Veyon Documentation

Release 4.1.91

Veyon Community

Mar 20, 2019

Contents

CHAPTER 1

Online documentation

1.1 Veyon Administrator Manual

1.1.1 Introduction

About this manual

This manual describes the installation and configuration of Veyon in a computer network and is addressed to system administrators and technically experienced users. For end users there is a separate user manual which describes the usage and individual functions of the user program (Veyon Master).

In the following sections of this chapter you will find basic information about Veyon and its components which are of fundamental importance for putting Veyon into operation.

Chapter *Installation* covers the installation of Veyon on a Windows or Linux computer. It also contains information on how to perform or implement an automated installation.

Chapter *Configuration* explains how to configure and integrate Veyon using the graphical configuration tool, whereas the *Configuration reference* describes all available configuration settings and options in detail. Information and examples on how to connect Veyon to an LDAP or ActiveDirectory server can be found in chapter *LDAP/AD integration*.

Veyon also has a command line interface (CLI) which can be used to modify the configuration, automate Veyon-related tasks and to use or control certain program features. All modules and commands of the command line tool are listed and explained in chapter *Command line interface*.

In case Veyon causes problem during its installation or configuration actions can be taken as described in chapter *Troubleshooting*. Frequently asked questions are answered in chapter *FAQ - Frequently Asked Questions*.

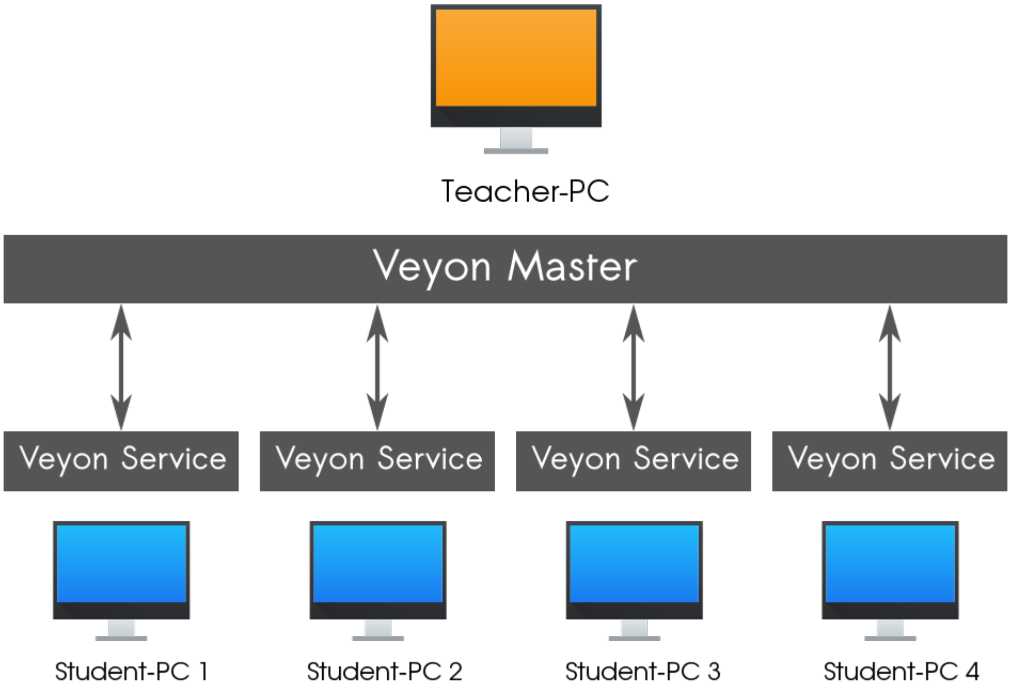
About Veyon

Veyon is a free and open source software for computer monitoring and class room management. It allows to monitor and control computer rooms as well as to interact with users, e.g. students. The following features are available in Veyon:

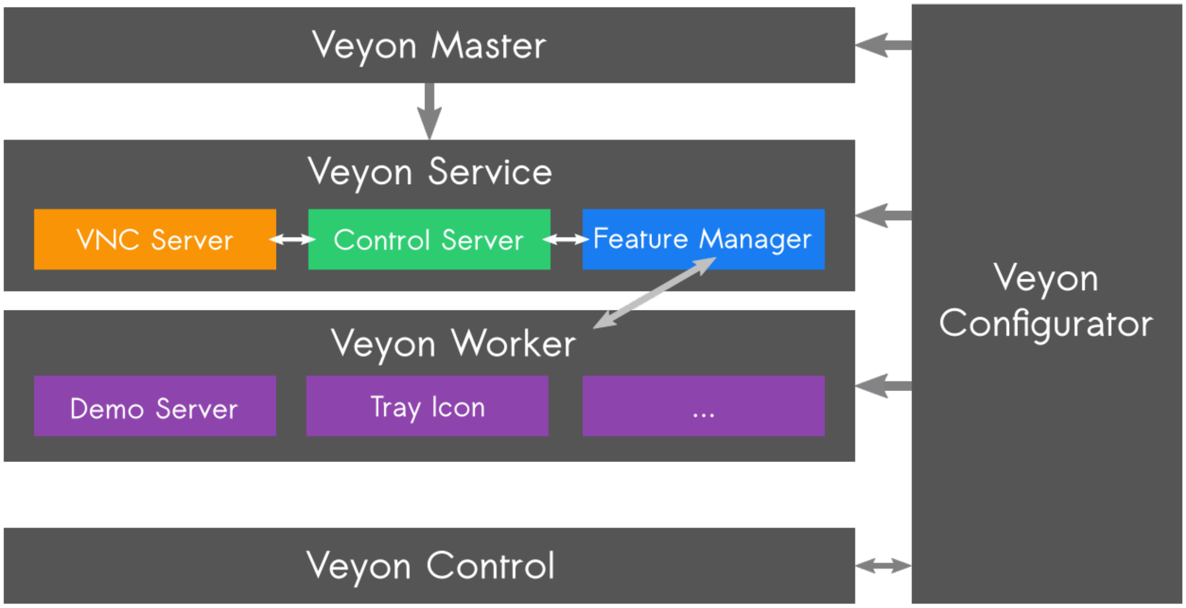
- Monitoring: overview of a (class) room with screen contents of computers being shown in thumbnails
- Remote view or control computers
- Broadcast the teacher's screen to all other computers in real time (full screen/window demo)
- Lock computers to control attention
- Distribute documents and other files to students
- Send text messages to students
- Power on, reboot or shutdown computers remotely
- Log out users
- Launch programs and open websites

Components

Veyon basically consists of a master and a service component which realize the interaction between teacher and student computers (also referred to as *master computer* and *client computer*):



In detail there are several software components that interact with each other in different ways:



Veyon Master An application program that can be used to monitor and control other computers and utilize further Veyon features. In normal use, the program is started by the end user and accesses other computers via the Veyon Service.

Veyon Service A non-graphical service application which monitors user sessions on a computer and starts Veyon Server instances within these sessions. The service and its server subprocesses are required to run on all computers including teacher computers.

Veyon Server A server application which provides access to a computer as well as control and application functions. In regular operation this program is started by the Veyon Service automatically and with elevated privileges so it can't be terminated by users.

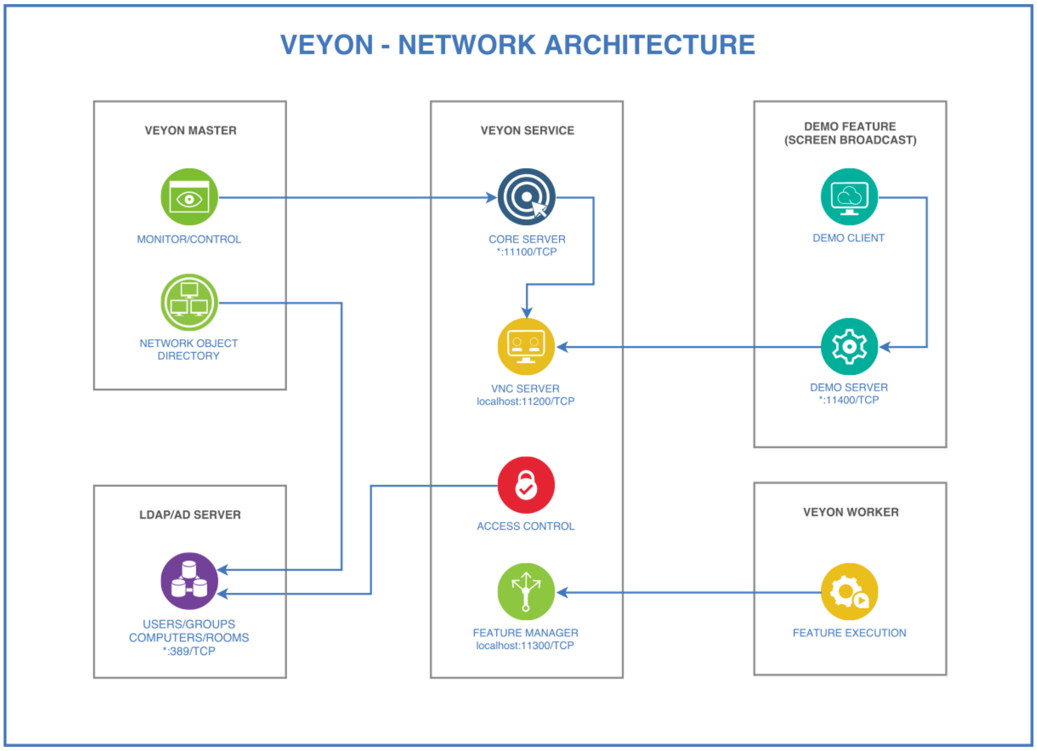
Veyon Worker A helper program started by the server to provide specific functions in an isolated environment or in the context of the currently logged-on user. Those specific functions include the demo server for the teacher computer and the demo client on the student computers.

Veyon Configurator A configuration tool which allows to configure and customize all components of a local Veyon installation through a graphical user interface. The program is started by the administrator with elevated privileges whenever necessary.

Veyon CLI A command line tool that in addition to the Veyon Configurator allows various configuration adjustments, automated tasks and the use of some Veyon features without graphical interaction. The program is run either interactively on the command line or script-controlled with usually administrative privileges.

Network architecture

From a network perspective the following components and TCP ports are involved:



1.1.2 Installation

Hardware and software requirements

Veyon is designed to run on standard computers running Windows or Linux. The minimum requirements for the hardware depend on the usage scenario and size of the environment in which Veyon is deployed. While there are no special requirements for client computers all master computers should be equipped with enough RAM and CPU cores to monitor the desired number of client computers.

- At least 2 GB RAM - Veyon Master requires 20-30 MB per client computer, depending on the client's screen resolution
- Multi-core system (2-4 CPU cores) highly recommended

All computers must be connected through a TCP-/IP-compatible network. Both wired and wireless network connections work. For using Veyon with more than 10 computers a Gigabit network is recommended, otherwise the performance of the demo mode feature (see user manual) may not be satisfactory. The same applies to wireless networks (*Wifi*) where at least the IEEE 802.11n standard should be used.

From a software point of view, an up-to-date operating system supported by the manufacturer or the community must be used. The following operating systems are supported:

- Windows 7, 8 or 10 (32/64 Bit)
- **Linux with at least version 5.5 of Qt**
  - Debian 9 or higher
  - Ubuntu 16.04 or higher
  - openSUSE 42.2 or higher
  - Fedora 24 or higher

- CentOS 7.3 or higher

The mixed operation of Veyon on Windows and Linux computers works without any restrictions.

Preparing the installation

First of all download the installation files for your platform from the Veyon download page. For Windows computers it is recommended to use the 64-bit version (*win64*). For 32-bit-installations you have to use the 32-bit version (*win32*) has to be used.

Installation on a Windows computer

Run the installer file with administrative privileges and follow the displayed instructions. On computers that do not require the Veyon Master application (e.g. student computers) you can deselect the component *Veyon Master* in the *Choose Components* dialog.

After the installation is finished the *Veyon Configurator* is started by default. This program allows to set up and customize your Veyon installation. In the next chapter *Configuration* the usage is described in detail.

Installation on a Linux computer

The installation of Veyon on Linux differs depending on the distribution used. If Veyon is available in the package archive of your distribution you can install the program through the appropriate software management application. Alternatively up-to-date binary packages for most major distributions are available at the Veyon download page. In all other cases it's always possible to build and install a current version of Veyon from source. For further information please visit the Github page of Veyon.

Automated/silent installation

Basics

The Veyon Windows installer provided by the community can be executed in *silent* mode, meaning that there is no user interaction and the installation is performed automatically. This is especially useful for automated deployments in larger environments. This way Veyon can be easily integrated with all common software distribution solutions and mechanisms.

By running the installer with the command line parameter `/S`, all operations are performed without further questions and dialogs. The same applies to the uninstaller.

Examples

Install Veyon in *silent* mode:

```
veyon-x.y.z-win64-setup.exe /S
```

Uninstall Veyon in *silent* mode:

```
C:\Program Files\Veyon\uninstall.exe /S
```

Specify an installation directory for an automated installation:

```
veyon-x.y.z-win64-setup.exe /S /D=C:\Veyon
```

Note: Because of a shortcoming of the installer software (NSIS) the option `/D=...` always has to be the last argument.

Import and apply a given Veyon configuration automatically after the installation:

```
veyon-x.y.z-win64-setup.exe /S /ApplyConfig=%cd%\MyConfig.json
```

Important: You must specify an absolute path for the configuration file, since the internally called command line tool (*Veyon CLI*) is executed with in a different working directory. Please use either the suggested `%cd`-variable or replace with an absolute path.

Automated installation without the Veyon Master component:

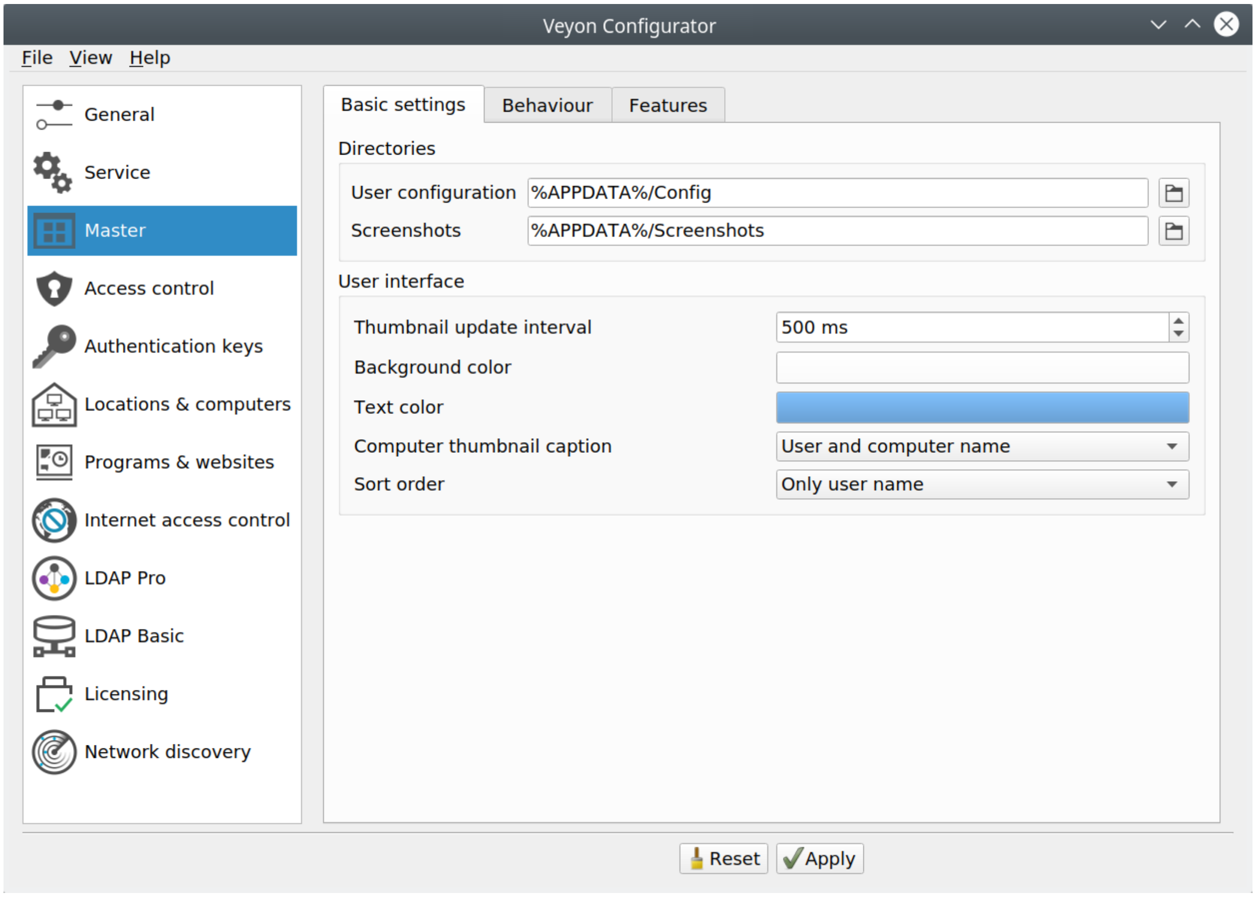
```
veyon-x.y.z-win64-setup.exe /S /NoMaster
```

Delete all Veyon-related settings during uninstallation:

```
C:\Program Files\Veyon\uninstall.exe /ClearConfig
```

1.1.3 Configuration

To begin with the setup, start the Veyon Configurator if this has not already been done automatically after the installation. With this program a local Veyon installation can be set up and customized. The graphical user interface is divided into different topic- or component-related configuration pages. Depending on the installed plugins there may be additional configuration pages.



Directories

User configuration: %APPDATA%/Config

Screenshots: %APPDATA%/Screenshots

User interface

Thumbnail update interval: 500 ms

Background color

Text color

Computer thumbnail caption: User and computer name

Sort order: Only user name

The *Configuration reference* describes all configuration pages and configuration options with their individual definitions and possible configuration values.

Overview

The basic settings on the configuration page *General* apply to all *Components* of Veyon. These include settings for the *User interface*, *Logging*, *Authentication* as well as the *Network object directory* which stores the locations and computers displayed in the Veyon Master.

The settings on the configuration page *Service* influence the functionality of the Veyon Service and are used for fine-tuning and adaptation to implement special application scenarious. For smooth operation the default settings should normally not be changed.

All setting on configuration page *Master* only affect the behavior and functions of the Veyon Master application and apply system-wide for all users.

Hint: For a quick start to get to know the software you only need to add a location and individual computers on configuration page *Locations & computers*. After the configuration has been *exported to all computers* the Veyon Master application can already be started and used. It should be ensured that the user used at logon exists with the same password on all computers.

Authentication

In order to access a computer running the Veyon Service the accessing user must first authenticate himself, i.e. he has to prove his identity and usage authorization. Otherwise unrestricted access from any user to any computer running the Veyon Service would be possible. Access without authentication is not supported. The setup is done via the configuration page *General* in section *Authentication* in Veyon Configurator.

Authentication methods

Basically Veyon offers two different authentication methods: key file authentication and logon authentication.

Key file authentication is based on Public-Key-Cryptography, meaning that a public key and a associated private key are used. Only certain users may have access to the private key. On each connection request the Veyon Service sends a random character sequence to Veyon Master, which Veyon Master has to sign cryptographically using the private key. The signature is sent back to the Veyon Service and verified with the corresponding public key. This verifiction only succeeds if the signature was generated with the appropriate private key. The authenticity of the counterpart is then guaranteed. If the signature verification fails, the connection is closed.

With **logon authentication** the counterpart encrypts its username and password and sends this data to the Veyon Service. The Veyon Service then attempts to perform an internal user login to the local system using the decrypted credentials. If this process is successful, the username and password are correct and the authenticity of the counterpart is ensured. If the login fails, the connection is closed.

Both methods have advantages and disadvantages so the choice of the right method depends on the environment, security requirements and desire for user comfort.

Key file authentication

Advantages	Disadvantages
• no login with username and password required when starting Veyon Master • access to computers can be handled centrally by access rights to the file containing the private key	• more effort for the setup • user identity can not be assured even after successful signature check • system-wide exchange of key files necessary if compromised

Logon authentication

Advantages	Disadvantages
• easy and effortless setup • identity of counterpart can be assured, allowing to use *Access control rules*	• login with username and password necessary whenever Veyon Master is used

The respective authentication method can be chosen and configured as described in section *Authentication* in the configuration reference.

Key management

In order to use the key file authentication, first a key pair consisting of a public and a private key has to be created. The configuration page *Authentication keys* is available for this purpose. A new key pair is generated via the *Create key pair* button. A short, concise term such as `teacher` should be chosen as the name. Then an access group must be set for both private and public keys. Only users who are to be allowed to access computers using Veyon Master should be member of the access group set for private keys. The public key should be assigned to a global access group so that the key is readable for all users and the operating system.

Once key file authentication is set up and working with one client computer, the keys can also be transferred to a shared network drive and the *Key file directories* can be changed accordingly. On the client computers only the Veyon configuration has to be imported, while the key files do not have to be imported manually.

> **Attention:** The private key file may only be accessible to users who should have access to other computers. If the file is stored on a network drive, it is therefore crucial to ensure that file access is restricted with using file ACLs or similar!

Access control

The access control module can be used to specify in detail which users may access certain computers. Access control is performed during connection initialization after a successful authentication. While authentication assures the authenticity of an accessing user, the access control functionality restricts computer access to authorized users such as teachers.

The setup is done on the *Access control* configuration page and is described in detail in the *Configuration reference* as well as chapter *Access control rules*.

> **Important:** Like all other settings the access control configuration is part of the local Veyon configuration. The configuration must therefore be *transferred to all other computers* to work properly.

Locations & computers

On the configuration page *Locations & computers* you can create the locations and computers displayed in the Veyon Master application when the *Network object directory* backend *Builtin* is used. Unlike backends such as *LDAP* this information is stored in the local configuration and must therefore be transferred to all computers.

The configuration page consists of two lists. The left list contains all configured locations. Using the two buttons below the list, locations may be added or removed. Existing locations can be edited and renamed by double-clicking.

The list on the right contains all computers stored for the currently selected location. The two buttons below the list can be used to add or remove computers. The individual cells in the table can be edited by double-clicking them. A computer name and a hostname or IP address must be specified for each computer. In case the Wake-on-LAN feature is to be used, the corresponding MAC address must also be supplied. Otherwise this column can be left blank.

LDAP

All information about connecting Veyon to an LDAP-compatible server such as *OpenLDAP* or *Active Directory* can be found in chapter *LDAP/AD integration*.

Importing/exporting a configuration

An imported prerequisite for the use of Veyon is an identical configuration on all computers. Transferring the Veyon configuration to another computer can be done manually at first, but should be automated later. Different methods are available for both ways.

In the Veyon Configurator you can find the entry *Save settings to file* in the *File* menu. This entry allows to export the current configuration to a file in JSON format. This file can be imported to another computer using the entry *Load settings from file* in the same menu. Please note, that the settings are loaded into the user interface during the import, but are applied and saved in the system only after the *Apply* button has been pressed.

The *Configuration management* module of the *Command line interface* can be used to automate/script configuration import and export.

Additionally, when performing an *automated installation* the configuration can be imported without requiring any further user interaction. In the example section an *example* is given for for the installer parameter `/ApplyConfig`.

Reset configuration

In some error situations it may be advisable to completely reset the Veyon configuration and then restart with the default values. For this purpose you can use the entry *Reset configuration* in the *File* menu in the Veyon Configurator.

Alternatively the configuration can also be reset using the *Configuration management* module of the *Command line interface*.

Furthermore the saved configuration can be reset on operating system level. On Linux the file `/etc/xdg/Veyon Solutions/Veyon.conf` has to be deleted, while on Windows the registry key `HKLM\Software\Veyon Solutions` and all of its subkeys have to be deleted.

1.1.4 Access control rules

Introduction

Access control rules can be used to provide detailed control over which users can access specific computers under specific circumstances. In the following, the term *rule* is used as a synonym for *access control rule*.

When a user attempts to access a computer, the defined access control rules are processed one after another until all conditions of a rule apply. As soon as all activated conditions of a rule apply, no further rules are processed and the stored action is executed (exception: rule is disabled).

The rules can be configured through the Veyon Configurator on the configuration page *Access control* in section *Access control rules*. The rules list is empty by default. In this case, all access attempts are denied since there is no rule that explicitly allows access. This means that at least one rule must be defined that allows access under certain conditions.

Add and modify rules

Upon clicking the button + a dialog opens which allows the creation of a new rule. Existing rules can be opened or edited by double-clicking them or by clicking the button with the pen symbol.

A rule basically consists of general settings, conditions and an action that is executed when all conditions apply. The dialog is divided into three sections. The meanings of the individual options in the various dialog sections are explained below.

General

A name for the rule should be defined in input field *Rule name* first. The name is later used to identify the rule and is displayed in the rules list. For documentation purposes an optional description can be added to the *Rule description* input field.

The option *Always process rule and ignore conditions* causes the conditions set below not to be examined for rule processing and the set action is always executed. This particularly useful for fallback rules at the botton of the rules list, where you can specify that the logged on user is asked for permission if no other rules apply.

You can use the *Invert all conditions* option to determine that all activated conditions are inverted before evaluation, meaning that activated conditions must not apply. For example, if the condition *No user logged on* is activated, the rule only applies if one or more users are logged on. If a condition is configured so that a user must be a member of a specific group, the rule only applies, if the said user is *not* a member of the group.

Conditions

For a rule to be processed, one or more conditions must apply.

User is member of group With this condition you can define that either the accessing or the locally logged on user must be a member of a specific group. The desired group can be chosen. If no or only wrong groups are selectable, the *User groups backend* under the general settings for *Computer access control* may have to be adjusted.

Computer is located at With this condition you can define that either the accessing or the local computer has to be located at a specific location. The desired location can be chosen. If no or only wrong locations are selectable the *Network object directory* has to be adjusted.

Accessing computer and local computer are at the same location With this condition you can determine that the accessing computer and the local computer have to be located at the same location. This can for example be used to prevent teachers from accessing computers in different classroom.

Accessing computer is localhost If this condition is enabled, the rule applies only if the accessing computer is the local computer. This ensures for example that teachers can access the local Veyon Service. This access is necessary for the Veyon Master to execute specific functions via the Veyon Service (e.g. the server for demo mode).

Accessing user has one or more groups in common with local (logged on) user You can use this condition to specify that the accessing and the local user have to be members of at least one common group, for example a user group for a class or a seminar.

Accessing user is logged on user As an alternative to the condition *accessing computer is localhost* you can also allow a user to access his own sessions. This condition must be activated for this purpose.

Accessing user is already connected In conjunction with the condition *Accessing computer and local computer are at the same location* an extended ruleset can be created allowing access to computer at other locations under certain conditions. This includes the possibility to access a computer if the accessing user is already connected. For example, if the teacher logs on to a teacher computer in room A and B simultaneously and displays the computers of room B displayed in Veyon Master, the computers in room B have a connection from the teacher. Then the teacher can also access room B from Veyon Master in room A if this condition is activated with an allow action.

No user logged on This condition determines how a computer can be accessed when no user is logged on. For easier computer administration, it can be helpful to always be able to access a computer when no user is logged on.

Action

If all the enabled conditions of a rule apply, a specific action is performed with respect to computer access. You can define this action in section *Action*:

Allow access Access to a computer is allowed and further rules are not processed. If there is a rule in the rules list below that would deny access, access is still allowed. There must be at least one rule with this action.

Deny access Access to a computer is denied and further rules are not processed. If there is a rule in the rules list below that would allow access, access is still denied.

Ask logged on user for permission This action displays a dialog on the computer that allows the logged-in user to choose whether to allow or deny access. No further rules are processed regardless of the user's decision.

None (rule disabled) This action makes the rule being ignore. Access control will be continued by processing the next rule. This option can be used to create an inactive dummy entry to visually subdivide the rules list.

By clicking the *OK* button the rule and the changes made are accepted and the dialog is closed.

Sorting rules

Important: The defined access control rules are processed one after the other in the order of the list. The action of the first matching rule is executed, even if subsequent rules would also apply and lead to a different action.

All rules can be reordered via the buttons with the arrow symbols. Rules that should fundamentally prevent or allow access based on certain criteria should be placed as high up as possible. Rules to cover special cases can follow below. Rules for the implementation of fallback behaviour should be at the bottom.

Logical concatenation of rules

If more than one condition is activated in a rule, *each* condition must apply for the rule to be applied (logical AND). If only one of several rules should apply (logical OR), several access control rules must be defined.

With basic knowledge of Boolean algebra, the option *Invert all conditions* can be used as negation operator in conjunction with inverted actions to model extended scenarios. For example, if a user must be a member of two specific groups to allow access to a computer, two seperate rules can be created that deny access, if the user is *not* a member of either group.

Note: If there is no matching access control rule so that all activated conditions apply, access is denied and the connection is closed. This prevents an attacker from being accidentally allowed access due to an incomplete ruleset.

Testing a ruleset

In section *Computer access control* the configured ruleset can be checked with various scenarios using the *Test* button. In the test dialog you can enter the parameters to simulate a scenario. With the button *OK* the rules are processed with the given parameters and a message with the test result is displayed.

1.1.5 LDAP/AD integration

This chapter covers the setup of Veyon for connecting it to LDAP-compatible servers. In the following the generic term *LDAP* will be used and refers to all LDAP-compatible products and technologies such as *OpenLDAP*, *Samba* or *Active Directory*. LDAP integration enables you to use information about users, user groups, computers and locations that already exist in most environments, instead of manually replicating it in the Veyon configuration. Once configured Veyon Master can retrieve locations and computers to be displayed directly from the directory service. Additionally LDAP users and user groups can serve as a base for *Computer access control*.

The configuration of the LDAP integration is done on configuration page *LDAP* in Veyon Configurator. The page is divided into several subpages for *Basic settings*, *Environment settings*, *Advanced settings* and *Integration tests*.

Basic settings

The basic settings affect all basic parameters for accessing an LDAP server. They are mandatory for a properly working LDAP integration.

General

LDAP server and port Enter the address of the LDAP server (hostname or IP address) here. If a port other than the default LDAP port 389 is used, the port parameter has to be adjusted accordingly.

Anonymous bind / Use bind credentials Depending on the environment and configuration of the LDAP server, LDAP queries can be performed either as an anonymous user or with valid usernames and passwords only. If the server access requires a username and password, the option *Use bind credentials* has to be selected and the credentials have to be entered in the input fields below. Otherwise the default option *Anonymous bind* can be used.

Bind DN The bind DN is the username used to log in at the server in order to perform LDAP operations. However, the required format heavily depends on the LDAP server and its configuration. Possible formats include `User`, `DOMAIN\User` or `cn=User,...,dc=example,dc=org`.

Bind password In addition to the bind DN the corresponding password has to be entered.

You can use the *Test* button to verify, whether server access is working with the supplied parameters.

Hint: Veyon only requires read access to the LDAP directory. As an additional security measure on the LDAP server a dedicated user with read-only access to the LDAP directory can be created, e.g. “Veyon-LDAP-RO”. Access to relevant attributes can be further restricted for this user.

Connection security

Veyon can establish encrypted connections to the LDAP server. For this purpose, settings are available in the section *:guilabel:‘Connection security*.

Encryption protocol You can choose between the encryption protocols *None*, *TLS* and *SSL*. The use of the modern TLS protocol is recommended.

Default: *None*

TLS certificate verification This setting determines how the security certificate of the LDAP server is to be checked when the encrypted connection is established. With the default setting *System defaults*, depending on the operating system, an attempt is made to verify the certificate using the root certificates installed system-wide. The Windows certificate store is not taken into account here, so that a separate CA certificate file may have to be stored. With the the *Never* setting, the server certificate is not verified at all. This however allows for case man-in-the-middle attacks and should therefore only be used in exceptional cases. The *User-defined CA certificate file* setting ensures that the certificate check is performed on the basis of a specified CA certificate file.

Default: *System defaults*

Custom CA certificate file If you use your own certification authority (CA), it may be necessary to store their certificate in a PEM file format so that Veyon can check the certificate of the LDAP server.

Base DN

The base DN defines the address of the root object in the directory. All objects are stored below the base DN. Usually the base DN comes from the DNS or AD domain (see also RFC 2247).

In most cases a fixed base DN is used so the default option *Fixed base DN* has to be chosen. The base DN then has to be entered in the corresponding input field or seleted from the server by using the *Browse* button. You can use the *Test* button to verify, whether the settings are correct and entries can be found.

If a generic Veyon configuration is to be used across multiple sites with different base DNs, Veyon can be configured so that the base DN is always queried dynamically using LDAP naming contexts. For this to work the *Discover base DN by naming context* has to be chosen and the naming context attribute must be adapted. You can use the *Test* button to verify, whether a Base DN could be determined.

After importing a generic Veyon configuration without a fixed base DN it is also possible to determine the base DN through the *Command line interface* and write it to the local configuration.

Environment settings

After the basic settings have been configured and tested, the environment-specific settings can now be made. These settings determine which trees contain objects of certain types as well as the names of certain object attributes. With these parameters Veyon can retrieve all required information from the LDAP directory.

Object trees

Object trees are organizational or structural units in which certain types of objects (users, groups, computers) are stored. The respective CNs (Common Names) or OUs (Organizational Units) must be entered **without the base DN part** in the respective input field. Next to each input field there are buttons for opening browse dialogs and for testing the individual setting.

User tree The LDAP tree (without base DN) in which the user objects are located must be entered here, e.g. `OU=Users` or `CN=Users`.

Group tree The LDAP tree (without base DN) in which the group objects are located must be entered here, e.g. `OU=Groups` or `CN=Groups`.

Computer tree The LDAP tree (without base DN) in which the computer objects are located must be entered here, e.g. `OU=Computers` or `CN=Computers`.

Computer group tree If the computer groups are located in a different tree than the regular user groups or in a subtree, the corresponding LDAP tree can be specified here. Otherwise the group tree is used to query computer groups and to filter them with a specific *object filter* if necessary.

Perform recursive search operations in object trees This option can be used to control whether objects should be queried recursively. The search then takes place not only in the specified tree but also in any existing subtrees.

Default: *disabled*

Hint: If objects of one type are stored in different object trees (e.g. users in both `CN=Teachers` and in `CN=Students`), the parameter for the corresponding object tree can be left empty and the option *Perform recursive search operations in object trees* can be activated. A recursive search is then performed in the entire LDAP directory starting from the base DN. In this case, however it is strongly recommended to set the *object filters* for the respective object type.

Object attributes

For Veyon to be able to retrieve the required information from the queried objects, the names of some object attributes have to be configured, as these differ substantially depending on the environment and LDAP server. Next to each input field buttons for browsing the attribute of an existing object and testing the respective attribute name are available.

User login name attribute This attribute must hold the login name of a user. The attribute is used to determine the LDAP user object associated with a particular username. In an OpenLDAP environment often the attribute name `uid` is used while the name `sAMAccountName` is common in Active Directories.

Group member attribute Members of a group are listed in group objects through this attribute. The attribute is used to determine the groups a particular user is a member of. Depending on the configuration the attribute also also used map computers to locations. In an OpenLDAP environment often the attribute name `member` is used while the name `memberUid` is common in Active Directories.

Computer display name attribute The content of this optional attribute is used to determine the name of a computer displayed in Veyon Master. If left blank the common name (`cn`) is used instead.

Default: *cn*

Computer host name attribute This attribute must hold the DNS name of the computer. It is used to determine the LDAP computer object associated with a particular computer hostname. In an OpenLDAP environment often the attribute name `name` is used while the name `dNSHostName` is common in Active Directories.

Hostnames stored as fully qualified domain names (FQDN, e.g. myhost.example.org) This option specifies whether to use the fully qualified domain name (FQDN) for mapping computer names to LDAP computer objects. If the computer names are stored without the domain part in the LDAP directory, this option has to be left disabled, otherwise it must be enabled.

Default: *disabled*

Computer MAC address attribute In addition to the computer name the MAC addresses of computers are stored in the LDAP directory in some environments, for example if the DHCP server also accesses the LDAP directory. If the Veyon feature is to be used to switch on computers via Wake-on-LAN, the corresponding attribute name must be entered here, since the MAC address is required for this functionality. Typical attribute names are `hwAddress` or `dhcpAddress`.

Hint: In a standard Active Directory there is no attribute which stores MAC addresses. You must therefore populate MAC addresses manually in an existing unused attribute such as `wwwHomepage` or extend the AD schema. Additionally you can grant computers group write access to `SELF` and use a PowerShell script to make each computer automatically store the MAC address of its first physical LAN adapter when booting.

Computer location attribute If the LDAP schema for computer objects provides a special attribute for the mapping to a location, this attribute name can be entered here. The *Test* button can be used to verify whether the computers at a location can be queried correctly using the configured attribute. In the advanced settings, you can then specify in section *Computer locations* that the computer location attribute is used.

Location name attribute When identifying computer locations via computer groups or computer containers, the value of a certain attribute can be displayed as the location name instead of the *Common Names* of these groups or objects. If, for example, computer groups have an attribute called `name` or `description`, a meaningful location name can be stored in this attribute and the attribute name can be entered here.

Advanced settings

With the advanced settings the LDAP integration and the use of the information from the LDAP directory can be customized to individual needs.

Optional object filters

With LDAP filters, the LDAP objects used by Veyon can be narrowed down if, for example, computer objects such as printers are not to be displayed in the Veyon Master. Next to each input field there is a button for checking the respective object filter.

As of Veyon 4.1 the optional filters follow the well-known scheme for LDAP filters (see for example RFC 2254 or Active Directory: LDAP Syntax Filters) such as `(objectClass=XYZ)`.

Filter for users You can define an LDAP filter for users here, e.g. `(objectClass=person)` or `(&(objectClass=person)(objectClass=veyonUser))`.

Filter for user groups You can define an LDAP filter for user groups here, e.g. `(objectClass=group)` or `(|(cn=teachers)(cn=students)(cn=admins))`.

Filter for computers You can define an LDAP filter for computers here, e.g. `(objectClass=computer)` or `(&(!(cn=printer*))(!(cn=scanner*)))`.

Filter for computer groups You can define an LDAP filter for computer groups here, e.g. `(objectClass=room)` or `(cn=Room*)`. If computer groups are used as locations, you can filter the displayed locations this way.

Filter for computer containers You can define an LDAP filter for computer groups here, e.g. `(objectClass=container)` or `(objectClass=organizationalUnit)`. If containers/OUs are used as locations, you can filter the displayed locations this way.

Group member identification

The content of the group membership attributes varies across different LDAP implementations. While in Active Directory the *distinguished name (DN)* of an object is stored in the member attribute, OpenLDAP usually stores the user login name (`uid` or similar) or the computer name. In order for Veyon to use the correct value for querying groups of a user or computer, the appropriate setting must be chosen here.

Distinguished name (Samba/AD) This option has to be chosen, if the distinguished name (DN) of an object is stored in a member attribute of the group. Usually Samba and AD server use this scheme.

Configured attribute for user login name or computer hostname (OpenLDAP) This option has to be chosen, if the login name of a user (username) or the hostname of a computer is stored in the member attributes of a group. Usually OpenLDAP server use this scheme.

Computer locations

Veyon offers several methods to represent computer locations in an LDAP directory. In the simple case there is one computer group for every location (e.g. room). All computers at a specific location are members of the corresponding group. If computers instead are organized in containers or organizational units (OUs), these parent objects can be used as locations. Both procedures do not require any adaptation of the LDAP schema. As a third possibility, the location name can also be stored as a special attribute in each computer object.

Computer groups This option specifies that computer locations are identified through computer groups. All computer groups are then displayed as locations in the Veyon Master. For each location all computers that are members of the corresponding group are displayed. If not all LDAP groups are to be displayed as locations, either a dedicated *computer group tree* must be configured or the computer groups must be restricted using a *computer group filter*.

Default: *enabled*

Computer containers or OUs This option specifies that the containers/OUs containing computer objects are used as computer locations. Containers are objects that are parents to computer objects in the LDAP tree. If not all containers are to be displayed as locations, a corresponding *computer container filter* can be set up.

Default: *disabled*

Location attribute in computer objects If the LDAP schema for computer objects provides a special attribute for mapping computer objects to locations, this option can be enabled and the attribute name can be entered. The *Test* button can be used to check whether the members of a computer location can be queried correctly using the configured attribute.

Default: *disabled*

Integration tests

The integration tests can be used to check the LDAP integration as a whole. The buttons allow various tests to be performed. All tests should be successful and provide valid results before the LDAP connection is used in production.

Using LDAP backends

With the successful configuration and testing of the LDAP integration, the LDAP backends can now be activated. For this, the *network object directory* and the user groups backend for the *computer access control* must be adapted. Only after switching the network object directory to *LDAP* the location and computer information from the LDAP directory are used in the Veyon Master.

> **Attention:** After changing the backend for the computer access control, all previously configured access rules should under all circumstances be checked, since group and location information change and in most cases access rules will no longer be valid or not be processed correctly.

Command line interface

The *Command line interface* of Veyon allows some LDAP-specific operations. All operations are available using the `ldap` module. A list of all supported commands is displayed via `veyon-cli ldap help`, while command-specific help texts can be displayed via `veyon-cli ldap help <command>`.

`autoconfigurebasedn`

This command can be used to automatically determine the used base DN and permanently write it to the configuration. An LDAP server URL and optionally a naming context attribute have to be supplied as parameters:

```
veyon-cli ldap autoconfigurebasedn ldap://192.168.1.2/ namingContexts
veyon-cli ldap autoconfigurebasedn ldap://Administrator:MYPASSWORD@192.168.1.
↪2:389/
```

Hint: Special characters such as `@` or `:` – especially in the password - can be specified by using URL percent-encoding.

`query`

This command allows to query LDAP objects (`locations`, `computers`, `groups`, `users`) and is mainly used for testing. The function can also be used to develop scripts for system integration tasks.

```
veyon-cli ldap query users
veyon-cli ldap query computers
```

1.1.6 Command line interface

For administrative tasks, the *Veyon Configurator* and the command line tool *Veyon CLI* are available. The program can be started via the command `veyon-cli` in the command line. On Windows there's an additional non-console version `veyon-wcli` which allows to automate tasks without irritating command line window popups. If the `$PATH` (Linux) or `%PATH%` (Windows) environment variable does not contain the Veyon installation directory, you must first change to the installation directory or prepend the directory to the program name.

If the program is called with the `help` parameter, a list of all available modules is displayed. The list can vary depending on the installed Veyon plugins:

```
$ veyon-cli help
Available modules:
    authkeys - Commands for managing authentication keys
    config - Commands for managing the configuration of Veyon
    ldap - Commands for configuring and testing LDAP/AD integration
    networkobjects - Commands for managing the builtin network object directory
    power - Commands for controlling power status of computers
    remoteaccess - Remote view or control a computer
    service - Commands for configuring and controlling Veyon Service
    shell - Commands for shell functionalities
```

Each CLI module supports the `help` command, so that a list of all available commands can be displayed for each module. Sample output for the `config` module:

```
$ veyon-cli config help
Available commands:
    clear - Clear system-wide Veyon configuration
    export - Export configuration to given file
    get - Read and output configuration value for given key
    import - Import configuration from given file
    list - List all configuration keys and values
    set - Write given value to given configuration key
    unset - Unset (remove) given configuration key
    upgrade - Upgrade and save configuration of program and plugins
```

For some modules the `help` command can be supplied with a command name as an additional argument to get specific help for a command:

```
$ veyon-cli remoteaccess help control

remoteaccess control <host>
```

Authentication key management

The `authkeys` module allows the management of authentication keys so that common operations such as importing an authentication key or assigning a user group can be automated easily.

`create <NAME>`

This command creates a authentication key pair with name <NAME> and saves private and public key to the configured key directories. The parameter must be a name for the key, which may only contain letters.

delete <KEY>

This command deletes the authentication key <KEY> from the configured key directory. Please note that a key can't be recovered once it has been deleted.

export <KEY> [<FILE>]

This command exports the <KEY> to <FILE> authentication key. If <FILE> is not specified a name will be constructed from name and type of <KEY>.

extract <KEY>

This command extracts the public key part from the private key <KEY> and saves it as the associated public key. When setting up another master computer, it is therefore sufficient to transfer the private key only. The public key can then be extracted.

import <KEY> [<FILE>]

This command imports the authentication key <KEY> from <FILE>. If <FILE> is not specified a name will be constructed from name and type of <KEY>.

list [details]

This command lists all available authentication keys in the configured key directory. If the `details` option is specified a table with key details will be displayed instead. Some details might be missing if a key is not accessible e.g. due to the lack of read permissions.

setaccessgroup <KEY> <ACCESS GROUP>

This command adjusts file access permissions to <KEY> so that only the user group <ACCESS GROUP> has read access to it.

Configuration management

The local Veyon configuration can be managed using the `config` module. Both the complete configuration as individual configuration keys can be read or written.

clear

This command resets the entire local configuration by deleting all configuration keys. Use this command to recreate a defined state without old settings before importing a configuration.

export

This command exports the local configuration to a file. The name of the destination file must be specified as an additional parameter:

```
veyon-cli config export myconfig.json
```

import

This command imports a previously exported configuration file into the local configuration. The name of the configuration file to be imported must be specified as an additional argument:

```
veyon-cli config import myconfig.json
```

list

This command shows a list of all configuration keys and their corresponding values. This way you can get the names of the configuration keys in order to read or write them individually via the `get` or `set` commands.

get

This command allows reading a single configuration key. The name of the key must be supplied as a parameter.

```
veyon-cli config get Network/PrimaryServicePort
```

`set`

This command can be used to write a single configuration key. The name of the key and the desired value must be passed as additional arguments:

```
veyon-cli config set Network/PrimaryServicePort 12345
veyon-cli config set Service/Autostart true
veyon-cli config set UI/Language de_DE
```

`unset`

With this command a single configuration key can be deleted, i.e. Veyon then uses the internal default value. The name of the key must be passed as an additional argument:

```
veyon-cli config unset Directories/Screenshots
```

`upgrade`

With this command the configuration of Veyon and all plugins can be updated and saved. This may be necessary if settings or configuration formats have changed due to program or plugin updates.

LDAP

The commands available in the `ldap` module are documented in section *Command line interface* in chapter *LDAP/AD integration*.

Network object directory

As described in the section *Locations & computers*, Veyon provides a built-in network object directory that can be used when no LDAP server is available. This network object directory can be managed in the Veyon Configurator as well as on the command line. Certain operations such as CSV import are currently only available on the command line. For most commands, a detailed description with examples is available in the command-specific help. The following commands can be used in the `networkobjects` module:

`add <TYPE> <NAME> [<HOST ADDRESS> <MAC ADDRESS> <PARENT>]`

This command adds an object, where `<TYPE>` can be `location` or `computer`. `<PARENT>` can be specified as name or UUID.

`clear`

This command resets the entire network object directory, i.e. all locations and computers are removed. This operation is particularly useful before any automated import.

`dump`

This command outputs the complete network object directory as a flat table. Each property such as object UID, type or name is displayed as a separate column.

`export <FILE> [location <LOCATION>] [format <FORMAT-STRING-WITH-VARIABLES>]`

This command can be used to export either the complete network object dictionary or only the specified location to a text file. The formatting can be controlled via a format string with variables inside. This allows to generate CSV file easily. Valid variables are `%type%`, `%name%`, `%host%`, `%mac%` and `%location%`. Various examples are given in the command help (`veyon-cli networkobjects help export`).

`import <FILE> [location <LOCATION>] [format <FORMAT-STRING-WITH-VARIABLES>] [regex <REGULAR`

This command can be used to import a text file into the network object directory. The processing of the input data can be controlled via a format string or a regular expression with variables inside. This way both CSV files and other types of structured data can be imported. Valid variables are `%name%`, `%host%`, `%mac%` and `%room%`. Various examples are given in the command help (`veyon-cli networkobjects help import`).

`list`

This command prints the complete network object directory as a formatted list. Unlike the `dump` command, the hierarchy of locations and computers is represented by appropriate formatting.

`remove <OBJECT>`

This command removes the specified object from the directory. OBJECT can be specified by name or UUID. Removing a location will also remove all related computers.

Power

The `power` module allows to use power-related functions from the command line.

`on <MAC ADDRESS>`

This command broadcasts a Wake-on-LAN (WOL) packet to the network in order to power on the computer with the given MAC address.

Remote access

The `remoteaccess` module provides functions for a graphical remote access to computers. These are the same function that can be accessed from the Veyon Master. The function provided by the command line tool can be used for example to create an program shortcut for direct access to a specific computer.

`control`

This command opens a window with the remote control function that can be used to control a remote computer. The computer name or IP address (and optionally the TCP port) must be passed as an argument:

```
veyon-cli remoteaccess control 192.168.1.2
```

`view`

This command opens a window with the remote view function to monitor a remote computer. In this mode the screen content is displayed in real time, but interaction with the computer is not possible until the corresponding button on the tool bar has been clicked. The computer or IP address (and optionally the TCP port) has to be passed as an argument:

```
veyon-cli remoteaccess view pc5:5900
```

Service control

The `service` module can be used to control the local Veyon Service.

`register`

This command registers the Veyon Service as a service in the operating system so that it is automatically started when the computer boots.

`unregister`

This command removes the service registration in the operating system so that the Veyon Service us no longer automatically started at boot time.

`start`

This command starts the Veyon Service.

`stop`

This command stops the Veyon Service.

`restart`

This command restarts the Veyon Service.

status
This command queries and displays the status of the Veyon Service.

Shell

Simple shell functionalities are provided by the `shell` module. If this module is called without further arguments, an interactive mode is started. In this mode, all CLI commands can be entered directly without having to specify and call the `veyon-cli` program for each command. The mode can be left by entering the keyword `exit`.

Furthermore the module can be used for automated processing of commands in a text file in order to implement simple batch processing:

run <FILE>
This command executes the commands specified in the text file line by line. Operations are executed independently of the result of previous operations, i.e. an error does not lead to termination.

1.1.7 Configuration reference

In this chapter all configuration pages within Veyon Configurator as well as all configuration options with their respective meanings are explained in detail. It mainly serves as a reference for looking up detailed configuration options. A manual and hints for the installation can be found in chapter *Configuration*.

Note: Some advanced settings are hidden in the standard view. You can switch to the advanced view using the menu.

General

User interface

Language The selected language can be configured for the graphical user interfaces as well as the command line tools. You can choose from all languages which have been translated so far. Please note that changing the language will require a program restart in order to take effect. Per default Veyon uses the language of the operating system if a translation is available for that language. Otherwise English will be used as a fallback.

Default: *Use system language setting*

Authentication

The *Configuration* chapter describes the *Authentication methods* available in Veyon.

Method This option defines which authentication method to use. *Logon authentication* does not require any further setup and can be used immediately. To use the *key file authentication*, appropriate authentication keys must first be created and distributed.

Default: *Logon authentication*

Network object directory

In Veyon a network object directory provides information about network objects. Network objects can either be computers or their locations. The data supplied by the network object directory is used by Veyon Master to populate the *Locations & computers* view with entries. The data from the network object directory is also used for access control rules making use of computer location information. By default a backend is used which stores computers and locations in the local Veyon configuration and queries them from the configuration whenever required. See section *Locations & computers* for details.

Backend You can use this setting to set the desired backend for the network object directory. Depending on the installation there may be several backends such as *LDAP/AD integration* available beside the default backend.

Default: *Builtin (computers and locations in local configuration)*

Update interval The network object directory automatically updates in background which especially is useful for dynamic backends such as LDAP. The time interval for these updates can be altered with this option.

Default: *60 seconds*

Logging

Veyon can log various kinds of messages to component-specific log files or the logging system of the operating system. These information can be very helpful when troubleshooting issues with Veyon. The following logging settings allow to change the logging behaviour.

Log file directory You can use this setting to specify which directory the log files will written in. It's strongly recommended to use placeholder variables here. All information on supported variables can be found in section *Placeholder variables for file paths*.

Default: *%TEMP%*

Log level The log level defines the minimum severity for which log messages are written. When analyzing program failures it may be useful to set the log level to *Debug messages and everything else*. This will generate huge amount of log data and is not recommended for production environments. The default log level *Warnings and errors* or higher should be used instead.

Default: *Warnings and errors*

Limit log file size In order for log files not to become too large and occupy disk space unnecessarily their size can be limited through this setting. When enabled an upper limit for the size of a single log file can be configured.

Default: *disabled / 100 MB*

Rotate log files In conjunction with limiting the size of log files it additionally may be useful to rotate the log files. When enabled each log file is renamed to `Veyon...log.0` after exceeding the configured limit. Previously rotated files are renamed so that the number of the file suffix is increased by 1. If the configured number of rotations is reached the oldest file (i.e. the one with the highest number as a suffix) is deleted.

Default: *disabled / 10x*

Log to standard error output When program components of Veyon are executed from a command line window (shell), you can use this option to specify, whether logging messages shall be printed to `stderr` or `stdout`. This setting primarily is relevant for scripting operations only.

Default: *enabled*

Write to logging system of operating system In some environments it may be desired to write log messages directly to the Windows event log e.g. in order to collect them afterwards. This option does not influence the normal recording of log files. On Linux this option currently has no effect.

Default: *disabled*

You can use the *Clear all log files* button to delete all Veyon log files in the log file directory of the current user as well as the ones of the system service. This will stop the Veyon Service temporarily.

Service

General

Hide tray icon By default the Veyon Service displays a tray icon (also called *system control panel*, *info area* or similar) to indicate proper operation and provide basic information such as the program version and network port which the service is listening at. The tray icon can be hidden by enabling this option.

Default: *disabled*

Show notification on failed authentication attempts This option specifies whether a notification should be displayed if there was a failed logon attempt to the Veyon Service. These messages usually indicate that the authentication settings are not set up correctly. Typical failure reasons are invalid authentication keys or (when using logon authentication) invalid user credentials (username/password).

Default: *enabled*

Show notification on remote connection In some environments it may be desired or even required to inform the user that his computer is being accessed remotely. This behaviour can be achieved by enabling this option. In case the user has to be asked for permission instead appropriate access control rules have to be configured. More information can be found in chapter *Access control rules*.

Default: *disabled*

Enable SAS generation by software (Ctrl+Alt+Del) On Windows per default it's impossible for applications to generate the *Secure Attention Sequence* (Ctrl+Alt+Del) in order to simulate the press of these keys. When enabling this option a policy is written to the Windows registry which changes this behavior. It is recommended to leave this option enabled in order to be able to send `Ctrl+Alt+Del` when remote controlling a computer. Otherwise it may be impossible to unlock a remotely controlled computer or logging on a user since in most cases the shortcut `Ctrl+Alt+Del` has to be issued first.

Default: *enabled*

Autostart Upon the installation of Veyon the Veyon Service is registered as a system service in order to launch the Veyon Server automatically for user sessions. The start of the Veyon Service can be prevented by disabling this option. You'll then have to start the Veyon Server in user sessions manually. The logon screen will not be accessible in this case.

Default: *enabled*

Network

Primary service port You can use this setting to define the primary network port which the Veyon Server is listening at for incoming connections.

Default: *11100*

Internal VNC server port You can use this setting to define the (localhost only) network port used by the internal VNC server. The VNC server will only listen to it at `localhost` so it never is reachable from the network directly. It's solely accessed by the Veyon Service which forwards screen data from and user inputs to the internal VNC server.

Default: *11200*

Feature manager port You can use this setting to define the (localhost only) network port used by the feature manager. This internal component is part of the Veyon Service and starts and stops processes to provide specific features. In contrast to the Veyon Service these processes in most cases have to run in the context of the logged on user and therefore have to communicate with the Veyon Service through this network port.

Default: *11300*

Demo server port You can use this setting to define the network port which the demo server is listening at. The demo server efficiently makes screen data from a selected computer available to all computers participating in a demonstration.

Default: *11400*

Enable firewall exception Depending on the system configuration it may be impossible to access a listening ports such as the Veyon Service port from the network. On Windows the Windows firewall usually will block any incoming connections. In order to provide access to the service port and the demo server port, exceptions for the Windows-Firewall must be configured. This is done automatically during the installation process. If this behavior is not desired and manual configuration is preferred, this option can be disabled.

Default: *enabled*

Allow connections from localhost only If you do not want the Veyon Service to be available to other computers in the network, you can use this option. This option must not be activated for normal computers that should be accessible from the Veyon Master application. However, this option can be useful for teacher computers to provide additional security beyond the access control functionality. Access to the demo server is not affected by this option.

Default: *disabled*

VNC server

Plugin By default Veyon uses an internal platform-specific VNC server implementation to provide the screen data of a computer. In some cases, however, it may be desirable to use a plugin with a different implementation. If a separate VNC server is already running on the computer, this server instance can be used instead of the internal VNC server by choosing the plugin *External VNC server*. In this case the password and network port of the installed VNC server have to be supplied.

Default: *Builtin VNC server*

Master

All settings on this page influence the appearance, behaviour and features of the Veyon Master application.

Basic settings

Directories

In order to make a configuration generic and independent of the user, you should use placeholder variables instead of absolute paths in the directory settings. All information on supported variables can be found in section *Placeholder variables for file paths*.

User configuration The user specific configuration of Veyon Master is stored in this directory. The configuration contains settings for the user interface as well as the computer selection of the last session.

Default: *%APPDATA%/Config*

Screenshots All image files that have been generated by using the screenshot feature are stored in this directory. In case you want to collect the files in a central folder, a different directory path can be supplied here.

Default: *%APPDATA%/Screenshots*

User interface

Thumbnail update interval This setting determines the time interval in which the computer thumbnails in Veyon Master are updated. The shorter the interval, the higher the processor load on the master machine and the overall network load.

Default: *1000 ms*

Background color This setting allows to customize the background color of the monitor view.

Default: *white*

Text color This setting allows to customize the color which is used for displaying the computer thumbnail caption in the monitor view.

Default: *black*

Computer thumbnail caption This setting allows to define the caption for computer thumbnails in the monitor view. If the computer name is not important to users only the name of the logged on user can be displayed instead.

Default: *User and computer name*

Sort order This setting allows to specify the sort order for computers in the monitor view. If the caption is configured to display only user names it may make sense to change the sort order to *Only user name* as well.

Default: *Computer and user name*

Behaviour

In the tab *Behaviour* settings are available to change the behaviour of Veyon Master regarding to *program start*, *computer locations* as well as *modes and features*.

Program start

Perform access control You can use this option to define whether the possibly configured *Computer access control* should also be perform whenever the Veyon Master application is started. Even though access control is enforced client-side in every case, this additional option assures, that users without proper access rights can not even start Veyon Master, making security even more visible.

Default: *disabled*

Automatically select current location By default all computers that have been selected the previous time are displayed after starting Veyon Master. If you want to display all computers at the master computer's location instead, this option can be enabled. Veyon Master will then try to determine the location of the local computer by using the configured *network object directory*. All computers at the same location will then be selected and displayed. For this function to work properly, a correctly functioning DNS setup in the network is required so that both computer names can be resolved to IP addresses and reverse lookups for IP addresses return valid computer names.

Default: *disabled*

Automatically adjust computer thumbnail size If the size of the computer thumbnails should be adjusted automatically upon starting Veyon Master (same effect as clicking the *Auto* button manually), this option can be enabled. The previously configured size will be ignored. This functionality is especially useful in conjunction with the *automatic location change*.

Default: *disabled*

Automatically open computer select panel You can use this option to define that the computer select panel is opened upon program start by default.

Default: *disabled*

Computer locations

Show current location only Per default, the computer select panel lists all locations provided by the configured *network object directory*. If this option is enabled only the location of the master computer will be displayed instead. This can make the user interface more clear especially in larger environments with many locations.

Default: *disabled*

Allow adding hidden locations manually When the option *Show current location only* is enabled the user can still be allowed to add otherwise hidden locations manually. If this option is enabled an additional button *Add location* is shown in the computer select panel. This button opens a dialog with all available locations.

Default: *disabled*

Hide local computer In regular usage scenarios it often is not desired to display the own computer as this would start globally started features on the own computer as well (e.g. screen lock). Enabling this option will always hide the local computer to prevent such issues.

Default: *disabled*

Hide empty locations In some situations the *network object directory* may contains locations without computers, for example due to specific LDAP filters. Such empty locations can be hidden automatically in the computer select panel by enabling this option.

Default: *disabled*

Hide computer filter field The filter field for searching computers can be hidden through this option. This allows to keep the user interface as simple as possible in small environments.

Default: *disabled*

Modes and features

Enforce selected mode for client computers Some of Veyon's features change the operating mode of a computer e.g. the demo mode or the screen lock mode. These modes are enabled only once and are not restored in case of a physical computer reboot. If this option is enabled, the mode will even be enforced after a connection has been closed.

Default: *disabled*

Show confirmation dialog for potentially unsafe actions Actions such as rebooting a computer or logging off users can have undesired side effects such as data loss due to unsaved documents. In order to prevent unintentional activation of such features a confirmation dialog can be enabled through this option.

Default: *disabled*

Feature on double click This setting allows to define a feature to be triggered whenever a computer is double-clicked. In most cases it's desired to use the *remote control* or *remote view* feature here.

Default: *no function*

Features

The two lists in the *Features* allow to define which features are made available in Veyon Master. Single features can be disabled if necessary so that respective buttons and context menu entries are not displayed. This can help to simplify the user interface if certain features are never used anyway.

A feature can be moved from one list to the other by selecting it and clicking the respective button with the arrow icon. Alternatively a feature can simply be double-clicked to move it to the other list.

Access control

Computer access control

User groups backend A user group backend provides user groups and their members (users) required for access control. While the default backend is suitable for system user groups the LDAP backends will make LDAP/AD user groups available for access control.

Enable usage of domain groups When using access control in combination with the default backend only the local system groups are available per default. By enabling this option all groups of the domain which a computer belongs to can be queried and used. This option is not enabled per default for performance reasons. In environments with a huge number of domain groups performing access control can take a long time. In such scenarios you should consider setting up the *LDAP/AD integration* and use one of the *LDAP* backends.

Default: *disabled*

Grant access to every authenticated user (default) If the selected authentication scheme is sufficient (e.g. when using a key file authentication with restricted access to the key files), this option can be enabled. In this mode no further access control is performed.

Restrict access to members of specific user groups In this mode access to a computer is restricted to members of specific user groups. These authorized user groups can be configured in section *User groups authorized for computer access*.

Process access control rules This mode allows detailed access control based on user-defined access control rules and offers the greatest flexibility. However, its initial setup may be slightly more complicated and time-consuming, so you should choose one of the other two access control modes for initial testing.

User groups authorized for computer access

Configuration of this access control mode is straightforward. The left list contains all user groups provided by the selected backend. By default these are all local user groups. If *LDAP/AD Integration* is configured, all LDAP user groups are displayed. You can now select one or more groups and move them to the right list using the corresponding buttons between the two lists. All members of each group in the right list can access the computer. Do not forget to transfer the configuration to all computers afterwards.

The *Test* button in the *Computer access control* section can be used to check whether a particular user is allowed to access a computer via the defined groups.

Access control rules

The setup of a ruleset for access control including use cases is described in detail in chapter *Access control rules*.

Authentication keys

Key file directories

Placeholder variables should be used for both base directories. All information on supported variables can be found in section *Placeholder variables for file paths*. On Windows UNC paths can be used instead of absolute paths.

Public key file base directory The specified base directory contains subdirectories for each key name (e.g. user role) with the actual public key file inside. This allows to set individual access permissions for the subdirectories. The public key files are placed in the corresponding subdirectory below the base directory on both creation and import. When loading the respective public key file for authentication the Veyon Service uses this base directory as well.

Default: *%GLOBALAPPDATA%/keys/public*

Private key file base directory The specified base directory contains subdirectories for each key name (e.g. user role) with the actual private key file inside. This makes it possible to define individual access rights for the subdirectories. During creation and import, the private key files are placed in the corresponding subdirectory below the base directory. Veyon Master searches for accessible private key files under this base directory and uses the private key files to authenticate against the Veyon Service on client computers.

Default: *%GLOBALAPPDATA%/keys/private*

Demo server

In the configuration page for the demo server, you can make some fine tunings to improve the performance of the demo mode. These settings should only be changed if the performance is not satisfactory or if only a small network bandwidth is available for data transfer.

Update interval This option can be used to set the interval between two screen updates. The smaller the interval, the higher the refresh rate and the smoother the screen transfer. However, a lower value leads to a higher CPU load and increased network traffic.

Default: *100 ms*

Key frame interval During a screen broadcast, only changed screen areas are sent to the client computers (incremental updates) in order to minimize the network traffic. These updates are performed individually and asynchronously for each client, so that after a while the clients may no longer run synchronously depending on bandwidth and latency. Therefore, complete screen contents (*key frames*) are transmitted at regular intervals, so that a synchronous image is displayed on all clients at the latest when the key frame interval expires. The lower the value, the higher the processor and network traffic.

Default: *10 s*

Memory limit All screen update data is stored by the demo server in an internal buffer and then distributed to clients. To prevent the internal buffer between two key frames from occupying too much memory due to too many incremental updates, the value specified here is used as a limit. This limit is a soft limit, so that if it is exceeded, a key frame update is attempted (even if the key frame interval has not yet expired), but the buffer still retains all data. The buffer is only reset when the double value is exceeded (hard limit). If there are repeated interruptions or delays while broadcasting a screen, this value should be increased.

Default: 128 MB*

LDAP

All options for connecting Veyon to an LDAP-compatible server are described in detail in chapter *LDAP/AD integration*.

Placeholder variables for file paths

Placeholder variables have to be supplied in the format `%VARIABLE%` on all platforms.

`%APPDATA%`

This variable is expanded to the user-specific directory for application data stored by Veyon, e.g. `...\User\AppData\Veyon` on Windows or `~/.veyon` on Linux

%HOME%
: This variable is expanded to the home directory/user profile directory of the logged on user, e.g. `C:\Users\Admin` on Windows or `/home/admin` on Linux

%GLOBALAPPDATA%
: This variable is expanded to the system-wide directory for Veyon's application data, e.g. `C:\ProgramData\Veyon` on Windows or `/etc/veyon` on Linux

%TEMP%
: This variable is expanded to the user-specific directory for temporary files, on Windows `C:\Windows\Temp` is used for the Veyon Service and `/tmp` on Linux

Environment variables

Veyon evaluates various optional environment variables allowing to override default settings for runtime settings such as session ID, log level and authentication keys to use.

VEYON_AUTH_KEY_NAME
: This variable allows to explicitely specify the name of the authentication key to use in case multiple authentication keys are available. This can be used to override the default behaviour of Veyon Master which uses the first readable private key even if multiple private key files are available.

VEYON_LOG_LEVEL
: This variable allows to override the configured log level at runtime, e.g. for debugging purposes.

VEYON_SESSION_ID
: This variable allows to specify the session ID and is evaluated by Veyon Server. When multi session support (multiple graphical sessions on the same host) is enabled each Veyon Server instance has to use distinct network ports for not conflicting with other instances. A server therefore adds the numerical value of this environment variable to the configured *network ports* to determine the port numbers to use. Usually this environment variable is set by Veyon Service for all Veyon Server instances automatically. In the *Network object directory* the absolute port (Primary service port + session ID) must be specified along with the computer/IP address, e.g. `192.168.2.3:11104`.

1.1.8 Troubleshooting

Important: If you encounter interaction or connection problems between master and client computers you should always ensure that an identical Veyon configuration is used on all computers. To avoid problems in general it's recommended to automate the configuration transfer during *installation* or via the *Command line interface* instead of importing the configuration manually using the Veyon Configurator. The configuration must also be transferred to all affected computers each time a change is made during troubleshooting.

Computers can't be accessed

There are multiple causes which can prevent the access to a computer using Veyon Master.

Networking problems

First of all the general network connectivity of the computer should be checked. Use the utility `ping` (which is usually included with every operating system) to diagnose connectivity problems.

Problems with the Veyon Service

If the computer can be pinged you should verify that the Veyon Service is running correctly. Open the Veyon Configurator and open the configuration page *Service*. In the section *General* the status of the service should be displayed with status *Running*. Otherwise the service can be started using the button *Start service*. If this is not successful you should try reinstalling Veyon. If a new installation does not help you can check the log files of the Veyon Service as well as the logging messages of the operation system for error messages and possible causes. Additionally you can find more hints or settings in the service management of your operating system.

Service and firewall settings

If the service is running you have to ensure that it is listening for incoming connections on the correct network port. You can verify that on the local computer using `telnet`:

```
telnet localhost 11100
```

Besides general program output the character string `RFB 003.008` must be displayed. If the output does not contain these characters you should check the *network settings*, especially the primary service port. You should try to reset them to their default values.

Next the same access has to be possible from a different computer in the network. The utility `telnet` can be used again for the diagnosis. The program argument `localhost` has to be replaced with the name or IP address of the corresponding computer. If the access fails please ensure that the option *Allow connections from localhost only* in the *network settings* is disabled. Additionally *computer access control* should be disabled initially as the service otherwise might listen on `localhost` only. This can happen if the external access would be denied because of currently matching rules. If both settings are correct the output of

```
netstat -a
```

has to indicate that the service is not (only) listening on `localhost` or `127.0.0.1` (status `LISTEN` or similar).

If the port access from remote computers still fails usually a firewall prevents the access and has to be reconfigured accordingly. On Linux this concerns settings of `iptables`, `ufw` etc. Consult the corresponding manuals of the used software. On Windows Veyon automatically configures the integrated Windows firewall if the option *Enable firewall exception* in the *network settings* is set to its default value (*enabled*). If a 3rd party firewall solution is used it must be configured to allow external access to TCP ports 11100 (primary service port) and 11400 (demo server).

Authentication settings

Another cause of error can be wrong or insufficient *authentication settings*. For first tests you should select *logon authentication* instead of *key file authentication* on both computers. As soon as the authentication test is successful on the local computer external access will also work.

If *key file authentication* is used the key files on master and client computers must match exactly. On client computers the public key file must have exactly the same content as on the master computer. If the access still fails the access permissions to the key files may be wrong. The Veyon Service needs to have read permissions on the *public key file* while the user of Veyon Master has to be able to read the *private key file*. If the problem persists the *key file directories* of the key files should be deleted on all computers and a new keypair generated on the master computer. The public key must then be imported again on all client computers.

Settings for computer access control

An incorrect configuration of computer access control can also lead to computers being inaccessible. Initially it's recommended to disable *computer access control* completely using the Veyon Configurator. This allows to determine which method for computer access control is possibly incorrectly configured.

If *authorized user groups for computer access* are used you should check whether the list of authorized user groups is complete and whether the accessing user is member of one of these user groups.

Improperly configured *access control rules* can also cause problems with accessing computers. It is necessary to always specify at least one rule to allow access under certain conditions. If this is ensured, a temporary test rule can be inserted at the end of the list for further debugging. This rule should be configured so that the option *Always process rule and ignore conditions* is enabled and the action *Allow access* is selected. This rule can then be moved up in the rule list step by step until the test returns the desired positive results and the access works. The access rule located directly below the test rule is then the cause for the access denial and can be examined more closely and corrected accordingly. Don't forget to remove the test rule afterwards to prevent unauthorized access.

Settings are not correctly saved/loaded

After updating to a new version of Veyon it may happen in rare cases that some configuration keys are inconsistent and need to be recreated. This can result in settings not being saved or reloaded correctly, such as the builtin location and computer information. In this case the *configuration should be reset* and rebuilt based on the default values.

Locations and computers from LDAP directory are not displayed in Veyon Master

Please make sure that:

- the *network object directory* on configuration page *General* is set to *LDAP Basic* or *LDAP Pro*
- LDAP integration tests *List all entries of a location* and *List all locations* are successful and return proper objects
- on the configuration page *Master* all options for fine-tuning the behavior are set to their default values

Selecting current location automatically doesn't work

If the *option automatically selecting the current location* is activated, but has no effect when starting Veyon Master, you should first make sure that the master computer is also listed as a computer for the respective room in the *network object directory*.

If the problem persists although all entries in the network object directory are correct, there is usually a problem with the DNS configuration in the network. Make sure that computer names can be resolved to IP addresses and reverse lookups of IP addresses return the corresponding computer names. On most operating systems, the DNS diagnostic tool `nslookup` is available for this purpose. Calling the program with the local computer name as argument must return a valid IP address. A second call with the determined IP address must again return the computer name.

If the function does not work as desired despite correct DNS setup, in the second step the *log level* can be set to the highest value (*Debug messages and everything else*). After restarting Veyon Master, you can search the log file `VeyonMaster.log` in the *log file directory* for further error causes. The lines with the messages *"initializing locations"* and *"found locations"* indicate which host names and IP addresses were used to determine the location and which locations were eventually determined on the basis of these information.

Screen lock can be bypassed via Ctrl+Alt+Del

To completely block all keystrokes and keyboard shortcuts in screen lock mode, you must restart your computer after installing Veyon on Windows. Without a restart, the Veyon-specific driver for input devices is not yet active and keystrokes cannot be intercepted.

In demo mode, only a black screen or window is displayed on client computers

Please make sure that:

- in the configuration page *Service* under *network settings* the demo server port is set to its default value `11400`
- on the configuration page *Service* the firewall exception is enabled on the master computer or a third party firewall is configured to allow incoming connections to TCP port `11400`
- the user of Veyon Master has access to its own computer (i.e. the local Veyon Service). In the *access control ruleset* there may exist a rule prohibiting access to the computer if a teacher is logged on. In this case you should create a rule with the condition *Accessing computer is localhost* enabled as far up the list of rules as possible. Otherwise the demo server is unable to access the teacher computer's screen content and distribute it to the client computers.

Veyon Server crashes with XIO or XCB errors on Linux

There are known issues with specific KDE and Qt versions on Linux causing the Veyon Server to crash. This affects several other VNC server implementations as well. If you're affected by such crashes consider upgrading KDE/Qt. As a last resort you can disable the X Damage extension in the VNC server configuration. This will however decrease overall performance and increase the CPU load.

1.1.9 FAQ - Frequently Asked Questions

Does Veyon run under Chrome OS (ChromeBooks) or MacOS?

Currently Veyon is only available for Linux- and Windows-based environments. Support for other platforms is being worked on though. The Veyon project relies on the help of experienced software developers, especially for porting Veyon to macOS and Android.

How can I add computers in order to access them?

If the default *Network object directory* is used, all you need to do is add the appropriate locations and computers on the *Locations & computers* configuration page. Afterwards the added resources are available in Veyon Master.

If *LDAP/AD integration* is configured the network object directory has to be changed to the appropriate LDAP backend so that the computers from the directory are displayed in the Veyon Master.

How can I migrate an existing iTALC installation to Veyon?

Although iTALC and Veyon are conceptually similar, a complete new installation and configuration is necessary to use Veyon, since configuration and file formats as well as their paths have changed and are not compatible. For a migration iTALC has to be uninstalled completely first. It is recommended to reboot the computer afterwards. Veyon can then be installed and configured in the same way as iTALC.

While the configuration of authentication methods is very similar, the configuration of locations and computers is done via the Veyon Configurator and no longer in the Master application. In this context you should check whether the new *LDAP/AD integration* can be used to make locations and computers automatically available in Veyon.

Is it possible to use Veyon Master on more than one computer?

The usage of Veyon Master on multiple computers is possible without any restrictions. For this to work an identical configuration has to be used on all master computers like its required for client computers in general. If logon authentication is used no further steps are necessary. If key file authentication is used the same private key has to be distributed to all master computers.

How can an existing VNC server be used in conjunction with Veyon?

In some environments a VNC server is already installed (e. g. UltraVNC) or is provided by the system (e. g. VNC-based access to virtual desktops in VDI environments). This may result in degraded performance or conflicts with the Veyon-internal VNC server. In such cases it is recommended to configure Veyon to use the existing (external) VNC server instead of starting the internal VNC server. The configuration is done through the Veyon Configurator on the configuration page *Service* in section *VNC server*.

Can I import/use an existing or generated file with location and computer information?

As of Veyon 4.1, there is a new *module for the command line interface*. This module can be used to import locations and computers from any kind of text files (including CSV files) into the builtin network object directory.

How can I view or control all monitors of a remote computer?

On Windows by default only the primary monitor of a computer is accessible with Veyon. You can however change this behaviour in the *VNC server* configuration. Select the VNC server plugin *Builtin VNC server* and enable the option *Enable multi monitor support*.

How can I import or export the selection of displayed computers?

The selection of displayed computers is saved in the personal *user configuration*. There are two ways to share this configuration with multiple users. Either the user configuration file can be copied into the profile of the user, e.g. via login scripts. Alternatively, the user configuration can be also be stored in a shared directory (e.g. a network drive) and the *user configuration setting* has to be changed accordingly so that the user configuration is loaded from this directory. Please note that the access rights may have to be adjusted so that changes made by users are not written back into the global user configuration.

In this context please also refer the function *Automatic switch to current classroom*, which can be used to directly realize the desired behavior.

How can I hide the master computer from computer locations?

All you need to do is enable the option *Hide local computer* in the master configuration page.

What happens if there is no matching access control rule?

If there is no rule where all activated conditions apply when processing the configured access control rules, access is denied and the connection is closed. This prevents an attacker from being accidentally granted access due to an incomplete ruleset.

1.1.10 Technical glossary

From Wikipedia, the free encyclopedia

ACL Access Control List

Client a piece of computer hardware or software that accesses a service made available by a server.

See also:

https://en.wikipedia.org/wiki/Client_(computing)

FAQ a list of frequently asked questions (FAQs) and answers on a particular topic.

See also:

https://en.wikipedia.org/wiki/FAQ

Host a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network address.

See also:

https://en.wikipedia.org/wiki/Host_(network)

Hostname a label that is assigned to a device connected to a computer network and that is used to identify the device in various forms of electronic communication, such as the World Wide Web.

See also:

https://en.wikipedia.org/wiki/Hostname

IP the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

See also:

https://en.wikipedia.org/wiki/Internet_Protocol

IP Address a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

See also:

https://en.wikipedia.org/wiki/IP_address

IPv6 the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

See also:

https://en.wikipedia.org/wiki/IPv6

Port an endpoint of communication. Physical as well as wireless connections are terminated at ports of hardware devices. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service.

See also:

https://en.wikipedia.org/wiki/Port_(computer_networking)

TCP one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.

See also:

https://en.wikipedia.org/wiki/Transmission_Control_Protocol

URL a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

See also:

https://en.wikipedia.org/wiki/URL

- genindex

1.2 Veyon User Manual

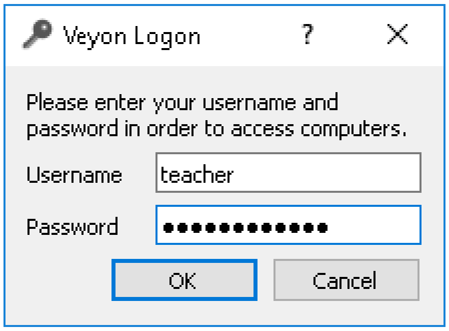
1.2.1 Introduction

Veyon is an application that allows to monitor and control a group of computers (e.g. classrooms) on a central computer (e.g. an instructor's computer) and to use different features and modes.

Program start and login

The program is started via the start menu or a desktop icon:

Depending on the system configuration you will be prompted for your username and your password:



Please enter your username and password in order to access computers.

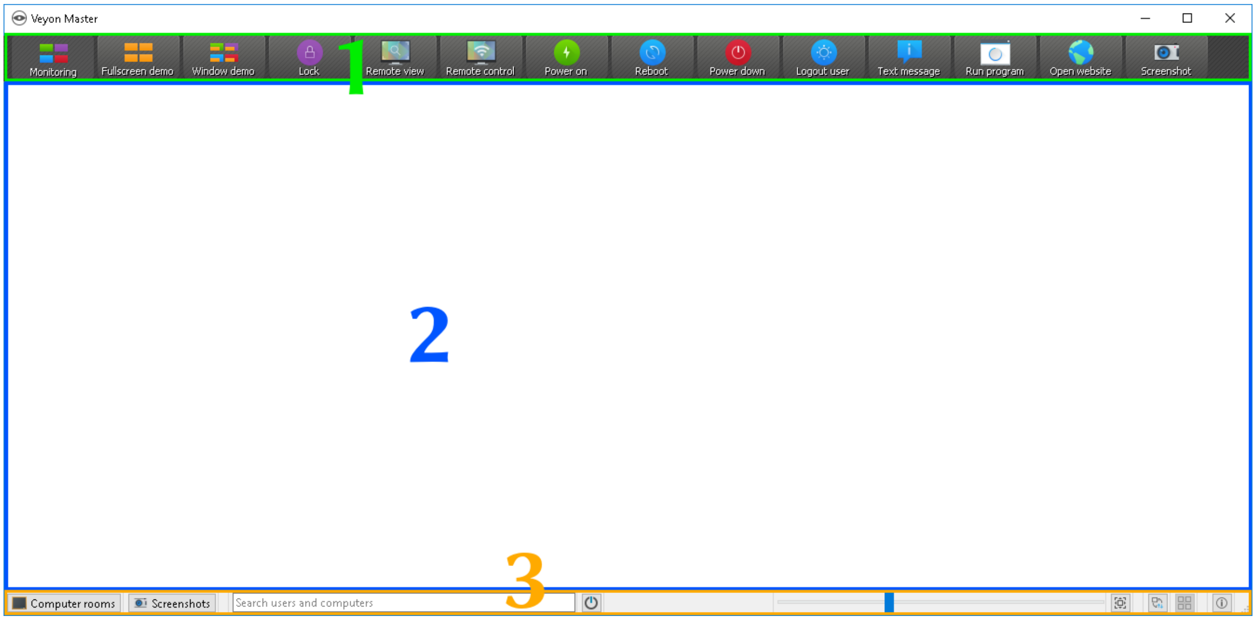
Username teacher

Password ●●●●●●●●●●●●

Enter your username and password here or – if given – the credentials of a special teacher account. If the entered data is correct and and a a login can be performed, the program will start. Otherwise, the login will be denied and an error message will be displayed. In this case you can try the login with corrected data again.

User interface

After the program start you will see the user interface with the toolbar (1), the monitor view (2) and the status bar with various controls (3):



The toolbar contains a number of buttons for activating different features. A detailed description of the individual features can be found in chapter *Program features*. The appearance and behavior of the toolbar can be customized as described in section *Toolbar*.

In the monitor view all computers to be monitored are displayed in a tile view. Depending on the system configuration and previous program starts you can already see the computers at your current location here. The *computer select panel* allows you to show or hide computers or entire locations.

The elements in the status bar are used to control the program interface and are described in detail in the following section.

Status bar

Using the *Locations & computers* and *Screenshots* buttons, you can open and close the *computer select panel* and the *screenshots panel*.

The search bar allows you to filter the computers displayed using computer names or user names as search terms. Technically savvy users can even enter regular expressions here to define advanced search filters.

The (*Only show powered on computers*) button hides all computers that are not powered on, disconnected or not reachable for some other reason. This allows simultaneous monitoring of a large number of computers or partially occupied rooms while focusing on the actually active computers.

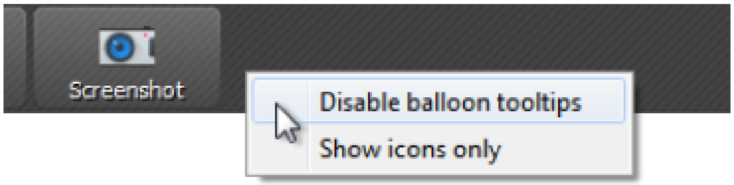
Use the slider to control the size of the computer screens displayed. When holding then `Ctrl` key, the size can also be changed using the mouse scroll wheel. The size is adjusted automatically by clicking the button (*Adjust optimal size*) to the right of it.

It is also possible to use a custom computer arrangement, e.g. to represent the actual arrangement of computers in classrooms. After clicking the button (*Use custom computer arrangement*) each computer individually or a selection of computers can be moved with the left mouse button pressed and arranged as desired. To align all computers in the custom arrangement, click the (*Align computers to grid*) button. If you want to use the sorted standard arrangement again, simply deactivate the button.

The ⓘ button (*About*) opens a dialog with information about Veyon such as version, manufacturer and license terms.

Toolbar

You can customize the appearance and behavior of the toolbar. A right click on either a free section or a button opens a context menu with several entries:



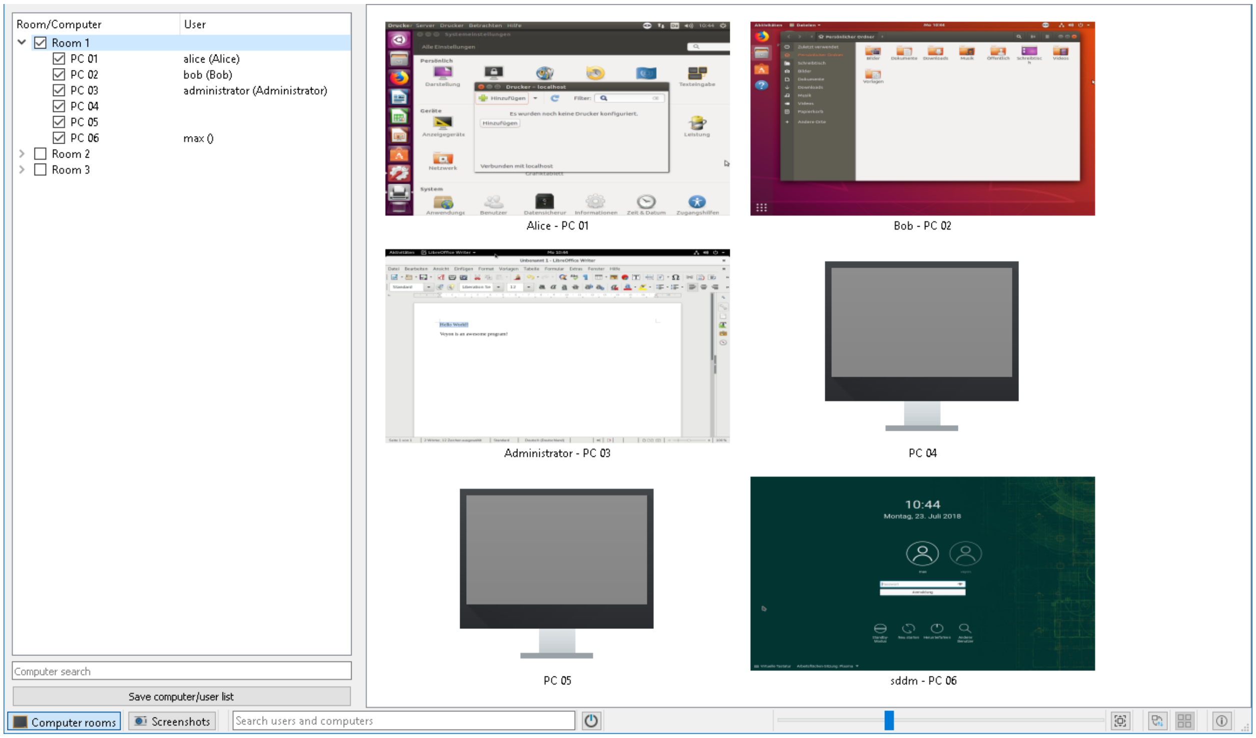
If you click the entry *Disable balloon tooltips* no tooltips will be displayed anymore whenever you hover the mouse over the buttons. You can open the context menu at any time and uncheck the item again.

The *Show icons only* option gives a compact view of the toolbar buttons by hiding the labels and displaying only icons. On smaller screens this option may be necessary to display all buttons.

Computer select panel

The *Locations & Computers* button in the status bar opens the computer select panel. This panel displays all available computer locations in a tree structure. You can expand individual location entries by clicking on the corresponding symbol in front of them.

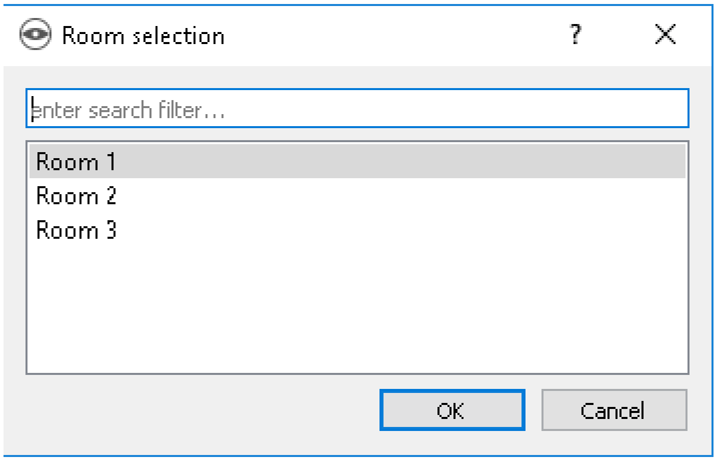
You can activate individual computers or entire locations by checking them. All checked computers will then be displayed in the monitoring view.



Room/Computer	User
☑ Room 1	
☑ PC 01	alice (Alice)
☑ PC 02	bob (Bob)
☑ PC 03	administrator (Administrator)
☑ PC 04	
☑ PC 05	
☑ PC 06	max ()
□ Room 2	
□ Room 3	

With the *Save computer/user list* button you can save the list of computers and logged in users in a CSV file. Typical use cases for this are subsequent presence checks or IT-based exams.

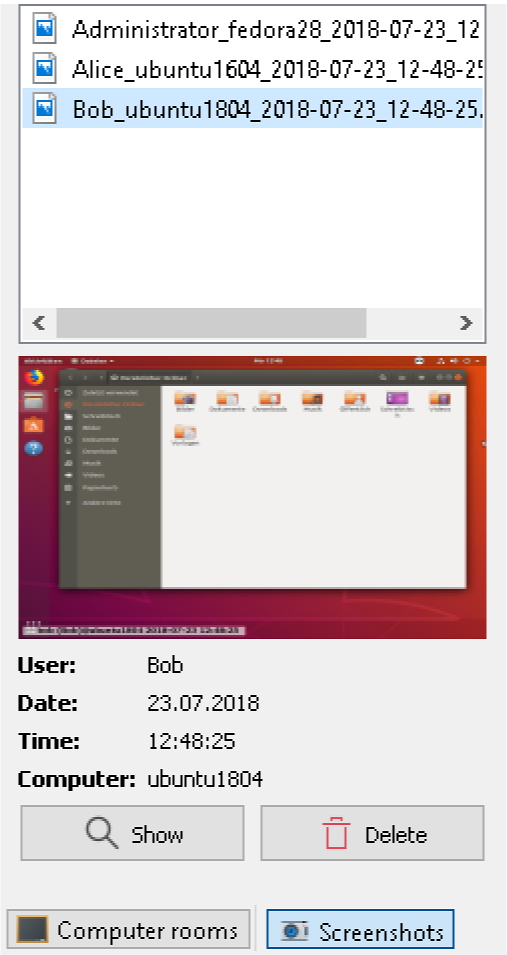
Depending on the system configuration, the button *Add location* is also available. This allows you to add more computer locations to the view. A click on the button opens a dialog where you can see all available locations:



You can filter the list using the input field, i.e. enter a search term. The list then only displays the location names containing the specified search term. Advanced users can also use regular expressions for the filter. Next you can select the location and confirm with *OK*. The selected location is now available in the location list until the next program start. You can also remove a previously added location by clicking on the location and pressing the `Del` key.

Screenshots panel

Using the screenshot management panel, you can view and delete all captured screenshots. The *Program features* chapter in section *Screenshot* explains how to take a screenshot.



Administrator_fedora28_2018-07-23_12

Alice_ubuntu1604_2018-07-23_12-48-2!

Bob_ubuntu1804_2018-07-23_12-48-25.

User: Bob

Date: 23.07.2018

Time: 12:48:25

Computer: ubuntu1804

You can now select individual screenshots from the list. Details of the screenshot, such as the date it was taken, user name, and computer, are then displayed in the table below. The *Show* button or a double-click in the list displays the selected screenshot in full size. If you no longer need the screenshot, you can permanently delete it using the *Delete* button. Please note that this process cannot be undone and the files will not be moved to the trash.

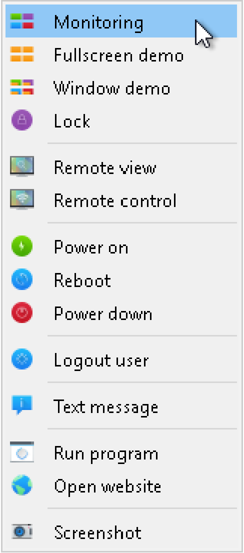
1.2.2 Program features

Veyon offers a variety of features that let you control and access computers. All available features are accessible through the buttons in the toolbar as well as the context menu of individual computers.

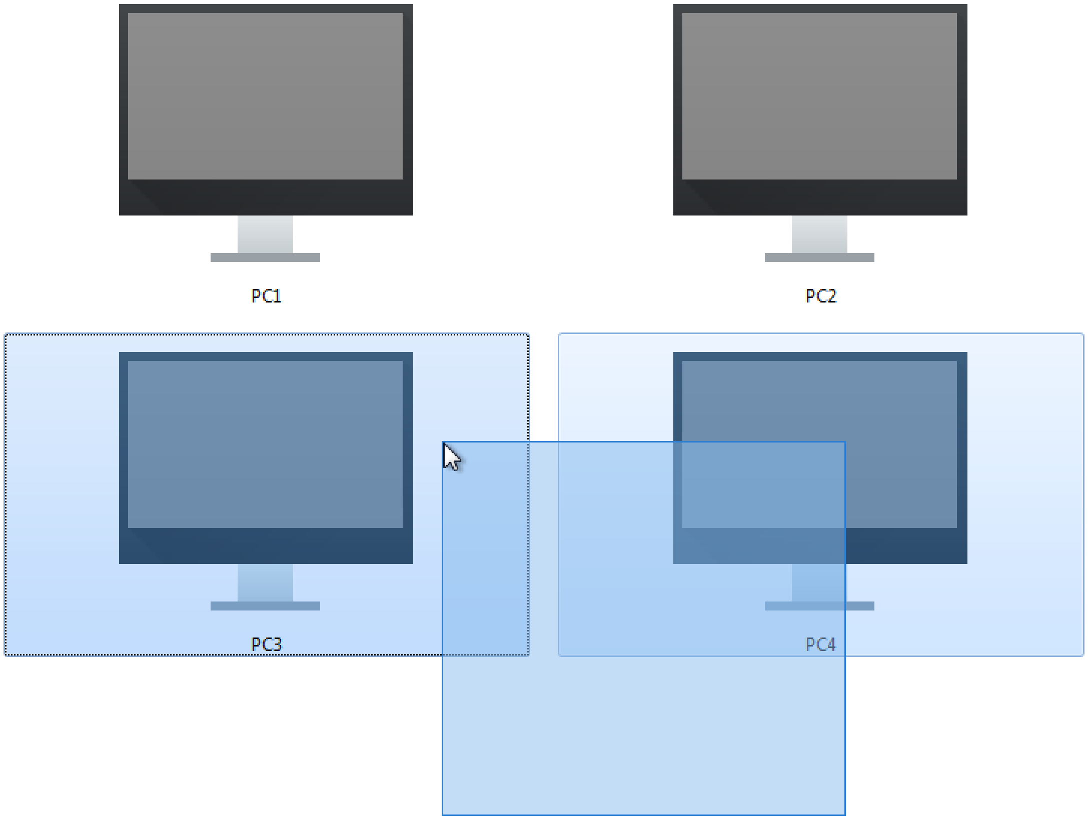
If you move the mouse over the individual buttons in the toolbar, a tooltip with a short help text is displayed unless you have disabled tooltips. Pressing a button activates the desired feature on all displayed computers.

Using functions on individual computers

If you only want to activate a function on a single computer, right-click the computer in the monitor view and select the desired function from the context menu. The entries in the context menu are displayed dynamically depending on the active functions.



You can also select multiple computers in the monitoring view by drawing a selection rectangle with the mouse that includes all desired computers:



Alternatively, you can press the `Ctrl` key and add computers individually to the selection via mouse click.

Monitoring mode

By default Veyon is running in monitoring mode. In this mode you have an overview of all computers and see their screen contents in thumbnails. The screen content is updated almost in real time, so you can monitor all activity at the selected locations.

As long as there is no connection to a computer, a computer icon is displayed instead of the screen content. After the program has been started, the icon is initially colored gray. As soon as the program detects that the computer is unreachable or access is denied, the color changes to red.

Some of the features described in the next sections switch the remote computers to a different mode. You can exit the respective mode by activating monitoring mode again.

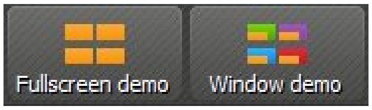
Demonstration mode

You can use the demonstration mode (demo mode) to start a presentation. In this mode, your screen content is broadcasted to all remote computers and displayed in real time. You can choose between a full screen and a window demo.

During a full screen demo your screen content will be displayed in full screen. Logged-in users cannot use their computers for other tasks in this mode because all input devices are locked. In this way you will gain the full attention of your students.

By contrast, a window demo allows users to switch between the demo window and their own applications. For example, course participants can arrange the windows side by side and try out the demonstrated steps themselves in parallel. The input devices are therefore not locked in this mode.

In order to start a full screen or window demo, you just have to press the *Fullscreen demo* or *Window demo* button:

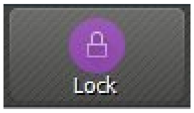


If you want to leave the demonstration mode again, simply press the button again or click on the *Monitoring* button to switch back to monitoring mode globally. The context menu can also be used to stop the demonstration mode on individual computers.

Lock screens

Another way to draw students' attention is to use the screen lock feature. As during a full-screen demonstration, all input devices on the students' computers are locked. The computers can then no longer be used. In addition, a blocking image is displayed to prevent distractions caused by open applications.

Press the *Lock* button to lock all displayed computers:



If you want to unlock the screens, simply press the button again or click the *Monitoring* button to switch back to monitoring mode globally.

If only individual computers are to be locked, you can select them as described in section *Using functions on individual computers* and select the feature in the context menu. The screen lock can then be deactivated either by selecting *Unlock* or switching back to *Monitoring* mode. The screen lock can also be activated globally at first and later deactivated for individual computers via the context menu.

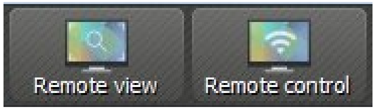
Note: Due to security restrictions of most operating systems, the lock screen can not be displayed if no used is logged on. The input devices are still locked, so that no user logon is possible.

Remote access

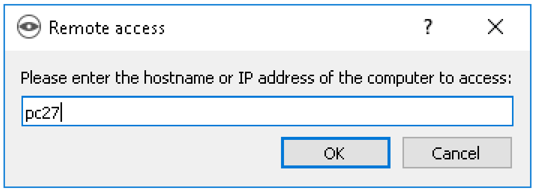
The function group *remote access* consists of two rather similar functions: *Remote View* and *Remote Control*. Both access modes retrieve the screen data of a remote computer and display it in full screen mode in a separate window. In contrast to the monitoring mode in the main window, you can the observe events on a computer in detail and interact, if necessary.

These functions can be activated in various ways. Depending on the system configuration, one of the two starts by double-clicking a computer. Alternatively you can open the context menu by clicking the right mouse button and choose the desired function.

If you want to access a computer that is not shown in the workspace, you can use the button in the toolbar:



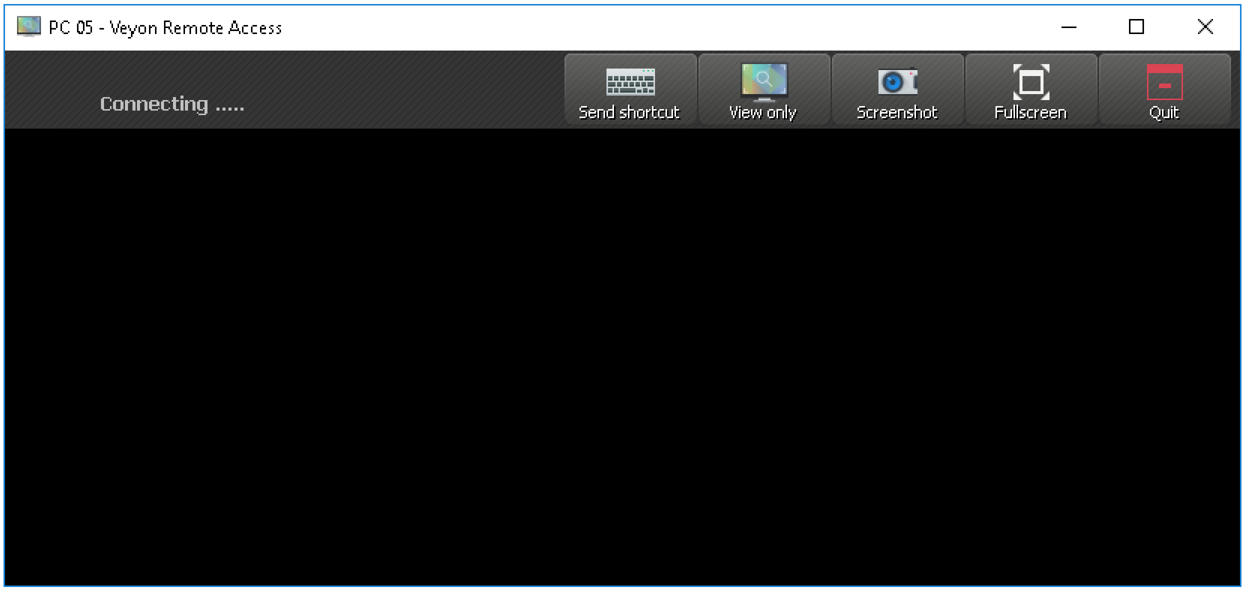
Upon confirmation a dialog opens up that prompts you for the computer name:



Please enter the hostname or IP address of the computer to access:

pc27

In all cases a new windows containing the remote view opens up:

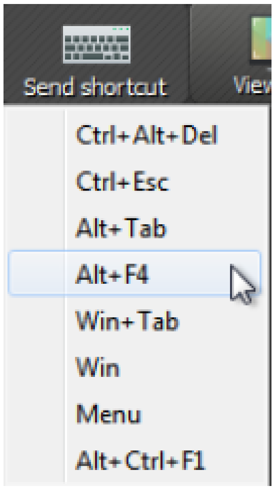


Connecting .....

The remote screen is usually displayed within a few seconds and is updated in real time. As in the main application you have a toolbar with buttons on the window's upper border. This toolbar is automatically hid after a few seconds. You can show it at any time by moving the cursor to the window's upper border.

Even during a running remote access session you can change the access mode at any time. For this it is sufficient to click the *Control from remote* resp. *Observe only* button. Please note, that these buttons do not indicate the current access mode, but the access mode that is switched to if the button is pressed.

As soon as you have entered the *Control from remote* mode, your keystrokes, mouse movements and mouse clicks are transmitted to the remote computer. Thus you can control it as you are used to. Depending on the system configuration there may be exceptions concerning some special keys or keystroke combinations (shortcuts) such as e.g. `Ctrl+Alt+Del`. If you want to use these shortcuts, you can use the additional *Send Shortcut* button. After clicking it, a menu opens up which allows for you to select the desired shortcut:



You can close the menu without triggering an action with a repeated click or the `Esc` key.

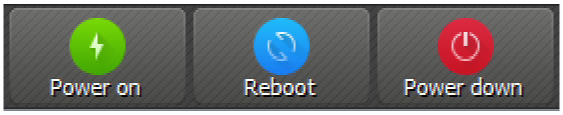
If you want to switch to full screen mode, you can use the *Full Screen* button. In full screen mode you can use the same button – now with the caption *Window* – to switch back to window mode.

The function *Screenshot* creates a screenshot an saves in to a file that can be viewed later on. A more detailed description can be found in sections *Screenshot* and screenshot management.

You can use the *Exit* button to close the window and terminate the remote access.

Boot, restart and shutdown a computer

It can be helpful for administrative purposes as well as for preparation and post-processing of courses and IT-supported exams to use the functions *Boot*, *Restart* and *Shutdown* for a computer. You find the respective buttons in the toolbar:



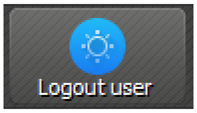
You can activate the respective button to boot, restart or shutdown all displayed computers. If you intend to use the function only for single computers, you can select them and choose the desired entry from the context menu.

Attention: Please note, that neither restart nor shutdown require the consent of the signed in user. Therefore make sure, that the signed in user has no unsaved work.

Note: Depending on the configuration of the network and the system settings of the single computer, booting may work only under specific technical conditions. At the same time there is no check for access control while booting so that you may be able to boot computers in other rooms or parts of the building. Please check the selected computers carefully if you use this function.

Log out user

The function *Log out User* complements the options described in the previous section in terms of controlling basic computer states. That's what the respective button in the toolbar looks like:



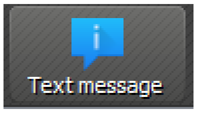
Activate this button to log out all users on all displayed computers. If you intend to use the function only for single computers, you can select them and choose the desired entry from the context menu.

Hint: A typical use case for this function could consist of terminating a course for all participants at a specified time.

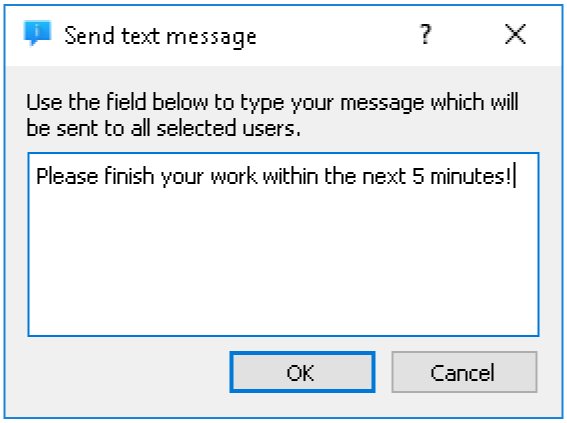
Attention: Please note, that the logout process does not require the consent of the signed in uesr. Hence make sure that the signed in user does not have any unsaved work.

Send text message

A further possibility for interaction consists of sending text messages to one or all course participants. This message is displayed as a message window on the respective participant's computer. You can use the *Text Message* button to this end:



After pressing the button, a dialog window opens up. Here you can enter the message to be transmitted:


Send text message

Use the field below to type your message which will be sent to all selected users.

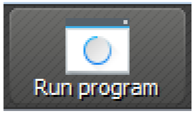
Please finish your work within the next 5 minutes!

You can send the typed message by pressing *OK*.

If you intend to use the function only for single computers, you can select them and choose the entry *Text Message* from the context menu.

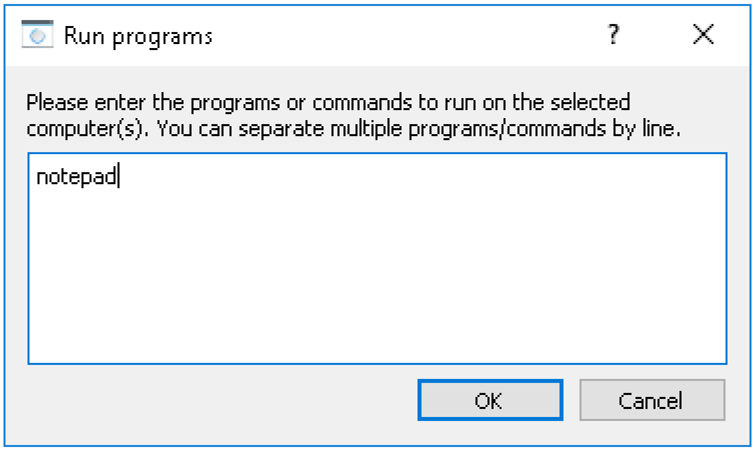
Start program

If a specific application is to be opened on all computers, you can use the *Start Program* function from the toolbar. To do this click the button shown:



If programs have been predefined by the administrator, a menu with the predefined programs opens. In this menu you can click on the desired program.

If you want to start a program that is not included in the menu, click on the last entry *guilabel:'Custom program*. Then the same dialog appears, which also appears if no programs are predefined. In this dialog box you can enter the name of the desired program file, e.g. `notepad`:



Please enter the programs or commands to run on the selected computer(s). You can separate multiple programs/commands by line.

notepad

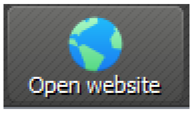
Subsequently confirm the dialog with *OK*. Please note, that the requested program often does not reside in the program path environment so that you have to specify the complete path to the program, e.g. `C:\Program Files\VideoLAN\VLC\vlc.exe`.

Hint: Most programs offer the option of getting passed an additional parameter containing the name of a file that is to be opened automatically. For example, if you want to play a video simultaneously on all computers, just add the path of the video file separated by a blank, e.g. `C:\Program Files\VideoLAN\VLC\vlc.exe X:\Videos\Example.mp4`.

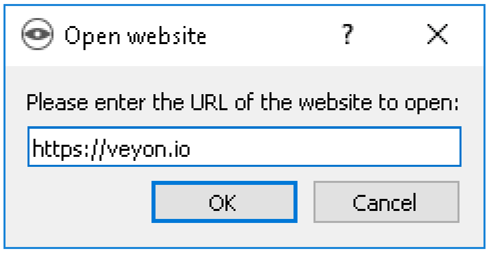
Attention: In case the program path or file name contains blanks, the complete path and file name has to be enclosed in quotes. Otherwise parts of the input can be interpreted as parameters. Example: `"C:\Program Files\LibreOffice 5\program\swriter.exe"`

Open Website

If all course participants shall navigate to a specific website, you can have this website automatically opened on all computers. Use the *Open Website* button for this:



If no websites have been predefined by the administrator, a dialog box opens in which you can enter the address of the website to be opened:



Please enter the URL of the website to open:

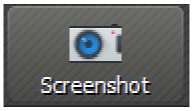
https://veyon.io

Confirm this dialog with *OK*.

Otherwise, a menu with the predefined websites opens from which you can select and click on the desired website. If you want to open a website that is not included in the menu, select the last item *:guilabel:'Custom Website*. The dialog shown above then opens.

Screenshot

With Veyon it is possible to save the current screen content of single or all computers in an image file. You can press the *Screenshot* button to make screenshots of all displayed computers:



If you intend to use this function only for single computers, you can select them and choose the entry *Screenshot* from the context menu.

Afterwards a message informs you about the successful completion of this action. Now you can view the images through the screenshot management as well as delete them if necessary.

1.2.3 FAQ - Frequently Asked Questions

Can other users see my screen?

Which user can access which computer under which circumstances depends on the system settings configured by your administrator. Usually the software is configured so that the course instructor can access the computers of course participants, but not vice versa. Whether other course instructors are able to see your screen or those of other course participants also depends on the settings. Contact your administrator in order to configure access control rules according to your needs as described in the administration manual.

How frequently are the computer thumbnails updated?

Usually the computer thumbnails in the monitoring view are updated once a second. Depending on the utilization of the network and the computer, there may be slight deviations. In contrast when remote controlling or viewing a computer, you see In contrast whe screen content of the remote computer in real time.

What happens if I accidentally close the Veyon Master application window?

Any active functions such as demo mode or screen lock are stopped when the program is closed. However, you can simply reopen the program and activate the mode again if necessary.

How can I broadcast the screen of a student to all other screens?

If you want to transfer a student's screen instead of your own screen in demo mode, first activate demo mode for all computers. Then stop demo mode for the student to be performing the demo using the context menu. Finally open the remote view for the students computer. This will transfer the remote view window - and therefore the student's screen - to all other computers.

1.2.4 Glossary

From Wikipedia, the free encyclopedia:

Button The term button (sometimes known as a command button or push button) refers to any graphical control element that provides the user a simple way to trigger an event, like searching for a query at a search engine, or to interact with dialog boxes, like confirming an action.

See also:

https://en.wikipedia.org/wiki/Button_(computing)

Context menu A context menu (also called contextual, shortcut, and pop up or pop-up menu) is a menu in a graphical user interface (GUI) that appears upon user interaction, such as a right-click mouse operation.

See also:

https://en.wikipedia.org/wiki/Context_menu

FAQ Frequently Asked Questions (FAQs) are a compilation of frequently asked questions and the corresponding answers to a topic. FAQs have become well-known in information technology, especially on the Internet, where many Usenet newsgroups have created a FAQ collection to relieve the pressure on the forums. Because the principle of the FAQ has proven itself, it exists in many areas.

See also:

https://en.wikipedia.org/wiki/FAQ

Graphical user interface Graphical user interface (GUI) refers to a form of user interface of a computer. It has the task of making application software operable on a computer by means of graphical symbols, controls or widgets. In computers, this is usually done by using a mouse as a control device to operate or select the graphic elements; in smartphones, tablets and kiosk systems, it is usually done by touching a sensor screen.

See also:

https://en.wikipedia.org/wiki/Graphical_user_interface

Input device Input devices are all devices that can be used to supply information to a computer so that interaction with computer programs is possible.

See also:

https://en.wikipedia.org/wiki/Input_device

Keyboard shortcut A keyboard shortcut is a series of one or several keys, such as "Ctrl+F" to search a character string. Such a directive invokes a software or operating system operation (in other words, cause an event) when triggered by the user.

See also:

https://en.wikipedia.org/wiki/Keyboard_shortcut

Password A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which is to be kept secret from those not allowed access.

See also:

https://en.wikipedia.org/wiki/Password

Screenshot A screenshot, also called screen capture or screen grab, is a digital image of what should be visible on a monitor, television, or other visual output device. A common screenshot is created by the operating system or software running on the device. A screenshot or screen capture may also be created by taking a photo of the screen.

See also:

https://en.wikipedia.org/wiki/Screenshot

Status bar A status bar is a graphical control element which poses an information area typically found at the window's bottom.[1] It can be divided into sections to group information. Its job is primarily to display information about the current state of its window, although some status bars have extra functionality. For example, many web browsers have clickable sections that pop up a display of security or privacy information.

See also:

https://en.wikipedia.org/wiki/Status_bar

Tooltip The tooltip or infotip or a hint is a common graphical user interface element. It is used in conjunction with a cursor, usually a pointer. The user hovers the pointer over an item, without clicking it, and a tooltip may appear—a small "hover box" with information about the item being hovered over.

See also:

https://en.wikipedia.org/wiki/Tooltip

Username A username is a name with which a user can log on to a computer, a website or a program. On the Internet, it is usually used to log on to a user account and requires registration.

See also:

https://en.wikipedia.org/wiki/User_(computing)

CHAPTER 2

PDF download

- Veyon Administrator Manual PDF
- Veyon User Manual PDF

Index