc)
(4.3.2) VISULOX File Transit and Sophos Endpoint Security and Control
(4.3.2) VISULOX FTP Service
(4.3.2) VISULOX Transit mapping
(4.3.2) VISULOX Transit Mapping and Ubuntu application servers
(4.3.2) VISULOX4_FileTransfer_(VFT)
Accessing the File Exchange web page
Allowing File Transfer from internal to internal
Automated transfer of files into Transit Zone (Passon)
Command Connect / Guard and FT Client with empty filters
Configuration of File Transfer in the VISULOX Cockpit
Custom vlxuser ID for transit users
Extended Transit Policy with hash check by provided hash file
File Transfer
File Transfer features
(4.3.3) File Transfer modules
File Transfer recommendations
File Transfer via command line



File Transit with approval
How to attach Chrome/Chromium download directory to vlxtransit
How to configure File Transfer content check
How to control File Transit Policy from the command line
How to control FT Client from the command line
How to discard filetypes from the Transit Zone synchronisation
How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
How to use SSH-Keys within Command Connect / Guard and FT Client
Object ID
Transit Policy
Transit script variables
VISULOX addon command line interface (CMD Connect / Guard, etc)
VISULOX File Transit and Sophos Endpoint Security and Control
VISULOX FTP Service
VISULOX Transit mapping
VISULOX Transit Mapping and Ubuntu application servers
(4.3.3) VISULOX4_FileTransfer_(VFT)
(4.1.1) File Transfer via command line
(4.1.1) How to control File Transit Policy from the command line
(4.1.1) How to discard filetypes from the Transit Zone synchronisation
(4.1.1) Object ID
(4.1.1) VISULOX File Transit and Sophos Endpoint Security and Control



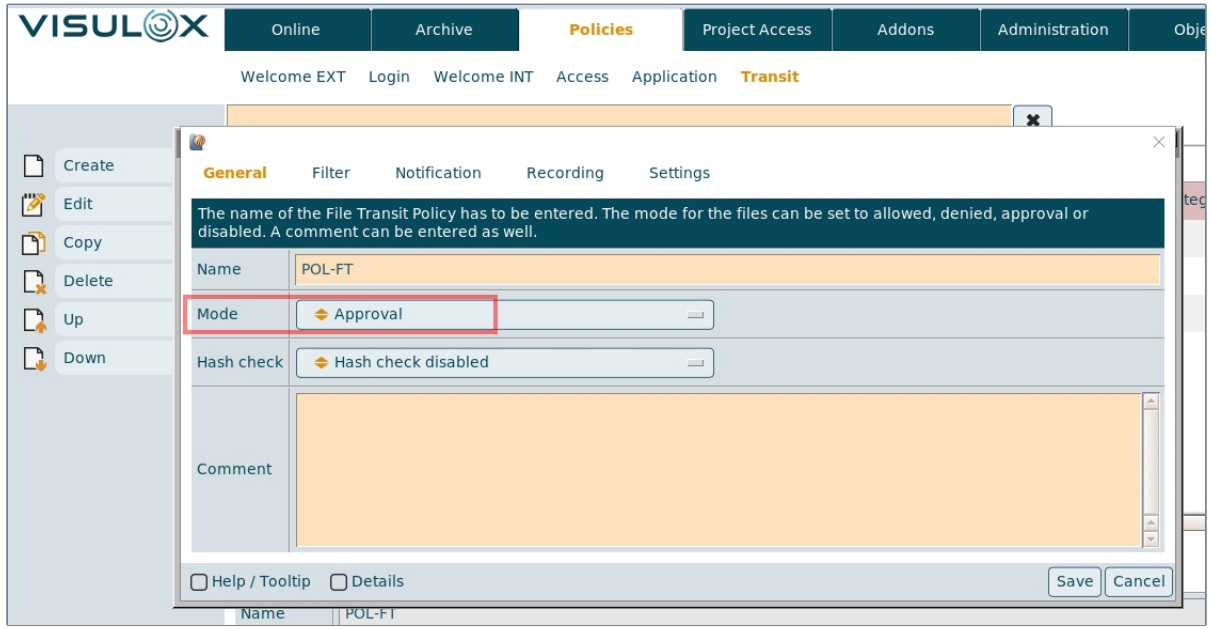
(4.1.1) VISULOX FTP Service
(4.2.0) Allowing File Transfer from internal to internal
(4.2.0) Custom vlxuser ID for transit users
(4.2.0) File Transfer recommendations
(4.2.0) File Transfer via command line
(4.2.0) How to discard filetypes from the Transit Zone synchronisation
(4.2.0) Object ID
(4.2.0) VISULOX File Transit and Sophos Endpoint Security and Control
(4.2.0) VISULOX FTP Service
(4.3.0) Allowing File Transfer from internal to internal
(4.3.0) Custom vlxuser ID for transit users
(4.3.0) File Transfer recommendations
(4.3.0) File Transfer via command line
(4.3.0) How to control File Transit Policy from the command line
(4.3.0) How to discard filetypes from the Transit Zone synchronisation
(4.3.0) VISULOX File Transit and Sophos Endpoint Security and Control
Accessing the File Exchange web page
Allowing File Transfer from internal to internal
Automated transfer of files into Transit Zone (Passon)
Command Connect / Guard and FT Client with empty filters
Configuration of File Transfer in the VISULOX Cockpit
Custom vlxuser ID for transit users



Extended Transit Policy with hash check by provided hash file
File Transfer
File Transfer features
File Transfer modules
File Transfer recommendations
File Transfer via command line
File Transit with approval
How to attach Chrome/Chromium download directory to vlxtransit
How to configure File Transfer content check
How to control File Transit Policy from the command line
How to control FT Client from the command line
How to discard filetypes from the Transit Zone synchronisation
How to setup File Exchange on a VISULOX Node without VISULOX PORTAL Service
How to use SSH-Keys within Command Connect / Guard and FT Client
Object ID
Transit Policy
Transit script variables
VISULOX addon command line interface (CMD Connect / Guard, etc)
VISULOX File Transit and Sophos Endpoint Security and Control
VISULOX FTP Service
VISULOX Transit mapping
VISULOX Transit Mapping and Ubuntu application servers

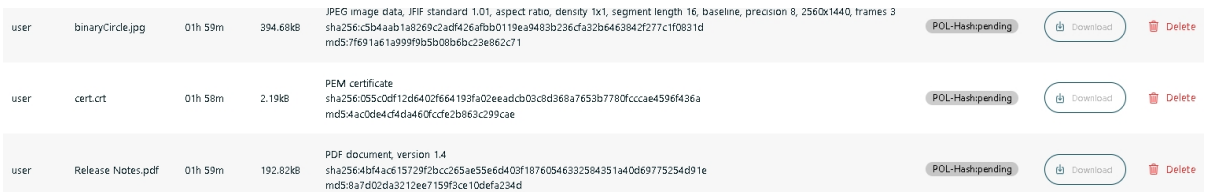
File Transit with approval

The basic setup for File Transit with approval is done by setting the **approval mode** in a Transit Policy:



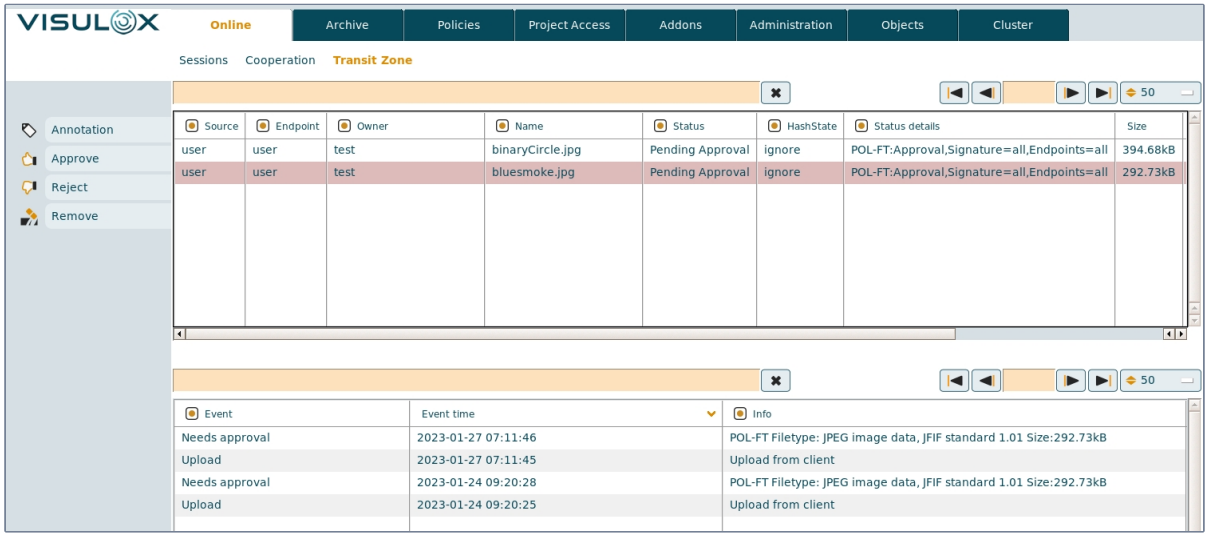
The **filter** settings have to be entered and a **notification** can be sent to an approver via action script, once a file is uploaded.
In the **settings** tab, the file based filter criteria can be set as usual.

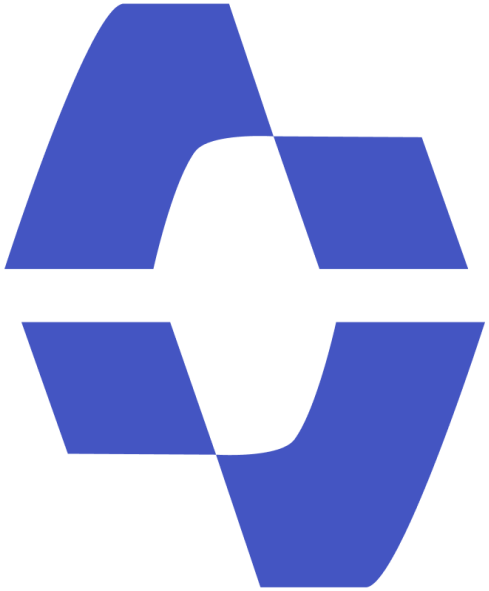
The user is able to see the uploaded files in his Workspace with the status: "**pending**":



Keep an eye on the lifetime for files in the Transit Zone.

The approver is able to see the current files and their status in **VISULOX Cockpit / Online / Transit Zone**:





Here the selected files can be **approved**, **rejected**, **removed** and an **annotation** can be entered.
Once a file is approved, the user is allowed to use the file in Transit Zone. Status is set to "**Allowed**".

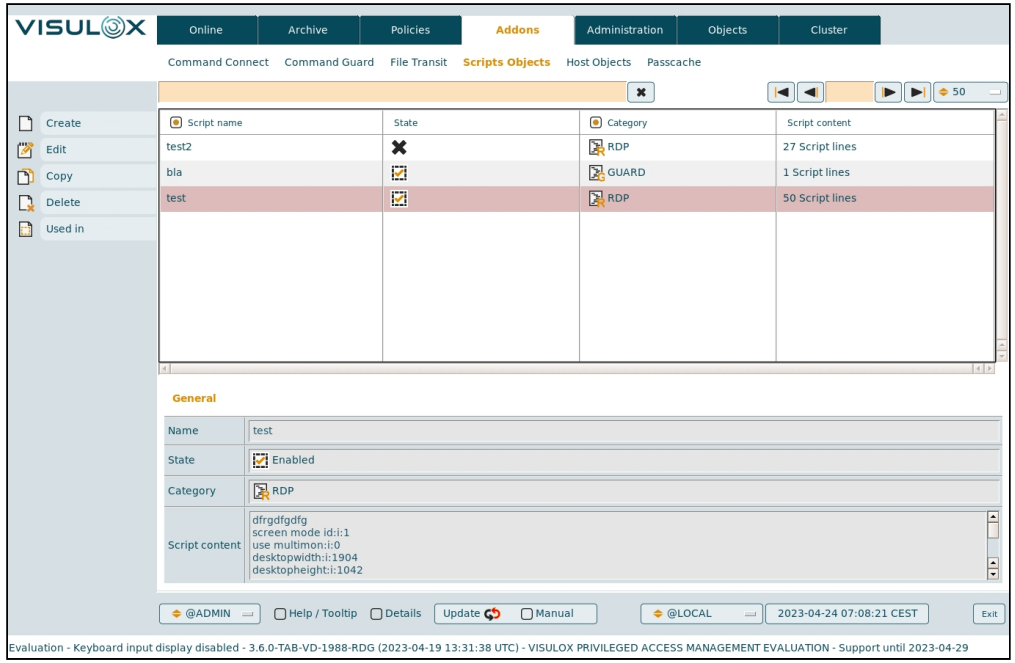
There are a lot more configuration options for File Transfer with approval depending on the used File Transfer method.

Also have a look at the following articles:

- Transit Policy
- Access and transit request via actionlink
- Automated transfer of files into Transit Zone (Passon)
- Extended Transit Policy with hash check by provided hash file

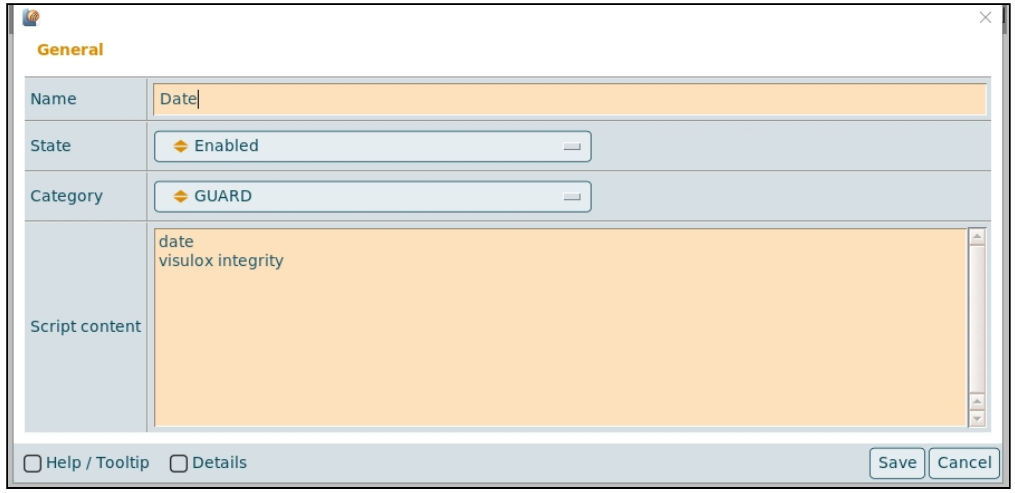
23.1.78 Script objects

System side scripts can be assigned to Command Guard and can be issued to the terminals at any time. As long the terminals belong to the group.
 	
RDP configuration files can be assigned as well to freerdp sessions.
RD Gateway authentication with common users is supported.
	• Command Guard system side shell scripts
	  • Assigning scripts to a Command Guard group
	  • Script writing rules
	• RDP configuration files
	  • vlxshell application with freerdp configuration file



Command Guard system side shell scripts

In Command Guard, it is possible to start such scripts in a single shell or in all connected shells at once.
Script category must be set to **GUARD**.

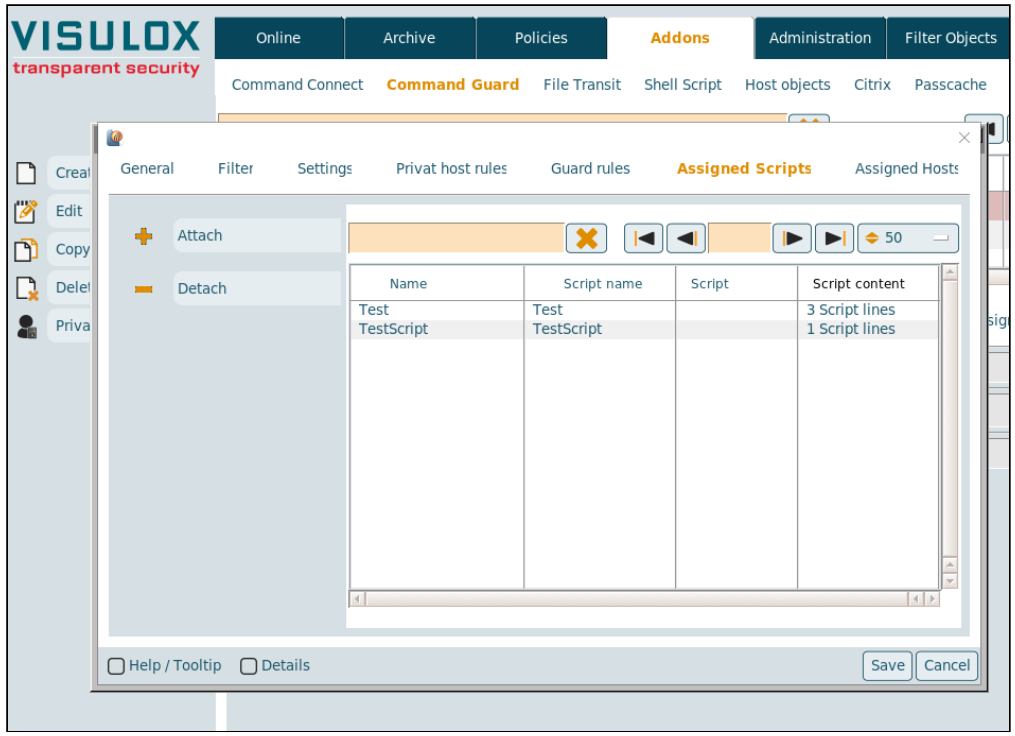


The script size is limited to 40 KB.

The size and the type of the script is configured here:

```
visulox config -name scriptobject.guard
    ------------------------------------------
    | changed | key                    | value  |
    ------------------------------------------
    |         | scriptobject.guard.size | 40.0kB |
    |         | scriptobject.guard.type | text   |
    ------------------------------------------
```

Assigning scripts to a Command Guard group



Available scripts can be attached / detached from the Command Guard group.

Script writing rules

A script is a list of lines. Mostly they are representing shell scripts.

For example:

Script

```
echo here
date
uptime
ntpq -p
```

Output

```
# echo here
here
#  date
Tue Jan 12 17:15:53 CET 2016
#  uptime
 17:15:53 up 25 days,  2:36,  9 users,  load average: 0.20, 0.20, 0.22
#  ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*xyz.tbsol.de     144.23.187.145   3 u  568 1024  377    0.862   -2.353   1.428
+xxx.tbsol.de    172.10.1.1      12 u   35 1024  377    0.458  -15.297  16.387
#
```

It would be better to put the commands into brackets:

Script

```
(
  echo here
  date
  uptime
  ntpq -p
)
```

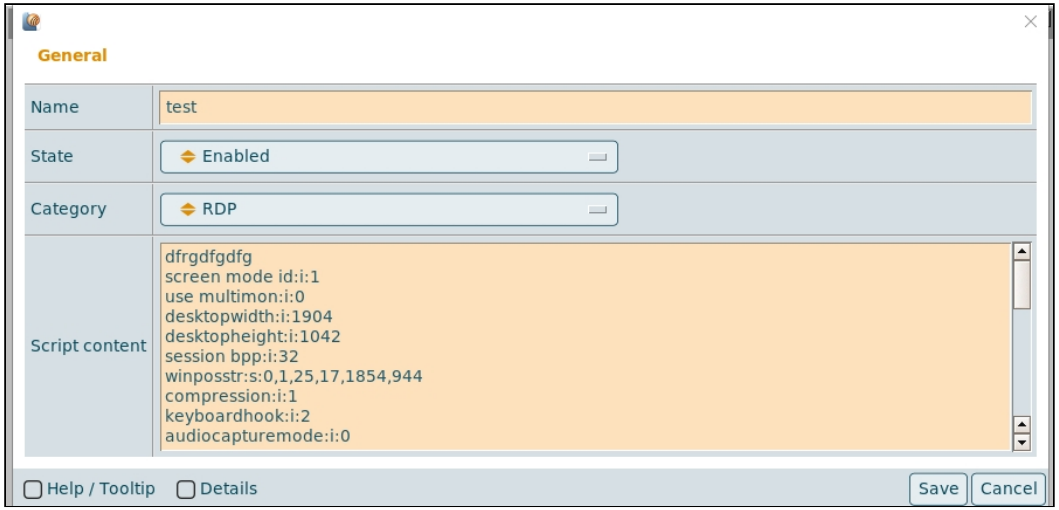
Output

```
# (
>  echo here
>  date
>  uptime
>  ntpq -p
> )
here
Tue Jan 12 17:06:36 CET 2016
 17:06:36 up 25 days,  2:27,  9 users,  load average: 0.28, 0.25, 0.24
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*xyz.tbsol.de     144.23.187.145   3 u   11 1024  377    0.862   -2.353   1.428
+xxx.tbsol.de    172.10.1.1       4 u  560 1024  377    0.296  -12.838  14.940
# uptime
 17:06:49 up 25 days,  2:27,  9 users,  load average: 0.32, 0.26, 0.24
[root@tab-ol6u4-sgd1-510 ~]#
```

RDP configuration files

In a vlxshell application, it is possible to use such a script for the freerdp connection.

Script category must be set to **RDP**.

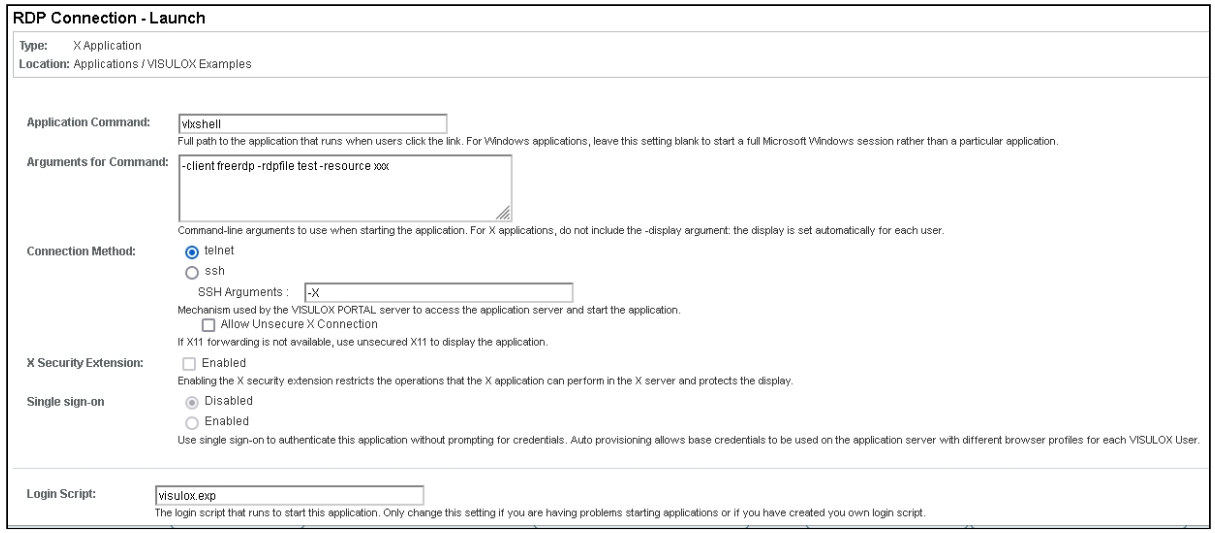


The script size is limited to 4 KB.

The size and the type of the script is configured here:

```
visulox config -name scriptobject.rdp
    ----------------------------------------
    | changed | key                  | value |
    ----------------------------------------
    |         | scriptobject.rdp.size | 4.0kB |
    |         | scriptobject.rdp.type | ASCII |
    ----------------------------------------
```

vlxshell application with freerdp configuration file



In this example a preconfigured **VISULOX resource** is used for the credentials of the RDP connection.

vlxshell parameters in "Arguments for Command":

```
-client freerdp -rdpfile <scriptname|filename> -- <freerdp-parameter>
```

vlxshell parameters with RD Gateway configuration:

```
-client freerdp -rdpfile RDP -resource <resource-name> -gateway-resource <resource-name> /g:<server.domain> /gateway-usage-
method:direct
```

To add an existing RDP file to the VISULOX Cluster, use:

```
visulox addon script add -name RDP -category rdp -script /tmp/testfile.rdp
```

For more RDP connection events, set:

```
visulox config -name vlxshell.event.rdpconnect=true
```

See also: How to configure FreeRDP for VISULOX PORTAL

How to control script objects from the command line

Overview The command line tool "**VISULOX addon script**" allows to control VISULOX shell scripts for Command Guard and RDP files used in a vlxshell application.	• Overview • Usage • Shell script elements (edit) • Examples

Usage

The following subcommands are available:

Command	Description
list	List and print shell scripts.
add	Add a shell script.
edit	Modify fields of a shell script.
delete	Remove a shell script.

Shell script elements (edit)

Element	Description
-name<>	Name of the script entry in the database <>
-category <>	Script category rdp / guard. Default value: rdp
-mode <>	Script enabled / disabled. Default value: on.
-script <>	Path to a readable existing script file "<>arg1 arg2 arg3"
-grant <>	Set granted user in database record <>

Examples

List current available shell scripts

```
visulox addon script list

    -------------
    | basicname |
    -------------
    |    Check1 |
    |    Check2 |
    -------------
```

Add script

```
visulox addon script add -name Check3 -category guard -script /tmp/test3
```

Add an existing RDP file to the VISULOX Cluster

```
visulox addon script add -name RDP -category rdp -script /tmp/testfile.rdp
```

Edit shell script

```
visulox addon script edit -name Check3 -category guard -mode off -script /tmp/test4
```

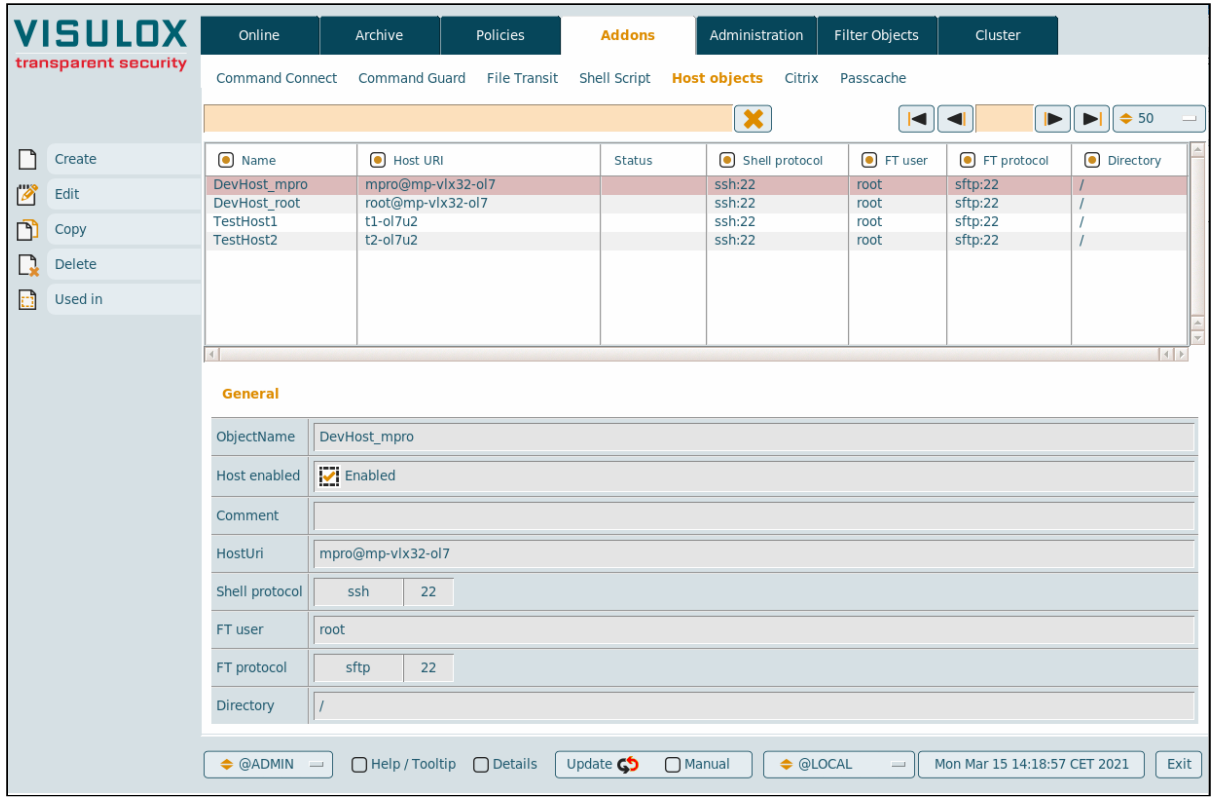
Remove an entry

```
visulox addon script delete -name Check3
```

23.1.79 Host objects

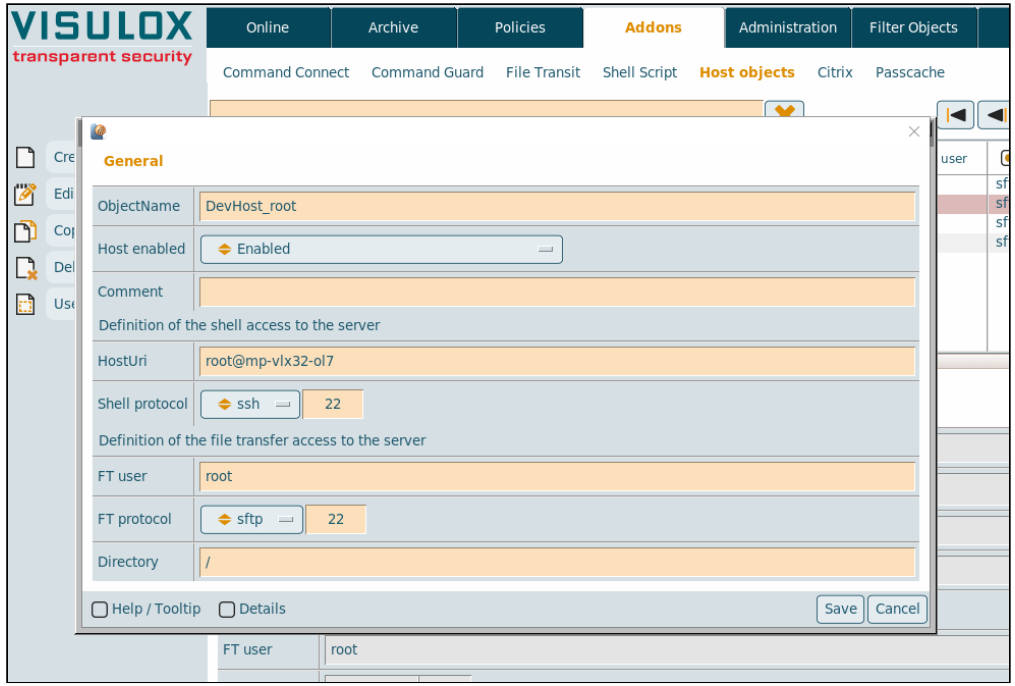
Host objects are available for File Transit, Command Guard and Command Connect groups.	• Host objects
	• Configuration
	  • Assigning a new host object to a Command Connect / Guard group
	  • Temporary hosts group

Host objects



New host objects can be created and existing objexts can be edited, copied or deleted.

With the **Used in** button It is possible to display, where the selected host is being used



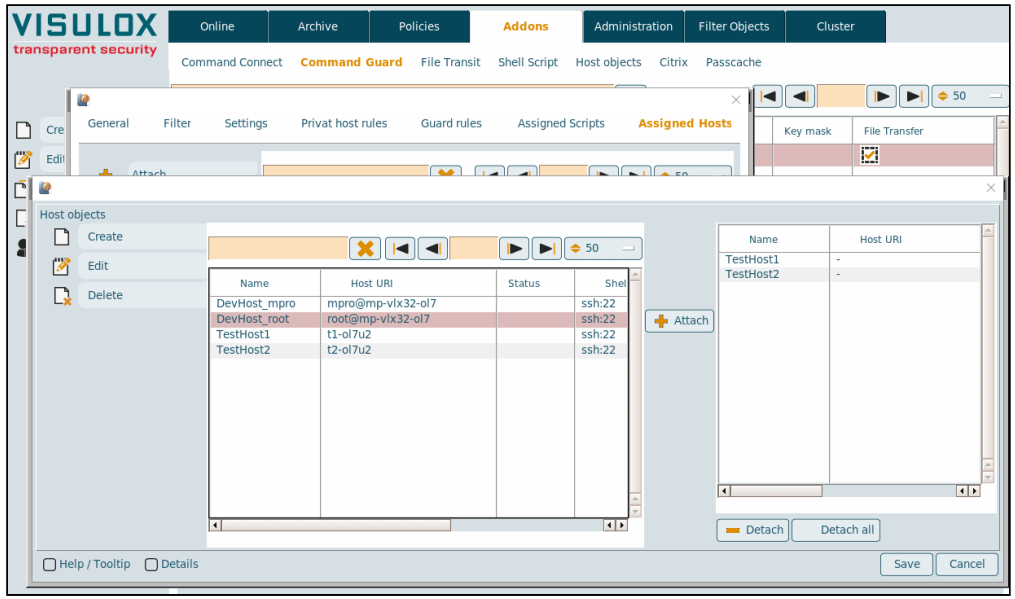
Setting	Description
Object name	Name of the host object (must be unique)

Setting	Description
Host enabled	Host enabled or disabled
Comment	Comment for the host
Host URI	Uniform Ressource Identifier: <*user*>@<*host*>, <*host*>, %USER%@<*host*>
Shell protocol	Shell protocol: SSH or Telnet and the port
FT user	File Transfer user for the access to the server
FT protocol	File Transfer protocol: SFTP, FTP.active or FTP.passive and the port
Directory	The base directory on the server

%USER% variable

- %USER *% will always be replaced with the username
- Also possible: %USER%@host, %USER1%@host, %USER2%@host
- The placeholder %USER% is always replaced by "vlxloginuser"
    - In case of the datastore: the name in the surname field (SN)
    - In case of Active Directory: the SAMAccountName
    - In case of LDAP: the UID

Assigning a new host object to a Command Connect / Guard group



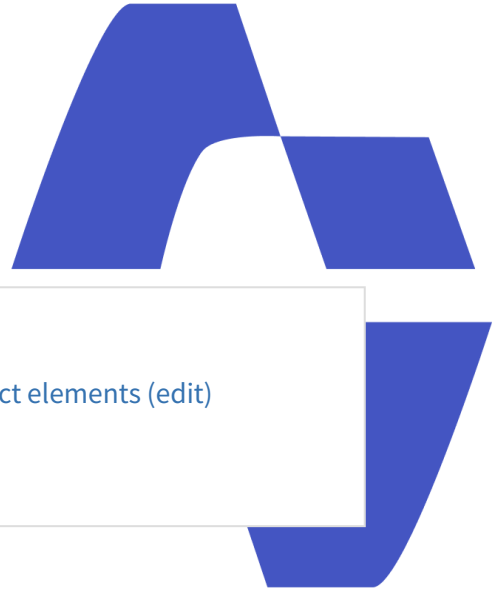
Host objects can be attached / detached from the Command Connect / Guard group.

Before hosts can be added to a new created group, the group must be saved once.

Temporary hosts group

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

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



How to control host objects from the command line

Overview

The command line tool "**VISULOX addon host**" allows to control the VISULOX host objects..

- Overview
- Usage
- Host object elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print host objects.
add	Add a host object.
edit	Modify fields of a host object.
delete	Remove a host object.
fields	List available database fields (**-raw** = enhanced output)

Host object elements (edit)

Element	Description
-name <>	Name of the host object in the database <>
-endpoint <>	URI to address the endpoint e.g. ssh://user@host <>
-comment <>	Comment for enpoint <CLI>
-mode <>	Endpoint enabled / disabled. Default value: on.
-ftprotocol <>	FT protocol e.g. ftp.passive:port <sftp:22>
-ftuser <>	Alternate FT user for this endpoint <>
-ftdir <>	FT directory for this endpoint <~>
-grant <>	Set granted user in database record <>

Examples

List current available host objects

```
visulox addon host list

    ------------------------------------------------
    |        basicname | host_enabled | sh_protocol |
    ------------------------------------------------
    | test1.amitego.de |  enabled.map |      ssh:22 |
    | test2.amitego.de | disabled.map |   telnet:23 |
    ------------------------------------------------
```

Add host object

```
visulox addon host add -name "Test3" -endpoint test3.amitego.de
```

Edit host object

```
visulox addon host edit -name "Test3" -mode off
```

Remove an entry

```
visulox addon host delete -name "Test3"
```

Private host tool

Users are able to add and configure their own hosts in Command Connect / Guard. These hosts are called private hosts.

Rules can be configured in Command Connect and Command Guard what kind of hosts / networks can be addressed by the user.

During operation users are removed from the environment and then the obsolete private host entries can be removed from time to time.

This maintenance task can be done with the private host tool:

```
/opt/visulox/lib/utils/privateHost.tcl
```

Available parameters:

Parameter	Description
info	Users with private hosts which are not known in the datasources
list	List the usage (see: -fields)
purge	Remove orphaned entries
-fields <*value*>	List of fields in output <user,host,protocol,comment>

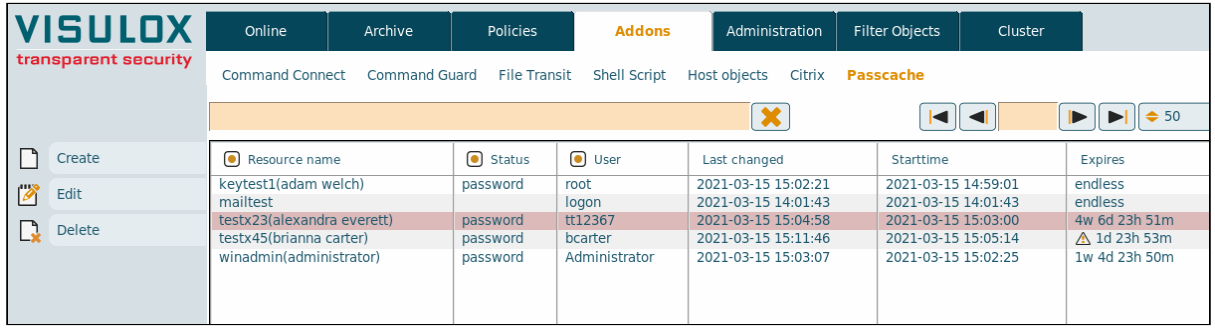
23.1.80 Passcache

Passcache is available for applications, File Transit, Command Connect and Command Guard.

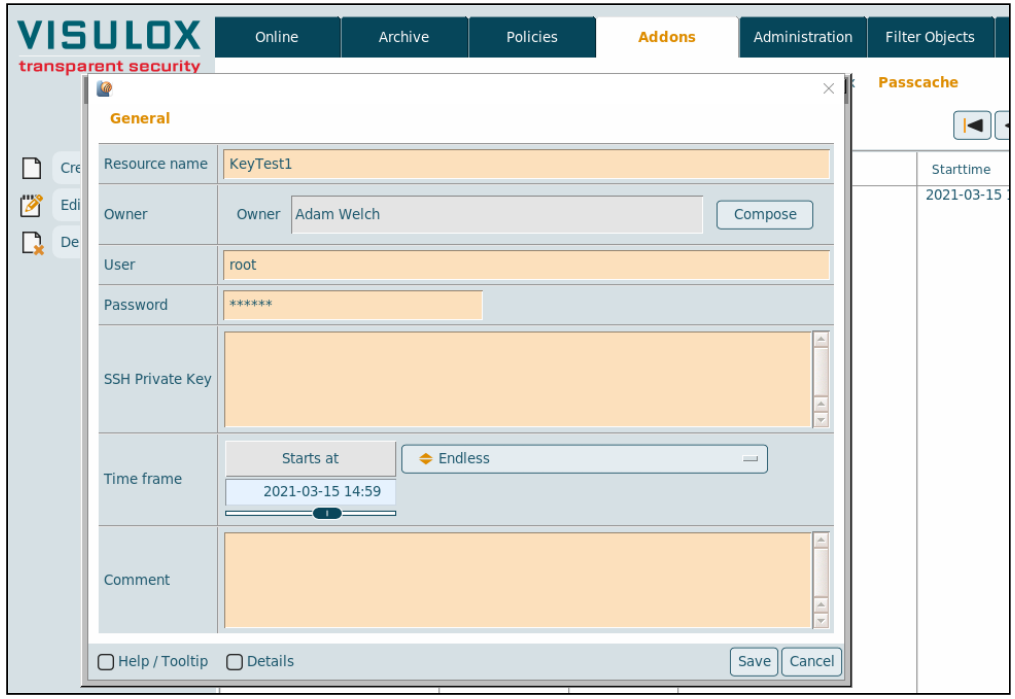
- Passcache
- Configuration
- SMS4
- Related articles

Passcache works for RDP and SSH. (**NOT** TELNET! If needed, please request implementation).

Passcache



New passcache entries can be created and existing entries can be edited or deleted.


VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
Passcache
General
Resource name
KeyTest1
Owner
Owner
Adam Welch
Compose
User
root
Password
******
SSH Private Key
Time frame
Starts at
Endless
2021-03-15 14:59
Comment
Help / Tooltip
Details
Save
Cancel
Starttime
2021-03-15

Setting	Description
Resource name	Name of the resource. A resource is limited to 15 characters, alphanumeric only.
Owner	Assigned user to the resource (leave empty for global ressources)
User	Resource user (%USER% variable can be used)
Password	Resource password
SSH Private key	Resource SSH Private Key
Time frame	Time frame. If expiration time is reached, the entry will be deleted.
Comment	Comment for the resource

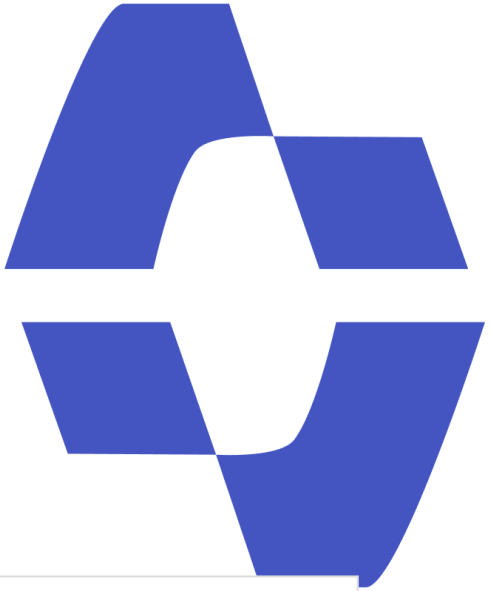
If an owner is set, the owner must be set also, where the resource is used, e.g. Command Connect resource field: ***<resource-name>*%OWNER%**

For standard applications, a resource can be set in the hint field of the application with **vlxResource=*<resource-name>***.

SMS4

Important: SMS4 needs three elements: CustomerID, a user and a password. VISULOX resource can manage only two elements: user and password.
For SMS4 the resuser is a concatenation of CustomerID and user with a "**:**".

```
visulox passcache edit -resource SMS4 -resuser <KDNR:USER> -respwd <PASSWORD>
```



Related articles

How to configure FreeRDP for VISULOX PORTAL

How to control passcache from the command line

How to control FT Client from the command line

VISULOX addon command line interface (CMD Connect / Guard, etc)

How to control passcache from the command line

Overview

The command line tool "**VISULOX passcache**" allows to control VISULOX passcache entries.

Passcache works for RDP and SSH.
(**NOT** TELNET! If needed, please request implementation).

- Overview
- Usage
- passcache entry elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print passcache entries.
edit	Edit/create a passcache entry.
fields	Modify fields of a passcache entry.

Command	Description
delete	Remove a passcache entry.

passcache entry elements (edit)

Element	Description
-resource <>	Resource <>*
-object <>	Mask or unique distinguished owner <>
-starttime <>	Start time of the resource: now or timestring. Default: <now>
-endtime <>	Resource expiration: endless or timestring. Default: <endless>**
-resuser <>	Resource user <> (%USER% variable can be used)
-reskey <>	Resource keys <>
-respass <>	Resource password (- from stdin) <> (Environment variable VLX_SECRET can be used)

Element	Description
-comment <>	Resource comment. Default <CLI>
-grant <>	Set granted user in database record <>

*A resource is limited to 15 characters, alphanumeric only.
**If expiration time is reached, the entry will be deleted.

-object <owner>: A resource for the user is created and will be addressed with [%OWNER%].

-resource <suffix> -object <owner>: A resource for the user is created and will be addressed with [<suffix>(%OWNER%)].

For Command Connect / Command Guard the resource is either

- **-resource <resourcename>** for all hosts, which have no explicit user name.

or

- **-hosts ssh://[<resourcename>]@<host>** , a user in brackets is treated as a resource in password cache.

Examples

List current available passcache entries

```
visulox passcache list

    ------------------------------------------------------------------------
```

```
| basicname | keystatus |       resuser | endtime |           starttime |
-------------------------------------------------------------------------
|  winadmin |           | Administrator | endless | 2019-10-07 10:17:23 |
-------------------------------------------------------------------------
```

Create passcache entry

```
visulox passcache edit -resource WinAdmin -resuser Administrator -respass
/opt/visulox/bin/apps/vlxshell.tcl -client freerdp -resource winadmin -- off-wts
```

Creating a resource [WIN:owner]

```
visulox passcache edit -resource win -object test -resuser tbsol\\test1 -respass
/opt/visulox/bin/apps/vlxshell.tcl -client freerdp -resource win%OWNER% -- off-wts
```

Remove an entry

```
visulox passcache delete -resource WinAdmin
```

23.1.81 How to control the VISULOX Cockpit

Controlling the VISULOX Cockpit

The VISULOX Cockpit is provided as a resumable and uncontrolled application as default.

This means, **vlxMode=NOSC** is set and the usage of the Cockpit cannot be restricted by an Access or Application Policy.

In general a recording of the Cockpit is not needed or does not make sense.

In contrast the access to the the Cockpit has to be under control, based on the Company's Security Rules, i.e. usage in Dual Control mode, usage from a dedicated remote IP or over a dedicated access point.

To achieve this, the VISULOX Cockpit has to be enabled for session control.

Remove **vlxMode=NOSC** from the application in the datastore.

Now all Access and Application Policies will be applied.

VISULOX Cockpit / vlxgui parameters

Parameter	Description
-title <*value*>	GUI title <>
-lang <*value*>	Language <>
-roles <*value*>	Role or role list. Default: <@ADMIN>
-grant <*value*>	Override the granting user <>
-groupaccess <*value*>	Access Profile for Group Access Manager <>
-project	Enable Project Access Manager
-projectmask <*value*>	Project mask (only with -project). Default: <*>
-ksr	Enforce displaying keyboard input lines in @ADMIN role

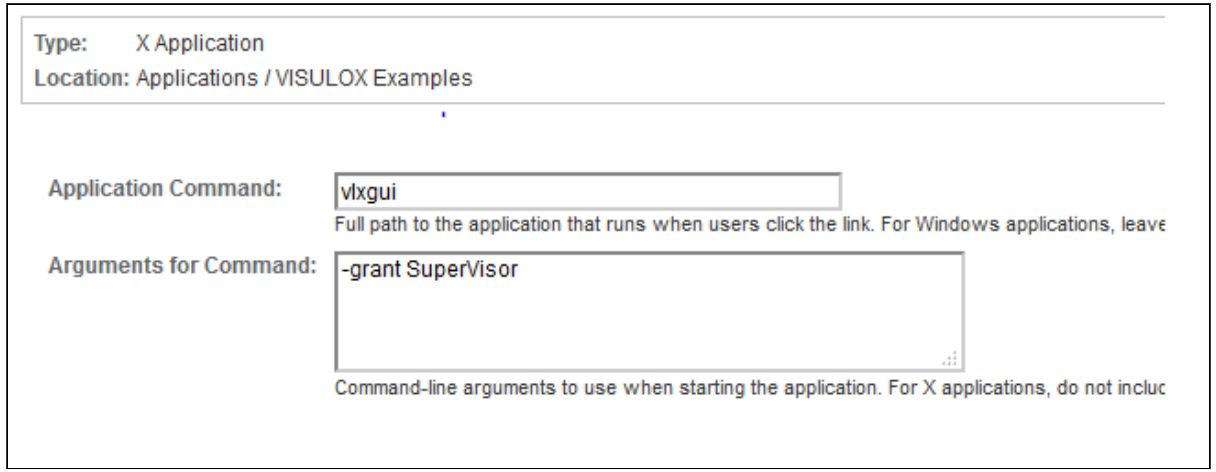
Parameter	Description
-kiosk	Use the whole screen
-personal	Use vlxgui in personal mode. The user's data only
-approver <*value*>	eMail of Approver: SESSION, REQUEST or ANY for request via GUI NONE: No approver. Cookpit user can approve all SESSION: Cookpit user can approve his tagged files only REQUEST: Approver mail will be requested once ANY: Approver mail can be changed
-sendlink <*value*>	Provide Checkout link via email to ZIP of files

See also: How to handle access for groups / Restrict default VISULOX Cockpit / How to configure role profiles for the VISULOX Cockpit

Starting VISULOX Cockpit with parameter -grant

All changes done in the Cockpit will be registered under the name of the user, who has started the Cockpit session.

If it is wanted, that certain changes are registered under another name (e.g. Supervisor, System, etc), this can be done with the **-grant** parameter in the "Arguments for Command" field of the application definition:



This vlxgui parameter will override all **created_by** and **updated_by** entries.

Changing the number of the displayed entries per page

```
visulox config -name guidefaults.sql.pager
    ------------------------------------------------
    | changed | key                   | value        |
    ------------------------------------------------
    |         | guidefaults.sql.pager | 50:75:100:250 |
    ------------------------------------------------
```

23.1.82 How to enable the VISULOX Cockpit for Dual Control and view films in player

Depending on a business process Dual Control is requested for viewing information in the VISULOX Cockpit. This includes also the recorded films.

Steps for the VISULOX PORTAL Datastore

Application definition:

- Give object a name to identify for Dual Control
- Remove environment variable **vlxMode=NOSC**
- Set environment variable **vlxMode=WM**
- Set presentation to **Independent Window**

VISULOX configuration steps

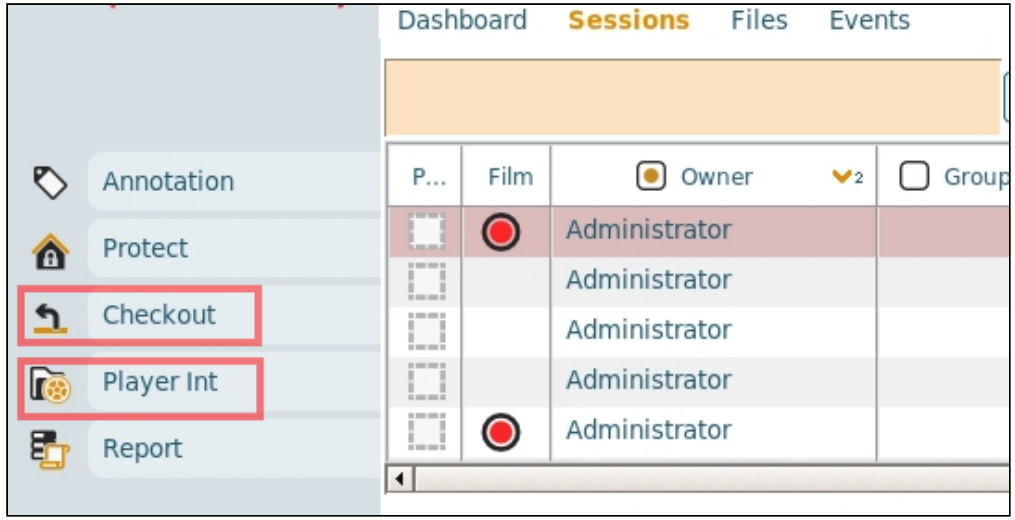
- Define Application Policy for the VISULOX Cockpit with the name from above, setting Dual Control to enabled

See also:

VISULOX Player: integrated or client side

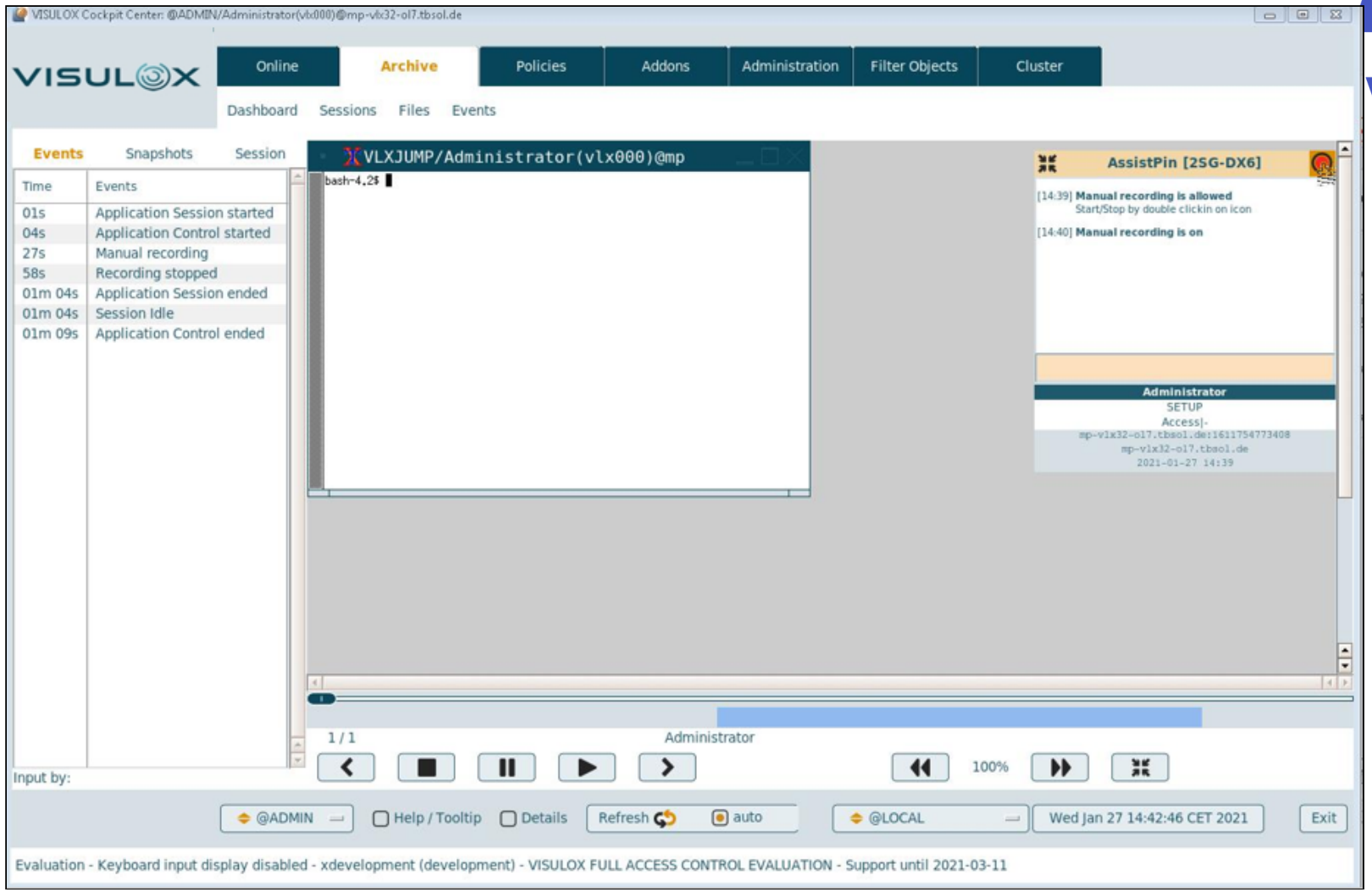
VISULOX Player: integrated or client side

VISULOX flims can be watched in the VISULOX Cockpit (integrated) or they can be checked out and are presented in the offline player (client side):

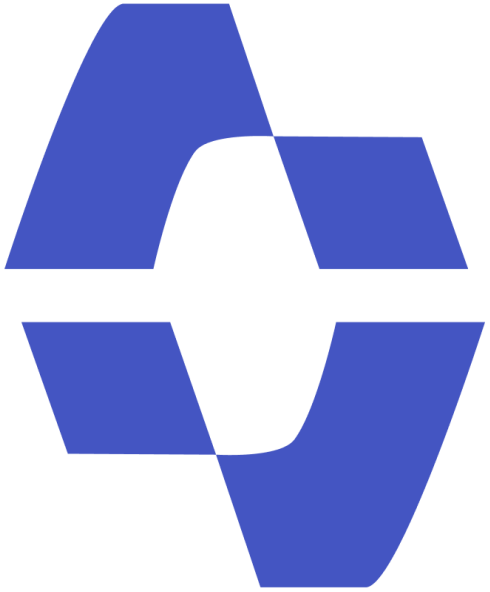


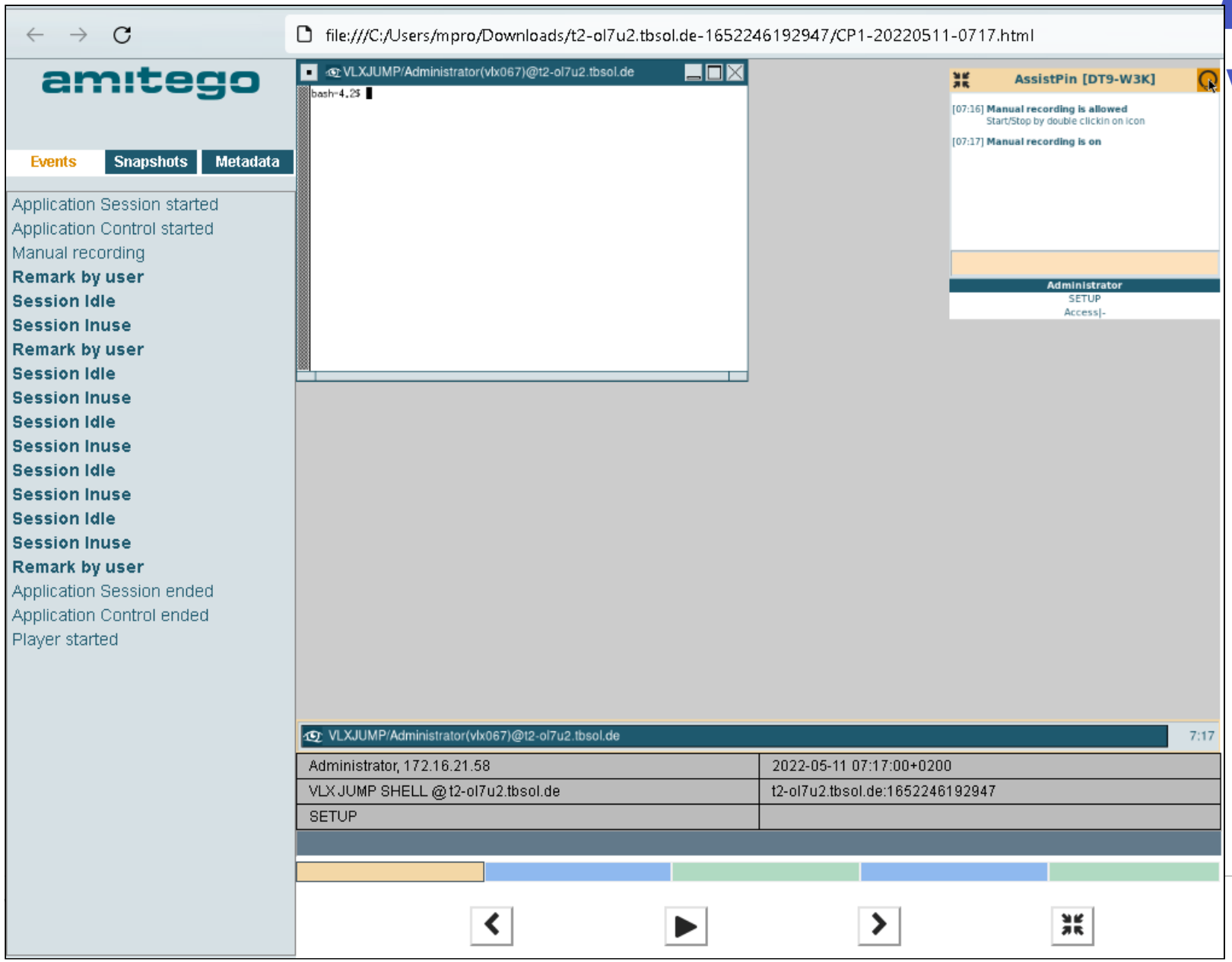
The server side player in the Cockpit has the advantage, that the inspection can be done in Dual Control or assisting mode.

Integrated player in the VISULOX Cockpit:


VISULOX Cockpit Center: @ADMIN/Administrator(vlx000)@mp-vlx32-ol7.tbsol.de
VISULOX
Online
Archive
Policies
Addons
Administration
Filter Objects
Cluster
Dashboard
Sessions
Files
Events
Events
Snapshots
Session
Time
Events
01s Application Session started
04s Application Control started
27s Manual recording
58s Recording stopped
01m 04s Application Session ended
01m 04s Session Idle
01m 09s Application Control ended
VLXJUMP/Administrator(vlx000)@mp
bash-4.2$
AssistPin [2SG-DX6]
[14:39] Manual recording is allowed
Start/Stop by double clickin on icon
[14:40] Manual recording is on
Administrator
SETUP
Access|-
mp-vlx32-ol7.tbsol.de:1611754773408
mp-vlx32-ol7.tbsol.de
2021-01-27 14:39
1 / 1
Administrator
100%
Input by:
@ADMIN
Help / Tooltip
Details
Refresh
auto
@LOCAL
Wed Jan 27 14:42:46 CET 2021
Exit
Evaluation - Keyboard input display disabled - xdevelopment (development) - VISULOX FULL ACCESS CONTROL EVALUATION - Support until 2021-03-11

VISULOX offline player




file:///C:/Users/mpro/Downloads/t2-ol7u2.tbsol.de-1652246192947/CP1-20220511-0717.html
amitego
Events
Snapshots
Metadata
Application Session started
Application Control started
Manual recording
Remark by user
Session Idle
Session Inuse
Remark by user
Session Idle
Session Inuse
Session Idle
Session Inuse
Session Idle
Session Inuse
Session Idle
Session Inuse
Remark by user
Application Session ended
Application Control ended
Player started
VLXJUMP/Administrator(vlx067)@t2-ol7u2.tbsol.de
bash-4.2$
AssistPin [DT9-W3K]
[07:16] Manual recording is allowed
Start/Stop by double clickin on icon
[07:17] Manual recording is on
Administrator
SETUP
Access|-
VLXJUMP/Administrator(vlx067)@t2-ol7u2.tbsol.de
7:17
Administrator, 172.16.21.58
2022-05-11 07:17:00+0200
VLX JUMP SHELL @t2-ol7u2.tbsol.de
t2-ol7u2.tbsol.de:1652246192947
SETUP

The offline player has three tabs: Events, Snapshots and Metadata.
A footnote with information about the session is attached on the bottom of the film.

How to install Google Chrome

Installation

Sadly, the Google Chrome browser no longer supports the most famous commercial distribution Red Hat and its free clones such as CentOS and Scientific Linux.

Installation can be done with:

Installation

```
yum install https://dl.google.com/linux/direct/google-chrome-stable_current_x86_64.rpm
```

Start

Login not as "root"

```
# google-chrome
```

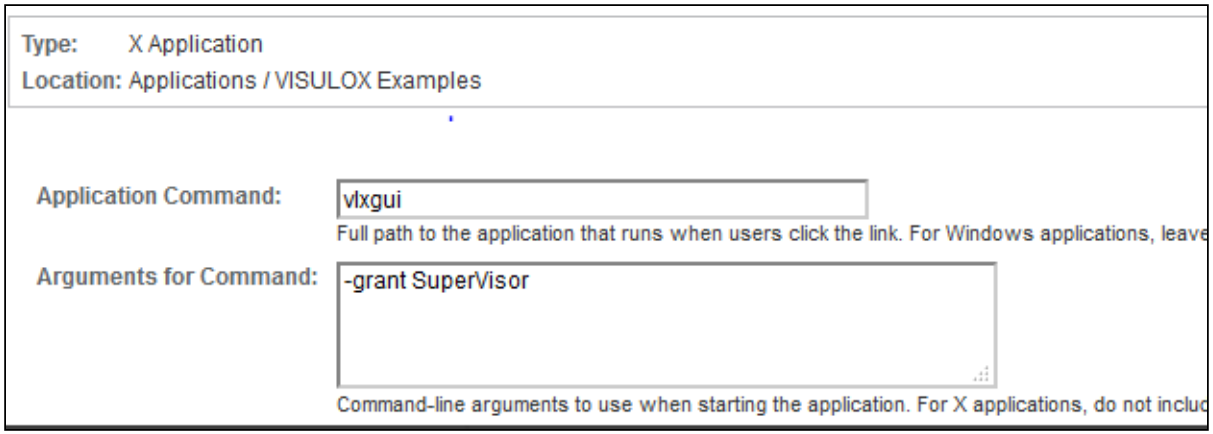
Google Chrome does not start with user "root"!

23.1.83 Starting VISULOX Cockpit with parameter -grant

All changes done in the VISULOX Cockpit will be registered under the name of the user, who has started the Cockpit session.

If it is wanted, that certain changes are registered under another name (e.g. Supervisor, System, etc).

This can be done with the **-grant** parameter in the "**Arguments for Command**" field of the application definition:



This **vlxgui** parameter will override all **created_by** and **updated_by** entries.

23.1.84 How to enable Dual Control in the VISULOX Cockpit

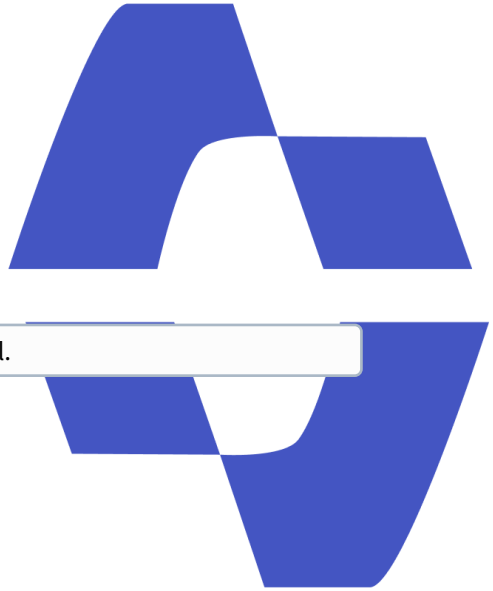
Based on the Company's Security Policy it could be requested, that keystrokes or films are **only** viewable in Dual Control mode.

Therefore it is necessary to setup a VISULOX Cockpit with Dual Control functionality.

The following steps are needed:

1. Set the Cockpit to session control mode in the datastore
2. Set the Cockpit presentation in the datastore to **Independent Mode**
3. Add the comandline parameter: Player on server

4. If necessary, assign the VISULOX Node, where the VISULOX Cockpit has to run (e.g. Dual Control on the Archive Database)
5. Configure an Application Policy with Dual Control enabled for this Cockpit



If a film is viewed in the Cockpit and the Dual Control session is locked (veto, time run out, etc), the playback of the film is paused as well.

See also:

- How to control the VISULOX Cockpit
- Dual Control
- How to configure role profiles for the VISULOX Cockpit

23.1.85 How to control Cockpit roles from the command line

Overview	
The command line tool "**VISULOX admin cockpit**" allows to control the VISULOX Cockpit roles..	• Overview • Usage • Cockpit role elements (edit) • Examples

Usage

The following subcommands are available:

Command	Description
list	List and print Cockpit roles.
add	Add a Cockpit role. A template is mandatory. A template has to be created before.

Command	Description
edit	Modify fields of a Cockpit role.
delete	Remove a Cockpit role.
fields	List available database fields (**-raw** = enhanced output)

Cockpit role elements (edit)

Element	Description
-name <>	Name of the Cockpit role or use Auto<>
-template <>	Name of the template. An existing Cockpit role has to be used as template.
-input <>	Keystroke data presentation on / off. Default value: off.
-refresh <>	Auto Cockpit Refresh on / off. Default value: off.
-tooltip <>	Tooltip on / off. Default value: off.
-object <>	Policy filter: Mask or unique distinguished object of user or group <>

Element	Description
-application <>	Policy filter: Mask or application name or application mask <>
-comment <>	Comment for the Cockpit role. default value: CLI
-grant <>	Set granted user in database record <>

Examples

List current available Cockpit role profiles

```
visulox admin cockpit list
    ------------------
    |      basicname |
    ------------------
    |          @VIEW |
    | @ALL-WITHINPUT |
    ------------------
```

Add Cockpit role

```
visulox admin cockpit add -name TestRole -template @VIEW
```

Edit Cockpit role

```
visulox admin cockpit edit -name TestRole -refresh on
```

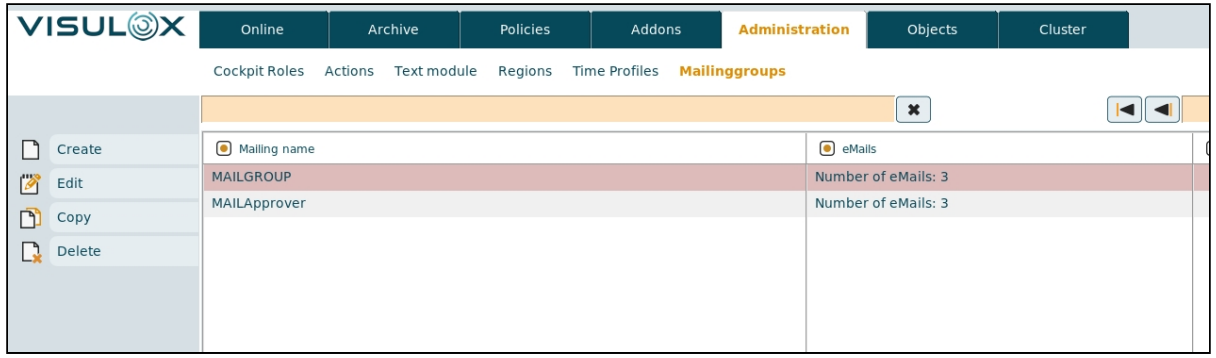
Remove an entry

```
visulox admin cockpit delete -name @VIEW
```

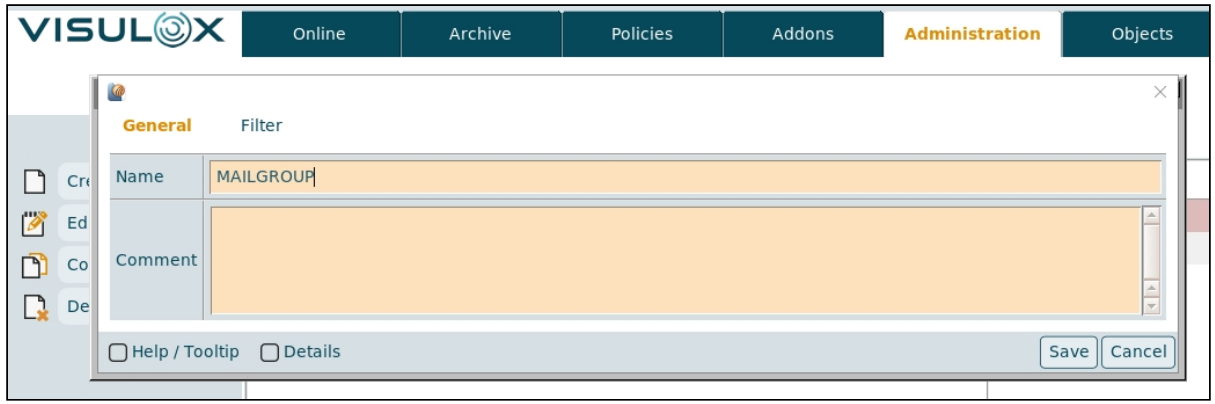
23.1.86 Mailinggroups

In VISULOX mailinggroups can be created, that can be used in other components, where mails have to be sent.

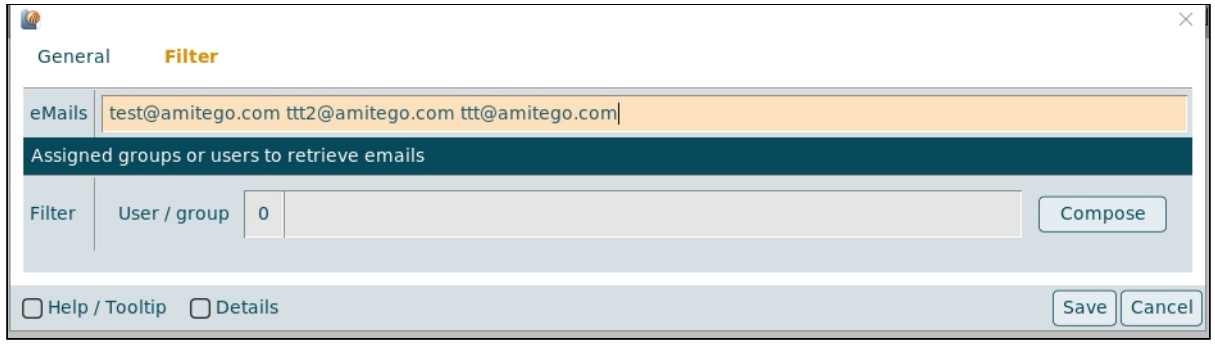
These mailinggroups are setup in **VISULOX Cockpit / Administration / Mailinggroups**.



The name and a comment for the mailinggroup can be set:

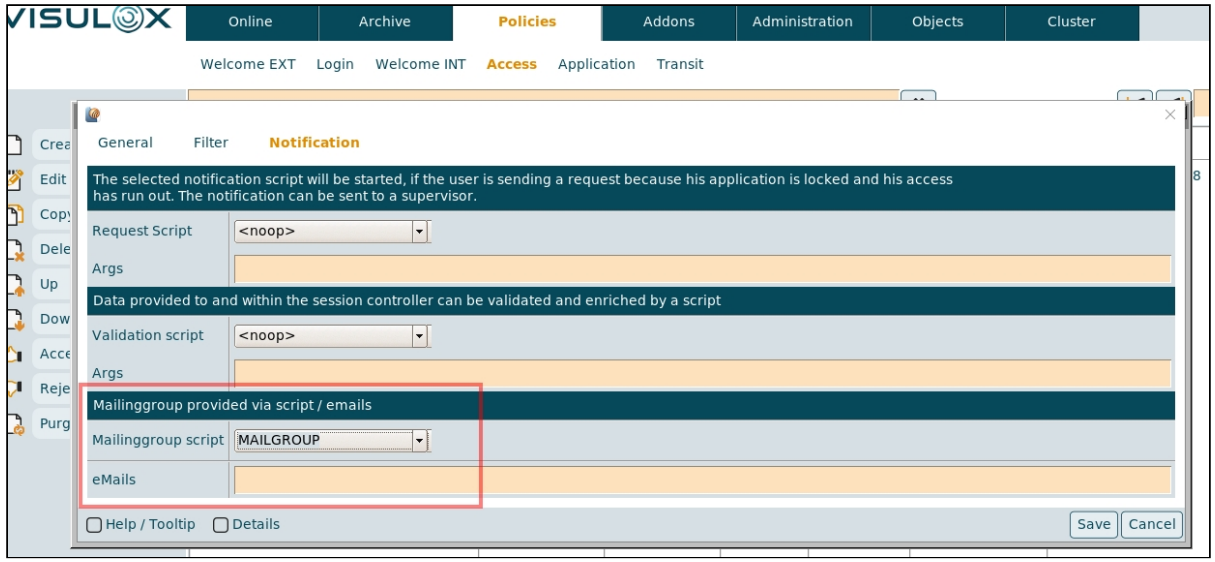


eMails can be entered either manually or selected from the existing users via the Compose button:



Once the mailinggroup is created it can be selected and used in other VISULOX components.

For example: **Access Policy**



In the Access Policy the created mailinggroup can be selected and / or an individual list of email addresses can be entered.

If an Access Request is triggered, the following event variables are provided:

- VLXMAILINGGROUP_UUID
- VLXMAILINGGROUP_EMAILS

The names, the UUID or other LDAP groups can be passed on to the mailclient.

```
date | ./mailclient.tcl -file stdin -mg $VLXMAILINGGROUP_UUID -to $VLXMAILINGGROUP_EMAILS
```

With the **-mg** parameter the individual email addresses of the mailinggroup and the deposited user emails of configured LDAP groups are collected.
The **-to** parameter is optional.

At the end, all e-mails are checked for syntax and duplicates are removed.

If no **-to** and no **-mg** is set, the default value from the configuration will be used.

Related information

How to control mailinggroups from the command line

How to control mailinggroups from the command line

Overview The command line tool "**VISULOX admin mailinggroup**" allows to control mailinggroups.	• Overview • Usage • Mailinggroup elements (edit) • Examples

Usage

The following subcommands are available:

Command	Description
list	List and print mailinggroups.

Command	Description
add	Add a mailinggroup.
edit	Modify fields of a mailinggroup.
delete	Remove a mailinggroup.
fields	List available database fields (**-raw** = enhanced output)

Mailinggroup elements (edit)

Element	Description
-name <>	Name of the mailinggroup <> (mandatory!)
-comment <>	Comment of the mailinggroup <>
-emails <>	List of emails <>
-groups <>	List of objects <>
-grant <>	Set granted user in database record <>

Examples

List current available mailinggroups

```
visulox admin mailinggroup list
    ----------------
    |    basicname |
    ----------------
    |    MAILGROUP |
    | MAILApprover |
    ----------------
```

Add new mailinggroup

```
visulox admin mailinggroup add -name Test -emails "ttt1@amitego.com ttt2@amitego.com ttt3@amitego.com"
```

Edit mailinggroup

```
visulox admin mailinggroup edit -name Test -comment "Test mailinggroup"
```

Remove an entry

```
visulox mailinggroup delete -name Test
```

23.1.87 Login with One Time Password (OTP)

About

It is possible to create a Login Policy also with a **One Time Passcode (OTP)** as a second factor.
The provided OTP is based on a secret key and the time via a smartphone APP.

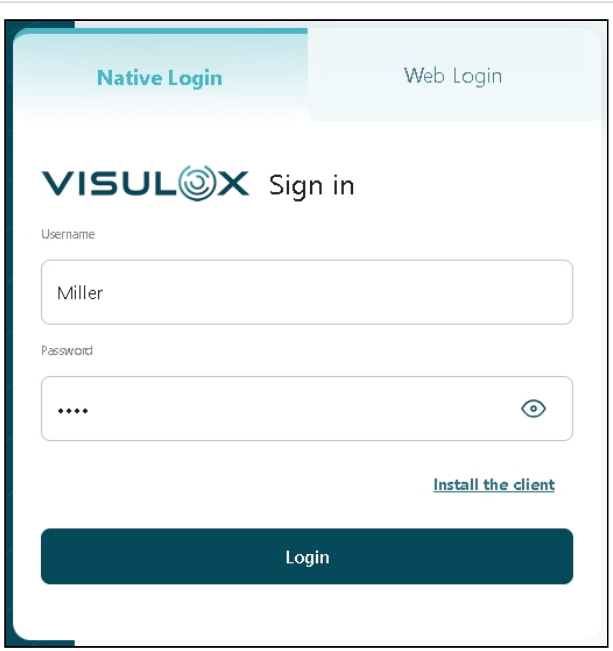
User can set his OTP by entering:

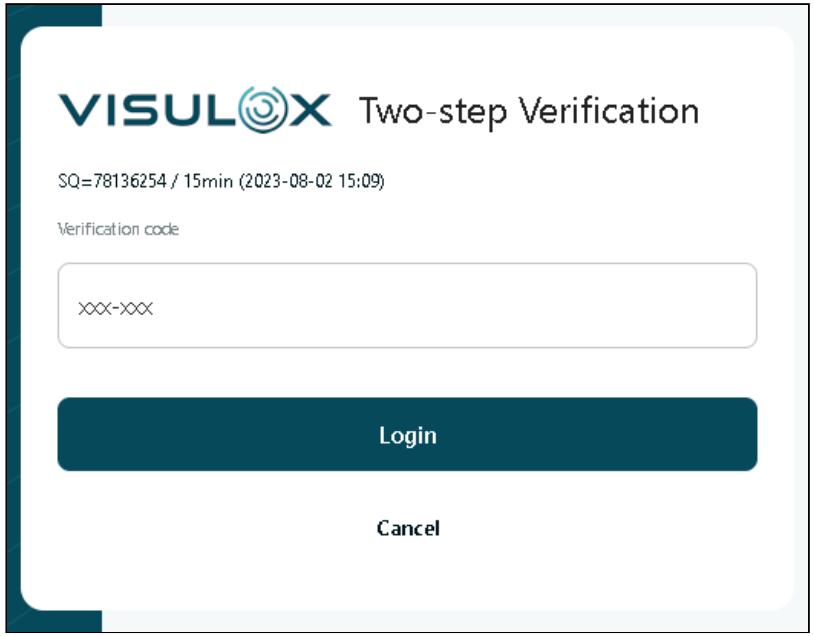
- the first valid OTP
- his password
- the provided token via a confirmation script

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

- About
- Initial key generation on the welcome page
- Configuration parameters
- Confirmation script example
- Adjusting the Login Policy
- Using the OTP setup type in the Login Policy
- Resetting OTP keys
- Related information
- Example authentication Apps

Login wiith username and password	2nd factor verbal PIN





Once logged in with a verbal token, the user can generate his secret key the welcome page and acknowledge the use of the OTP mechanism by confirming with a first OTP from his device.

It is also possible to generate the key before changing the Login Policy to OTP, so the first login via verbal PIN is not necessary, see: Migrating to One Time Password Authentication

OTP and Multi-User Login Profile
If a profile is tagged as a **Multi-User Login Profile** multiple persons can use the credentials. As result multiple independent sessions exist.
The mechanism of the VISULOX user password cache is disabled, and the user cannot create an OTP within the Workspace.

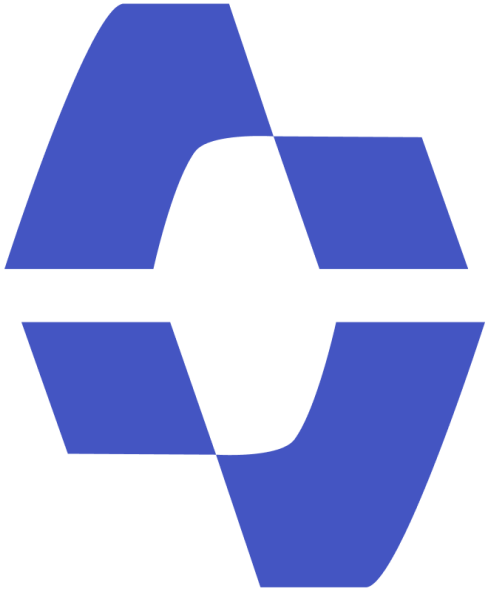
The function to create OTPs during the first login is still available. If this is used, the person who logs in for the first time has to communicate the OTP secret to participants.
Alternatively, the OTP setup can be done within a user deployment process by the admin using the CLI.

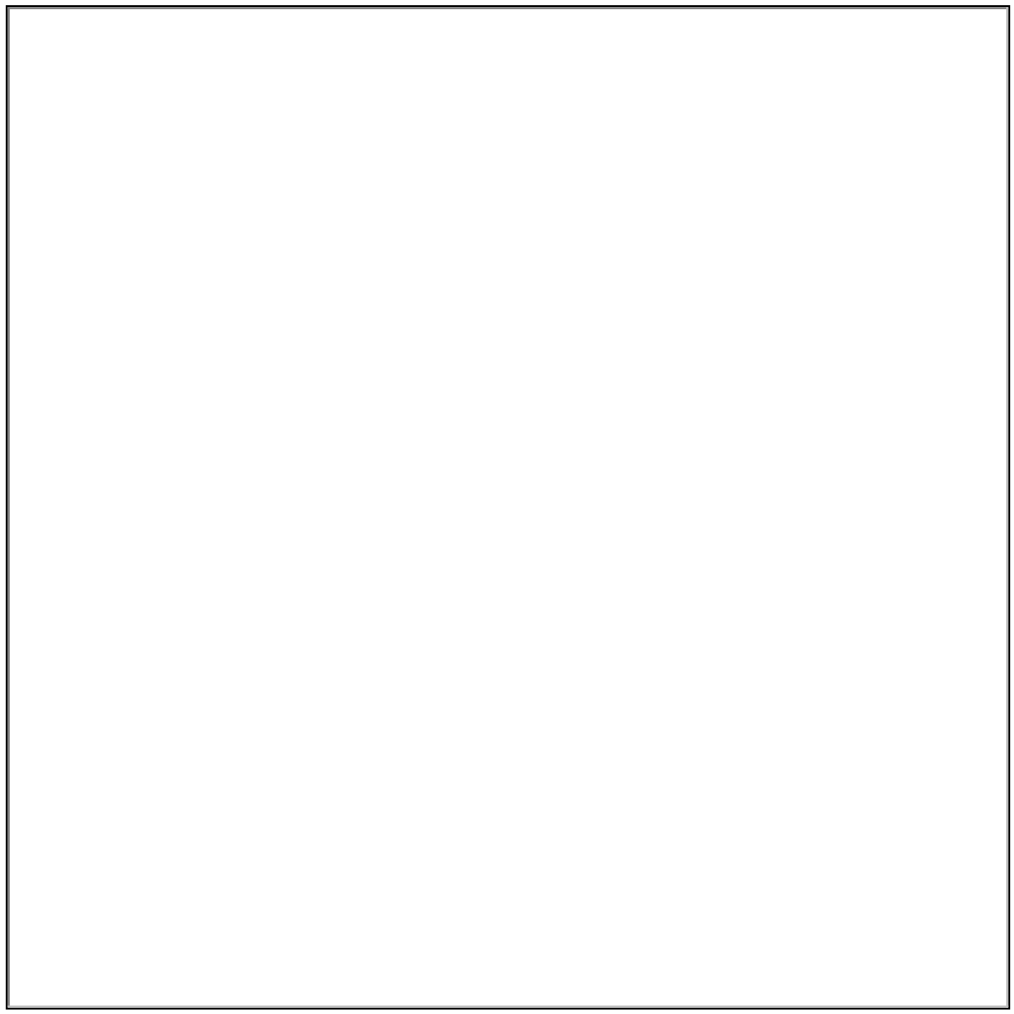
For compatability reasons SHA1 is used as default value for the OTP authentication.
In case of the OTP authentication in VISULOX this is not relevant, because it is not possible to recalculate the secret key from the OTP key and time, which would be the only possible attack.
However VISULOX is able to use SHA-256 for the OTP hash values.

```
visulox config -name otp.hash=sha256
```

If SHA-1 is not wanted, the client must be set to use SHA-256 as well. For example, the Google Authenticator application only supports SHA1.

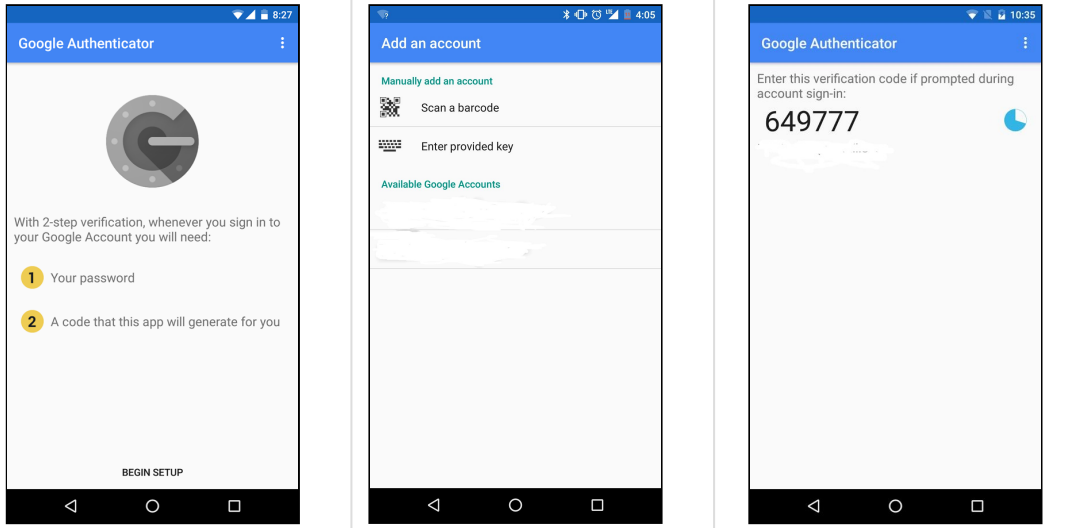
Initial key generation on the welcome page



The QR code (and the OTP Key) is displayed in the Workspace. To initialize OTP, the user's password has to be entered as well.	

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

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



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

⚠ The initial code is crypted with the cluster key. If the cluster key is changed, the users will loose their OTP-configuration.

Configuration parameters

```
visulox config -name otp
   ------------------------------------------------------------------------------------------------
   | changed | key                 | value                                                      |
   ------------------------------------------------------------------------------------------------
   |         | otp.always          | false                                                      |
   |         | otp.confirm         | false                                                      |
   |         | otp.confirmscript   |                                                            |
```

```
|         | otp.enforcedmessage | Please, enter the One Time Password!                                    |
|         | otp.label           | PIN/OTP                                                                 |
|         | otp.label.usertip   |                                                                         |
|         | otp.name            | %LICENSE%                                                               |
|         | otp.setupmode       | enabled                                                                 |
|         | otp.strict          | false                                                                   |
|         | otp.wait.text       | Registration closes in <span id="time">few</span> minutes!<br /> |
|         | otp.wait.timeout    | 600                                                                     |
-------------------------------------------------------------------------------------------------
```

Parameter	Description	Default value
otp.always	In environments where users have to request the PIN, it makes sense to hide the third entry until a PIN for such a user is known.	false
otp.confirm	Enable OTP 2FA confirmation	false
otp.confirmscript	Name of the VISULOX action script for confirmation	
otp.enforcedmessage	It is possible to use HTML tags e.g. <b>, <i>, <a href>, etc.	Please, enter the One Time Password!
otp.label	Entry label text for second factor on the VISULOX PORTAL login page	PIN/OTP
otp.label.usertip	Tooltip for the label for second factor on the VISULOX PORTAL login page	
otp.name	Displayed In the QR App. It is possible to use other placeholders e.g. %OWNERSHORT% or %FULLNAME%. A free Text can also be displayed.	%LICENSE%

Parameter	Description	Default value
otp.setupmode	Operation mode for OTP setup: enabled (OTP Dialog in Workspace), enforced (forwarding to OTP page), disabled or external	enabled
otp.strict	OTP has to correlate with the current time (otp.strict=true), otherwise previous and next OTPs are taken into account as well (otp.strict=false).	false

⚠ After **otp.always** and **otp.label** have been adjusted **visulox portal attach -jspconf** is needed.

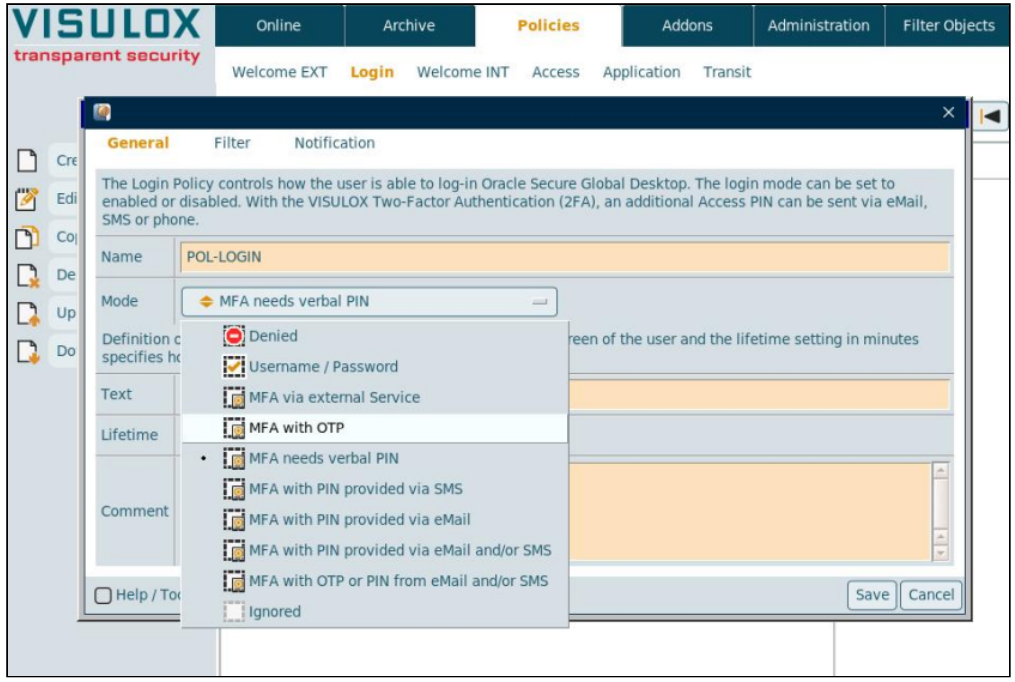
Confirmation script example

```
#!/bin/bash
#
VLXRECIPIENT=${VLXEMAIL:- root}
$VLXUTIL/mailclient.tcl -file stdin -subject "OTP Confirmation PIN $VLXPIN" -to $VLXRECIPIENT << EOF
Hello $VLXFULLNAME
Your OTP conformation request code: $VLXPIN_SEQUENCE
Enter your OTP Confirmation PIN: $VLXPIN
EOF
exit $?
```

The confirmation script is a VISULOX action script.

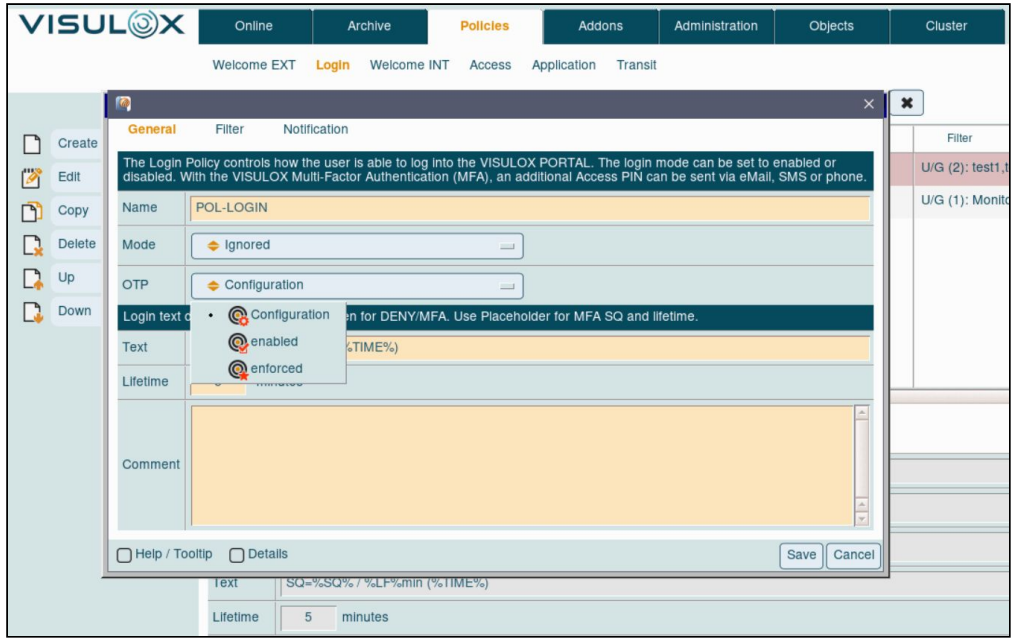
Adjusting the Login Policy

To enable login via OTP for the users, the Login Policy has to be set to **MFA Login with OTP**, **MFA Login with PIN** or **OTP from eMail and/or SMS**



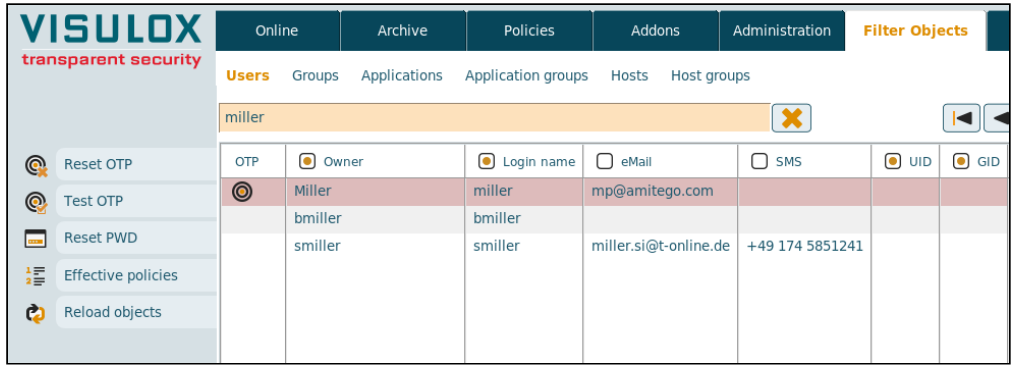
Using the OTP setup type in the Login Policy

In case of an OTP Login Policy, the setup type can be chosen: Configuration, enabled or enforced:



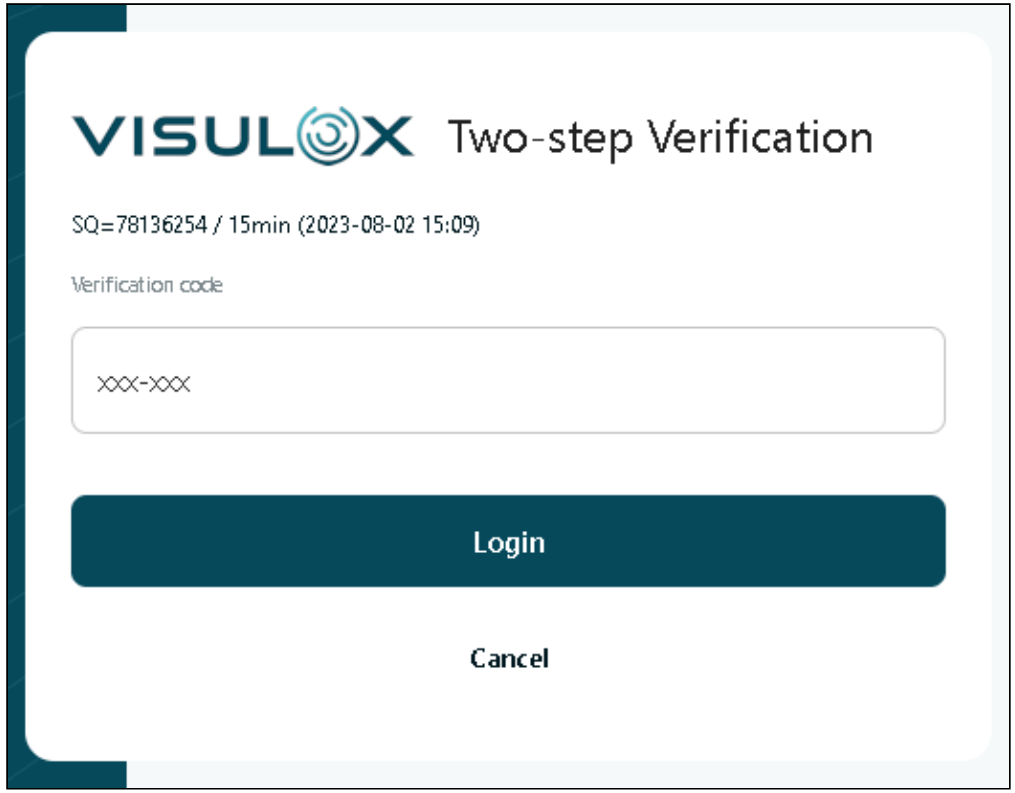
With OTP setup type configured via Login Policy it is possible to use OTP login for selected groups / users.
Setting the OTP type via configuration parameters will be applied to all users.

Resetting OTP keys



The OTP keys of selected users can be resetted via Cockpit on the **Filter Objects / Users** page.

Users can reset existing OTP configurations also by themselves in their Workspace:



⚠ Resetting the OTP configuration via Cockpit is not available for Unix users. Unix users are able to reset the configuration only in their Workspace.

Related information

How to control OTP from the command line

Example authentication Apps

OS	Link
IOS	https://support.microsoft.com/de-de/account-billing/microsoft-authenticator-app-verwenden-9783c865-0308-42fb-a519-8cf666fe0acc https://itunes.apple.com/de/app/google-authenticator/id388497605?mt=8
Android	https://support.microsoft.com/de-de/account-billing/microsoft-authenticator-app-verwenden-9783c865-0308-42fb-a519-8cf666fe0acc https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=de
Windows	https://support.microsoft.com/de-de/account-billing/microsoft-authenticator-app-verwenden-9783c865-0308-42fb-a519-8cf666fe0acc
BlackBerry	https://appworld.blackberry.com/webstore/content/29401059/?lang=en&countrycode=DE

Migrating to One Time Password Authentication

Migration to OTP for all users via configuration

Scenario:

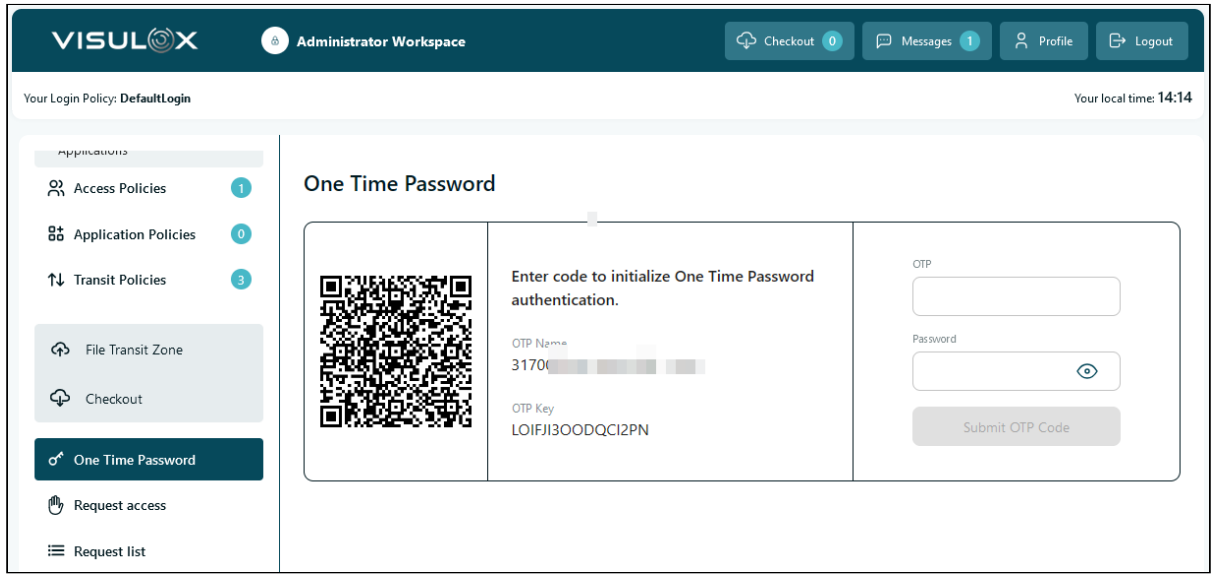
The user gets the second factor for login via message or eMail. It is wanted, that all users get their second factor via One Time Password App.

At first the user should get aware of the plan and be provided with the information, what One Time Password means and how it works.

After the users are informed, the OTP setup can be enabled:

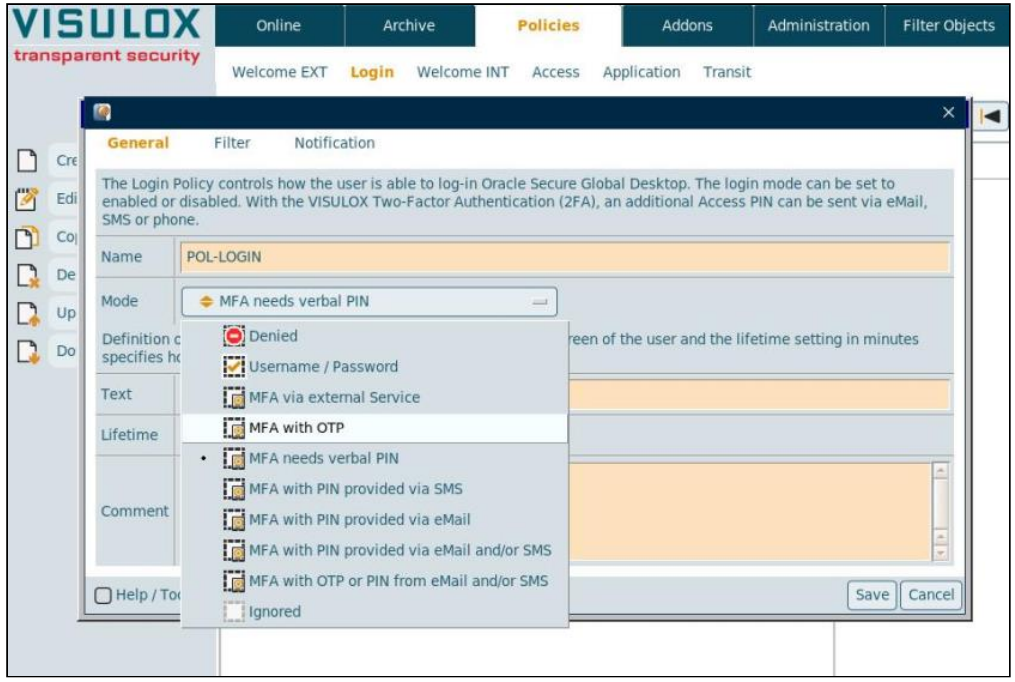
```
visulox config -name otp.setupmode=enabled
```

Now the users can setup OTP in the **One Time Password Dialog** section in their Workspace.



The user has to enter his password as well to initialize OTP.

The policy mode now can be switched to "**MFA Login with OTP"** or **"PIN from eMail and/or SMS**".



Now the user is able to login with the new OTP PIN or with the old method.

The following steps are necessary, if login should be allowed only via OTP:

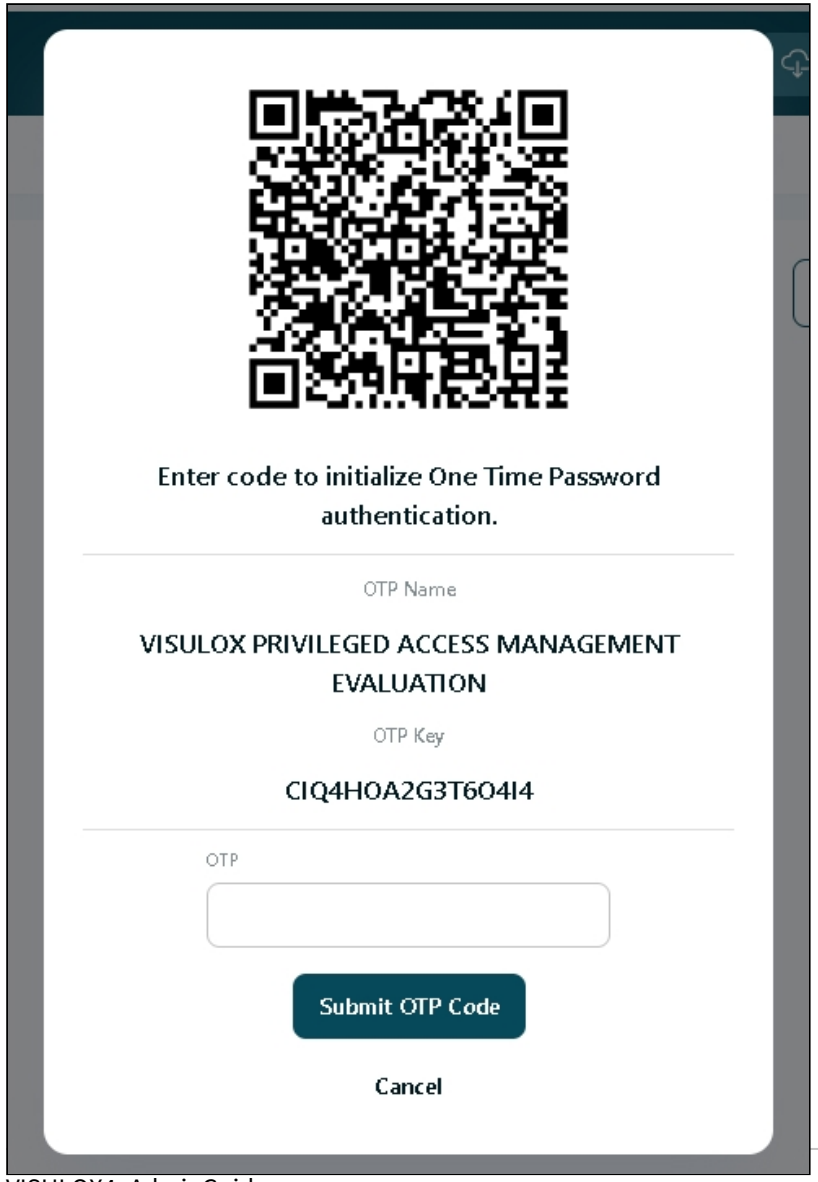
With **otp.always=true** a user can always enter a valid OTP and gets access. Otherwise he is able to request a PIN using eMail or SMS.

If OTP Login should be enforced, the policy mode can be switched to "**MFA Login with OTP**" after a period of time.

A short period before the OTP login is enforced, the setup of OTP should be enforced (e.g. if the users login in every day ~ 3 days before switching).

```
visulox config -name otp.setupmode=enforced
```

After this setting, every user who has not setup OTP yet will be forwarded to a setup page instead of his Workspace.

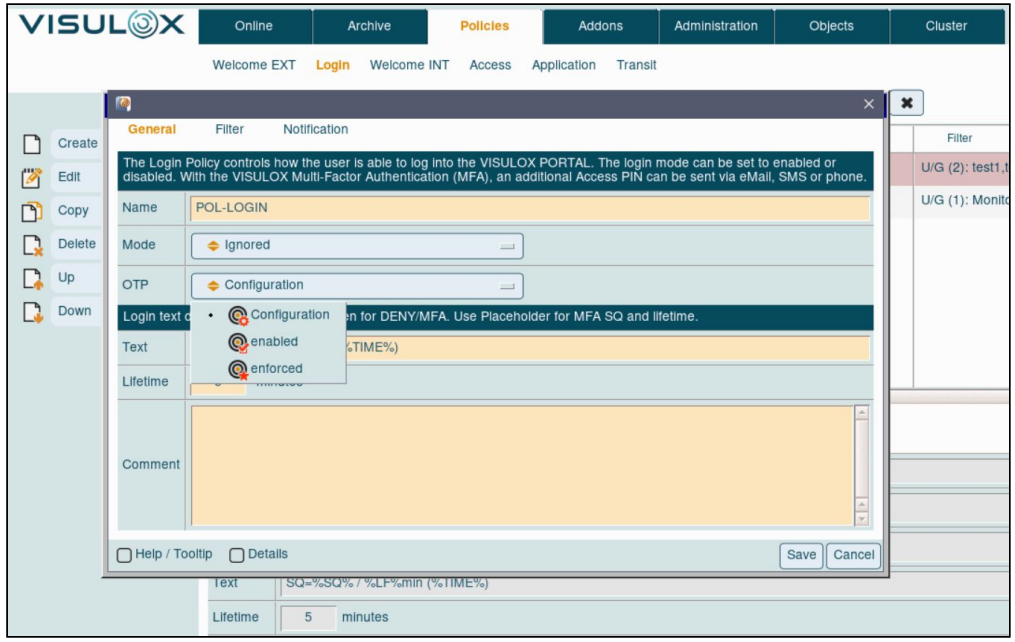

Enter code to initialize One Time Password authentication.
OTP Name
VISULOX PRIVILEGED ACCESS MANAGEMENT EVALUATION
OTP Key
CIQ4HOA2G3T6O4I4
OTP
Submit OTP Code
Cancel

After the setup and initialization, the user will be redirected to his normal Workspace.

The only other option is the **Cancel** button, which will exit the VISULOX PORTAL.

Migration to OTP for selected groups / users via the Login Policy

In case of an OTP Login Policy, the setup type can be chosen: Configuration, enabled or enforced:



With OTP setup type configured via Login Policy it is possible to use OTP login for selected groups / users.
Setting the OTP type via configuration parameters will be applied to all users.

23.1.88 MFA via external service

About

Multi Factor Authentication can be used with external services.

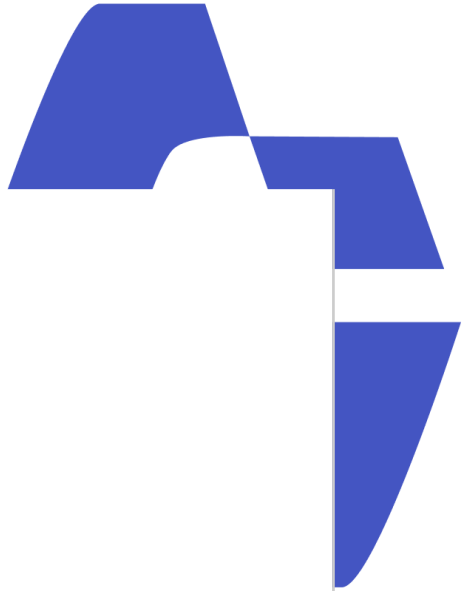
There are two possible scenarios:

1. The external service provides the MFA PIN. Once the user has entered the MFA PIN in the login mask, it is sent to the external service for validation.

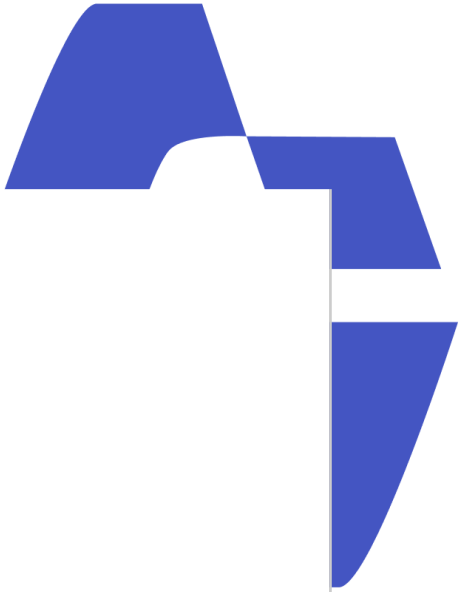
Configuration
A Login Policy has to be created with the mode: **MFA via external Service** (an example script is available, which can be used to setup the policy and the according action script).
The PIN script for this policy has to be created and assigned, for example:

```
#!/bin/bash
# create policy for external MFA using action links

WORKBASE=$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )
export WORKBASE

trap 'Script Error lineno=${LINENO} : $BASH_COMMAND ; exit 1' ERR
set -eu

NAME=externalWaitTest
SCRIPTNAME=$0

VLX_HOME=${VLX_HOME:-/opt/visulox}

LOGFILE=/tmp/${NAME}.log
SCRIPTRACE=/tmp/${NAME}.trace

VLXCMD=$VLX_HOME/bin/visulox
```

```
TRACE=0

# policy Name
PNAME=P-$NAME
# script Name
SNAME=S-$NAME

#####################################################################
cleanerLog() {
    echo "--------------------------" > $LOGFILE
    echo "" >> $LOGFILE
    echo "" >> $LOGFILE
}
header() {
    local date=$(date +%H:%M:%S)
    echo "" >> $LOGFILE
    echo $date $SUBCOMMAND $$ $* >> $LOGFILE
}
#####################################
dump() {
    #env | sort | grep VLX | grep -v VLX_ >> $LOGFILE
    (
    echo "VLXPIN: $VLXPIN"
    echo "VLXPIN_SEQUENCE: $VLXPIN_SEQUENCE"
    echo "VLXOWNER: $VLXOWNER"
    ) >> $LOGFILE
}

#####################################################################
usage () {
    echo "use setup"
    return 1
}
```



```
#####################################################################
runSetup() {
    cleanerLog
    $VLXCMD admin action add -name $SNAME \
        -category pin \
        -scriptfile $SCRIPTNAME \
        -force

    $VLXCMD policy login delete -name $PNAME  -force || true

    $VLXCMD policy login add -name $PNAME \
        -mode external -pinscript  $SNAME -force

    #$VLXCMD config reset -name extendsession.login.entry1
    #$VLXCMD config -name otp.always=true
    #$VLXCMD config -name otp.label="*** TEST $NAME ***"
 }


###################################
runExternal () {
    if [[ "$TRACE" == "1" ]]; then
        # for debugging
        exec 9> "$SCRIPTRACE"
        BASH_XTRACEFD=9
        set -x
    fi

    VLXMFADATA=${VLXMFADATA:-undef}
    VLXMFATOKEN=${VLXMFATOKEN:-}

    noteData="(has <${VLXMFADATA}>)"
    note="${VLXOWNERSHORT} |  0000=WAIT / 5678=REQUEST / 1234=OK / other=DENY / ${noteData}"
```



```
    if [[ "$VLXMFATOKEN" = "" ]]
      then
        # create session / init a session
        sessionData=SD$$

        $VLXUTIL/scriptAnswer.tcl -format base64  -code MFAREQUEST \
          -info "$note / (init <${sessionData}>)" \
          -data "$sessionData"

       elif [[ "$VLXMFATOKEN" = "0000" ]]
        then
          $VLXUTIL/scriptAnswer.tcl -format base64  -code MFAWAIT  \
            -info "$note"  -data "$VLXMFADATA"

      elif [[ "$VLXMFATOKEN" = "5678" ]]
        then
          $VLXUTIL/scriptAnswer.tcl -format base64  -code MFAREQUEST \
            -info "CHALLANE $note" -data "$VLXMFADATA"

      elif [[ "$VLXMFATOKEN" = "1234" ]]
        then
          $VLXUTIL/scriptAnswer.tcl -format base64  -code SUCCESS  \
            -info "OK / ${noteData}"

      else
        $VLXUTIL/scriptAnswer.tcl -format base64  -code MFADENY \
          -info "Your request was denied / ${noteData}"
      fi

}
#####################################################################
runUndef() {
        header "SUBCOMMAND=$SUBCOMMAND unknown"
        >&2 echo SUBCOMMAND $SUBCOMMAND unknown
```

```
        return 255
}
################################################################
SUBCOMMAND=${1:-}
header

case $SUBCOMMAND in
    "")
        usage
        ;;
    "setup")
        runSetup
        ;;
    "external")
        runExternal
        ;;
    *)
        usage
        runUndef
esac
exit $?
```

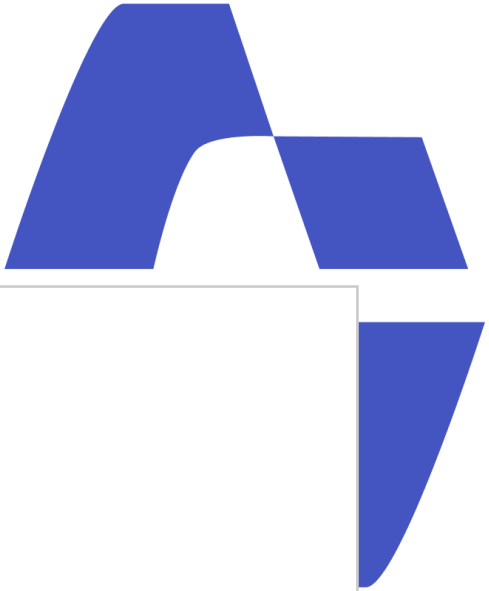
The check against the external service with username / VLXMFAToken has to be implemented.

- If $? then -code SUCCESS
- If not then -code MFADENY

> ⚠ Be careful if this script is created via the setup method. The according Login Policy will be on the first position and matches with all users.
> Before starting setup, open a Visulox Cockpit as Administrator and once setup is done move the created Policy to the end of the policy list.

2. The user logs in with his credentials and VISULOX Service waits for the answer of external service. The external service checks the login and gives feedback to VISULOX.

Configuration



A Login Policy has to be created with the mode: **MFA via external Service**

The PIN script for this policy has to be created and assigned, for example:

```
# exitcode 0: script run without error
# any other exitcode: script error
# State results on stdout
# echo "ok:a free text (currenly no seen by the user"
# echo "request: Message in the login dialog"
# echo "denied: Message in the login dialog"
#
# enviroment as variable. see documentation
# Example with pin request:
examplePinRequest () {
  if [[ "$VLXPIN" = "1234" ]]
    then
     echo "ok:any text ..."
   elif [[ "$VLXPIN" = "NULL" ]] || [[ "$VLXPIN" = "" ]]
    then
     echo "request: ... enter pin ..."
   else
      echo "denied: ....pin is wrong...."
   fi
}
exampleLoginConfirmed () {
    local result=$( external service)
    [[ -z "$result" ]] && echo "ok" || echo "failed:$result"
    exit 0
 }
#examplePinRequest
#exampleLoginConfirmed
echo "denied: modify template script"
exit 0
```

This script has to be adjusted according to the needs of the external service.

In the example the section **examplePinRequest** has to be adjusted for the first method, where the MFA PIN is provided by the external service.

For the second method, where the user logs in with his credentials, the section **exampleLoginConfirmed** has to be adjusted.

> ⚠ If the external service takes time to respond, the proxy timeout setting has to be adjusted on the VISULOX GATEWAY.

External MFA via email with action links

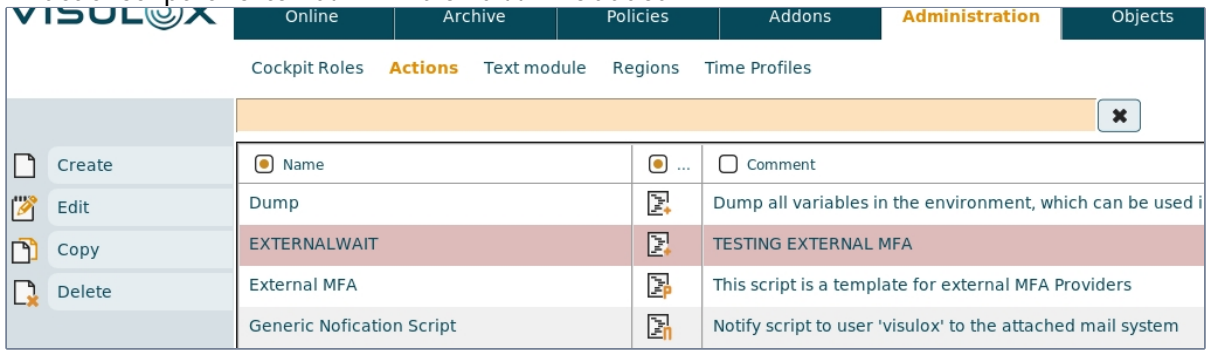
It is also posssible to send a mail to the user, once he has entered his username and password on the login page.
In this mail the user can click on **Click to Confirm** and his Workspace will be opened in his browser.

For this setup an example script is available, use:

```
sh /opt/visulox/setup/actionscripts/mfaConfirmationViaEmailLink.sh setup
```

With this setup:

- The webservice is enabled and started
- An actionscript for external MFA via email link is added



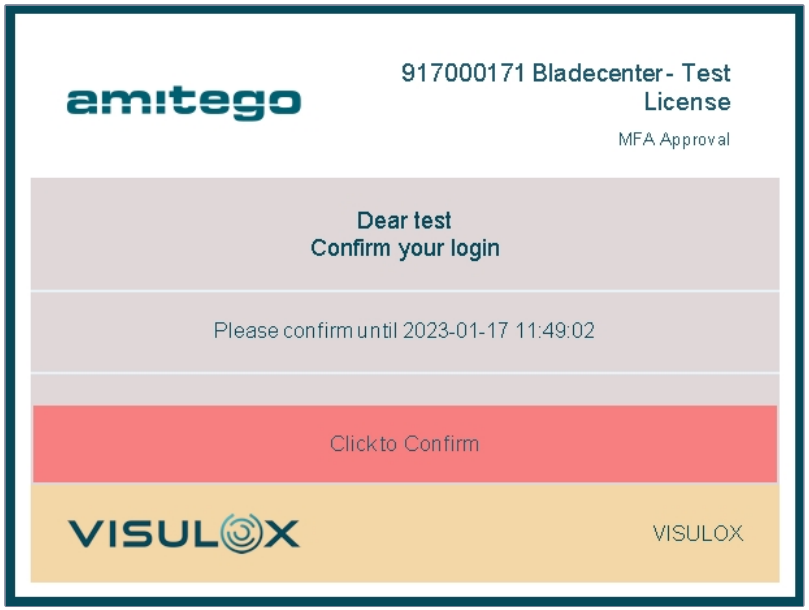
Within this script **$VLXUTIL/confirmStatus.tcl -uuid $VLXACKNOWLEDGEUUID** is used for external MFA via email links.

- An example Login Policy for external MFA is added and the actionscript is assigned

User login

After the user assigned to this Login Policy has entered his credentials, the following page is displayed:

The user will get the following mail, where he can confirm the login:



After confirmation the Workspace is opened directly.

23.1.89 RSA SecureID Implementation via RSA API

- Abstract
- Background
- Command
- VISULOX policy implementation

Abstract

VISULOX login with AD user and AD password extended by an RSA token can be implemented. This can be done either with the VISULOX external MFA service or with VISULOX login Validation.

The VISULOX project script **rsaSecureId.tcl**, provided for customers on request, allows to verify username and token.

The VISULOX login user (VLXLOGINUSER) has to be the same as in AD and the RSA server (extra mapping is possible on project request).

The current implemenation just verifies the user and the RSA token. The "CHALLENGE" is currently not implemented and the user needs the RSA selfservice. (The "CHALLENGE" can be implemented on project request.)

The RSA validation can be implemented as a VISULOX external MFA Policy or as a VISULOX Validation to any Login Policy. It requires a VISULOX 2FA license.

Background

RSA provides an API to verify a user and his current token. A description can be found here:

https://community.rsa.com/t5/securid-access-knowledge-base/how-to-set-up-the-rest-rsa-securid-authentication-api-for/ta-p/4960

The implemented API method is initialized (with SecureID) with user authentication and token in one request.

An API request needs an URL and a client-key. This information is stored in a VISULOX resource.

For example:

Create a VISULOX RSA SECUREID resource with an URL and a client key

```
visulox passcache edit -resource mokeid \
    -resuser "https://a06136c9-cbe2-44dc-8049-fd95c4236cdb.mock.pstmn.io" \
```

```
    -respass "dummy-85o8xe8534r7g484581wi225c1h4o"
```

Command

```
rsaSecureId.tcl -resource <name of resource> -username VLXLOGINUSER -token <current token> -id <message>
```

Live system

```
su vlx -c "/opt/visulox/lib/utils/rsaSecureId.tcl -resource rsasecureid -user <user> -token <token>"
```

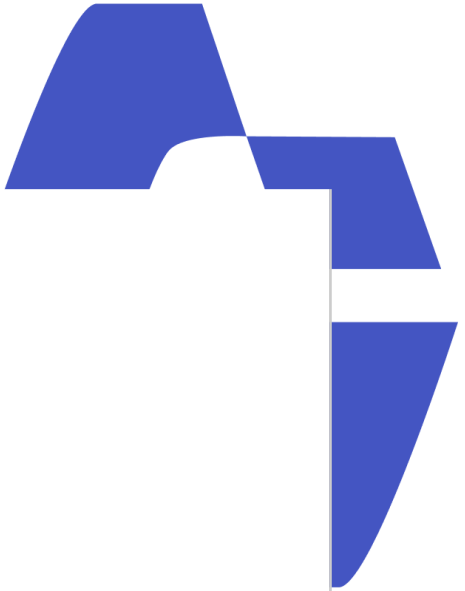
Additional options:

```
-id for messageid
-verbose to see response data
-debug : debugging data into logs/rsasecurid.log
```

VISULOX policy implementation

VISULOX external MFA Login Policy

```
#!/bin/bash
export BASE=$( cd "$(dirname "${BASH_SOURCE[0]}" )" && pwd )

# Implement RSA validation via VISULOX external MFA

VLX_HOME=${VLX_HOME:-/opt/visulox}
```



```
VLX_CMD=$VLX_HOME/bin/visulox

$VLX_CMD admin action add -name rsaPIN \
    -category pin \
    -scriptfile $BASE/script_rsaSecureId_pin.sh \
    -force

$VLX_CMD policy login delete -name rsa\*  -force

$VLX_CMD policy login add -name rsaLoginPIN \
    -mode external -pinscript rsaPIN -force

$VLX_CMD config reset -name extendsession.login.entry1
$VLX_CMD config -name otp.always=true
$VLX_CMD config -name otp.label="RSA TOKEN"

echo "Copy rsaSecureId  in place "
cp $BASE/rsaSecureId.tcl  $VLX_HOME/lib/utils

echo "Register VISULOX at PORTAL"
```

Action script for external MFA confirmation:

script_rsaSecureId_pin.sh

```
#!/bin/bash
export BASE=$( cd "$(dirname "${BASH_SOURCE[0]}" )" && pwd )

#$VLXPATH/bin/cmd/config.tcl env > /tmp/vlxVar.data
#TESTING=test

result=$($VLXUTIL/rsaSecureId.tcl $TESTING -resource rsasecureid -user "$VLXLOGINUSER" -token "$VLXPIN" 2>&1 | cut -d : -f 2-)
```

```
[[ -z "$result" ]] && echo "ok" || echo "failed:$result"
exit 0
```

23.1.90 How to setup MFA with SMS response from the SMS Provider

General behaviour

A SMS is sent with eMail or another mechanism via the VISULOX script service to the SMS provider. The SMS provider delivers the SMS to the recipient. When this is done, the SMS provider can notify the sender about the delivery results. This is mainly done by a HTTP request from the SMS provider.

Within the **VISULOX webservice** the response from a SMS provider can be inserted into the event database.

VISULOX provides integration examples on request.

> In Germany **text messages** are **SMS**.

Planning

The SMS is sent via the SMS PIN script. The script has access to server information (VLXPIN_*) (See also: Variables in notifications).

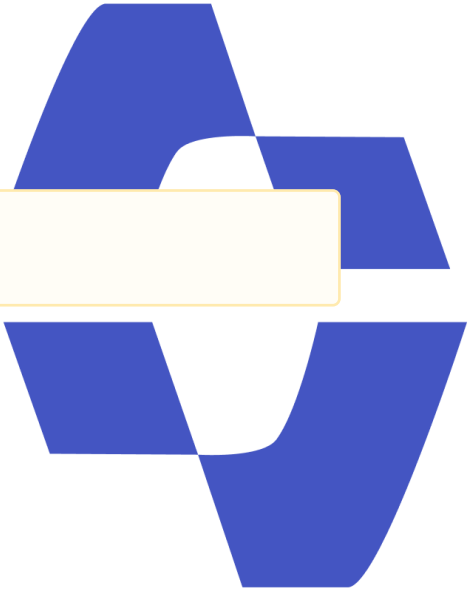
A SMS text should not be longer than 160 characters and should contain at least VLXPIN and the VLXPIN_SEQUENCE.

Depending on the SMS provider a back channel is possible. Therefore a port is needed, which is reachable by the SMS provider.

This port ends in the SMS response service.

The **VISULOX webservice** needs to be configured.

SMS delivery script



> In this example SMS4.de and Kannel is used.
> The Interface to SMS-Expert is no longer supported, because SMS-Expert closed the service at the end of 2016.
> Alternate interfaces will be provided on request or OTP can be used as well.

Add the script to the VLX action scripts (example: SMS4.de)

- In SMS4.de a account is needed. SMS4.de will provide a custid (KDNR)
- In SMS4.de a budget is needed.
- in SMS4.de a user (which is not the login user) with a password is needed: USER/PWD

Example script and parameters for SMS via Kannel

Configuration parameters for Kannel

```
visulox config -name sms
    ------------------------------------------------------------------------------
    | changed | key                    | value                                   |
    ------------------------------------------------------------------------------
    |         | regexp.sms             | ^[0-9 +.\(\)-]{6,}$                     |
    |         | smskannel.feedbackurl  | http://<server>:<port>/smsKannelfeedback |
    |         | smskannel.gwurl        | <url>                                   |
    |         | smskannel.password     | <password>                              |
    |         | smskannel.postquery    | /cgi-bin/sendsms                        |
    |         | smskannel.sender       | VISULOX RA 2FA PIN                      |
    |         | smskannel.user         | <user>                                  |
    ------------------------------------------------------------------------------
```

The Webservice is listening initially only on local host.

If SMS Kannel is used with the feedback URL the Webservice has to listen to all interfaces, which can be configured in **/opt/visulox/etc/service.conf**:

```
{program webservice.tcl
 enabled false
 requires {webservice}
 args {-interface ""}
}
```

Another possible solution is via port 443 with a reverse proxy in the **Apache**:

```
<Location /smsKannelfeedback>
 ProxyPass        https://localhost:%WEBSERVICESSLPORT%/smsKannelfeedback
 ProxyPassReverse https://localhost:%WEBSERVICESSLPORT%/smsKannelfeedback
</Location>
```

The text is stored in the **VLXPIN_TEXT** variable, which is defined in the Login Policy - Notification - Content block.

The format of the message can be enhanced for all messages at once (e.g. to display more than one row):

```
#/bin/bash
read -d '' VLXPIN_TEXT << EOF
NICE formatted text
PIN: $VLXPIN_FMT
VALID UNTIL: $VLXPIN_EXPIRATIONTIME
SEQUENCE: $VLXPIN_SEQUENCE
EOF

export VLXPIN_TEXT

$VLXUTIL/SMSviaKannel.tcl
```

The SMS delivery script has to be assigned to an MFA Login Policy.

A timeout parameter can be set for SMSviaKannel.tcl

Related articles

(4.2.0) How to setup MFA with SMS response from the SMS Provider
(4.2.0) How to configure a user account as a group account
(4.2.0) RSA SecureID Implementation via RSA API
(4.2.0) VISULOX Webservice
(4.2.0) Migrating to One Time Password Authentication
(4.2.0) The VISULOX PIN Service
(4.2.0) MFA via external service
(4.2.0) VISULOX Mail Client and Send PIN
(4.2.0) How to enable, configure and use MFA
(4.3.2) How to configure a user account as a group account
(4.3.2) RSA SecureID Implementation via RSA API
(4.3.2) MFA via external service
(4.3.2) How to enable, configure and use MFA
(4.3.2) Migrating to One Time Password Authentication
(4.3.2) VISULOX Webservice

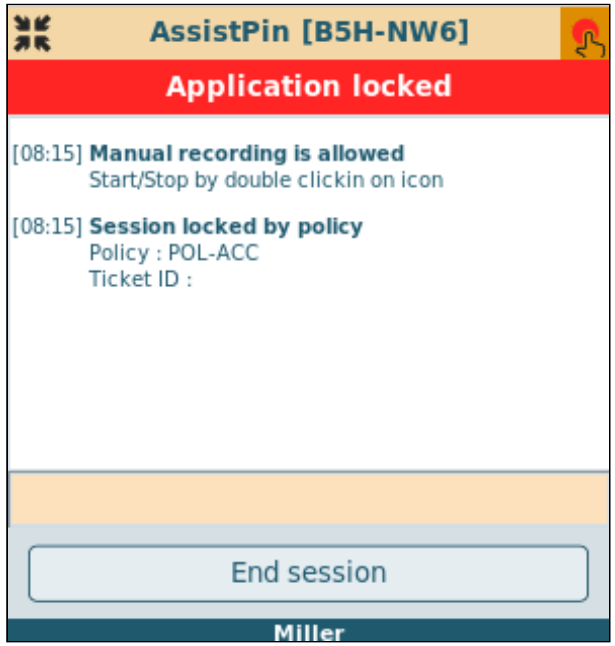
23.1.91 In-Time Access

With in-time access a supervisor is able to give spontaneous access to a session locked by policy.

Processes for application access can be implemented without advanced planning.

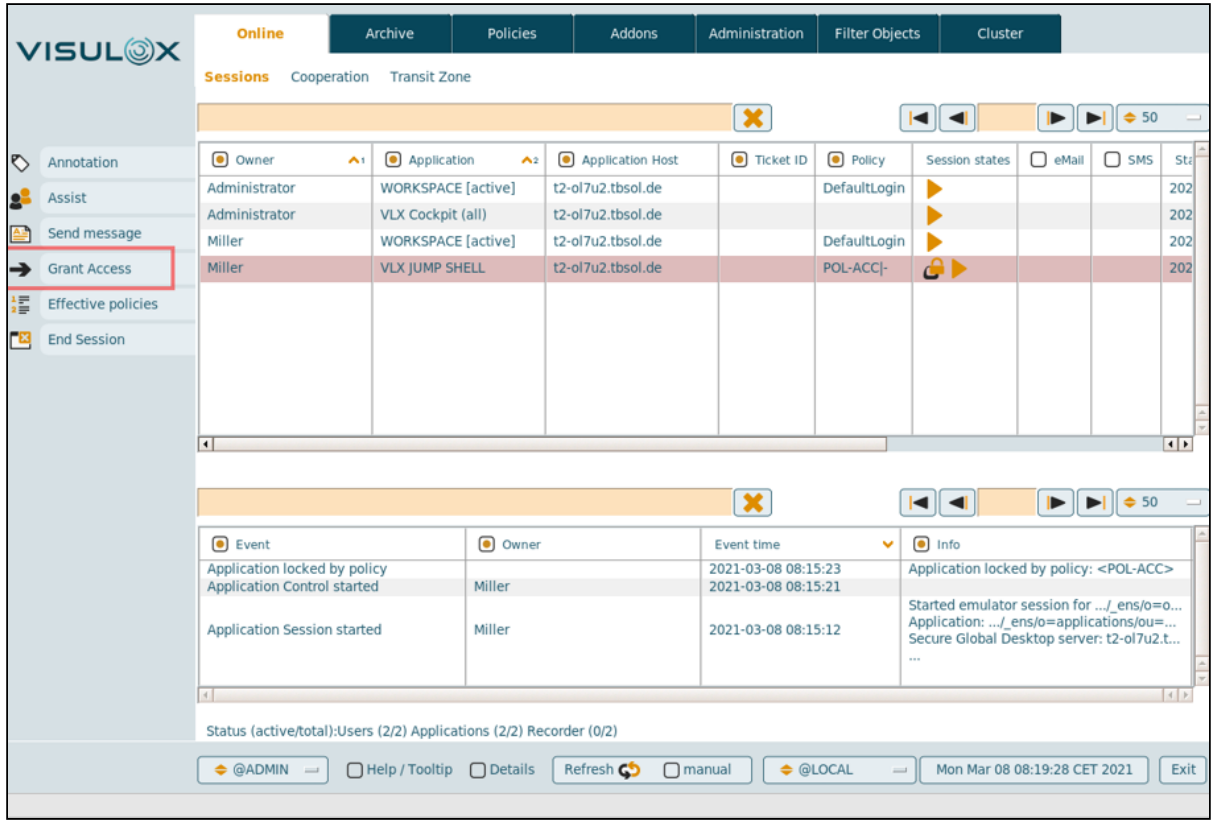
A user logs into the VISULOX PORTAL and starts an application from his Workspace.

The user`s application is locked, if no Access Policy is found or if an Access Policy is set to denied.



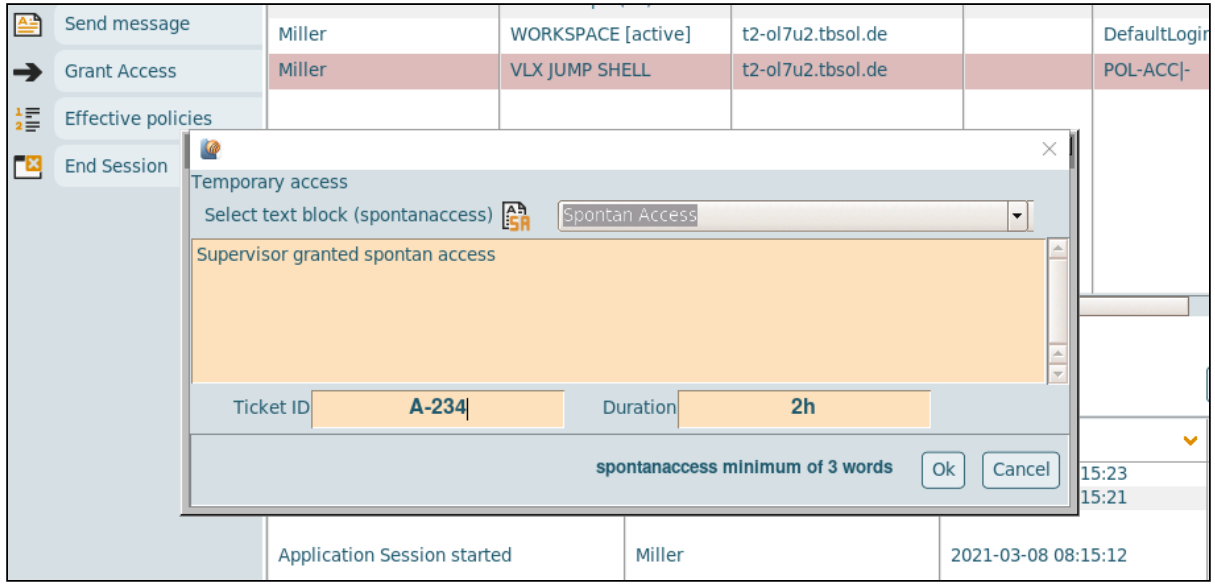
If a **notification** script is assigned to a denied policy, a "**Send Request**" button is displayed, with which a mail is sent to an approver, who can grant access via Cockpit.
If a **request** script is assigned to a denied policy, a "**Send Request**" button is displayed, with which mails are sent to the requester and the approver, who is able to allow or reject the request via mail.

Within **VISULOX Cockpit / Online**, the supervisor is able to grant an in-time access for the user.



A text for the access has to be filled out and the temporary access is based on a ticket ID and a period of time. (See: Handling ticket IDs from external systems)

The value of the time period can be entered in hours (h, no unit) or in minutes (m).

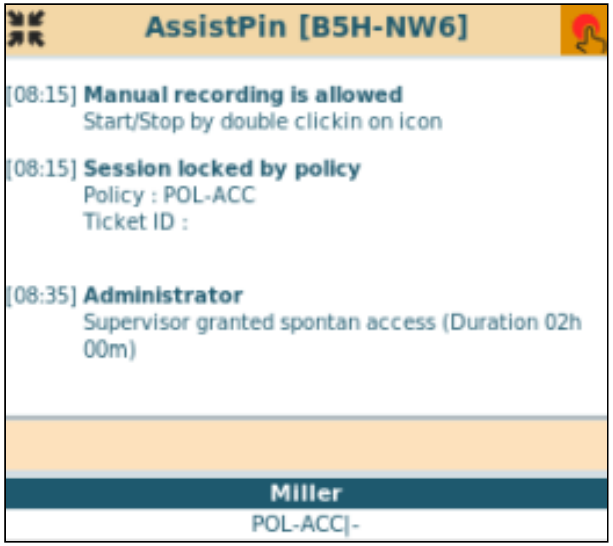


Configuration parameters

Parameter	Description	Default
entry.defaultduration.spontanaccess	Default duration	
entry.spontanaccess.maxduration	Max duration of temporary access	48
entry.minwords.spontanaccess	Min words in comment	3

Parameter	Description	Default
entry.spontanaccess.ticketid	Reg expression for the ticket ID	^A-.+$

Once the temporary access is granted, the user can work with the application:



23.1.92 Access and transit request via actionlink

- About
- Configuration

        - Webservice
        - Reverse proxy configuration
        - Configuration paraneters
        - Request setup via script
    - Configuration after setup
        - In-time access
        - Workspace access
        - Transit access
        - Optional arguments
    - Requester and approver mails / HTML
        - Example: Access request confirmation
        - Example: Transit request confirmation
    - Modification
    - Templates and testing
    - Related articles

About

Users without access to one or more applications are able to request access within the locked session (in-time request) or with the "VLX Request" application via a form in the Workspace.

With actionlinks it is possible to send a mail to the approver, who is able to grant access via an actionlink in the mail.
The requester also receives mails, when request is sent, approved, rejected or expired.

It is also possible to use actionlinks for files that have to be approved, when they are uploaded into Transit Zone.

Actionlinks are available for:

- Planned application access via Workspace - request and approval via mail
- In-time application access via session controller - request and approval via mail
- File Transit - request and accept via mail

The requester always gets a mail, when he has sent a request and when the request has been approved, rejected or expired.

The approver gets a mail to approve the request. Depending on the request, he is able to accept, accept for a time period or reject.
Once he has chosen an option in the mail, a HTML page is diplayed with the information.

If a request has expired, the approver also gets a mail.

Configuration

The configuration and setup can be done easily with a script:

```
/opt/visulox/setup/actionscripts/requestScriptTemplate.sh
```

⚠ This script has to be adjusted before setup.

The request script template:

- enables the webservice on the local server
- adds necessary configuration parameters
- adds the request script to the action scripts in VISULOX

Webservice

Run the script on all VISULOX Portal Servers to enable the webservice.
At least one webservice must be enabled. If the setup via script is only started on one server, the webservices on the other VISULOX Portal Servers should be enabled manually.

```
visulox config -name layout.vT2OL7U2.webservice
    ------------------------------------------------
    | changed | key                          | value |
    ------------------------------------------------
    | changed | layout.<log name>.webservice | true  |
    ------------------------------------------------
```

Reverse proxy configuration

The necessary proxy settings are needed in **/opt/tarantella/webserver/apache/default/conf/httpd-visulox.conf** on the VISULOX Portal Servers.
This configuration is created with the **visulox portal attach** command:

```
<Directory "/opt/tarantella/var/docroot">
RewriteEngine on
RewriteRule ^$ /sgd/index.jsp [R,L]
RewriteRule ^/$ /sgd/index.jsp [R,L]
RewriteRule ^index_([A-z]*)\.html$ /sgd/index.jsp?langSelect=$1 [R,L]
RewriteRule ^index.html$ /sgd/index.jsp [R,L]
</Directory>

### END REDIRECT ###
<IfDefine SSL>
       SSLProxyEngine On
      SSLProxyCheckPeerCN off
       SSLProxyCheckPeerName off
       SSLProxyCheckPeerExpire off
       SSLProxyProtocol ALL -SSLv2 -SSLv3
</IfDefine>
<Location /vack>
        ProxyPass        https://localhost:8115/vack
        ProxyPassReverse https://localhost:8115/vack
</Location>
```

Configuration paraneters

The following configuration parameters are set, at least the **generalapprover** parameter should be adjusted in the request script before setup.

```
   visulox config -name request.
    ------------------------------------------------------------------------------------------------------------------
    | changed | key                                  | value                                                       |
```

```
-------------------------------------------------------------------------------------------------------------------
|         | request.dumpvars                  | false                                                             |
|         | request.feedback.url              |                                                                   |
|         | request.mfa.requestlifetime       | 5                                                                 |
|         | request.session.autoclose         | 15                                                                |
| changed | request.session.requestlifetime   | 60                                                                |
| changed | request.transit.requestlifetime   | 60                                                                |
| changed | request.workspace.access          | Dump                                                              |
|         | request.workspace.ahead           | 10                                                                |
|         | request.workspace.duration        | 200                                                               |
| changed | request.workspace.request         | REQUEST                                                           |
| changed | request.workspace.requestlifetime | 60                                                                |
|         | request.workspace.timeprofile     | 24x7                                                              |
|         | request.workspace.validation      |                                                                   |
|         | request.workspace.validation.args |                                                                   |
-------------------------------------------------------------------------------------------------------------------
```

Depending on the module, the **request.<module>.requestlifetime** has to be greater than **0**, then the request action script will be triggered.
request.<module>.requestlifetime is always in minutes and request.session.autoclose in seconds.

Lifetimes in minutes (reaction time for approval)

- Access via Workspace: request.workspace.requestlifetime
- Access via application: request.session.requestlifetime
- Transit access: request.transit.requestlifetime

At least for the access request via Workspace, the GENERALAPPROVER has to be adjusted:

```
# at least needed
VLXAPPROVER=${VLXAPPROVER:-visulox@amitego.com}
VLXEMAIL=${VLXEMAIL:-visulox@amitego.com}
GENERALAPPROVER=visulox@amitego.com
```

- VLXAPPROVER can be set via args in the policy.

- VLXEMAIL is the email of the user set in datastore.
- GENERALAPPROVER is used for a configuration parameter, which set during script setup for Workspace access and **has to** be adjusted.

The fallback user visulox@amitego.com should be set to an existing user in the environment.

Request setup via script

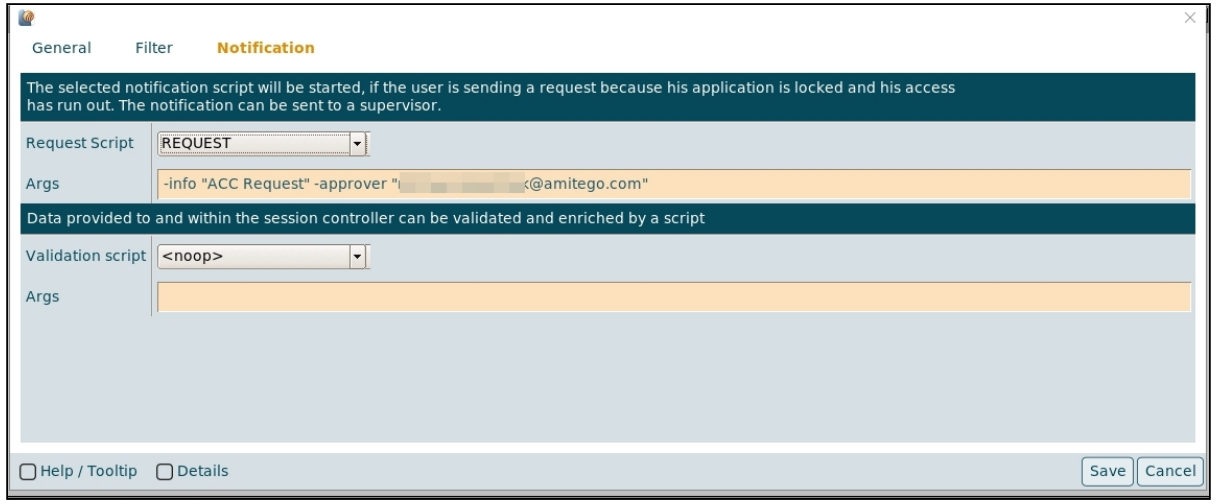
After the script has been adjusted, run the script with:

```
sh requestScriptTemplate.sh setup

Done: action -name <REQUEST> modified!
layout.<log-name>.webservice : Needs restart of VISULOX Node
Start Webservice
 *** Make sure on any relevant note the webservice is enabled as well
 *** Make sure your VISULOX Gateway has a assoziated reversproxy configuration for the feeback links
 *** Make sure you configured the VISULOX Mail service
 *** Make sure you have the necessary policy (access,transit)
```

Configuration after setup

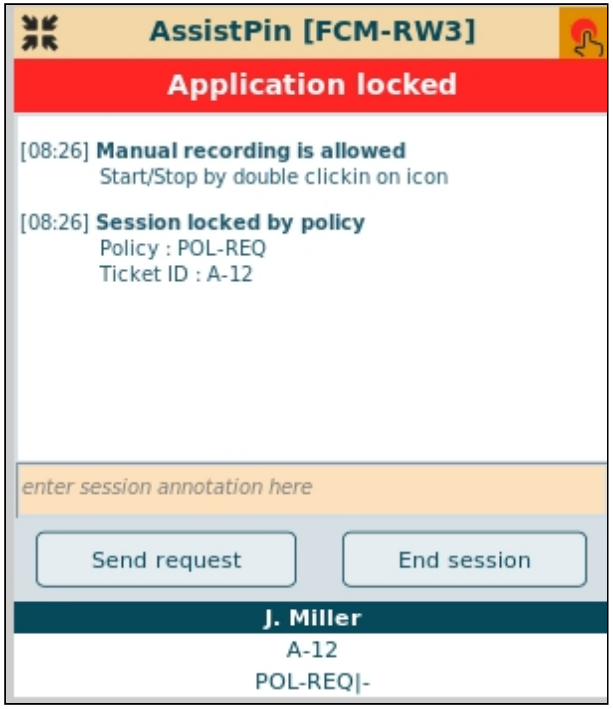
In-time access

An Access Policy must be created and set to **denied**.
The request action script has to be chosen and the arguments can be set.



The **-approver** argument is the mail address of the approver.

The user requests his access with the **Send Request** button in the session controller of the application:

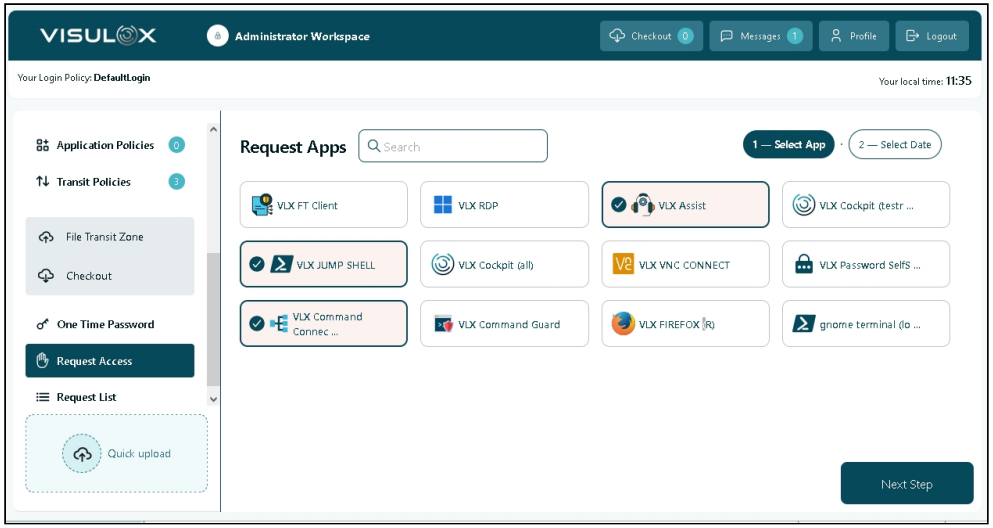


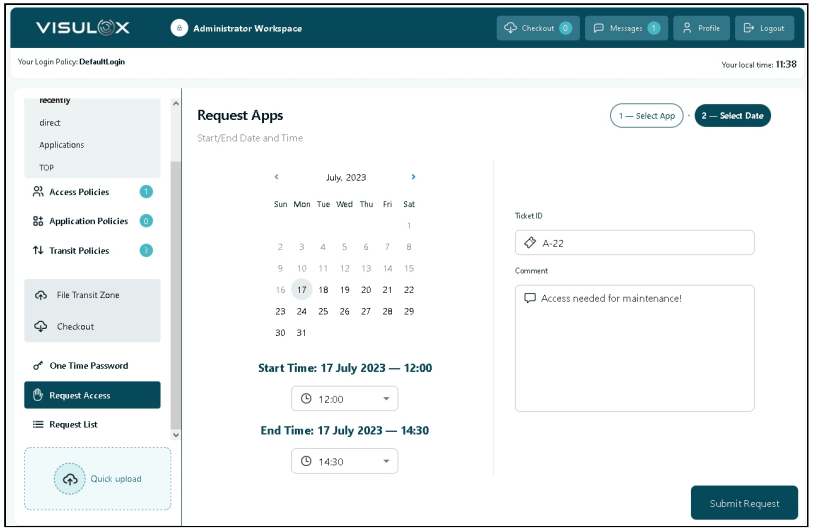
Workspace access

All necessary configurations have been set via the adjusted script.

```
| changed | request.workspace.request | REQUEST |
| changed | request.workspace.request.args | -info "A comment from the policy ...." -approver mail@amitego.com |
```

The user requests his access with the **VLX Request** application:

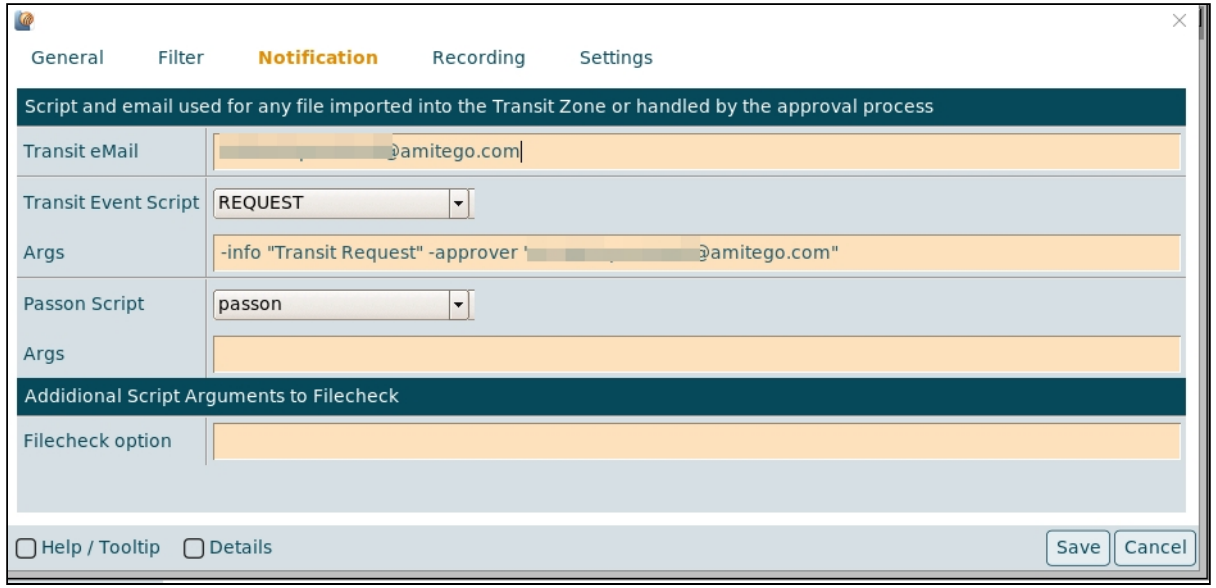




The user can request access for all selected applications. He has to enter a time frame, the ticket ID and a comment. All is checked against the configured ruleset.

Transit access

A Transit Policy must be created and set to **approval** or **Passon after approval**.
The request action script has to be chosen and the arguments can be set.



Once the user has uploaded a file into Transit Zone, that has to be approved, the mails are sent to the requester and approver.
The status of the file can also be seen in the File Transit Zone section of the Workspace.

Optional arguments

The optional arguments are **-info** "<text>'" and **-approver** "<mail@domain.de>" and are provided as VLXAPPROVERINFO and VLXAPPROVER .
If the arguments are set, they will be displayed in the session controller.

If **-approver** is not set via arguments, the approver configured in the action script will be used.

```
VLXAPPROVER=${VLXAPPROVER:-visulox@amitego.com}
```

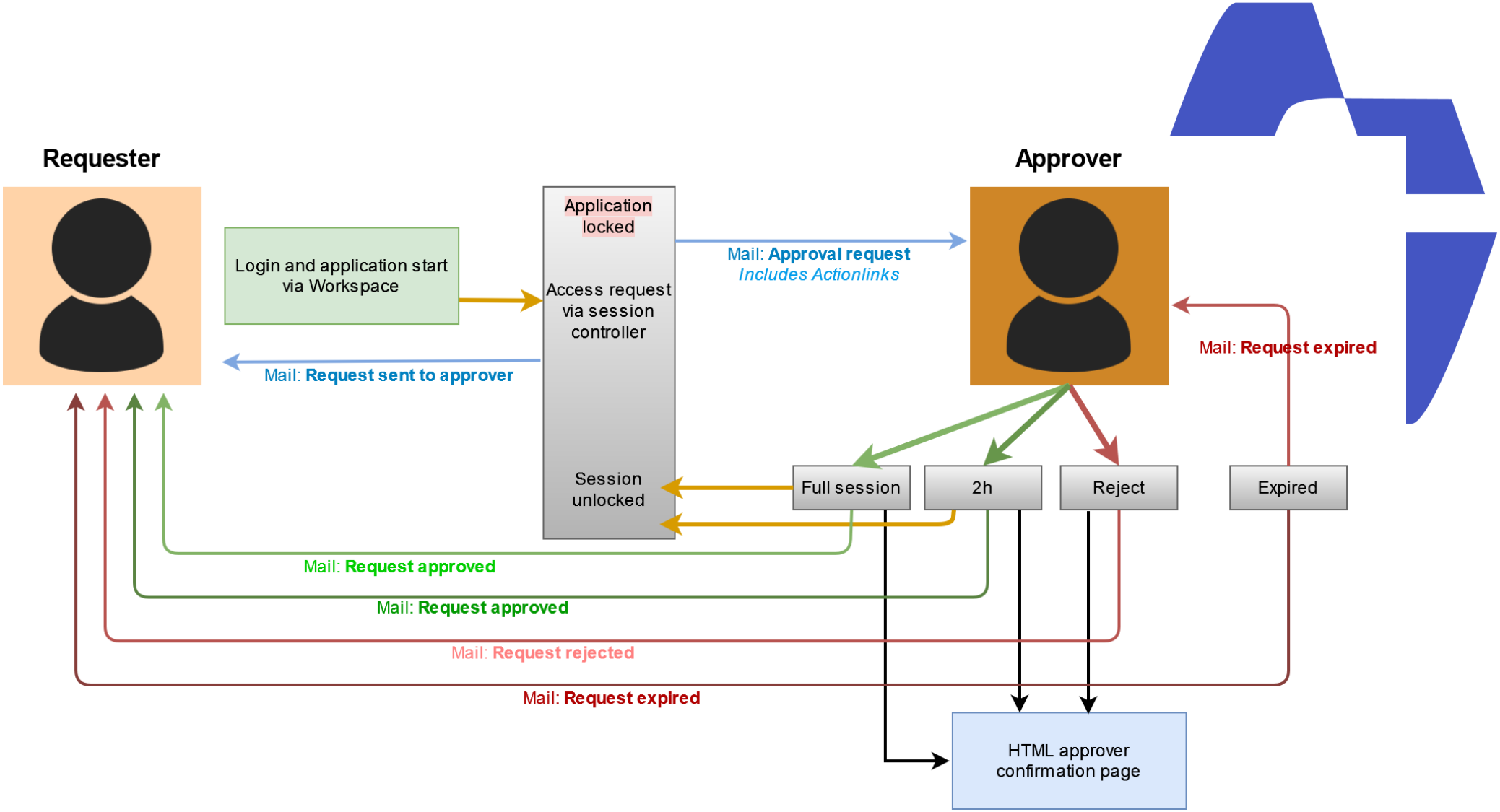
The default system send address for the mails can be adjusted with:

```
visulox config -name mail.sender
    ------------------------------------------------
    | changed | key         | value               |
    ------------------------------------------------
    | changed | mail.sender | noreply@amitego.com |
    ------------------------------------------------
```

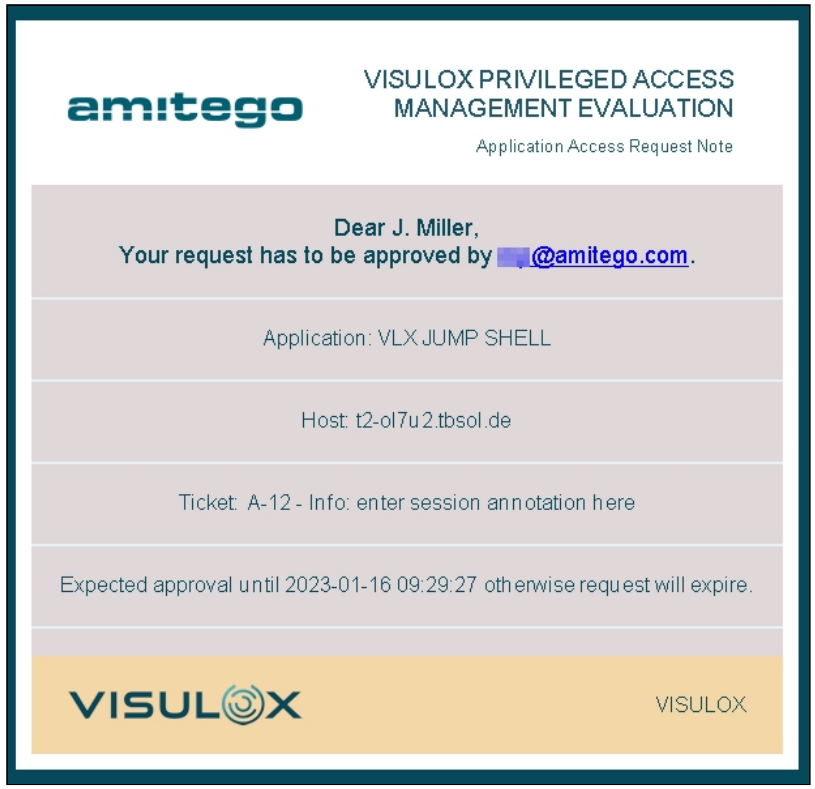
Requester and approver mails / HTML

Example: Access request confirmation

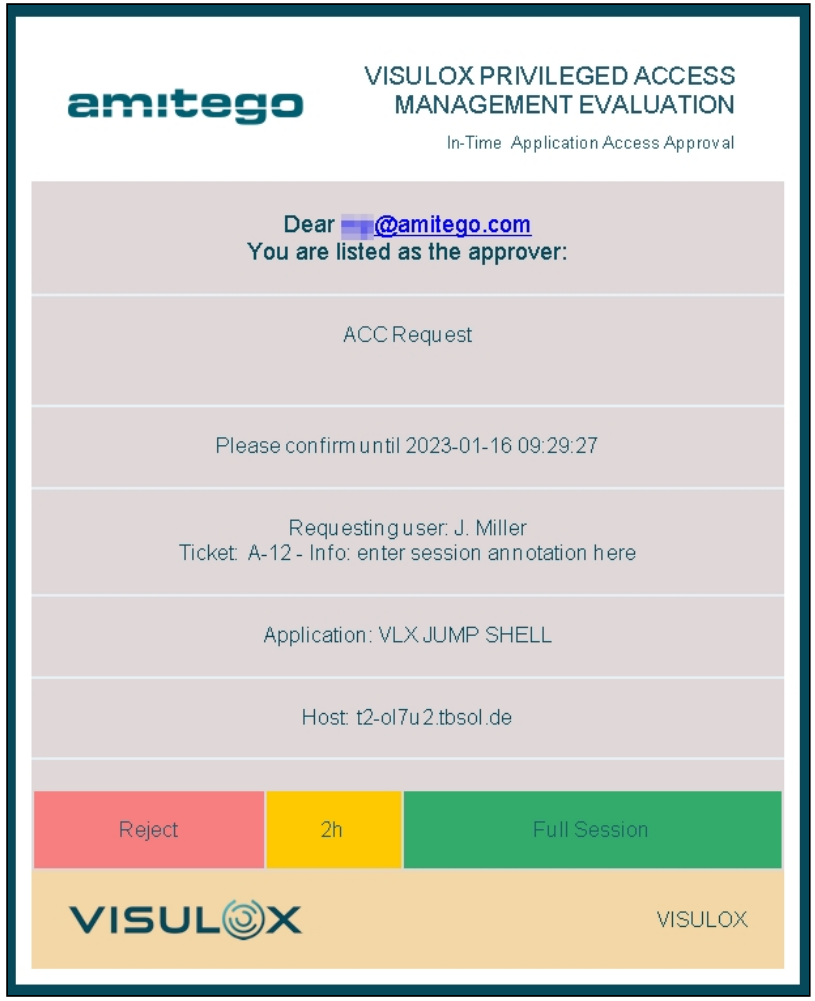
Overview:


Requester
Approver
Login and application start via Workspace
Application locked
Access request via session controller
Session unlocked
Mail: Approval request
Includes Actionlinks
Mail: Request sent to approver
Mail: Request expired
Full session
2h
Reject
Expired
Mail: Request approved
Mail: Request approved
Mail: Request rejected
Mail: Request expired
HTML approver confirmation page

The **requester** always gets a confirmation mail for his Workspace or in-time request:



The configured **approver** gets the mail with the actionlink to approve, reject the access:

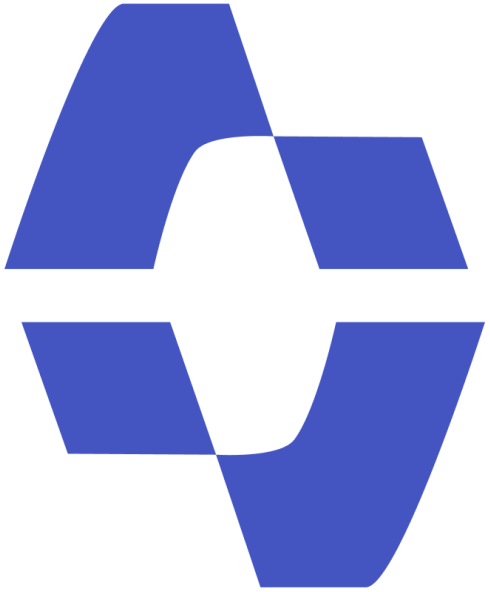

amitego
VISULOX PRIVILEGED ACCESS MANAGEMENT EVALUATION
In-Time Application Access Approval
Dear @amitego.com
You are listed as the approver:
ACC Request
Please confirm until 2023-01-16 09:29:27
Requesting user: J. Miller
Ticket: A-12 - Info: enter session annotation here
Application: VLX JUMP SHELL
Host: t2-ol7u2.tbsol.de
Reject
2h
Full Session
VISULOX
VISULOX

In case of an in-time session request. the approver can choose **Reject**, **2h** or **Full Session**.
In case of a Workspace request **Accept** or **Reject** can be chosen.

The approver is forwarded to a HTML confirmation page once he has pressed a button.

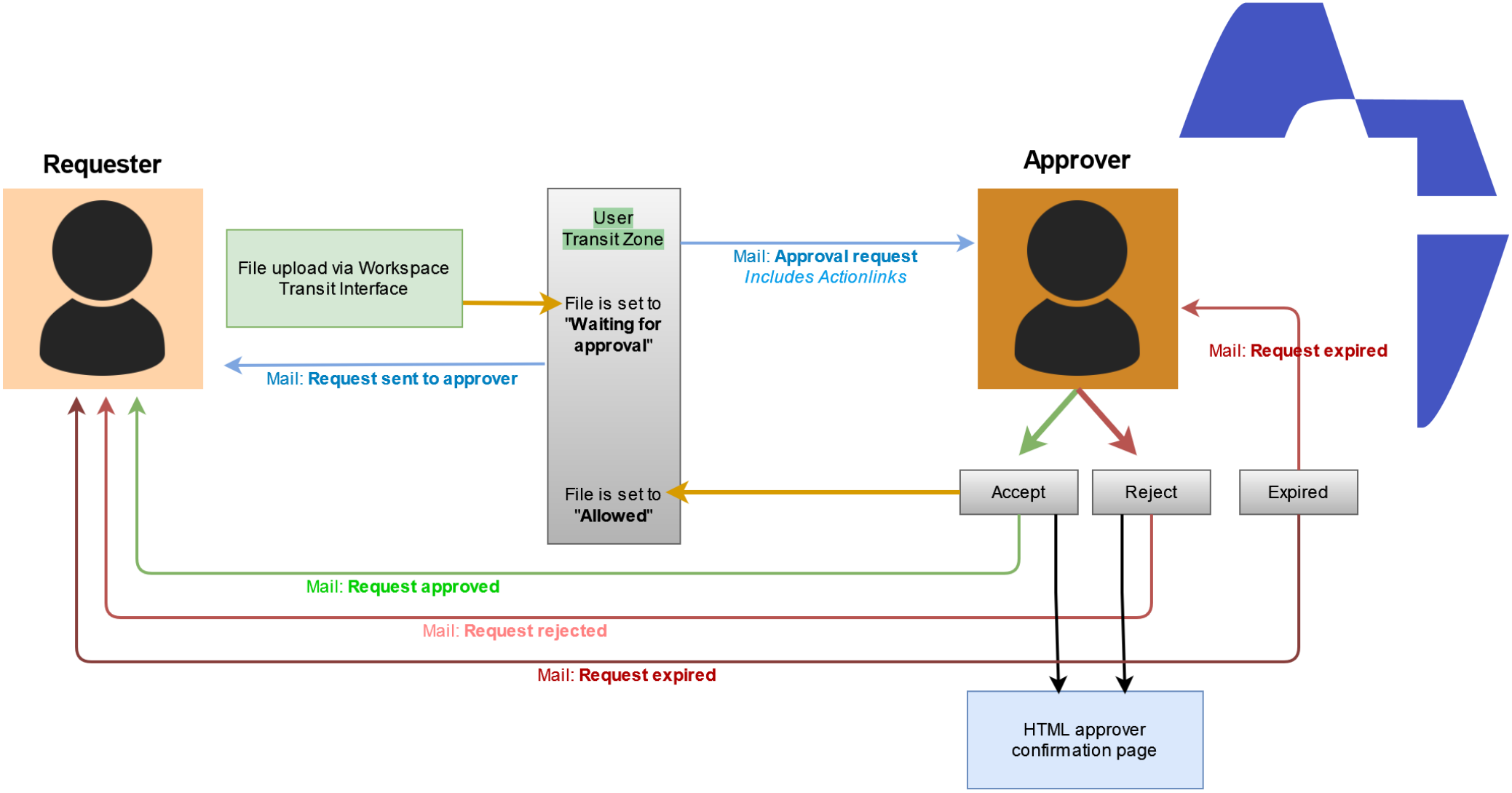
Now the **requester** receives a mail depending on the result of his request: **approved**, **rejected** or **expired**:

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

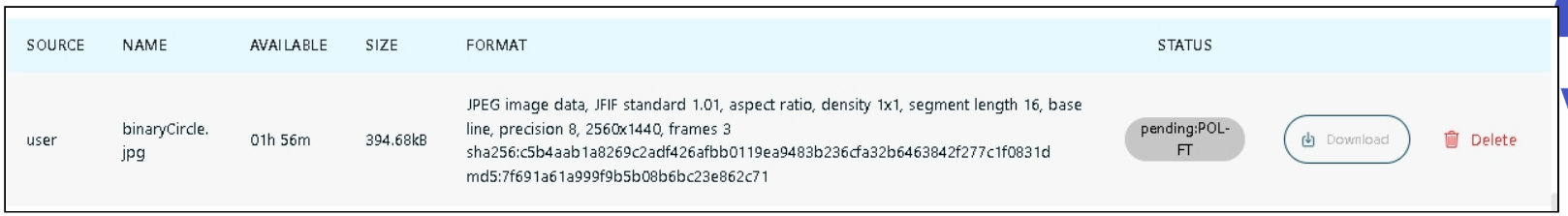


Example: Transit request confirmation

Overview:

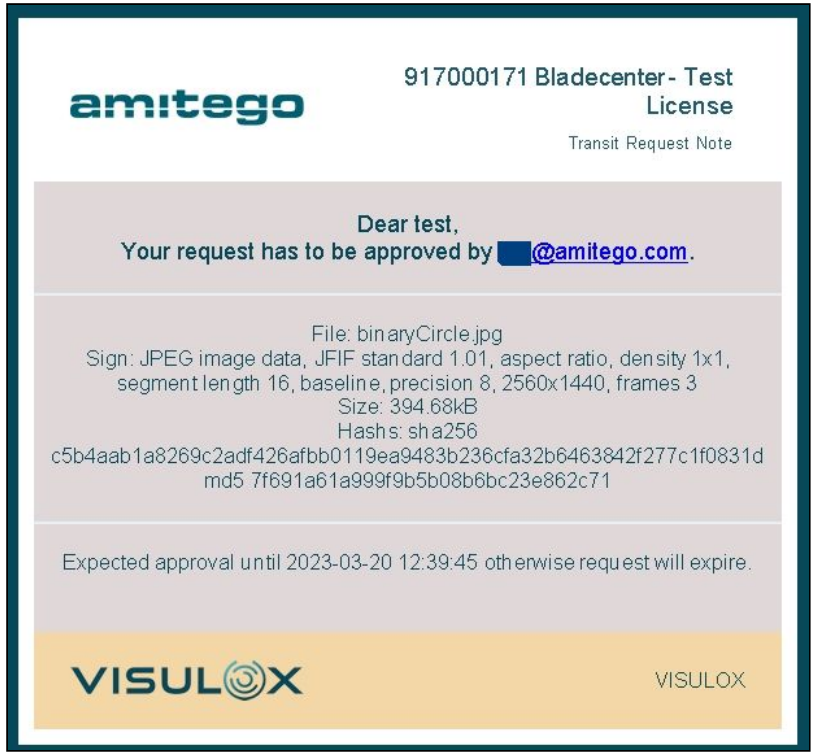


Once the **requester** has uploaded a file into Transit Zone, the status of the file in Workspace is "**Pending**":

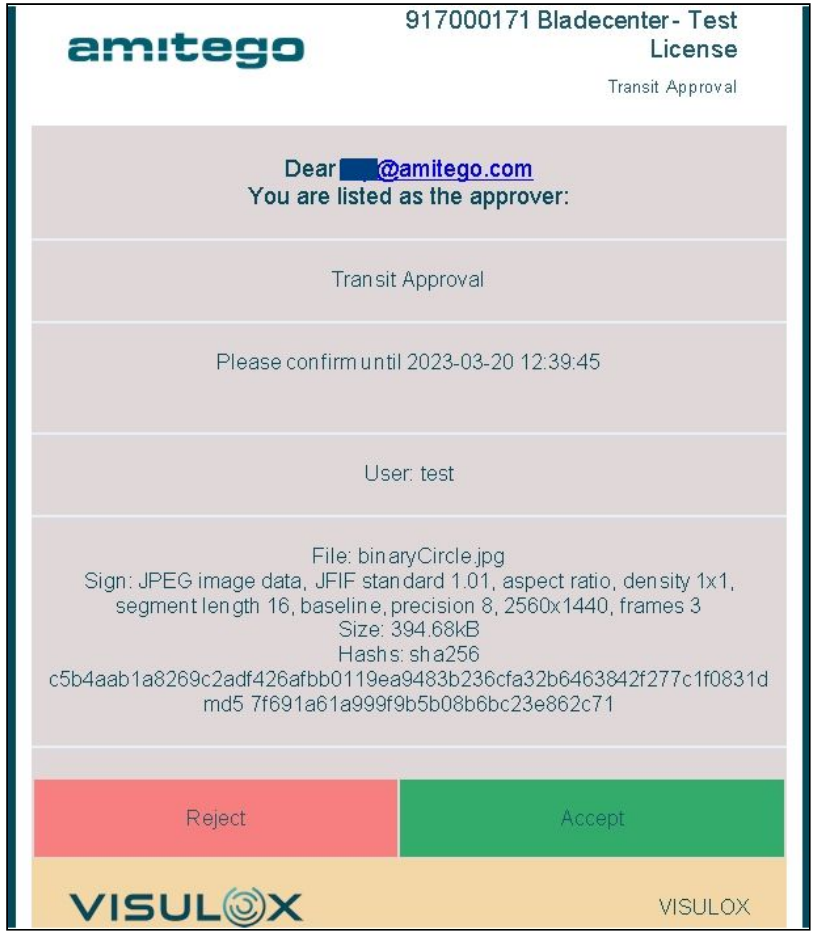


SOURCE	NAME	AVAILABLE	SIZE	FORMAT	STATUS		
user	binaryCircle.jpg	01h 56m	394.68kB	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 2560x1440, frames 3 sha256:c5b4aab1a8269c2adf426afbb0119ea9483b236cfa32b6463842f277c1f0831d md5:7f691a61a999f9b5b08b6bc23e862c71	pending:POL-FT	Download	Delete

The **requester** always gets a confirmation mail for his file request:

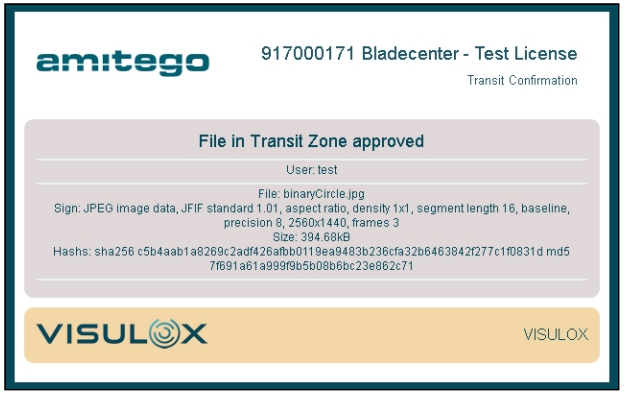
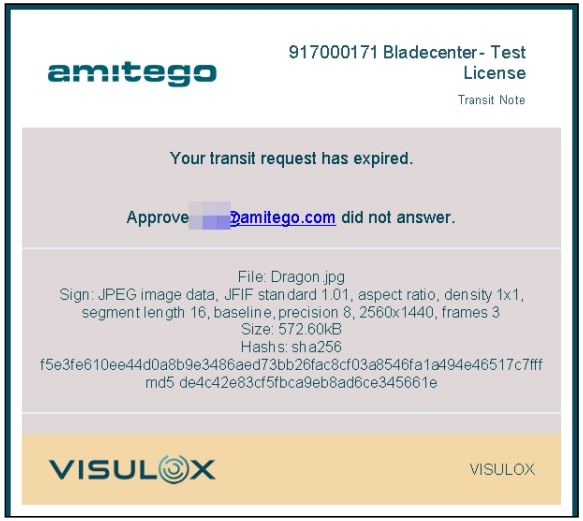


The configured **approver** gets the mail with the actionlink to approve or reject the file:

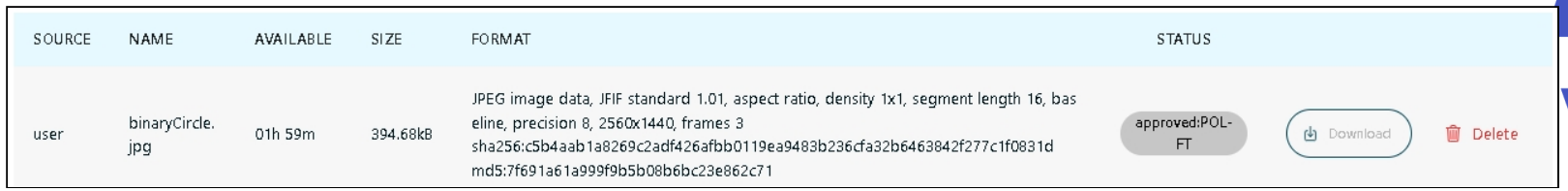


The approver is forwarded to a HTML confirmation page once he has pressed a button.

Now the **requester** receives a mail depending on the result of his request: **approved**, **rejected** or **expired**:

Approved	Rejected	Expired
		
File is approved and allowed to transfer.	File is rejected by the approver and not allowed to transfer.	When the approver does not react, the request will expire, a mail is sent to the requester and the approver.

If the file is approved, the status of the file in the Workspace is set to "**Approved**":



Modification

The modification of the default request / approve mails and the HTML page is possible.

The CSS templates can be found in: **/opt/visulox/etc/html/css/**
The HTML templates can be found in: **/opt/visulox/etc/html/templates/**

> If the texts should be displayed in other languages, the templates have to be adjusted.

The mails / HTML pages, that are used can be adjusted or added in the request action script;

```
...
case $SUBCOMMAND in
    "")
        usage
        ;;
    "setup")
        runSetup
        ;;
     "accessRequestedByUser")
        checkParams
        mailToRequester WS-Req requesterWorkspaceEmail
        mailToApprover  WS-Req approverWorkspaceEmail
```

```
        ;;
    "accessRequestedFromSession")
        checkParams
        mailToRequester ACC-Req requesterSessionEmail
        mailToApprover  ACC-Req approverSessionEmail
        ;;
    "accessRequestApproved")
        checkParams
        mailToRequester ACC-Confirm requesterEmailApproved
        ;;
    "accessRequestRejected")
        checkParams
        mailToRequester ACC-Rejected requesterEmailReject
        ;;
    "accessRequestExpired")
        checkParams
        mailToRequester ACC-Expired requesterEmailExpired
        mailToApprover  ACC-Expired approverEmailExpired
        ;;
    "transitRequestedByUser")
        checkParams
        mailToRequester TZ-Req requesterTransitEmail
        mailToApprover  TZ-Req approverTransitEmail
        ;;
    "transitRequestApproved")
        checkParams
        mailToRequester TZ-Confirm requesterEmailTransitApproved
        ;;
    "transitRequestRejected")
        checkParams
        mailToRequester TZ-Rejected requesterEmailTransitReject
        ;;
    "transitRequestExpired")
        checkParams
```

```
        mailToRequester TZ-Expired requesterEmailTransitExpired
        mailToApprover  TZ-Expired approverEmailTransitExpired
        ;;
    *)
        usage
esac
...
```

All system logos used in the mails should have **96dpi**.
If the design is adjusted, the mails and the HTML page should be checked with different mail clients and browsers.

Templates and testing

The HTML page templates can be viewed with:

```
https://<server>/ack/test?page=<name>
```

The mail templates can be tested with:

```
/opt/visulox/lib/utils/mailclient.tcl -html <template>-subject 'TEST: <template>' -to <mail@domain.com>
```

With **visulox config -name request.dumpvars=true**, a list of the current VLX variables is attached to the footer.

Available variables

```
VLXTTAMODE VLXUSERPROFILE VLXUSERPROFILESHORT VLXSESSIONMODE VLXAPPLICATIONHOST VLXAPPLICATIONARGUMENTS
VLXGATEWAYIP VLXAPPROVERINFO VLXOWNERID VLXSESSIONID VLXCREATETIME_FMT VLXAPPLICATIONUSER
VLXAPPLICATIONCOMMAND VLXEVENTINFO VLXSESSIONSTARTTIME_FMT VLXAPPROVER VLXLOGINUSER VLXREPOSITORY
VLXPOLICY VLXRECIPIENT VLXCUSTOMERLOGO VLXACCESSPOINT VLXPATH VLXBANNER VLXCLIENTIP VLXSESSIONHOST
VLXOWNERSHORT VLXACKNOWLEDGE VLXWEBTOPBASE VLXAPPLICATIONSHORT VLXREMOTEIP VLXLOGINSCRIPT VLXEMAIL
```

```
VLXGROUPLIST VLXACKNOWLEDGELIFETIME VLXOWNER VLXSURNAME VLXACKNOWLEDGEUUID VLXAPPLICATIONID
VLXTICKETID A-12 VLXCREATETIME VLXCONNECTIONINFO VLXFULLNAME VLXUTIL VLXGROUPLIST_FMT
VLXACKNOWLEDGELIFETIME_FMT VLXSESSIONSTARTTIME VLXLANG VLXAPPLICATION VLXTEXTCOLOR VLXBASECOLORDARK
VLXBANNERCOLOR VLXACCENTCOLOR VLXPRODUCTLOGO VLXBANNERTEXTCOLOR VLXPRODUCTTITLE VISULOX
```

Related articles

(4.1.1) Access and transit request via actionlink

(4.1.1) Access Branding

(4.1.1) Access Policy

(4.1.1) Access request and access to applications

(4.1.1) Handling ticket IDs from external systems

(4.1.1) How to control access from the command line

(4.1.1) How to control groupaccess from the command line

(4.1.1) How to enable access to applications

(4.1.1) How to handle access for groups

(4.1.1) How to lock a user permanently for using an application after keyword detection

(4.1.1) How to use the VISULOX Command Line Interface from a remote server

(4.1.1) In-time access

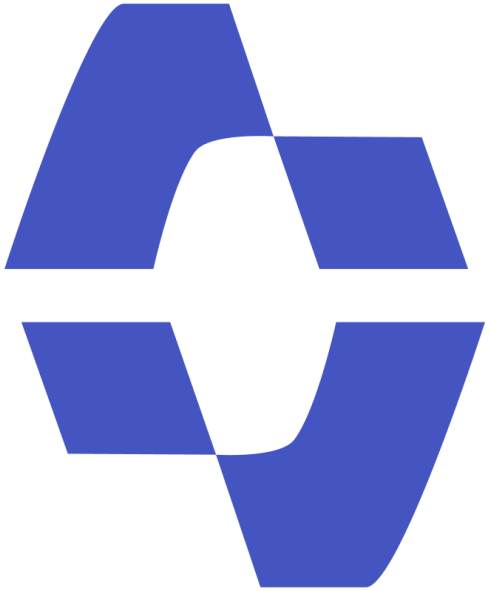
(4.1.1) Login and Access Management

(4.2.0) Access and transit request via actionlink

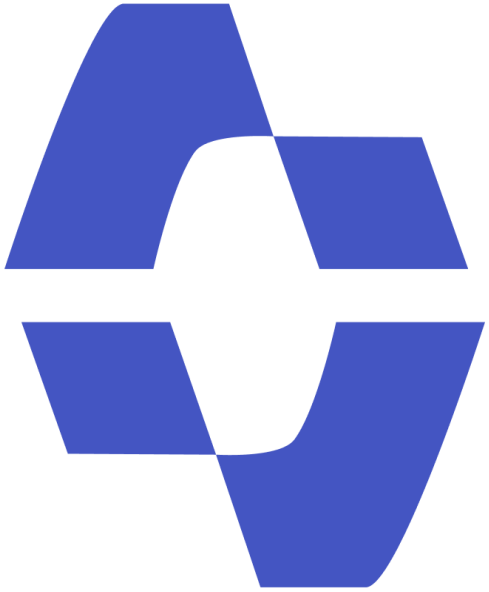
(4.2.0) Access Branding

(4.2.0) Access Policy

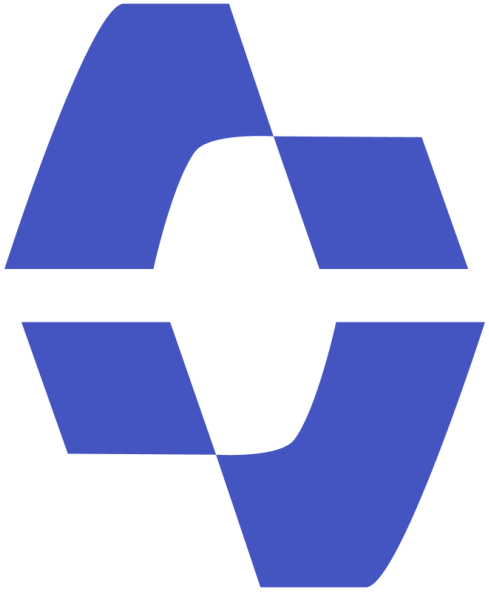
(4.2.0) Access request and access to applications



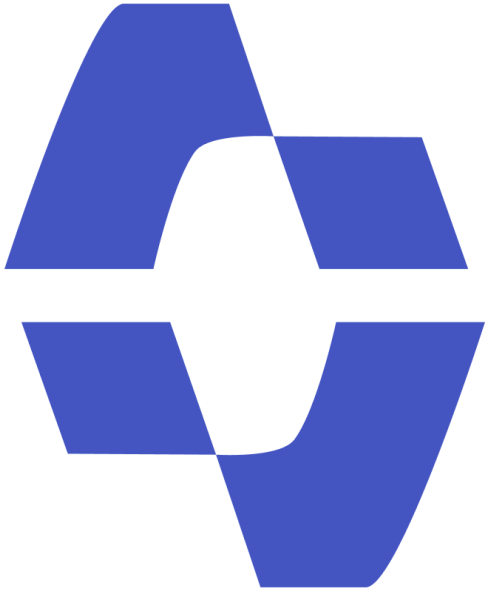
(4.2.0) Handling ticket IDs from external systems
(4.2.0) How to control access from the command line
(4.2.0) How to control groupaccess from the command line
(4.2.0) How to enable access to applications
(4.2.0) How to handle access for groups
(4.2.0) How to lock a user permanently for using an application after keyword detection
(4.2.0) How to use the VISULOX Command Line Interface from a remote server
(4.2.0) In-Time Access
(4.2.0) Login and Access Management
(4.3.0) Access and transit request via actionlink
(4.3.0) Access Branding
(4.3.0) Access Policy
(4.3.0) Access request and access to applications
(4.3.0) Handling ticket IDs from external systems
(4.3.0) How to control access from the command line
(4.3.0) How to control groupaccess from the command line
(4.3.0) How to enable access to applications
(4.3.0) How to handle access for groups
(4.3.0) How to lock a user permanently for using an application after keyword detection
(4.3.0) How to use the VISULOX Command Line Interface from a remote server
(4.3.0) In-Time Access
(4.3.0) Login and Access Management



(4.3.1) Access and transit request via actionlink
(4.3.1) Access Branding
(4.3.1) Access Policy
(4.3.1) Access request and access to applications
(4.3.1) Handling ticket IDs from external systems
(4.3.1) How to control access from the command line
(4.3.1) How to control groupaccess from the command line
(4.3.1) How to enable access to applications
(4.3.1) How to handle access for groups
(4.3.1) How to limit the granting endtime in Access Policies
(4.3.1) How to lock a user permanently for using an application after keyword detection
(4.3.1) How to use the VISULOX Command Line Interface from a remote server
(4.3.1) In-Time Access
(4.3.1) Login and Access Management
(4.3.1) Time zones, holidays and time profiles
(4.3.2) Access and transit request via actionlink
(4.3.2) Access Branding
(4.3.2) Access Policy
(4.3.2) Access request and access to applications
(4.3.2) Access termination enforced
(4.3.2) Handling ticket IDs from external systems
(4.3.2) How to control access from the command line



(4.3.2) How to control groupaccess from the command line
(4.3.2) How to enable access to applications
(4.3.2) How to handle access for groups
(4.3.2) How to limit the granting endtime in Access Policies
(4.3.2) How to lock a user permanently for using an application after keyword detection
(4.3.2) How to use the VISULOX Command Line Interface from a remote server
(4.3.2) In-Time Access
(4.3.2) Login and Access Management
(4.3.2) Time zones, holidays and time profiles
Access and transit request via actionlink
Access Branding
Access Policy
Access request and access to applications
Access termination enforced
Handling ticket IDs from external systems
How to control access from the command line
How to control groupaccess from the command line
How to enable access to applications
How to handle access for groups
How to limit the granting endtime in Access Policies
How to lock a user permanently for using an application after keyword detection
How to use the VISULOX Command Line Interface from a remote server



In-Time Access
Login and Access Management
Time zones, holidays and time profiles
(4.1.1) How to limit the granting endtime in Access Policies
(4.1.1) Time zones, holidays and time profiles
(4.2.0) How to limit the granting endtime in Access Policies
(4.2.0) Time zones, holidays and time profiles
(4.3.0) How to limit the granting endtime in Access Policies
(4.3.0) Time zones, holidays and time profiles
Access and transit request via actionlink
Access Branding
Access Policy
Access request and access to applications
Access termination enforced
Handling ticket IDs from external systems
How to control access from the command line
How to control groupaccess from the command line
How to enable access to applications
How to handle access for groups
How to limit the granting endtime in Access Policies
How to lock a user permanently for using an application after keyword detection
How to use the VISULOX Command Line Interface from a remote server

23.1.93 How to handle access for groups

- Group based access
- Enhanced configuration if user is not set
- Project based application access
- Related articles

Group based 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.

VISULOX Access Policy allows two methods:

1) One Access Policy for all users in the group. This is a standard Access Policy

2) Individual access for members in the group based on an access template. The access template includes starttime, endtime and a timeprofile. This is called a Group Access.

The Access Policy set to mode "**Group Access**" now defines:

- The timeframe, when this policy is valid: timeprofile, start and endtime
- The members of this policy
- The applications to what this policy is applied.

If the policy does not match in timeprofile, start, endtime, user and application filter, the next policy will be checked.

If the policy is applied, the next step is to check, if the current user belongs to this Group Access with his application, and if he is allowed to use the application, within his definition of start and endtime.

The method of Group Access is used to coordinate projects and project teams.

Example to use this access method

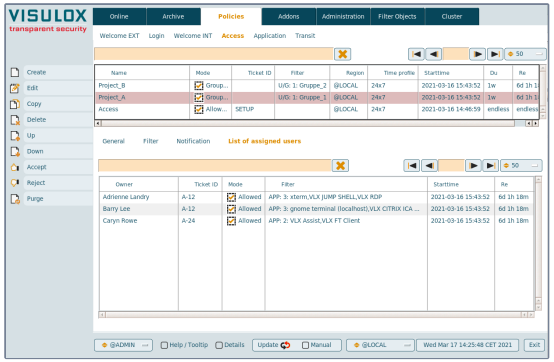
In an organisation, there are two projects:

Project (A) for a group of users represented with G1 and applications (app1,app2)
Project (B) for a group of users represented with G2 and applications (app1,app2)

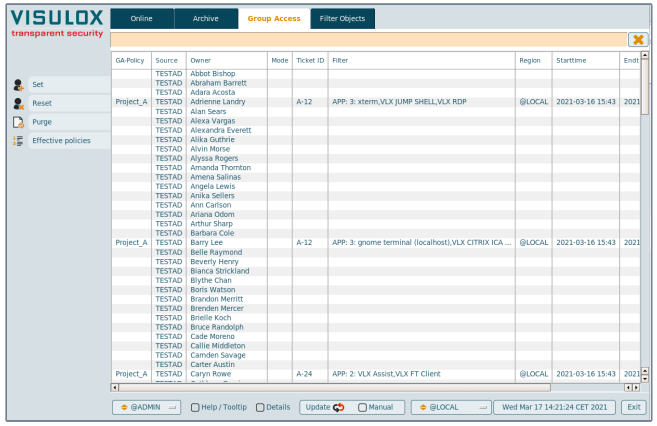
A Group Access Console can be defined for Project_A and Project_B:

Arguments for command
-name vlxaccess -groupaccess Project_A
-name vlxaccess -groupaccess Project_B

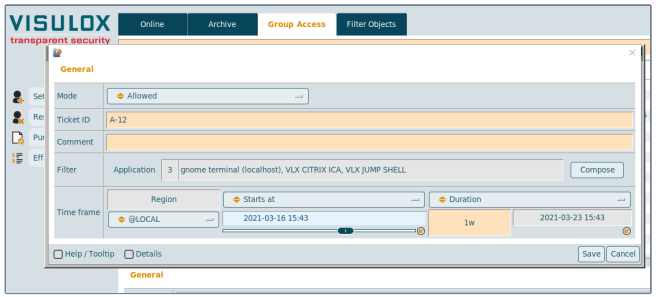
Users who have this applications assigned can now add and remove users with the assigned Group Access Policy (Project_A or Project_B):



Users must be members of the Group Access Policy



Group Access Console



Adding a user to Group Access

Within the vlxacess application, the Online and Archive view is presented additionally.

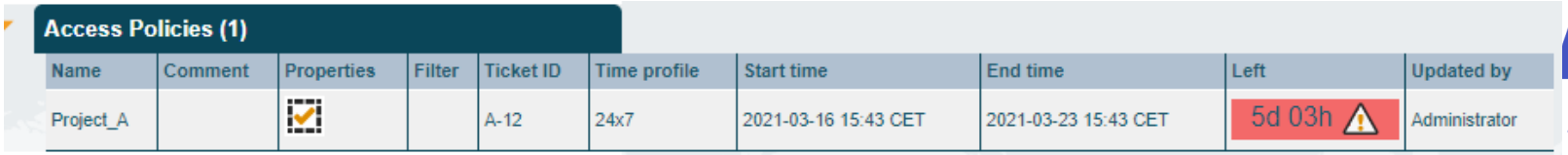
The view filters for Online and Archive are used from the Group Access Policy. This achives to provide a "VISULOX Cockpit for Project_A or Project_B" automatically.

More control within vlxaccess can be done with the parameter -roles as usual.

```
vlxgui -name vlxaccess -groupaccess Project_B -roles B
```

Outdated entries on the Group Access page can be purged via the "**Purge**"-button.

Example for Group Access in the user's Workspace:



Specials:

- Group Access Policy does not enforce the ticket ID. The ticket ID is enforced on the assigned users.
- Group Access Policy can not be configured with an empty user/group filter.
- Group Access can not be controlled by a Cockpit filter rule. This object is ignored.
- The comment in Group Access Policy and the comment in the user access is concatenated.
- A user can be in multiple Group Access groups.
- Currently Online and Archive views can only be filtered by user/group and application.

Enhanced configuration if user is not set

With the existing policy model, a matching `GroupAccess` policy becomes the effective Access Policy even if the user is not listed in the corresponding Access Group.

In this case, the GroupAccess evaluation results in **DENY** and policy evaluation stops. Any following Access Policies are ignored.

This prevents configurations where, for example:

- **Admin GER** can grant access to GER and EU applications.
- **Admin EU** can grant access only to EU applications.

A preceding `GroupGER` policy may match by its policy filters, but if the user is not configured in this group, evaluation stops and a following `GroupEU` policy is never reached.

In case of this scenario, the following configuration parameter can be adjusted:

```
general.skipNonMatchingGroup
```

It can be enabled with:

```
visulox config -name general.skipNonMatchingGroup=true
```

The default is:

```
false
```

With `false`, the existing policy behavior remains unchanged.

With `true`, if a GroupAccess policy results in DENY because the user is not listed in the corresponding Access Group, the Policy Client remembers this policy in an `ignorePolicyList`.

The Policy Client then queries the Policy Service again and passes the `ignorePolicyList`. The Policy Service skips these policies during the new evaluation.

If another non-matching GroupAccess policy is returned, it is also added to the `ignorePolicyList` and evaluation continues.

This process is repeated until either:

- a GroupAccess policy allowing access is found, or
- no further applicable policy is available.

This allows multiple GroupAccess policies to be evaluated in sequence while keeping the existing policy model as the default behavior.

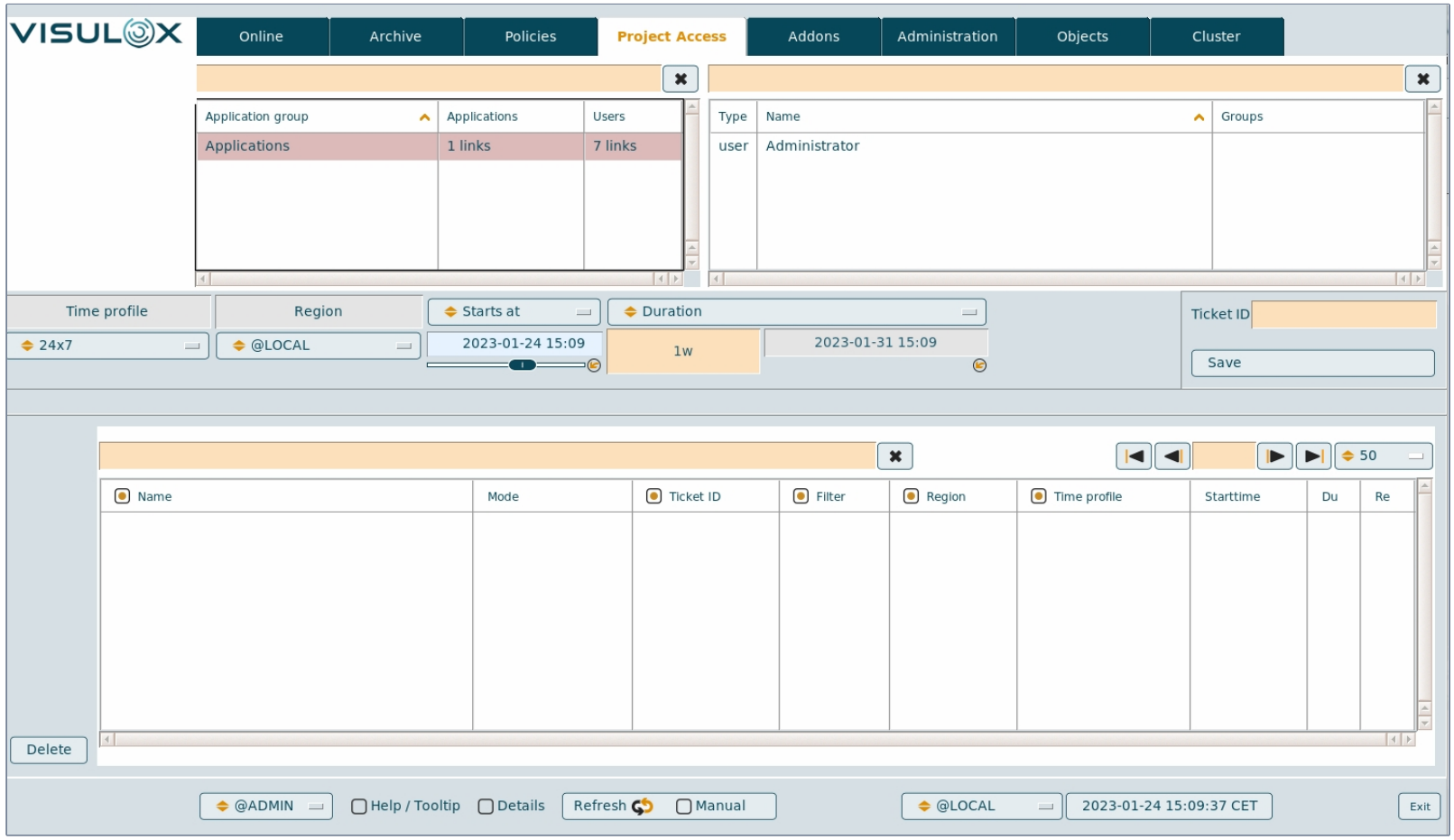
Project based application access

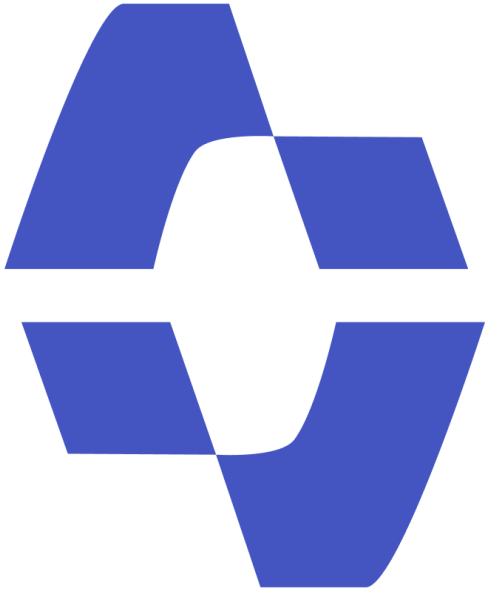
A project based access needs a special organization hierarchy of projects and the assigned applications in the datastore.

Parameters to enable the project view in VISULOX Cockpit are **-project** and **-projectmask** <mask>. The default project mask is "*****"

```
vlxgui -name ProjectAccess -project "Test Applications"
```

With these start parameters for VISULOX Cockpit / vlxgui, the Project Access tab is displayed to setup and configure user application access based on application groups.





Related articles

How to control groupaccess from the command line

23.1.94 Creating VISULOX user groups based on an AD/LDAP attribute

Some AD/LDAP setups do not use AD/LDAP groups assigned to users. So policies based on an AD/LDAP attribute are not possible.

VISULOX supports creating up to four internal groups based AD/LDAP attributes.

Therefore a single step with a VISULOX mapping cust file is needed.

For example:

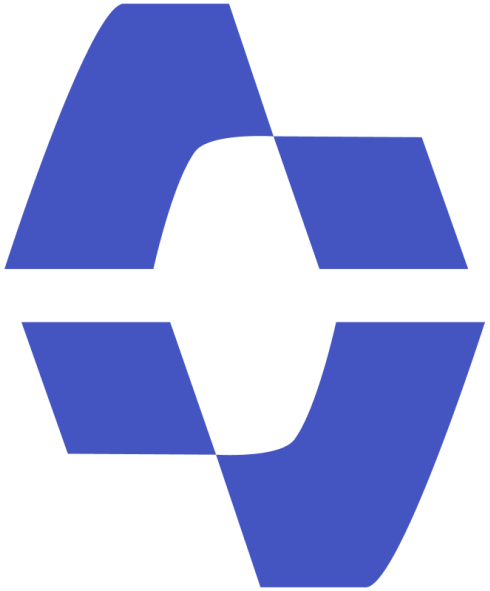
Example employeeType

```
{
    varmapping {
        columns {source external internal convert}
        rows {
            {{MSAD.USER} {employeeType}            {vlxuserdata1}    {}}
            }
    }
}
```

Instead of **vlxuserdata1**, it is also possible to use **vlxuserdata2**, **vlxuserdata3** or **vlxuserdata4**.

It is also possible to assign multiple tags with "**:**" as delimiter:

```
attribute=zone1:zone2:zone3
```



Each user with the LDAP attribute set gets a group assigned with: **cn=ATTR$id-$name,dc=internal**

- With ID = 1, 2, 3, 4 - based on **vlxuserdata**
- With name = “Content of the AD/LDAP group”

The example above adds the employeeType to each user: **cn=ATTR1-External,dc=internal**, **cn=ATTR1-Internal,dc=internal**

Now it is possible to create a policy bassed on the employeeType by using ATTR1-External as a User/group filter.

Configurable regexp for LDAP attributes

An LDAP attribute, e.g. email can be analyzed, so that only the domain will be returned. Then a group will be created for each domain, that can be used by policies.

If polices should be created on an LDAP attribute, **vlxuserdata1 to 4** can be used.

If the attribute is unambiguously (like the email address), then it is needed to extract the ambiguous part (like the domain from the email).

Therefore a custom datasource mapping has to be created with the mapping of the unambiguously attribute to vlxuserdata1 to 4, using the function **extractvar**. The function extractvar uses the configuration parameter **regexp.extractvar**.

For example:

```
{
    varmapping {
        columns {source external internal convert}
        rows {
            {{MSAD.USER} {mail} {vlxuserdata2} {extravar}}
            }
    }
}
```

⚠ Currently only one LDAP attribute can be send over extractvar, more on request.

Since VISULOX 3.2 always internal groups for the domains are created.

Related information

How to work with VISULOX datasources

Active Directory Attributes

How to configure alternate mappings for datasources

23.1.95 How to handle different client versions on one platform with vlxshell

VLX Shell is being used as a framework to different clients (Xterm, Gnome, Firefox, RDesktop, ICA, freeRDP).
Depending on the client, the vlxtransit directory is provided. (Firefox as the default download directory, RDP or ICA drive redirection).

The client binary is searched in some dirctories during startup:

```
/usr/bin, /usr/local/bin, /usr/lib/ICAClient, /usr/opt/Citrix/ICAClient, /opt/Citrix/ICAClient
```

If the client is not found an error is thrown. It is also possible to address the client binary directly using the **-clientcmd** option.

```
vlxshell.tcl -client firefox -clientcmd /path1/firefox
```

With this option it is possible to address different versions of the client with the same type on the same platform.

vlxshell.tcl -client
`vlxshell.tcl -client firefox -clientcmd /path1/firefox`

```
vlxshell.tcl -client firefox -clientcmd /path2/firefox
vlxshell.tcl -client firefox -clientcmd /path3/firefox

vlxshell.tcl -client ica -clientcmd /path1/wfica
vlxshell.tcl -client ica -clientcmd /path2/wfica
```

More useful parameters of vlxshell.tcl

- When application launch is slow, the session is closed by the VISULOX PORTAL Service because of an empty screen.
  The following parameter will keep the session open, so the application now has time to launch:

  ```
  vlxshell.tcl -wait <sec>
  ```

  This allows to give slow connections a chance for presentation.

- Activate **vlxtransit** and **vlxupload** for the application:

  ```
  vlxshell.tcl -sync
  ```

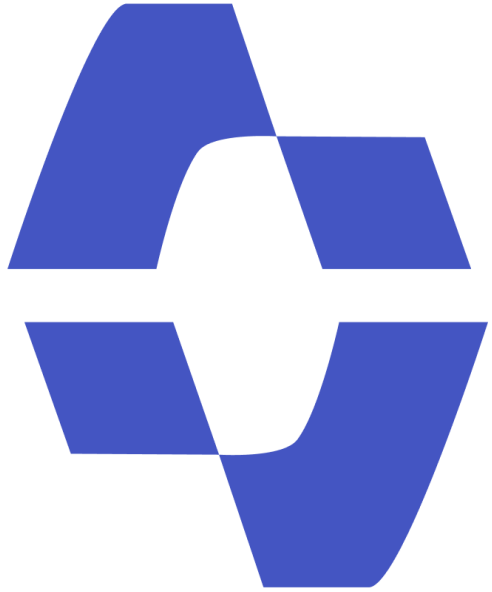
Related articles

VISULOX user sandbox (vlxjail)

Enable events for VLX Shell, FreeRDP and File Transit connections

VISULOX Firefox Wrapper setup

VISULOX Firefox integration



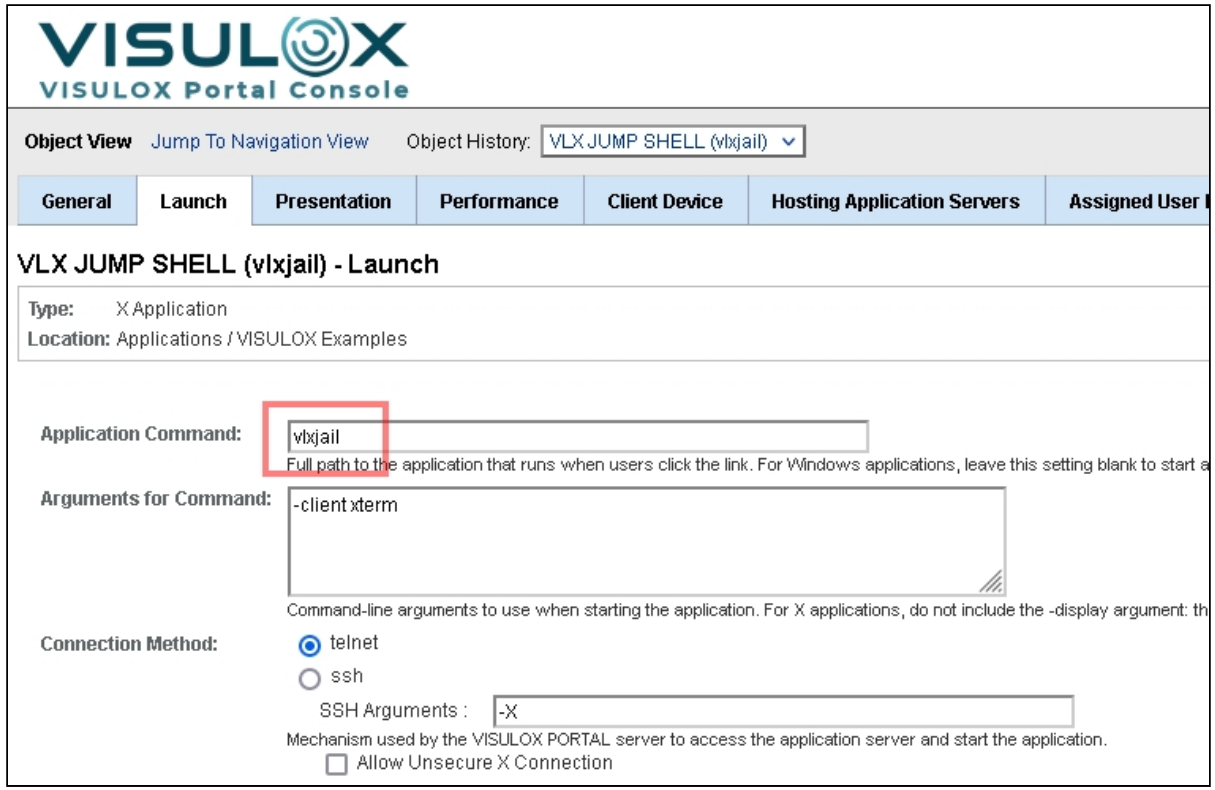
23.1.96 VISULOX user sandbox (vlxjail)

vlxshell is used as a framework to different clients (Firefox, ICA, RDesktop, freeRDP).
Depending on the client, the vlxtransit directory is provided. (Firefox as the default download directory, RDP or ICA drive redirection).

Applications can be adjusted to restrict the access of the users within the startet application.
The user is able to see only his own processes and files, but he can still start all applications.

Therefore **vlxjail** has to be used instead of vlxshell.

For example: VLX Jump Shell - the Application Command **vlxshell** must be changed to **vlxjail**.



⚠ Functionality with other / different clients or shells, if the system deviates from the standard cannot be guaranteed.
In case of issues contact the VISULOX Support Team.

For setup / configuration of a Firefox Wrapper sandbox application, see: VISULOX Firefox Wrapper setup

Configuration

vlxjail parameters

Parameter	Description
-client <*value*>	Client type: chrome, chromium, ffwrapper, firefox, xterm, gnome. Default: xterm
-clientcmd <*value*>	Alternate path to client <>
-title <*value*>	Title of the GUI <>
-lang <*value*>	Language. Default: en
-id <*value*>	Session ID <>
-owner <*value*>	Owner who runs this GUI <>
-allowedSites <*value*>	List of allowedSites in Firefox profile <>
-nolang	Enforce no language
-usermask <*value*>	Mask to add a prefix and/or suffix to sso_user (prefix%USER%suffix) <>

Parameter	Description
-E <*value*>	Extension list for Firefox <>
-P <*value*>	Firefox profile archive or directory <>
-rdpfile <*value*>	RDP file or VISULOX Script Object <>
-profile <*value*>	Name of Citrix profile in database. Default: CITRIX
-gateway-resource <*value*>	Name of gateway passcache resource <>
-resource <*value*>	Name of passcache resource <>
-bwrap <*value*>	Bubblewrap-specific options <>
-sync	Enable vlxtransit to application
-wait value	Wait for connection in seconds. Default: 0

Related articles

How to handle different client versions on one platform with vlxshell

Enable events for VLX Shell, FreeRDP and File Transit connections

VISULOX Firefox Wrapper setup

VISULOX Firefox integration

23.1.97 Extended VISULOX PORTAL Service commands

VISULOX extends the PORTAL Service with a set of helpful commands.

List all objects in datastore

```
visulox-portal object list_all
```

Test an object in datastore

```
visulox-portal object exists --name "/dc=de/dc=xxx/ou=xxx/ou=xxx/cn=xxx"
```

return code 0 --> exists!
return code 1 --> does not exist!
return code 255 --> error!

More commands

- visulox-portal object info
- visulox-portal license count
- visulox-portal license count --max
- visulox-portal license count --report

The license count commands can be used for documentation of the usage of the VISULOX PORTAL, therefore a cron job has to be created:

```
1 03 * * * /bin/su ttasys -c "visulox-portal license count" >/dev/null 2>/dev/console
```

23.1.98 VISULOX Cockpit / Online

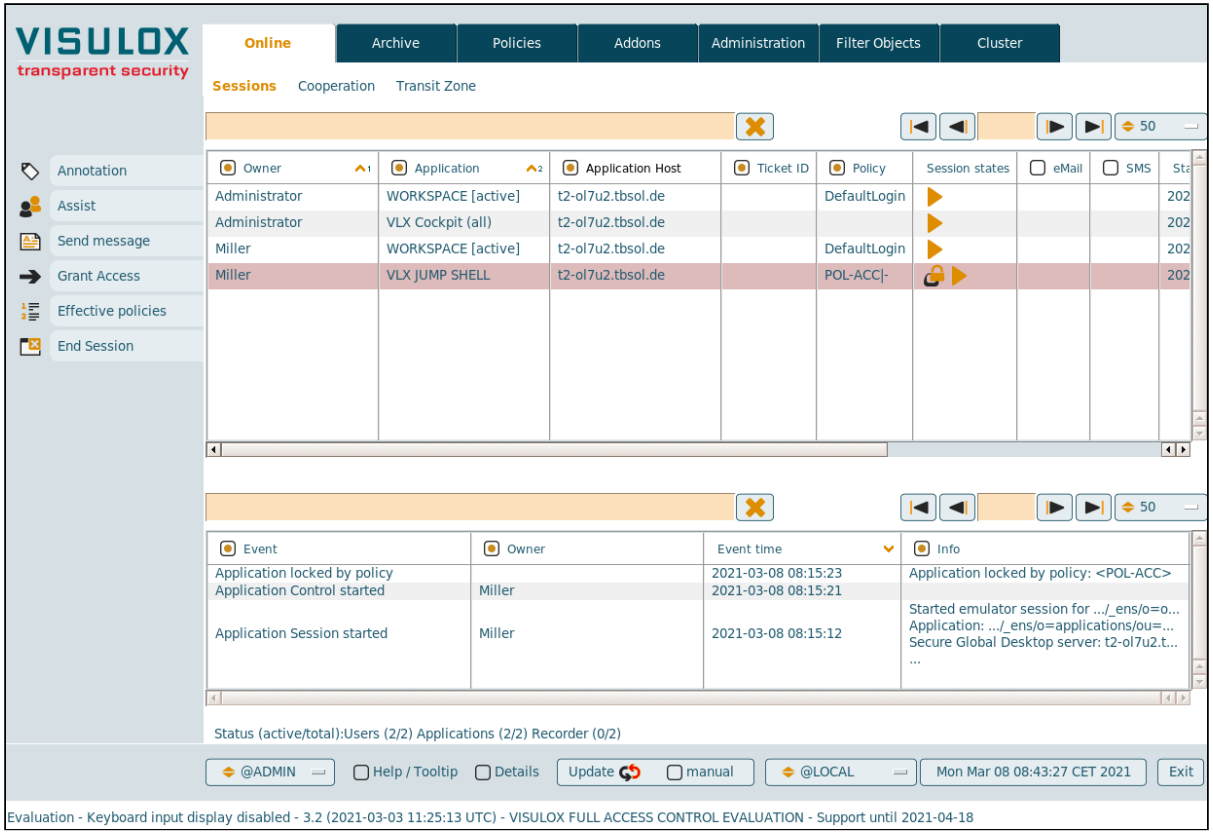
- VISULOX Cockpit Online / Sessions
- VISULOX Cockpit Online / Transit Zone

VISULOX Cockpit Online / Sessions

In the sessions tab the currently logged in users and their active applications are displayed in a table.

If there is a pending Two-Factor Authentication process for a user, his token can be shown by selecting the user entry in the table.

A remark can be added to a session. It is also possible to send messages to application sessions, display the effective policies, grant temporary access and to end application sessions.



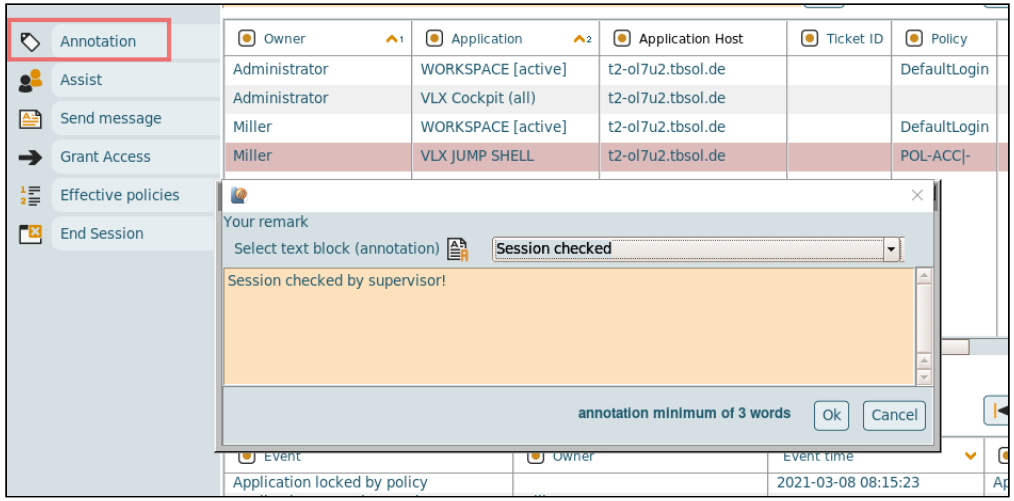
VISULOX Command Line Interface

With the **visulox online** command, the online status can be displayed as well:

Command	Description	Additional commands / args
visulox online	VISULOX online status	getpin, fields (list available fields), -i (ignore case), -object <> (owner or group mask), -application <>, -fields <>, sortby <> (sort by field) List of fields to present <vlxowner,vlxapplication,vlxsessionstarttime,vlxremoteip,vlxapplicationstate>

Available features

- **Annotation**

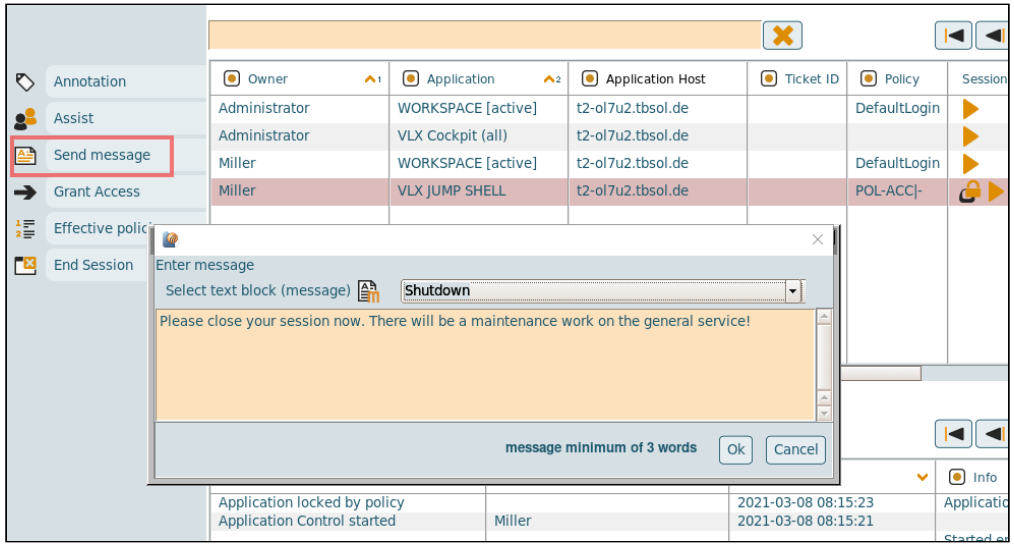


A remark can be added to a session by the supervisor. Remarks are shown in the events section of a selected session.

- **Assist**

A cooperation can be started with a selected session**.** The user controls the cooperation and he has to choose the mode.
The focus switches to **Online / Cooperation**. (See: Example: Assistance)

- **Send message**



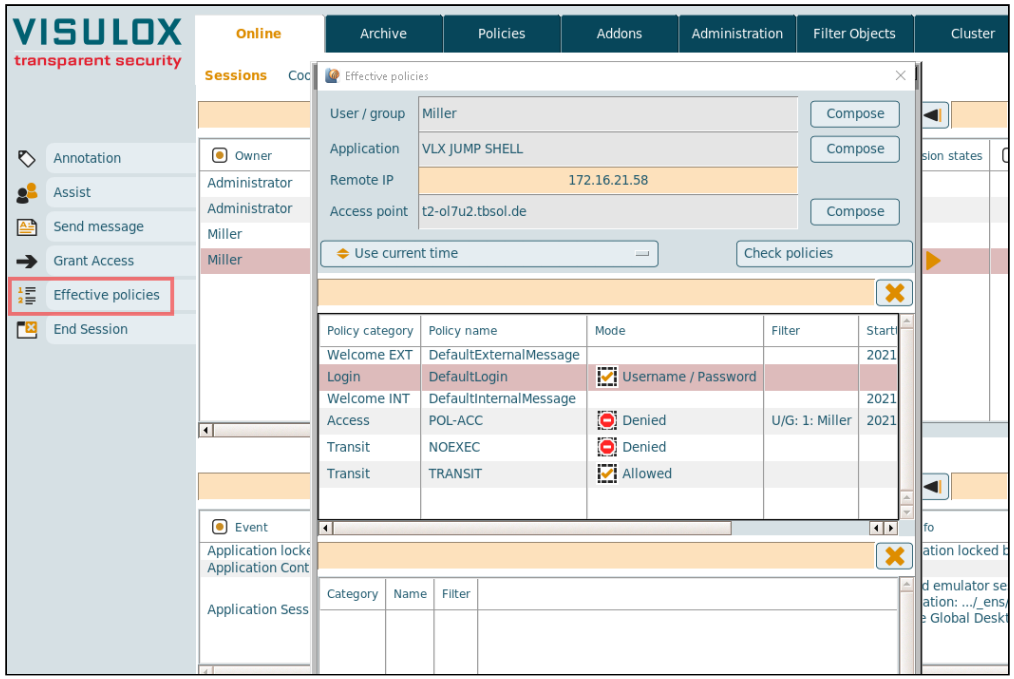
  Supervisors are able to send messages to users, who are working with an application.
  This message is displayed in a popup-window and the application is locked.
  The user has to confirm the message to continue working. The user is also able to give feedback.
  The supervisor gets an overview for the pending and acknowledged messages with comments.

- **Grant access**

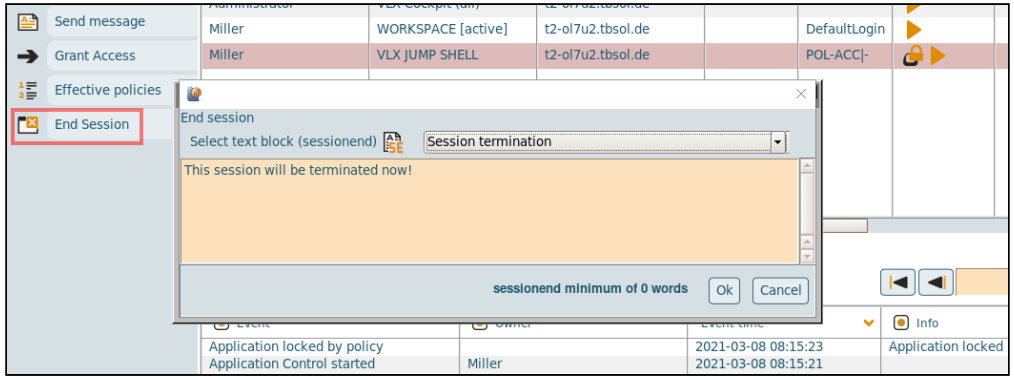
  With access on demand a supervisor is able to give spontaneous access to a session locked by policy. (See: In-Time Access)

- **Effective policies**

  The effective policies for a session can be displayed.

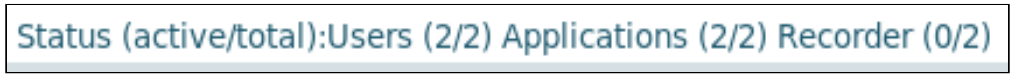

VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
Cluster
Sessions
Annotation
Assist
Send message
Grant Access
Effective policies
End Session
Effective policies
User / group
Miller
Compose
Application
VLX JUMP SHELL
Compose
Remote IP
172.16.21.58
Access point
t2-ol7u2.tbsol.de
Compose
Use current time
Check policies
Policy category
Policy name
Mode
Filter
Welcome EXT
DefaultExternalMessage
2021
Login
DefaultLogin
Username / Password
Welcome INT
DefaultInternalMessage
2021
Access
POL-ACC
Denied
U/G: 1: Miller
2021
Transit
NOEXEC
Denied
Transit
TRANSIT
Allowed
Owner
Administrator
Administrator
Miller
Miller
Event
Application Sess
Category
Name
Filter

- **End session**



The selected sessions will be terminated. A text has to be entered.

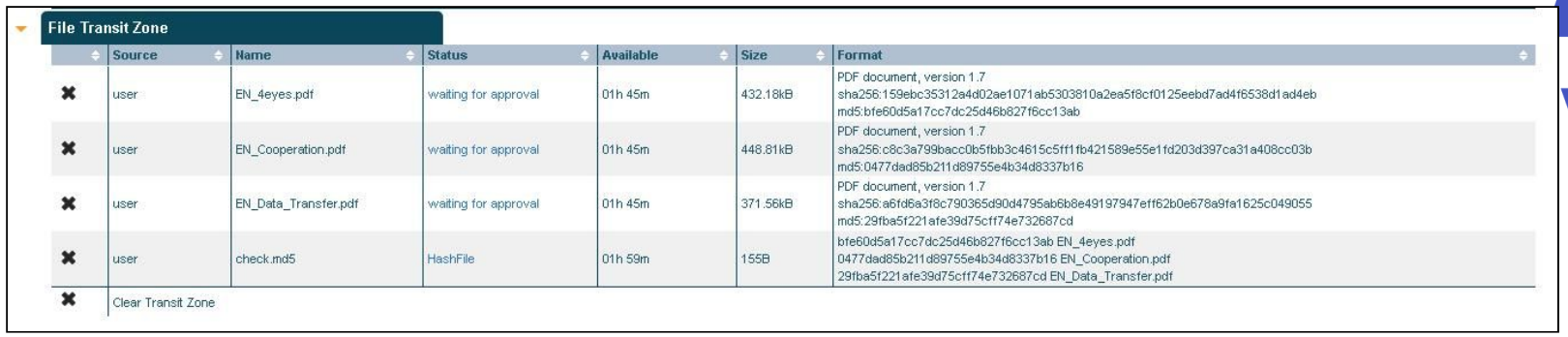
- **Online view - status line**



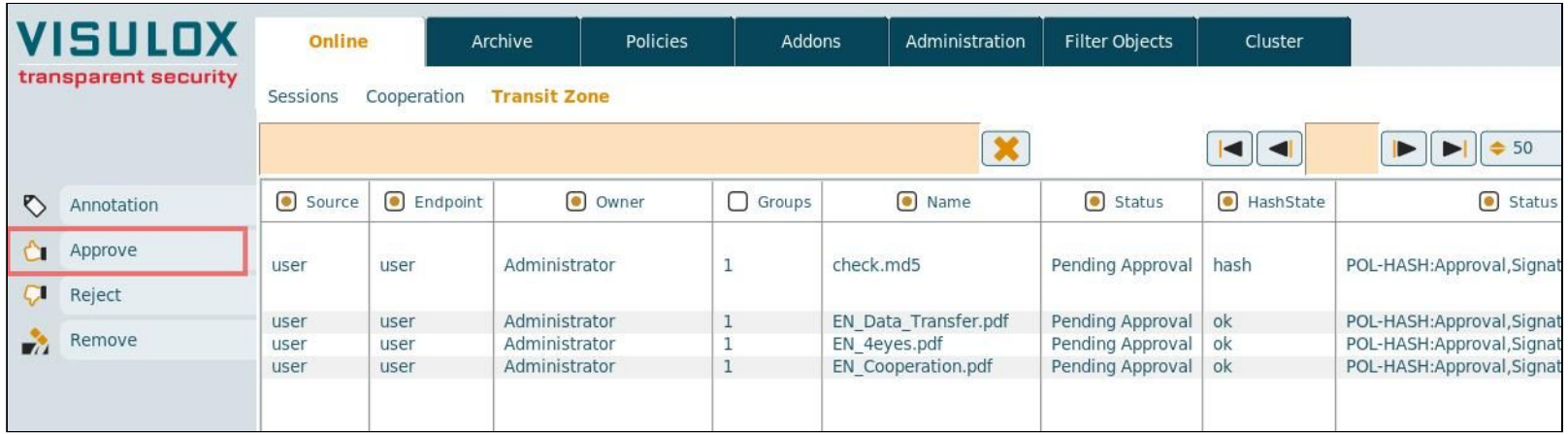
The status line shows the current **active users**, **applications** and **recorders**.
The status of the Workspace session can also be seen directly in the application object column in brackets: **(active)**.
(A Workspace session is considered to be active, if at least one application session is running.)

VISULOX Cockpit Online / Transit Zone

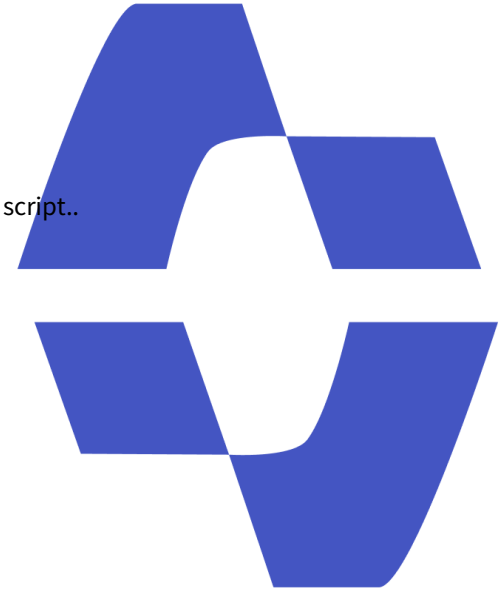
Depending on the underlying Transit Policy files can have the status set to "**Waiting for approval**":



Approval is done by a supervisor in VISULOX Cockpit / Online / Transit Zone or via mail with an assigned request script:



The supervisor is able to approve, reject and remove files. An annotation for a file can also be set.



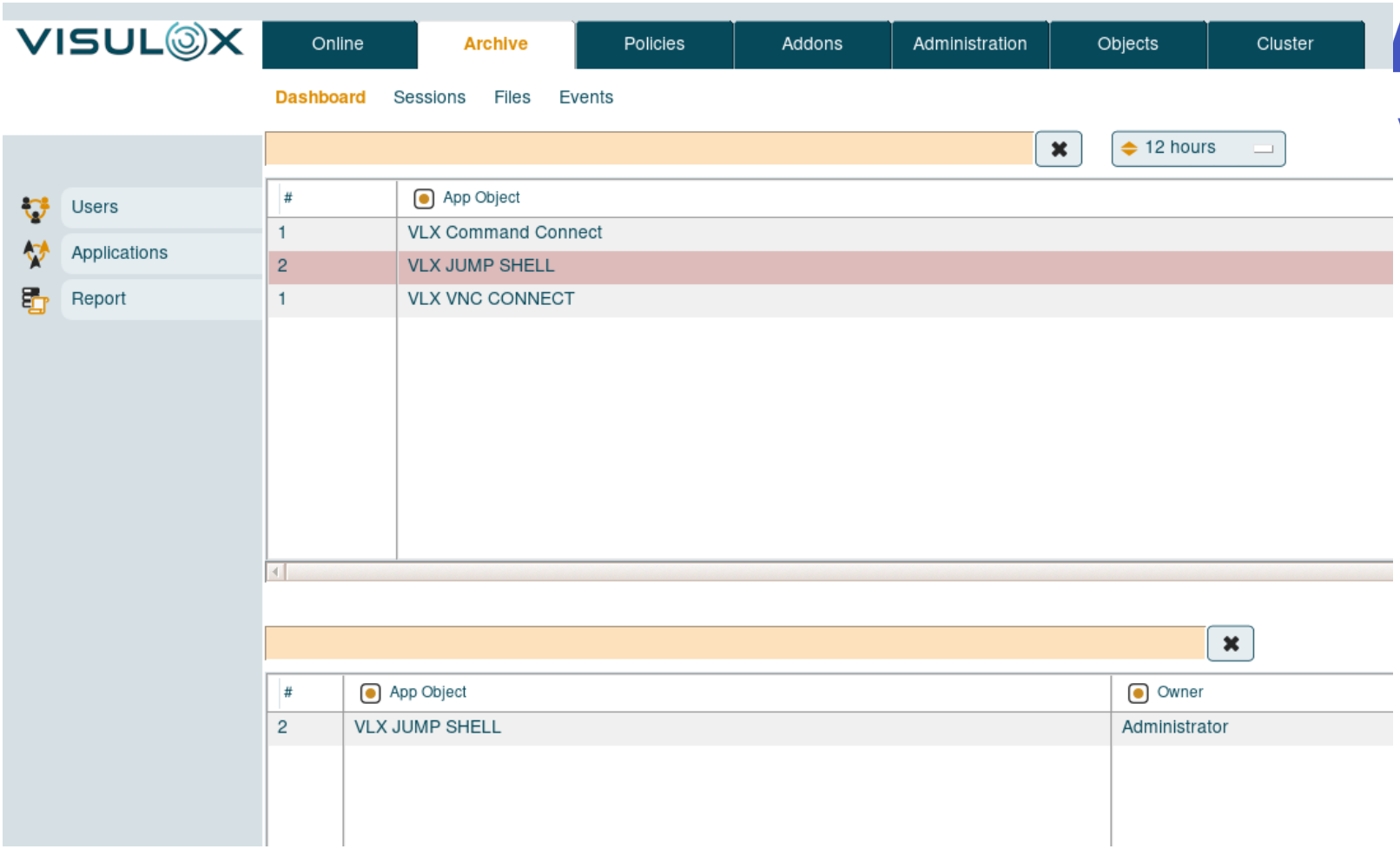
Approving and rejecting files can also be done via command line interface (see: **VISULOX transit command**) or via mail with assigned request script..

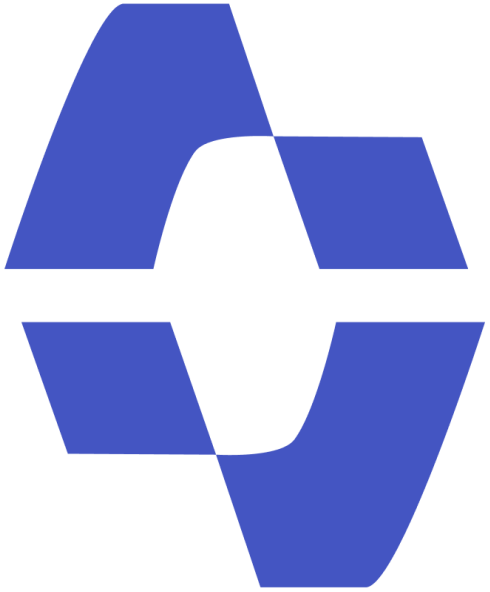
23.1.99 VISULOX Cockpit / Archive

- VISULOX Cockpit Archive / Dashboard
- VISULOX Cockpit Archive / Sessions
- VISULOX Cockpit Archive / Files
- VISULOX Cockpit Archive / Events

VISULOX Cockpit Archive / Dashboard

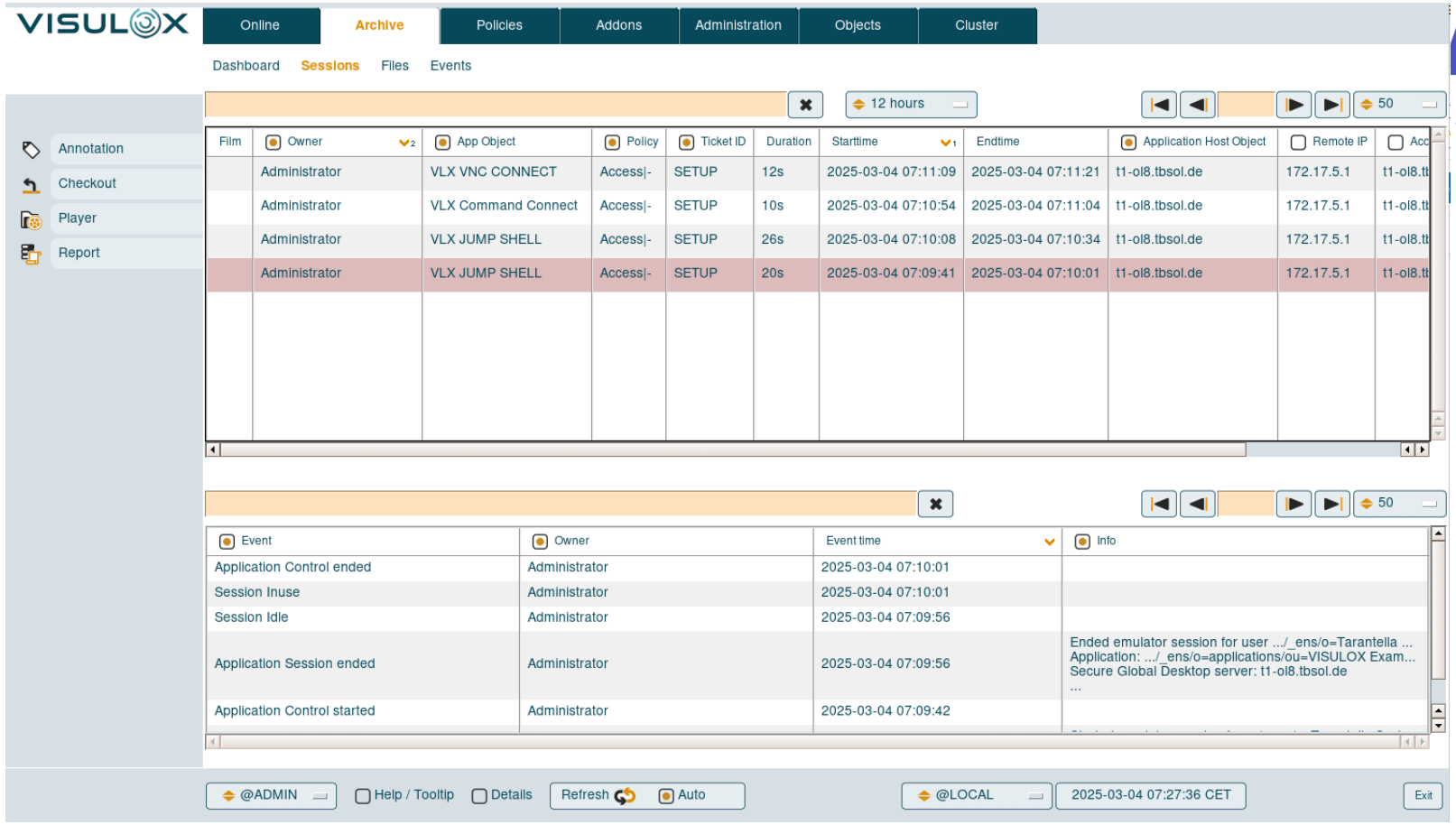
In the dashboard tab information of ended user / application sessions can be found.
Previously logged in users and their used applications are displayed in a table and reports can be generated.


VISULOX
Online
Archive
Policies
Addons
Administration
Objects
Cluster
Dashboard
Sessions
Files
Events
12 hours
Users
Applications
Report
App Object
1 VLX Command Connect
2 VLX JUMP SHELL
1 VLX VNC CONNECT
App Object Owner
2 VLX JUMP SHELL Administrator



VISULOX Cockpit Archive / Sessions

All application sessions with all the available information is displayed in a table.
Once a session is selected all archived events for this session are displayed in a separate table.



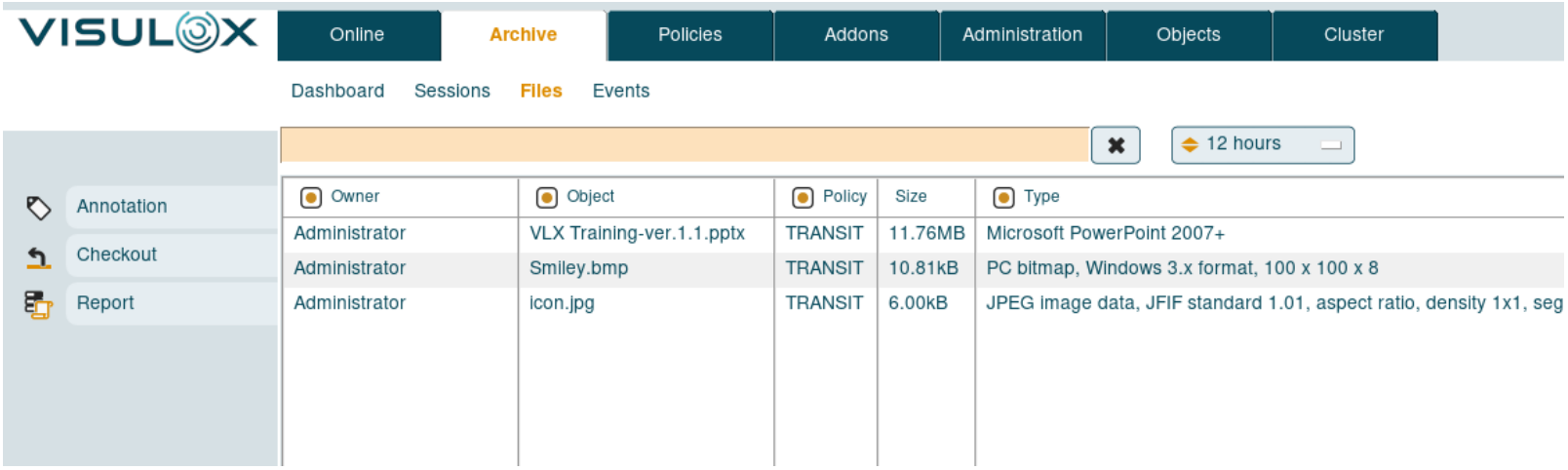
Available features

- **Annotation**
  A remark can be added to a session by the supervisor. Remarks are shown in the events section of a selected session.

- **Checkout**
  Selected sessions can be checked out into Transit Zone, where they can be downloaded to the client.
- **Player**
  Recorded sessions can be viewed with the online player directly in the VISULOX Cockpit. See also: VISULOX Player
- **Report**
  Reports can be generated for the selected sessions.

VISULOX Cockpit Archive / Files

All transferred files from all users and directions are displayed with the available information.



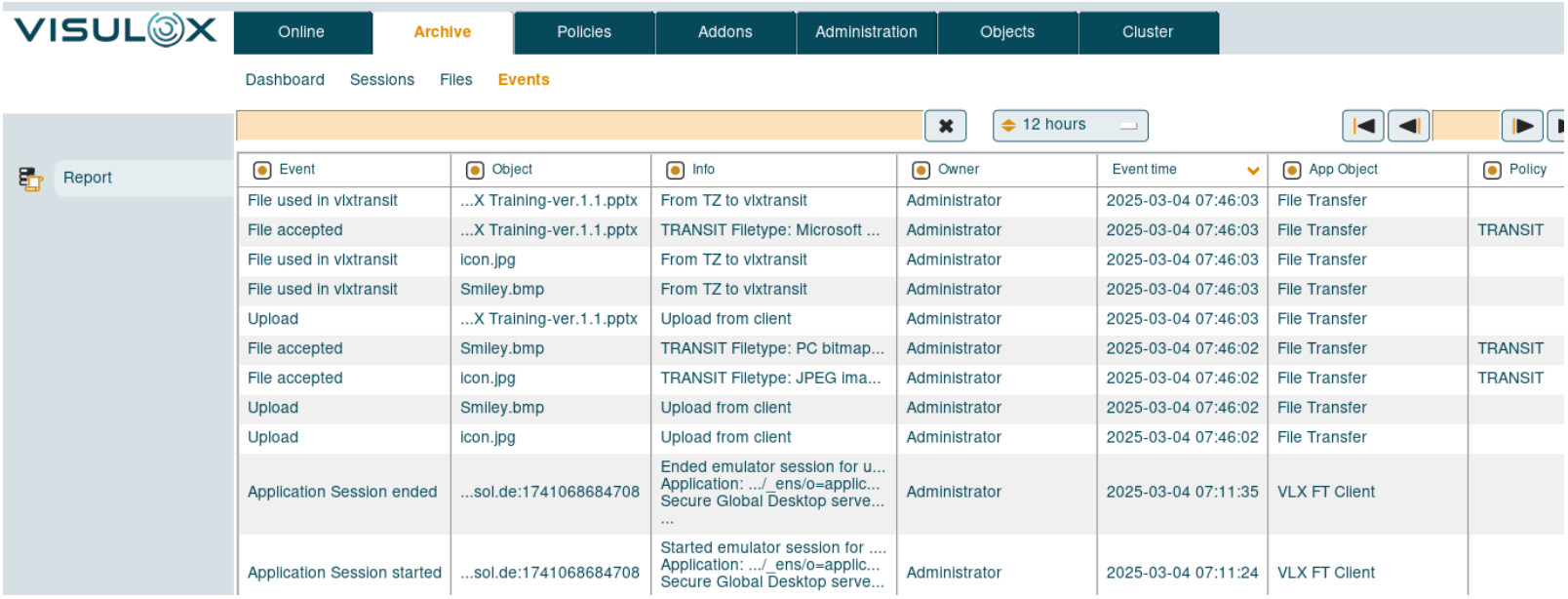
Available features

- **Annotation**
  A remark can be added to a file by the supervisor. Remarks are shown in the events section of a selected session.

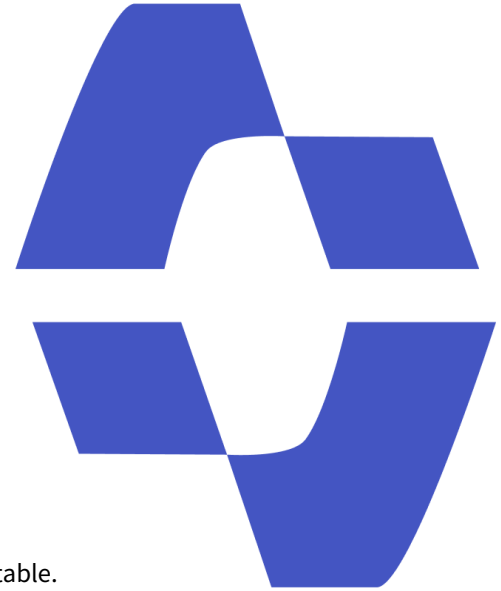
- **Checkout**
  Selected files can be checked out into Transit Zone, where they can be downloaded to the client.
- **Report**
  Reports can be generated for the selected files.

VISULOX Cockpit Archive / Events

In the Events tab all VISULOX events are listed.



Event	Object	Info	Owner	Event time	App Object	Policy
File used in vlxtransit	...X Training-ver.1.1.pptx	From TZ to vlxtransit	Administrator	2025-03-04 07:46:03	File Transfer	
File accepted	...X Training-ver.1.1.pptx	TRANSIT Filetype: Microsoft ...	Administrator	2025-03-04 07:46:03	File Transfer	TRANSIT
File used in vlxtransit	icon.jpg	From TZ to vlxtransit	Administrator	2025-03-04 07:46:03	File Transfer	
File used in vlxtransit	Smiley.bmp	From TZ to vlxtransit	Administrator	2025-03-04 07:46:03	File Transfer	
Upload	...X Training-ver.1.1.pptx	Upload from client	Administrator	2025-03-04 07:46:03	File Transfer	
File accepted	Smiley.bmp	TRANSIT Filetype: PC bitmap...	Administrator	2025-03-04 07:46:02	File Transfer	TRANSIT
File accepted	icon.jpg	TRANSIT Filetype: JPEG ima...	Administrator	2025-03-04 07:46:02	File Transfer	TRANSIT
Upload	Smiley.bmp	Upload from client	Administrator	2025-03-04 07:46:02	File Transfer	
Upload	icon.jpg	Upload from client	Administrator	2025-03-04 07:46:02	File Transfer	
Application Session ended	...sol.de:1741068684708	Ended emulator session for u... Application: .../_ens/o=applic... Secure Global Desktop serve... ...	Administrator	2025-03-04 07:11:35	VLX FT Client	
Application Session started	...sol.de:1741068684708	Started emulator session for .... Application: .../_ens/o=applic... Secure Global Desktop serve...	Administrator	2025-03-04 07:11:24	VLX FT Client	



Available features

- **Report**
  Reports can be generated for the selected events.

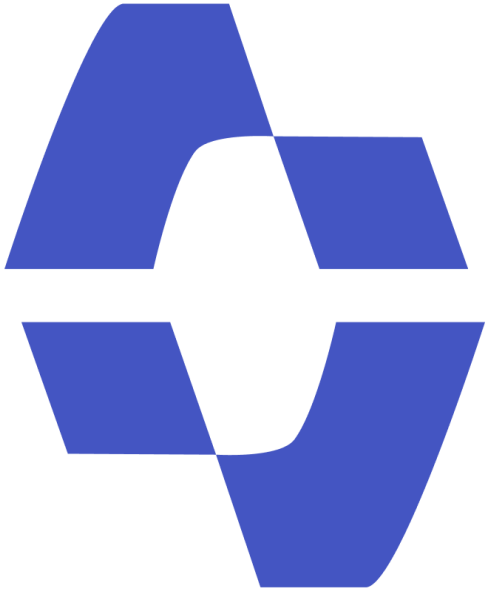
23.1.100 VISULOX Cockpit / Objects

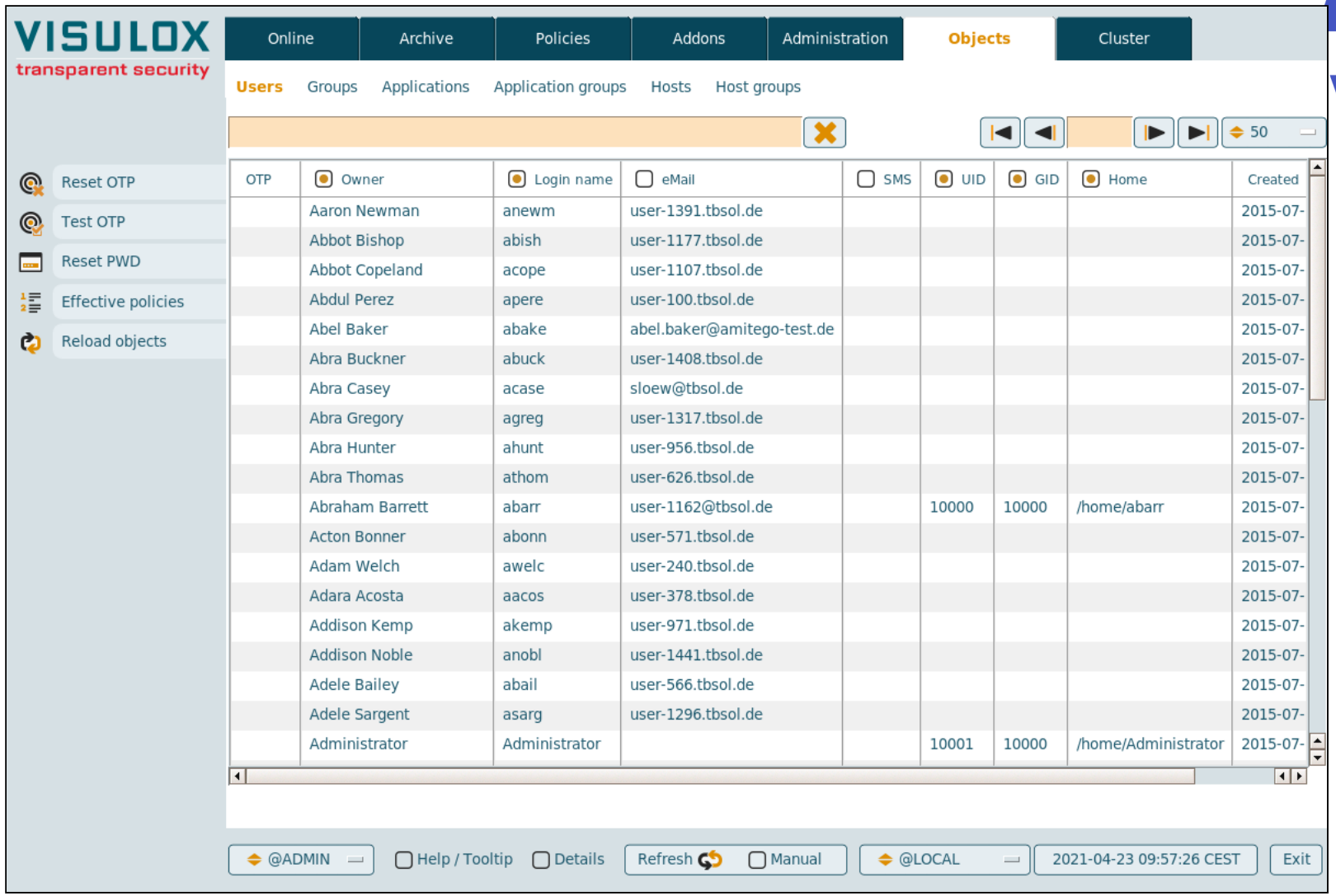
Overview

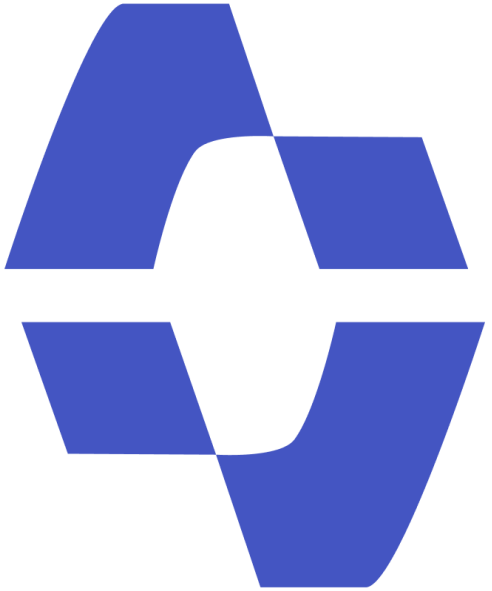
In **Cockpit / Objects** the users, groups, applications, application groups, hosts and host groups imported from datasources are displayed in a table.

In **Objects / Users**, the OTP configuration of users can be handled and passwords can be reset. The effective policies belonging to a selected user can be displayed.
It is also possible to start import from datasources manually.

In **Objects / Applications** applications can be edited or created and the host / service availability can be checked for the selected entry.



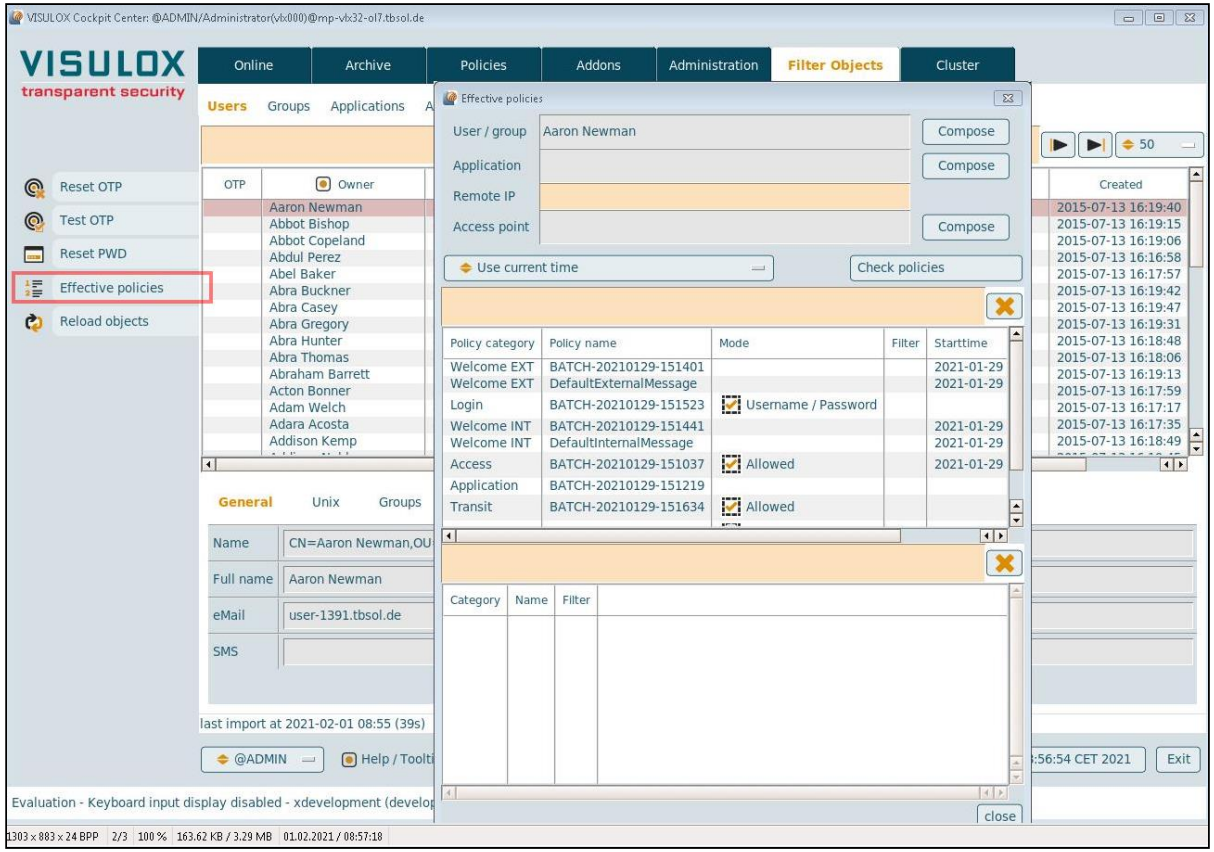

VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Objects
Cluster
Users
Groups
Applications
Application groups
Hosts
Host groups
50
Reset OTP
Test OTP
Reset PWD
Effective policies
Reload objects
OTP
Owner
Login name
eMail
SMS
UID
GID
Home
Created
Aaron Newman anewm user-1391.tbsol.de 2015-07-
Abbot Bishop abish user-1177.tbsol.de 2015-07-
Abbot Copeland acope user-1107.tbsol.de 2015-07-
Abdul Perez apere user-100.tbsol.de 2015-07-
Abel Baker abake abel.baker@amitego-test.de 2015-07-
Abra Buckner abuck user-1408.tbsol.de 2015-07-
Abra Casey acase sloew@tbsol.de 2015-07-
Abra Gregory agreg user-1317.tbsol.de 2015-07-
Abra Hunter ahunt user-956.tbsol.de 2015-07-
Abra Thomas athom user-626.tbsol.de 2015-07-
Abraham Barrett abarr user-1162@tbsol.de 10000 10000 /home/abarr 2015-07-
Acton Bonner abonn user-571.tbsol.de 2015-07-
Adam Welch awelc user-240.tbsol.de 2015-07-
Adara Acosta aacos user-378.tbsol.de 2015-07-
Addison Kemp akemp user-971.tbsol.de 2015-07-
Addison Noble anobl user-1441.tbsol.de 2015-07-
Adele Bailey abail user-566.tbsol.de 2015-07-
Adele Sargent asarg user-1296.tbsol.de 2015-07-
Administrator Administrator 10001 10000 /home/Administrator 2015-07-
@ADMIN
Help / Tooltip
Details
Refresh
Manual
@LOCAL
2021-04-23 09:57:26 CEST
Exit



Available features

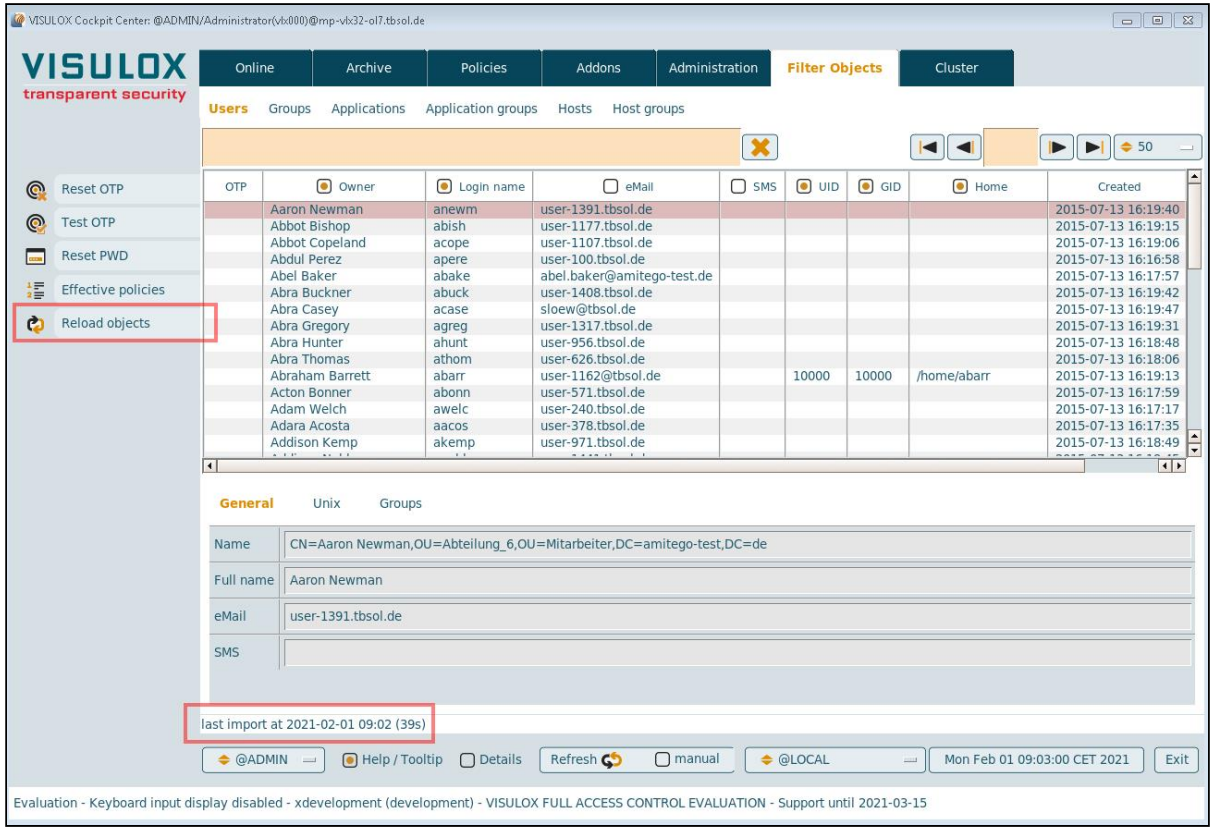
- **Reset OTP:** The OTP keys of selected users can be reset via the **Reset OTP** button.
- **Test OTP:** Test of the OTP configuration of the selected user.
- **Reset PWD:** Passwords can be reset for the selected AD / LDAP users.
  - **password.reset=true** has to be set and datastore must have an AD user with the necessary rights
  - **password.notify** can have an action script name, which will be triggered to inform the user about the new password
  - Multiple passwords can be reset at once
  - Information is copied to clipboard on request.
  - With the command **visulox pwdmgmt**,, the password status can be checked and an action script can be used, e.g. if a password expires in x days (See: How to control Password Management from the command line)
  - Multiple connected datasources are supported
- **Effective policies**

  The effective policies for an entry can be displayed:



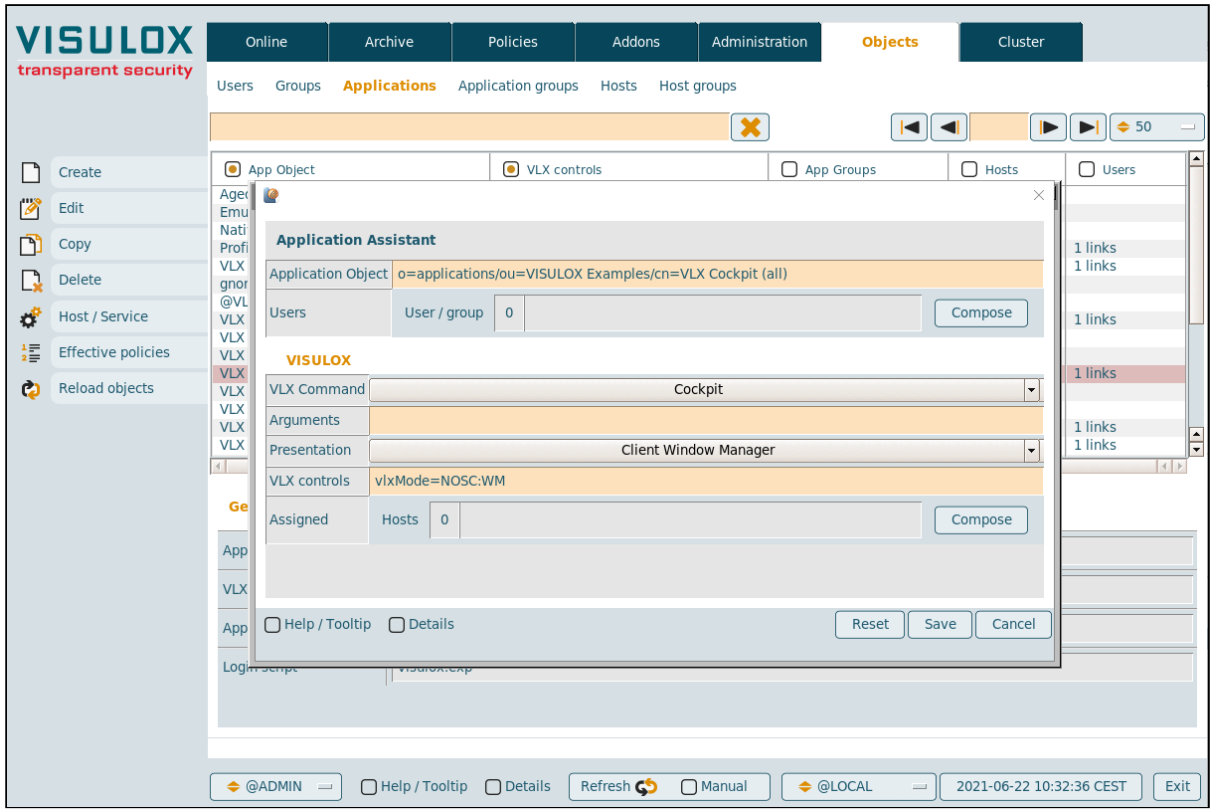
- **Reload Objects**

  Objects are imported from the connected datasources and the duration is shown:



- **Application Assistant**

  Create, edit, copy and delete commands are available for applications:



Applications can be edited or created and assigned without using the VISULOX PORTAL Console. Character applications, dynamic applications and documents are **not** available.

How to enable Password Selfservice

Password Selfservice needs a datasource configuration with pwdchange protocol enabled.

Enable Selfservice

```
/opt/visulox/setup/actionscripts/passwordSelfService.sh setup
```

This enables the "**forgot password?**" link on the login page.

An action script will be added using the following template:

```
/etc/html/templates/PasswordSelfServiceEmail.html
```

Configuration parameters after script:

```
visulox config -name password.
    ------------------------------------------------------------------------
    | changed | key                                | value               |
    ------------------------------------------------------------------------
    |         | password.lowercase.count           | 1                   |
    |         | password.max                       | 12                  |
    |         | password.min                       | 6                   |
    |         | password.notify                    |                     |
    |         | password.numbers.count             | 1                   |
    | changed | password.selfservice               | true                |
    |         | password.selfservice.linklifetime  | 5                   |
    | changed | password.selfservice.script        | passwordSelfService |
    |         | password.specials                  | !$%&/()=#-_<>|      |
    |         | password.specials.count            | 1                   |
    |         | password.uppercase.count           | 1                   |
    |         | password.warning                   | 6                   |
    ------------------------------------------------------------------------
```

How to control Password Management from the command line

- Overview
- Usage
- Example

Overview

The command line tool "**VISULOX pwdmgmt**" allows to control password management for Active Directory (AD) and Oracle Unified Directory (OUD).

Usage

The following commands are available:

Command	Description
expired	List users with an expired password
locked	List users which accounts are locked
mustchange	List users which have to change their password
neverexpires	List users which accounts never expire
notify	Notify those accounts which will expire
warn	Warn users which have to change their password

In VISULOX Cockpit, the supervisor is able to reset passwords to a rolled random password for users from a datasource with a password change protocol.
password.notify can have an action script name, which will be triggered to inform the user about the new password.

From the command line the supervisor can retirieve information about the users password states.

If the "**VLX Password SelfService**" application is assigned, the user can set a password with this Workspace application.

⚠ The AD user for the VISULOX / AD connection needs write access with the necessary rights and **password.reset** set to **true**.

ℹ If **visulox datasource edit -name <> pwdprotocol** is set to **none** and the password has to be changed, the user cannot log in and a message is displayed in the login mask, that he has to change his password.

Example

List users with an expired password

```
visulox pwdmgmt expired
looked Accounts
    ------------------------------------------------------------------
    |               vlxowner |        vlxpwdexpiretime | expired since |
    ------------------------------------------------------------------
    |           Frank Miller | 2021-10-12 10:28:43.000 |      140d 02h |
    |              John Snow | 2021-09-07 15:02:38.000 |      174d 21h |
    |                 Test12 | 2020-07-20 11:00:45.000 |      589d 01h |
    ------------------------------------------------------------------
```

Customizable action buttons in VISULOX Cockpit / Objects

A customizable action for example is selecting a user in **VISULOX Cockpit** / **Objects** / **Users** and start a shell script to reset the password of the selected user.

There are 5 buttons for which an individual script can be set. These buttons can be arranged individually on the VISULOX Cockpit / Objects pages for **users**, **groups** and **applications** (other GUI parts on request).

Each button needs four elements:

Element	Description
Place in GUI	**do-users**, **do-groups** and **do-application** can be used to place the buttons (others on request)
Text for the button	Short free text
Description	The description text is presented as the tooltip
Selection type	Flag can be **none** or **single**. If single is used, a selection in the GUI is needed and the selection content is passed to the script.

Configuration parameters in VISULOX

Configuration parameters

```
visulox config -name vlxgui.buttonscript.0="do-users:Remove:Remove user from Datasource:single"
visulox config -name vlxgui.buttonscript.1="do-users:Reset:Reset password:single"
```

Button script

A template is available: **/opt/visulox/tools/buttonscript.sh.template**

This template should be renamed to **buttonscript.sh**.

Notes on the buttonscript:

- When the button is pressed, **/opt/visulox/tools/buttonscript.sh** is called.
- The script has the VLX parameters of the selection.
- The script has the calling user data.
- The script has the button index.
- The script can have an error code and an text on stdout. This is presented to the user in the GUI.
- The script runs with "**vlx**" ID (not with transit vlx id).

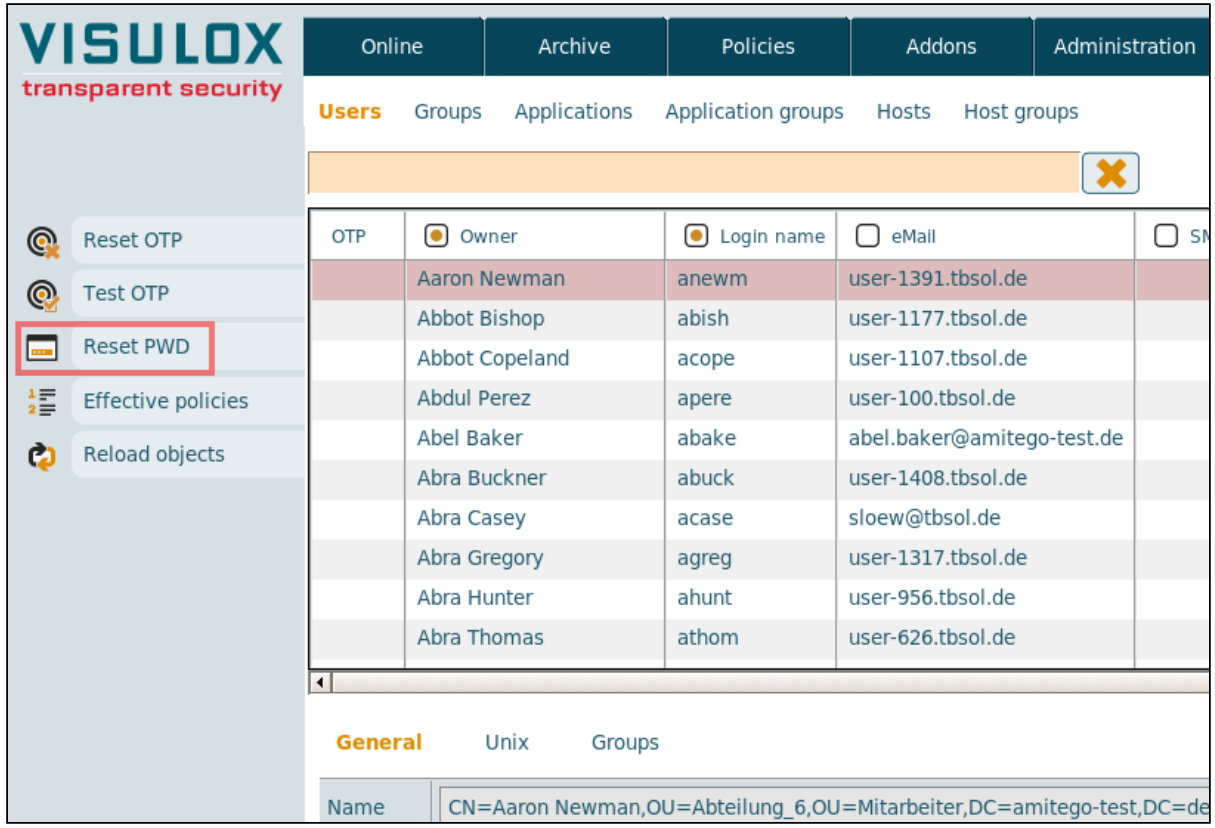
buttonscript.sh.template

```
#!/bin/bash
########################################################################
#  Copyright (c) amitego engineering GmbH, www.amitego.com
########################################################################
#
# This is the general button action script.
# With the configuration several buttonscripts can be defined within the GUI.
# All of them are calling the same script. The script has general data
# + data based on the selection.
# General data:
#   VLXSCRIPTCALLER
#   VLXSCRIPTCALLER_FMT
#   VLXSCRIPTCALLERLOGIN
#
#   VLXSCRIPTID       : The buttonscript ID from the configuration vlxgui.buttonscript.<VLXSCRIPTID>
#   VLXSCRIPTGROUP    : Groupname in the definition
#   VLXSCRIPTTEXT     : Buttontext in the definition

set -E
trap 'exit 255' ERR
exec 2>&1
```

```
debug () {
    (
    echo "--------- $(date) -------------"
    env | grep VLX
    ) >> /tmp/buttonscript.log
}
cmd0 () {
    echo "Buttonscript 0: $VLXSCRIPTTEXT"
}
cmd1 () {
    echo "Buttonscript 1: $VLXSCRIPTTEXT"
}
cmd2 () {
    echo "Buttonscript 2: $VLXSCRIPTTEXT"
}
cmd3 () {
    echo "Buttonscript 3: $VLXSCRIPTTEXT"
}
cmd4 () {
    echo "Buttonscript 4: $VLXSCRIPTTEXT"
}
#debug
cmd$VLXSCRIPTID
echo "Done"
exit 0
```

Reset / test buttons for Objects / Users

Several reset and test buttons for OTP and LDAP / AD users are available;

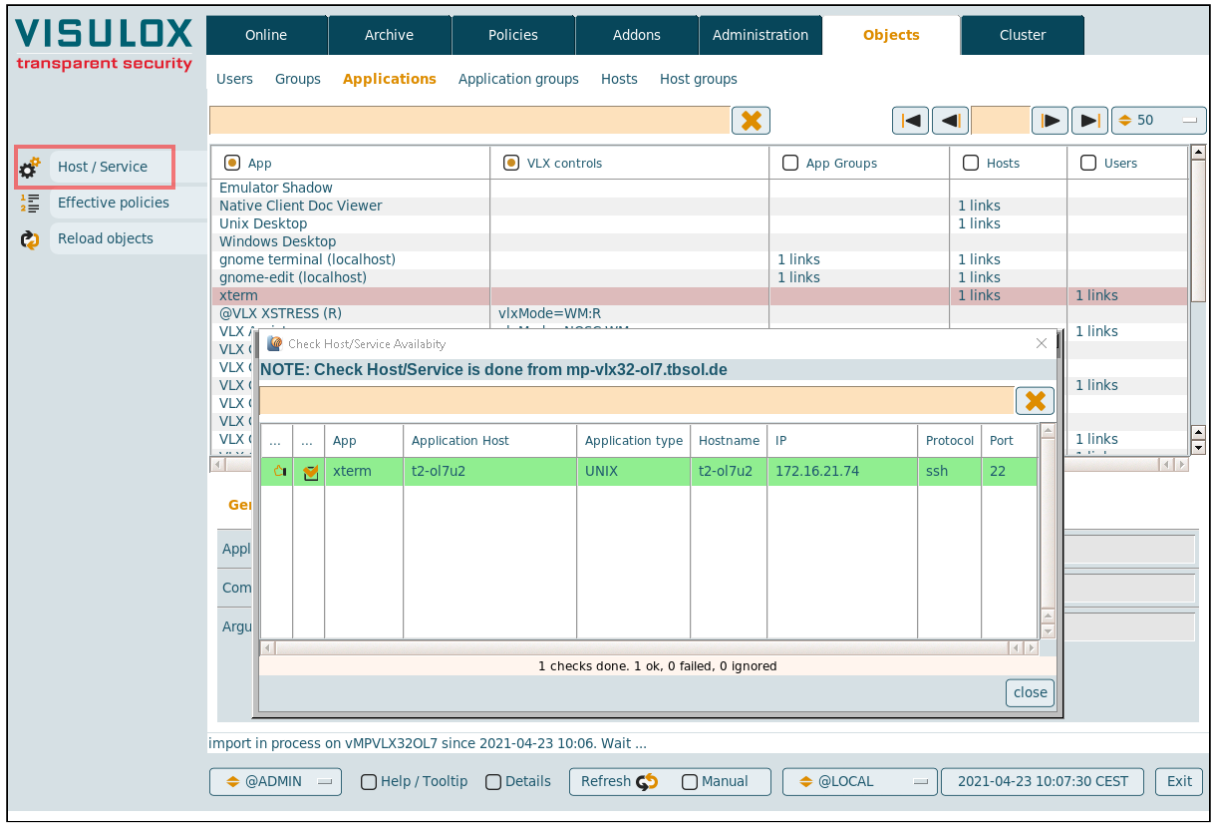


With the **Reset PWD** button it is possible to reset the password for **LDAP / Active Directory** users.

⚠ Password reset for Unix users is not possible.

Host / Service button for VISULOX Cockpit / Objects / Applications

With the **Host / Service** button in **VISULOX Cockpit / Objects / Applications** the SSH and RDP Connection to application servers can be checked:



Reload Objects button

On all Object pages a **Reload Objects** button is displayed. With this button the reload of the LDAP import can be triggered by the user.

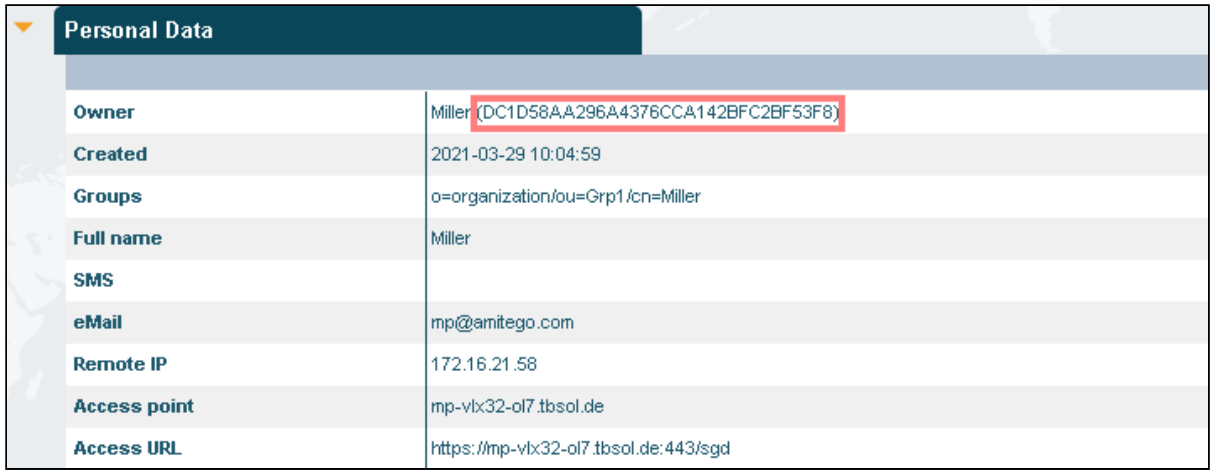
23.1.101 Object ID

Every user has an owner name and additionally an object ID, which is the hash value of the owner name.
Whenever a command is referencing the owner, it is a good idea to use the **object ID**, which has no difficulties interpreting special characters.

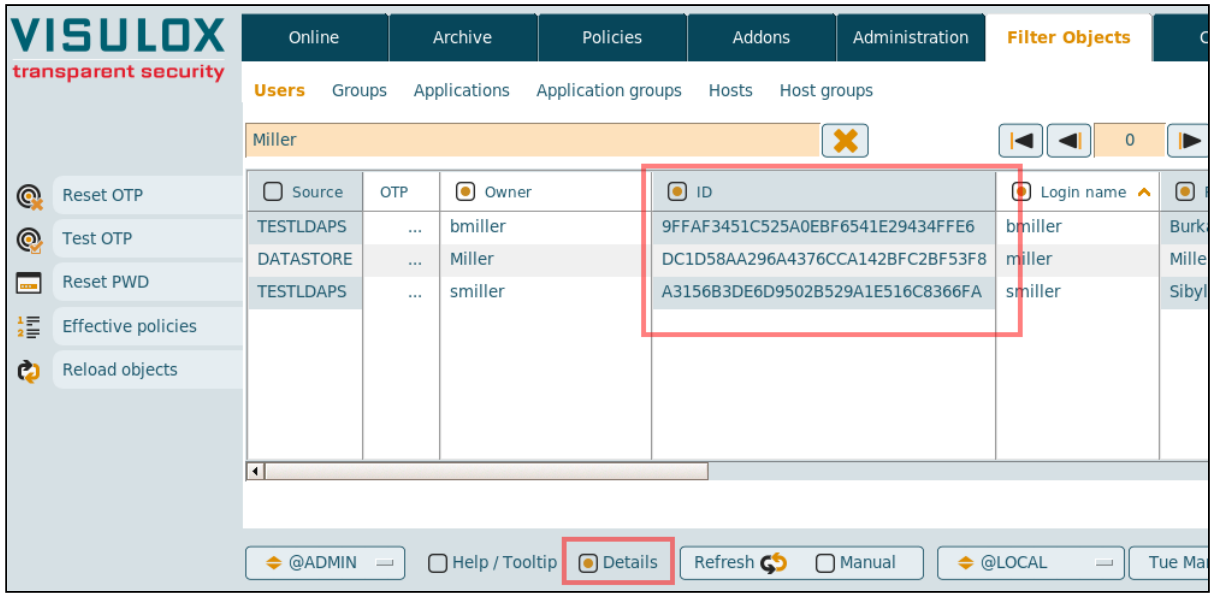
An object ID based on a hash value is available for **owner**, **application** and **application group**.

The object ID is displayed

- in the **Workspace / Personal Data** section of the user:



- in **Cockpit / Filter Objects** for administrators, e.g. object ID of the owner:



Details must be enabled to display the column with the **object ID**.

Examples, where the object ID can be used:

```
visulox policy application add -name test -object 5F7AB10DADC9EDA6EE7D2034B5545E18

visulox otp set -object 5F7AB10DADC9EDA6EE7D2034B5545E18 -otp 460136 -key Y2HLYFMPI44EDK3X

visulox passcache edit -resource Test -object 5F7AB10DADC9EDA6EE7D2034B5545E18 -resuser root -respass -

visulox admin cockpit  add -template @VIEW -object 5F7AB10DADC9EDA6EE7D2034B5545E18 -name Test

...
```

23.1.102 Setting the min/max length for messages, contents and comments

The **minimum words** and the **maximum length** (in characters) of messages, contents and comments can be set via configuration parameters.

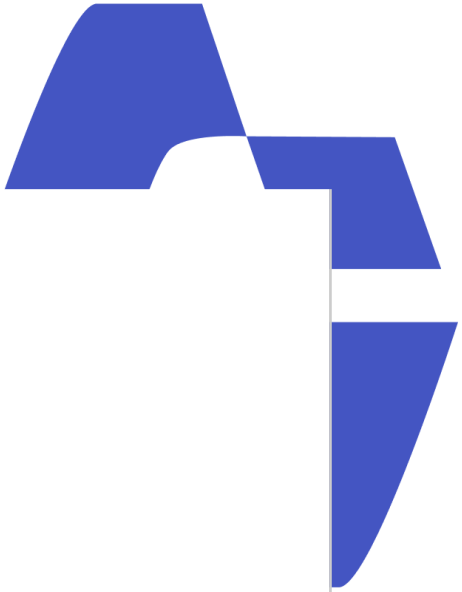
List of entries with minimum words setting

```
visulox config list -name entry.minwords

    ------------------------------------------------------------
    | changed | key                                    | value   |
    ------------------------------------------------------------
    |         | entry.minwords.access_policy           | default |
    |         | entry.minwords.annotation              | 3       |
    |         | entry.minwords.application_policy      | default |
    |         | entry.minwords.checkout                | 3       |
    |         | entry.minwords.citrixobject_form       | 0       |
    |         | entry.minwords.commandconnect          | default |
    |         | entry.minwords.commandguard            | default |
    |         | entry.minwords.default                 | 0       |
    |         | entry.minwords.external_message_policy | 1       |
    |         | entry.minwords.filetransit             | default |
    |         | entry.minwords.ftapproved              | 3       |
    |         | entry.minwords.ftreject                | 3       |
    |         | entry.minwords.host_object             | default |
    |         | entry.minwords.internal_message_policy | 1       |
    |         | entry.minwords.login_policy            | default |
    |         | entry.minwords.cockpit                 | default |
    |         | entry.minwords.message                 | 3       |
    |         | entry.minwords.region                  | default |
    |         | entry.minwords.resource                | default |
```

```
    |         | entry.minwords.script                  | default |
    |         | entry.minwords.script_object           | 1       |
    |         | entry.minwords.sessionend              | default |
    |         | entry.minwords.sessionlock             | default |
    |         | entry.minwords.spontanaccess           | 3       |
    |         | entry.minwords.textblocks              | 3       |
    |         | entry.minwords.timeprofile             | default |
    |         | entry.minwords.transit_policy          | default |
    ------------------------------------------------------------
```

List of entries with maximum length setting

```
visulox config list -name  entry.maxlength

    ------------------------------------------------------------
    | changed | key                                    | value   |
    ------------------------------------------------------------
    |         | entry.maxlength.access                 | default |
    |         | entry.maxlength.access_policy          | default |
    |         | entry.maxlength.annotation             | default |
    |         | entry.maxlength.application_policy     | default |
    |         | entry.maxlength.checkout               | default |
    |         | entry.maxlength.citrixobject_form      | 2048    |
    |         | entry.maxlength.commandconnect         | default |
    |         | entry.maxlength.commandguard           | default |
    |         | entry.maxlength.default                | 255     |
    |         | entry.maxlength.external_message_policy | default |
    |         | entry.maxlength.filetransit            | default |
    |         | entry.maxlength.ftapproved             | default |
    |         | entry.maxlength.ftreject               | default |
    |         | entry.maxlength.host_object            | default |
    |         | entry.maxlength.internal_message_policy | default |
    |         | entry.maxlength.login_policy           | default |
```



```
|         | entry.maxlength.cockpit                | default |
|         | entry.maxlength.message                | default |
|         | entry.maxlength.region                 | default |
|         | entry.maxlength.resource               | default |
|         | entry.maxlength.script                 | default |
|         | entry.maxlength.script_object          | default |
|         | entry.maxlength.sessionend             | default |
|         | entry.maxlength.sessionlock            | default |
|         | entry.maxlength.textblocks             | default |
|         | entry.maxlength.timeprofile            | default |
|         | entry.maxlength.transit_policy         | default |
-------------------------------------------------------------
```

If **default** is set, the default value will be used for the message. These default values can also be adjusted:

⚠ All configuration parameters set to **default** will also have the new values after these settings are changed.

visulox config list -name entry.minwords.default

```
-------------------------------------------
| parameter           |    type | value |
-------------------------------------------
| entry.minwords.default | OPERATION | 0    |
-------------------------------------------
```

visulox config list -name entry.maxlength.default

```
-------------------------------------------
| parameter           |    type | value |
-------------------------------------------
```

| entry.maxlength.default | OPERATION | 255 |

23.1.103 How to control action scripts from the command line

Overview

The command line tool "**VISULOX admin action**" allows to control action scripts.

- Overview
- Usage
- Action script elements (edit)
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print action scripts.
add	Add an action script.
edit	Modify fields of an action script.
delete	Remove an action script.

Command	Description
categories	Show all available action script categories
fields	List available database fields (**-raw** = enhanced output)

Action script elements (edit)

Element	Description
-name <>	Name of the action script <> (mandatory!)
-category <>	Textblock category <> (mandatory!)
-comment <>	Comment of the action script <>
-scriptfile <>	Action script from file <> (mandatory!)
-grant <>	Set granted user in database record <>

Examples

List current available action scripts

```
visulox admin action list
    ------------------------------------------------
    |                    basicname |    category |
    ------------------------------------------------
    |                    PINScript |         pin |
    |                  LoginScript |       login |
    |        Generic Access Script |      access |
    |   Generic Application Script | application |
    |         Generic NotifyScript |           * |
    | Generic Transit Notification | transitzone |
    |                         Dump |           * |
    ------------------------------------------------
```

Add new action script

```
visulox admin action add -name Test -category login -scriptfile testfile
```

Edit action script

```
visulox admin action edit -name Test -comment "Using test script testfile"
```

Display available categories

```
visulox admin action categories
login,access,application,pin,transitzone,commandconnect,report,*
```

Remove an entry
`visulox admin action delete -name Test`

23.1.104 How to control reports from the command line

Overview

The command line tool "**VISULOX report**" allows to control all kind of reports.

- Overview
- Usage
  - Available predefined queries
  - Extended report with vendor and project field
    - Example for user naming
    - Deliverable
    - Adjusting naming convention
- Examples
- Related information

Usage

The following subcommands are available:

Command	Description
-help	Prints a help on report (useful for creating own reports) [1]
-list	List available predefined reports

Command	Description
-title <>	Title of the report
-mctitle <>	messagecat title
-name <>	Name of the report, **default:** <report>
-type <>	Type of the report pdf / csv / json / xml / html, **default:** <csv>
-xslt <>	xslt filename for pdf <>
-metadata <>	metaData for xml
-query <>	Name of query or path to queryfile
-tframe <>	TFRAME() in SQL will be substituted. Use **-tframe HELP** [2]
-from <>	Starttime instead of tframe (dd/mm/yyyy)
-to <>	Endtime instead of tframe (dd/mm/yyyy)
-sql <>	SQL statement of the report
-lang <>	Language for the report, **default:** <en>, in case of a strange output, try: "-lang -"

Command	Description
-filename <>	Timefile to store the result
-mailto <>	Send email
-mailsubject <>	Subject of the mail, **default:** <VISULOX REPORT>
-maildescription <>	Mail description
-maildescriptionfile <>	Mail description file
-archive <>	Use database on archive node
-dry	Show SQL only

[1] Using visulox report help

With **help** the report tables and the tframe options are displayed.

Using **help -table** <table name> lists the available columns of a table for report queries

For example: **Table: Sessions**

Columns	Format	Description
sessions.chaptercounter	INTEGER	Number of chapters
sessions.chaptersize	INTEGER	Total size of all chapters

Columns	Format	Description
sessions.chaptertype	TEXT	Type of the chapter
sessions.snapshotcounter	INTEGER	Number of snapshots
sessions.vlx_create_timems	INTEGER	Create time of the session in milliseconds
sessions.vlx_created_by	TEXT	Created by
sessions.vlx_expiration_time	INTEGER	Session expiration time in seconds
sessions.vlx_update_timems	INTEGER	Update time in milliseconds
sessions.vlx_updated_by	TEXT	Updated by
sessions.vlxaccesspoint	TEXT	URL of the access point
sessions.vlxapplication	TEXT	Application object
sessions.vlxapplicationarguments	TEXT	Parameter for the application
sessions.vlxapplicationcommand	TEXT	Command of the application
sessions.vlxapplicationhost	TEXT	Host, where the application was started

Columns	Format	Description
sessions.vlxapplicationuser	TEXT	User of the application
sessions.vlxclientip	TEXT	Client IP
sessions.vlxlisthash	TEXT	Hash value
sessions.vlxloginscript	TEXT	Login script
sessions.vlxowner	TEXT	Owner of the session
sessions.vlxpolicy	TEXT	Applied Policy
sessions.vlxremoteip	TEXT	Remote IP
sessions.vlxsessionendtime	INTEGER	End time of the session in seconds
sessions.vlxsessionid	TEXT	VISULOX Session ID
sessions.vlxsessionstarttime	INTEGER	Start time of the session in seconds
sessions.vlxsessiontype	TEXT	Type of the session
sessions.vlxticketid	TEXT	Ticket ID from an incident management system

Columns	Format	Description
sessions.vlxvalidationdata	TEXT	Validation data

[2] More tframe options

```
tframe is a timeframe and presets -from and -to,
based on the value provided to -tframe
The value can be
current: CURRDAY | CURRWEEK | CURRMONTH
CURRQUARTER | CURRHALFYEAR | CURRYEAR

last: LASTDAY | LASTWEEK | CURRMONTH
LASTQUARTER | LASTHALFYEAR| LASTYEAR

next to last: NEXT2LASTDAY | NEXT2LASTWEEK | NEXT2LASTMONTH
NEXT2LASTQUARTER | NEXT2LASTHALFYEAR| NEXT2LASTYEAR

absolute: W<week number>
M<month number>
Q<quarter>
<year>
- year suffix: <year>W<week number>
<year>M<month number>
<year>Q<quarter>

examples: -tframe CURRQUARTER | -tframe 2019W10 | -tframe 2018
```

⚠ If a limit is used inside the SQL query **-force** has to be added to the command to bypass an SQL limit error.

Available predefined queries

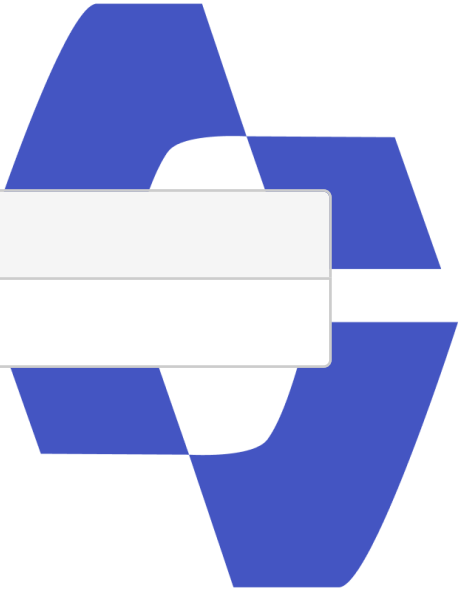
```
visulox report list

List of available reports in
   averageFiletransferPerMonth : /visulox/etc/reports/averageFiletransferPerMonth.rpt
                  averageFilm : /visulox/etc/reports/averageFilm.rpt
          averageFilmPerMonth : /visulox/etc/reports/averageFilmPerMonth.rpt
   averageStorageUsagePerMonth : /visulox/etc/reports/averageStorageUsagePerMonth.rpt
           examplePlaceholder : /visulox/etc/reports/examplePlaceholder.rpt
                inactiveUsers : /visulox/etc/reports/inactiveUsers.rpt
                listUserGroup : /visulox/etc/reports/listUserGroup.rpt
                 loginFailure : /visulox/etc/reports/loginFailure.rpt
                    session30 : /visulox/etc/reports/session30.rpt
          session30TimeFormat : /visulox/etc/reports/session30TimeFormat.rpt
                    top25User : /visulox/etc/reports/top25User.rpt
               topApplication : /visulox/etc/reports/topApplication.rpt
                totalFilmSize : /visulox/etc/reports/totalFilmSize.rpt
           unusedApplications : /visulox/etc/reports/unusedApplications.rpt
```

⚠ Keep in mind, that the information is always based on the provided lifetimes.

Depending on the lifetime (30/60/90/etc days) the session information is deleted. If a report of the application usage or of the users is needed to clean up the datastore / LDAP, the set lifetimes mostly are too low.

A report based on "LASTYEAR" is not possible because the information is not available.

Therefore the variable "**sgdusage**" has been implemented, for which an additional lifetime can be set:



Setting the lifetime for sgdusage

```
visulox config -name lifetime.sgdusage=365
```

This lifetime is set for:

- loginResultRejected
- webtopSessionStartedDetails
- sessionStartedDetails

Placeholder

It is possible to use placeholders via command line in the SQL statements e.g. SELECT ... WHERE ... columname='%P1%' ...

The placeholder has the format "key=value", where key can be any alpnumerical string. If value has a space, the value must be quoted, e.g. NAME="surname name".

Usage:

```
visulox report -query <name> P1=abc P2=ext
```

Extended report with vendor and project field

If a user repository has no vendor field, it is still possible to generate reports based on such a vendor field.

The vendor can be extracted from the distinguished name in the datastore profile or from the distinguished name in the Active Directory.

Example for user naming

There are two naming conventions:

```
cn=user,ou=procjet,ou=vendor,......
... ou=vendor/ou=project/cn=user
```

Deliverable

The vendor is extracted from the username (vlxowner) during user import into "**vlxvendor**". The vendor field is listed in the VISULOX Cockpit.

This vendor field cannot be in the audit data (session or event) information. Therefore an extended database function is provided to list the vendor and/or project out of vlxowner during database querries.

Example report with vendor and project

```
SELECT  vlxsessionid, (vlxeventtimems/1000) as vlxeventstamp, vlxevent, vlxpolicy, vlxowner, getUnit(vlxowner,1) as project,
getUnit(vlxowner,2) as customer, vlxticketid, vlxvalidationdata
FROM    events
WHERE   %TFRAME(vlxeventtimems)% and vlxevent in ('2faPinAccepted','2faPinRejected')
```

Adjusting naming convention

If necessary it is possible to adjust the naming convention in VISULOX with the following parameters:

```
visulox config -name importer.map
    ----------------------------------------
    | changed | key                  | value |
    ----------------------------------------
    |         | importer.map.project | 0     |
    |         | importer.map.vendor  | 0     |
    ----------------------------------------
```

Examples

List unused applications of the current month

```
visulox report -query unusedApplications -tframe CURRMONTH -raw -format json
```

The report "unused applications" shows all applications, that have not been used in the last 14 days.

List most used application of the current year

```
visulox report -query topApplication -tframe CURRYEAR -raw
```

List all login failures of the last week

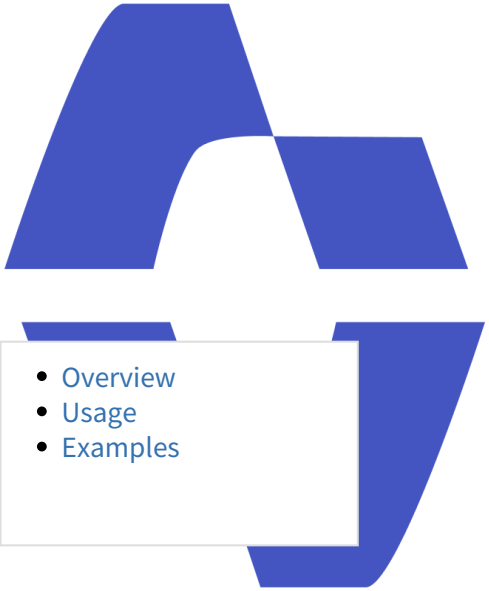
```
visulox report -query loginFailure -tframe LASTWEEK -raw
```

```
visulox report -query top25User -lang - -tframe CURRMONTH -force
```

In this example "**-lang -**" has to be used for a better output and "**-force**" to bypass an SQL limit error.

Related information

Useful database queries: Size of film chapters, snapshots, files, usage



23.1.105 How to control regions from the command line

Overview

The command line tool "**VISULOX admin region**" allows to control regions.

- Overview
- Usage
- Examples

Usage

The following subcommands are available:

Command	Description
list	List and print regions.
delete	Delete a region.
fields	List available database fields (**-raw** = enhanced output)

Examples

List current available regions

```
visulox admin region list
    ------------------------------------------
    |        basicname |              timezone |
    ------------------------------------------
    |           @LOCAL |        :Europe/Berlin |
    |        Argentina | :America/Buenos_Aires |
    |           Brazil |          :Brazil/West |
    |           France |         :Europe/Paris |
    |          Germany |        :Europe/Berlin |
    |        Guatemala |    :America/Guatemala |
    |         Portugal |        :Europe/Lisbon |
    |            Spain |        :Europe/Madrid |
    |      Switzerland |        :Europe/Zurich |
    |   United Kingdom |        :Europe/London |
    | USA / California |  :America/Los_Angeles |
    ------------------------------------------
```

Display available fields

```
visulox admin region fields
```

Display selected fields

```
visulox admin region list -fields basicname,timezone,comment
```

Remove an entry

```
visulox admin region delete -name France
```

23.1.106 Time zones, holidays and time profiles

Time zones

Each VISULOX installation has different time zone aspects.

- The time zone of the users
- The time zone of the access plattform (VISULOX)
- The time zone of the applications

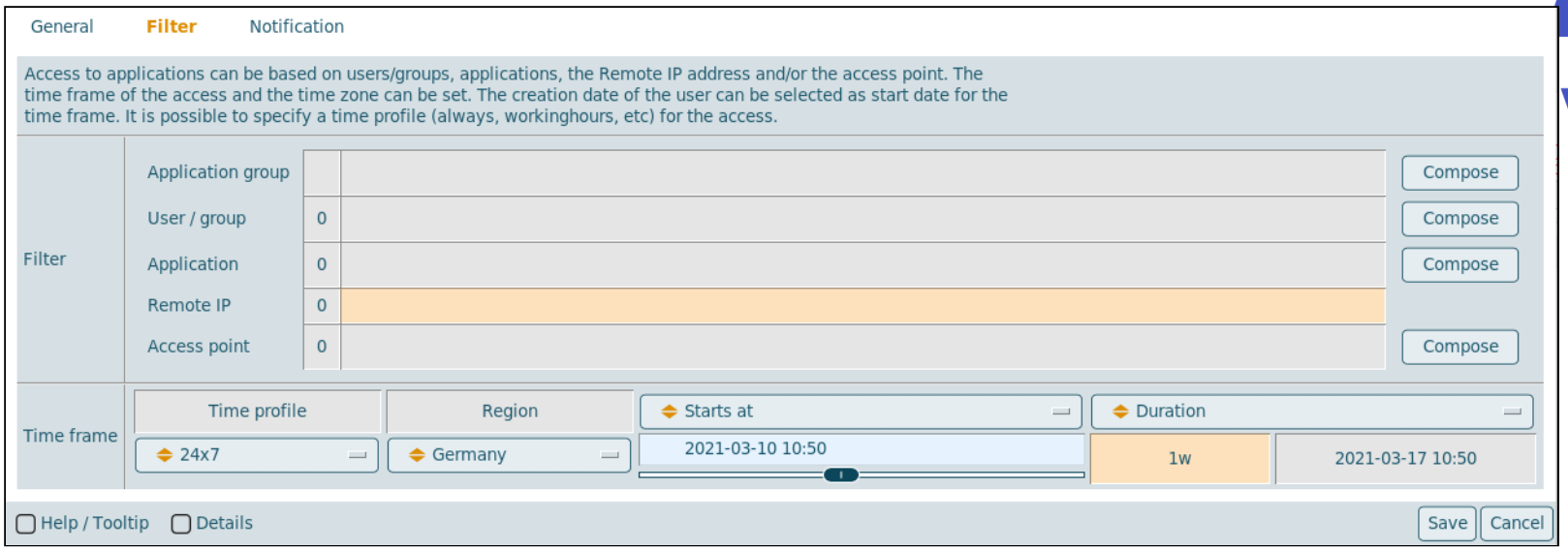
VISULOX handles everything in UTC internally.

The VISULOX Cockpit has the ability to select a time zone. This allows the user to see, what a presented time would be in that selected time zone.

The important part is the access control of a user through VISULOX to an application.

User	VISULOX	Application
	Access control	Application control • Recorded • Dual Control • Keyboard control
	Starttime - endtime Time profile	Time zone
User1 / TZ(1)	VLX1 / TZ(a)	Appl1 / TZ(α)
User2 / TZ(2)		Appl2 / TZ(β)
User3 / TZ(3)	VLX2 / TZ(b)	Appl3 /TZ(γ)
User4 / TZ(4)		Appl4 / TZ(δ)

VISULOX Access Control defines when a user has access to an application. The time zone view is the access platform, this means the time zone of VISULOX.

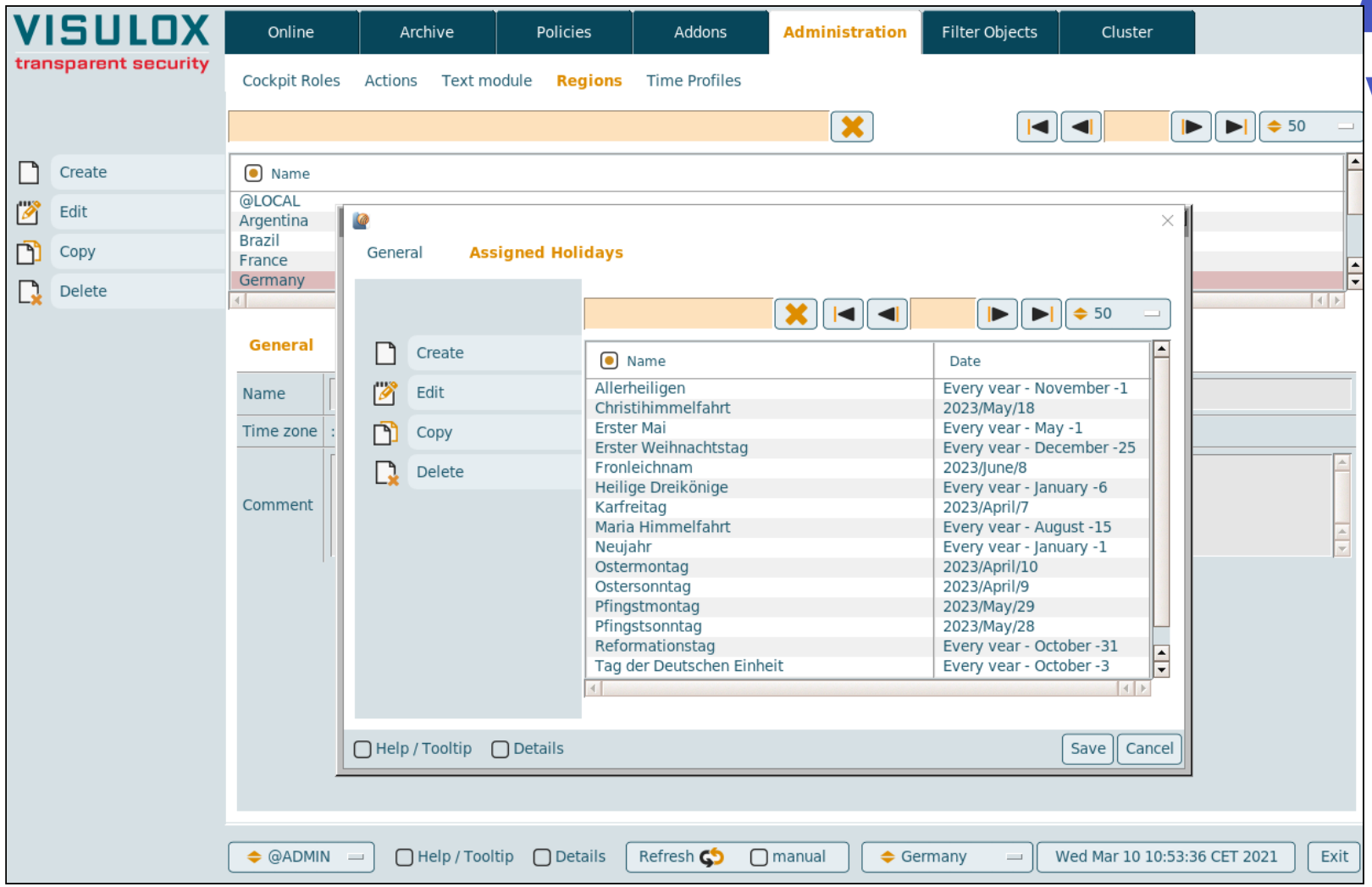


To control the access to the application based in the profile, the access control system must know in what time zone the application is.

If the time zone is set for the application starttime, endtime and time profiles are checked against this alternate time zone.

Holidays

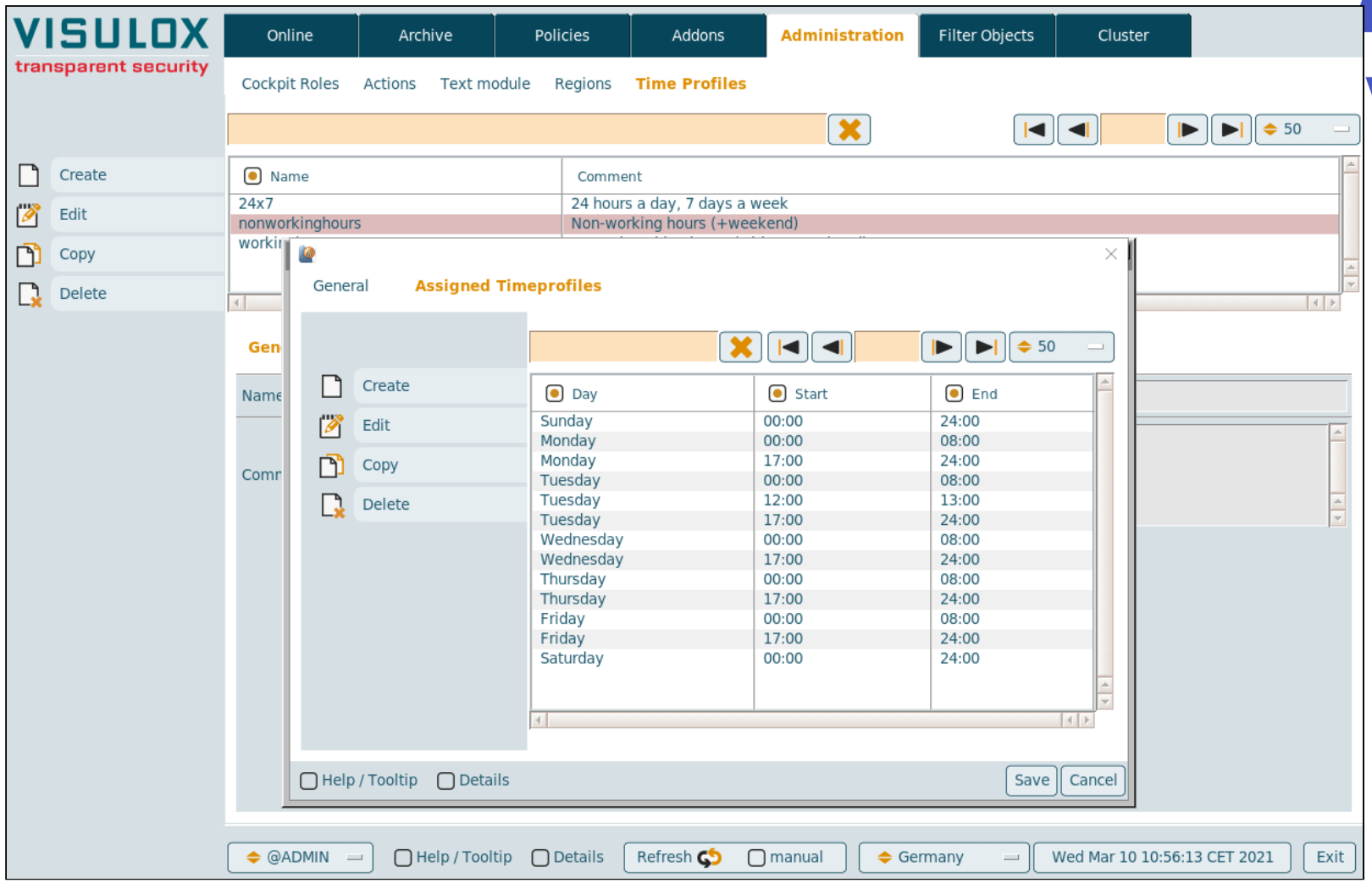
In **VISULOX Cockpit / Administration/ Regions** the available regions are displayed with their predefined holidays:


VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
Cluster
Cockpit Roles
Actions
Text module
Regions
Time Profiles
Create
Edit
Copy
Delete
Name
@LOCAL
Argentina
Brazil
France
Germany
General
Assigned Holidays
Name
Time zone
Comment
Date
Allerheiligen Every vear - November -1
Christihimmelfahrt 2023/May/18
Erster Mai Every vear - May -1
Erster Weihnachtstag Every vear - December -25
Fronleichnam 2023/June/8
Heilige Dreikönige Every vear - January -6
Karfreitag 2023/April/7
Maria Himmelfahrt Every vear - August -15
Neujahr Every vear - January -1
Ostermontag 2023/April/10
Ostersonntag 2023/April/9
Pfingstmontag 2023/May/29
Pfingstsonntag 2023/May/28
Reformationstag Every vear - October -31
Tag der Deutschen Einheit Every vear - October -3
Help / Tooltip
Details
Save
Cancel
@ADMIN
Refresh
manual
Germany
Wed Mar 10 10:53:36 CET 2021
Exit

A new region and holidays can be created or existing entries can be adjusted.

Time profiles

New time profiles can be created in **VISULOX Cockpit / Administration / Time Profiles**:


VISULOX
transparent security
Online
Archive
Policies
Addons
Administration
Filter Objects
Cluster
Cockpit Roles
Actions
Text module
Regions
Time Profiles
50
Create
Edit
Copy
Delete
Name
Comment
24x7
24 hours a day, 7 days a week
nonworkinghours
Non-working hours (+weekend)
General
Assigned Timeprofiles
Day
Start
End
Sunday 00:00 24:00
Monday 00:00 08:00
Monday 17:00 24:00
Tuesday 00:00 08:00
Tuesday 12:00 13:00
Tuesday 17:00 24:00
Wednesday 00:00 08:00
Wednesday 17:00 24:00
Thursday 00:00 08:00
Thursday 17:00 24:00
Friday 00:00 08:00
Friday 17:00 24:00
Saturday 00:00 24:00
Help / Tooltip
Details
Save
Cancel
@ADMIN
Help / Tooltip
Details
Refresh
manual
Germany
Wed Mar 10 10:56:13 CET 2021
Exit

Existing default profiles are:

- **24x7:** 24 hours a day, 7 days a week
- **workinghours:** Normal working hours (without weekend)
- **nonworkinghours:** (+weekend)

23.1.107 How to control timeprofiles from the command line

- Overview
- Usage
- Examples

Overview

The command line tool "**VISULOX admin timeprofile**" allows to control timeprofiles.

Usage

The following subcommands are available:

Command	Description
list	List and print timeprofiles.
delete	Delete a timeprofile.
fields	List available database fields (**-raw** = enhanced output)

Examples

List current available timeprofiles

```
visulox admin timeprofile list
    -------------------
    |       basicname |
    -------------------
    |            24x7 |
    |    workinghours |
    | nonworkinghours |
    -------------------
```

Display available fields

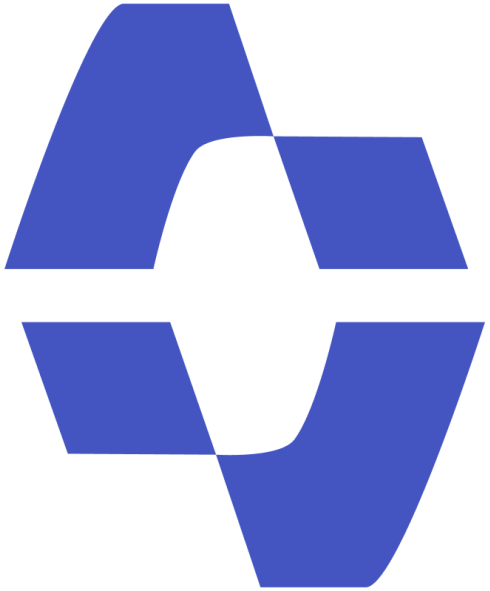
```
visulox admin timeprofile fields
```

Display selected fields

```
visulox admin timeprofile list -fields basicname,comment
```

Remove an entry

```
visulox admin timeprofile delete -name nonworkinghours
```



23.1.108 VISULOX Certificates

VISULOX uses certificates for https services with the following modules:

- fx4
- transit
- webservice

SSL Certifcate handling for transit / webservice

During installation selfsigned ceritfcates are created for transit and webservice. The VISULOX PORTAL Certificates are no longer used.

These certificates

- are valid for 10 years
- are checked by integrity check
- have to be exchanged with already existing certificates
  -- copy existing certificates to: /opt/visulox/etc/ssl/
  -- use visulox config -name fileexchange.certfile=/keyfile/caFile to use the certificate
  -- use visulox config -name fx4.certfile=/keyfile/caFile to use the certificate
  -- use visulox config -name webservice.certfile=/keyfile/caFile to use the certificate

On VISULOX Nodes or if it is necessary to use other certificates on VISULOX Access Nodes, the keyfiles can be adjusted:

```
visulox config list -name keyfile
    ------------------------------------------------------
    | changed | key                  | value            |
    ------------------------------------------------------
    |         | fileexchange.keyfile | visulox.self.key |
    |         | fx4.keyfile          | visulox.self.key |
    |         | webservice.keyfile   | visulox.self.key |
```

```
    ------------------------------------------------------
```

The ports can be adjusted here:

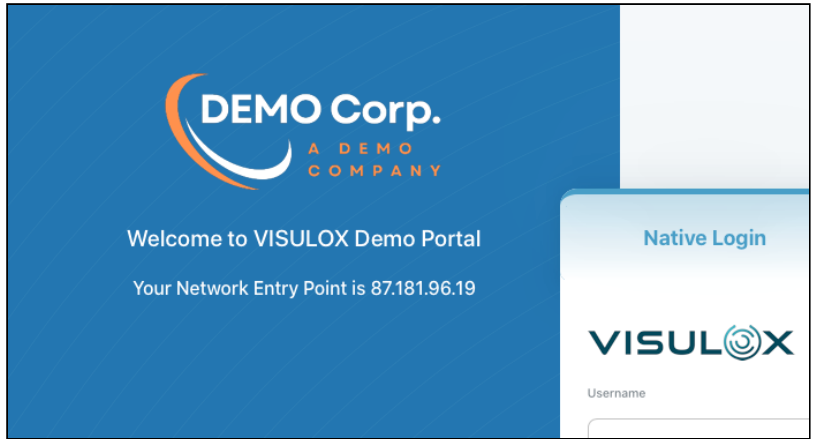
```
visulox config list -name webservice.port,fx4.port,fileexchange.port

    ------------------------------------------------------
    | changed | key                              | value |
    ------------------------------------------------------
    |         | fileexchange.port                |       |
    |         | fx4.port                         |       |
    |         | webservice.port                  | 8114  |
    ------------------------------------------------------
```

The keyfiles and the ports are global settings. To change these settings only on a single node, **/opt/visulox/etc/service.conf** has to be used.

23.1.109 How to change the license name / banner

There are three elements on the VISULOX login page header:

- The customer logo
- The banner
- The connection line



Banner and connection line can be fully configured. Cluster and node related.

The license name / banner configuration can be changed with the following command for a node:

```
visulox config -name .banner


-----------------------------------------------------------------------------------------------------------------------------------
    | parameter                   |      type |
value                                                                                                                  ... |

-----------------------------------------------------------------------------------------------------------------------------------
    | fileexchange.banner         |     SETUP |
%LICENSE%                                                                                                              ... |
    | ftpd.banner                 | OPERATION | VISULOX FTP Server: to login with username/pin. You will find your pin in your
T ... |
```

```
    | layout.vMPOL6U3DEVEL.banner |     SETUP
|                                                                                            ... |
    | portal.banner                |     SETUP |
%LICENSE%                                                                                  ... |

-----------------------------------------------------------------------------------------------------------------------------------

visulox config -name .connection

    ---------------------------------------------------------------------------
    | parameter                        |  type | value                       |
    ---------------------------------------------------------------------------
    | fileexchange.connection          | SETUP | From %RIP% on %NODE% (%HOST%) |
    | layout.vMPOL6U3DEVEL.connection  | SETUP |                             |
    | portal.connection                | SETUP | From %RIP% on %NODE% (%HOST%) |
    ---------------------------------------------------------------------------
```

The node related texts are concatenated to the cluster wide parameters.

Example: Changing the portal.banner name

```
visulox config -name portal.banner="VLX Demo System"
```

⚠ Configuration parameters set while the node is **offline** will only be applied to the local VISULOX Node.
If a parameter should be changed for the whole VISULOX Cluster, the parameter has to be set again once the node is **online** again.

Available placeholders:

Variable	Description
%SYSTEMID%	Unique system ID
%LICENSE%	License name
%CUSTOMER%	Name of the customer
%OWNER% (Filexchange only)	Name of the owner
%OWNERSHORT% (Filexchange only)	Short name of the owner
%FULLNAME% (Filexchange only)	Full name of the owner
%HOST%	Hostname
%HOSTSHORT%	Short name of the host
%NODE%	Logical name of the node
%RIP%	Remote IP address
...	...

For individually customized login pages based on different access URLs, see: Access Branding

23.1.110 How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

In installations with Load Balancer and multiple VISULOX GATEWAYS, the Load Balancer is probing the vitality of the VISULOX GATEWAYS by accessing port 443.

During maintenance the VISULOX GATEWAY could have 443, but should be removed from the load balancing policy.

Therefore an extra probing is needed with a special response from the VISULOX GATEWAYS: VISULOX GATEWAY can be used for production (ON), VISULOX GATEWAY from probing (OFF).

After setup of the VISULOX Gateway, the load balancer probing template file is available.

This article explains how to configure special answer pages on the VISULOX GATEWAY

Create feedback page

```
echo "<html><head> </head><body> Gateway is on </head></html>" > /opt/SUNWsgdg/httpd/httpd-default/htdocs/lb_endpoint.html
```

Add extra webserver in /opt/SUNWsgdg/httpd/httpd-default/conf/extra/gateway/http-gateway.conf

```
ProxyPass /lb_endpoint.html !
```

Restart VISULOX GATEWAY webserver

Restart Apache in VISULOX GATEWAY

```
GWPATH=/opt/SUNWsgdg
APACHEPATH=$GWPATH/httpd/httpd-$(cat /opt/SUNWsgdg/var/info/apacheversion)
$APACHEPATH/bin/apachectl -k restart -d $APACHEPATH -D SSL
```

Testing from Load Balancer

URL to check availability of feedback name from the Load Balancer

https://<gateway/lb_endpoint.html

To disable the VISULOX GATEWAY rename lb_endpoint.html to OFF-lb_endpoint.html.

The feedback name can be any name which is found in the documentroot.
If the feedback name is not available (because of renaming), the client, which is the Load Balancer gets as the error code 404. This has to tell the Load Balancer to remove this VISULOX GATEWAY temporarily until the name is available again.

23.1.111 VISULOX Portal maintenance mode

VISULOX Gateway probes all VISULOX Portal Servers.

If one of these servers is not responding (stopped, Tomcat not working as expected, etc) or the VISULOX Portal is in maintenance mode, requests are handled by the remaining VISULOX Portals.

If **no** VISULOX Portal Server is availabe, the maintenance page is presented to the user.

```
visulox portal mode -all -set off -note "Maintenance mode enabled ..."
```

Available parameters

Parameter	Description
-all	Set mode on all Servers
-set <*value*>	Portal mode accepting, on, maintenance, off
-server <*value*>	Server or node of VISULOX PORTAL to manage
-note <*value*>	Message on maintenance page

```
visulox portal mode
    ----------------------------------------
    |   Node |  VISULOX Portal |     state |
    ----------------------------------------
    | vMPOL8 | mp-ol8.tbsol.de | accepting |
    ----------------------------------------
Offline/Maintance note:
  VISULOX Portal is in maintenance mode. Please retry later
```

This allows to disable acceptance of one or all VISULOX Portal Nodes.

If all nodes are in **maintenance** state, the VISULOX Gateway displays the maintenance page.

There is a default maintenance page on the VISULOX Gateways.

The displayed maintenance HTML page can be found here: `/opt/visulox/etc/html/templates/maintenance.html`

To get a maintenance design run (on each server):

```
visulox-gateway design
```

Use the following command:

```
visulox portal mode -set off -all -note "Text info Page"
```

Then get the design with:

```
visulox-gateway design
```

The text "**Text info Page**" is seen by the user.

23.1.112 Whats new

VISULOX Release 4.3.3 (October 2026)

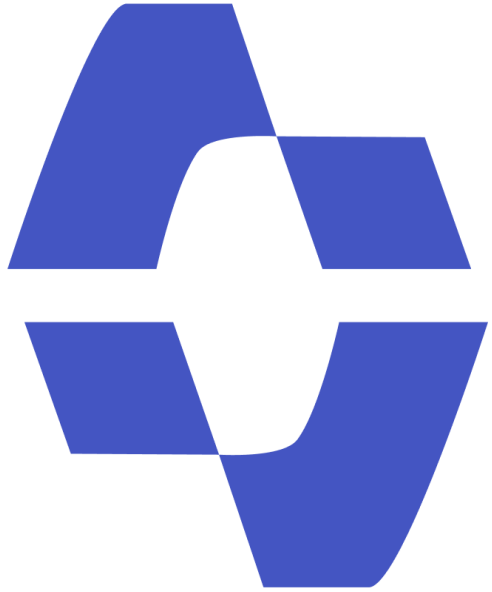
- Intel applications no longer supported on macOS 28
- rsync issues solved, update possible again
- SEC: Apache updated to version 2.4.69
- SEC: Tomcat updated to version 9.0.122
- SEC: Information disclosure improved
- All enhancements and fixes of previous released hotfixes are included.

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task, VSLX = New VISULOX Devolpment Task

VISULOX Release 4.3.2 (January 2026)

- SEC: Apache updated to version 2.4.66
- SEC: Tomcat updated to version 9.0.112



- SEC: Added missing HTTP Headers (VSLX-146)
- REDACT feature for Command Connect output (VSLX-101)
- ENH: SSH-Agent implemented into Command Connect and File Transfer client (VSLX-142)
- ENH: Command Connect / FT Client host URIs for CyberArk (VSLX-143)
- ENH: Enforced Workspace disconnect (applications suspended) after a configured time (VSLX-159)
- ENH: Enforced application session disconnect after a configured time (VSLX-159)
- ENH: Mod evasiv for gateway (VSLX-190)
- ENH: Display of upload/download size in Transit Zone (VSLX-170)
- ENH: Changed password view on hover to on click (VSLX-183)
- FIX: SCX Validation Info (VSLX-128)
- FIX: Updated Hyperscan packages for Red Hat 9 / Oracle Linux 9 (VSLX-171)
- FIX: Updated mesa packages for Red Hat 9 / Oracle Linux 9 (VSLX-172)
- FIX: vlxjwm.tcl: JWM warning: bad color (VSLX-190)
- FIX: New updated React-dom library version 19.2.0 (VS-1928)
- All enhancements and fixes of previous released hotfixes are included.

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task, VSLX = New VISULOX Devolpment Task

VISULOX Release 4.3.1 (August 2025)

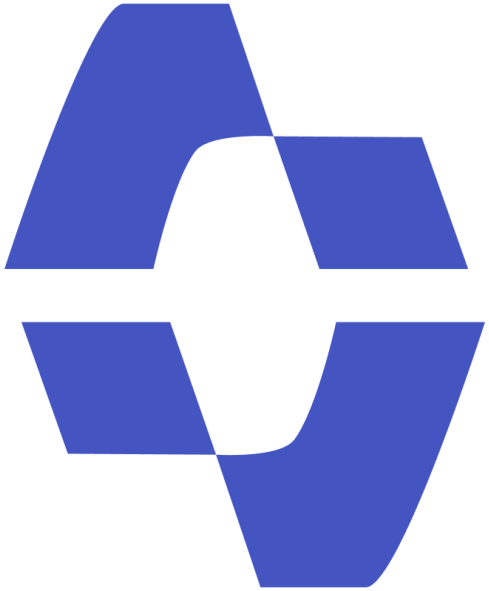
- SEC: Apache updated to version 2.4.64
- SEC: Tomcat updated to version 9.0.107
- FIX: Integrity X11 Check only on VISULOX Portal Servers (VSLX-110)
- All enhancements and fixes of previous released hotfixes are included.

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task, VSLX = New VISULOX Devolpment Task

VISULOX Release 4.3.0 (May 2025)

- SEC: Apache updated to version 2.4.63



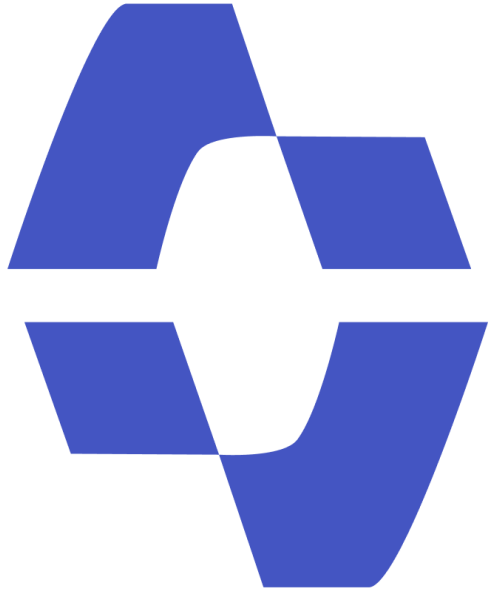
- SEC: Tomcat updated to version 9.0.104
- ENH: Entra/3rdParty integration (VSLX-7)
- ENH: Improved landing page configuration (VSLX-39)
- ENH: Transit file hash displayed in event stream (VSLX-34)
- ENH: Added VISULOX accesspoint edit color (VSLX-47)
- ENH: Added VISULOX accesspoint logo (VSLX-50)
- ENH: Printing on Oracle Linux 9 (VD-2429)
- ENH: Added SELinux context to /opt/visulox/var/log (VD-2490)
- ENH: Added the application description to VISULOX Cockpit (VD-2501)
- ENH: Send access request info about approved access to all available approvers (VD-2505)
- FIX: Session transfer (VSLX-46)
- FIX: MFAToken WAIT status disappears from Cockpit session view (VSLX-55)
- FIX: ttagw not among existing services (VSLX-61)
- FIX: Cockpit Archive database timeout (VSLX-63)
- FIX: Mailinggroups with direct user assignment (VSLX-64)
- FIX: VISULOX Portal Service - PID Files - Permissions (VSLX-67)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task, VSLX = New VISULOX Devolpment Task

VISULOX Release 4.2.0 (November 2024)

- SEC: Tomcat updated to version 9.0.90
- SEC: JK Connector updated to version 1.2.50
- ENH: New end2end / VLX Monitoring (VD-2022)
- ENH: Microsoft Entra authentication supported (VD-2425)
- ENH: Printing on OL9 supported (VD-2429)
- ENH: Authentication for local users via PAM (VD-2430)
- ENH: Variable %%TTA_UserSecurityEquivalent%% replaces the user for freerdp (VD-2464)
- FIX: Updated versions of several Javascript files (VD-2188)
- FIX: Window Management with VISULOX Cockpit on MAC (VD-2254)
- FIX: Accesspoint expected boolean value (VD-2474)



- FIX: x11forwarding tunnel not used (VD-2481)
- FIX: Sessioncache permissions (VD-2483)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 4.1.1 (August 2024)

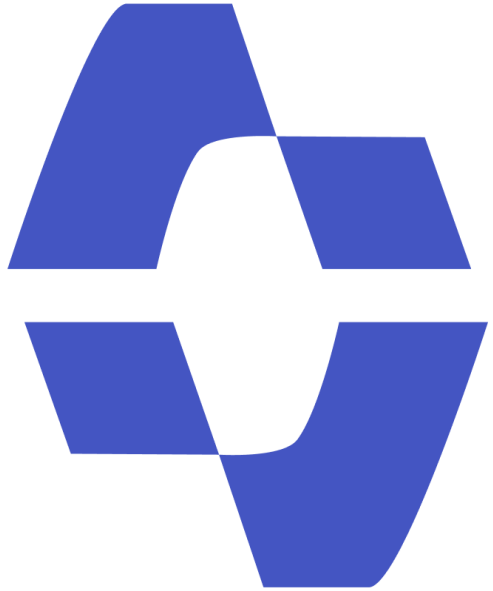
- SEC: Apache updated to version 2.4.62
- SEC: Redesign session token (VD-2416)
- SEC: Session fixation (VD-2417)
- FIX: Special chars in Distinguished Name (VD-2431)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 4.1.0 (July 2024)

- SEC: Apache updated to version 2.4.61
- SEC: Tomcat updated to version 9.0.88
- ENH: Updated mobile view capabilities
- ENH: New design for File Exchange
- ENH: Client certificates
- ENH: Revised 3rd party authentication
- ENH: Asynchronous OCR implemented - not for existing films (VD-2331)
- ENH: Improved HTML5 Client performance with enhanced Graphics enabled (VD-1730)
- ENH: Availability probing maintenance mode for VISULOX Gateways (VD-1879)
- ENH: More OTP configuration events (VD-2080)
- ENH: Unified log formats (VD-2172)
- ENH: More options for Command Connect (Arrange/Iconify (fix)on/off) (VD-2242)
- ENH: Improved cache handling for Apache header (VD-2267)
- ENH: Checkout link for approver (VD-2306)



- ENH: Control consent and captcha based on the accesspoint (VD-2320)
- ENH: Command Connect/Guard option to configure the terminal (VD-2328)
- FIX: Discard editing or deleting admin elements (VD-1656)
- FIX: Latest versions of several Javascript files (VD-1730)
- FIX: %USER% variable for alternate File Transfer users (VD-2256)
- FIX: VNC-Viewer (lastest version) works with -resource and vlxResource and vlxPwd (VD-2280)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

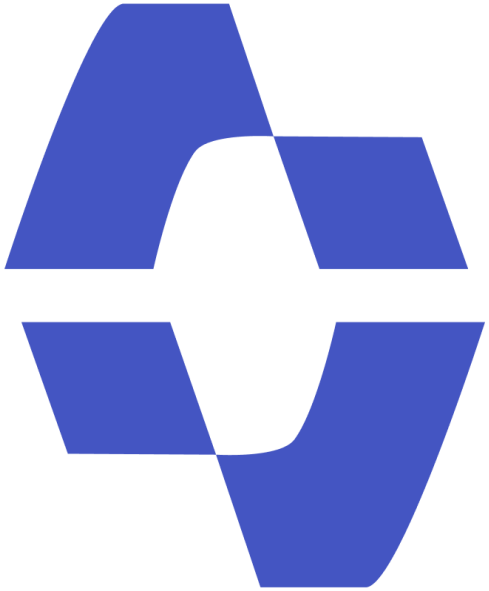
VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 4.0.1 (December 2023)

- Oracle Linux / Red Hat 7 deprecated
- SEC: Several adjustments after pentests (VD-2165)
- SEC: Several adjustments after pentests (VD-2167)
- SEC: Support for new Java-11 (VD-2221)
- ENH: Additional color for login page (VD-2161)
- ENH: Backend Captcha (VD-2166)
- ENH: Configuration option to hide PIN values in frontend (VD-2193)
- ENH: User feedback in VISULOX Cockpit for messages to users (VD-2202)
- ENH: Filtering application online states in VISULOX Cookpit (VD-2203)
- ENH: Privat host management import / export (VD-2208)
- ENH: Client language taken into account (VD-2210)
- ENH: Alternate sshpass prompt detection (VD-2218)
- ENH: Audit usage of VISULOX Portal Console (VD-2229)
- FIX: Handling passcache secrets via piping on CLI (VD-1984)
- FIX: Sporadic Workspace timeout (VD-2220)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task



VISULOX Release 4.0.0 (September 2023)

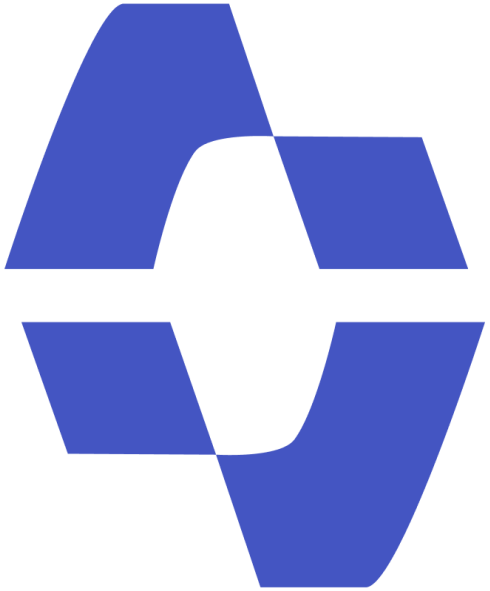
- New improved login and Workspace
  Captcha, Password Reset, Application Request via Workspace, Checkout Zone, Quick Upload Section,
  Favourites, Application Groups, Recently Used, Running applications, Force Authentication, enhanced Search and Sort
- SEC: New Tomcat version for VISULOX Gateway and VISULOX Portal
- ENH: Bruce Force prevention (VD-1947)
- ENH: Policy based OTP setup (VD-1978)
- ENH: Support of Native Client on Ubuntu 22.04 (VD-1982)
- ENH: OTP with SHA1 and SHA256 (VD-1993)
- ENH: transitimport validates characters in filenames (VD-2010)
- ENH: Diskprotection for VISULOX Filestore (VD-2011)
- ENH: New VISULOX end2end Monitoring (VD-2017)
- ENH: Sandbox for VISULOX Transit Shell and Firefox Wrapper - vlxjail (VD-2038)
- ENH: PAM user authentication (VD-2107)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.6.3 (July 2023)

- SEC: New Apache version for VISULOX Gateway and VISULOX Portal
- ENH: Mailinggroups in GUI and CLI (VD-1986)
- ENH: Mailinggroup CLI parameter for Access Policy (VD-2006)
- ENH: Filetransit with project tagging (VD-1977)
- ENH: Diskprotection extended to file store (VD-2008)
- ENH: RD Gateway authenication with common user (VD-1996)
- FIX: HTML5 client in Firefox version 106 and later is now supported (VD-1992)
- FIX: Cleanup of temp file (VD-2021)
- FIX: LDAP Connection with umlauts (VD-2012)
- FIX: Transitimport with "space" in filename (VD-2004)



ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.6.1 (March 2023)

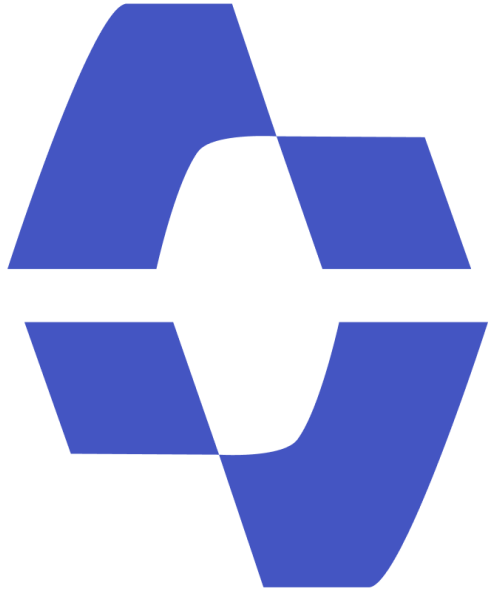
- Actionlinks in mails for access and transit approval (VD-1919)
- ActionlInks in mails for external MFA (VD-1933)
- VISULOX Runtime Environment 1.2 (VD-1872)
- SEC: Protecting sgdadmin URL (VD-1715)
- ENH: File check script for Microsoft Defender (VD-1827)
- ENH: Microsoft LAPS integration (VD-1860)
- ENH: All scripts can have additional arguments (VD-1921)
- ENH: Mail client with templates (VD-1926)
- ENH: VISULOX freeRDP applications with RDP configuration file (VD-1988)
- ENH: RD Gateway authentication with common user (VD-1996)
- ENH: Diskprotection extended to File Store (VD-2008)
- ENH: Transitimport validates characters in filename (VD-2010)
- FIX: MFA does not fail on Gateway timeout (VD-1102)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.5.0 (October 2022)

- New VISULOX logging facility based on journald
- New licensed module: OCR extension
- VISULOX Runtime Environment updated to VISULOX RTE 1.2
- ENH: Update to ETCD v3.5 (VD-1659)
- ENH: License usage reports (VD-1702)
- ENH: visulox portal admin command to change the VISULOX Portal Admin (VD-1713)
- ENH: visulox status command with fields parameter (VD-1733)



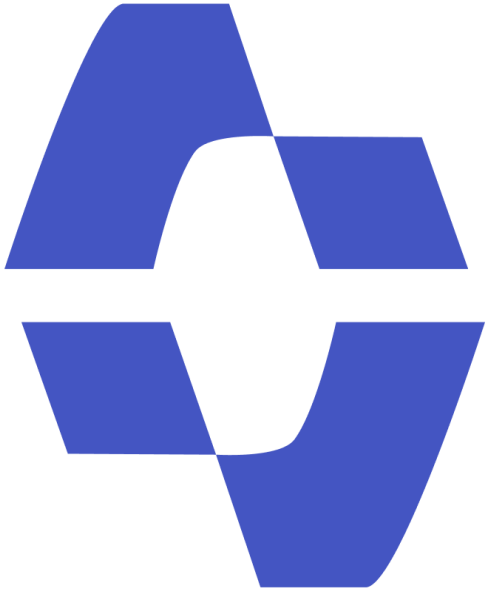
- ENH: Presave internal rejected files in Transit Zone (VD-1738)
- ENH: Prevent Unix bash history tracking during login, using vlxUnix.exp (VD-1734)
- ENH: New datasource is enabled by default (VD-1755)
- ENH: Separate MFA request during login process (VD-1626, VD-1769)
- ENH: RHEL8 IDM (VERSION: 4.9.6, API_VERSION: 2.245) supported (VD-1770)
- ENH: Testing and howto for VISULOX Transit on Ubuntu (VD-1804)
- ENH: Live player in session controller (VD-1809)
- ENH: Provide VLX Resource to standard application connections Unix/Windows (VD-1810)
- ENH: Event content search in online player (VD-1816)
- ENH: New default VISULOX window manager: JVM (VD-1818)
- ENH: Update to VISULOX RTE 1.2 (VD-1828)
- ENH: Configurable GUI offset for Session Conmtroller (VD-1846)
- FIX: Several text / message corrections and renaming
- FIX: MFA does not fail on Gateway timeout (VD-1102)
- FIX: Warning of unconfigured action scripts in Integrity-Check removed (VD-1729)
- FIX: Latest versions of some javscript files (VD-1730)
- FIX: Accounts with "password never expires" handled correctly in VISULOX Cockpit (VD-1731)
- FIX: Firefox Wrapper now in extra archive (VD-1732)
- FIX: Command Guard script validation in VISULOX Cockpit (VD-1752)
- FIX: LDAP pagesize is configurable (VD-1832)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.4.1 (May 2022)

- CVE-2021-42340 CVE-2021-40438
- SEC: Extended header for X-XSS-Protection (VD-1666)
- ENH: Support pull external OTP validation (VD-1102)
- ENH: Offline player canvas with scaling and scrollbars (VD-1657)
- ENH: Added visulox-gateway support command (VD-1673)
- ENH: Login feedback based on policy (VD-1681)



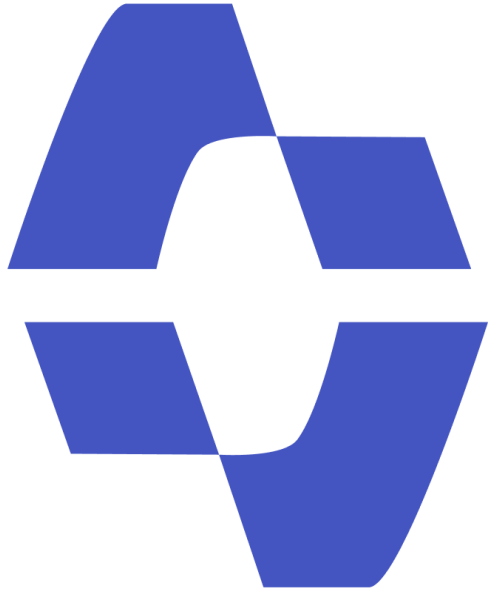
- ENH: Sort on filesize and filesignature in Cockpit Archive File View (VD-1695)
- ENH: License usage reports (VD-1702)
- ENH: MFA script for RSA SecureID added (VD-1710)
- ENH: Update VISULOX Logos (VD-1712)
- FIX: Wrong download URLs for client after update (VD-1591)
- FIX: Command Connect re-arrange during login optimized (VD-1665)
- FIX: Missing CLI option in Transit Policy -recording on|off (VD-1679)
- FIX: Offline player style issues (VD-1680)
- FIX: store migrate on archive (VD-1694)
- FIX: VLXNODE: host and user profile with the same name (VD-1699)
- FIX: Curl and proxy (VD-1696)
- FIX: VISULOX transit import fails with relative path to file (VD-1703)

ENH = Enhancement, FIX = Fixed, SEC= Security CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.4.0 (March 2022)

- BigUpload will be discontinued and is **now integrated in File Transfer**
- ENH: Checkout password displayed in File Checkout Area, Reports and in VISULOX Cockpit (VD-1285)
- ENH: Integrity-Check of database connection (VD-1545)
- ENH: Recorder improved (smaller files) (VD-1572)
- ENH: Gateway IP listed in VLX Cockpit / Online view (VD-1584)
- ENH: Checkout password displayed in Workspace and event table (VD-1589)
- ENH: Better usablity during download of large files (VD-1597)
- ENH: Extended webserver header for security reasons (VD-1603)
- ENH: Extended check for transitmapping (VD-1604)
- ENH: Better Integrity Check in VISULOX X11 Forwarding (VD-1606)
- ENH: visulox transit delete supported (VD-1609)
- ENH: GUI title with serveral placeholders (VD-1614)
- ENH: Integrity-Check verifies FQDN length (VD-1625)
- ENH: Improved Integriity-Checks (VD-1630)



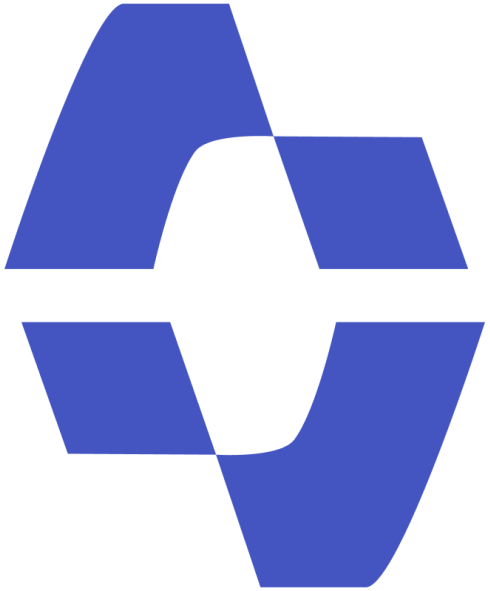
- ENH: New archive mode: nosnapshot (VD-1644)
- FIX: Matching objects in VISULOX Command Line Interface (VD-847)
- FIX: Adding an Archive Server to VISULOX Cluster without restart (VD-984)
- FIX: yum update on local gateway setups (VD-1582)
- FIX: Wrong download URLs for client after update (VD-1591)
- FIX: Matching objects in VLX Commandline Interface (VD-847) (VD-1608)
- FIX: SIEM integration with error logging (VD-1617)
- FIX: Returncode of visulox status of several commands corrected (VD-1621)
- FIX: Webservice user now uses logical name (VD-1636)
- FIX: Command Connect handles resource with wrong password (VD-1641)
- FIX: Large snaphot creation removed in session controller (VD-1647)

ENH = Enhancement, FIX = Fixed, CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.3.3 (November 2021)

- Major update for VISULOX PORTAL
- CVE-2021-35649 CVE-2021-35650 CVE-2021-33037
- ENH: Handling five digit toplevel domains (VD-1579) (VS-920)
- ENH; Recoder optimization (VD-1572) (VD-1574)
- ENH: Placeholders in messages (VD-1562)
- ENH: VISULOX PORTAL uses pam stack only for local Unix users (VD-1560)
- ENH: More design parameters added (VD-1536)
- ENH: With no Transit Policy, the Transit Policy and the Transit Zone is disabled in Workspace (VD-1541)
- ENH: Integrity-Check supports timedatectl (VD-1535)
- ENH: Template and configuration for load balancer probing file (VD-1559)
- ENH: Fluxbox design (VD-1491)
- FIX: Player handling with screen change before recording started (VD-1580)
- FIX: Cookpit - correction in application creation (VD-1471)
- FIX: Cookpit - correction in application creation / AppWizzard vlx Controls (VD-1465)
- FIX: Upload multiple selected files in FT-Client (VD-1368)



- FIX: bindfs not cancelled correctly in Big Upload mode - additional fixes (VD-1517)
- FIX: File Transfer with spaces in directory (VD1526)
- FIX: Core file Fluxbox (VD-1563)
- FIX: Error closing Command Connect (VD-886)

ENH = Enhancement, FIX = Fixed, CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.3.2 (September 2021)

- ENH: Customizable Login / Workspace color design and company logos (VD-1513)
- ENH: SMS Kannel interface support timeout (VD-1519)
- FIX: Resize Command Connect shell arrangement (VD-1511)
- FIX: bindfs not cancelled correctly in Big Upload (VD-1517)
- FIX: (Security) information process table reduced (VD-1421)

ENH = Enhancement, FIX = Fixed, CVE = Common Vulnerabilities and Exposures

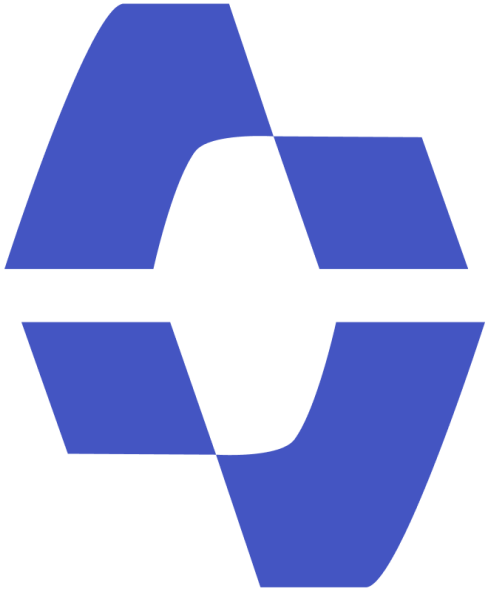
VS = VISULOX Support Ticket, VD = VISULOX Development Task

VISULOX Release 3.3.1 (August 2021)

- CVE-2019-17567 CVE-2020-1935 CVE-2020-1938 CVE-2020-8284 CVE-2020-8285 CVE-2020-8286 CVE-2020-13938 CVE-2020-13950 CVE-2019-17569 CVE-2021-2446 CVE-2021-2447 CVE-2021-22901 CVE-2021-25122 CVE-2021-25329 CVE-2021-26690 CVE-2021-26691 CVE-2021-30641 CVE-2021-31618 CVE-2020-35452
- ENH: end2end availability monitoring (VD-1302)
- ENH: VISULOX PORTAL configuration from VISULOX Service without registration (VD-1420)
- FIX: Connection AD with dh key too small (VD-1494)
- FIX: Application Assistant and application presentation (VD-1488)

ENH = Enhancement, FIX = Fixed, CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task



VISULOX Release 3.3 (June 2021)

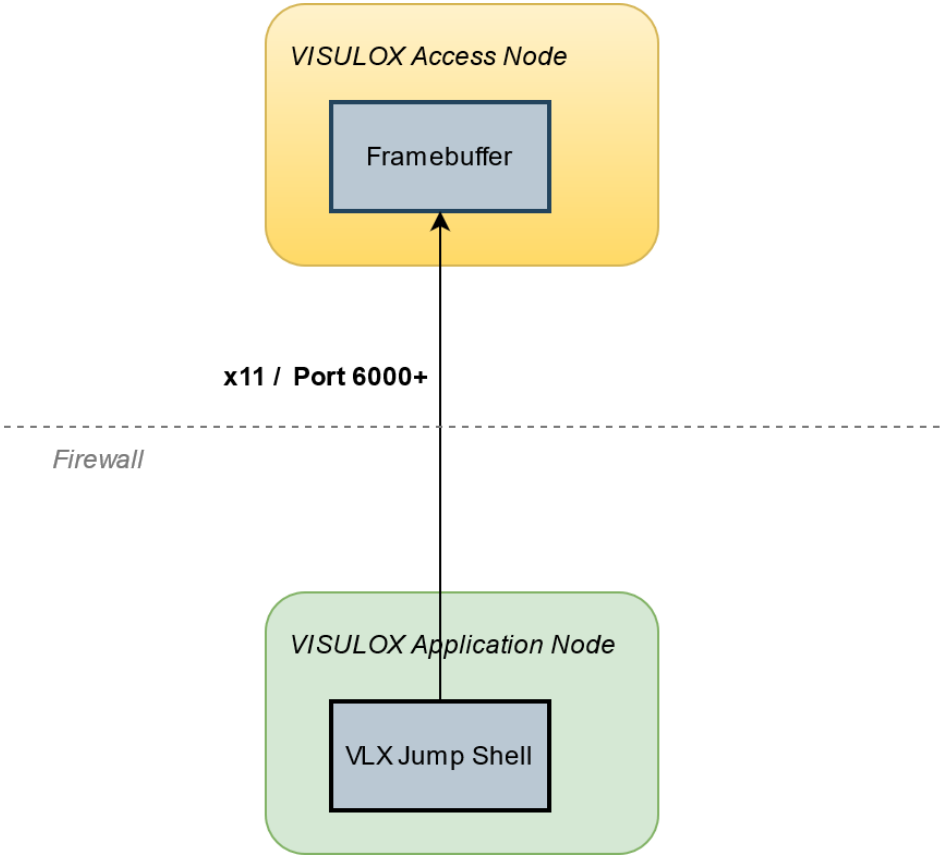
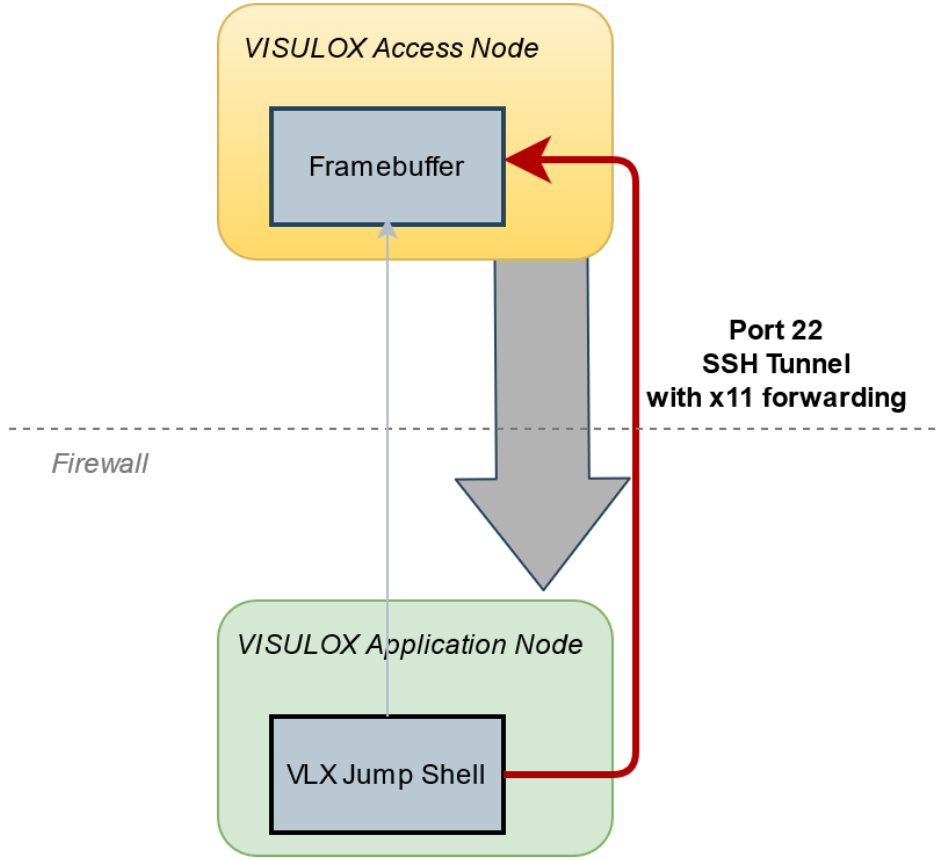
- **VISULOX PORTAL Service Embedded**
- VISULOX Helpdesk is no longer available
- RPM package signatures can be used for the VISULOX RPM packages
- New Application Assistant in VISULOX Cockpit
- ENH: Branding of login page (.Access Branding) (VD-1459)
- ENH: Accesspoint management (VD-1477)
- ENH: end2end monitoring (How to setup VISULOX end2end monitoring) (VD-1302)
- ENH: Integrity-Check for Transit Zone (VD-1455)
- ENH: Access consent during login (VD-1444)
- CVE: CVE-2021-2248 CVE-2021-3450 CVE-2021-2177 CVE-2021-2221

ENH = Enhancement, FIX = Fixed, CVE = Common Vulnerabilities and Exposures

VS = VISULOX Support Ticket, VD = VISULOX Development Task

23.1.113 VISULOX SSH X11 Forwarding to VISULOX Application Nodes

The X11 server is not always addressed directly by VISULOX.
This means the application server needs an X11 connection (port 6000+) to the VISULOX Access Nodes.
If it is not wanted to open these ports in the firewall, VISULOX X11 Forwarding can be used instead.

Connection with port 6000+	Connection with VLX x11 forwarding
	

⚠ A firewall between nodes in the cluster (VISULOX and VISULOX PORTAL) must be configured with the following setting "**session time out=never**".

Whenever the X11 Forwarding is enabled, a new key is generated and populated:

```
visulox config x11forward -enable
```

Disabling X11 Forwarding also includes removing the common key:

```
visulox config x11forward -disable
```

Whenever the cluster key changes, the X11 Forwarding has to be re-enabled:

```
visulox config x11forward -enable
```

Excluding servers from VISULOX X11 Forwarding:
It is possible to exclude a list of servers from X11 Forwarding. The list delimiter is ":". Each element can be either the nodename, FQDN or regexp.

```
visulox config x11forward -exclude server1:server2:"^abc:192"
```

visulox integrity and **visulox config x11forward -check** only check the access to the servers in the cluster. They do not check X11 forwarding enabled:

```
   visulox integrity -x11forward
   visulox config x11forward -check
```

23.1.114 How to configure FreeRDP for VISULOX PORTAL

Introduction

The goal is to call a Windows remote application using FreeRDP. The configuration is done in the VISULOX PORTAL Console.
In this example the preconfigured application VLX RDP is used, which is setup by the VISULOX installation.
It is also possible to configure own applications by using the VISULOX PORTAL Console.

- Introduction
- Step 1 : Configuring passcache, single sign on, script object
- Step 2 : Configuring FreeRDP as an integrated part of VISULOX
- Step 3 : Configuring Window Manager

Step 1 : Configuring passcache, single sign on, script object

Resource:

VISULOX PORTAL Console / Launch tab / Arguments for Command
`-resource <name>`

Resources can be configured in the V**ISULOX Cockpit / Addons / Passcache** or via Command Line Interface.

Script object

VISULOX PORTAL Console / Launch tab / Arguments for Command
`-rdpfile <name>`

RDP configuration files can be configured in **VISULOX Cockpit / Addons / Script Objects** or via Command Line Interface.

See also: Script objects / RDP configuration files

Single sign on:

VISULOX PORTAL Console / General tab / Hints field

```
vlxSSO=1;
```

These steps can be skipped, but in this case user and password must be entered everytime the WTS is connected, before the remote application will be started.

Step 2 : Configuring FreeRDP as an integrated part of VISULOX

VISULOX PORTAL Console / Launch tab / Application Command field

```
vlxshell
```

In this example a preconfigured script object and a resource will be used:

VISULOX PORTAL Console / Launch tab / Arguments for Command field

```
-client freerdp -rdpfile test -resource <resource-name> -- <freerdp-parameter>
```

vlxshell parameters with RD Gateway configuration and resource:

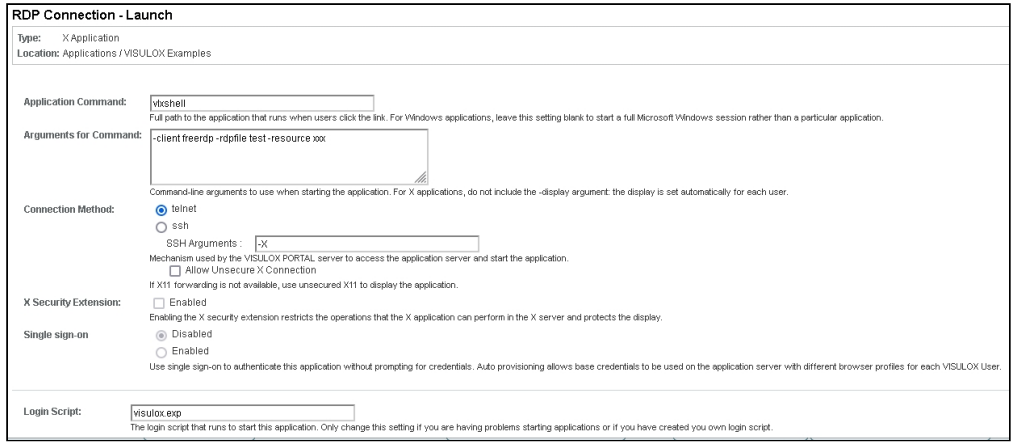
```
-client freerdp -rdpfile RDP -gateway-resource test /g:<server.domain> /gateway-usage-method:direct
```

Please check the freeRDP documentation of the installed version regarding how to use the parameters for freerdp, if necessary.

The commands of xfreerdp have been changed in version 2.x.
If the new version is used, also the new parameters have to be used in the Arguments for Command field of the vlxshell application.

VISULOX PORTAL Console / Launch tab / Login Script field

```
visulox.exp
```



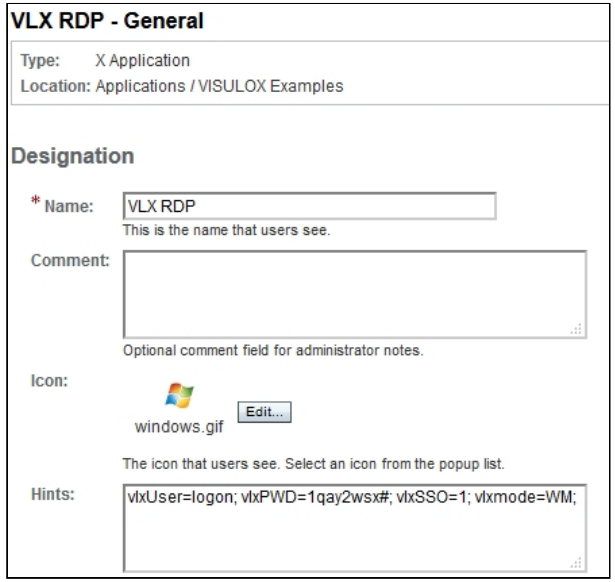
Step 3 : Configuring Window Manager

The Window Manager has to be configured in the **General** tab:

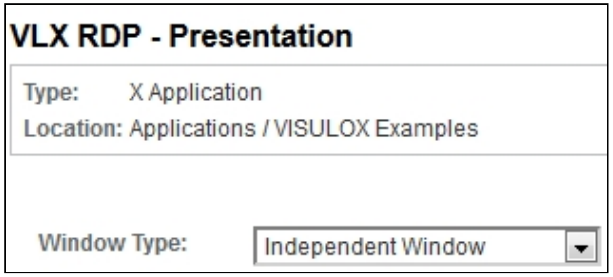
VISULOX PORTAL Console / General tab / Hints field

```
vlxMode=WM;
```

If WM mode is not set freerdp may throw a bad atom error.



Set the VISULOX PORTALConsole / Presentation tab / Window Type field to "**Independent Window**"



Remote applications will not be terminated after ending the RDP session, if the WTS is not configured otherwise.

23.1.115 freeRDP with NLA support statement

It is possible to use Windows 2012 with NLA support enabled. NLA is supported by VISULOX PORTAL with ttatsc.
If a Windows 2012 / NLA session is connected to Filetransfer, **vlxShell -client freerdp -drive X** has to be used.

If freeRDP is used without NLA, the **--no-nla** parameter must be set.

vlxShell with **freeRDP** is working with **vlxSSO=1** to provide primary login credentials to Windows. If needed, also with extra **vlxUser** and **vlxPWD**.

If a drive is assigned with -drive <letter>, the according Windows or Citrix server must provide this drive.

23.1.116 Enable logging of SQL queries in database service

Sometimes it can be useful to see what queries are processed by the database service.

To enable the logging of queries a message has to be sent to the database service:

```
/opt/visulox/bin/cmd/msg.tcl -to database -command DEBUG-SQL -sqldebug 1
```

The queries can be seen in **database.log**.

To disable logging set the flag to "**0**".

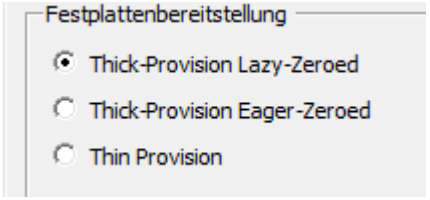
To query the state, just send the DEBUG-SQL command.

23.1.117 How to use VISULOX on virtualized VMWare disks

VISULOX can be installed on virtualized disks on platforms like VMWare.

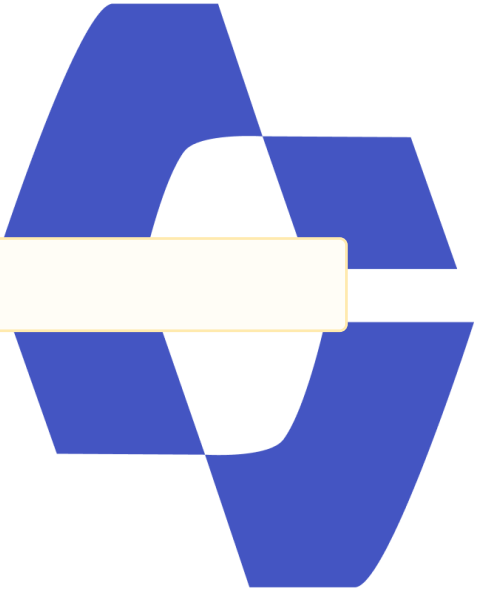
If such disks are used, it is necessary, that these disks are **NOT** setup as "t**hin provisioned**".

"**Thick provisioning**" has to be used instead.



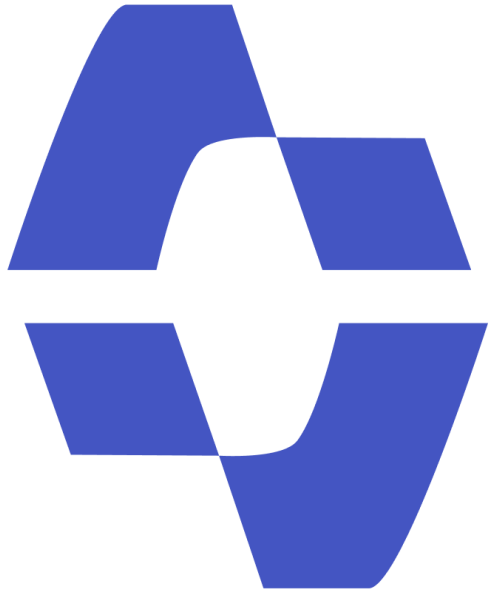
Thin provisioning can not be recognized by VISULOX and will lead to errors like: "No space on device", "Database or disk full" in the logs.

This happens although the operation system is showing, that there is enough disk space via "**df**" command.



⚠ In actual VMware versions it may happen, that thin provisioning is the only available option for disks.
In this case **thin provisioning** with **hard zero** has to be chosen.

Checking existing disks in Virtual Machine Properties of VMWare:



23.1.118 Custom vlxuser ID for transit users

Normally during installation the vlxtransit users are created with the next available user ID.

To assign other UIDs, the transit users have to be deleted first:

```
/opt/visulox/setup/vlxusers/mgmt.tcl del
```

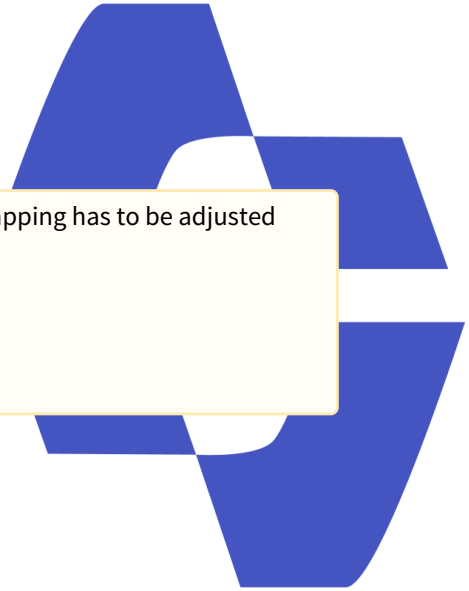
Then vlxusers can be recreated with a new start UID. The UIDs are continuous:

```
/opt/visulox/setup/vlxusers/mgmt.tcl add -startuid <number> -# <amount>
```

Configuration parameters

/opt/visulox/setup/vlxusers/mgmtl.tcl **add**

Parameter	Description
-startuid <>	Start User ID for the vlxusers
-home <>	Base directory of vlxusers. Default value: </opt/visulox/vlxusers>
-shell <>	Shell for the user. Default value: </bin/bash>
-# <>	Amount of vlxusers, which will be generated. Default value: <100>



If the transit users have been customized with **/opt/visulox/setup/vlxuser/mgmt.tcl** and visulox-transitmapping is installed, then the mapping has to be adjusted too:

```
/opt/visulox/setup/vlxusers/mgmt.tcl add -# 10
/opt/visulox-transit/bin/transitmapping.sh enable
```

23.1.119 Manual restart of a missing VISULOX service

Normally the monitor detects a crashed service and restarts it. This can happen 3 times, then the monitor will give up.

To bring the service back online, without a whole VISULOX Service restart, the missing service can be restarted with the following method:

Restart via VISULOX command:

- Log into the VISULOX Node where the service is missing.
- Restart the service with:

```
visulox restart -service <vlxservice1>,<vlxservice2> ...
```

The parameters are the same as in **service.conf.**

Show available running VISULOX services:

```
visulox restart -service --?

running services:

    configuration  | importer       | router
    database       | monitor        | scripts
    dict           | objects2Portal | sessioncache
```

```
download        | pin             | stats
filecache       | policy          | store
filecopy        | portal2node     | transitzone
fileexchange    | publish         |
health          | replication     |
```

23.1.120 Monitoring tool: checkPortal.sh

The availability of the VISULOX Access Node and its components is essential for operation.
The script **checkPortal.sh** allows to check the availaiblity from three different viewpoints and can be found in **/opt/visulox/setup/examples/**.

1) From outside, like the user (**-lb**)

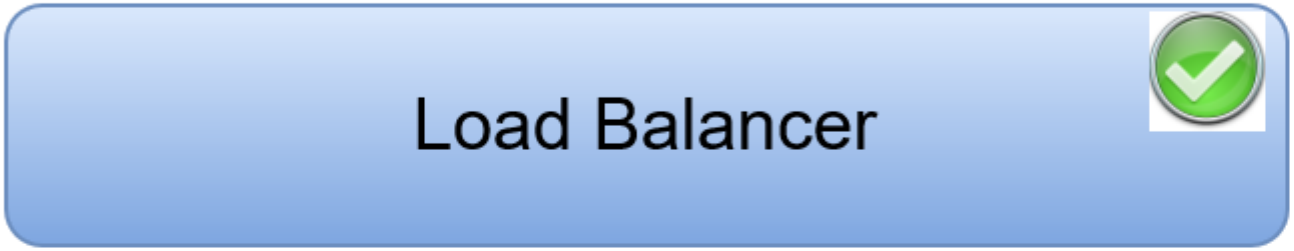
2) From the VISULOX GATEWAY (**-gw**)

3) From the VISULOX PORTAL Node (**-sgd**)

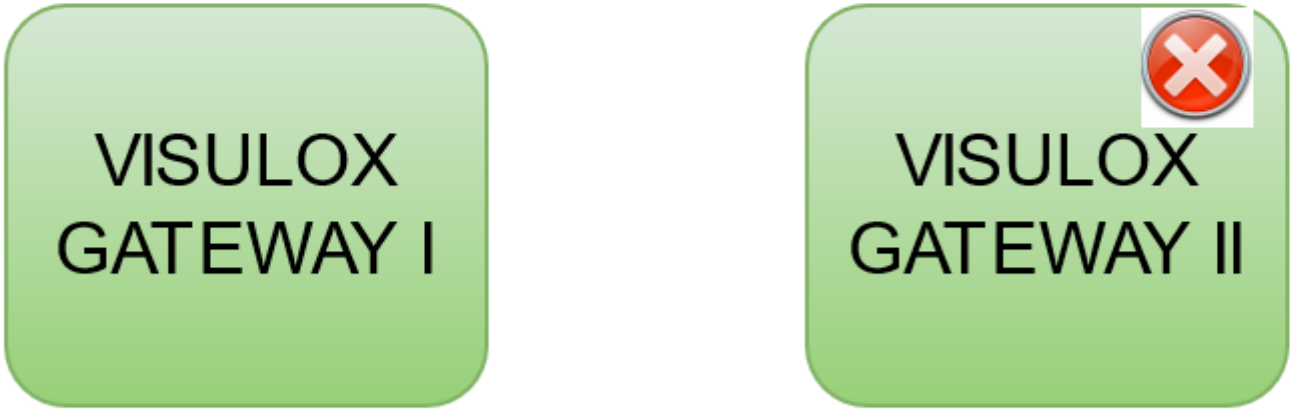
A check from outside (1) will show the result, wether the portal is available or not.

If a single VISULOX GATEWAY (2) or VISULOX PORTAL instance (3) is not available, this will not be detected by (1).

Therefore the explicit checks for each VISULOX GATEWAY and/or each VISULOX PORTAL are needed.



1



2

Checking the **service:**

Service check

```
checkPortal.sh -lb -server <accessserver>
```

Can run on any system, which has access to the service.

Checking the **VISULOX GATEWAY**:

Gateway check

```
checkPortal.sh -gw -server <gwserver>
```

This check runs on each Gateway server

Checking the **VISULOX PORTAL**:

Portal check
`checkPortal.sh -sgd -server <VISULOX Access Node)`

This check runs on each VISULOX Access Node.

Path: /opt/visulox/setup/example/**checkPortal.sh**

Available options:

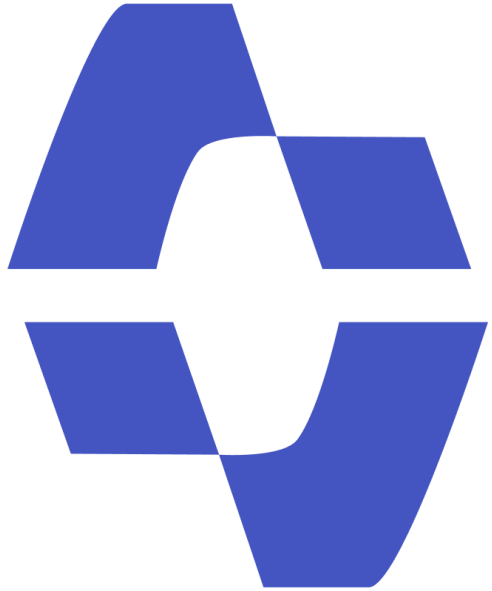
Command	**Description**
-lb	Test via Loadbalancer
-gw	Test via VISULOX GATEWAY
-sgd	Test VISULOX PORTAL(default)
-server <arg>	Endpoint to test <$ACCESSSERVER>
-port <arg>	Port of the endpoint to test <$PORT>

Command	Description
-e	Check includes GW-enable file (lb_endpoint.html)
-q	Quiet mode
-nagios	exitcode related for nagios
-verbose	Verbose mode
-debug	Debug mode

Return codes:

Return code	Description
0	Ok
1	Warning
2	Critical
3	Unknown
10	Gateway Java proxy not available

Return code	Description
11	Gateway Apache revers proxy not available
12	None of the portal Apaches is answering
13	None of the portal Tomcats is answering
14	GW cannot see any portal
15	VISULOX GATEWAY disabled (lb_endpoint.html)
20	VISULOX PORTAL Array service not available
21	VISULOX PORTAL Service not available
22	VISULOX PORTAL Apache not available
23	VISULOX PORTAL Tomcat not available
126	Missing or cannot be executed
127	General error



Other useful tools

gwApache.sh allows VISULOX GATEWAY Apache start / stop / restart without disconnecting users sessions.
gwCheck.sh to check VISULOX GATEWAY connectivity.

These scripts can be found in **/opt/visulox/setup/example/gateway/.**

23.1.121 Modify VISULOX PORTAL Datastore via CLI

With the tool **/opt/visulox/tools/migration/buildEditDatastore.tcl** entries can be read and edited from the datastore.

It is also possible to use a created datstore file.

buildEditDatastore.tcl options

Option	Description
-example	Print examples
-i	Ignore case distinctions in all masks / regexp
-print <*value*>	Print objects or attributes <>
-dsFile <*value*>	Path to datastore CSV dump file or use local portal connector <>
-contentmask <*value*>	Regexp into objects string <>

Option	Description
-valuemask <*value*>	Regexp on value <>
-attribute <*value*>	Name or name mask of attribute to change <>
-newvalue <*value*>	New value for attribute <>
-ttaChangeScript <*value*>	File for 'tarantella object edit --file' </tmp/ttaChange.tta>
-aslistvalue	newValue treaded as a list: scottamemberusers scottahosts scottamembergroups
-addlistvalue	newValue added to list: scottamemberusers scottahosts scottamembergroups
-format <*value*>	Format of output (text,xml, csv, json, tcl) <text>
-verbose	More messages on stdout
--	Forcibly stop option processing
-help	Display commands
-?	Display commands

For example:

List all objects

```
./buildEditDatastore.tcl -print o
```

List all attributes

```
./buildEditDatastore.tcl -print a
```

Useful to find attribute names.

List all attributes and content

```
./buildEditDatastore.tcl -print v
```

Useful to find attribute names and content.

Using a datastore file

```
./buildEditDatastore.tcl -dsFile <filename>
```

Datastore files are created with the following program:

Create datastore file

```
/opt/visulox/lib/utils/sgd.tcl datastore -format csv -raw > /tmp/ds
```

With this program a VISULOX PORTAL Object edit script is created.

Show all application with -pos set

```
./buildEditDatastore.tcl -contentmask scottafilepath=vlxgui -attribute scottaarguments -valuemask "-pos"  -print v
```

Remove “-pos”

```
./buildEditDatastore.tcl -contentmask scottafilepath=vlxgui -attribute scottaarguments -valuemask "-pos" -newvalue ""
```

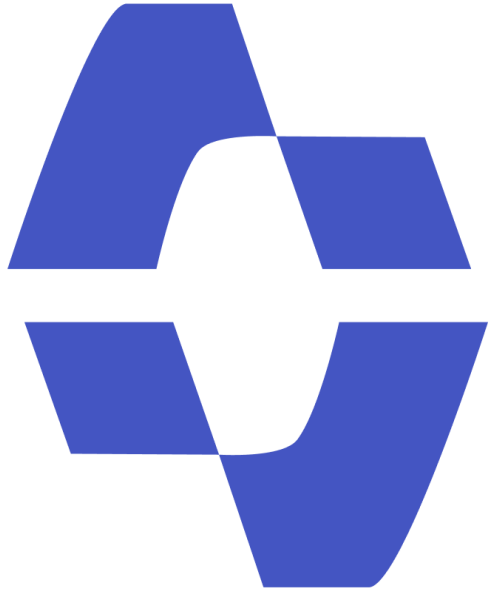
Example for tta change script command:

```
--name "o=applications/ou=TestingApps/cn=@xterm(R:OCR:RESOURCE)" --scottamembergroups "cn=allowedusers,cn=group,dc=corp,dc=cyta"
"cn=arieso-admin,cn=group,dc=corp,dc=cyta" -addlistvalue
```

Related articles

(4.2.0) Modify VISULOX PORTAL Datastore via CLI

(4.2.0) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x



(4.2.0) Migrating from VISULOX 3.x to 4.x
(4.3.2) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.2) Modify VISULOX PORTAL Datastore via CLI
(4.3.2) Migrating from VISULOX 3.x to 4.x
(4.1.1) Migrating from VISULOX 3.x to 4.x
(4.1.1) Modify VISULOX PORTAL Datastore via CLI
(4.1.1) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.1) Modify VISULOX PORTAL Datastore via CLI
(4.3.1) Migrating from VISULOX 3.x to 4.x
(4.3.1) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.0) Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
(4.3.0) Migrating from VISULOX 3.x to 4.x
(4.3.0) Modify VISULOX PORTAL Datastore via CLI
Modify VISULOX PORTAL Datastore via CLI
Migrating from VISULOX 3.x to 4.x
Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
Migrating from OSGD 5.x / VLX 3.x to VISULOX 4.x
Modify VISULOX PORTAL Datastore via CLI
Migrating from VISULOX 3.x to 4.x

23.1.122 Enable events for VLX Shell, FreeRDP and File Transit connections

VISULOX Events for **VLX Shell** and **FreeRDP** connections can be enabled with:

```
visulox config -name vlxshell.event.rdpconnect=true
```

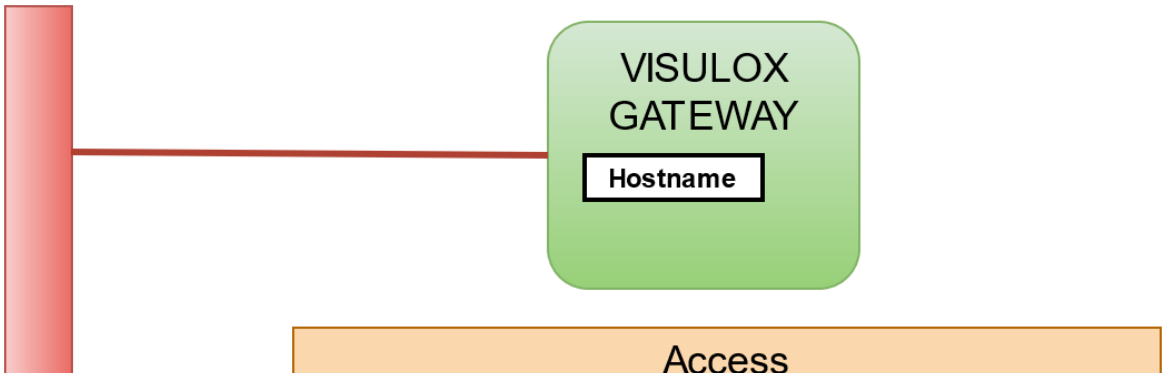
The events are displayed in the VISULOX Cockpit with additional information: **host/IP**, **username**.

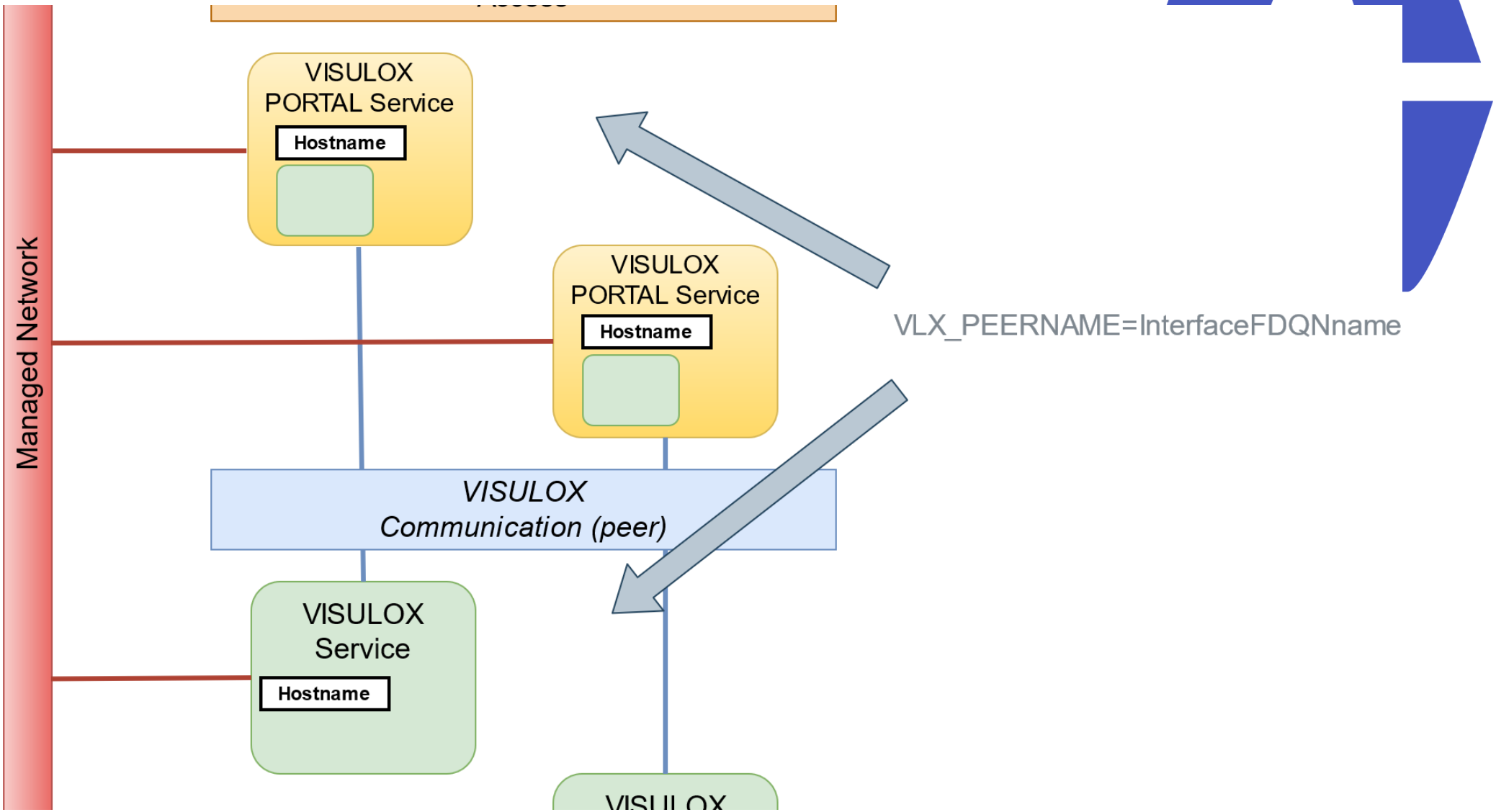
VISULOX events for **File Transit** connections to servers are adjusted with:

```
ftclient.event.connect          | default |
ftclient.event.default          | false   |
ftclient.event.disconnect       | default |
```

23.1.123 How to use VISULOX with multiple network cards

Each VISULOX Node has a logical name. The logical name is derived from the servers hostname.
The hostname of the server is mostly assigned to one network card.
The communication within an VISULOX Cluster is also based on the FQDN of each node.




Managed Network
VISULOX
PORTAL Service
Hostname
VISULOX
PORTAL Service
Hostname
VLX_PEERNAME=InterfaceFDQNname
VISULOX
Communication (peer)
VISULOX
Service
Hostname

From these two aspects, two issues can arise:

1. The logical name is not the same, that has to be used in the architecture.
2. The communication should be routed through other interfaces.

To change the logical name, the directive **VLX_LOGNAME** in **/opt/visulox/etc/vlx.profile** can be set to an alternate name.

```
export VLX_LOGNAME=other
```

Internally "**other**" is mapped to "**vOTHER**". Check with: .**visulox config mynodename**

To change the cluster routing, the directive **VLX_PEERNAME** in **/optvisulox/etc/vlx.profile** can be set to the related name of the interface.

```
export VLX_PEERNAME=other.domain.de
```

To attach another node via that alternate route, the attach command is:

```
visulox attach <FQDN of destination peer name>
```

Keep in mind, that this handles the communication between VISULOX Nodes. It is also recommended to think about the VISULOX PORTAL Array and VISULOX PORTAL application server communication.

Therefore the following command has to be taken into account:

```
visulox-portal serverrename --peername <FQDN>
```

VISULOX recorders and VISULOX application servers are addressing the portal X11 server (ttaxpe) based on the VISULOX PORTAL peer name.

See also:

VISULOX SSH X11 Forwarding to VISULOX Application Nodes

23.1.124 How to use the VISULOX Command Line Interface from a remote server

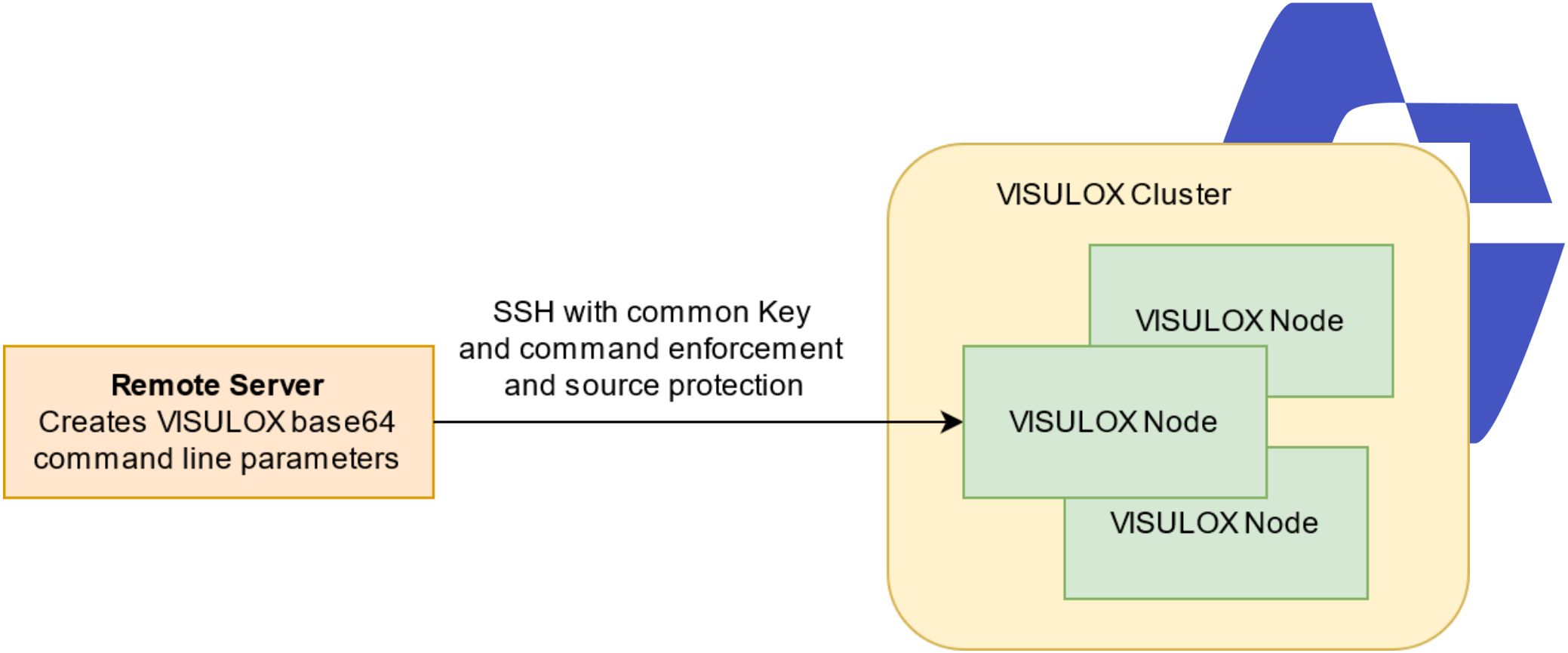
Background

Conceptional the VISULOX Command Line Interface is created on a remote server and sent via SSH to an available VISULOX Node.

Therefore a trusted SSH communication between the remote server and the VISULOX Node has to be established.

This trusted communication enforces the configured VISULOX command only (no other usage possible, like shell access).

- Background
- Create keypair anywhere
- Import public Key to VISULOX
- Execute command from remote
- Related articles



SSH has the possibility to add a command enforcement.

Create keypair anywhere

```
ssh-keygen -t dsa -C <keyname> -f <keyfilename>  -N ""
```

Modify key with command by editing the public part of the key: <keyfilename.pub>

If the options phrase at the beginning of a line contains the keyword command="**string**", then any SSH connection, that authenticates using this particular key will **only** run the command specified, even if the command line has specified another command.

```
command="visulox access add -stdin" ssh-dss AAAAB3NzaC1kc3 .... 19g4D3UCHNi1RIO08DeOq98yuW <keyname>
```

An additional argument could be "**from=**", to restrict the servers.

If the options phrase at the beginning of a line contains the keyword from="**string**", this restricts the use of the key on that line to sessions that originate from hosts that match "**string**".
Examples might be:

- from="trusted.eng.cam.ac.uk"
- from="*.eng.cam.ac.uk,!untrusted.eng.cam.ac.uk"
- from="tw?00.eng.cam.ac.uk"

The hostname used has to be the hostname reported, when the IP (network) address of the connecting machine is looked up in the DNS. The "*****" wildcard matches one or more characters, while "**?**" matches a single character. If the connecting host name matches an entry prefixed by "**!**", then it will be rejected.

```
command="visulox policy access add -stdin" from="<name>"  ssh-dss AAAAB3NzaC1kc3 .... 19g4D3UCHNi1RIO08DeOq98yuW <keyname>
```

Import public Key to VISULOX

Add the pubic key to the VISULOX Nodes, which are called remotely:

```
mkdir /opt/visulox/.ssh
cat <keyname.pub> >>  /opt/visulox/.ssh/authorized_host
chmod 0400 /opt/visulox/.ssh/authorized_host
chmod 0500 /opt/visulox/.ssh
chown -R vlx:vlxgroup /opt/visulox/.ssh
```

Because the vlx user normally does not have a password, the command ssh-copy-id can not be used.

Execute command from remote

The private key <keyname> is transferred to the remote server.

There are two possibilities to provide parameters: clear text and base64. Base64 is recommended, because the command does not need any quoting or code page.

example

```
echo "-name AUTO -object64 Q049VGlsbG1hbm4gQmFzaWVuLE9VPU1pdGFyYmVpdGVyLE9VPVRvb2xCb3gsREM9dGJzb2wsREM9ZGU= \
-ticket64 MTIzNA== \
-endtime64 MjAxNi0wMS0wMQ==" | ssh -i <keyname> vlx@<nodename>
```

Related articles

VISULOX Command Line Interface (CLI)

Passcache

Access Policy

How to control access from the command line

23.1.125 CORS adjustment on VISULOX Gateway

Cross-**O**rigin **R**esource **S**haring (**CORS**) is an HTTP-header based mechanism that allows a server to indicate any origins (domain, scheme, or port) other than its own from which a browser should permit loading resources.

CORS also relies on a mechanism by which browsers make a "preflight" request to the server hosting the cross-origin resource, in order to check that the server will permit the actual request.
In that preflight, the browser sends headers that indicate the HTTP method and headers that will be used in the actual request.

For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts.
This means that a web application using those APIs can only request resources from the same origin the application was loaded from unless the response from other origins includes the right CORS headers.

To protect requests in VISULOX with an origin HTTP the following adjustments have to be done on VISULOX Gateways.
The internal and the external site URLs must be registered in **httpd-gateway-rest.conf** and **httpd.conf**.

httpd-gateway-rest.conf

```
/opt/SUNWsgdg/httpd/httpd-default/conf/extra/gateway/httpd-gateway-rest.conf

<Location "/sgdadmin">
    # Reject any ; path delimiter under the /sgdadmin path
    RewriteEngine on
    RewriteCond "%{REQUEST_URI}" ".*[;].*"
    RewriteRule "^.*$" - [R=404,L]
</Location>

AllowEncodedSlashes NoDecode

### Add this and edit the site urls
<Location "/api">
    # Reject any origin not allowed under the /api path
    RewriteEngine on
    RewriteCond "%{HTTP:Origin}" "!^($|https\:\/\/site1\.com|https\:\/\/site2\.de|https\:\/\/site3\.com)"
    RewriteRule "^.*$" - [R=403,L]
</Location>
### Add end

ProxyPass / balancer://mysgdservers/ lbmethod=byrequests stickysession=balanceid nocanon
```

httpd.conf

```
/opt/SUNWsgdg/httpd/httpd-default/conf/httpd.conf
<IfModule headers_module>
    Header set Content-Security-Policy "frame-ancestors 'self'"
    Header set X-Frame-Options "SAMEORIGIN"
    Header set Referrer-Policy "same-origin"
    Header set X-Content-Type-Options "nosniff"
    Header set Strict-Transport-Security "max-age=31536000;"

### Add this and edit the site urls
<If "!(%{HTTP:Origin} in { 'https://host.domain', 'https://site1', 'https://site2.de', 'https://site3.com' })">
    Header unset Access-Control-Allow-Origin
    Header unset Access-Control-Allow-Credentials
</If>
### Add end

</IfModule>
```

23.1.126 VISULOX PORTAL Console

The VISULOX PORTAL Console

This article describes how to run the VISULOX PORTAL Console.

It also includes details of how to avoid some common problems when using the VISULOX PORTAL Console.

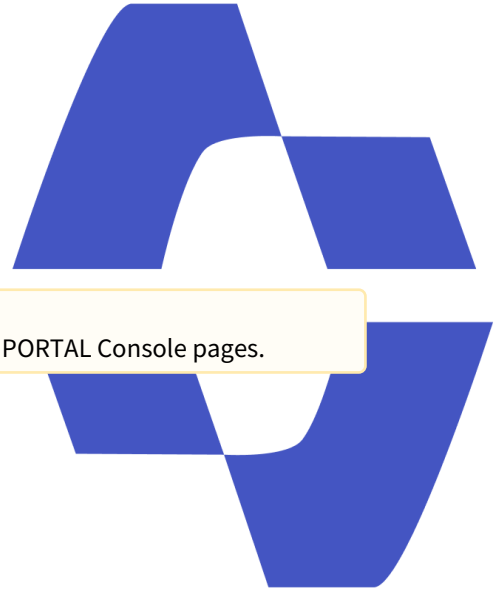
- The VISULOX PORTAL Console
- Supported browsers for the VISULOX PORTAL Console
- Starting the VISULOX PORTAL Console
- Avoiding VISULOX PORTAL Datastore update problems
- Performing array operations using the VISULOX PORTAL Console
- VISULOX PORTAL Console configuration settings
  - Number of search results
  - DNS lookups
  - Searching and displaying LDAP data
  - Session timeout
- Working with the VISULOX Portal Console
  - Starting the VISULOX Portal Console
  - Creating an Application Server Object
  - Adding an application to the VISULOX Portal Workspace

Supported browsers for the VISULOX PORTAL Console

To display the VISULOX PORTAL Console, you can use a supported browser.
A list of the current supported browsers can be provided on request.

- The VISULOX PORTAL Console is not supported on Safari browsers.
- Beta versions or preview releases of browsers are not supported.
- Browsers must be configured to accept cookies.

- Browsers must have the JavaScript programming language enabled.



> When using the VISULOX PORTAL Console, do not use the browser's **Back** button.
> Instead, use the **Jump to Object View** and **Jump to Navigation View** links, or the **Object History** list, to navigate through the VISULOX PORTAL Console pages.

Starting the VISULOX PORTAL Console

The VISULOX PORTAL Console works best when you run it on the Primary VISULOX PORTAL Server in the array.

The VISULOX PORTAL Console can be started in the following ways:

- Click on the **VISULOX PORTAL Console** link in the Workspace of a VISULOX PORTAL Administrator
- Go to the https://portal-*server.example.com*/sgdadmin URL

The VISULOX PORTAL Console uses the preferred language for the browser. The current Workspace language is not used.

> The VISULOX PORTAL Console is for VISULOX PORTAL Administrators only.
> To use the VISULOX PORTAL Console the user must log in as, or be logged in as, a VISULOX PORTAL Administrator.

Avoiding VISULOX PORTAL Datastore update problems

You can perform operations on the VISULOX PORTAL Datastore, such as creating new objects and editing object attributes, using the VISULOX PORTAL Console from any VISULOX PORTAL Server in the array.

When you edit the VISULOX PORTAL Datastore, the changes you make are sent to the Primary VISULOX PORTAL Server. The Primary VISULOX PORTAL Server then replicates these changes to all secondary servers in the array.

By running the VISULOX PORTAL Console from the Primary VISULOX PORTAL Server, you can avoid problems due to the following:

- **Slow network:** If the network is slow, “Object not found” or “Object not created” errors can be returned. Also, problems with stale data can occur, where configuration changes are not shown correctly.
- **Primary down:** If the primary server is down, or unavailable, VISULOX PORTAL Datastore changes are not applied.

Performing array operations using the VISULOX PORTAL Console

The following limitations apply when using the VISULOX PORTAL Console to perform array operations, such as array joining or array detaching:

- **Use the Primary VISULOX PORTAL Server:**
  Running the VISULOX PORTAL Console on the primary server avoids data replication problems.
  See also: "Avoiding VISULOX PORTAL Datastore update poblems”.

- **All servers involved in an array operation must be up:**
  For example, the VISULOX PORTAL Console cannot be used to detach a secondary server that is down.
  Instead, use the **visulox-portal array detach** command.

- **Clocks must be synchronized on all servers involved in an array operation:**
  For example, a secondary server cannot be added if its clock is out of synchronization by more than a minute.
  NTP software or the rdate command can be used to ensure the clocks on all VISULOX PORTAL Nodes are synchronized.

VISULOX PORTAL Console configuration settings

The deployment descriptor for the VISULOX PORTAL Console web application contains settings that control the operation of the VISULOX PORTAL Console.

The deployment descriptor is the following file: **/opt/tarantella/webserver/tomcat/default/webapps/sgdadmin/WEB-INF/web.xml**

⚠ Most of the settings are context parameters, contained in <context-param> elements.
Any other settings in the web.xml file **must not** be changed.

- Only change web.xml if it is understood what is done.
- Always create and keep a backup of the original web.xml, in case it is needed to revert to a previous version.
- After changing web.xml, the VISULOX PORTAL web server **must always be restarted** for the changes to take effect.
- Changes to web.xml **only** apply for the server that is hosting the VISULOX PORTAL Console.
- The order of the XML elements contained in web.xml **must not** be change.

Number of search results

The **com.sun.tta.confmgr.DisplayLimit** context parameter enables you to configure the maximum number of search results you can display in the VISULOX PORTAL Console.

The default setting is: **150**.

If there are more results than the display limit, the VISULOX PORTAL Console displays a message. Increasing the display limit can have an effect on performance.

Set the display limit to **0** to see unlimited search results.

DNS lookups

By default, VISULOX PORTAL Service uses a query class of ANY for DNS lookups. Some firewall configurations may block this class of DNS lookups.

This can lead to problems, for example when configuring Active Directory authentication using the VISULOX PORTAL Console.

To configure the VISULOX PORTAL Console to use a query class of IN for all DNS lookups, set the **sgd.naming.dns.in_class_only** context parameter to **true**.

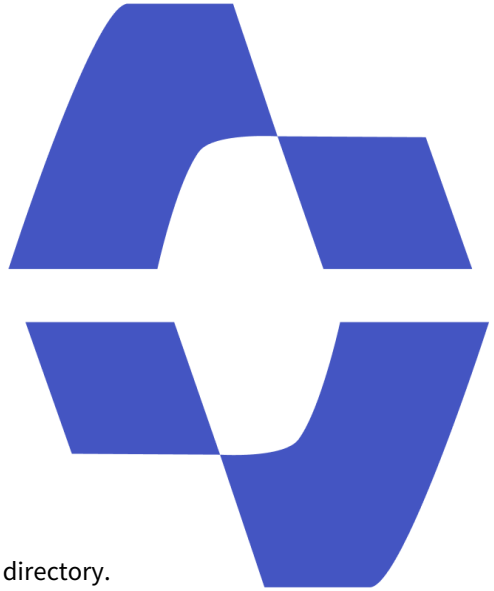
Searching and displaying LDAP data

The **com.sun.tta.confmgr.LdapSearchTimeLimit** context parameter enables you to configure the maximum time, in milliseconds, to allow for a search of a Lightweight Directory Access Protocol (LDAP) directory.

The default setting is: **0**, which means the search time is unlimited. This context parameter should only be changed if the LDAP directory servers are particularly slow.

The following context parameters are used to filter the display of LDAP data, when Local + LDAP is selected in the repository list in VISULOX PORTAL Console:

- Filters used by the navigation tree. These are the following context parameters:
  - com.sun.tta.confmgr.LdapContainerFilter
  - com.sun.tta.confmgr.LdapUserFilter



    - com.sun.tta.confmgr.LdapGroupFilter

- Filters used when searching an LDAP directory. These are the following context parameters:
    - com.sun.tta.confmgr.LdapContainerSearchFilter
    - com.sun.tta.confmgr.LdapUserSearchFilter
    - com.sun.tta.confmgr.LdapGroupSearchFilter

- Filters used when loading the LDAP assignments on the Assigned Applications tab for a user profile.
  This is the com.sun.tta.confmgr.LdapMemberFilter context parameter.

These context parameters contain the definitions of what the VISULOX PORTAL Console considers as LDAP containers, users, and groups.
These filters can be changed to improve performance, or to change the definition of these LDAP object types to match those used in your LDAP directory.

For example, if an LDAP directory uses the computer object class edit the com.sun.tta.confmgr.LdapUserFilter context parameter to remove the (!(objectclass=computer)) entry.

To avoid inconsistencies, if a filter for the navigation tree is changed, it can be also needed to change the filter used for the LDAP search.

Session timeout

The session-timeout setting defines the period of time after which the user is logged out if there is no activity, meaning no HTTP requests, in the VISULOX PORTAL Console.

The default setting is 30 minutes, to ensure unattended VISULOX PORTAL Console sessions are not left open indefinitely.

The session-timeout setting is independent of the timeout attribute for inactive user sessions, webtop-session-idle-timeout.

Working with the VISULOX Portal Console

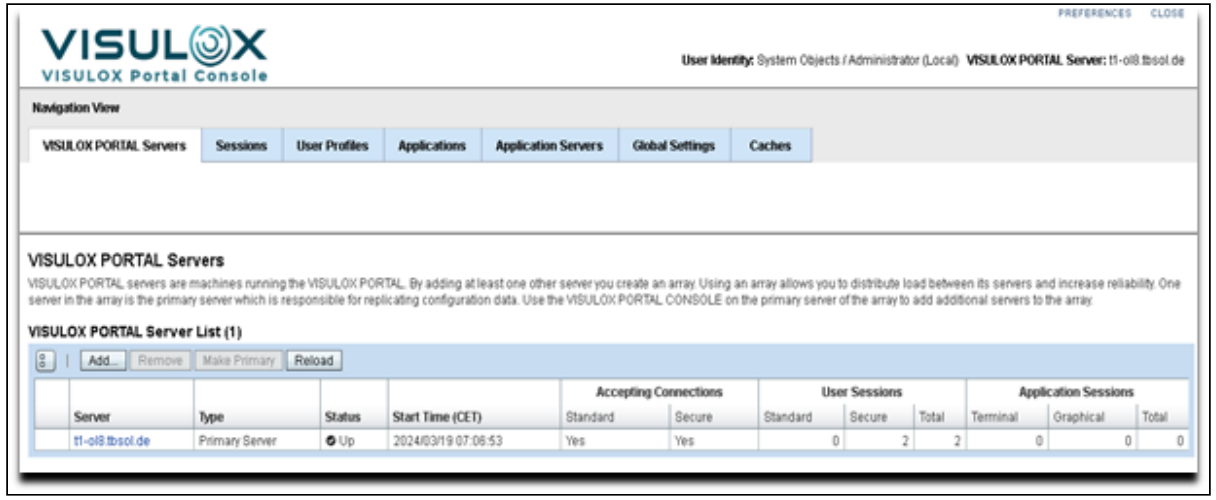
Starting the VISULOX Portal Console

The VISULOX Portal Console is a web application that enables you to configure and manage a VISULOX Portal server using a browser. The browser must have JavaScript software enabled.

The following procedure describes how to run the Portal Console from the VISULOX Portal Administrator's Workspace.

1. Start the VISULOX Portal Console.
   Click the **VISULOX PORTAL Console** link on the Workspace.

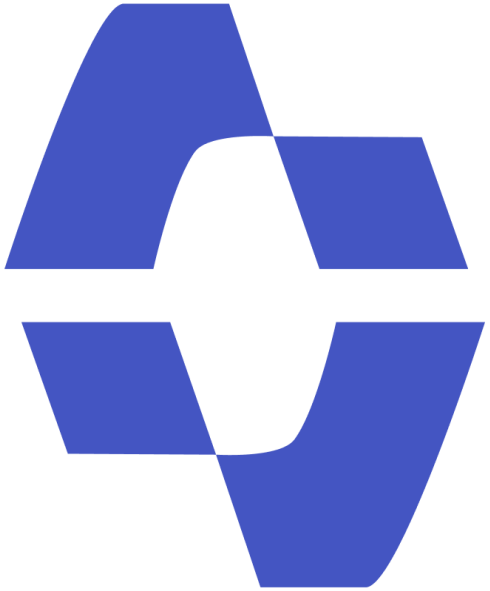
2. The VISULOX Portal Console opens in Navigation View



Creating an Application Server Object

You can use the VISULOX Portal host as an application server. An application server object for the VISULOX Portal host is created automatically when you install VISULOX Portal.

If you are using a different application server to host applications, use the following procedure to create an application server object.



1. In the VISULOX Portal Console, click the **Application Servers** tab.

2. In the content area, click **New**.
   The Create a New Object window is displayed.

3. In the **Name** field, enter the fully qualified domain name for the application server.
   For example, amitego.example.com.

4. Ensure the **Application Server** option is selected and click **Create**.
   The Create a New Object window closes and the content area is updated with the new object.

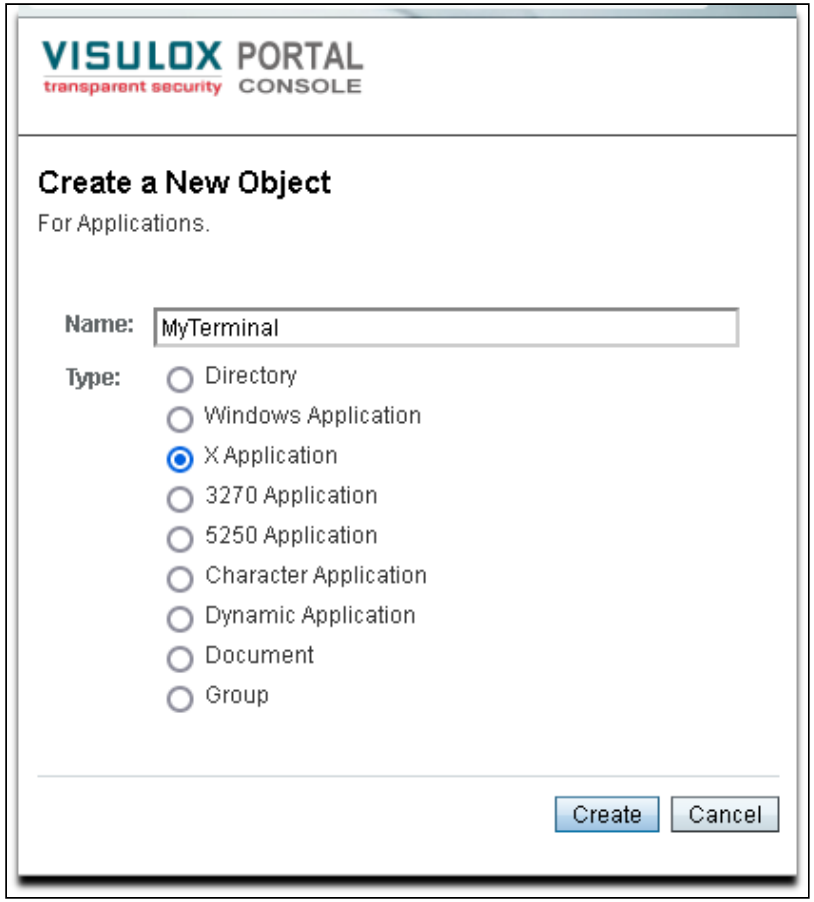
Adding an application to the VISULOX Portal Workspace

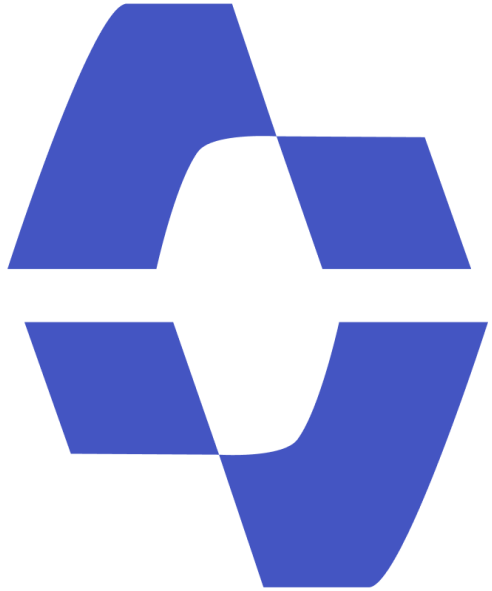
The following procedure describes how to use the VISULOX Portal Console to create an application that can be displayed through VISULOX Portal, and how to add a link for the application to the VISULOX Portal Workspace.
In the following example, you create a new X terminal application.

1. Create an application object.

   a. In the VISULOX Portal Console, click the **Applications** tab.

   b. In the content area, click **New**.
   The Create a New Object dialog box is displayed.


VISULOX PORTAL
transparent security CONSOLE
Create a New Object
For Applications.
Name:
MyTerminal
Type:
Directory
Windows Application
X Application
3270 Application
5250 Application
Character Application
Dynamic Application
Document
Group
Create
Cancel



c. In the **Name** field, enter the name of the application. For example, MyTerminal.
The name you enter is used for the application link on the Workspace.

d. Ensure the **X Application** option is selected and click **Create**.
The Create a New Object window closes and the content area is updated with the new object.

2. Configure the application object.

a. Click the **View New Object** link and configure settings for the application.
In the **Application Command** field on the **Launch** tab, enter the application command.
Use the full path of the command that runs the MyTerminal application.
For example, /usr/bin/xterm.

b. Click **Save** to save the configuration changes.

3. Assign an application server to the application object.
In this example, we use the VISULOX Portal host as the application server.

a. Click the **Hosting Application Servers** tab.

b. In the Editable Assignments table, click **Add**.
The Add Application Server Assignment window is displayed.

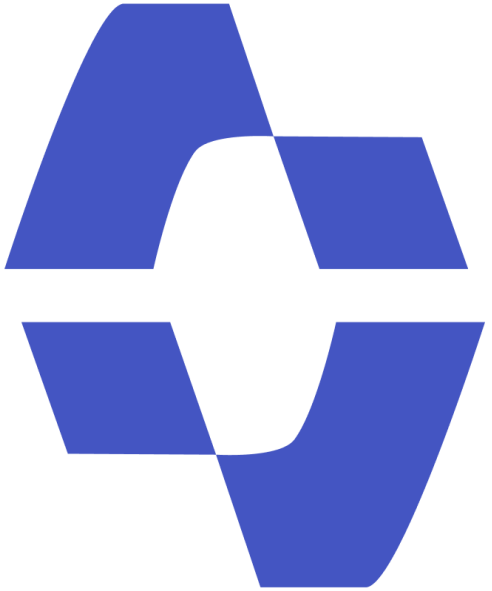
c. Select the check box next to the application server object and click **Add**.
For this example, select Tarantella server localhost, where localhost is the VISULOX Portal host.
The Effective Application Servers table is updated with the selected application server object.

4. Add your application to the Workspace.
You add your application as a member of the Applications group.
The Applications group contains the default set of applications for the workspace.

a. In Navigation View, click the **Applications** tab and click the **Applications** group.
The General tab is displayed.

b.Click the **Members** tab.

c. In the Editable Members table, click **Add**.
The Add Application Member window is displayed.



d. Select the check box for the MyTerminal application and click **Add**.
The Effective Members table is updated with the selected application.

e. The MyTerminal application is shown on your Workspace.

5. Start the application.
Click the MyTerminal application link on the Workspace.
6. Close down the application.
Use the window decoration for the application, or the Workspace Close icon.

23.1.127 VISULOX PORTAL Server Array

On the VISULOX PORTAL Servers tab in the VISULOX PORTAL Console or with the **visulox-portal array** command in a shell it is possible to group VISULOX PORTAL Servers together to form an *array*.
An array is a collection of VISULOX PORTAL Servers that share configuration information.

> ⚠ Keep in mind that VISULOX Service must be installed before the VISULOX PORTAL Service and the VISULOX PORTAL Servers can be joined to an array.

An array contains the following:

- **One primary server** – This server is the authoritative source for global VISULOX PORTAL information, and maintains the definitive copy of the organizational hierarchy
- **One or more secondary servers** – The primary server replicates information to these servers

A single, *standalone* server is considered to be the primary server in an array with no secondary servers.

VISULOX PORTAL Servers in an array may run different operating systems. However, all the array members must run the same version of VISULOX PORTAL Service.

Arrays have the following benefits:

- User sessions and application sessions are load-balanced across the array. To scale more users, simply add more VISULOX PORTAL Servers to the array.
- With more than one server, there is no single point of failure. You can decommission a server temporarily with the minimum of disruption to your users.

Configuration information, including all the objects in your organizational hierarchy, is replicated to all array members. All array members have access to all information. Users see the same Workspace and can resume applications no matter which VISULOX PORTAL Server they log in.

A VISULOX PORTAL Server is added to an array by clicking **Add** in the VISULOX PORTAL Servers List table or by using the following command in a shell:

```
visulox-portal array join --primary <server> --secondary <server>
```

23.1.128 How to export Gateway frontend certificate including key

Abstract

This article describes how to export the certificates on a Gateway, if the certificate files are not available, but needed for an update or a migration.

Convert JKS keystore to PKCS12 (5.4 or earlier)

Check if needed keystore type: PKCS12 or JKS:

Check keystore type

```
keytool -list --keystore /opt/SUNWsgdg/proxy/etc/keystore.client --storepass $(cat /opt/SUNWsgdg/etc/password)
Keystore type: PKCS12
```

```
Keystore provider: SUN

Your keystore contains 1 entry
```

Convert if needed, otherwise just copy:

Export

```
keytool -importkeystore \
  -srckeystore /opt/SUNWsgdg/proxy/etc/keystore.client \
  -srcstorepass $(cat /opt/SUNWsgdg/etc/password)
  -srcstoretype JKS \
  -destkeystore /tmp/keystore.p12
  -deststoretype PKCS12 \
  -deststorepass $(cat /opt/SUNWsgdg/etc/password)
```

Convert

```
openssl pkcs12 -in /tmp/keystore.p12 -nodes -nocerts -out private_key.pem
openssl pkcs12 -in /tmp/keystore.p12 -nokeys -out cert.pem
```

The **cert.pem** includes intermidate CA if exists.

Reuse old keystore after migration

Safe keystore to a folder outside of **/opt/SUNWsgdg/**:

Copy keystore

```
cp /opt/SUNWsgdg/proxy/etc/keystore.client /tmp/
```

```
cp /opt/SUNWsgdg/etc/password /tmp/
```

After update migrate the keystore to the new environment with the new password:

Migrate keystore

```
rm /opt/SUNWsgdg/proxy/etc/keystore.client
keytool -importkeystore -srckeystore /tmp/keystore.client -destkeystore /opt/SUNWsgdg/proxy/etc/keystore.client -srcstorepass $
(cat /tmp/password) -deststorepass $(cat /opt/SUNWsgdg/etc/password) -deststoretype PKCS12 -destkeypass  $(cat /opt/SUNWsgdg/etc/
password)
```

Related articles (on request)

(4.2.0) Configuration example for Client Site Certificates

certremove.sh Script zum Löschen von certs im Firefox

Access Certifcates on Gateway

Certificates within an VISULOX Portal Setup

(4.3.2) Configuration example for Client Site Certificates

(4.1.1) Configuration example for Client Site Certificates

(4.3.1) Configuration example for Client Site Certificates

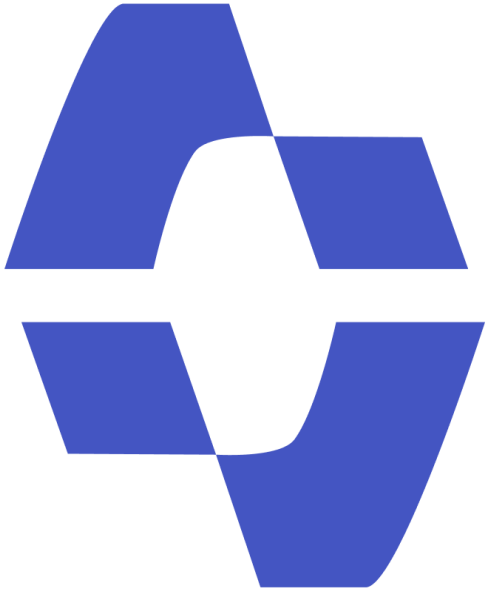
(4.3.0) Configuration example for Client Site Certificates

Configuration example for Client Site Certificates

New Spacewalk cert

List of installed Certificates

How to work with XCA (X Certifcate and Key Management) -draft-



New certificates for hmailer
tbsol.de - Root CA
Certifcates
OL9-RH9 - SHA1withRSA Issue
Certificates in OSGD Setups
Certificate Revoke List in Gateway
Installing and testing official certifcates in OSGD
How to test certificates
Configuration example for Client Site Certificates

23.1.129 How to attach Chrome/Chromium download directory to vlxtransit

Chromium and Chrome can be configured with enterprise policies. One usecase is to set the download directory to vlxtransit and disable the "save as" function.

To change the download directory system-wide in chromium, create an enterprise policy.

See: http://www.chromium.org/administrators/linux-quick-start

List of available parameters

See: https://chromeenterprise.google/policies/

vlxtransit as download directory

/etc/chromium/policies/managed/amitego.json

```
{
        "AllowFileSelectionDialogs": false,
        "DownloadDirectory": "/opt/visulox/vlxusers/${user_name}/vlxtransit"
}
```

23.1.130 How to check VISULOX PORTAL ports 443 & 5307

About

For communication between the VISULOX PORTAL Nodes in the array and to the VISULOX GATEWAY, it is essential that the ports 443 & 5307 are open.

Howto

In order to check for the ports 443 & 5307, run the below script (hostnames have to be adjusted):

```
#!/bin/bash
basepath=$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )
export basepath

PORTAL="<vlx-portal1 vlx-portal2 vlx-portal3>"
echo "-----------------------------------"
echo "use for tesing"
echo 'echo | openssl s_client -connect $host:443'
echo 'echo | openssl s_client -connect $host:5307'
echo '/opt/SUNWsgdg/bin/bin/ttahostprobe $host:443'
echo '/opt/SUNWsgdg/bin/bin/ttahostprobe $host:5307'
echo "-----------------------------------"

for host in $PORTAL
do
        com443=$(timeout 2  bash -c  "echo | openssl s_client -connect $host:443 >/dev/null 2>&1 " && echo ok || echo NOCERT)
```

```
        com5307=$(timeout 2  bash -c  "echo | openssl s_client -connect $host:5307 >/dev/null 2>&1 " && echo ok || echo NOCERT)

        answer443=$(/opt/SUNWsgdg/bin/bin/ttahostprobe $host:443)
        answer5307=$(/opt/SUNWsgdg/bin/bin/ttahostprobe $host:5307)

        echo "$(hostname) -> $host: 443=$answer443/$com443 5307=$answer5307/$com5307"
done
```

Example output

23.1.131 How to setup keepalived

About

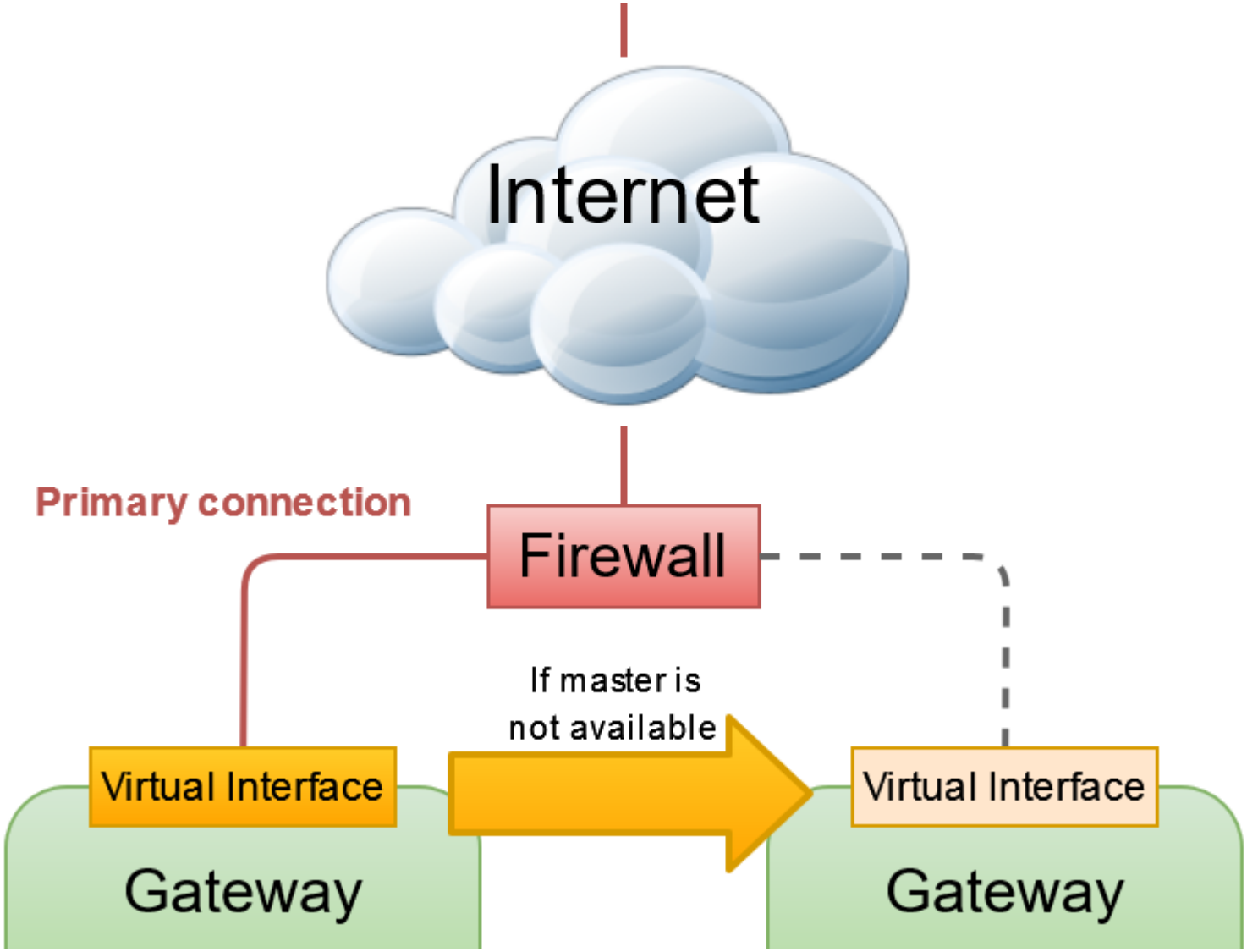
The common method to implement a single access URL for a VISULOX Portal environment and more than one VISULOX Gateway is the use of a load balancer to distribute the sessions between the Gateways.
But in some projects no load balancer is available, nevertheless a single URL is required to allow high available access to the system.

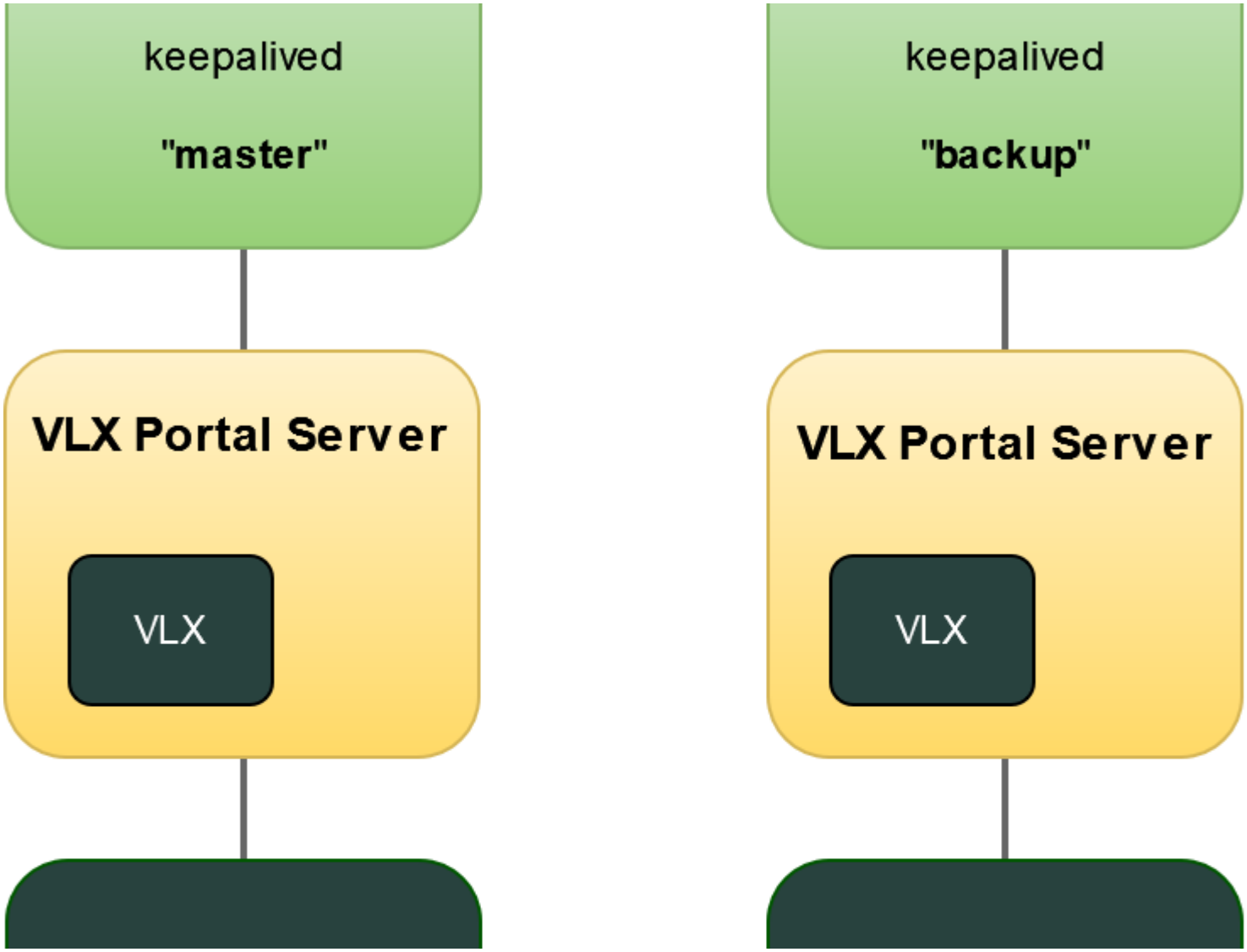
A possibility to solve this issue is to set up the keepalived daemon to provide the single URL to all portal users.
keepalived runs on all involved GW servers, checks the availability of the virtual IP address on the network and starts it on a local Secure Gateway in case of failure.

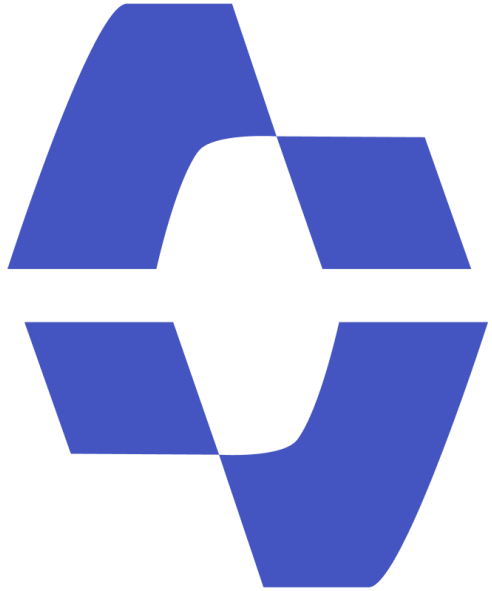
In this constellation the "**master**" Gateway provides the network interface with the virtual IP address and all sessions are running through this Gateway will be redirected by the Gateway distribution mechanism to one of the available VISULOX Portal Servers.

Then the Gateway process is not running on the "**master**" Gateway, the keepalived process disables the virtual interface.
The keepalived daemon on the "**backup**" Gateway notices that the IP address is not accessible on the network and initializes the virtual interface locally to make the portal accessible.

- About
- Installation
- Configuration
- Settings
- Creating new Access Point
- Related articles
- Websites


Internet
Primary connection
Firewall
If master is
not available
Virtual Interface
Virtual Interface
Gateway
Gateway


keepalived
"master"
VLX Portal Server
VLX
keepalived
"backup"
VLX Portal Server
VLX



Installation

The keepalived RPM is available in the Linux distribution and can be installed via dnf or yum.

The rpm package has to be installed on all VISULOX Gateway Servers:

Install

```
dnf install keepalived
```

Copy **/opt/visulox/setup/monitoring/checkPortal.sh** to the **/etc/keepalived/** directory.

Configuration

Configuration on the master GW:

Master: /etc/keepalived/keepalived.conf

```
! Configuration File for keepalived
global_defs {
   notification_email {
     sysadmin@firewall.loc
   }
   notification_email_from lb1@firewall.loc
   smtp_server localhost
   smtp_connect_timeout 30
 }

vrrp_script chk_gateway {
    script       "/etc/keepalived/checkPortal.sh -gw -e -q"
    interval 15  # check every 5 seconds
    fall 2       # require 2 failures for KO
    rise 2       # require 2 successes for OK
    timeout 4
}
vrrp_instance VI_EXTERNAL {
    state MASTER
    interface ens160
    virtual_router_id 51
    priority 255
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        192.168.10.222/24
    }
    track_script {
```

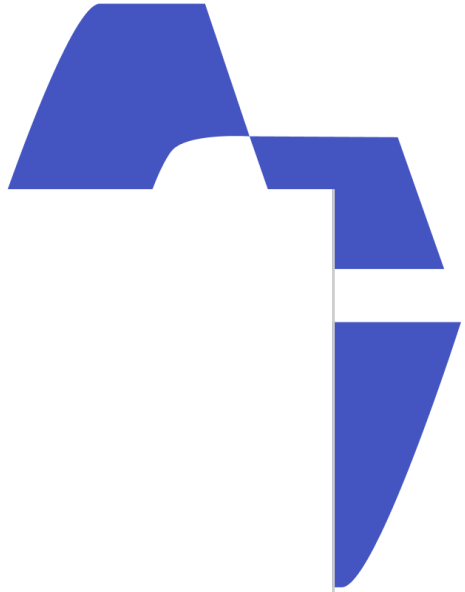
```
        chk_gateway
    }
}
```

⚠ Make sure, that no **vrrp_strict** entry is set in keepalived.conf.

Configuration on the backup GW:

Backup: /etc/keepalived/keepalived.conf

```
! Configuration File for keepalived

global_defs {
   notification_email {
     sysadmin@firewall.loc
   }
   notification_email_from lb1@firewall.loc
   smtp_server localhost
   smtp_connect_timeout 30
 }
vrrp_script chk_gateway {
    script       "/etc/keepalived/checkPortal.sh -gw -e -q"
    interval 15  # check every 5 seconds
    fall 2       # require 2 failures for KO
    rise 2       # require 2 successes for OK
    timeout 4
}
vrrp_instance VI_EXTERNAL {
    state BACKUP
    interface ens160
    virtual_router_id 51
    priority 200
```



```
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        192.168.10.222/24
    }
    track_script {
        chk_gateway
    }
}
```

Settings

SELINUX

```
chcon -t keepalived_unconfined_script_exec_t /etc/keepalived/checkPortal.sh
```

FIREWALL

```
firewall-cmd --add-rich-rule='rule protocol value="vrrp" accept' --permanent
firewall-cmd --reload
```

Start and enable

```
systemctl enable --now keepalived
```

Creating new Access Point

When VISULOX Access Points are configured, login with the keepalive - URL is not possible.

Configure a new Access Point with both GW IP addresses as source.

```
visulox config accesspoint add -name <keepalived_name> -banner "banner on login page" -connection "text on login page" -gatewayip
<gw01_ip>:<gw02_ip>
```

Related articles

(4.1.1) Gateway Session Balancing

(4.1.1) Monitoring tool: checkPortal.sh

(4.2.0) Gateway Session Balancing

(4.2.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

(4.3.0) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

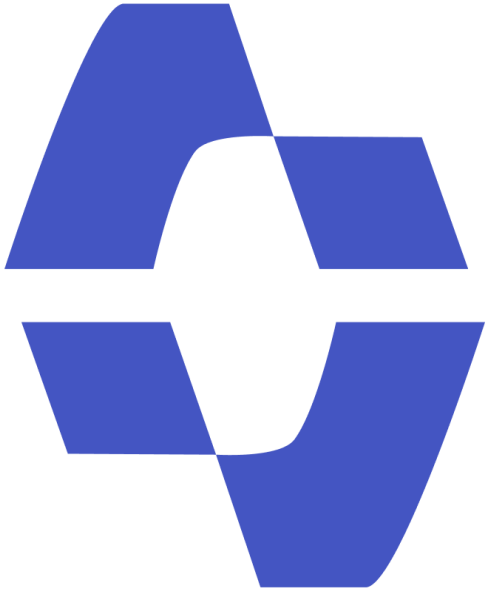
(4.3.0) How to setup keepalived

(4.3.0) VISULOX Portal maintenance mode

(4.3.1) Additional integration aspects

(4.3.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

(4.3.1) How to setup keepalived

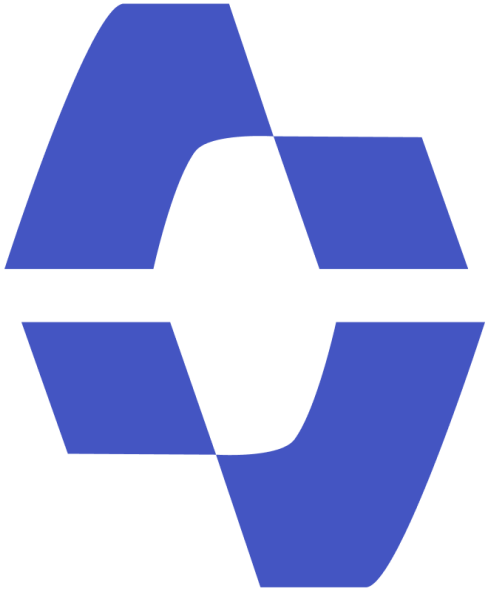


(4.3.1) Monitoring tool: checkPortal.sh
(4.3.1) VISULOX Portal maintenance mode
(4.3.2) Additional integration aspects
(4.3.2) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.3.2) How to setup keepalived
(4.3.2) Monitoring tool: checkPortal.sh
(4.3.2) VISULOX Portal maintenance mode
(4.3.3) Additional integration aspects
How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
How to setup keepalived
Monitoring tool: checkPortal.sh
VISULOX Portal maintenance mode
(4.1.1) Additional integration aspects
(4.1.1) How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration
(4.1.1) How to setup keepalived
(4.2.0) Additional integration aspects
(4.2.0) How to setup keepalived
(4.2.0) Monitoring tool: checkPortal.sh
(4.3.0) Additional integration aspects
(4.3.0) Monitoring tool: checkPortal.sh
Additional integration aspects
How to create a feedback page for Load Balancers in the VISULOX GATEWAY configuration

How to setup keepalived

Monitoring tool: checkPortal.sh

VISULOX Portal maintenance mode



Websites

- https://www.redhat.com/sysadmin/keepalived-basics
- https://docs.linuxfabrik.ch/software/keepalived.html

23.1.132 How to use Unix user profiles

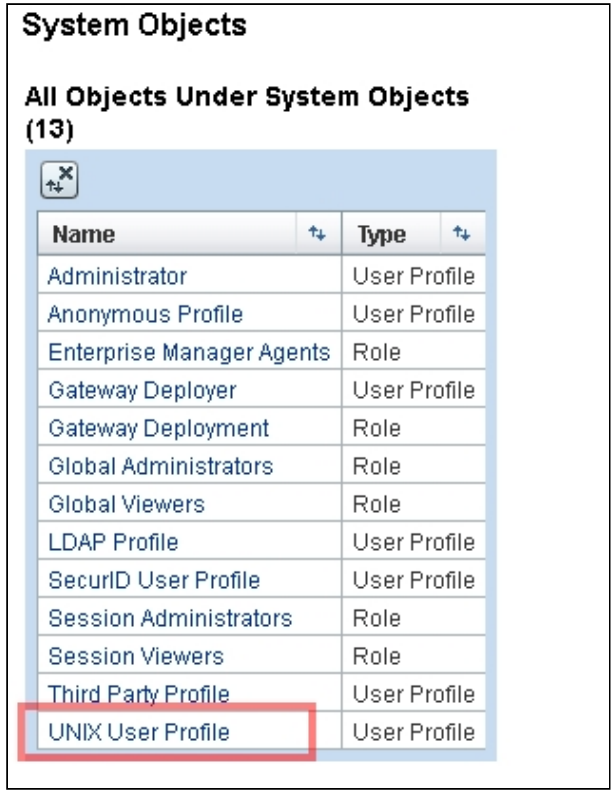
It is possible for Unix users to login via a Unix user profile without having a configured personal profile in VISULOX Portal.

Therefore the Unix user profile has to be enabled:

```
visulox-portal object edit --name "o=tarantella system objects/cn=unix user profile" --enabled 1
```

Unix users are in the group: **LOCAL_PAM_USER**. This group can be used in VISULOX policies.

To assign applications to the Unix users, the **UNIX User Profile** has to be selected in the VISULOX Portal Console.


System Objects
All Objects Under System Objects (13)
Name
Type
Administrator
User Profile
Anonymous Profile
User Profile
Enterprise Manager Agents
Role
Gateway Deployer
User Profile
Gateway Deployment
Role
Global Administrators
Role
Global Viewers
Role
LDAP Profile
User Profile
SecurID User Profile
User Profile
Session Administrators
Role
Session Viewers
Role
Third Party Profile
User Profile
UNIX User Profile
User Profile

23.1.133 Printing in VISULOX

In the default VISULOX Portal setup printing is disabled.

Follow this guide to setup and enable printing in VISULOX Portal.

- Requirements
- Enable printer in Workspace
- Check / enable printer device sharing for the client
- Example setup with PDF Viewer
- Check status
- Troubleshooting

Requirements

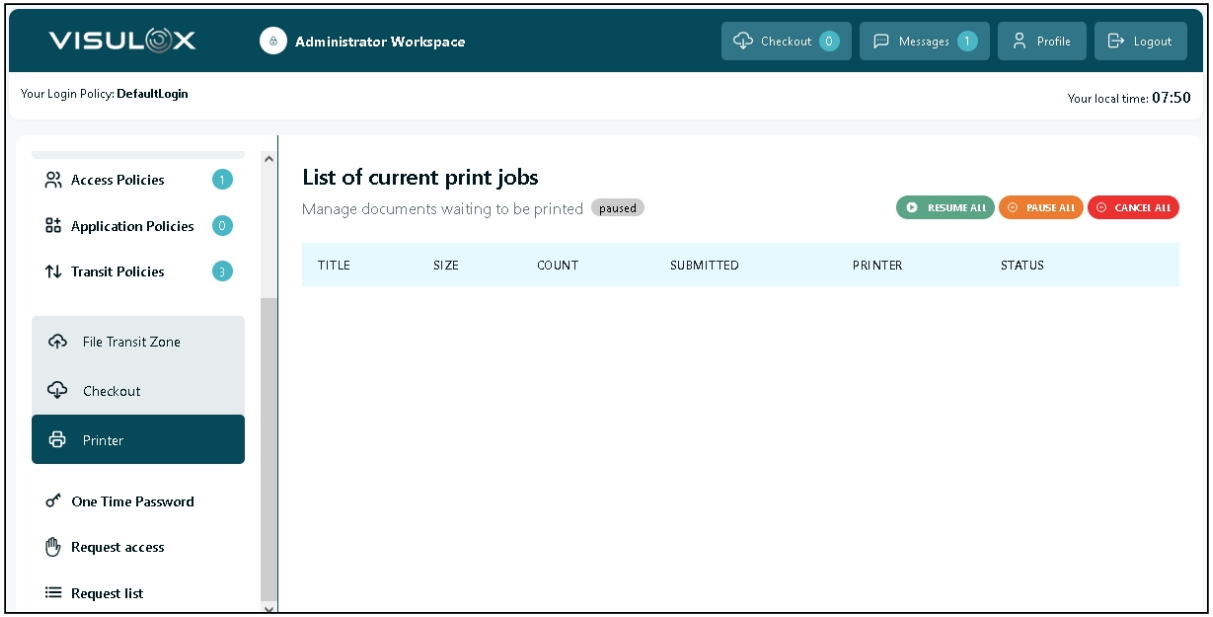
The following packages are needed for printing in VISULOX:

```
dnf install cups

systemctl start cups
systemctl enable cups

dnf install visulox-printing-4.2.0-1.el8.x86_64.rpm
```

Enable printer in Workspace

To display the list of current print jobs in the Workspace, use:

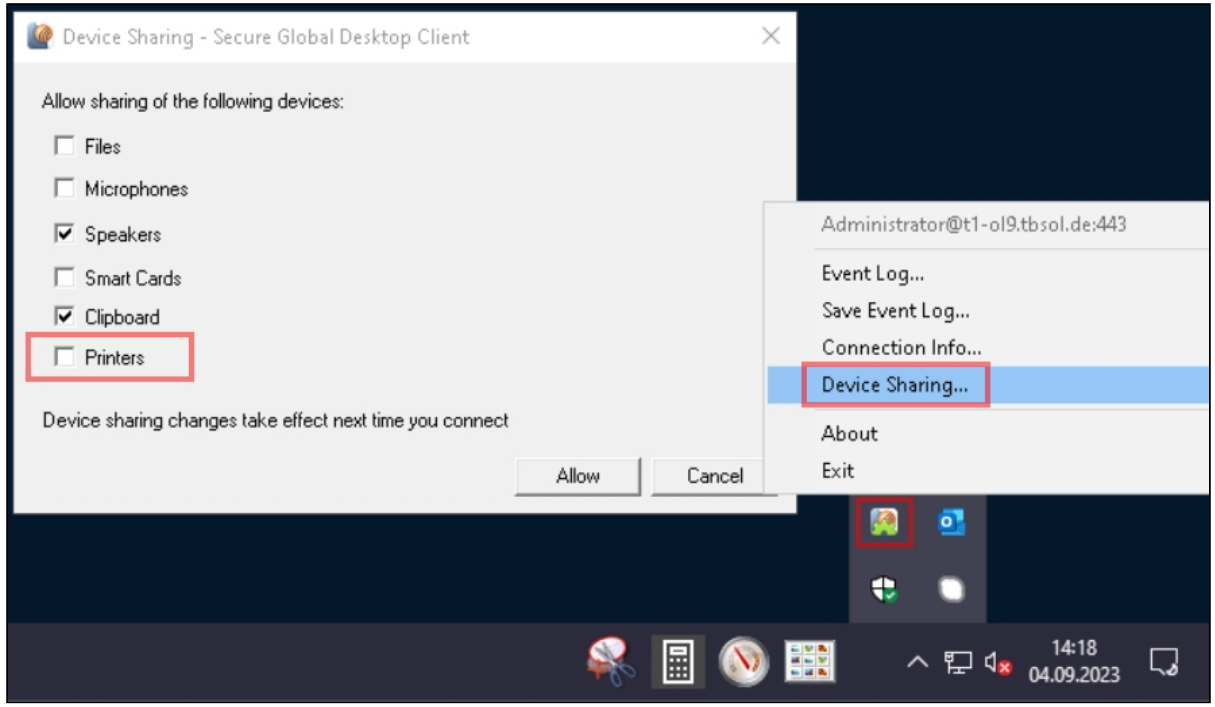
```
visulox config -name workspace.showPrinting.expand=enable
```



All print jobs are displayed here and can be paused, resumed and cancelled via the according buttons.

Check / enable printer device sharing for the client

Right click on the TCC-Client tray icon, select "**Device Sharing...**" and check "**Printers**":



Example setup with PDF Viewer

For a first test, the PDF-Viewer has been set as printer during installation.

Example test via shell:

```
lp /opt/visulox/setup/example/tiger.ps
```

```
(type lp must be /opt/tarantella/bin/lp)
```

For this test command, make sure that the following lines are not commented in **/etc/ttaprinter.conf**:

```
LPDEST=tta_pdfviewer export LPDEST #TTA_HOST=<hostname>
PATH=/opt/tarantella/bin:$PATH export PATH
```

Check status

Check the setup with the **lpstat** and **visulox-portal print status** command:

```
lpstat -p -d
printer tta_pdfviewer is idle.  enabled since Thu 07 Sep 2023 07:04:58 AM CEST
no system default destination

visulox-portal print status
<host.domain>:
 - Printing services available
 - Jobs spooled: 0
```

Troubleshooting

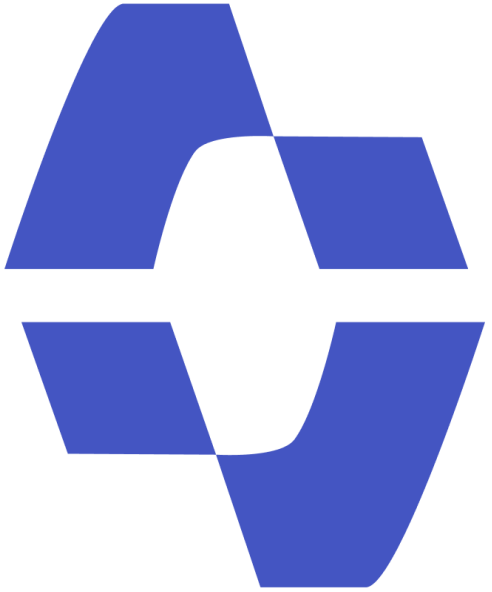
If print jobs are not shown in Workspace as expected, use the following command:

```
visulox-portal print cancel --all
```

Delete files in the spool folder:

```
rm -rf /opt/tarantella/var/spool/*
```

Then restart the services.



Printing configuration VISULOX Portal / application server

- Actions on VISLOX Portal (each array member)
    - Install CUPS / VISULOX Printing
    - 3 queues are defined automatically after installation of VISULOX Printing
- Actions on application servers
    - Install CUPS
    - Printer queues
    - Define printer
    - Change DeviceURI (stop cups)
    - Set of env variable LPDEST

Actions on VISLOX Portal (each array member)

Install CUPS / VISULOX Printing

```
dnf install cups

dnf install visulox-printing-4.0.0-1.el8.x86_64.rpm

systemctl start cups
systemctl enable cups
```

3 queues are defined automatically after installation of VISULOX Printing

visulox-printing-<*version*>.rpm

- tta_printer
- tta_pdfprinter

- tta_pdfviewer

⚠ Port 631 must be open in the firewall.

/etc/cups/cupsd.conf:

```
Listen localhost:631 -> Listen *:631
```

Allow remote printing in /etc/cups/cupsd.conf:

```
<Location />
  # Allow remote access...
  Order allow,deny
  Allow all
</Location>
```

Actions on application servers

Install CUPS

```
dnf install cups

systemctl start cups
systemctl enable cups
```

Printer queues

On application servers use the **/opt/tarantella/bin/scriptsprtinstall.en.sh** script to create printer queues for each array member (!):

```
sh prtinstall.en.sh

    [--ttahost SGD_hostname]
    [--ttaprinter printer_name]
    [--appprinter printer_name]
    [--uninstall [printer_name]]
    [--cups y | n | auto]
    [--cupsconf filename]
    [--cupscontrol filename]
    [--gsbindir gs_bin_dir]
    [--append]
    [--help]
```

Default to use:

--ttahost	DNS name VISULOX Portal Server reachable from application server
--appprinter	Name of the printer queue on the application server (redirects the print file to tta_printer on VISULOX Portal
--append	Add new printer queues (not replace)

Define printer

/etc/cups/printers.conf:

```
<Printer tta_printer>
```

```
AuthInfoRequired none
Info tta_printer
DeviceURI ipp://<DeviceURI>:631/printers/tta_pdfviewer
Type 6
Accepting Yes
Shared No
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy stop-printer
</Printer>
```

Change DeviceURI (stop cups)

DeviceURI ipp://*<DeviceURI>*:631/printers/tta_pdfviewer

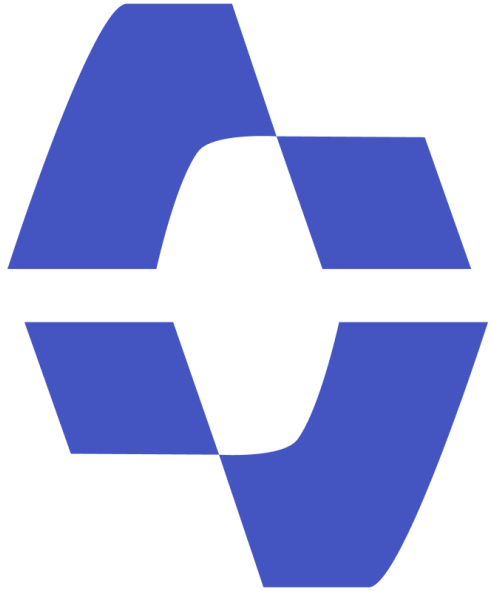
After login on the application server (VISULOX Portal session), the default printer is set to the right queue, which points to the tta_printer queue on VISULOX Portal running the user's emulator session.

Set of env variable LPDEST

```
/etc/ttaprinter.conf
```

23.1.134 Service fingerprinting via expect script

VISULOX expects (to a certain extend) to be in secure environment.
Secure connections are used by VISULOX, but peer connections are not checked in some cases.



Therefore **vlxRdpFingerprint.exp** can be used (/opt/tarantella/var/serverresource/expect/) in Windows applications.

The fingerprints are stored in /opt/tarantella/var/fingerprint/.

This expect script is available since VISULOX version 4.1.0. In older versions the script has to be added manually.

Expect check:

In the expect layer the fingerprint of host:port is checked against known fingerprints before starting the application.
Will be blocked if changed.

Service fingerprinting montoring:

In the service layer the fingerprint of host:port is periodically checked against known fingerprints.
Throws event if not available or changed.

23.1.135 Configuration example for Client Site Certificates

Configuration for client certificate authentication

Server side

Gateway certificate import

Gateway certificate import

```
visulox-gateway sslkey import --certfile <certificate.pem> \
--keyfile <private_key.key> \
--cacertfile <certificate.pem> \
--alwaysoverwrite
```

```
visulox-gateway stop
visulox-gateway start
```

Create and/or check user

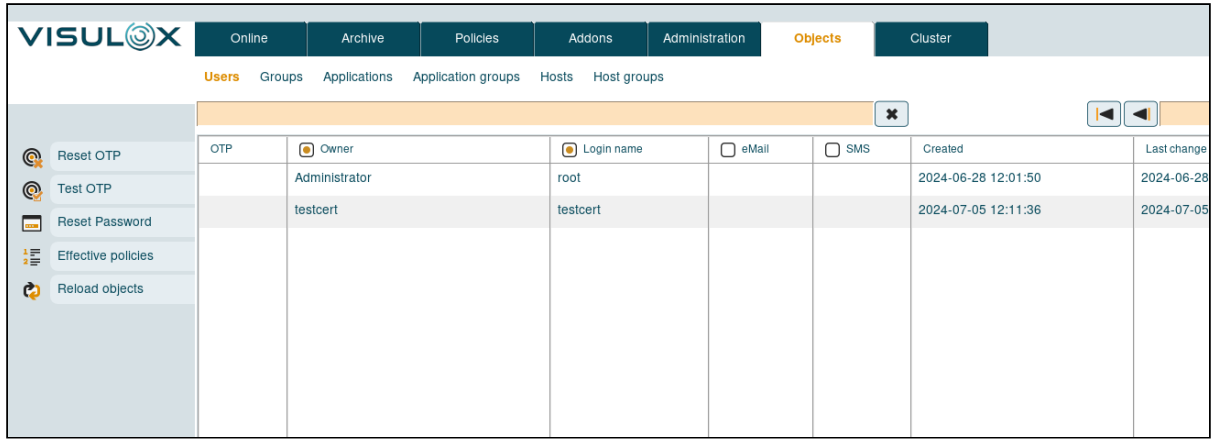
1. Add Unix user (testcert)
2. Create profile in VISULOX-Portal

For example:

Type:	User Profile
Location:	User profiles / amitego / support
Login user:	testcert

Create certificate for this user (testcert).

Check if user was imported correctly:



Client certificate

Generating private key

```
openssl req -x509 -newkey rsa:4096 -keyout myKey.pem -out cert.pem -days 365 -nodes

Generating a RSA private key
.....................................................................................+++
.........................................+++
writing new private key to 'myKey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:DE
State or Province Name (full name) []:BW
Locality Name (eg, city) [Default City]:Stuttgart
Organization Name (eg, company) [Default Company Ltd]:amitego
Organizational Unit Name (eg, section) []:support
Common Name (eg, your name or your server's hostname) []:testcert
Email Address []:xxx@amitego.com
```

Export

```
openssl pkcs12 -export -out keyStore.p12 -inkey myKey.pem -in cert.pem

  Enter Export Password:****
  Verifying - Enter Export Password:****
```

Import

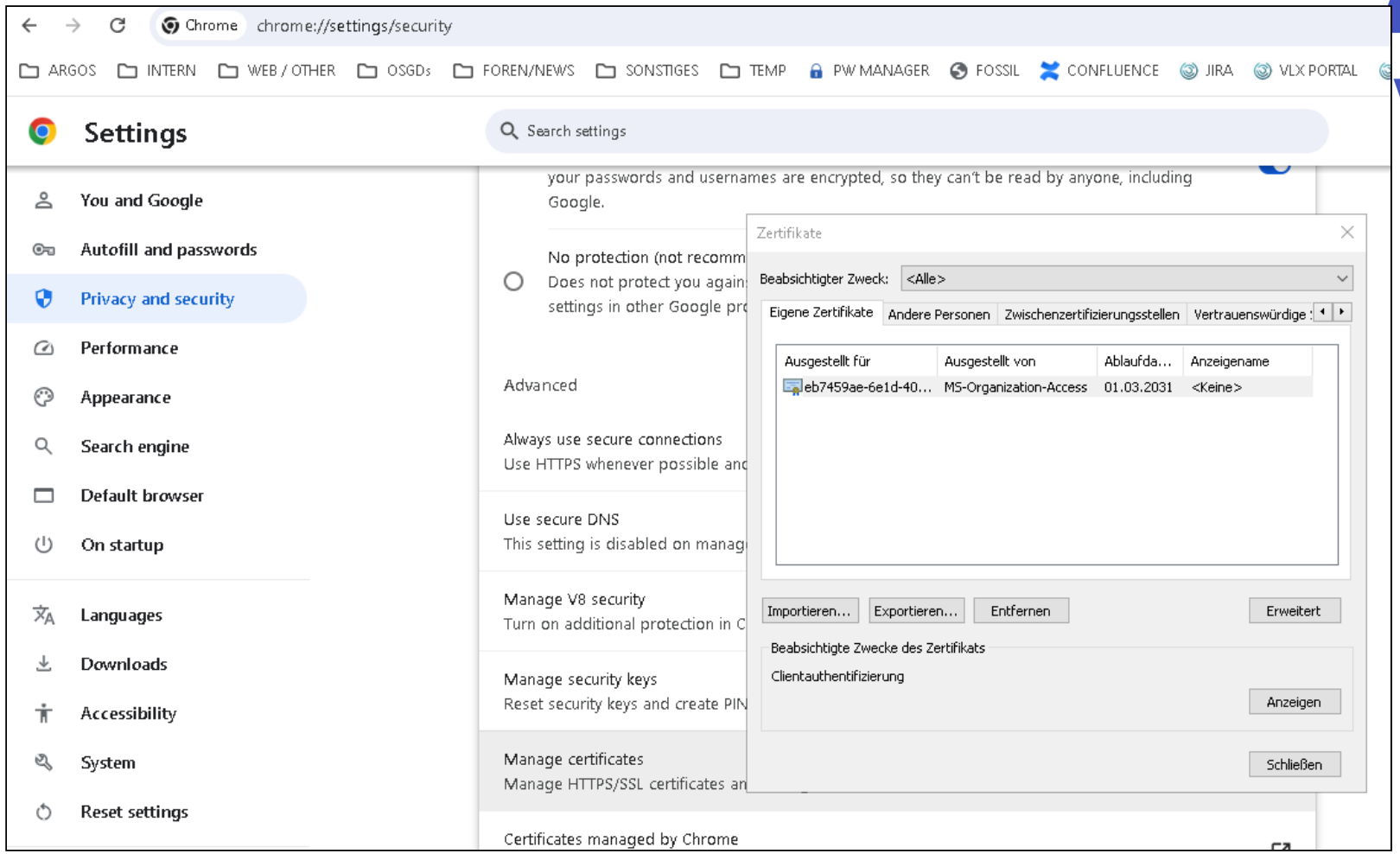
```
visulox-gateway clientcert import --certfile cert.pem --alias mycert
  Certificate was added to keystore

visulox-gateway config edit --services-clientcerts required
  You will need to restart VISULOX Gateway for this change to take effect

visulox-gateway stop
visulox-gateway start
```

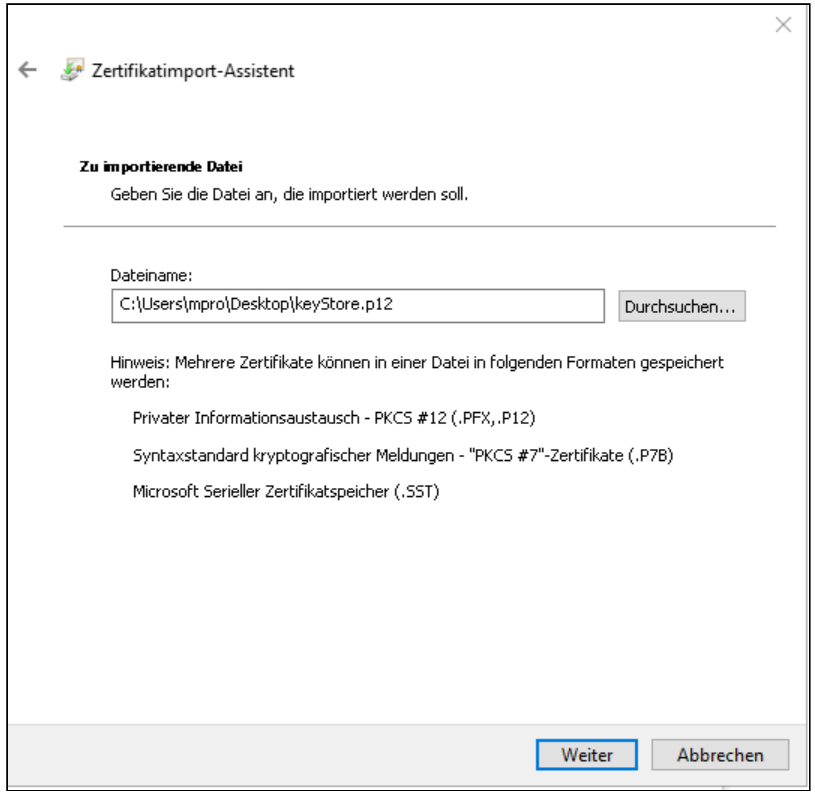
```
visulox-portal config edit --tarantella-config-signed-data-auth-enabled 1
  Changed attribute tarantella-config-signed-data-auth-enabled.
visulox-portal config edit --login-thirdparty 1
  Changed attribute login-thirdparty.
visulox-portal config edit --login-thirdparty-nonens 1
  Changed attribute login-thirdparty-nonens.
visulox-portal config edit --login-thirdparty-ens 1
   Changed attribute login-thirdparty-ens.

visulox-portal restart

visulox config -name portal.clientcertificate=true
visulox portal attach
visulox-portal restart
```

If there are issues with the usermapping, set also **visulox config -name api.portal.auth.external.strict=false** and try again.

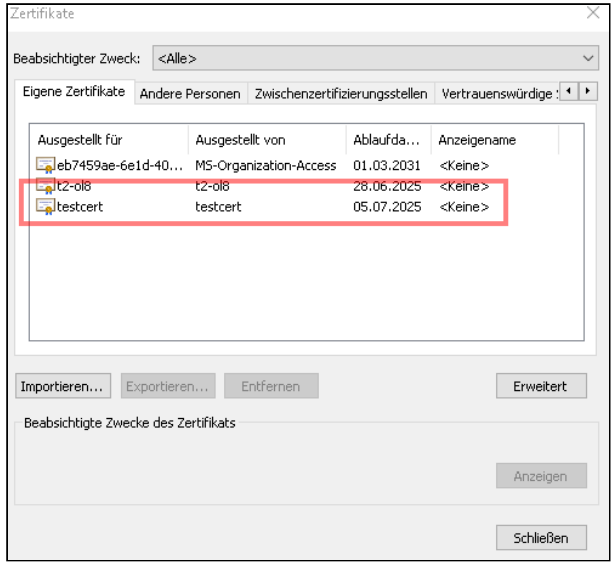
Client side

For example add the exported certificate to Chrome (keyStore.p12):

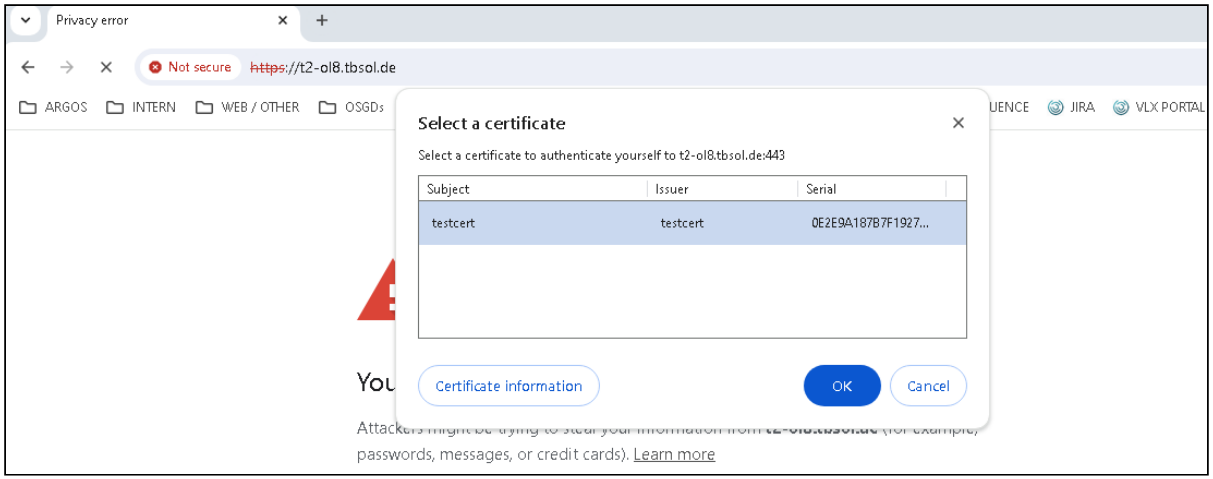

Chrome
chrome://settings/security
ARGOS
INTERN
WEB / OTHER
OSGDs
FOREN/NEWS
SONSTIGES
TEMP
PW MANAGER
FOSSIL
CONFLUENCE
JIRA
VLX PORTAL
Settings
Search settings
You and Google
Autofill and passwords
Privacy and security
Performance
Appearance
Search engine
Default browser
On startup
Languages
Downloads
Accessibility
System
Reset settings
your passwords and usernames are encrypted, so they can't be read by anyone, including Google.
No protection (not recomm
Does not protect you again
settings in other Google pr
Advanced
Always use secure connections
Use HTTPS whenever possible and
Use secure DNS
This setting is disabled on manag
Manage V8 security
Turn on additional protection in C
Manage security keys
Reset security keys and create PIN
Manage certificates
Manage HTTPS/SSL certificates an
Certificates managed by Chrome
Zertifikate
Beabsichtigter Zweck:
<Alle>
Eigene Zertifikate
Andere Personen
Zwischenzertifizierungsstellen
Vertrauenswürdige
Ausgestellt für
Ausgestellt von
Ablaufda...
Anzeigename
eb7459ae-6e1d-40...
MS-Organization-Access
01.03.2031
<Keine>
Importieren...
Exportieren...
Entfernen
Erweitert
Beabsichtigte Zwecke des Zertifikats
Clientauthentifizierung
Anzeigen
Schließen



Certificate imported:

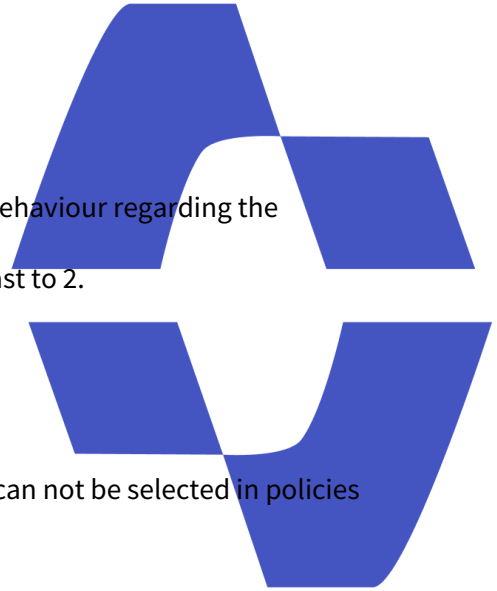

Zertifikate
Beabsichtigter Zweck:
<Alle>
Eigene Zertifikate
Andere Personen
Zwischenzertifizierungsstellen
Vertrauenswürdige
Ausgestellt für
Ausgestellt von
Ablaufda...
Anzeigename
eb7459ae-6e1d-40...
MS-Organization-Access
01.03.2031
<Keine>
t2-ol8
t2-ol8
28.06.2025
<Keine>
testcert
testcert
05.07.2025
<Keine>
Importieren...
Exportieren...
Entfernen
Erweitert
Beabsichtigte Zwecke des Zertifikats
Anzeigen
Schließen

Login with certificate



23.1.136 VISULOX 4 - known issues

- **Access Management**
  - VISULOX 2FA is not supported in case of a Third Party Authentication.
  - 2FA & Unix user profiles without a profile in datastore are not supported (Created profiles in datastore based on Unix users are supported).
  - Reset OTP keys via VISULOX Cockpit is not available for Unix users.
- **File Transit**
  - Files with non-ASCII characters sometimes are presented wrong.
  - File names with special chars like "\ / : * ? " <> |" that are transferred to Windows servers will be substituted.
  - VISULOX FTPD does not support IPv6.
  - Depending on the Tomcat version, the file size is limited to 4GB.



  - If two persons are using the same user name to connect to a Unix application server, this can lead to an undefiined behaviour regarding the Transit Zone.
  - For File Transfer within Command Connect, MaxSessions in sshd_config on the destination server has to be set at least to 2. With a MaxSession setting of 1, only the FT Client can be used without Command Connect.
- **Cooperation / Assistance**
  - If the source and destination displays in a cooperation have different keyboard layouts, this can cause side effects.
  - Dual Control is currently only possible in observation mode for members.
- **Objects / Datastore**
  - Character and doc applications are displayed in VISULOX Cockpit / Online and Filter Objects, but these applications can not be selected in policies and can not be recorded, locked, etc.
  - Objects in the datastore do not support the following special chars: "/ ; #=\+" for VISULOX PORTAL Administrators.
- **VISULOX Portal**
  - The VISULOX PORTAL Console is not supported on Safari browsers.
  - After the command visulox-portal discover gateway –local, the following entries are missing in /opt/SUNWsgdg/httpd/httpd-default/conf/extra/gateway/httpd-gateway.conf: SSLProxyCheckPeerExpire off and ProxyPass /lb_endpoint.html.
  - Secondary VISULOX Portal servers must be online and have a connection to the Primary to attach VISULOX.
  - TTAXPE and RDP session must have the same color depth.
  - XRDP on VISULOX Portal servers is not supported (VISULOX Portal supports x11 native, so it makes no sense using an x11-client to map RDP to x11 from a server which maps x11 to RDP).
  - Redrawing issues with session controller in seamless RDP sessions.
  - Launching Windows applications using the HTML5 client in a Firefox private window is not supported.
  - HTML5 applications closed via X on the tab will still be displayed as running in the Workspace.
  - Enhanced graphics application setting has to be enabled for HTML5 client connections to resolve performance issues.
  - Dynamic applications are not supported in VISULOX 4.
- **Miscellaneous**
  - Time zone interval for Bangalore / India is not a full hour.
  - Nested groups are not supported.
  - In a checked out ZIP archive special chars sometimes are not displayed properly on the info page.
  - Effective Policies in Cockpit / Online for Access and Application Policies are only displayed completely, if the Access Point has been provided.
  - Linux file command is not reliable on Oracle Linux 8. A workaround is available on request.

- Platform with SELINUX and Unix vlxtransit based on NFS Home Shares works only with NFS4.2.
- AD LDAP paging with a pagesize of 100 can cause issues (an LDAP paging configuration parameter has been implemented).
- Printing with HTML5 client requests a valid VISULOX-Portal certificate.

23.1.137 Authentication with Microsoft Entra

Microsoft Entra can be used to authenticate users to VISULOX environments.

To achieve this some preconditions have to be met.

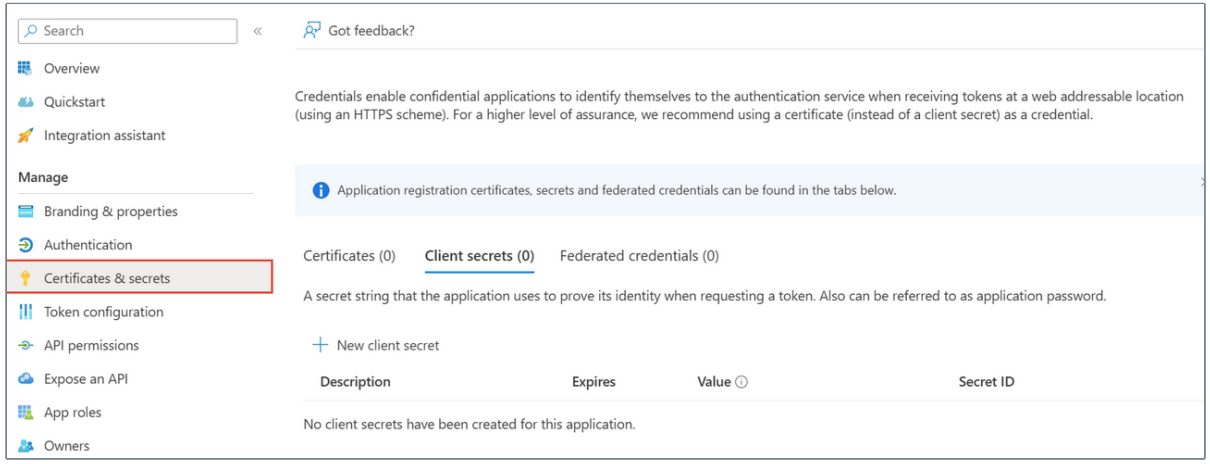
- **A VISULOX application must be created in Microsoft Entra.**
- **Microsoft Entra authentication has to be enabled on the VISULOX Portal server**
- **Microsoft Entra parameters have to be entered in VISULOX**

- Microsoft Entra - VISULOX application settings
- Settings on the VISULOX Portal server
- VISULOX login with Microsoft Entra authentication
- VISULOX Portal server with proxy

Microsoft Entra - VISULOX application settings

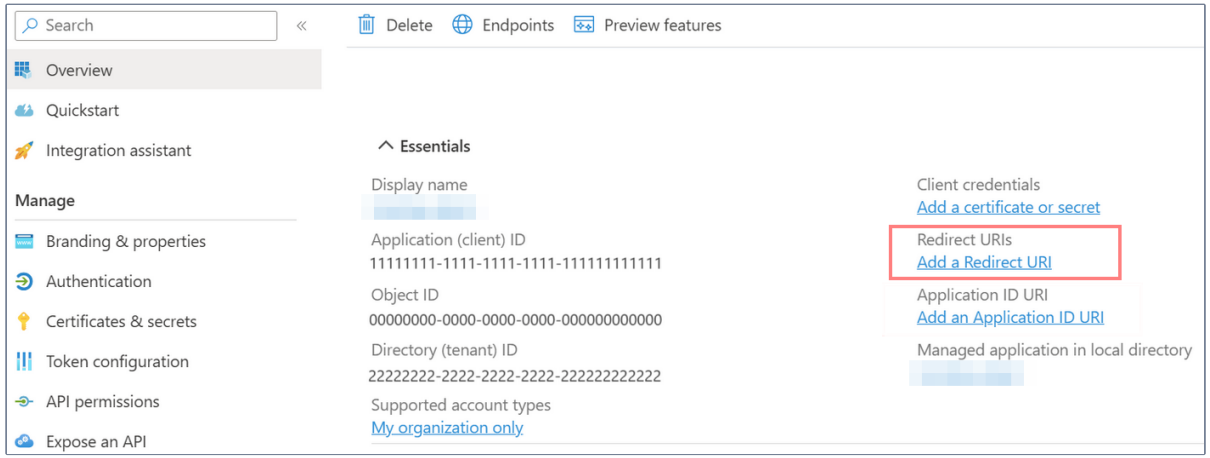
Once the Entra application is setup, two entries are needed:

- **Certificates & secrets:**



The secret / key has to be set, for example: aVl8Q~IhnT8fiLsO1qOB9AV5Em1vuasNOxCS3aGD

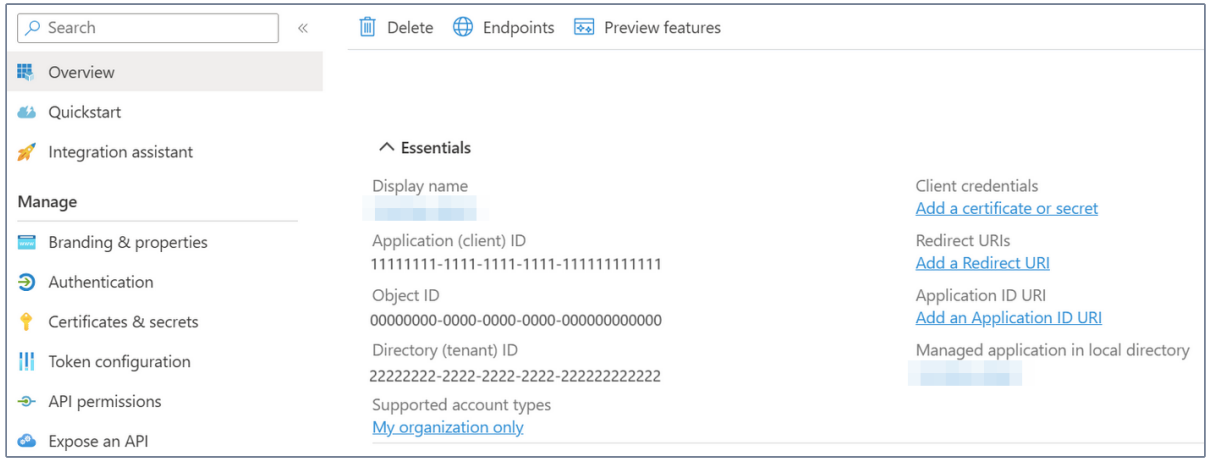
- **Authentication:**



As Redirect URL, the VISULOX Portal URL must be entered, for example: https://vlx-portal-host.domain/visulox/entra/auth/redirect

The following information is now available in the Entra application:

- Application (client) ID, for example: c157417f-d7a8-4147-9b09-d3bdc2d21b55
- Directory (tenant) ID, for example: 3e1ccbff-07dc-40f7-9843-1323aaad2376
- Secret / key, for example: aVl8Q~IhnT8fiLsO1qOB9AV5Em1vuasNOxCS3aGD
- VISULOX Portal URL, for example: https://vlx-portal-host.domain/visulox/entra/auth/redirect



Settings on the VISULOX Portal server

The following parameters have to be set in VISULOX for Microsoft Entra :

```
visulox config 3rdparty -enabled true
visulox config edit -name portal.entra.enabled=true

visulox config edit -name portal.entra.clientid=c157417f-d7a8-4147-9b09-d3bdc2d21b55
visulox config edit -name portal.entra.secret=aVl8Q~IhnT8fiLsO1qOB9AV5Em1vuasNOxCS3aGD
visulox config edit -name portal.entra.tenantid=3e1ccbff-07dc-40f7-9843-1323aaad2376
visulox config edit -name portal.entra.nameclaim=preferred_username
```

Check parameters with:

```
visulox config -name portal.entra
    ------------------------------------------------------------------------
    | changed | key                    | value                             |
```

```
-------------------------------------------------------------------------
| changed | portal.entra.clientid | c157417f-d7a8-4147-9b09-d3bdc2d21b55 |
| changed | portal.entra.enabled  | true                                 |
| changed | portal.entra.homepage | https://vlx-portal-host.tbsol.de     |
| changed | portal.entra.nameclaim| preferred_username                   |
| changed | portal.entra.secret   | Concealed for Confidentiality        |
| changed | portal.entra.tenantid | 3e1ccbff-07dc-40f7-9843-1323aaad2376 |
-------------------------------------------------------------------------
```

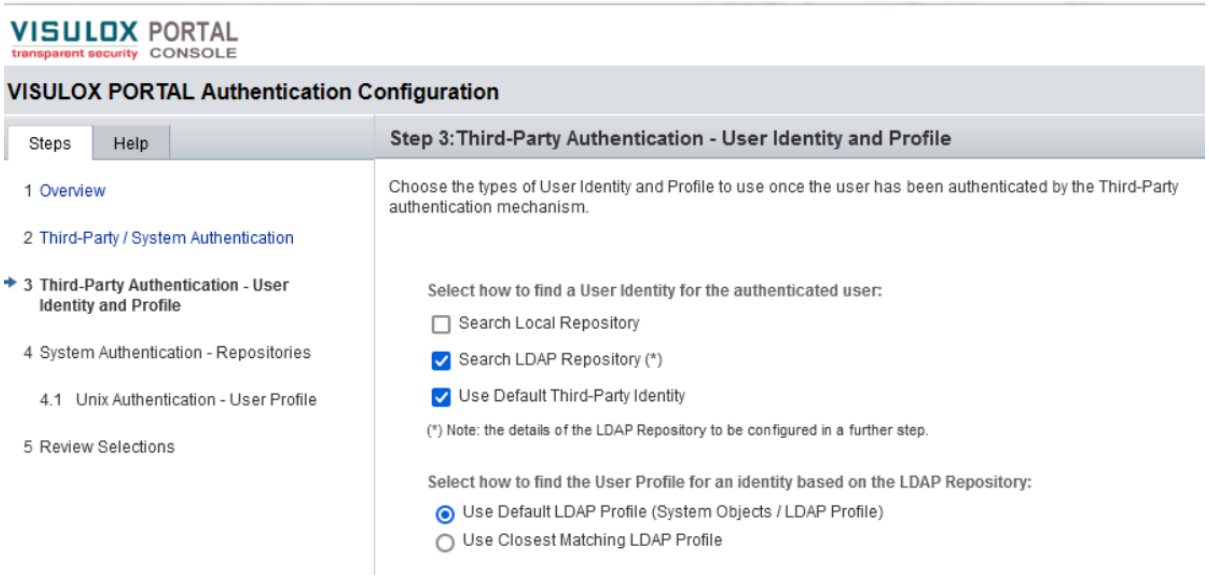
The **nameclaim** parameter can be set to the according available registered claims in Microsoft Entra.

portal.entra.home is set by default, but can be set in special cases to an explicit URL.

After these adjustments VISULOX must be attached and the VISULOX Portal has to be restarted:

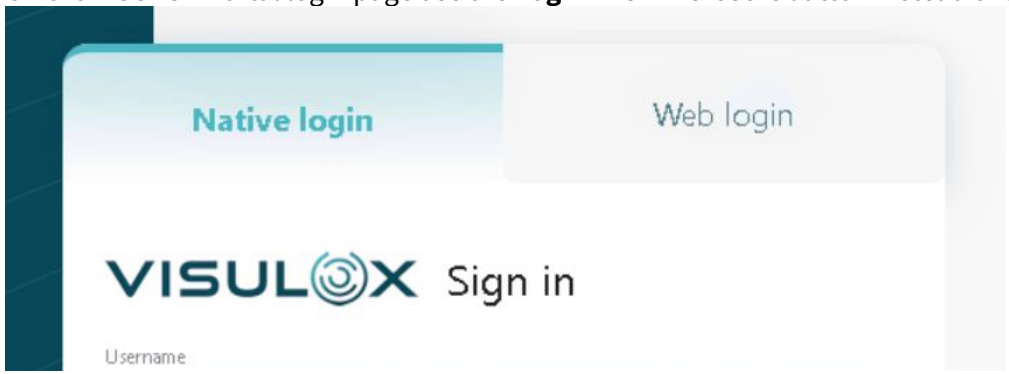
```
visulox portal attach
visulox-portal restart
```

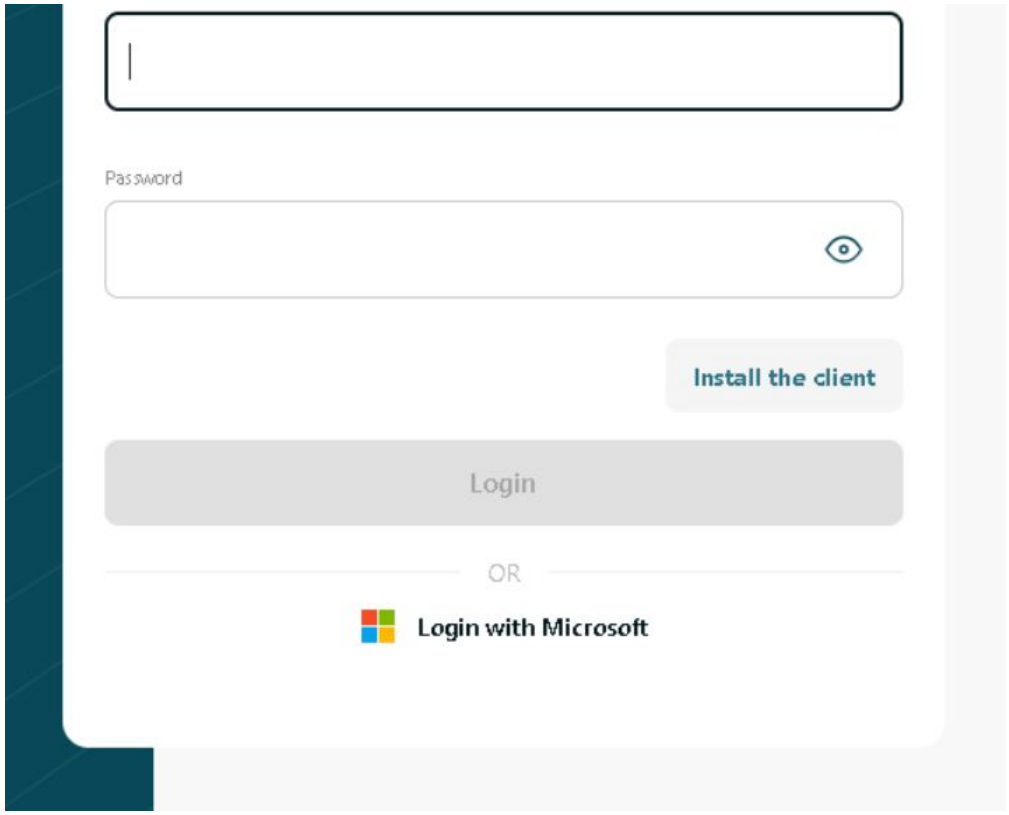
Example settings in VISULOX Portal Console using LDAP/AD and Third-Party:



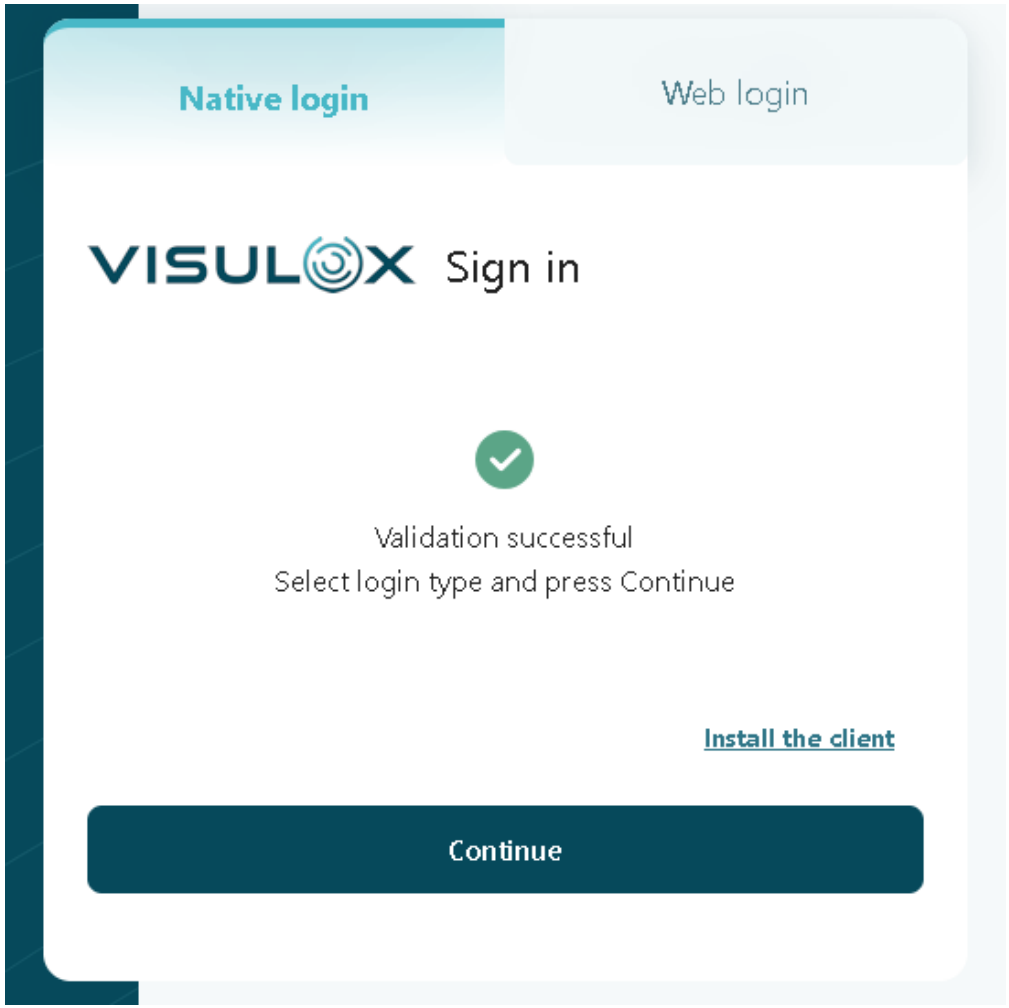
VISULOX login with Microsoft Entra authentication

1. On the VISULOX Portal login page use the **Login with Microsoft** button instead of directly entering username / password:





2. Use your Microsoft credentials in the opened Microsoft login mask.
3. If the login was successful, the VISULOX login page is displayed again:



4. Press **continue** to open the Workspace.

VISULOX Portal server with proxy

If the VISULOX Portal server needs a proxy for internet access, the the following configuration is necessary:

/opt/tarantella/webserver/tomcat/default/bin/setenv.sh:

```
CATALINA_OPTS+=" -Dhttp.proxyHost=<proxy> -Dhttp.proxyPort=3128"
CATALINA_OPTS+=" -Dhttps.proxyHost=<proxy> -Dhttps.proxyPort=3128"
```

If the **internal** communication should not use the proxy, add:

```
CATALINA_OPTS+=" -Dhttp.nonProxyHosts='*.internal'"
CATALINA_OPTS+=" -Dhttps.nonProxyHosts='*.internal'"
```

23.1.138 How to change the VISULOX Portal Favicon

The Favicon can be changed with the following command:

```
visulox config icons -favname <path_to_icon>
```

For best results the icon should be in .ico, .png or .gif picture format.

> It can not be guaranteed that any picture format will work with supported/unsupported browsers.

> Favicons are cached on the clientside, changes may not immediately be visible, use curl/wget to check.

23.1.139 Browser agent switch for TCC file or URL call

Some browsers have a limit for get requests of 2k, other browsers have no limit.
Currently we limit the start via browser for **all** browsers, if the URL is longer than 2k.

Our findings so far:

Browser / OS	Limit
Firefox on Windows	no limit (tested up to 16k)
Chrome / Chromium / Edge on Windows	limit 2k
Chrome / Chromium / Edge on Mac	no limit

This should be changed according to each browser, that is used:

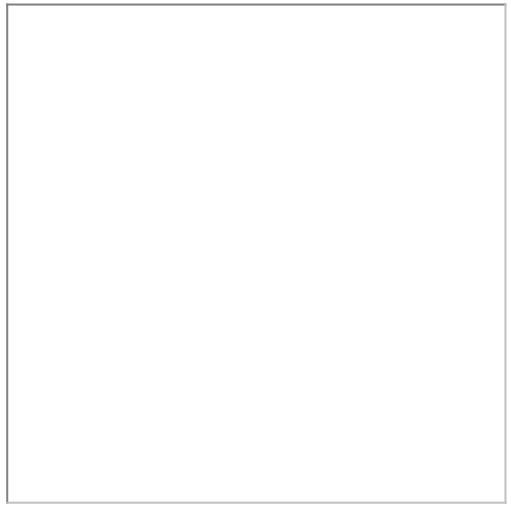
```
visulox config -name  portal.clients.launch
    ------------------------------------------------------------------
    | changed | key                       | value                      |
    ------------------------------------------------------------------
    | changed | portal.clients.launch.0 | Windows NT.+Firefox:20000 |
    | changed | portal.clients.launch.1 | Macintosh:20000           |
    |         | portal.clients.launch.2 |                           |
    |         | portal.clients.launch.3 |                           |
    |         | portal.clients.launch.4 |                           |
    |         | portal.clients.launch.5 |                           |
    |         | portal.clients.launch.6 |                           |
```

```
|         | portal.clients.launch.7 |                          |
|         | portal.clients.launch.8 |                          |
|         | portal.clients.launch.9 |                          |
-------------------------------------------------------------
```

Format of the value is: **<regexp>:<integer>**

- **regexpr**: Regular expression for the browser agent
- **integer**: Byte up to the URL method that is used

23.1.140 Web server basic authentication with VISULOX



Steps to enable web server basic authentication with VISULOX

- Generate the web server password file:

```
cd /opt/tarantella/webserver/apache/default/bin/
./htpasswd -b -c /etc/websrvpasswd test letmein
```

- Change the permissions on the web server password file. The password file must be accessible by the ttaserv user.
  Run the following commands:

```
chmod 440 /etc/websrvpasswd
chown ttaserv:ttaserv /etc/websrvpasswd
```

- Create a back-up copy of the Apache configuration file:

```
cd /opt/tarantella/webserver/apache/<version>/conf/
cp httpd.conf httpd.conf.bkp
```

- Edit the Apache configuration file to protect the /sgd URL:

```
<Location "/visulox/basic/">
AuthType Basic
AuthBasicProvider file
AuthUserFile /etc/websrvpasswd
AuthName secure
Require valid-user
</Location>
```

The Apache configuration file can be found here: **/opt/tarantella/webserver/apache/default/conf/httpd.conf**.

- Create a back-up copy of the Tomcat configuration file:

```
cd /<tarantella install path>/tarantella/webserver/tomcat/default/conf/
cp server.xml server.xml.bkp
```

- The Tomcat component of the VISULOX Portal web server must be configured to trust the web server's authentication.
  Edit the Tomcat configuration file - add "**tomcatAuthentication="false**" to the configuration of the AJP 1.3 Connector:

```
<!-- The SGD AJP connector -->
<Connector protocol="AJP/1.3"
               address="127.0.0.1"
               port="${tomcat.ajp.port}"
               tomcatAuthentication="false"
               secret="fltb6dZJA8lfFw" secretRequired="true" />
```

The Tomcat configuration file can be found here: **/opt/tarantella/webserver/tomcat/default/conf/server.xml**.

Enable 3rd party for user not in ENS (testing)

```
visulox-portal config edit --login-thirdparty-nonens 1
```

Add the VISULOX 3rd party configuration

```
visulox config 3rdparty -enabled true
visulox portal attach -3rdparty
```

See also: 3rdParty configuration parameters

Restart VISULOX

```
visulox-portal stop --kill
visulox stop
visulox-portal start
visulox start
```

Test login with the following URL: **https://<host.domain>/visulox/basic/**

Revert steps

If the above steps render your system unusable for some reason, you can revert to the original state by following these steps:

```
rm /etc/websrvpasswd.txt
```

```
cd /opt/tarantella/webserver/apache/default/conf/
cp httpd.conf.bkp httpd.conf
```

```
cd /opt/tarantella/webserver/tomcat/default/conf/
cp server.xml.bkp server.xml
```

```
/opt/tarantella restart webserver
```

23.1.141 3rdParty configuration parameters

Overview

The configuration option "**VISULOX config 3rdparty**" allows to control the 3rdparty authentication.

Usage

Command	Description
add	Create a 3rdParty access location
delete	Delete a 3rdParty configuration

Command	Description
edit	Edit a 3rdParty location configuration
list	List all configured 3rdParties

The following edit subcommands are available:

Parameter	Description
-name <*value*>	Name of 3rdParty access Location <>
-to <*value*>	Url <>
-detach <*value*>	Url <>
-enabled <*value*>	Location is enabled <false>

Examples

```
visulox config 3rdparty list
3rdParty configurations
    --------------------------------
    | active |  name | to | detach |
    --------------------------------
    |    yes | basic |    |        |
    --------------------------------
*** 3rdParty is generally disabled ***
```

```
visulox config 3rdparty -enabled true

*** Apply 3rdParty configuration by running  'visulox portal attach -3rdparty' ***
```

Always use **visulox portal attach -3rdparty** after changes.

See also: Web server basic authentication with VISULOX

23.1.142 Secure HTTP Gateway headers

Secure HTTP headers in application session responses can be added on the gateways, which can help to protect users of the application.

There is no direct security impact associated without the headers, but supporting them aids in achieving security in depth.

Adjust **http.conf** on the Gateway:

```
Header set Cross-Origin-Embedder-Policy "require-corp"
Header set Cross-Origin-Opener-Policy "same-origin"
Header set Permissions-Policy "geolocation=(self), camera=()"
```

```
Header set X-Permitted-Cross-Domain-Policies "none"
```