

OpenVPN4UCS



Quick Setup Guide

Table of Contents

i. Disclaimer.....	3
ii. WARNING regarding version differences between 1.1 and 2.0.....	4
1. Introduction.....	5
2. Prerequisites.....	5
3. Scenario 1 – Access for mobile users and home offices.....	6
3.1 Server setup.....	6
3.2 User setup.....	8
3.3 Client configuration.....	11
3.4 Connection overview.....	14
4. Scenario 2 – <i>site-to-site</i>	15
4.1 Server setup.....	15
5. Migration – <i>OpenVPN4UCS</i> 1.1 to <i>OpenVPN4UCS</i> 2.0.....	17
5.1 Version overview.....	18
5.1.1 Version matrix 1 – VPN functionality.....	18
5.1.2 Version matrix 2 – availability of <i>ready2go</i> packages.....	18
5.2 Upgrade / migration steps.....	19
5.2.1 Installing the <i>OpenVPN4UCS</i> update on <i>UCS</i> 4.4.....	19
5.2.2 Distribute new <i>ready2go</i> packages.....	20
5.2.3 Upgrade to <i>UCS</i> 5.0.....	20
5.2.4 Upgrade to <i>OpenVPN4UCS</i> 2.0.....	21

i. Disclaimer

Please be aware that *OpenVPN* is a powerful tool, which can be used for securing communication channels in a great variety of ways and use cases.

The integration package *OpenVPN4UCS* focuses on two common cases: providing secure access for users to a specific network / domain, as well as the connection between two sites. This also means that the integration package is not a graphical tool set for all possible setups *OpenVPN* could be used for.

With version 1.0 *OpenVPN4UCS* will be available free of charge for up to five users. Higher user amounts and site-to-site connectivity will be offered for a fee. More Details can be found on our product page:

<https://www.bytemine.net/openvpn4ucs/>

The product page is in German language only at the moment. We speak English - please contact us, if you need assistance.

To ensure the stability and usability of this integration package we (bytemine GmbH) invite you to get in touch with us to share your ideas and requirements.

If you are in need of further assistance, bytemine GmbH offers high quality *OpenVPN* and *Univention Corporate Server* consultancy.

Furthermore this quick setup guide is not meant as a replacement for fundamental VPN and IT security knowledge. People (administrators) using this software should have a general idea on IT security and Linux based systems.

End of disclaimer

ii. WARNING regarding version differences between 1.1 and 2.0

OpenVPN4UCS is available in two versions, which are **NOT (!)** directly compatible to one another! This is due to the changed public key infrastructure used by *OpenVPN4UCS* starting with *UCS 5.0*.

As a consequence a simple upgrade via the *Univention App Center* is not possible and is to be prepared and accompanied with manual steps involved!

Should you intend to switch *OpenVPN4UCS* from version 1.1 to 2.0 you are required to note the outlined migration steps at the end of this quick setup guide (see chapter 5)! **Disregarding the steps might lead to loss of connection!**

Therefor please read the document once in it's entirety. Should you gain the impression not to understand or comprehend (partial) aspects, please contact us **BEFORE** you start with the switch of versions on your own!

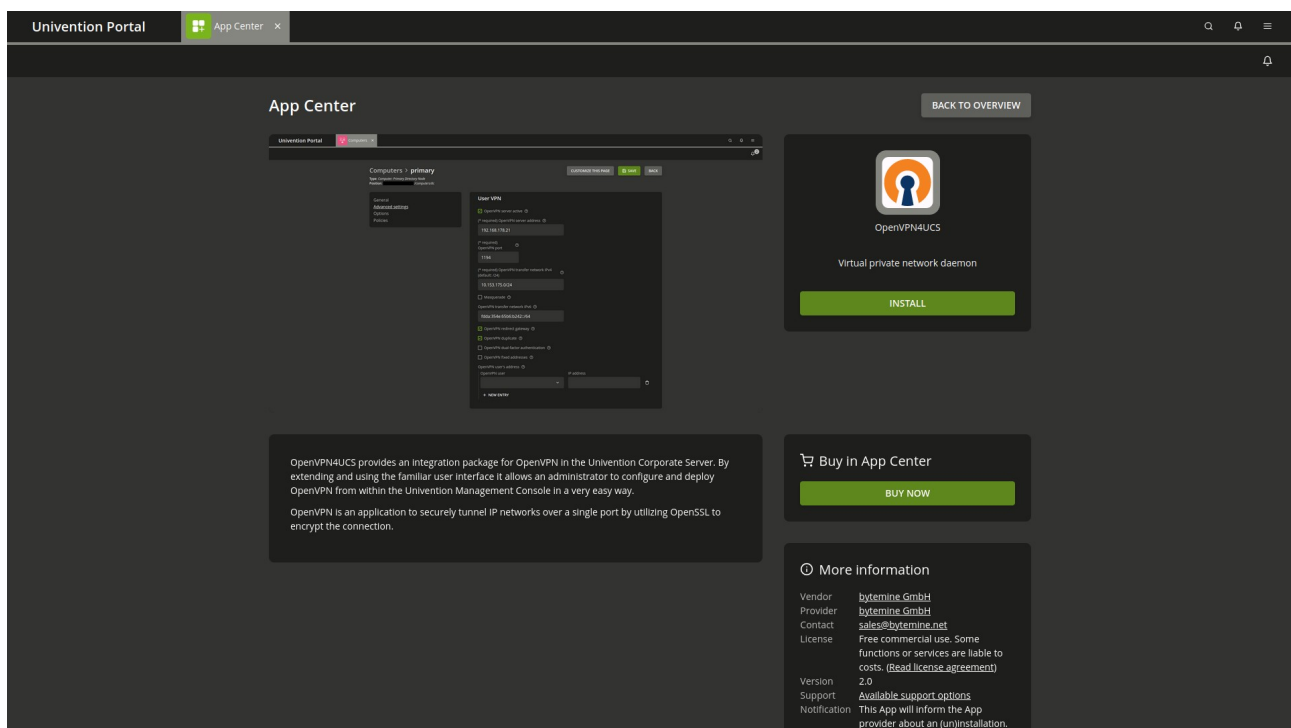
Unless stated otherwise the general instructions (not regarding the migration directly) are identical for both versions. Should there be any discrepancies between both versions, they will be hinted at.

1. Introduction

This guide will show how to use the **OpenVPN4UCS** integration module. Two typical scenarios will be taken as examples and their configuration will be shown and illustrated.

2. Prerequisites

- *Univention Corporate Server ; UCS 4.4 (for version 1.1) ; UCS 5.x (for version 2.x)*
- *TOTP functionality requires version 2.1 as a minimum.*
- *Administrative access to the **Univention Management Console (UMC)***
- *OpenVPN4UCS installed via the **Univention App Center**.*

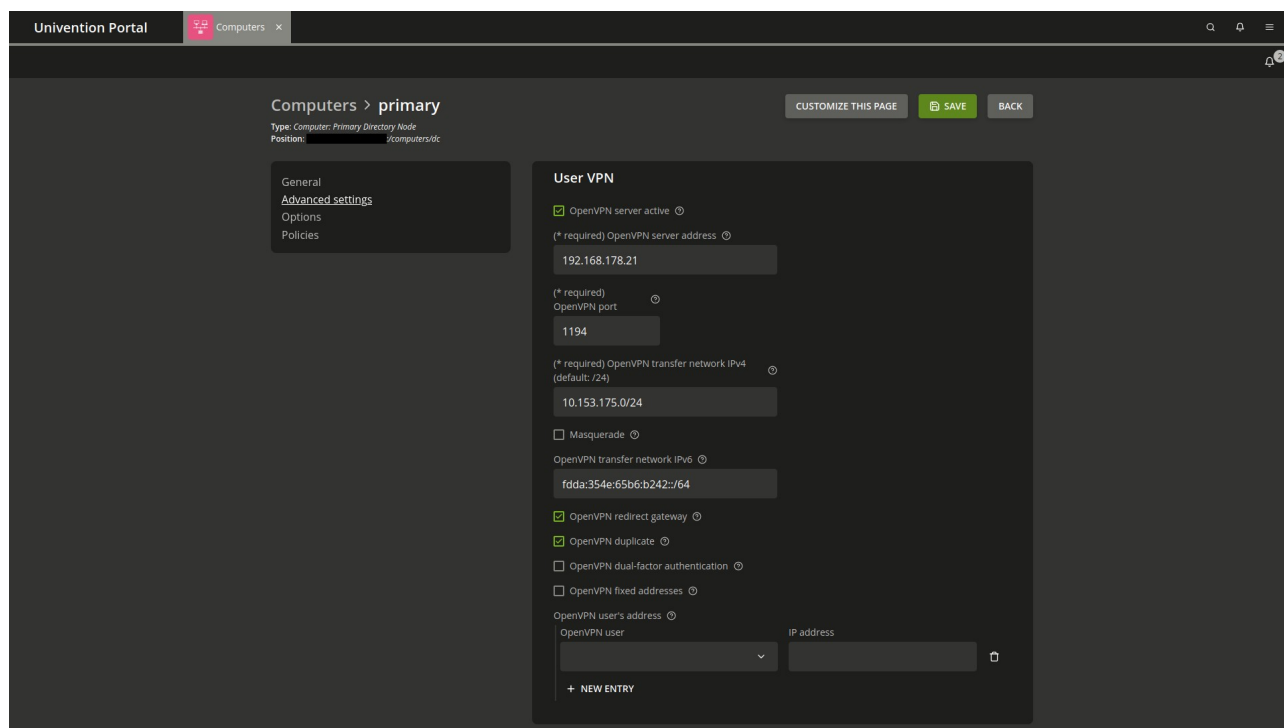


3. Scenario 1 – Access for mobile users and home offices

A common scenario for a VPN setup is to enable road warriors to access the company network and internal services while working from a remote location.

This can be achieved by setting up an *OpenVPN* server (also called VPN concentrator) easily.

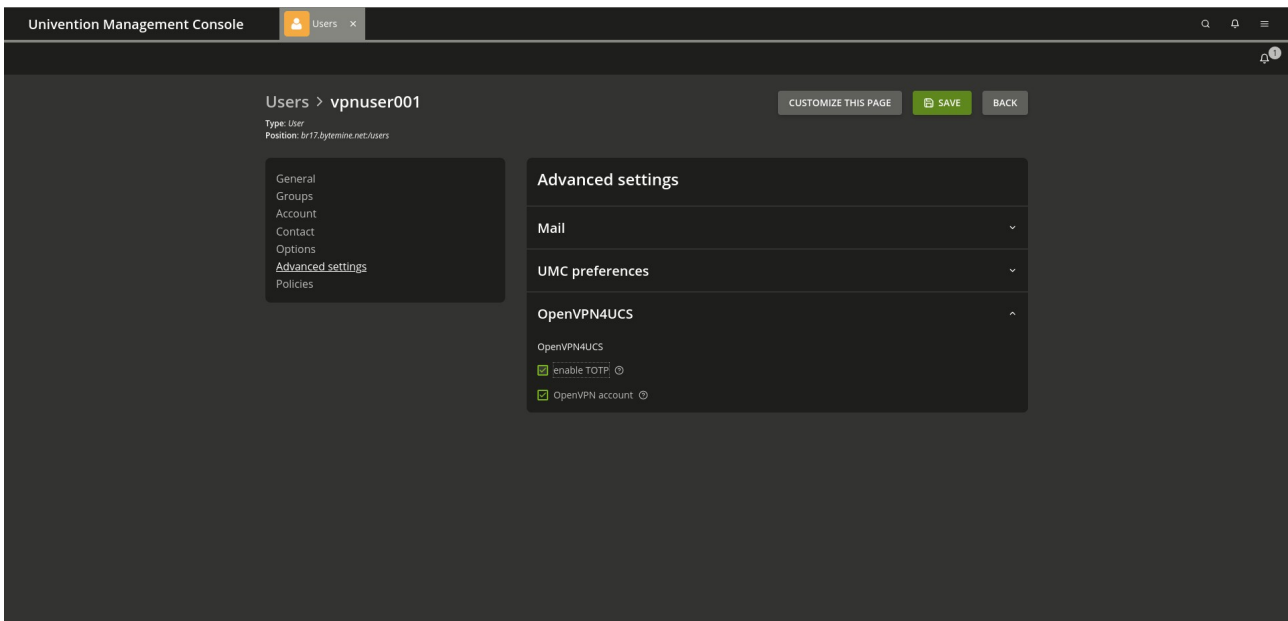
3.1 Server setup



- Within the *UMC* navigate to the member server that shall function as *OpenVPN* concentrator.
- Select “*Advanced settings*” and unfold the *OpenVPN4UCS* section.

- Edit the settings according to your desired setup:
 - The “*OpenVPN4UCS license key*” is only required if commercial features shall be used.
Default: none – Essential: no
 - Check the option “*OpenVPN server active*” to enable the *OpenVPN* services on the server.
Default: deactivated – Essential: yes
 - The “*OpenVPN server address*” is the IP used by clients to connect to the *OpenVPN* server.
Default: none (0.0.0.0) – Essential: yes
 - The “*OpenVPN port*” has to be accessible via the internet. Since version 1.0 this port will be open in the firewall.
Default: 1194 – Essential: yes
 - The “*OpenVPN transfer network*” is the actual VPN. You have to ensure, that the values do not collide with other existing networks.
Default: 10.173.175.0/24 – Essential: yes
 - The “*OpenVPN transfer network IPv6*” can be considered equally.
Default: 2001:db8:0:123::/64 – Essential: no
 - Check the option “*OpenVPN duplicate*” if users are allowed to connect with multiple devices simultaneously.
 - Check the option “*OpenVPN redirect gateway*” if the clients computer shall route all traffic through the VPN network.
 - “*OpenVPN fixed addresses*” can be used to assign static IPs within the VPN to a specific user. The drop down menu below shows users which have been defined as *OpenVPN* users already.
- Save the changes. The *OpenVPN* process will be started on the member server within a short period.

3.2 User setup



- Navigate inside the *UMC* to the user that you want to grant VPN access.
- Select “*Advanced settings*” and unfold the “*OpenVPN4UCS*” section.
- If usage of a *time-based one-time password* as a second factor during the authentication of a VPN user is desired, check the option “*enable TOTP*” (available with version 2.1).
- Check the option “*OpenVPN account*”.

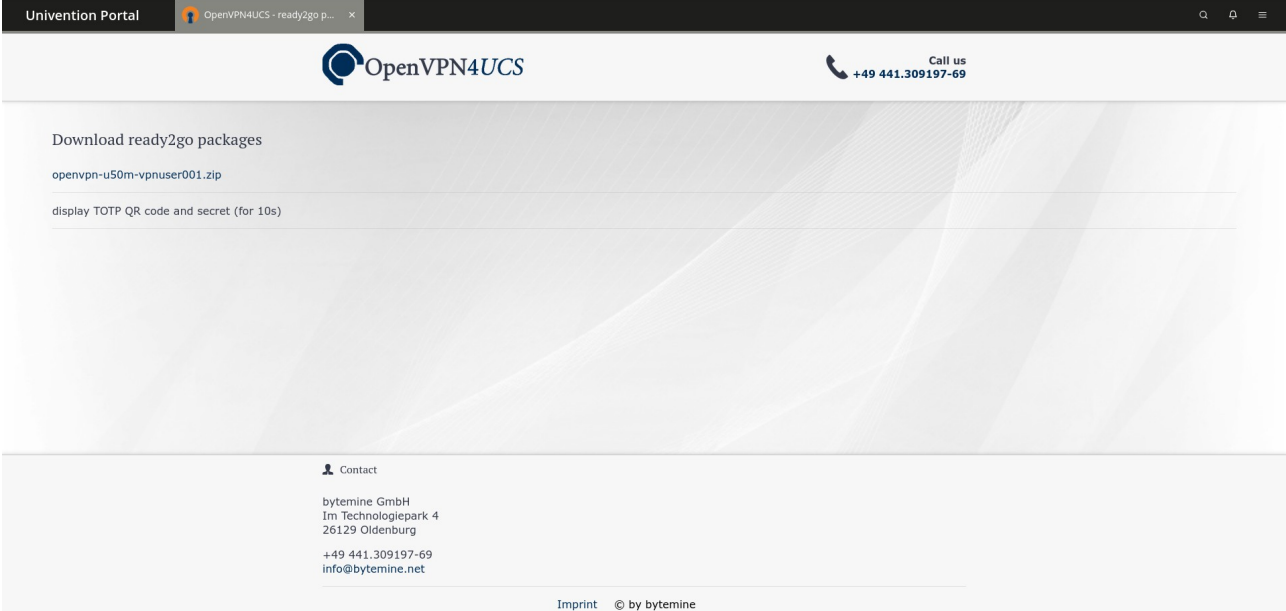
Hint: To be able to use *TOTP* a *TOTP* client, which is either able to read QR codes or able to process the *TOTP secret* via manual input, is required. These are available by various vendors for different types of systems, f.e. as a browser extension or an app on mobile phones.



- Certificates and client configuration (for Windows and Linux systems) are available as so called ready2go packages via a website for download.

https://<server>/download/

- The site is linked to via a tile in the *UCS portal* as well and can easily be accessed by users.
- The download is password protected and can only be retrieved by the specific user with their domain password.



Univention Portal OpenVPN4UCS - ready2go p... x

OpenVPN4UCS Call us +49 441.309197-69

Download ready2go packages

openvpn-u50m-vpnuser001.zip

display TOTP QR code and secret (for 10s)

Contact

bytemine GmbH
Im Technologiepark 4
26129 Oldenburg
+49 441.309197-69
info@bytemine.net

Imprint © by bytemine

- Click on the listed ZIP file to download the *ready2go* package.
- Click on “*display TOTP QR code and secret (for 10s)*” to display the QR code required for generating the *time-based one-time password (available with version 2.1)*.

Disabling the option “*OpenVPN account*” in the user section will revoke the users certificate (see above). The user is not allowed to connect to the VPN anymore.

Hint: Connections established prior to the cancellation will not be affected. If the connection of a user is to be terminated immediately, you have to do this manually (see section: connection overview).

Re-enabling the account will result in a new *ready2go* package. The certificates need to be replaced by the user, since the old ones have been revoked during the deactivation process.

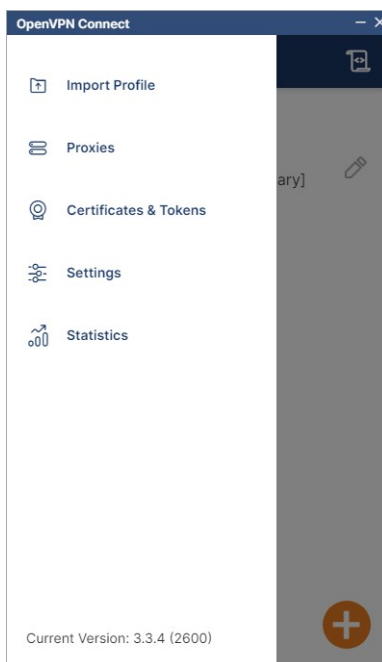
3.3 Client configuration

As there are many different operating systems and VPN clients existing this document only covers the configuration of the *OpenVPN Connect* client (here: version 3.x ; <https://openvpn.net/vpn-client/>) on a *Windows* system.

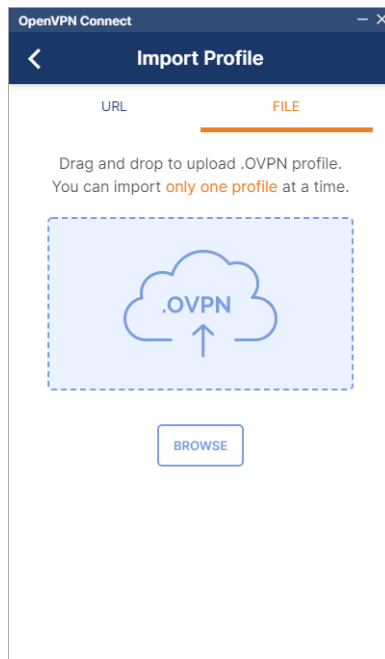
Hint: The following steps assume the usage of *OpenVPN4UCS 2.0*. In older versions configurations, keys and certificates are provided separated from one another in the *ready2go* packages, and not combined in a single file. In case an older version is used, those contents have to imported separately.

Assuming *OpenVPN Connect* is installed on the client already:

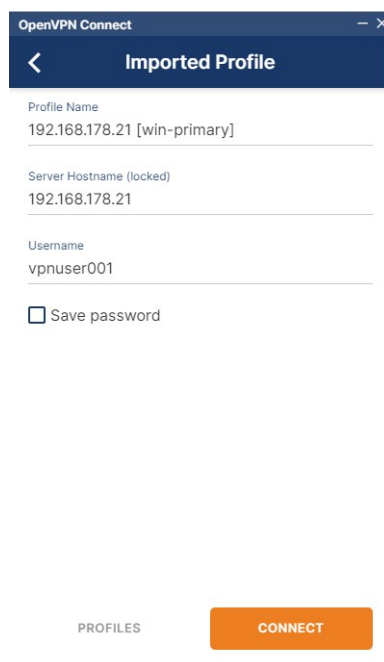
- Download the *ready2go* package for a certain user onto the client system and extract the content in a folder of your choosing.
- Start *OpenVPN Connect*, click on the burger menu and select *Import Profile*.



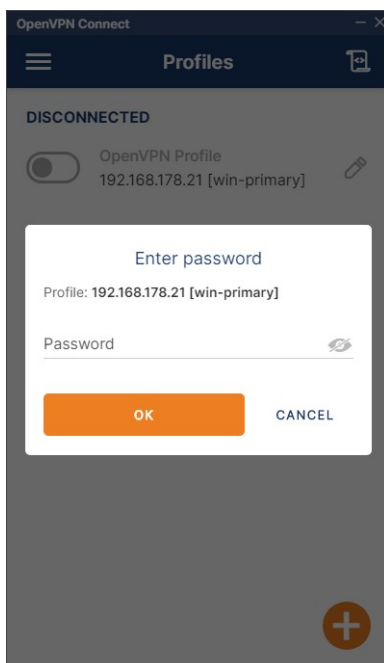
- Afterward choose *File* and drag the configuration file (with prefix *win-* in the filename) over the drag'n'drop field. Alternatively click on *Browse* and select the corresponding file.



- Subsequent a portion of the configuration will be shown. Add the domain username. Optionally you could change the profile name and set the password to be saved by checking the box *Save password*. Subsequent click on *Connect*.

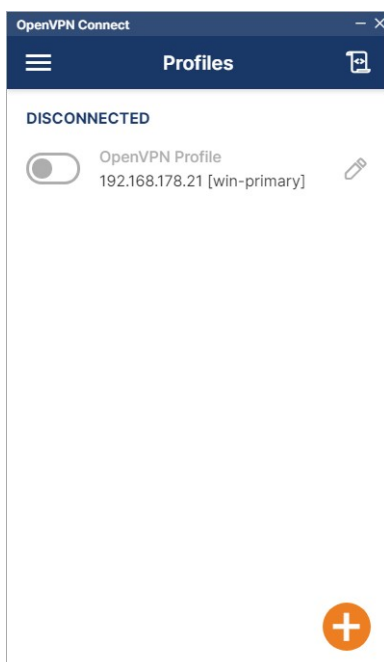


- Provide the user's password as requested and click on **OK**.

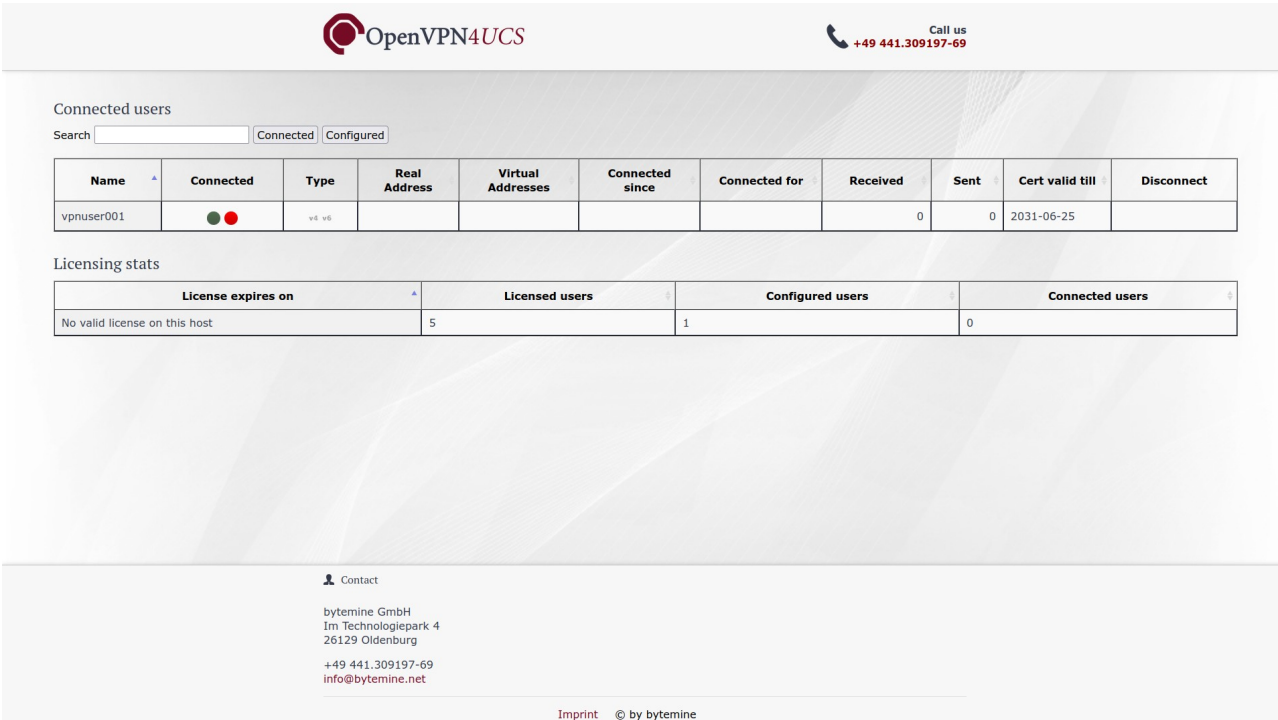


Hint: Is *TOTP* enabled as a second factor (see section user setup), the user will be prompted to enter the second factor separately.

- The Connection will be established. The profile is set for further usage in *OpenVPN Connect*. The usage of VPN can be toggled on and off by the switch left beside the profile name.



3.4 Connection overview



OpenVPN4UCS Call us +49 441.309197-69

Connected users

Search Connected Configured

Name	Connected	Type	Real Address	Virtual Addresses	Connected since	Connected for	Received	Sent	Cert valid till	Disconnect
vpnuser001	● ●	v4 v6					0	0	2031-06-25	

Licensing stats

License expires on	Licensed users	Configured users	Connected users
No valid license on this host	5	1	0

Contact

bytemine GmbH
Im Technologiepark 4
26129 Oldenburg
+49 441.309197-69
info@bytemine.net

Imprint © by bytemine

On the connection overview page *OpenVPN4UCS* displays an overview of all currently connected users, via this view it is possible to terminate each connection as well.

Hint: typically VPN clients tend to re-connect after if a session is terminated. If it is the goal to permanently disable the access for a specific user, the rights have to be revoke prior to the disconnect (see section: user setup).

The connection overview can be accessed via the *UCS portal* or directly:

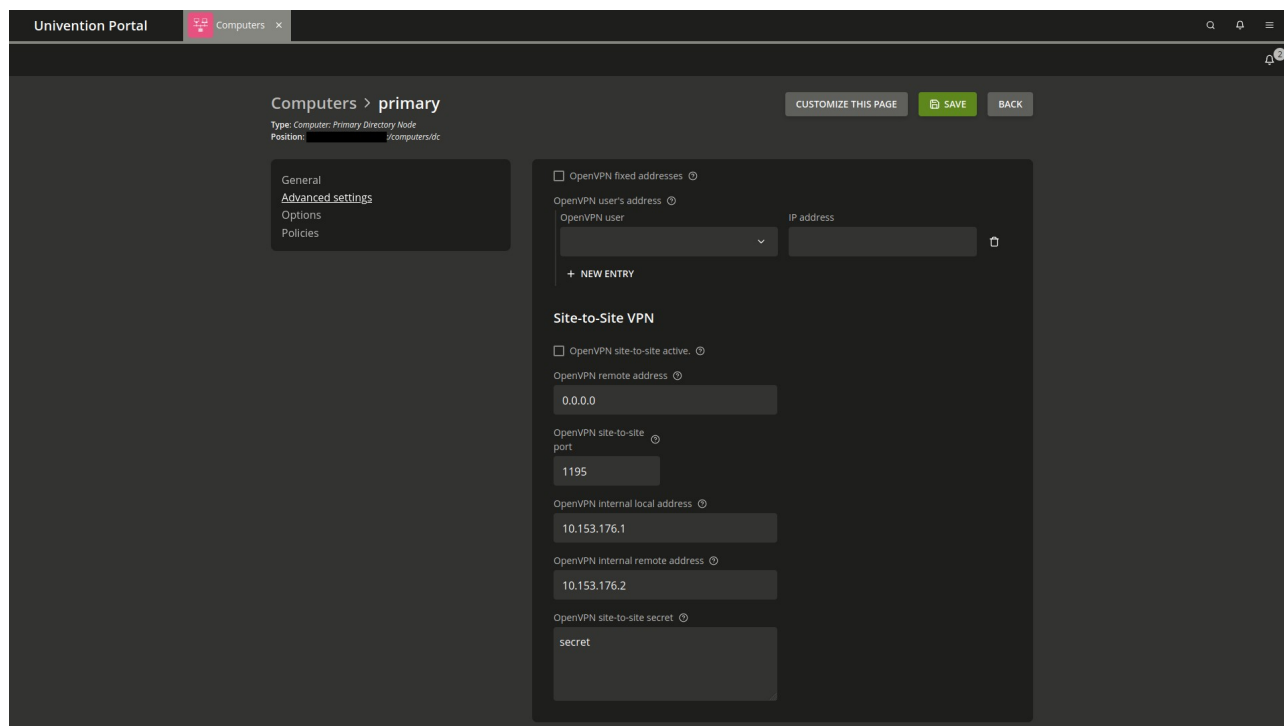
`https://<server>/display_users/`

The access is password protected and only available for the administrator.

4. Scenario 2 – *site-to-site*

The second scenario is the connection between two sites, called *site-to-site*, typically the connection of a main facility and a branch office. This feature is only available after entering a license key (see section: Scenario 1 – Access for mobile users and home offices). A valid license key can be obtained from us.

4.1 Server setup



To make use of the *site-to-site* connectivity it is essential to get the basic server setup properly (see scenario 1).

Furthermore the following options need to be configured:

- “*OpenVPN site-to-site active*” enables the site-to-site connectivity.
Default: deactivated – Essential: yes
- “*OpenVPN remote address*” is the IP address of the remote host, which a connection is to be established with.
Default: none (0.0.0.0) – Essential: yes
- “*OpenVPN site-to-site port*” defines the port over which the VPN is going to be build. Since version 1.0 this port will be opened in the firewall.
Default: 1195 – Essential: yes
- “*OpenVPN internal local address*” is the IP of the computer within the VPN. You have to ensure, that the values do not collide with other existing networks.
Default: 10.153.176.1 – Essential: yes
- “*OpenVPN internal remote address*” is the IP of the second computer inside the VPN.
Default: 10.153.176.2 – Essential: yes
- “*OpenVPN site-to-site secret*” is the key for the VPN. The key is generated dynamically during the installation process, since it needs to be assured that it is different on each installation. The key has to be added to the second computer manually.
Default: dynamic – Essential: yes

If the second computer, which the site-to-site connection is to be established with, is an *UCS* system of the same domain, it may be configured via the *UMC* as well.

5. Migration – OpenVPN4UCS 1.1 to OpenVPN4UCS 2.0

Hint: This chapter does not concern users, who are doing a first (initial) installation of OpenVPN4UCS 2.0 on UCS 5.x.

Background: Until UCS 4.4 OpenVPN4UCS used a function of the *Univention App Center (DefaultPackagesMaster)*, which allowed the installation of additional packages on the primary DC (Master). That function however is now deprecated and no longer available. Portions of OpenVPN4UCS had to be rewritten entirely and a new product variant originated, which provides its own public key infrastructure.

This led to the following consequences:

1. In this case an upgrade means a switch (migration) from one product variant (OpenVPN4UCS 1.1) to another (OpenVPN4UCS 2.0).
2. User configurations and certificates (*ready2go* packages), which were generated with OpenVPN4UCS 1.1, can no longer be used with OpenVPN4UCS 2.0.

To address these issues as good as possible OpenVPN4UCS 1.1.21 was made available. This version serves as a bridge for a migration to OpenVPN4UCS 2.0.

5.1 Version overview

Hint: Version 1.1.21 on UCS 5.0 has no installation candidate of its own. It is only present on UCS 5.0 systems due to a prior installation of *OpenVPN4UCS* on UCS 4.4. On UCS 5.0 there is only one installation candidate, which is *OpenVPN4UCS* 2.0.

5.1.1 Version matrix 1 – VPN functionality

OpenVPN4UCS version on UCS version	old VPN functional	old VPN configurable	new VPN functional	new VPN configurable
<= 1.1.19 on 4.4	yes	yes	no	no
1.1.21 on 4.4	yes	yes	no	no
1.1.21 on 5.0	yes	no	no	no
>= 2.0 on 5.0	no	no	yes	yes

Version matrix 1 shows which functionality is available on each version during the migration steps.

5.1.2 Version matrix 2 – availability of *ready2go* packages

OpenVPN4UCS version on UCS version	old <i>ready2go</i> packages available	old <i>ready2go</i> packages download	new <i>ready2go</i> packages available	new <i>ready2go</i> packages download
<= 1.1.19 on 4.4	yes	primary DC	no	primary DC
1.1.21 on 4.4	yes	primary DC	yes	OpenVPN server
1.1.21 on 5.0	yes	primary DC	yes	OpenVPN server
>= 2.0 on 5.0	no	OpenVPN server	yes	OpenVPN server

Version matrix 2 shows where the (new) *ready2go* packages can be downloaded. In version 1.1 this has always been the primary DC (Master). Starting with version 2.0 it is the server on which *OpenVPN4UCS* has been installed – this could be a primary DC (Master) as well.

5.2 Upgrade / migration steps

Subsequent a migration path is described, which allows to execute a switch to *OpenVPN4UCS* 2.0 and an upgrade to *Univention Corporate Server* 5.0.

Hint: During the entirety of the migration process it is never required to change configurations of *OpenVPN4UCS* servers and/or users via the *UMC*!

Recommendation: Carry out the steps completely in a testing environment, before you re-trace the steps in a productive environment.

Recommendation: Should you require assistance and/or you want to take advantage of services, please contact us.

5.2.1 Installing the *OpenVPN4UCS* update on UCS 4.4

Update *OpenVPN4UCS* to version 1.1.21 via the App Center. In addition to the regular functionality this version provides the public key infrastructure, as it is used in *OpenVPN4UCS* 2.0 on UCS 5.0.

After the installation a secondary *ready2go* package will be generated with the new public key infrastructure. It is made available via the download page linked in the *UCS portal* as well:

`https://<server>/download/`

Hint: To differentiate both *ready2go* packages the naming scheme of the downloads is deviating and structured as follows:

version < 1.1.21, with old PKI: `openvpn-<servername>-<username>.zip`

version = 1.1.21, with new PKI: **npki**/`openvpn-<servername>-<username>.zip`

On the server the new *ready2go* packages lie in a subfolder below the previous packages:

`/var/www/readytogo/<username>/npki/`

instead of

`/var/www/readytogo/<username>/`

Hint: The deviation is exclusive to version 1.1.21! *Ready2go* packages, which are later generated via *OpenVPN4UCS* 2.0 will reuse the older naming scheme and paths.

Case difference:

- a) Has *OpenVPN4UCS* been installed on a primary DC (Master), the new *ready2go* packages will be made available alongside the old ones via the same download page.
- b) Has *OpenVPN4UCS* been installed on a different server role, the download of the new *ready2go* packages will be made available on that particular server. In the *UCS portal* will be another tile (new *ready2go* packages), which links to the corresponding server. The older *ready2go* packages remain available via the download page on the on the primary DC (Master).

Should other users be provided with VPN access before the following steps are taken, both *ready2go* packages will be provided.

5.2.2 Distribute new *ready2go* packages

Distribute the new *ready2go* packages to the VPN users and advise them to **NOT USE** them immediately.

Define a point in time, when an upgrade to *UCS 5.0* and switch to *OpenVPN4UCS 2.0* shall take place and inform the users, that they are to switch to the new *ready2go* packages afterwards.

Hint: The new *ready2go* packages contain an all-in-one configuration for the clients (see chapter 3.3). These configuration files contain required settings, certificates and keys united in one single file. In *OpenVPN4UCS 1.1* those were provided as individual components in the *ready2go* packages.

5.2.3 Upgrade to *UCS 5.0*

!WARNING! A VPN generated on *UCS 4.4* and the corresponding *ready2go* packages can still be used after the upgrade to *UCS 5.0*. **However the VPN can no longer be configured via the UMC!**

Hint: This step should be taken, if you are able to execute the following steps immediately thereafter. This however requires you to have provided the VPN users with their *ready2go* packages.

Commence the upgrade to *UCS 5.0*.

5.2.4 Upgrade to OpenVPN4UCS 2.0

Hint: This step should be taken immediately after the upgrade to UCS 5.0.

Case difference:

a) If *OpenVPN4UCS* was installed on a primary DC (Master) the upgrade to version 2.0 can be done immediately after the upgrade to UCS 5.0.

b) If *OpenVPN4UCS* was installed on a different server role the script

```
/usr/lib/openvpn-int/cleanup-dmp
```

should be executed **DIRECTLY BEFORE** the upgrade is started. It removes the old packages remaining from *OpenVPN4UCS* 1.1. Only afterwards should the upgrade be started.

Commence the upgrade to *OpenVPN4UCS* 2.0 according to case.

Hint: From this point in time only the new *ready2go* packages are functional.

Hint: From this point in time the old *ready2go* packages are no longer offered for download on the primary DC (Master).

Hint: The old *ready2go* packages are no longer needed and should be removed manually from the primary DC (Master). They reside in the folder:

```
/var/www/readytogo/
```

Be aware of the hints in chapter 5.2.1! If *OpenVPN4UCS* was installed on the primary DC (Master) and there were new *ready2go* packages created before you start cleaning up, try incorporate timestamps and / or the content of the zip files to identify the obsolete ones. The new *ready2go* packages contain only two files.