Veyon Administrator Manual

Release 4.1.2

Tobias Junghans

Sep 06, 2018

Contents

CHAPTER 1

Introduction

1.1 About this manual

This manual describes the installation and configuration of Veyon in a computer network and is addressed to system administrators and technically skilled users. For end users a separate user manual exists explaining usage and specific functions of the user program (Veyon Master).

The further sections of this chapter contain basic information about Veyon and its components which are of fundamental importance for putting Veyon into operation.

Chapter *Installation* deals with 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 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 is furthermore equipped with a command line interface (CLI) that can be used for modifying the configuration, automate Veyon-related tasks and for using or controlling specific program functions. 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*.

1.2 About Veyon

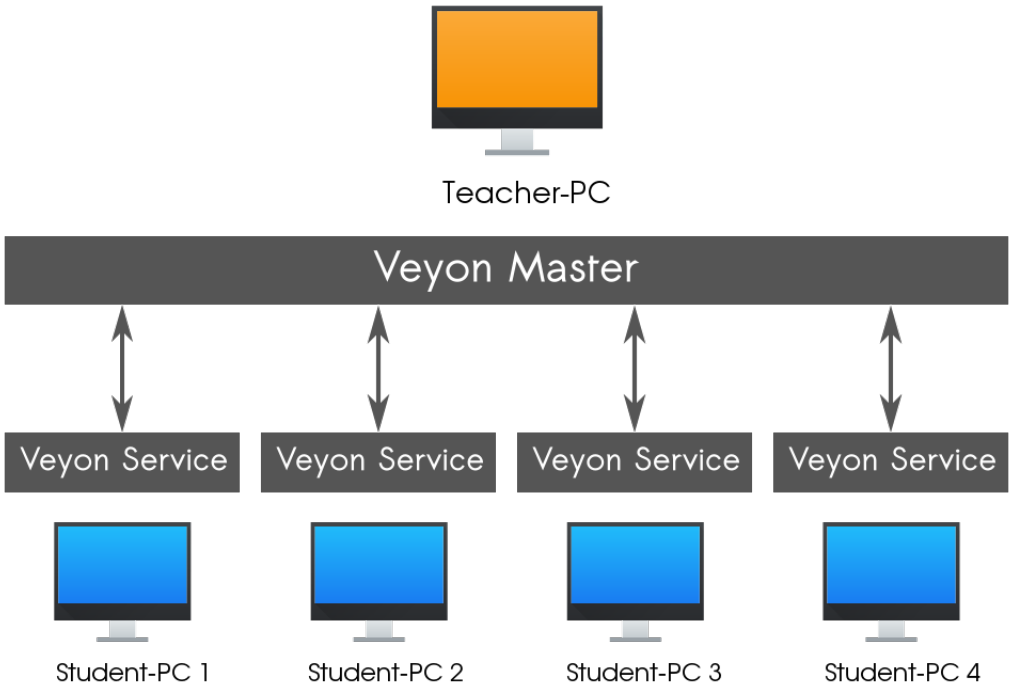
Veyon is a free and open source software for computer monitoring and class room management. It allows to monitor and control computer rooms as well as to interact with users, e.g. students. The following functions are available in Veyon:

- Overview of a (class) room with screen contents of computers being shown in thumbnails
- Remote view or control computers
- Broadcast the teacher's sceen to all other computers in real time (full screen/window demo)

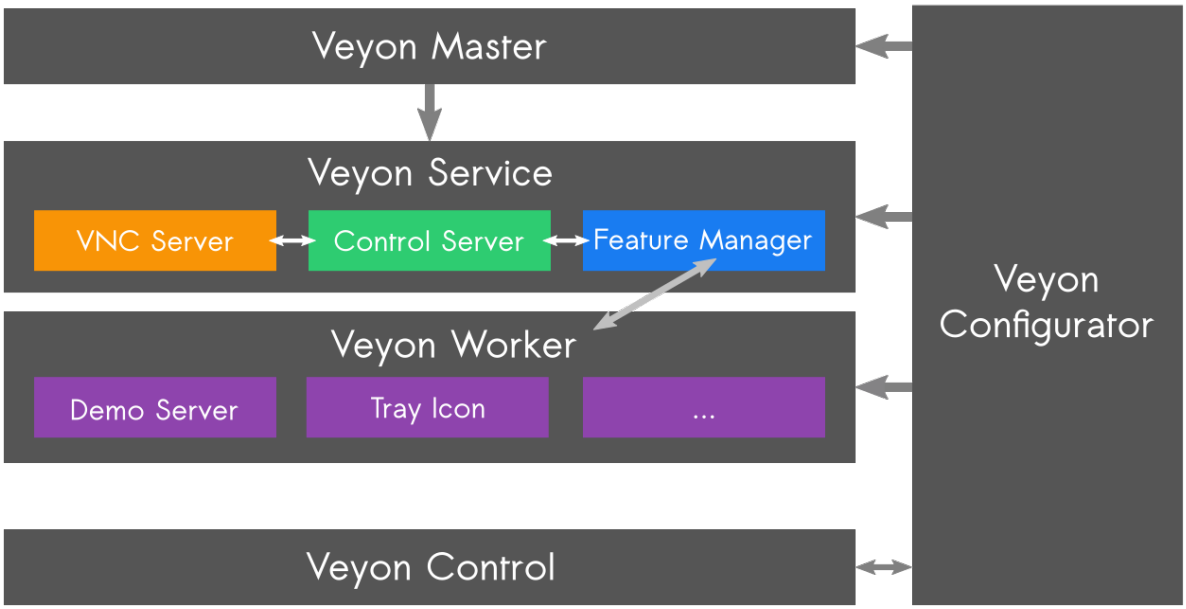
- Lock computers to control attention
- Send text messages to students
- Power on, reboot or shutdown computers remotely
- Log out users
- Launch programs and open websites

1.3 Components

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



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



Veyon Master An application program that can be used for monitoring and controlling other computers as well as for accessing Veyon features. Usually the program is started by the end user. It accesses other computers through 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. Under normal conditions this program is started by the Veyon Service automatically and with elevated privileges so it can't be terminated by users.

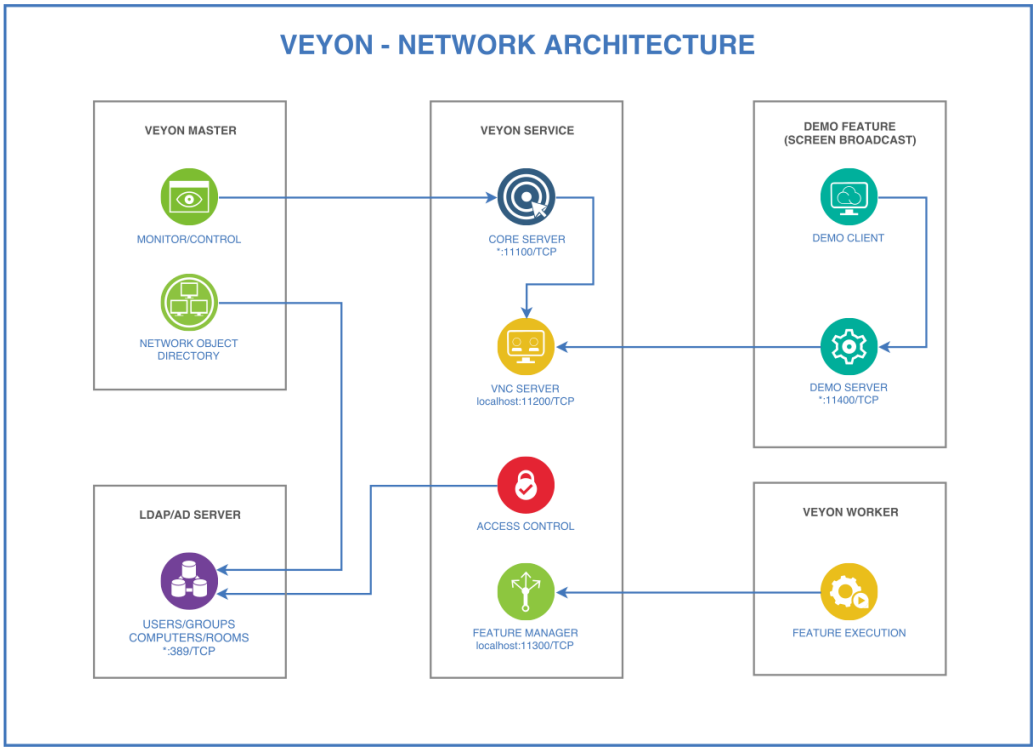
Veyon Worker A helper program started by the server to provide specific functions in an isolated environment or in the context of the user that is currently logged in. Those specific functions include the demo server for the teacher computer and the demo client on the student computers.

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

1.4 Network architecture

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


VEYON - NETWORK ARCHITECTURE
VEYON MASTER
MONITOR/CONTROL
NETWORK OBJECT DIRECTORY
VEYON SERVICE
CORE SERVER
*:11100/TCP
VNC SERVER
localhost:11200/TCP
ACCESS CONTROL
FEATURE MANAGER
localhost:11300/TCP
DEMO FEATURE (SCREEN BROADCAST)
DEMO CLIENT
DEMO SERVER
*:11400/TCP
LDAP/AD SERVER
USERS/GROUPS
COMPUTERS/ROOMS
*:389/TCP
VEYON WORKER
FEATURE EXECUTION

CHAPTER 2

Installation

2.1 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 processors 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 CPUs) 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.

On the software side an up-to-date operating system supported by the vendor or the community must be run. Those include:

- 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

Mixing Windows and Linux computers is no problem.

2.2 Preparing the installation

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

2.3 Installation on a Windows computer

Run the installer file with administrative privileges and follow the displayed instructions. On all computers on which no master application is required (e.g. student computers) you uncheck the component *Veyon Master* in the *Choose components* dialogue.

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

2.4 Installation on a Linux computer

The installation of Veyon on Linux heavily depends 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 different distributions are available at the Veyon download page. In all other cases it's always possible to compile and install a current version of Veyon from source. For further information please visit the Github page of Veyon.

2.5 Automated installation (silent installation)

2.5.1 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 helpful for automated deployments in larger environments. Veyon can thus be easily integrated with all common software distribution/deployment mechanisms.

After the installer has been run with command line parameter `/S`, all further operations are executed without requests for feedback or output. The same applies to the uninstaller.

2.5.2 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.

Apply Veyon configuration automatically after the installation:

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

Important: You must provide an absolute path to the configuration file, since the internally called command line tool (*Veyon Control*) is not listed as working directory in the installation directory. Please use either the suggested `%cd`-variable or replace with an absolute path.

Automated installation without Veyon Master:

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

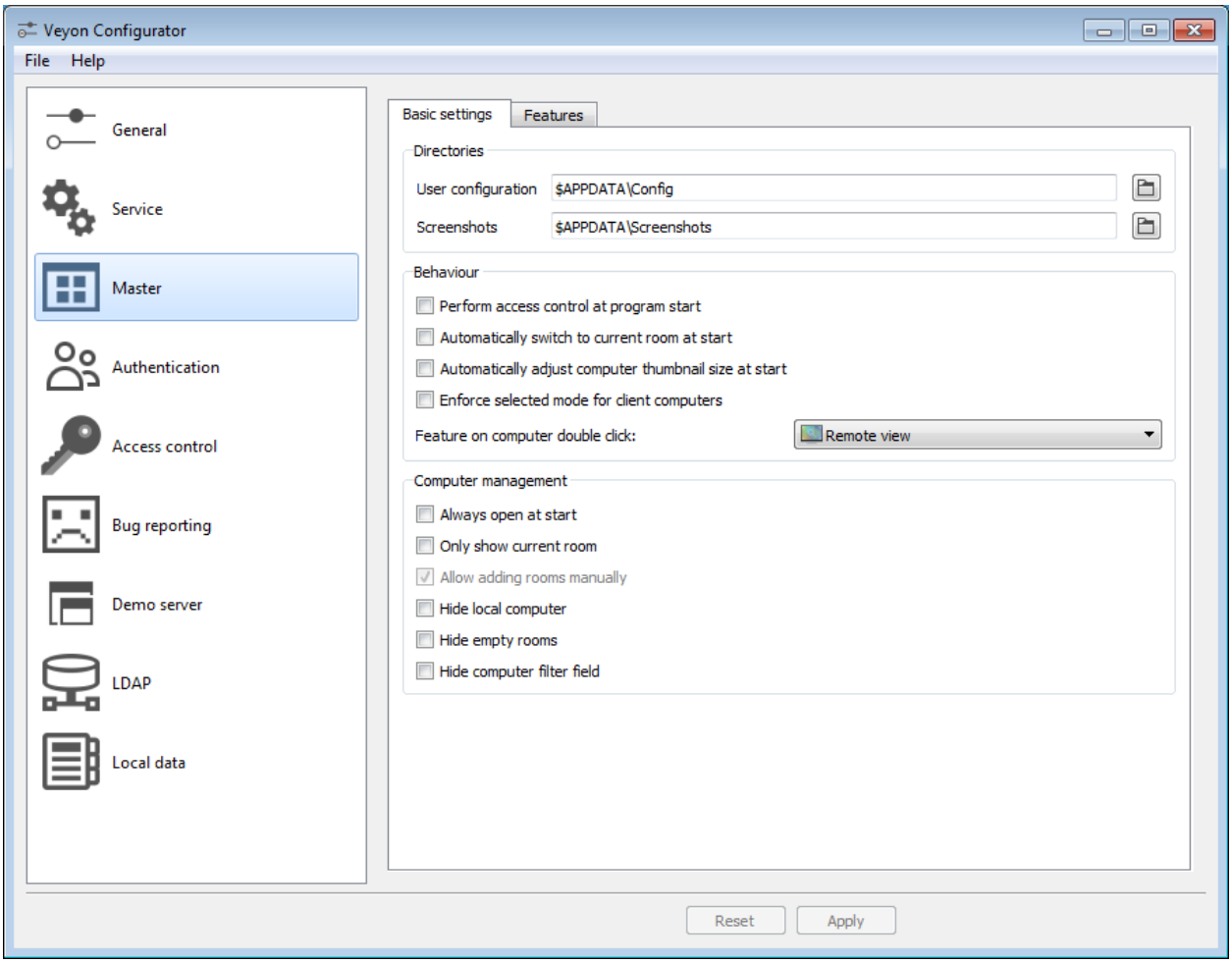
Delete all Veyon-related settings during uninstalling:

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

CHAPTER 3

Configuration

To start the setup, start the Veyon Configurator if that has not already been done automatically upon completing the installation. With this program it is possible to set up and customize a local Veyon installation. 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.



The *Configuration reference* describes all configuration pages and configuration options with their respective meanings.

3.1 Overview

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

The settings in 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 and apply system-wide for all users.

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

3.2 Authentication

In order to access a computer running the Veyon Service the accessing user has to authenticate himself at first, meaning that he has to prove his identity resp. usage authorization. Otherwise an unrestricted access from every user on every computer running the Veyon Service would be possible. Access without authentication is not possible. The configuration can be done in the configuration page *General* in section *Authentication* in Veyon Configurator.

3.2.1 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 corresponding private key are used. Thereby the private key is just accessible for specific users. In case of a connection request the Veyon Service sends a random char sequence to the Veyon Master and the Master signs this random data with his private key. The signature is sent back to the Veyon Service and checked with the corresponding public key. This check is only successful, if the signature has been generated with the matching private key. In this case the authenticity of the signing party is guaranteed. If the signature check fails, the connection is closed.

In case of the **logon authentication** the counterpart encrypts his user name and password for the Veyon Service. Using this logon data the Veyon Service attempts to connect to the local system. If the attempt fails, the conection is closed. Otherwise user name and password are correct, such that the authenticity of the counterpart is guaranteed.

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 centrally handled by access rights to the file containing the private key	• more effort during configuration • user identity can not be assured even after successful signature check • exchange of compromised key pairs must be done system-wide

Logon authentication

Advantages	Disadvantages
• easy and effortless setup • identity of counterpart can be assured, allowing for effective and secure access control	• login with username and password necessary whenever Veyon Master is used

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

3.2.2 Key management

In order to use the key file authentication, at first a key pair consisting of a public and a private key has to be generated. The configuration page *Authentication keys* is available for this purpose. A new key pair is generated via the *guilabel:'Create key pair* button. A short, concise term such as `teacher` should be chosen as the name. An access

group must then be set for both private and public keys. The private key access group may only include users who are to be allowed to access other computers via the Veyon Master. The public key should be assigned to a global access group so that the key is readable by all users and the operating system.

As soon as the keyfile-authentication is set up and working with one client computer, the keys can be deposited on a shared network drive and the *Key file directories* can be changed accordingly. Now the client computers just have to import the Veyon configuration, however, the files containing the keys don't have to be manually imported.

Attention: The private key file shall only be accessible for users that should have access to other computers. If the file is stored on a network drive, it must be thoroughly ensured that file access is restricted with an ACL or similar!

3.3 Access control

With the help of the Access control module it can be specified in detail which users may access a computer. Access control is performed during connection initialisation after the authentication. While authentication assures the authenticity of an accessing user, the access control functionality restricts computer access to authorised users, e.g. teachers.

Setup is done from the *Access control* configuration page and is described in detail in chapter *Access control rules*.

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

3.4 Rooms & computers

In the configuration page *Rooms & computers* you can create the rooms and computers that are displayed in Veyon Master 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 rooms. Using the two buttons below the list, rooms may be added or deleted. Existing rooms can be edited and renamed by double-clicking.

The list on the right contains a computers that are stored for the currently selected rooms. Using the two buttons below the list, computers may be added or deleted. The individual cells in the table can be edited by double-clicking. A name and a computer/IP-address has to be specified for each computer. In case the Veyon function Wake-on-LAN shall be used, the corresponding MAC address has also to be provided. Otherwise this column can be left blank.

3.5 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*.

3.6 Importing/exporting a configuration

An imported prerequisite for the use of Veyon is an identical configuration on all computers. A transfer of 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 menu *File*. This entry can be used to export the current configuration in JSON format to a file. 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 only applied and saved in the system only after pressing the *Apply* button.

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

Additionally, when performing an *automated installation* the configuration can be imported without any further interaction. In the example section you find an *Example* for the install parameter `/ApplyConfig`.

3.7 Reset configuration

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

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

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

CHAPTER 4

Access control rules

4.1 Introduction

Access control rules can be used to provide detailed control over which users can access certain computers under certain 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 rule 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.

4.2 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 dialogue is divided into three sections. The meanings of the individual options in the various dialog sections are explained below.

4.2.1 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 rule 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 rule 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 such 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.

4.2.2 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 in room With this condition you can define that either the accessing or the local computer has to be located in a specific room. The desired room can be chosen. If no or only wrong rooms are selectable, the *Network object directory* has to be adjusted.

Accessing computer is located in the same room as local computer With this condition you can determine that the accessing computer and the local computer have to be located in the same room. This can for example prevent a teacher from accessing computers in another 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 is located in the same room as the local computer* an extended ruleset can be created allowing access to other rooms 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 example, to assist with computer administration, it can be helpful to always be able to access a computer when no user is logged in.

4.2.3 Action

If all the enabled conditions of a rule apply, a specific action is performed concerning the access to the computer. 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 rule 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 rulelist below that would allow access, access is still denied.

Ask logged on user for permission This action displays a dialog on the computer in question where the logged on user can choose whether to allow or deny access. No further rules are processed, regardless of the user decision.

None (rule disabled) With this action the rule is ignored and processing is continued with the next rule. This option can be chosen to create an inactive dummy entry to visually subdivide the rule list.

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

4.3 Sorting rules

Important: In general access control rules are processed in the order they appear in the list. However, the action of the first matching rule will be taken even if subsequent matching rules exist and would lead to different actions.

All defined rules can be reordered using the buttons with the arrow symbols. Rules containing criteria meant for general granting or denial of access should be placed as high up as possble. Rules for coping with special cases may be listed further down the list. Rules defining some sort of fallback behavior should be at the bottom of the list.

4.4 Logical concatenation of rules

If multiple conditions are activated in a rule, *each* conditions must apply in order for the rule to be applied (logical AND). If only one of several rules must apply (logical OR), several access control rules have to be defined.

With a 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 has to be a member of two specific groups to grant access to a computer, two seperate rules may be generated that deny access, if the user is *not* a member of either group.

Note: If there is no matching access control rule such 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.

4.5 Testing a ruleset

In section *Computer access control* the configured rule set may be tested against 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 help of the parameters and a message with the test result is displayed.

CHAPTER 5

LDAP/AD integration

This chapter deals with connecting LDAP-compatible servers to Veyon. Below we will just use the generic term *LDAP* and thereby mean all LDAP-compatible products and technologies such as *OpenLDAP*, *Samba* or *Active Directory*. LDAP integration enables you to use most of the information about users, user groups, computers and rooms from existing environments, instead of manually reshaping them through the Veyon configuration. On the one hand LDAP users and user groups may serve as data base for *Computer access control* and on the other hand the Veyon Master can load rooms and computers to be displayed directly from the directory service.

The configuration of LDAP integration can be 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*.

5.1 Basic settings

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

5.1.1 General

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

Anonymous Bind / Bind credentials Depending on the environment and configuration of the LDAP server, LDAP queries can be performed either as an anonymous user or only with proper user name and password. If the server access requires a user name and password, the option *Bind credentials* has to be activated and the credentials have to be entered into the following input fields. Otherwise the default option *Anonymous Bind* can be used.

Bind DN The Bind DN is the user name needed for a login at the server in order to process LDAP operations. However, the required format vastly depends on the LDAP server and its configuration. Possible formats include `User`, `DOMAIN\User` or `cn=User,...,dc=example,dc=org`.

Bind Password In connection with the Bind DN the respective password has to be entered.

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

Hint: Veyon exclusively perform reading LDAP operations. For security reasons it may be a good option to create a read-only user, for example "Veyon-LDAP-RO". Access to relevant attributes can be further restricted for this user.

5.1.2 Connection security

Veyon can establish an encrypted connection with 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 certificate of the LDAP server is to be checked when the encrypted connection is established. The default setting *System defaults* attempts to verify the certificate against the root certificates installed system-wide, depending on the operating system. The Windows certificate store is not taken into account here, so that a separate CA certificate file may have to be stored. The *Never* setting does not verify the server certificate at all, but this allows 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*

User-defined 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.

5.1.3 Base DN

An essential foundation which holds all objects that are to be used, is defined through the Base DN. This foundation usually is taken from the DNS or AD domain (see also RFC 2247).

In case a fixed Base DN is used, the default option *Fixed Base DN* has to be activated and the Base DN has to be entered in the input field. You can use the *Test* button to verify, whether the settings are correct and new entries can be found.

If a generic Veyon configuration is to be used for example at several sites with different Base DNs, Veyon can be configured such that the Base DN is always dynamically queried using the LDAP naming contexts. Therefore the equally named option has to be activated and the naming context attribute must be changed. You can use the *Test* button to verify, whether a Base DN can be found.

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

5.2 Environment settings

After the basic settings have been configured and tested, the environment settings can be processed. These settings define which trees hold objects and how particular object attributes are named. Using these parameters, Veyon can query the information needed from the LDAP directory.

5.2.1 Object trees

Object Trees are organizational and structural units, in which specific types of objects (users, groups, computers) reside. The corresponding CNs (Common Names) or OUs (Organizational Units) must be entered in the respective input field, if *no Base DN* is used. Next to each input field there is a button to check the corresponding object tree.

User Tree Enter the LDAP tree (without Base DN) the users (user objects) reside in. Typical examples are `OU=Users` or `CN=Users`.

Group Tree Enter the LDAP tree (without Base DN) the groups (group objects) reside in. Typical examples are `OU=Groups` or `CN=Groups`.

Computer Tree Enter the LDAP tree (without Base DN) the computers (computer objects) reside in. Typical examples are `OU=Computers` or `CN=Computers`.

Computer Group Tree If the computer groups are located in different tree than the regular (user-)groups or in a subtree, the respective LDAP tree can be entered here. Otherwise the group tree is also used to query computer groups and filter them with a specific *object filter* if necessary.

Perform recursive search operations in object trees You can use this option to control whether objects shall be queried recursively. In this case the search is not only performed in the determined tree but also in all possible subtrees.

Default: *disabled*

Hint: If objects of a single type reside in various object trees (e.g. users in `CN=Teachers` and also in `CN=Students`), the parameter for the respective object tree can be left empty and the option *Perform recursive search operations in object trees* can be activated. In this case a recursive search through the complete LDAP directory starting from the Base DN is performed. However, you should by all means set the *object filter* for the respective object type.

5.2.2 Object attributes

In order for Veyon to retrieve the required information from the queried objects, the names of some object attributes have to be configured, as they may vary broadly depending on the specific environment and LDAP server. Next to each input field there is a button that can be used to check each attribute name.

User Login attribute This attribute must contain the login name of a user. It is used to determine the LDAP user object belonging to a specific user. In an OpenLDAP environment often the attribute name `uid` is used to this end, whereas Active Directory frequently uses `sAMAccountName`.

Group Member attribute Members of a group are listed in group objects through this attribute. It is used to determine the groups a particular user is a member of. Depending on the configuration they attribute also also used for mapping computers and rooms. In an OpenLDAP environment often the attribute name `member` is used to this end, whereas Active Directory frequently uses `memberUid`.

Computer Name attribute This attribute takes the DNS name of the computer. It is used to determine the LDAP computer object belonging to a specific computer name (host name). In an OpenLDAP environment often the attribute name `name` is used to this end, whereas Active Directory frequently uses `dNSHostName`.

Computer names are saves as fully qualified domain names. This option determines whether the fully qualified domain name (FQDN) is used for the mapping of computer names to LDAP computer objects. If the computer names are saved without the domain part in the LDAP directory, this option has to be disabled.

Default: *disabled*

Computer MAC address attribute Additionally to the computer name the MAC addresses of computers are stored in the LDAP directory in some environments, for example, if the DHCP server is also accessing the LDAP directory. If the Veyon function Wake-on-LAN shall be used, the respective attribute name has to be entered here, since the MAC address is required for this function. Typical examples are `hwAddress` or `dhcpAddress`.

Hint: A standard Active Directory does not have an attribute for storing MAC addresses. You'll need to populate MAC addresses manually in an existing unused attribute such as `wwwHomepage` or extend the AD scheme. Additionally you can grant computers group write access to `SELF` and let them store the MAC address of the first physical LAN adapter by using a PowerShell startup script.

Computer room attribute If the LDAP scheme for computer objects needs a special attribute for the mapping to a room, this attribute name can be entered here. You can use the *Test* button to verify, whether the members of a computer room can be correctly queried using the configured attribute. In the advanced settings, you can configure in section *Computer rooms* that the computer room attribute is used.

Computer room name attribute If computer groups or computer contains are used as rooms, instead of the *Common Names* of these groups or objects, the value of a specific attribute for the displayed room name can be used. For example, if computer groups have an attribute `name` or `description`, you can store a meaningful room declaration in this place.

5.3 Advanced settings

With the advanced settings the LDAP integration and usage of information from the LDAP directory can be tailored to fit individual needs.

5.3.1 Optional object filters

By using LDAP filters the LDAP objects used by Veyon can be limited, e.g., if computer objects such as printers should not be displayed in Veyon Master. Next to each input field there is a button to check the respective attribute name.

Since 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), e.g. `(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 rooms, you can limit the rooms to be displayed with this method.

Filter for computer container You can define an LDAP filter for computer groups here, e.g. `(objectClass=container)` or `(objectClass=organizationalUnit)`. If container/OUs are used as rooms, you can limit the rooms to be displayed with this method.

5.3.2 Identification of group members

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

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

5.3.3 Computer rooms

Veyon provides several methods to map computer rooms to an LDAP directory. In the most simple case there is one computer group for every computer room which all computers of a room are a member of. If computers reside in containers or Organizational Units (OUs), these superior objects can be used as rooms. In both cases do not entail an update of the LDAP scheme. As a third possibility the room name can be stored as special attribute in each computer object.

Computer groups You can use this option to define, that computer rooms are mapping using computer groups. All computer groups will be displayed as rooms in Veyon Master. In each room all computers that are members of the specific group are displayed. In case not all LDAP groups shall be displayed as rooms, you must either configure a dedicated computer group tree or restrict the computer groups by using a computer group filter.

Default: *activated*

Computer container or OUs This settings defines that the containers/OUs in which the computer objects reside are used as computer rooms. Containers are objects that are superior to computer objects in the LDAP tree. In case not all containers shall be displayed as rooms, a respective computer container filter can be defined.

Default: *disabled*

Common attribute If the LDAP scheme expects a special attribute for the mapping of computer objects to a room, this option can be activated and the attribute name can be entered. You can use the *Test* button to check, whether the members of a computer room can be queried correctly with the configured attribute.

Default: *disabled*

5.4 Integration tests

By using integration tests the LDAP integration as a whole can be tested. The buttons allow for various tests to be performed. All tests should be run successfully and return valid results before the LDAP connection is used in production.

5.5 Using LDAP backends

After successful configuration of the LDAP integration, the LDAP backend can be activated. Both *Network object directory* as well as the user groups backend for the *Computer access control* have to changed. Only after the network object directory has been changed to *LDAP* the room and computer information from the LDAP directory are used in Veyon Master.

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

5.6 Command line interface

There are several LDAP specific opertions provided through the *Command line interface* of Veyon. All operations are provided through the `ldap` module. All list of all supported commands is printed on entering `veyon-ctl ldap help`, whilst command specific help texts can be shown via `veyon-ctl 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-ctl ldap autoconfigurebasedn ldap://192.168.1.2/ namingContexts
```

```
veyon-ctl ldap autoconfigurebasedn ldap://Administrator:MYPASSWORD@192.
168.1.2:389/
```

`query` This command allows querying LDAP objects (`rooms`, `computers`, `groups`, `users`) and is designed mainly for debugging purposes. However, the function can also be used for developing scripts that may be helpful for system integration.

```
veyon-ctl ldap query users
```

```
veyon-ctl ldap query computers
```

CHAPTER 6

Command line interface

For administrative tasks, the *Veyon Configurator* and the command line tool *Veyon Control* are available. The program can be started via the command `veyon-ctl` in the command line. If the Veyon installation directory is not in the `$PATH` (Linux) or `%PATH%` (Windows) environment variable, 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-ctl 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
    remoteaccess - Remote view or control a computer
    service - Commands for configuring and controlling Veyon Service
    shell - Commands for shell functionalities
```

Each 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-ctl 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 each command:

```
$ veyon-ctl remoteaccess help control

remoteaccess control <host>
```

6.1 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 easily automated.

`create <NAME>` This command creates a new pair of authentication keys and stores the private and public keys in the configured key directory. The parameter must be a name for the key, which may only contain letters.

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

`export <KEY> [<FILE>]` This command exports the `<KEY>` to `<FILE>` authentication key. If `<FILE>` is not specified, the file name is derived from the 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. The public key can then be extracted.

`import <KEY> [<FILE>]` This command imports the authentication key `<KEY>` from `<FILE>`. If `<FILE>` is not specified, the file name is derived from the 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 is output instead. Some details may be missing if a key cannot be accessed, e.g. due to missing read permissions.

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

6.2 Configuration management

The local Veyon configuration can be managed using the `config` module. Both the complete configuration and individual *:index:'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 before importing another configuration:

```
veyon-ctl config clear
```

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

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

`list` This command shows a list of all configuration keys and their corresponding values.

```
veyon-ctl config list
```

Using this command you can find the names of configuration keys in order to `get` oder `set` them one by one.

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

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

set With this command a single configuration key can be written. The name of the key and the desired value must be passed as additional arguments:

```
veyon-ctl config set Network/PrimaryServicePort 12345
```

```
veyon-ctl config set Service/Autostart true
```

```
veyon-ctl config set UI/Language de_DE
```

unset This command deletes a single configuration key resulting in Veyon using the internal *index:'default value* for this key. The name of the key must be passed as an additional argument:

```
veyon-ctl 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.

6.3 LDAP

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

6.4 Network object directory

As described in the section *ref:'Rooms and 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 `room` or `computer`. `<PARENT>` can be specified as name or UUID.

clear This command resets the entire network object directory, i.e. all rooms 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> [room <ROOM>] [format <FORMAT-STRING-WITH-VARIABLES>] This command can be used to export either the complete network object dictionary or only the specified room to a text file. The formatting can be controlled via a format string and the variables it contains, so that, for example, a CSV file can be generated. Valid variables are `%type%`, `%name%`, `%host%`, `%mac%` and `%room%`.

import ``FILE> [room < SPACE>] [format `FORMATSTRING-MIT-VARIABLEN>] [regex `REGULAR EXPRES 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 and contained variables. This way both CSV files and otherwise structured data can be imported. Valid variables are `%name%`, `%host%`, `%mac%` and `%room%`. Various examples are given in the command help.

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

remove <OBJECT> This command removes the specified object from the directory. <OBJECT> can be specified as name or UUID. When a room is removed, all computers in it are also removed.

6.5 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. For example, the function provided by the command line tool can be used to create a program shortcut for direct access to a particular 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-ctl 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-ctl remoteaccess view pc5:5900
```

6.6 Service control

The local Veyon service can be controlled using the service module.

register This command registers the Veyon service in the operating system as a service so that it starts automatically when the computer starts up.

```
veyon-ctl service register
```

unregister This command removes the service registration in the operating system so that the Veyon service will not start automatically on startup.

```
veyon-ctl service unregister
```

start This command starts the Veyon service.

```
veyon-ctl service start
```

stop This command stops the Veyon service.

```
veyon-ctl service stop
```

restart This command restarts the Veyon service.

```
veyon-ctl service restart
```

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

```
veyon-ctl service status
```

6.7 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-ctl program for each command. The mode can be exited by entering the keyword exit.

Additionally 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.

CHAPTER 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*.

7.1 General

7.1.1 User interface

Language

The selected language can be adapted for the graphical user interfaces as well as the command line tools. You can choose from all the languages that are already provided in a partly or complete translation. Please note, that changing the language will take effect after a program restart. In default configuration Veyon uses the language of the operating system, if this language is already supported. Otherwise, English will be used as a fallback.

Default: *use system language settings*

7.1.2 Logging

You have several options at hand to influce the logging within Veyon. These options are primarily of interest if you are experiencing problems using Veyon. The log files may indicate potential causes for errors.

Logfile directory You can use this option to specify in which directory the log files will reside. Normally you should use a placeholder variable in this place. A more detailed description about possible values can be found in section *Placeholder variables for file paths*.

Default: *$TEMP*

Loglevel

The loglevel defines how detailed logging messages are recorded. For analysis of program failures it may be useful to even set the loglevel to *Debugmessages and everything else*. Thus, however, huge amounts of log data can be produced fast. In normal operating mode only warnings and errors should be recorded.

Vorgabe: *Information, warnings and errors*

Limit logfile size

In order for logfiles not to become too large and occupy memory unnecessarily, their size can be limited with this option. If activated, an upper limit for the size of a single logfile can be configured.

Default: *disabled / 1 MB*

Rotate logfiles

In conjunction with limiting the size of a single logfile, it may be useful furthermore to rotate the logfiles. In this case one logfile is renamed to `Veyon...log.0` after exceeding the configured limit. Previously rotated files are renamed such that the number of the file suffix is increased by 1. If the maximum number of rotations is reached, the oldest file (i.e. the one with the highest number as a suffix) is deleted.

Vorgabe: *disabled / 10x*

Log to stderr If program components of Veyon are executed from a command line window (i.e. a terminal), you can use this option to specify, whether logging messages shall be printed to `stderr` or `stdout`. This option is primarily relevant for scripting operations.

Default: *activated*

Log to Windows-Event Log For in central management in may be useful in some cases to log logging messages directly to the Windows-Event Log. This option does not influence the normal recording of logfiles. Under Linux this option has no effect.

Default: *disabled*

You can use the *Clear all Logfiles* button to delete all Veyon logfiles in the logfile directory of the current user as well as the ones of the system service.

7.1.3 Network object directory

In Veyon a NetworkObjectDirectory provides information about network objects. Network objects include computers and rooms that computer are based in. The data from the network object directory is used by Veyon Master to supply the computer room management with entries. On top of that data from the network object directory is used for access control. By default a backend is used, that stores the data in the local Veyon configuration and queries them from this location. See section *Rooms & computers* for more information.

Backend You can use this option to define 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: *Standard (store objects in local configuration)*

Update interval The network object directory can be automatically updated in the background which may come in handy if dynamic backends such as LDAP are used. The time interval for these updates can be altered with this option.

Default: *60 seconds*

7.1.4 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*

7.2 Service

7.2.1 General

Hide info area icon By default the Veyon service displays an info area icon (see also *system section of the control panel*) to indicate proper operation and information concering program version and used network ports. Displaying the icon can be prohibited by activating this option.

Default: *disabled*

index:*Show notification* on failed authentication attempts This option specifies whether a notification should be displayed if there was a failed logon attempt via the Veyon service. These messages usually indicate that the authentication settings are not set up correctly, for example, incorrect authentication keys or dissimilar users/passwords on computers when using logon authentication.

Default: *activated*

Show notification on remote connection If the user is to be informed that his computer is being remotely accessed, he can be notified. This option must be activated for this. However, if the user is to be asked for permission, appropriate access control rules must be configured. More information can be found in the chapter *Access control rules*.

Default: *deactivated*

Activate SAS generation in the software (Ctrl+Alt+Del) In standard configuration it is not possible for applications running under Windows to generate the Secure-Attention-Sequence (Ctrl+Alt+Del) and simulate pressing these keys. With this option a policy is written to the Windows-Registry that alters this behavior. It is recommended to leave this option activated in order to be able to send `Ctrl+Alt+Del` to a remotely controlled computer. Otherwise it may for example not possible to unlock the remotely controlled computer. A user login can also be prohibited since the keys `Ctrl+Alt+Del` usually have to be pressed to this end.

Default: *activated*

Autostart With this option you can specify whether the Veyon service is registered as a system service in the operating system meaning that is automatically started on booting the computer.

Default: *activated*

7.2.2 Network

Primary service port You can use this option to define the primary network port the Veyon service is working with, meaning that it listens to incoming connections and accepts them.

Default: *11100*

Port of the interval VNC server You can use this option to define the network port the interval VNC server is working with. This port is not reachable from the outside and is used exclusively by the Veyon service to access screen data via an internal VNC server and forward them.

Default: *11200*

Port for function manager You can use this option to define the network port the function manager is working with. This internal components of the Veyon service is an interface between the Veyon service and function processes. In contrast to the Veyon service these function processes are running in the context of the signed in user and therefore have to communicate with the Veyon service through this interface. This port is not reachable from the outside.

Default: *11300*

Port for demo server You can use this option to define the network port the demo server is working with. The demo server provides screen data from a teacher computer to the network during a demonstration.

Default: *11400*

Activate firewall exception Depending on the system configuration can may be impossible for a process running under Windows to listen to a specific port since the Windows-Firewall may be blocking connection requests. In order to provide access to the service port and the demo server port, exceptions for the Windows-Firewall have to be configured. This is automatically done during the installation process. If this behavior is unwanted and a manual configuration is preferred, this option can be disabled.

Default: *activated*

Only allow connections from the local computer If the Veyon service shall not be reachable for other computers in the network, you can use this option. For normal computers which shall be access from the Veyon Master, this option must not be activated. However, the option could be useful for teacher computers in order to provide an additional security layer beside the access control settings. Access to the demo server is not influenced by this option.

Default: *disabled*

7.2.3 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 utilize a plugin with a different implementation. For example if a separate VNC server is already installed on the computer, this server 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 entered.

Default: *Built-in VNC server*

7.3 Master

7.3.1 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. A more detailed explanation of possible values can be found in section *Placeholder variables for file paths*.

User configuration The user specific configuration of the Master program resides in the directory defined here. This configuration includes the settings for the user interface and the computer choice from the last session.

Default: *$APPDATA/Config*

Screenshots All image files that have been generated by the screenshot function reside in the directory defined here. For example if you want to store the files in a central collection folder, a different directory path can be entered here.

Default: *$APPDATA/Screenshots*

User interface

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

Default:* *1000 ms*

Background color With this setting the background color of the workspace in Veyon Master can be changed.

Default: *white*

Computer thumbnail caption With this setting you can choose which caption to use for the computer thumbnails in Veyon Master. For example, if the computer name is not important, only the name of the logged on user can be displayed instead.

Default: *User and computer name*

7.3.2 Behaviour

In the tab *Behaviour* settings are available to change the behaviour of Veyon Master with respect to *program start*, *computer rooms* and *modes and functions*.

Program start

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

Default: *disabled*

Automatically switch to current room By default all computers that have been selected the previous time are displayed after starting Veyon Master. If instead all computers in the Master computer's room shall be displayed, this option can be activated. The Veyon Master will then try to solve which room the local computer belongs to using the configured *Network object directory*. All computers in the room are listed in this case. Precondition for this function is a correctly working DNS setup in the network which translated computer names to IP addresses and vice versa.

Default: *disabled*

Automatically adjust computer thumbnail at start If the size of the computers' thumbnail is to be automatically adjusted upon starting Veyon Master (takes the same effect as clicking the *Auto* button), this option can be activated. The previously configured size will be ignored. This functionality primarily comes into play in conjunction with the *automatic room change*.

Default: *disabled*

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

Default: *disabled*

Computer rooms

Only show current room As a default, the computer management lists all rooms in the configured *Network object directory*. By activating this option you can assure that only the room the Master computer is based in is listed. This can increase lucidity especially in larger environments.

Default: *disabled*

Allow adding rooms manually

In conjunction with the option *only show current room* is can be additionally specified, that further rooms can be added to the computer management manually. If this option is activated, an additional *Add Room* button is shown that opens a dialogue with all available rooms.

Default: *disabled*

Hide local computer In normal operation mode it is often not desired to display one's own computer and activated room-wide activated function on one's own computer as well (e.g. screen lock). Hiding a local computer can be activated through this option.

Default: *disabled*

Hide empty rooms Under certain circumstanced the *Network object directory* contains rooms without computers, for example due to specific LDAP filters. These empty rooms can be hid away from the computer management through this option.

Default: *disabled*

Hide computer filter field The filter field for searching computers can be hid through this option, 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 functions change the operating mode of a computer. Examples are the demo mode or the screen lock. These mode function are activated only once per default and, for example, are not restored in case of a physical computer reboot. If this option is activated, the mode will even be enforced after a connection has been closed.

Default: *disabled*

Show confirm dialogue for potentially dangerous actions Actions such as rebooting a computer or logging off of a user are potentially hazardous such that an unintentional activation is not desired. You can use this option to define that such actions have to be confirmed in a confirm dialogue.

Default: *disabled*

Function on double-click If a computer is double-clicked in Veyon Master, a predefined function can be triggered. The usage of the functions *remote control* or *remote view* is conventional.

Default: *<no function>*

7.3.3 Features

With the help of the two lists in the *Features* tab is can be defined which functions are available in Veyon Master. Single features can therefore be deactivated if necessary, such that respective buttons and context menu entries are not displayed in Veyon Master. This may increase lucidity of the user interface if certain features are not to be used anyway.

A feature can be moved from one list to the other by marking and confirming the respective button with the arrow keys. A double-click has the same effect on a feature.

7.4 Authentication keys

7.4.1 Key file directories

Placeholder variables should be used for both base directories. A detailed description of possible values can be found in the *Configuration reference* in section *Placeholder variables for file paths*. Under Windows *UNC paths <https://de.wikipedia.org/wiki/Uniform_Naming_Convention>* _ can be used instead of absolute paths.

Base directory of the public key file The keyfile-assistant places the role specific public key files in this directory after the keys have been generated or imported. On top of that the Veyon Service loads the respective public key file for authentication purposes from this directory.

Default: *$GLOBALAPPDATA/keys/public*

Base directory of the private key file The keyfile-assistant places the role specific private key files in this directory after the keys have been generated. On top of that the Veyon Master loads the respective private key file to authenticate itself to clients from this directory.

Default: *$GLOBALAPPDATA/keys/private*

7.5 Access control

7.5.1 Computer access control

Data backend A data backend is required as a data base for access control. It provides users and groups as well as computers and rooms. Thereby you can choose between the standard backend and other plugin-specific backends such as LDAP. With a standard backend local users and groups as well as computers and rooms are loaded from the local configuration; see also section *Rooms & computers*. If an LDAP connection is used, you should select the backend *LDAP* here.

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

Default: *disabled*

Grant access to all authenticated users (default) If the predefined authentication is sufficient (e.g. when using a keyfile authentication with restricted access to the key files), this option can be selected. 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 for a detailed access control using user defined access control rules and offers maximum flexibility. However, its initial configuration is slightly more complicated such that one of the other two access control modes is recommended for initial testing.

7.5.2 User groups authorized for computer access

Configuration of this access control mode is straightforward. The left list contains all user groups provided by the data backend. By default these are all local user groups. If *LDAP/AD Integration* is configured, all LDAP user groups are shown. 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. Remember to mirror the configuration to all computers.

Using the *Test* button in section *Computer Access Control* it can be checked, whether are specific user could potentially access a computer through the current group configuration.

7.5.3 Access control rules

Configuration of a rule set for access control including use cases are described in detail in chapter *Access control rules*.

7.6 LDAP

All options that describe how to connect Veyon to an LDAP compatible server are explained in detail in chapter *LDAP/AD integration*.

7.7 Demo Server

Fine tuning can be done through the configuration page for the demo server to enhance performance in demo mode. These configurations should only be altered if performance is not satisfying or if only a small bandwith is available for transferring data.

Update interval

> You can use this option to specify the interval between to screen updates. The smaller this interval is, the higher the update frequency and the smoother the screen transmission. However, a considerably low value might lead to higher CPU load and more network traffic.

Default: *100 ms*

Key frame interval During transmission of screen data only the parts of the screens that have actually changed are sent to the clients (incremental update) in order to minimize network load. These updates are carried out individually and asynchronously for each client. Thus, clients may not be running synchronously after a while depending on bandwidth and latency. To this end complete *key frames* are sent in equidistant intervals, such that after one key frame intervall all client will have a synchronized screen. The lower the value chosen, the higher the resulting CPU and network load will be.

Default: *10 sec*

Memory limit All screen update data is internally buffered by the demo server to be distributed to the clients later on. In order not to use too much memory space for the internal buffer due to incremental updates between two key frames, the value defined here serves as a limit. This limit is a soft-limit meaning that on exceeding it a key frame updated is tried (even if the key frame interval has not passed entirely), but the buffer still holds all data. Only if the specified limit is exceeded twofold (hard-limit) the buffer is reset. If there are frequent disruptions or lagging during a screen transmission, this value should be increased.

Default: 128 MB*

7.8 Placeholder variables for file paths

Placeholder variables can be used with each operating system in both the Windows and Linux format `$VARIABLE` and `%VARIABLE%`.

Variable	Expanded path
APPDATA	User specific directory for application data from Veyon, e.g. `...\User\AppData\Veyon` under Windows or `~/.veyon` under Linux
HOME, PROFILE	Home directory of the signed in user, e.g. `C:\Users\Admin` under Windows or `/home/admin` under Linux
GLOBALAPPDATA	System-wide directory for application data from Veyon, e.g. `C:\ProgramData\Admin` under Windows or `/home/admin` under Linux
TMP, TEMP	User specific directory for temporary files, under Windows `C:\Windows\Temp` is used for the Veyon Service and `/tmp` under Linux

7.9 Environment variables

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

Variable	Description
`VEYON_AUTHKEY_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`.

CHAPTER 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. During debugging the configuration needs to be transfered onto all computers on every change.

8.1 Computers can't be accessed

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

8.1.1 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.

8.1.2 Problems with the Veyon Service

If the computer can be pinged you should check whether 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 a reinstallation of Veyon. If a reinstallation 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 possibilities for adjustments in the service management of your operating system.

8.1.3 Service and firewall settings

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

```
telnet localhost 11100
```

Besides general program output the string `RFB 003.008` has to be displayed. If the output does not match the expectations you should check the *Network*, especially the primary service port, and 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* is disabled. Additionally *Computer access control* should be disabled initially, as the service listens on `localhost` only 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 external port access 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 software used. On Windows the integrated Windows Firewall is configured by Veyon automatically as long as the option *Enable firewall exception* in the *Network* is set to its default value (*enabled*). If a 3rd party firewall solution is used it has to be configured such that the TCP ports 11100 (primary service port) as well as 11400 (demo server) can be accessed externally.

8.1.4 Authentication settings

Another cause of error can be wrong or insufficient *Authentication*. For initial tests you should (on both computers!) enable *logon authentication* and disable *Key file authentication*. As soon as the logon authentication is successful at the local computer external access should work too.

When using *key file authentication* it has to be enabled and the key files on master and client computers have to correspond. On client computers the public key file needs to have the same content as on the master computer. If the access still fails in some circumstances the access permissions are 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 remains the *Key file directories* of the key files should be deleted on all computers and a new keypair generated on the master computer. Then the public key needs to be imported again on all client computers.

8.1.5 Settings for computer access control

An erroneous configuration of computer access control can lead to problems with accessing computers. Initially it's recommended to disable the *Computer access control* completely using the Veyon Configurator. Now you can determine which configured computer access control method is configured improperly.

When using *User groups authorized for computer access* you have to check whether the list of authorized user groups is complete and whether the accessing user is member of one of these groups.

Improperly configured *Access control rules* can also cause problems with accessing computers. There always has to be at least one rule which allows the access under certain conditions. Once ensured for further debugging a temporary test rule can be inserted at the end of the list which has the option *Always process rule and ignore conditions* enabled and the action *Allow access* selected. This rule stepwise can be moved upwards inside the rule list until the access

works or the test gives the desired positive results. The access rule below the temporary test rule likely causes the access being denied and can be examined in detail and corrected appropriately.

Another potential cause in case of prohibited computer access may be the *Access control rules*. There always has to be at least one rule granting access under certain conditions. Using this method, you can add another rule at the bottom of the list for debugging purposes. This rule should have the option *Always process rule and ignore conditions* activated and the action *Allow Access* should be selected. This rule can now be moved upwards step by step until access is granted or the test produces the desired results. In this case the access rule directly below the test rule has to be the cause for the denial of access and can be closely inspected and corrected accordingly.

8.2 Settings are not correctly saved/loaded

If one or more configuration keys are inconsistent or broken settings can't be loaded or save correctly, e.g. room and computer information. In this case the configuration (*should be reset completely*) and recreated from scratch using the default values.

8.3 Rooms and computers from the LDAP directory are not displayed in Master

Please make sure that:

- the *Network object directory* on configuration page *General* is set to *LDAP*
- LDAP integration tests *List all members of a computer room* and *List all computer rooms* are successful and return objects
- all options for fine tuning the behavior on configuration page *Master* are set to their default values

8.4 Automated switching to the current room doesn't work

If the *option for automated switching to the current room* is activated, but doesn't show any effect when starting Veyon Master, it should be ensured, that the master computer is set as computer for the respective room in the *Network object directory*. Independent from this option, the master computer can be hid in the computer room management using the option *Hide local computer in computer room management*.

If all entries in the network object directory are correct, there arguably is a problem with the DNS-configuration in the network. Make sure that computer names can be converted into IP-addresses and vice versa. Most common operating systems offer the diagnosis tool `nslookup` for this purpose. Calling the program with the local computer name as a parameter should return a valid IP-address. A second call with the returned IP-address should in turn return the computer name.

In case the function doesn't work as desired despite a correct DNS setup, it can be useful to set the *Loglevel* to the highest value (*Debug*) and search the log file `VeyonMaster.log` in the *Logfile Directory* for potential causes. Thereby the messages *"initializing rooms"* and *"found local rooms"* might be particularly helpful to detect possible problems.

8.5 Screen lock can be bypassed with Ctrl+Alt+Del

In order to completely block all keyboard input and shortcuts in screen lock mode, under Windows a reboot is required after completion of the Veyon installation. Without a reboot the Veyon-specific driver for input devices is not yet active

and keyboard input cannot be caught.

8.6 When in demo mode, client computer screens just show a black screen or a black window

Please make sure that:

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

8.7 The 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. In case 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 likely decrease overall performance.

CHAPTER 9

FAQ - Frequently Asked Questions

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

Currently Veyon is only available for Linux- or Windows-based environments. Support for other platforms is in progress. The Veyon project depends on the help of experienced software developers, especially for porting to macOS and Android.

9.2 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 rooms and computers on the *Rooms & computers* configuration page. Afterwards the added resources are available in the Veyon master.

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

9.3 How can I migrate an existing iTALC installation to Veyon?

Although iTALC and Veyon are conceptually similar, a complete reinstall and reconfiguration is necessary to use Veyon, because configuration and file formats as well as their paths have changed and are not compatible with each other. For a migration iTALC has to be uninstalled completely at first. It is recommended to reboot the computer thereafter. Afterwards Veyon can be installed and configured analogously to iTALC.

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

9.4 Is it possible to use Veyon Master on multiple computers?

The usage of Veyon Master on multiple computers is possible without any problems. 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 authentication is used the same private key has to be distributed to all master computers.

9.5 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 being provided by the system (e. g. VNC-based access to virtual desktops in VDI environments). This can lead to performance losses or conflicts with the Veyon-internal VNC server in some circumstances. In such cases it's recommended to configure Veyon to use the existing (external) VNC server instead of starting its internal VNC server. The configuration is done through the Veyon Configurator in the configuration page *Service* in section *VNC server*.

9.6 Can I import or use a self-generated file with room and computer information?

Since Veyon 4.1 there is a new *ref:'module for the command line interface <CLINetworkObjectDirectory>*. This module can be used to import rooms and computers from text files like CSV files into the network object directory.

9.7 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 dual monitor support*.

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

The selection of displayed computers is saved in the personal *user configuration*. To extend this more multiple user, there a two options. First, the user configuration file can be copied into the respective profile of the user, using login scripts for example. Second the user configuration can be moved to a shared directory (e.g. a network drive) and the *setting* has to be changed accordingly, such that the user configuration is loaded from this directory. However, you have to ensure that the access rights may have to be changed, for that changes made by the user are not rewritten into the global user configuration.

In this context we point you to the function for *Automatic switch to current classroom*, that may permit to realize the desired behavior directly.

9.9 How can I hide the master computer from computer rooms?

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

9.10 What happens if there is no matching access control rule?

If there is no previously defined access control rule that matches all activated conditions, access is denied and the connection is closed. In doing so we prohibit that an attacker may have access because of an unfinished rule set.

- genindex

Index

I

K

L

M

N

O

P

Q

R

S

T

U

V

W