bytemine GmbH | Im Technologiepark 4 | 26129 Oldenburg

OpenVPN4UCS

How-To / First Steps

OpenVPN4UCS >= 1.1

Table of Contents

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 toolset 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.html. 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 How-To 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.

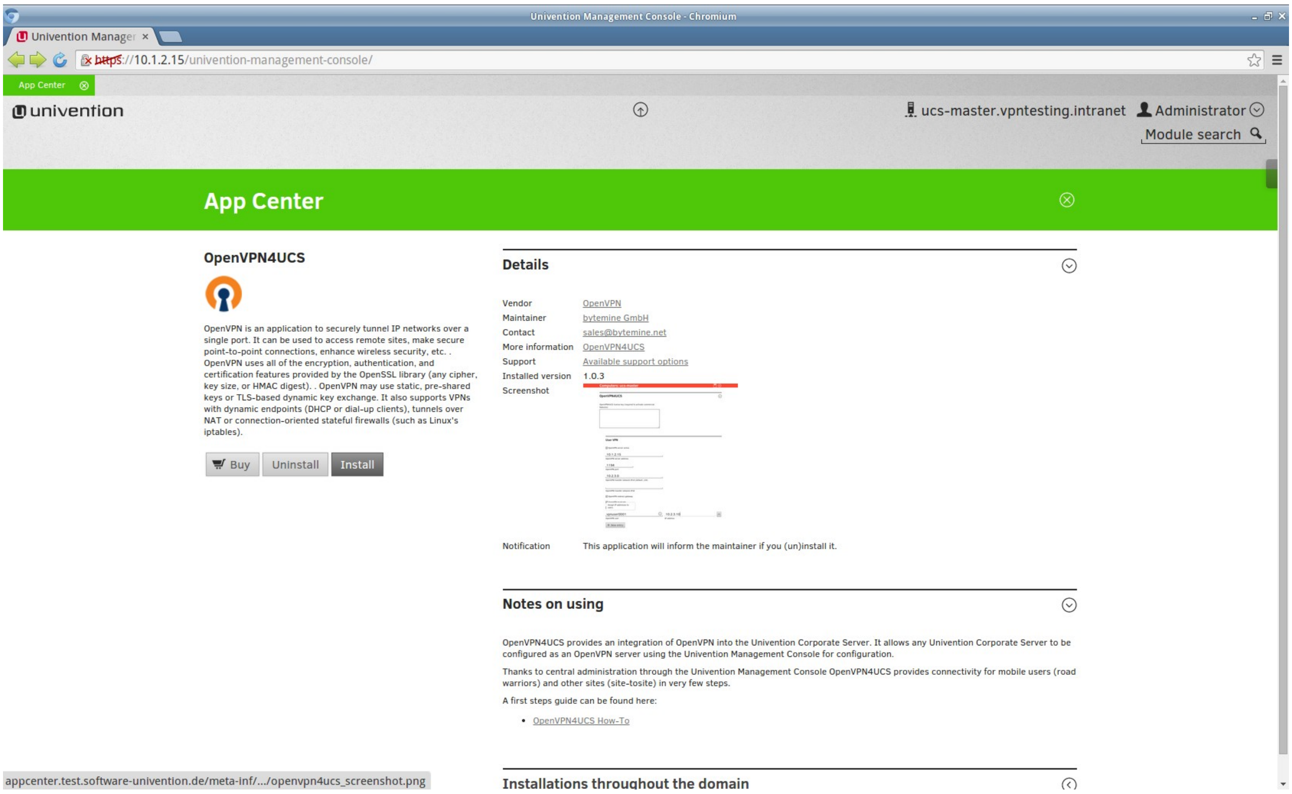
End of disclaimer

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.

Prerequisites

- Univention Corporate Server, at least version 3.2
- IPv6 connectivity requires *UCS* 4.0
- Administrative access to the *Univention Management Console (UMC)*
- ***OpenVPN4UCS*** installed via the *Univention App Center* (We are assuming the usage of a *memberserver* in this document.)


Univention Management Console - Chromium
Univention Manager ×
https://10.1.2.15/univention-management-console/
App Center
univention
ucs-master.vpntesting.intranet
Administrator
Module search
App Center
Buy
Uninstall
Install
appcenter.test.software-univention.de/meta-inf/.../openvpn4ucs_screenshot.png

OpenVPN4UCS

OpenVPN is an application to securely tunnel IP networks over a single port. It can be used to access remote sites, make secure point-to-point connections, enhance wireless security, etc. . OpenVPN uses all of the encryption, authentication, and certification features provided by the OpenSSL library (any cipher, key size, or HMAC digest). . OpenVPN may use static, pre-shared keys or TLS-based dynamic key exchange. It also supports VPNs with dynamic endpoints (DHCP or dial-up clients), tunnels over NAT or connection-oriented stateful firewalls (such as Linux's iptables).

Details

Vendor	OpenVPN
Maintainer	bytemine GmbH
Contact	sales@bytemine.net
More information	OpenVPN4UCS
Support	Available support options
Installed version	1.0.3
Screenshot	
Notification	This application will inform the maintainer if you (un)install it.

Notes on using

OpenVPN4UCS provides an integration of OpenVPN into the Univention Corporate Server. It allows any Univention Corporate Server to be configured as an OpenVPN server using the Univention Management Console for configuration.

Thanks to central administration through the Univention Management Console OpenVPN4UCS provides connectivity for mobile users (road warriors) and other sites (site-tosite) in very few steps.

A first steps guide can be found here:

- OpenVPN4UCS How-To

Installations throughout the domain

Hints regarding default settings and required fields in UMC

OpenVPN4UCS brings a lot of configurable options and predefined values with them. But in most cases you'll not be able to see them inside the *Univention Management Console*. The following lines explain this behavior.

To ensure that settings can be altered and saved accordingly the *Univention*-specific mechanism of *extended attributes* in the *UMC* and corresponding objects in *LDAP* are being used.

The options that accompany the integration as defaults are read out if a new computer object is being created. This means, that (1.) for existing objects (like the *UCS master* for example) no default values are being added and (2.) that (essential) settings, which ensure the proper work of the application, can not be defined as such – otherwise all prior existing objects would miss those essential settings.

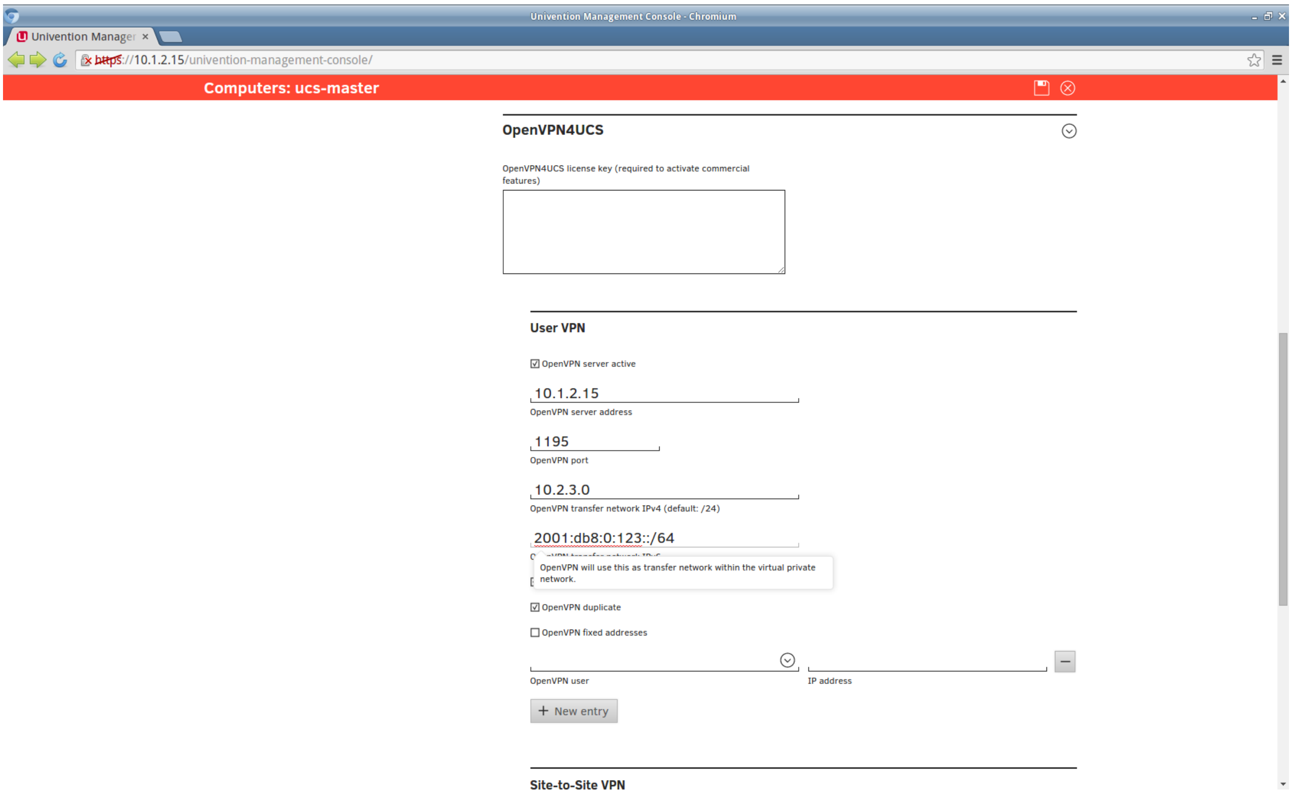
If an existing server is used as the *OpenVPN* server, the settings need to be set manually!

To take a look on the default settings, even if you do not want to add a real computer to the domain, you may add a *dummy* computer via the *UMC* after you installed ***OpenVPN4UCS***.

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) on an *UCS memberserver*, and distributing certificates and configurations to the user.

1. Server setup


Univention Management Console - Chromium
Univention Manage
~~https~~://10.1.2.15/univention-management-console/

Computers: ucs-master

OpenVPN4UCS

OpenVPN4UCS license key (required to activate commercial features)

User VPN

☑ OpenVPN server active

10.1.2.15
OpenVPN server address

1195
OpenVPN port

10.2.3.0
OpenVPN transfer network IPv4 (default: /24)

2001:db8:0:123::/64

OpenVPN will use this as transfer network within the virtual private network.

☑ OpenVPN duplicate

□ OpenVPN fixed addresses

OpenVPN user

IP address

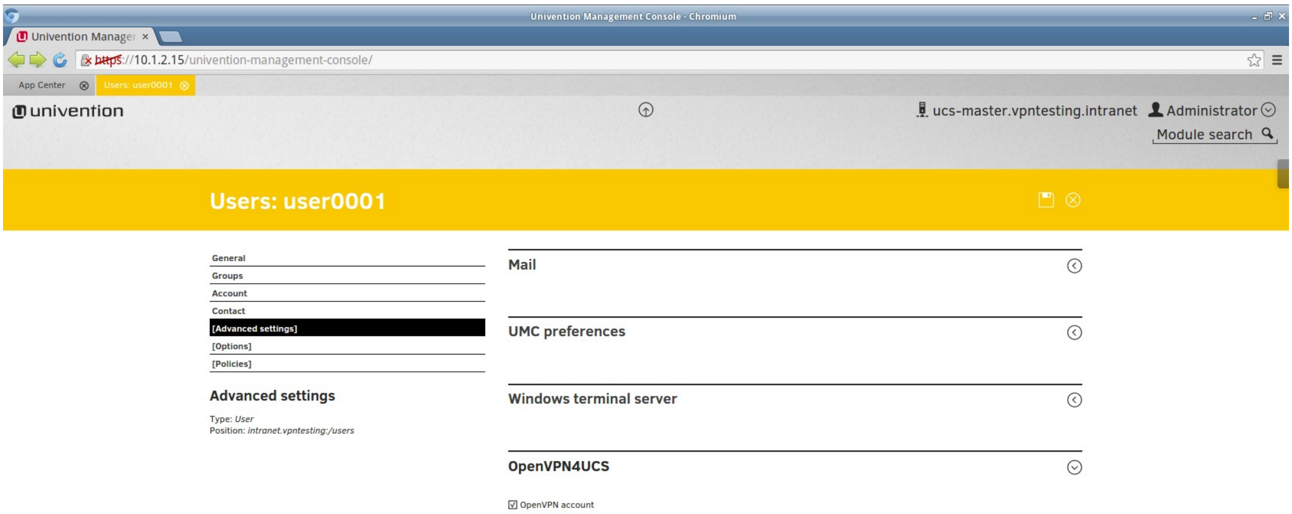
Site-to-Site VPN

- 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 accessable 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 concidered equaly.
    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.
  - Check the option "*OpenVPN dual-factor authentication*" if you want to have dual-factor authentication via privacyIDEA. Note that therefore privacyIDEA-pam should be configured correctly via its UCR variables.
  - "*OpenVPN fixed addresses*" can be used to assign static IPs within the VPN to a specific user. The dropdown 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.

2. User setup



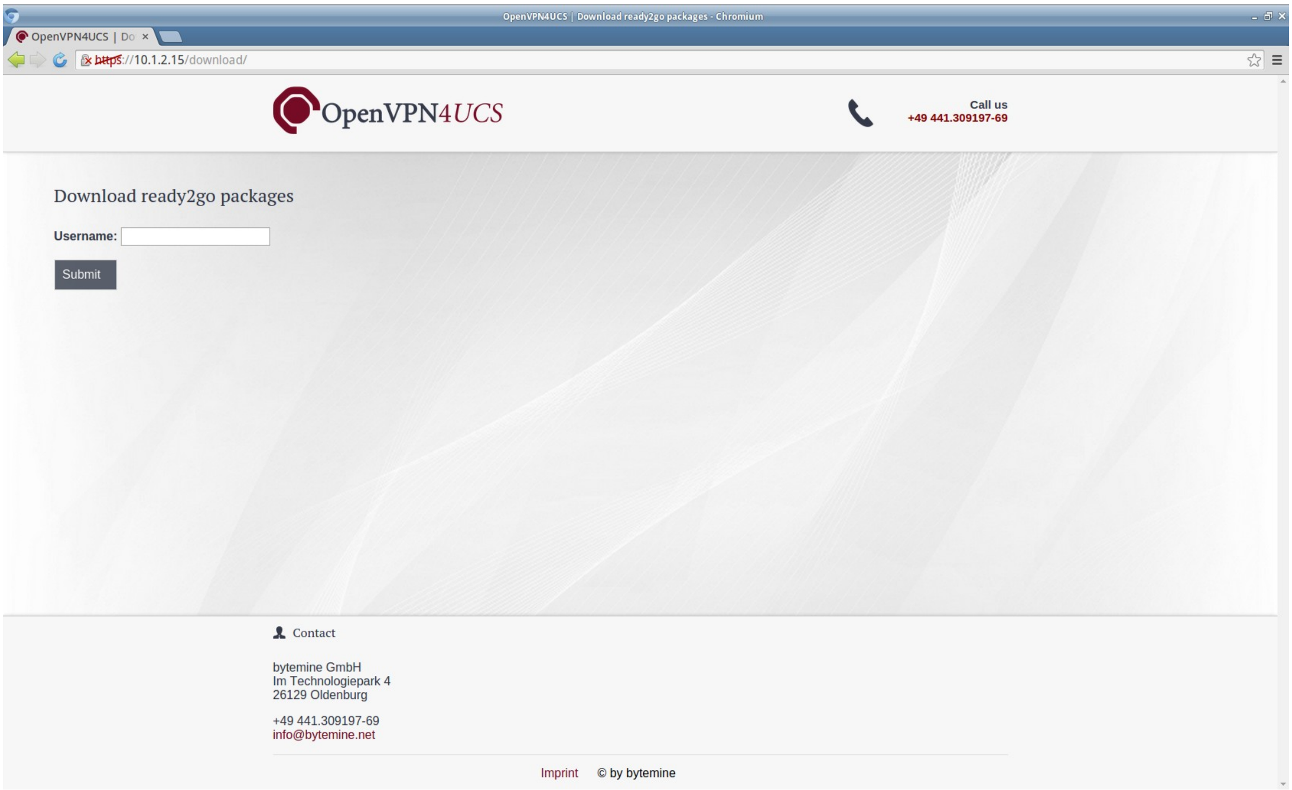
Users: user0001

Advanced settings

Type: *User*
Position: *intranet.vpntesting:/users*

☑ OpenVPN account

- Navigate inside the *UMC* to the user that you want to grant VPN access.
- Select "*Advanced settings*" and unfold the "***OpenVPN4UCS***" section.
- Check the option "*OpenVPN account*".



Download ready2go packages

Username:

bytemine GmbH
Im Technologiepark 4
26129 Oldenburg

+49 441.309197-69
info@bytemine.net

- 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 accessible via the *UCS overview* as well.

- The download is password protected and can only be retrieved by the specific user with their domain password.

Disabling the option "*OpenVPN account*" in the user section will revoke the users certificate. 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).

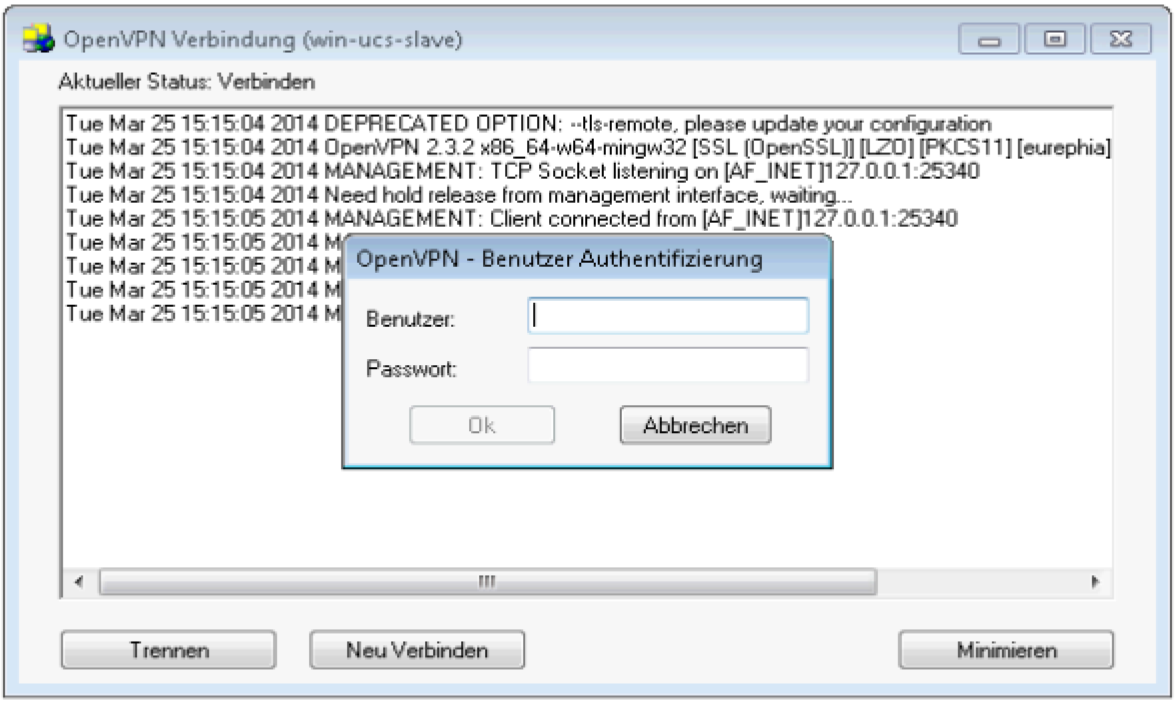
Re-enabling the account will result in a new *ready2go* package. The certificates need to be replaced by the user, since the old ones have been revoked during the deactivation process.

3. Client setup

As there are many different operating systems and VPN clients existing this document only covers the configuration of the *OpenVPN* client on a *Windows 7* system.

Assuming the OpenVPN software has already been installed:

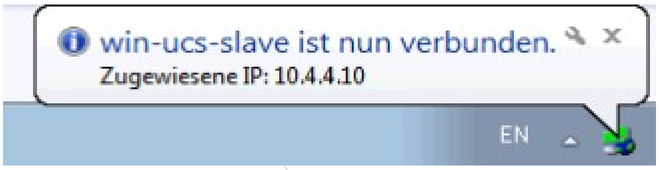
- Copy the ***OpenVPN4UCS*** *ready2go* package from your home directory to the OpenVPN\config directory and extract it there.
- Delete the *.ovpn* file that does **not** start with “win-”
- Open the *OpenVPN* GUI
  - Choose either “*Connect*” if this is the only *OpenVPN* connection, or
  - Choose the *OpenVPN* connection to the *UCS* member server if multiple configurations exist, and click “*Connect*”
  - Enter your username and password (same credentials as for the *UCS*)



OpenVPN Verbindung (win-ucs-slave)

Aktueller Status: Verbinden

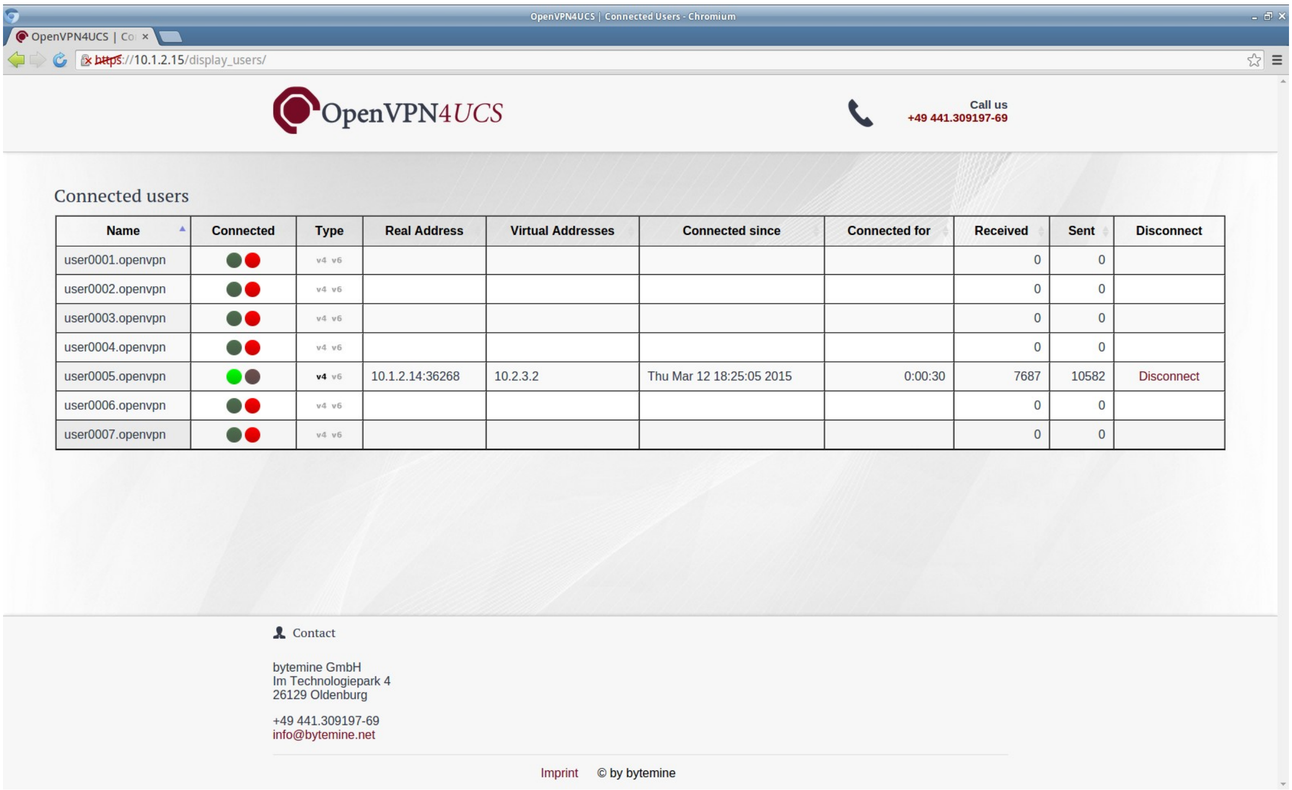
```
Tue Mar 25 15:15:04 2014 DEPRECATED OPTION: --tls-remote, please update your configuration
Tue Mar 25 15:15:04 2014 OpenVPN 2.3.2 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [eurephia]
Tue Mar 25 15:15:04 2014 MANAGEMENT: TCP Socket listening on [AF_INET]127.0.0.1:25340
Tue Mar 25 15:15:04 2014 Need hold release from management interface, waiting...
Tue Mar 25 15:15:05 2014 MANAGEMENT: Client connected from [AF_INET]127.0.0.1:25340
Tue Mar 25 15:15:05 2014 M
Tue Mar 25 15:15:05 2014 M
Tue Mar 25 15:15:05 2014 M
Tue Mar 25 15:15:05 2014 M
```



win-ucs-slave ist nun verbunden.

Zugewiesene IP: 10.4.4.10

4. Connection Overview



OpenVPN4UCS | Connected Users - Chromium
OpenVPN4UCS | Co ×
~~https~~://10.1.2.15/display_users/

OpenVPN4*UCS*

Call us
+49 441.309197-69

Connected users

Name	Connected	Type	Real Address	Virtual Addresses	Connected since	Connected for	Received	Sent	Disconnect
user0001.openvpn	● ●	v4 v6					0	0	
user0002.openvpn	● ●	v4 v6					0	0	
user0003.openvpn	● ●	v4 v6					0	0	
user0004.openvpn	● ●	v4 v6					0	0	
user0005.openvpn	● ●	v4 v6	10.1.2.14:36268	10.2.3.2	Thu Mar 12 18:25:05 2015	0:00:30	7687	10582	Disconnect
user0006.openvpn	● ●	v4 v6					0	0	
user0007.openvpn	● ●	v4 v6					0	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 OpenVPN 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 overview* or directly:

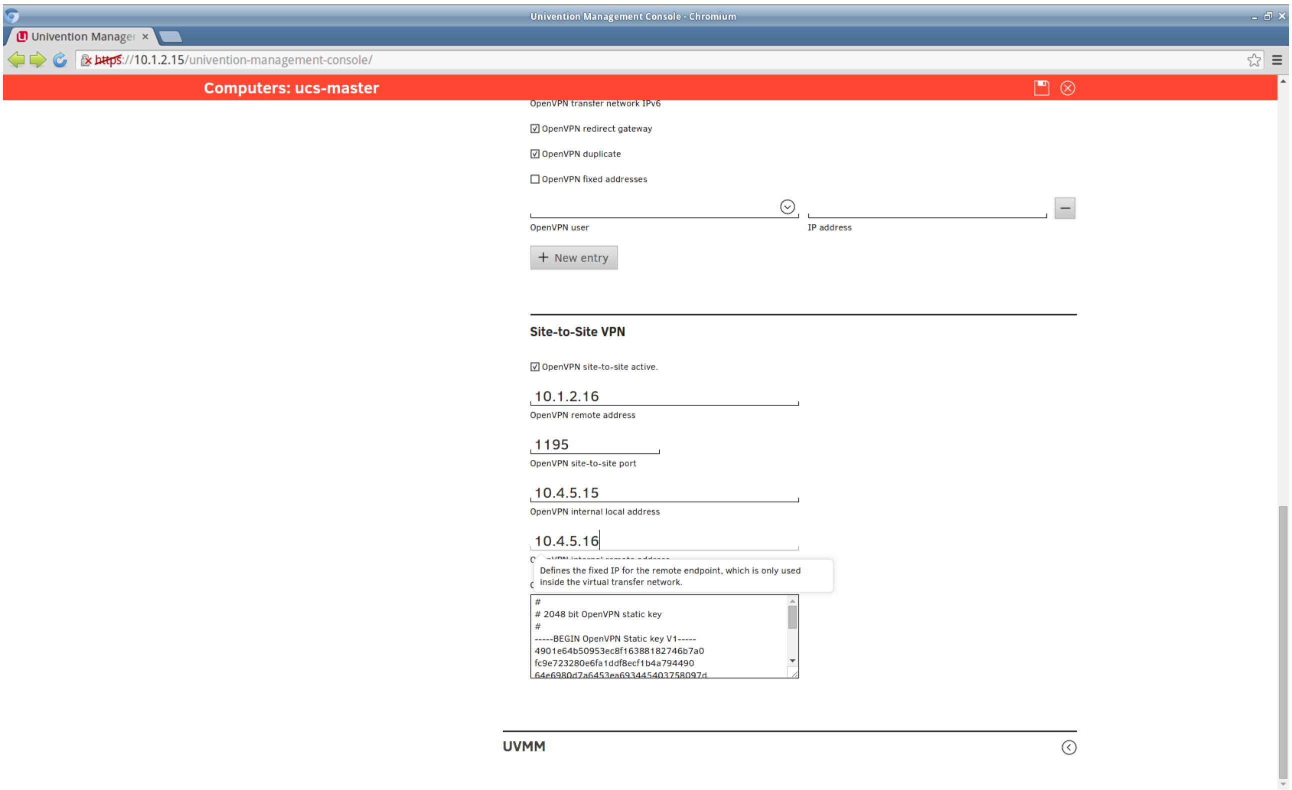
https://<server>/display_users/

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

Scenarion 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.

1. Server setup



Univention Management Console - Chromium
Univention Manager
https://10.1.2.15/univention-management-console/
Computers: ucs-master

OpenVPN transfer network IPv6

☑ OpenVPN redirect gateway

☑ OpenVPN duplicate

☐ OpenVPN fixed addresses

OpenVPN user

IP address

Site-to-Site VPN

☑ OpenVPN site-to-site active.

10.1.2.16
OpenVPN remote address

1195
OpenVPN site-to-site port

10.4.5.15
OpenVPN internal local address

10.4.5.16

Defines the fixed IP for the remote endpoint, which is only used inside the virtual transfer network.

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
4901e64b50953ec8f16388182746b7a0
fc9e723280e6fa1ddf8ecf1b4a794490
64e6980d7a6453ea693445403758097d
```

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.
  Deafult: 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.