Veyon Administrator Manual

Release 4.0.7

Tobias Junghans

Apr 24, 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 adept users. For end users there is a separate user manual 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 paramount for putting Veyon into operation.

Chapter *Installation* deals with the installation von Veyon on a Windows or Linux computer. It also contains hints on how to perform or implement an automated installation.

Chapter *Configuration* describes configuration and integration using the graphical configuration tool, whereas the *Configuration Reference* deals with the details of configuration options. Chapter *LDAP/AD Integration* explains in detail how to connect to an existing LDAP-/ActiveDirectory server.

Veyon is furthermore equipped with a command line interface (CLI) that can be used for editing the configuration 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.

If you are experiencing problems using Veyon, please see chapter *Troubleshooting* for help. Here you can find measures for problem analysis and remedy. Frequently asked questions are answered in chapter *FAQ - Frequently Asked Questions*.

1.2 About Veyon

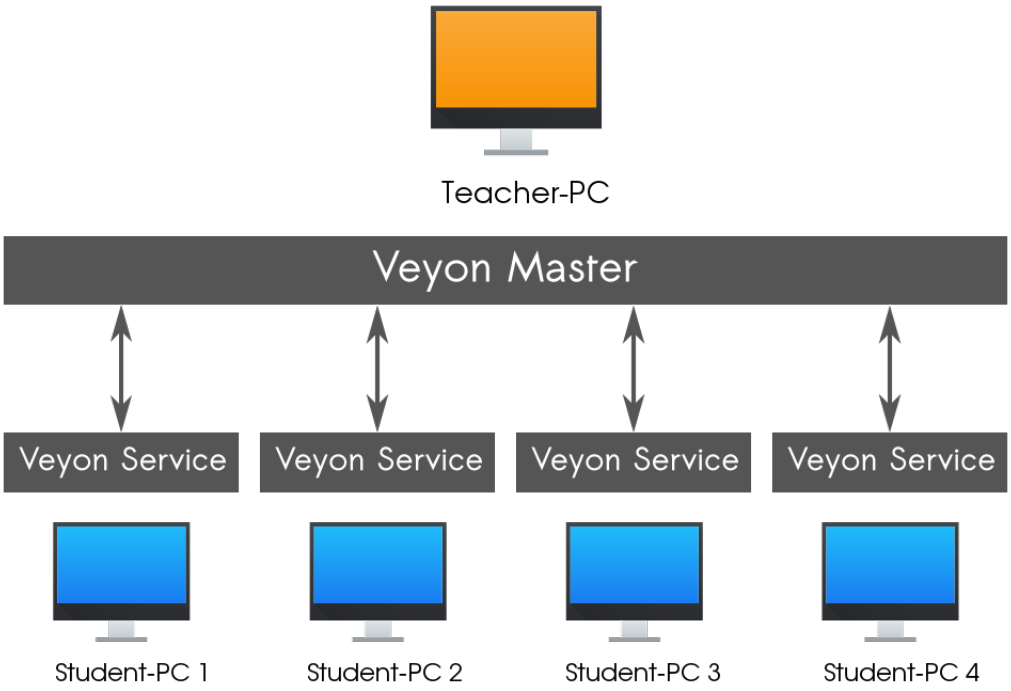
Veyon is a open source software for computer monitoring and class room administration. It permits observation and control of computer rooms as well as interaction with the user. The core functions of Veyon are the following:

- Overview of a (class) room with all screen contents in a tile view
- Remote control of computers
- Mirroring of the teacher's sceen to all other computers in real time (full screen/window)

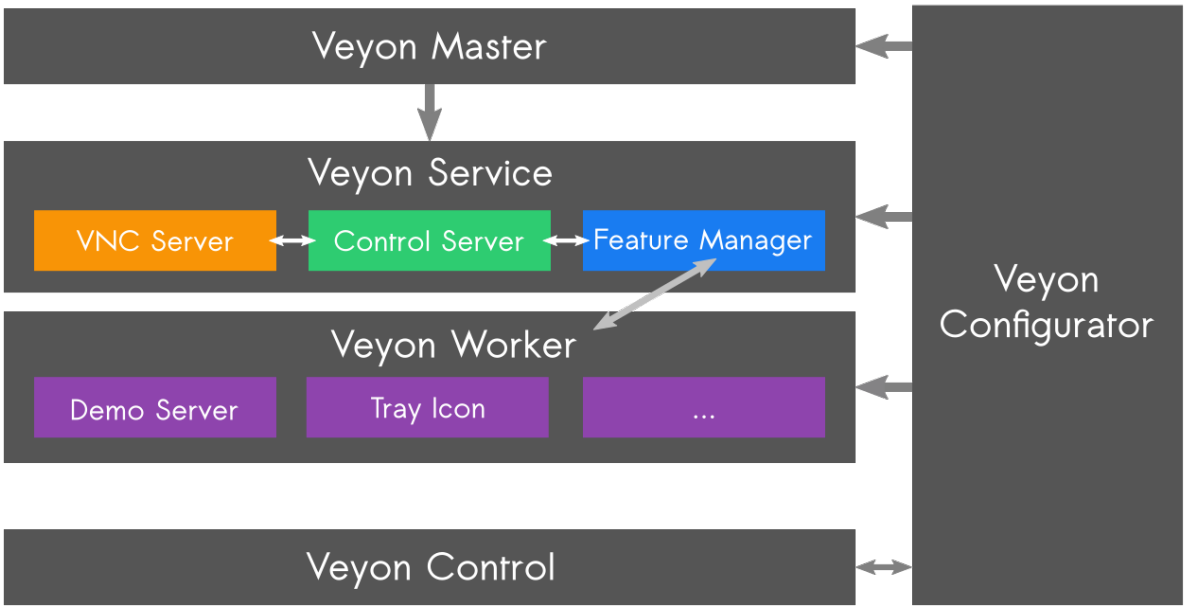
- Blocking workplaces (computers) to enhance attention
- Sending text messages to students
- Remote (re-)booting or shutdown of computers
- Logging out users
- Executing programs or opening websites

1.3 Components

In essence Veyon consists of of a master and a service component that realize interaction between teacher computers and student computers (often dubbed *master computer* and *client computer*):



In a more detailed view there are several program components that interact with each other in various ways:



Veyon Master An application program that can either be used for observing and controlling other computers or for utilizing functions within Veyon. In a regular case, this program is started by an enduser and accesses other computers through the Veyon service.

Veyon Service A service that provides access to a computer, controlling functions and application functions. In a regular case the program is started by the operating system as a service with elevated privileges and can not be terminated by the user. The service is required to run on all computers including teacher computers.

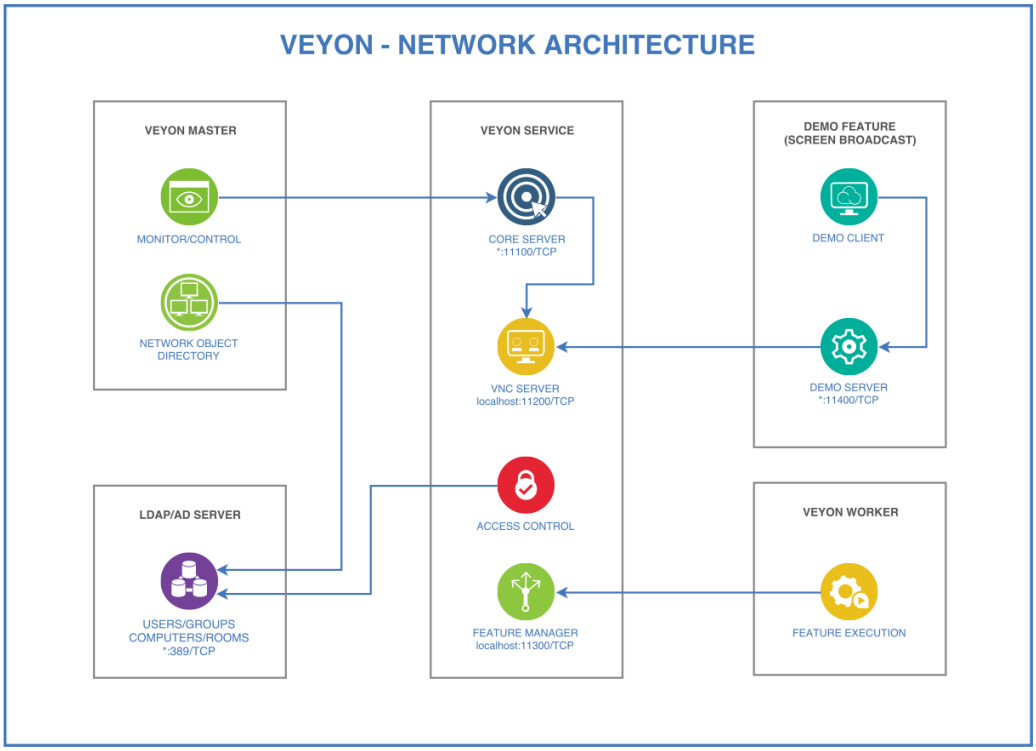
Veyon Worker A helper program started by the service to provide an environment for specific functions in an insulated way or in the context of the user that is currently logged in. Those specific functions include the demo server for the teacher computer and the demo client on the student computers.

Veyon Configurator A configuration tool that allows configuration and customization of all components in a local Veyon installation through a graphical user interface. If needed, the program is started by the administrator with elevated privileges.

Veyon Control A command line tool serving as an addition to the Veyon configurator that allows reconfiguration and the use of some Veyon functions without graphical interaction. This program is run either interactively on the command line or script controlled with (usually) administrator's 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 System Requirements

Veyon is designed for operating on standard computers running Windows or Linux. There are no special minimum requirements for the hardware. However, an up-to-date operating system supported by the manufacturer or the community must be run. Those include:

- Windows 7, 8 or 10 (32/64 Bit)
- **Linux with Qt 5.6 or newer**
  - Debian 9
  - Ubuntu 16.04
  - openSUSE 42.2
  - Fedora 24

Parallel usage of Windows and Linux computers is easily possible. All computers must be connected to each other through a TCP-/IP-compatible network, however, transmission technology (wired vs. wireless) is only of importance concerning the maximum performance. A gigabit network is strongly recommended for environments that run Veyon on more than 10 computers, since the demo mode (see user manual) may otherwise not be performant enough. The same holds true for wireless networks (WLAN) where at least standard IEEE 802.11n should be used.

2.2 Preparing the Installation

At first download the installation files for your platform from the Veyon download page[1]. For Windows computers we recommend using the 64-bit-option (*win64*). For 32-bit-installations, the 32-bit-option (*win32*) has to be used.

[1] https://github.com/veyon/veyon/releases/

2.3 Installation on a Windows-Computer

Execute the installation file with administrator privileges and follow the instructions. For computers that do not need a master application (e.g. student computers) you may uncheck the component *Veyon Master* in the *Choose Components* dialogue.

After successful completion of the installation by default the *Veyon Configurator*, a tool for configuring and customizing your installation, is started. Its usage is explained in detail in the (upcoming) chapter *Configuration*.

2.4 Installation on a Linux-Computer

The installation procedure for Veyon under Linux vastly depends on the distribution used. Usually you can download the program through your software management, if Veyon is available for the packet archive of your distribution. However, there is always the possibility of compiling a current version of Veyon from the sources and install it thereafter. For further information please visit the project's page on github [#github].

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 installation is done automatically. This is especially helpful for automated deployment in larger environments. Veyon is therefore easily integrated with all common software 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 holds true for the unstalling program.

2.5.2 Examples

Installation of Veyon in *silent* mode:

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

Uninstalling of 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 applying Master application:

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

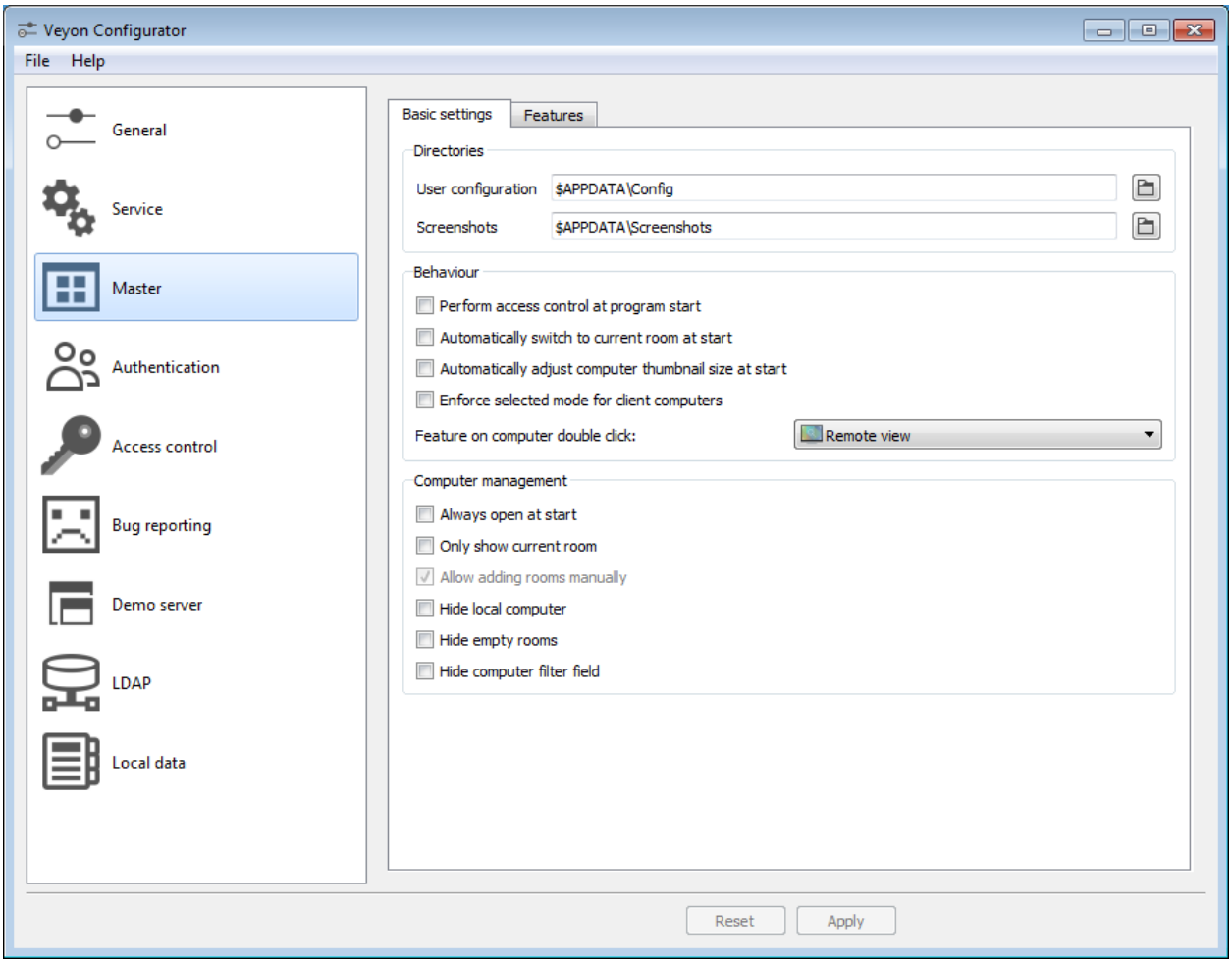
Delete all Veyon-related settings during uninstalling:

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

CHAPTER 3

Configuration

To commence the configuration, start Veyon Configurator if that has not been done automatically upon completing the installation. This program allows you to configure and customize a local Veyon installation. Thereby the graphical user interface is divided into several topic or component related configuration pages. Depending on the installed plugins there may be additional configuration pages.



In the *Configuration Reference* you can find a detailed description of all configuration pages and configuration options with their respective meanings.

3.1 Overview

The basic configurations on configuration page *General* refer to all *Components* of Veyon. This includes settings of user interface, *Logging* and the network object directory in which the rooms and computers displayed in the Master are located.

The setting on configuration page Service Configuration influence the functionality of the Veyon Service and serve for fine tuning and customization for implementation of special scenarios. For smooth operation the default settings should normally not be changed.

All setting on configuration page Master Configuration concern only behavior and functionality of the Veyon Master and apply system-wide for all users.

Hint: For a quick start to get to know the software you just have to activate the *Logon authentication* on configuration page Authentication Configuration and add one room and some computers on configuration page Local Data. After the configuration has been *exported to all computers* the Veyon Master can already be started and used.

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 on configuration page Authentication Configuration in Veyon Configurator.

3.2.1 Authentication Methods

In essence Veyon offers two different authentication methods, the keyfile authentication and logon authentication, that may be used singly or in parallel.

Keyfile authentication is based on Public-Key-Cryptography, meaning that a public key and a respective 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 their respective assets and drawbacks. Thus the better choice depends on the environment, the security requirement and desire for user comfort.

Keyfile 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
• configuration with low expenditure • 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 chosen authentication method can be activated and configured as described in section authentication configuration of the configuration reference.

3.2.2 Key Management

In order to use the keyfile-authentication, at first a key pair consisting of a public and a private key has to be generated. For this purpose you can use the according assistant. Start the assistant and follow the proposed steps.

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 *Base 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 carried out during connection initialisation after the authentication. Whilst authentication assures the authenticity of an accessing user, the access control functionality restricts computer access to authorised users, e.g. teachers.

Configuration can be done via configuration page *Access Control* and is described in detail in section Access Control in the configuration reference.

Important: As with all other settings, the configuration of access control is part of the local Veyon configuration. Hence the configuration must be *exported to all other computers* in order to work properly.

3.4 Local Data

On configuration page *Local Data* the Rooms and Computers can be created, such that they can be displayed in Veyon Master if the network object directory-backend *Standard* is used. In contrast to backend such as *LDAP* this information is stored in the local configuration and therefore must be transmitted 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 with a double-click.

The right list contains a computers that are based in the currently selected rooms. Using the two buttons below the list, computers may be added or deleted. The single lies in the table can be edited with a double-click. For each computer a name and a computer/IP-address has to be provided. In case the Veyon function *Wake-on-LAN <https://en.wikipedia.org/wiki/Wake-on-LAN> _* shall be used, the respective MAC-address has to be provided as well. Otherwise this column can be left empty.

3.5 LDAP

All information dealing with connecting Veyon to an LDAP-compatible server such as *OpenLDAP* or *Active Directory* are collated in chapter *LDAP/AD Integration*.

3.6 Error Report

Configuration page *Error Report* contains a step-by-step guide for creation of an error report. This information can be used to provide feedback concerning errors or faulty behavior to the developers. However, before you create an error

report, make sure you have extensively consulted the chapter *Troubleshooting*, since the problem may potentially be a configuration error.

3.7 Importing/Exporting a Configuration

One important premise for the use of Veyon is an identical configuration on all computers. A transmission of the Veyon configuration to another computer can be carried out manually for a start, but should be automated later on. There are several methods available for both ways.

In 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 by another computer using the entry *Load Settings from File* in the same menu. Please note, that any settings that are imported through the graphical user interface are immediately loaded, but are saved in the system only after pressing the *Apply* button.

Through the Configuration Management module within the command line interface configuration import and export can be carried out automated or script-controlled.

Additionally, when using 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`.

3.8 Reset Configuration

In some faulty situations it may be helpful to reset the entire Veyon configuration and rebuild it from scratch 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 a 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

Rule Set for Computer Access

4.1 Introduction

In case a detailed control over access to specific computers under specific circumstances for a user are needed, you can realize this control with the help of access control rules. For convenience, throughout this text we will use the term *rule* synonymously with *access control rule*.

If a user tries to access a computer, all previously defined access control rules are flicked through until all conditions of a rule match. As soon as all activated conditions of a rule match, no further rules will be processed and the defined action will be triggered. (Exception: the rule is disabled.)

The rules can be configured through the Veyon Configurator at the configuration page Access Control in section *Access Control Rules*. By default the list of rules is empty. In this case all attempts for access are denied, since there is no rule explicitly granting access. It follows, that there must be at least one rule defined which allows access under certain conditions.

4.2 Add and modify rules

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

In essence a rule consists of general settings, conditions and an action, that is triggered, if all conditions match. Hence the dialogue is splitted in three sections. Hereafter we will explain the meaning of the specific options in the different areas of the dialogue.

4.2.1 General

At first a name for the rule should be defined in input field *rule name*. We use the name to identify the rule and display it in the list of rules. For documentation purposes an optional description can be entered in the *Rule Description* input field.

The option *Always process rule and ignore conditions* ensures that while processing the rules the conditions specified below are not checked and the defined action is always triggered. This behavior is particularly helpful for the fallback rules located at the botton of the list of rules to make sure that the signed in user is asked for permission if no other rule applies.

Through the option *Invert all conditions* you can determine that all activated conditions are inverted before evaluation, meaning that activated conditions must not be satisfied. For example, if the condition *No user logged in* is activated, the rule will only be applied if one or more users are logged in. 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 this group.

4.2.2 Conditions

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

User is member of group With this condition you can define that either the accessing or the locally signed in user must be a member of a specific group. The desired group can be choosen. If no or only wrong groups are selectable, you might adjust the *data backend* in the general settings for computer access control.

Computer is based in room With this condition you can define that either the accessing or the local computer has to be based in a specific room. The desired room can be choosen. If no or only wrong rooms are selectable, you might adjust the *data backend* in the general settings for computer access control.

Accessing computer is based in the same room as the local computer With this condition you can define that the accessing and the local computer have to be based in the same room. Thus is can be prohibited that a teacher accesses computers used in a different class in a different room.

Accessing computer is localhost If this condition is activated, the rule applies only if the accessing computer is the local host. Thus is can be ensured that teachers can access the local Veyon Service. This access is necessary for the Veyon Master to execute specific functions via the Veyon Service (i. a. the server for demo mode).

Accessing user has one or more groups in common with local (signed in) user With this condition you can define that the accessing and the local user have to be common members of at least one group, for example a user group for a class or a seminar.

Accessing user is signed in user As an alternative to the condition *accessing computer is localhost* you can permit for a user to have access to his own sessions. Therefore this condition has to be activated.

Accessing user is already connected In conjunction with the condition *accessing computer is based in the same room as the local computer* an extended rule set can be created allowing access to other rooms under certain conditions. Included is the possibility to access a computer, if the accessing user is already connected. For example, if the teacher logs into a teacher computer in room A and B simultaneously and has the computers of room B displayed by Veyon Master, the Veyon Service running on the computers in room B receives a connection from the teacher. Thus the teacher can access resources in room B from within room A, if this condition is activated with a permissive action.

No user logged in With this condition you can define how a computer may be accessed, if no user is currently logged in. As a support in computer administration it may be helpful in some cases to be able to access a computer even though no user is logged in.

4.2.3 Action

If all activated conditions of a rule are satisfied, a predefined action is triggered 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 existed a rule further down the list of rules denying access, however, access would still be granted. There must be at least one rule containing this action.

Deny Access Access to a computer is denied and further rules are not processed. If there existed a rule further down the list of rules allowing access, however, access would still be denied.

Ask signed in user for permission This action shows a dialogue on the screen by which the signed in user can choose whether he or she wants to allow or deny access. Independent of the outcome no further rules are processed.

Rule disabled With this action the rule is ignored and processing is continued with the following rule. This option can be chosen to create an interactive dummy entry for visual subdivision of the list of rules.

By clicking the *OK* button the rule resp. the changes carried out are taken over and the dialogue is closed.

4.3 Sorting Rules

Important: The defined access control rules will be processed in the order they are defined in the list. However, the action for the first matching rule will be triggered even if there are subsequent rules that would also match and result in triggering another action.

All defined rules can be rearranged (meaning re-prioritized) using the arrow symbols. Rules containing criteria meant for general granting or denial of access should be listed topmost. Rules for coping with special cases may be listed further down the list. Rules defining some sort of fallback behavior should be and the bottom of the list.

4.4 Logical Concatenation of Rules

If more than one condition is activated, *all* conditions must be satisfied in order for the rule to be applied (logical AND). If only one out of several rules must be satisfied (logical OR), several access control rules have to be defined.

Using basic knowledge of Boolean algebra, the option *Reverse 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 said user is *not* a member of one of these groups.

Note: If there is no matching access control rule such that all activated conditions are satisfied, access is denied and the connection is closed. Thus we prevent that an attacker can access resources because of an unfinished rule set.

4.5 Testing a Rule Set

In section *Computer Access Control* the configured rule set may be tested against various scenarios using the *Test* button. You can enter the parameter for reconstructing a specific scenario in the test dialogue. Press *OK* and the rules will be tested with the given parameters and a report with the test result is shown.

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 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 frames 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 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 eponymic 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 LDAP-CLI 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.

Important: These optional filters follow the well-known scheme for LDAP filters (see for example RFC 2254 or Active Directory: LDAP Syntax Filters). However, they have the feature that outer brackets must not be specified. For example, a simple objectClass filter must be defined as `objectClass=XYZ` rather than `(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 Utilizing LDAP Backends

After successful configuration of the LDAP integration, the LDAP backend can be activated. To this end the network object directory as well as the database backend for the computer access control have to be customized. 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 database backend has been reconfigured for the computer access control, the 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 you can use *Veyon Configurator* as well as the command line tool *Veyon Control*. The program can be opened by the `veyon-ctl` command via the command line. If the installation directory of Veyon is not listed in the environment variable `$PATH` (Linux) resp. `%PATH%` (Windows), you have to change to the installation directory or prefix the program name with this directory.

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

```
$ veyon-ctl help
Available modules:
    config - Commands for administering the Veyon-configuration
    ldap - Commands for configuring and testing the LDAP/AD integration
    service - Commands for configuring and controlling the Veyon-service
    remoteaccess - Remote view or remote control of a computer
```

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

```
$ veyon-ctl config help
Available commands:
        clear - delete system wide Veyon-configuration
        export - export configuration to the given file
        get - read and print configuration value for the given key
        import - import configuration from the given file
        list - list key-value-pairs for all configuration keys
        set - write given value to the given configuration key
        unset - reset given configuration key
```

In some modules the `help` command can be supplied with a command name as a second parameter to display specific help for the inferred command:

```
$ veyon-ctl remoteaccess help control

remoteaccess control <host>
```

6.1 Administration of your Configuration

You can administrate your local Veyon-configuration by using the `config` command. Thereby you can read or write an entire configuration as well as single configuration key.

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 allows exporting the local configuration to a file. The name of the target file must be supplied as a parameter:

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

import

This command imports a previously exported configuration file into the local configuration. The name of the file containing the configuration to be imported must be supplied as a parameter:

```
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

This command allows writing to a single configuration key. The name of the key and its desired value must be supplied as parameters.

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

```
veyon-ctl config set Authentication/KeyAuthenticationEnabled true
```

unset

This command allows deleting a single configuration key resulting in Veyon using the internal default value for this key. The name of the key must be supplied as a parameter.

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

6.2 Control of Services

You can control the local Veyon-service by using the module `service`.

register

This command registers the Veyon-service as a service running on the operating system, such that the service is automatically started when booting.

```
veyon-ctl service register
```

unregister

This command removes the registration of the service on the operating system, such that the Veyon-service is no longer automatically started when booting.

```
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
```

6.3 LDAP

The commands available in the `ldap` module are documented in section LDAP-CLI in chapter *LDAP/AD Integration*.

6.4 Remote Access

The `remoteaccess` module provides functions for a graphical remote access to remote computers. These are the same function that can be used from within the Veyon master. For example, a function provided by the command line tool can be used to create a link for directly access on a specific computer.

control

This command opens a remote control that can be used to control a remote computer. A computer name or IP-address (and optionally a TCP-port) has to be supplied as a parameter:

```
veyon-ctl remoteaccess control 192.168.1.2
```

view

This command opens a remote view that can be used to monitor a remote computer. In this mode the content on the screen is displayed in real time, but interaction isn't possible until the corresponding button in the tool bar has been clicked. A computer name or IP-address (and optionally a TCP-port) has to be supplied as a parameter:

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

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*

High-DPI-Scaling In case Veyon is used on high resolution screens with a high pixel density (DPI>150) this option should be activated. In this case the user interfaces are displayed larger such that readability especially of visual elements with text caption is improved.

Default: *disabled*

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.

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 network object directory 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 local data 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*

7.2 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*

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*

Additional parameters If the Veyon service is registered as a system service, you can use this option to supply additional parameters which the operating system passes to the Veyon service upon starting. A more detailed explanation of possible options can be found in section *Program Parameters for Veyon Service*.

Default: <*empty*>

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 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.

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*

7.3.2 Behavior

Perform access control on 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*

Adjust computers' thumbnail size automatically upon starting 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*

Enforce chosen mode for client computer 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 hazardous 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 Computer Management

Always open on start You can use this option to define that the computer management is opened upon program start by default. **Default:** *disabled*

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 filter field for computers 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*

7.3.4 Functions

With the help of the two lists in the *Functions* tab is can be defined which functions are available in Veyon Master. Single functions 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 functions are not to be used anyway.

A function 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 function.

7.4 Authentication

7.4.1 Authentication Methods

There are same-named options provided for the *Authentication Methods* described in chapter *Configuration*. After an option has been activated, the configuration of the respective authentication method is possible.

Keyfile authentication You can use this option is activate keyfile authentication. The configuration can afterwards be done using the keyfile-assistant.

Default: *disabled*

Login authentication You can use this option to activate login authentication. No further configuration is required and you can test the functionality directly after activation using the *Test* button.

Default: *disabled*

7.4.2 Key Management

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. 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 local data. 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 local data: 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 authorized user groups 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 Authorized User Groups 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 Rules Set for Computer Access.

7.6 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*

7.7 LDAP

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

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 Program Parameters for Veyon Service

Dependening on the operating system under which Veyon is run, the Veyon Service can take various program parameters. The desired parameters have to be entered in the *general service settings*.

Parameter	Operating System	Meaning
`-session <ID>`	*all*	An integer between `0` and `99` can be used as optional session-ID, to have multiple instances of the Veyon Service running in different user sessions on the same computer. The session-ID is added to the number of the port configured in the network settings, such that each instace of the Veyon Service is working with different ports. You have to enter the absolute port (primary service port plus session-ID) together with the computer/IP-address, e.g. `192.168.2.3:11104`.
`<x11vnc parameter>`	Linux	The Veyon Service can take all parameters supported by the program `x11vnc`. For more information on this topic, please see the *x11vnc manual <http://...>* _.

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 configuration. 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 settings, 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 settings 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 settings 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 settings. 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 Base 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

Following the update of early beta-versions of Veyon 4 it may be the case that some configuration keys are inconsistent and must be recreated. This may imply that settings cannot be correctly saved or reloaded, for example local information on room and computers. In this case the configuration should be reset completely (*Completely Reset Configuration*) 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 Settings 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. However, one goal among others in the process of further development is to port Veyon to other platforms and provide respective installation files. In this context the Veyon project is dependent on support from experienced software developers, especially for porting Veyon to MacOS and Android.

9.2 How can I add computers in order to access them?

If the preconfigured network object directory is used, the only action required is adding the respective rooms and computers on the configuration page local data. Afterwards the added resources are available to the Veyon master.

If *LDAP/AD Integration* is configured the network object register has to be reconfigured to LDAP in order to make the computers listed in the register available to 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.

Whilst the configuration of authentication methods is very similar, the configuration of rooms and computers is done via the Veyon configurator and not via the master anymore. 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 configuration in section *VNC server*.

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

This is not possible with Veyon 4.0, but Veyon 4.1 will provide a an import feature as well as a command line interface for room and computer administration.

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 activate 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 in the room administration?

Just activate the option *Automatically hide local computer in room administration*.

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

T

U

V

W