Veyon Administrator Manual

Release 3.99.7

Tobias Doerffel

Aug 17, 2017

Contents

Important: The English version of this manual is not ready yet as it still needs to be translated from German. Please refer to the machine-translated version.

CHAPTER 1

Introduction

Veyon is a didactic software program, which was developed especially for computerwork at schools. Nevertheless it can be used in other learning environments.

Veyon provides the opportunity to monitor and influence trainee activities and consequently supports the work with modern technique in the classroom.

For example you are able to see the content of the trainee's screens on your own screen. If one of the trainees needs assistance, you can access the trainee's desktop and engage supportively. The trainee sees all of your actions and is so able to learn new procedures.

If you have to make a new circumstance understandable for the trainee, you can change to the demo-mode. The trainee has also the possibility to demonstrate something. For this action it is necessary to click on his desktop screen to bypass his screen to the screens of other trainees.

Veyon has other functions, too. Like locking the trainee screens, so that they are not able to work any further and are constrained to give you attention.

CHAPTER 2

Installation

Silent installation on Windows

Introduction

The NSIS installers provided by the Veyon project can be run in silent mode. This is useful for automated deployments in larger environments and should integrate easily with most software distribution mechanisms.

By passing the command line parameter "/S" to the installer all operations will be performed silently. The same applies to the uninstaller.

Examples

- Install Veyon silently:

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

- Uninstall Veyon silently:

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

- Specify installation directory with silent installation:

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

Please note that due to a bug in NSIS the /D=... switch always has to be passed as last argument.

- Automatically appy Veyon configuration from file after installation:

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

IMPORTANT: You have to specify an absolute path for the configuration file as the Veyon Configurator (which is used internally for applying the configuration) is not launched with the installer directory as current directory. Therefore either use the proposed *%cd%* variable or replace it with an absolute path.

- Silent auto installation without Master component:

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

- Clear configuration during uninstallation:

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

CHAPTER 3

Configuration

Access control

Introduction

The configuration page “Access control” allows to configure which users are allowed to access computers in an Veyon network in detail. Access control is performed during the connection initialization after the authentication. While the authentication is validating the authenticity of an accessing user, the access control functionality restricts the computer access to authorized users such as teachers.

The desired access control mode can be selected at the top of the access control configuration page. If authentication is sufficient (e.g. when using key authentication with limited access to the authentication keys) you can select the first option which does not perform any further access control at all. Select the second option to restrict access to members of certain user groups. The third option allows to configure fine-grained access control using custom access control rules. It is the most flexible mode while the initial configuration can be more complex to set up.

The access control configuration is part of the whole (machine-)local Veyon configuration just like all settings in the other configuration pages. The configuration has to be transfered to and applied on all client computers in order to work properly. Use the Veyon Configurator to easily perform this task in an automated manner (see section “Configuration management”).

Simple access control by user groups

The configuration of this access control mechanism is quite simple. The left list contains all available user groups. By default all local user groups are listed here. If you set up LDAP/AD integration all LDAP user groups will be shown here instead. You can select one or more groups and move them to the right list using the appropriate button between the two lists. All members of each group moved to the right list will be allowed to access computers. As usual don’t forget to update the configuration on all clients.

Access control rules

If you require fine-grained control of which user is allowed to access which computer you can make use of this access control mode. If an user tries to connect to a computer all access control rules are processed consecutively until the conditions of one rule match. In the following the term "rule" will be used synonymous for "access control rule".

By default the rule list is empty which leads to every access attempt being denied because there's no rule which explicitely allows access. This means that you will have to add at least one rule which allows access under certain conditions.

Adding and editing rules

Use the "Add" button to open a dialog which allows to set up a new rule. In the section "General" you should enter at least a rule name which will be used to identify the rule and represent it in the rule list. Optionally you can enter a description for documentation purposes. Next you have to configure one or more conditions by selecting the desired entity (accessing user, accessing computer, ...) and activating the appropriate condition(s). You then have to select an argument for each activated condition such as the group the selected entity should be member of. You can also invert all conditions by checking the appropriate checkbox. However be careful with this option for not making the configuration too complex. See subsection "Logical linking of rules" for possible use cases.

Finally the desired action has to be selected. This can be either "Allow access" or "Deny access". If you want to disable the rule you can select the action "None".

Ordering rules

Rules are processed consecutively which means the action of the first matching rule will be taken even if subsequent rules would also match and possibly would lead to a different action. This is very important to know when defining the ruleset.

In consequence all rules leading to access denial should be placed in front of those rules allowing access. You can use the "Move up" and "Move down" buttons to change the order of rules.

Logical linking of rules

If more than one condition of a rule is activated each condition has to meet in order to make the rule apply (logical AND). If only one of multiple conditions has to meet (logical OR) multiple rules have to be created.

With a little knowledge of boolean algebra the "Invert all conditions" option can be used to set up advanced scenarios. Imagine the case where it is desired that a teacher is only allowed to access computers in the same computer lab as he is currently logged on. You could create a simple rule which says "Accessing computer is located in the same computer lab as local computer" with action "allow". However this would allow the access regardless of the user while it might be necessary to further restrict the access to members of a teacher group. The solution is to invert the rule by checking the "Invert all conditions" option and changing the action to "Deny access". Now every access attempt is denied if an accessing computer is not member of the same computer lab. Further rules afterwards can now safely allow access to individual users, groups or computers.

CHAPTER 4

FAQ - Frequently Asked Questions

CHAPTER 5

Glossary

From Wikipedia, the free encyclopedia

ACL Access Contol List

Client a computer system that accesses a (remote) service on another computer by some kind of network.

See also:

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

FAQ Frequently Asked Questions is a list of commonly asked question and there answers.

See also:

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

host any machine connected to a computer network, a node that has a hostname.

See also:

<https://en.wikipedia.org/wiki/Host>

hostname the unique name by which a network attached device is known on a network.

See also:

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

IP Internet Protocol is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched internetwork.

See also:

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

IP Address a unique number that devices use in order to identify and communicate with each other on a network utilizing the Internet Protocol standard.

See also:

<https://en.wikipedia.org/wiki/IP_Address>

IPv6 IPv6 (Internet Protocol version 6) is the latest revision of the Internet Protocol (*IP*), designed to deal with the long-anticipated problem of its precedessor IPv4 running out of addresses.

See also:

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

port a connection through which data is sent and received.

See also:

<https://en.wikipedia.org/wiki/Port_(computing)>

TCP Transmission Control Protocol is one of the core protocols of the Internet protocol suite.

See also:

<https://en.wikipedia.org/wiki/TCP>

URL Uniform Resource Locator is a sequence of characters, conforming to a standardized format, that is used for referring to resources, such as documents and images on the Internet, by their location.

See also:

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

Index