

OpenVPN4UCS



Kurzanleitung zur Einrichtung

Inhaltsverzeichnis

i. Disclaimer.....	3
ii. WARNUNG zu Versionsunterschieden zwischen 1.1 und 2.0.....	4
1. Einleitung.....	5
2. Anforderungen.....	5
3. Szenario 1 – Zugang mobiler Nutzer und Heimarbeitsplätze.....	6
3.1 Serverkonfiguration.....	6
3.2 Benutzerkonfiguration.....	8
3.3 Clientkonfiguration.....	11
3.4 Verbindungsübersicht.....	14
4. Szenario 2 – Standortvernetzung.....	15
4.1 Serverkonfiguration.....	15
5. Migration – OpenVPN4UCS 1.1 zu OpenVPN4UCS 2.0.....	17
5.1 Versionsübersicht.....	18
5.1.1 Versionsmatrix 1 – VPN-Funktionalität.....	18
5.1.2 Versionsmatrix 2 – Verfügbarkeit der <i>ready2go</i> -Pakete.....	18
5.2 Upgrade- / Migrationsschritte.....	19
5.2.1 OpenVPN4UCS Update unter UCS 4.4 einspielen.....	19
5.2.2 Neue <i>ready2go</i> -Pakete verteilen.....	20
5.2.3 Upgrade auf UCS 5.0 durchführen.....	20
5.2.4 Upgrade auf OpenVPN4UCS 2.0.....	21

i. Disclaimer

OpenVPN ist ein komplexes Werkzeug. Mittels *OpenVPN* ist es möglich die verschiedensten Varianten von virtuellen privaten Netzen zu konfigurieren.

Das Integrationspaket *OpenVPN4UCS* konzentriert sich auf zwei typische Standardfälle: Sicherer Zugang von unterwegs und Heimarbeitsplätzen in das Firmennetzwerk, sowie die Anbindung einer Außenstelle. Dies bedeutet auch, dass das Integrationspaket kein grafisches Werkzeug für alle mit *OpenVPN* möglichen Konstellation darstellt.

OpenVPN4UCS steht ab Version 1.0 für bis zu fünf Benutzer als kostenlose Integration zur Verfügung. Größere Nutzergruppen, sowie die Standortvernetzung werden kostenpflichtig angeboten. Weitere Details hierzu finden Sie auf unserer Produktseite unter:

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

Für Verbesserungsvorschläge, weitere Ideen haben wir bei der bytemine GmbH stets ein offenes Ohr.

Des Weiteren bietet die bytemine GmbH auch weiterführende Dienstleistung und Beratung rund um den *Univention Corporate Server* und *OpenVPN* an.

Diese Kurzanleitung ersetzt kein Basiswissen im Bereich VPN und IT Sicherheit. Bei der Anwendung des wird ein Grundwissen im Bereich IT Sicherheit und Umgang mit Linux-basierten Servern vorausgesetzt.

Ende des Disclaimer

ii. WARNUNG zu Versionsunterschieden zwischen 1.1 und 2.0

OpenVPN4UCS ist in zwei miteinander **NICHT (!)** direkt kompatiblen Versionen verfügbar! Dies liegt an der geänderten Public Key Infrastruktur, welche von *OpenVPN4UCS* ab *UCS* 5.0 genutzt wird.

Dies hat zur Folge, dass ein einfaches Upgrade der Software über das *Univention App Center* nicht möglich ist und mittels manueller Eingriffe vorbereitet und begleitet werden muss!

Sollten Sie vorhaben von Version 1.1 auf Version 2.0 von *OpenVPN4UCS* zu wechseln, so beachten Sie bitte unbedingt die skizzierten Migrationsschritte am Ende dieser Kurzanleitung (vgl. Kapitel 5)!
Bei Missachtung droht Verbindungsverlust!

Lesen Sie daher dieses Dokument einmal vollständig durch. Sollten Sie den Eindruck haben (Teil-) Aspekte nicht zu verstehen bzw. nachvollziehen zu können, so kontaktieren Sie uns bitte **BEVOR** Sie mit einem Versionswechsel eigenständig beginnen!

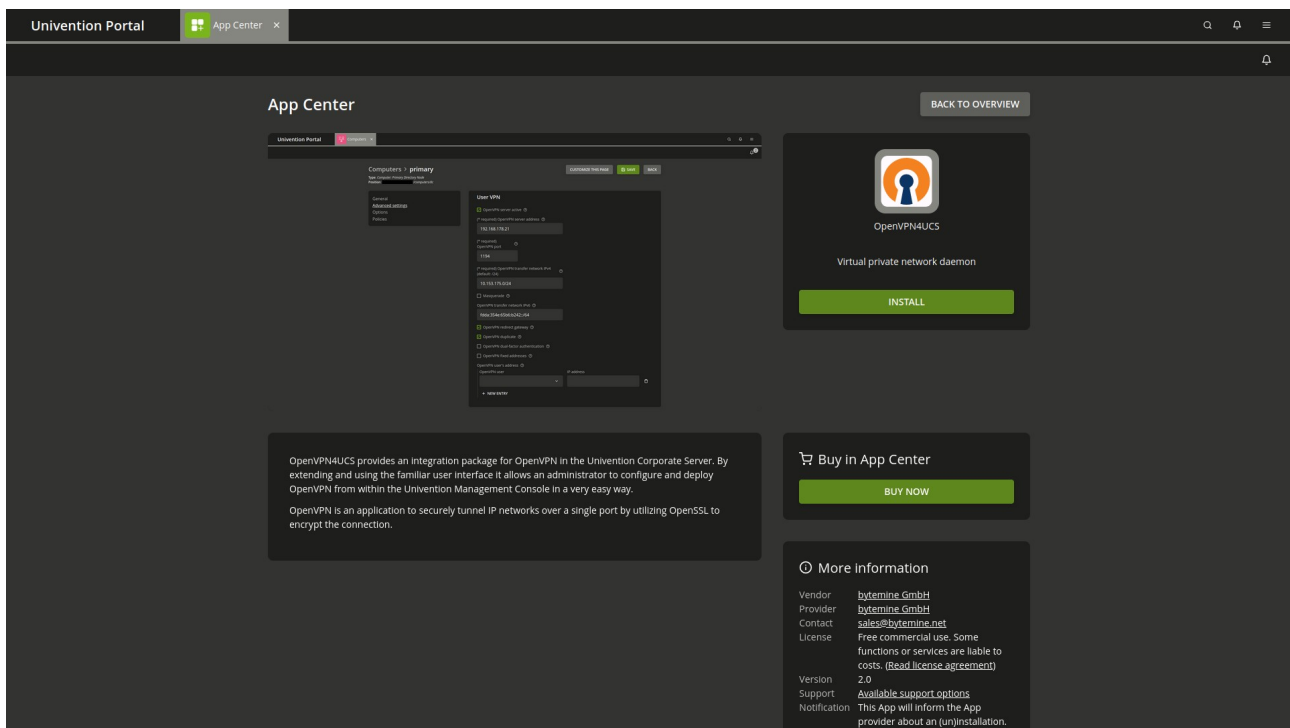
Soweit nicht explizit beschrieben sind die allgemeinen Handlungsanweisungen (also nicht die Migration betreffend) für beide Versionen identisch durchzuführen. Sollte es an einzelnen Stellen zu Abweichungen zwischen beiden Versionen kommen, so werden diese an den betreffenden Stellen ausgewiesen.

1. Einleitung

Auf den folgenden Seiten wird die Verwendung der *OpenVPN4UCS* Integration erklärt. An zwei typischen Szenarien wird die Funktionsweise und Einrichtung veranschaulicht.

2. Anforderungen

- *Univention Corporate Server ; UCS 4.4 (für Version 1.1) ; UCS 5.x (für Version 2.x)*
- Für die Verwendung von *TOTP* wird mindestens Version 2.1 benötigt.
- Zugang als *Administrator* zur *Univention Management Console (UMC)*
- *OpenVPN4UCS* installiert aus dem *Univention App Center*.



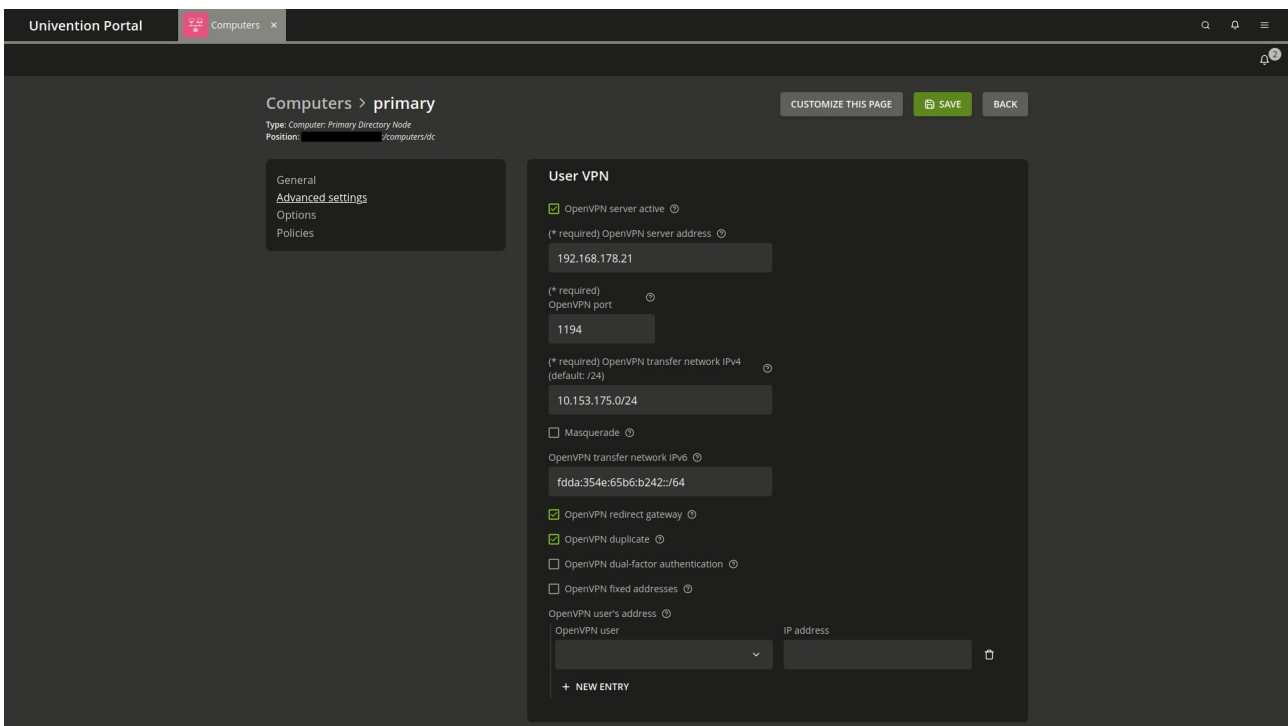
The screenshot displays the Univention App Center interface. At the top, there's a navigation bar with 'Univention Portal' and 'App Center'. The main content area features a 'BACK TO OVERVIEW' button, a search bar, and a list of applications. The 'OpenVPN4UCS' application is highlighted, showing its icon (a keyhole with a blue key) and the text 'OpenVPN4UCS Virtual private network daemon'. Below the application card, there's a green 'INSTALL' button. To the left, a preview window shows the configuration interface for OpenVPN4UCS, with fields for 'Server', 'Client', and 'User VPN'. Below the preview, there's a text box explaining that OpenVPN4UCS provides an integration package for OpenVPN in the Univention Corporate Server, allowing administrators to configure and deploy OpenVPN from within the Univention Management Console. To the right of the application card, there's a 'Buy in App Center' section with a green 'BUY NOW' button. At the bottom right, there's a 'More information' section with details about the vendor (bytemine GmbH), provider (bytemine GmbH), contact (sales@bytemine.net), license (Free commercial use), version (2.0), support (Available support options), and notification (This App will inform the App provider about an (un)installation).

3. Szenario 1 – Zugang mobiler Nutzer und Heimarbeitsplätze

Ein typisches Beispiel für die Verwendung eines VPN ist die Anbindung von Heimarbeitsplätzen und mobile Anbindung von Nutzern.

Durch die Bereitstellung eines *OpenVPN* Servers (auch VPN Konzentrator genannt) ist dies schnell erreicht.

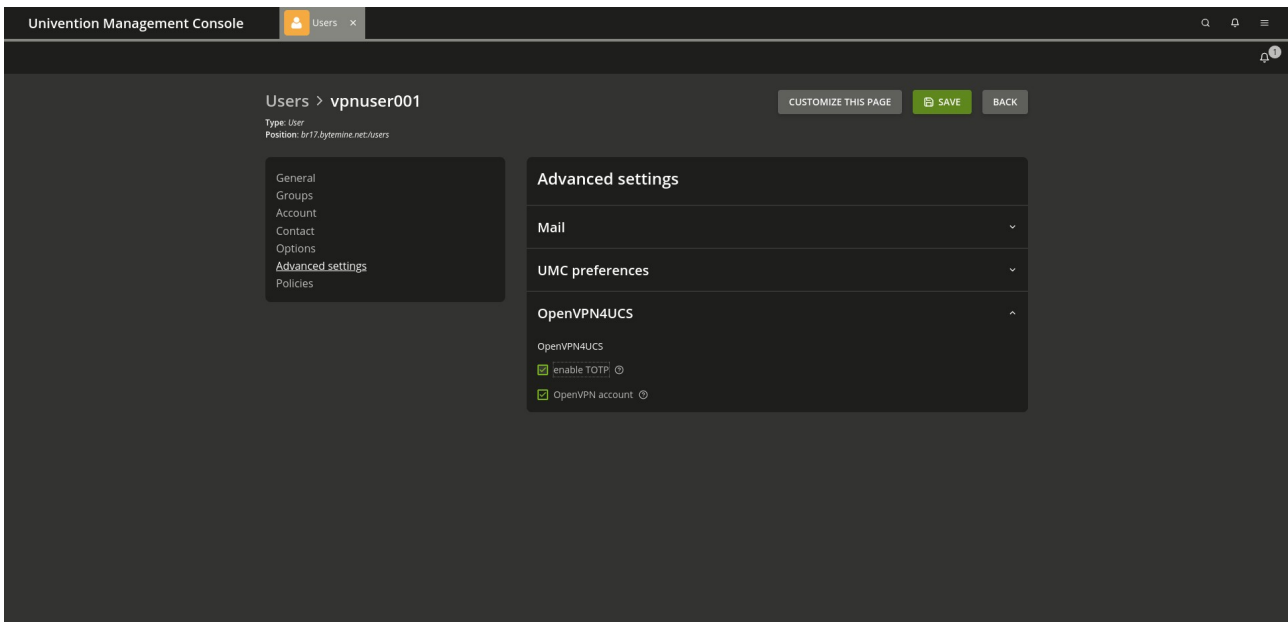
3.1 Serverkonfiguration



- In der *UMC* bei den Computerobjekten den Rechner öffnen, der als *OpenVPN* Server dienen soll.
- In den „Erweiterten Einstellungen“ des Rechnerobjektes den Punkt „*OpenVPN4UCS*“ aufklappen.

- Die Einstellungen entsprechend konfigurieren:
 - Der „*OpenVPN4UCS Lizenzschlüssel*“ muss nur eingetragen werden, wenn kommerzielle Features genutzt werden sollen.
Default: kein – Pflichtangabe: nein
 - „*OpenVPN Server aktiviert*“ stellt den *OpenVPN* Dienst auf dem gewünschten Rechner bereit.
Default: deaktiviert – Pflichtangabe: ja
 - Die „*OpenVPN Serveradresse*“ ist die IP an die die Clients verbinden. Je nach Infrastruktur kann dies ggf. auch ein Router sein.
Default: kein, bzw. 0.0.0.0 – Pflichtangabe: ja
 - Der „*OpenVPN Port*“ muss aus dem Internet erreichbar sein. Ab Version 1.0 wird dieser Port auch in der Firewall geöffnet.
Default: 1194 – Pflichtangabe: ja
 - Das „*OpenVPN Transfernetzwerk*“ ist das eigentliche VPN. Hier sollte sichergestellt werden, dass die Einstellungen nicht mit anderen Netzkonfigurationen kollidieren.
Default: 10.153.175.0/24 – Pflichtangabe: ja
 - Das „*OpenVPN Transfernetzwerk für IPv6*“ ist analog zu betrachten.
Default: 2001:db8:0:123::/64 – Pflichtangabe: nein
 - Wenn sich Benutzer mit Ihrem Zertifikat gleichzeitig mit mehreren Geräten einwählen können sollen, muss die Option „*OpenVPN Mehrfachverbindung*“ aktiv sein.
 - Damit der gesamte Internetverkehr des Benutzers über das VPN geleitet wird, muss die Option „*OpenVPN setzt sich beim Client als Standard-Gateway Umleitung*“ aktiviert werden.
 - „*Feste Adressen*“ ist zu verwenden, wenn einzelnen Benutzern statische IPs innerhalb des VPN zur Verfügung gestellt werden sollen. Die darunter liegende Dropdown-Liste zeigt Benutzer an, die als *OpenVPN*-Benutzer konfiguriert wurden. Hinweis: Eine multiple Einwahl eines einzelnen Benutzers ist nicht mehr möglich, wenn dieser auf eine Adresse fixiert ist.
- Speichern Sie die Einstellungen. Der *OpenVPN* Dienst wird in Kürze gestartet.

3.2 Benutzerkonfiguration



- In der UMC den Benutzer, der das VPN verwenden können soll, öffnen.
- In den „Erweiterten Einstellungen“ den „OpenVPN4UCS“ Bereich aufklappen.
- Wahlweise die Option „TOTP aktivieren“ aktivieren, sofern ein *time-based one-time password* als zweiter Faktor bei der Anmeldung des Benutzers am VPN genutzt werden soll (verfügbar ab Version 2.1).
- Die Option „OpenVPN Account“ aktivieren.

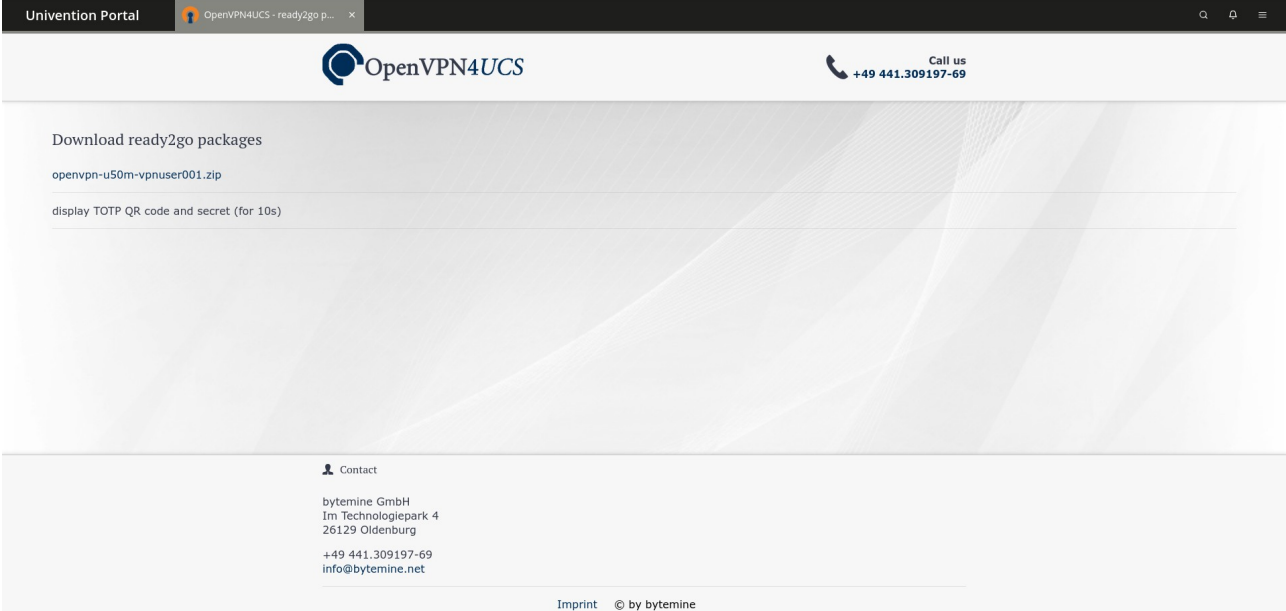
Hinweis: Für die Nutzung von *TOTP* wird ein *TOTP*-Client, der entweder QR-Codes lesen oder das *TOTP-Secret* durch direkte Eingabe verarbeiten kann, benötigt. Diese sind von verschiedenen Anbietern für unterschiedliche Systeme erhältlich, z.B. als Browsererweiterung oder App auf Mobiltelefonen.



- Zertifikate und Clientkonfiguration (aktuell für Windows und Linux Systeme) werden in den sogenannten *ready2go*-Paketen über eine Webseite zum Download bereitgestellt.

https://<server>/download/

- Die Seite ist über eine Kachel direkt im *UCS-Portal* verlinkt und kann von Benutzern einfach aufgerufen werden.
- Der Download ist mit dem Domänenpasswort des jeweiligen Benutzers abgesichert und so nur für diesen Benutzer verfügbar.



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

- Durch Klick auf die gelistete ZIP-Datei das *ready2go*-Paket herunterladen.
- Durch Klick auf „*display TOTP QR code and secret (for10s)*“ den QR-Code zur Generierung des *time-based one-time password* anzeigen (verfügbar ab Version 2.1).

Wird der Haken bei „*OpenVPN Account*“ wieder entfernt (siehe oben), wird dem Benutzer die Möglichkeit zur VPN Nutzung entzogen. Die Zertifikate sind nicht länger gültig.

Hinweis: Bereits bestehende Verbindungen werden hierdurch nicht beeinflusst. Wenn die Verbindung eines Benutzers unmittelbar getrennt werden soll, so muss die Verbindung zusätzlich manuell getrennt werden (sieh auch Abschnitt: Verbindungsübersicht).

Durch erneutes Aktivieren wird ein neues *ready2go*-Paket für den Benutzer erstellt. Die Zertifikate müssen beim Nutzer durch die neu erstellten Zertifikate ersetzt werden, da jeweils beim Deaktivieren der Option die Zertifikate gesperrt werden.

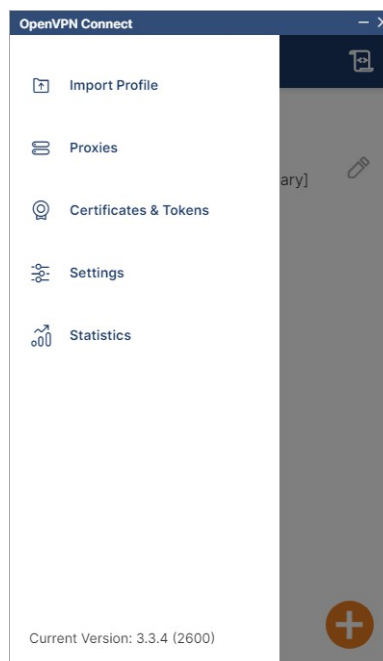
3.3 Clientkonfiguration

Da es *OpenVPN* für viele verschiedenen Plattformen gibt, beschränkt sich diese Anleitung auf ein Setup unter *Windows* mit dem offiziellen Client *OpenVPN Connect* (hier: Version 3.x ; vgl. <https://openvpn.net/vpn-client/>).

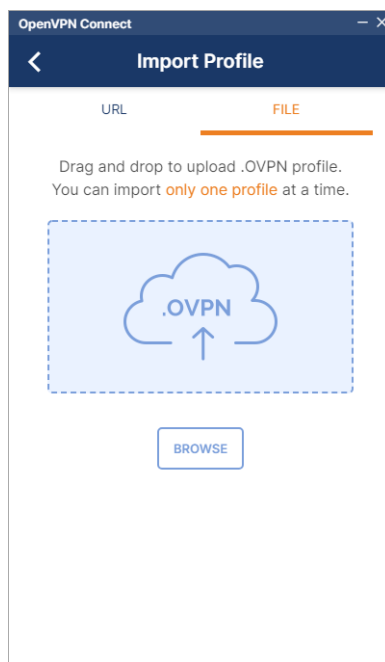
Hinweis: Nachfolgende Schritte gehen von der Verwendung von *OpenVPN4UCS 2.0* aus. In älteren Versionen liegen Konfigurationen, Schlüssel und Zertifikate getrennt und nicht in einer Datei im *ready2go*-Paket vor. Bei Verwendung älterer Versionen müsste die Zertifikate etc. entsprechend separat importiert werden.

Von der Annahme ausgehend, das *OpenVPN Connect* als Software auf dem Client bereits installiert ist:

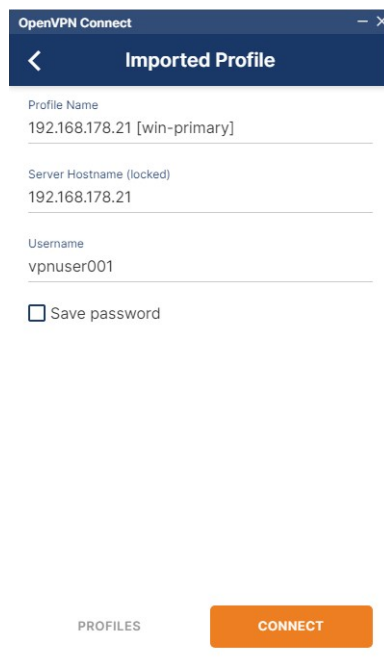
- Laden Sie das für den jeweiligen Benutzer bestimmte *ready2go*-Paket herunter und extrahieren sie die Inhalte in einen beliebigen Ordner auf dem Clientsystem.
- Starten Sie *OpenVPN Connect*, klicken auf das Hamburger-Menü und wählen *Import Profile*.



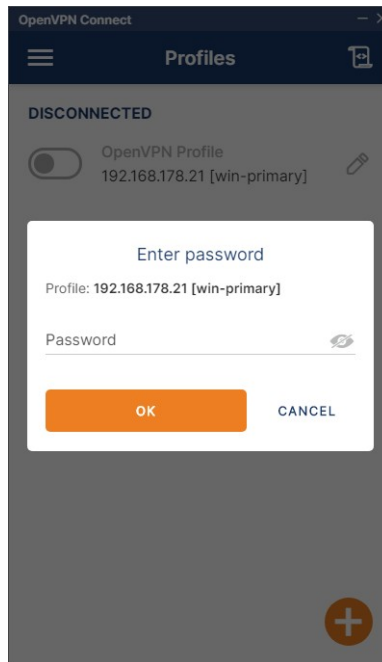
- Wählen Sie anschließend *File* und ziehen die Konfigurationsdatei (mit Präfix *win-* im Dateinamen) in das Drag'n'Drop-Feld oder klicken alternativ auf *Browse* und wählen die entsprechende Datei.



- Nachfolgend wird Ihnen ein Teil der Profildaten angezeigt. Ergänzen Sie den Domänenbenutzernamen. Optional können Sie den Profilnamen anpassen und ggf. das zu verwendende Passwort durch anhängen von *Save Password* speichern lassen. Anschließend klicken Sie auf *Connect*.

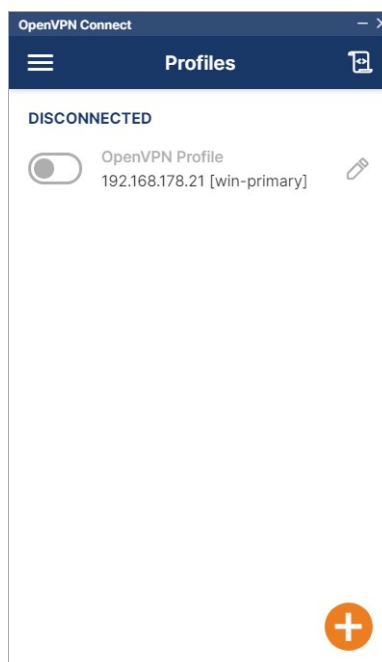


- Geben Sie wie gefordert das Passwort des Benutzers ein und klicken auf OK.

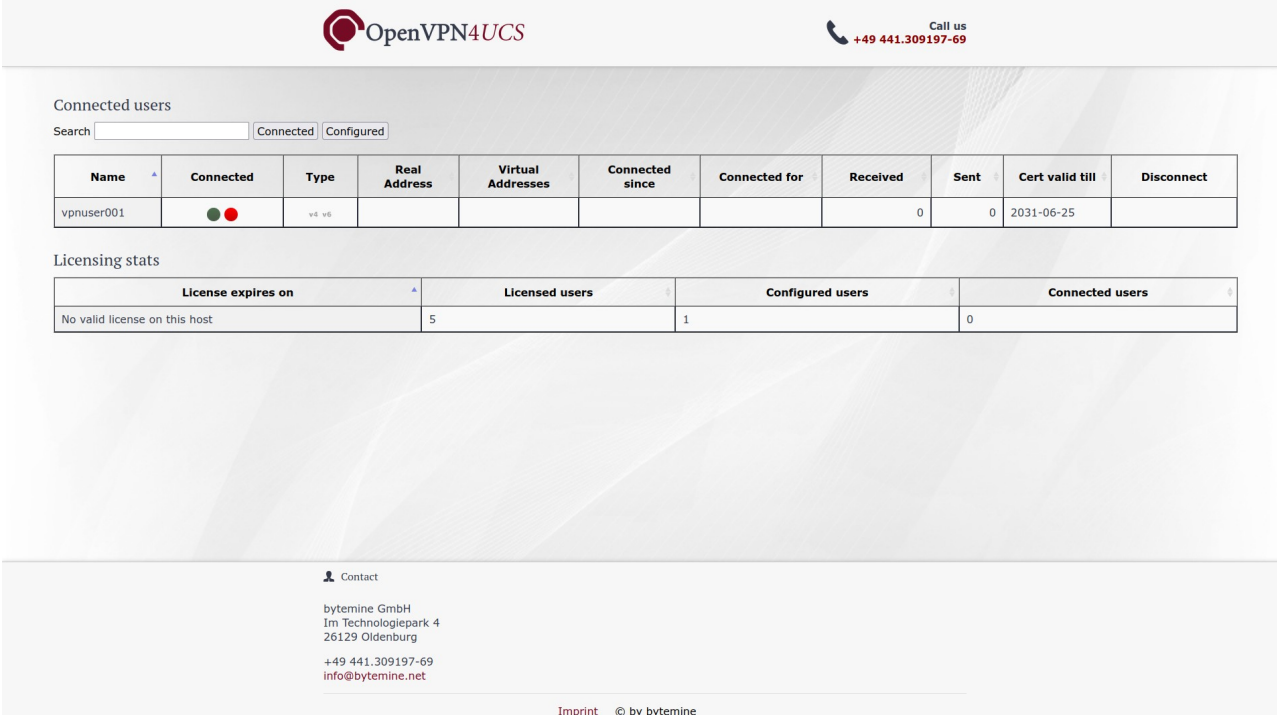


Hinweis: Wird *TOTP* als zweiter Faktor eingesetzt (siehe Abschnitt *Benutzerkonfiguration*), so wird zur Eingabe des zweiten Faktors zusätzlich separat aufgefordert.

- Die Verbindung wird aufgebaut. Das Profil steht zur weiteren Verwendung in *OpenVPN Connect* bereit. Die Nutzung des VPNs kann über den Schalter links neben dem Profilnamen ein- und ausgeschaltet werden.



3.4 Verbindungsübersicht



The screenshot shows the OpenVPN4UCS web interface. At the top, there is a header with the OpenVPN4UCS logo and a 'Call us +49 441.309197-69' button. Below the header, the 'Connected users' section is visible, featuring a search bar and two tabs: 'Connected' (selected) and 'Configured'. A table lists the connected users with columns for Name, Connected status, Type, Real Address, Virtual Addresses, Connected since, Connected for, Received, Sent, Cert valid till, and Disconnect. One user, 'vpnuser001', is listed as connected. Below this, the 'Licensing stats' section shows a table with columns for License expires on, Licensed users, Configured users, and Connected users. The stats indicate 'No valid license on this host', 5 licensed users, 1 configured user, and 0 connected users. At the bottom, there is a 'Contact' section with the company name, address, phone number, and email. The footer contains 'Imprint © by bytemine'.

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	

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

OpenVPN4UCS stellt eine Verbindungsübersicht aller verbundenen Benutzer zur Verfügung. Es ist auch möglich Verbindungen über die Übersicht zu unterbrechen.

Hinweis: Typischerweise versuchen VPN-Clients eine unterbrochene Verbindung von alleine wieder aufzubauen. Wenn es das Ziel ist die Verbindung eines Benutzers dauerhaft zu verhindern, so muss zunächst das Zugriffsrecht entzogen werden (vergleiche Abschnitt: Benutzer Konfiguration).

Die Verbindungsübersicht steht über das *UCS-Portal* als Link zur Verfügung oder kann direkt aufgerufen werden:

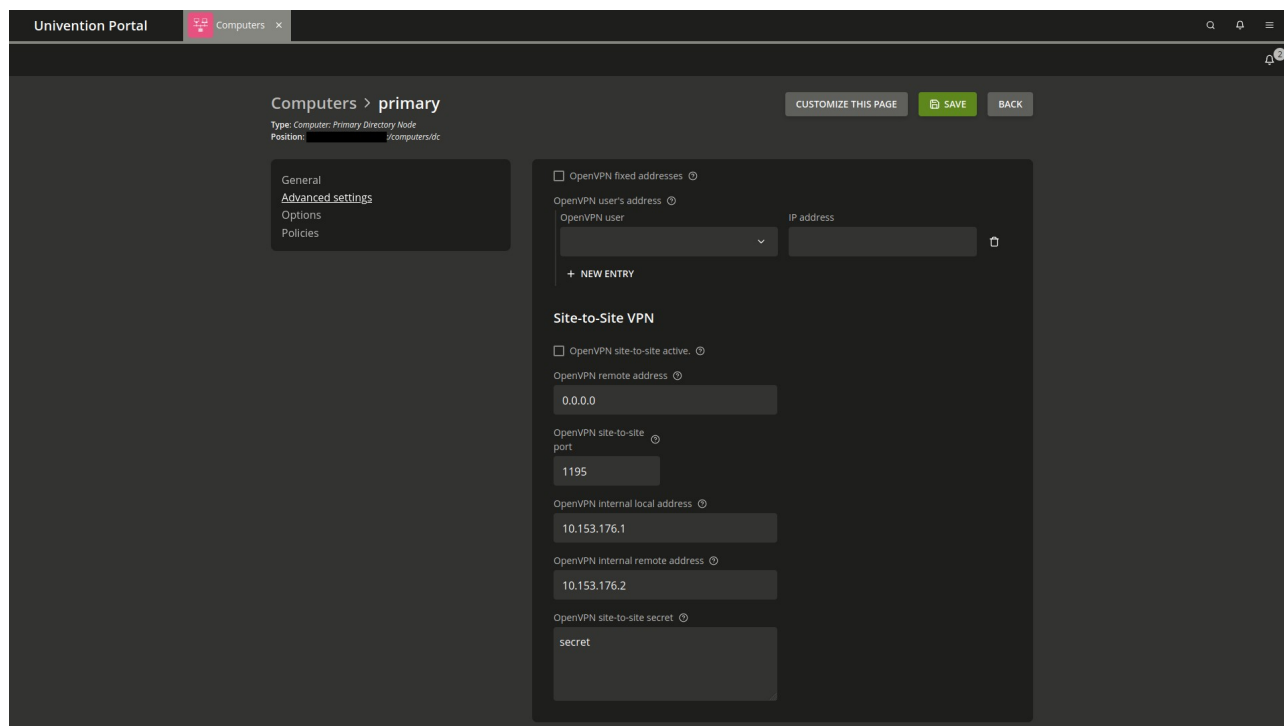
`https://<server>/display_users/`

Der Zugriff ist passwortgeschützt und steht nur dem Administrator zur Verfügung.

4. Szenario 2 – Standortvernetzung

Das zweite Szenario ist die Verbindung von zwei Standorten – auch *Site-to-Site* genannt, beispielsweise einer Firmenzentrale mit einer Außenstelle. Diese Funktion steht erst nach Einspielen eines Lizenzschlüssels (vgl. Szenario 1 – Server Konfiguration) zur Verfügung. Einen gültigen Lizenzschlüssel können Sie bei uns beziehen.

4.1 Serverkonfiguration



Damit die Standortvernetzung genutzt werden kann, ist die grundlegende Serverkonfiguration erforderlich (vgl. Szenario 1).

Es sind weiterhin folgende Optionen entsprechend zu konfigurieren, wenn diese Funktion genutzt werden soll:

- „*OpenVPN Site-to-Site aktiviert*“ stellt die Standortvernetzung bereit.
Default: deaktiviert – Pflichtangabe: ja
- „*Adresse der OpenVPN Gegenstelle*“ ist die IP Adresse eines weiteren Rechners, mit dem eine VPN Verbindung aufgebaut werden soll.
Default: kein, bzw. 0.0.0.0 – Pflichtangabe: ja
„*OpenVPN Site-to-Site Port*“ definiert den Port, über den das VPN aufgebaut wird. Ab Version 1.0 wird die Firewall entsprechend geöffnet.
Default: 1195 – Pflichtangabe: ja
- „*OpenVPN interne lokale Adresse*“ beschreibt die IP Adresse des Rechners innerhalb des VPN. Die Adresse sollte so gewählt werden, dass sie nicht mit einem anderen bestehenden Netz kollidiert.
Default: 10.153.176.1 – Pflichtangabe: ja
- „*Interne Adresse der OpenVPN Gegenstelle*“ ist analog die IP Adresse der zweiten Rechners innerhalb des VPN.
Default: 10.153.176.2 – Pflichtangabe: nein
- „*Geheimnis für Site-to-Site-VPNs*“ ist der Schlüssel für das VPN. Dieser wird bei jeder Installation dynamisch generiert und ist somit bei keiner Installation gleich. Der Schlüssel muss beim zweiten Rechner manuell hinzugefügt werden.
Default: dynamisch – Pflichtangabe: ja

Sofern es sich bei dem zweiten Rechner, mit dem die Standortvernetzung aufgebaut werden soll, ebenfalls um ein UCS System aus der selben Domäne handelt, so kann dieser ebenfalls über die UMC konfiguriert werden.

5. Migration – OpenVPN4UCS 1.1 zu OpenVPN4UCS 2.0

Hinweis: Dieses Kapitel ist für Anwender, die eine Erstinstallation von *OpenVPN4UCS 2.0* unter *UCS 5.x* vornehmen nicht von Bedeutung.

Hintergrund: *OpenVPN4UCS* nutzte in *UCS 4.4* eine Funktion des *Univention App Centers (DefaultPackagesMaster)*, welches es erlaubte bei Installationen weitere Pakete auf dem Primary DC (Master) zu installieren. Diese Funktion gilt als veraltet und steht in *UCS 5.0* nicht mehr zur Verfügung, so dass Teile von *OpenVPN4UCS* komplett neu geschrieben werden mussten und eine neue Produktvariante entstand, die ihre eigene Public Key Infrastruktur mitliefert.

Dies hat zunächst folgende Konsequenzen:

1. Ein Upgrade bedeutet in diesem Fall einen Wechsel (Migration) von einer Produktvariante (*OpenVPN4UCS 1.1*) auf eine andere (*OpenVPN4UCS 2.0*).
2. Benutzerkonfigurationen und -zertifikate (*ready2go*-Pakete), welche mit *OpenVPN4UCS 1.1* erstellt wurden, können nicht in *OpenVPN4UCS 2.0* weiter genutzt werden.

Um diese Probleme so gut es geht zu adressieren wurde *OpenVPN4UCS 1.1.21* bereitgestellt. Sie dient als Brücke für eine Migration hin zu *OpenVPN4UCS 2.0*.

5.1 Versionsübersicht

Hinweis: Version 1.1.21 auf UCS 5.0 hat keinen eigenen Installationskandidaten. Es besteht lediglich auf UCS 5.0 Systemen, da es zuvor unter UCS 4.4 installiert wurde. Unter UCS 5.0 gibt es nur einen Installationskandidaten, welcher *OpenVPN4UCS* 2.0 ist.

5.1.1 Versionsmatrix 1 – VPN-Funktionalität

<i>OpenVPN4UCS</i> Version auf UCS Version	Altes VPN funktional	Altes VPN konfigurierbar	Neues VPN funktional	Neues VPN konfigurierbar
<= 1.1.19 auf 4.4	ja	ja	nein	nein
1.1.21 auf 4.4	ja	ja	nein	nein
1.1.21 auf 5.0	ja	nein	nein	nein
>= 2.0 auf 5.0	nein	nein	ja	ja

Versionsmatrix 1 zeigt welche Funktionalitäten innerhalb der einzelnen Versionen (und somit während der Migrationsschritte) zur Verfügung stehen.

5.1.2 Versionsmatrix 2 – Verfügbarkeit der *ready2go*-Pakete

<i>OpenVPN4UCS</i> Version auf UCS Version	Alte <i>ready2go</i> - Pakete verfügbar	Alte <i>ready2go</i> - Pakete Download	Neues <i>ready2go</i> - Pakete verfügbar	Neues <i>ready2go</i> - Pakete Download
<= 1.1.19 auf 4.4	ja	Primary DC	nein	Primary DC
1.1.21 auf 4.4	ja	Primary DC	ja	OpenVPN-Server
1.1.21 auf 5.0	ja	Primary DC	ja	OpenVPN-Server
>= 2.0 auf 5.0	nein	OpenVPN-Server	ja	OpenVPN-Server

Versionsmatrix 2 zeigt, wo die *ready2go*-Pakete heruntergeladen werden können. In Version 1.1 war dies stets am Primary DC (Master) der Fall. Mit Version 2.0 ist dies der Server auf dem *OpenVPN4UCS* installiert wurde – dies kann ggf. auch ein Primary DC (Master) sein.

5.2 Upgrade- / Migrationsschritte

Nachfolgend wird ein Migrationspfad beschrieben, welcher es ermöglicht einen Wechsel auf *OpenVPN4UCS* 2.0 und ein Upgrade auf den *Univention Corporate Server* Version 5.0 zu vollziehen.

Hinweis: Während der Migration ist es zu keinem Zeitpunkt erforderlich die Konfigurationen von *OpenVPN4UCS* Servern und/oder Benutzern über die *UMC* anzupassen!

Empfehlung: Führen Sie die Schritte vollständig in einer Testumgebung durch, bevor Sie die Schritte in einer produktiven Umgebung anwenden.

Empfehlung: Sollten Sie Hilfe benötigen und/oder Dienstleistung in Anspruch nehmen wollen, so kontaktieren Sie uns.

5.2.1 *OpenVPN4UCS* Update unter UCS 4.4 einspielen

Aktualisieren Sie *OpenVPN4UCS* auf Version 1.1.21. Diese Version bringt neben dem regulären Funktionsumfang zusätzlich Teile der Public Key Infrastruktur, wie sie auch in *OpenVPN4UCS* 2.0 unter UCS 5.0 im Einsatz ist, mit.

Nach der Installation wird automatisch je ein zweites *ready2go*-Paket mit der neuen Public Key Infrastruktur generiert und ebenfalls über die im *UCS-Portal* verlinkte Downloadseite bereitgestellt:

https://<server>/download/

Hinweis: Zur Unterscheidung der beiden *ready2go*-Pakete ist die Namensgebung der Downloads wie folgt abweichend strukturiert:

Version < 1.1.21, mit alter PKI: *openvpn-<servername>-<username>.zip*

Version = 1.1.21, mit neuer PKI: **npki/***openvpn-<servername>-<username>.zip*

Auf dem Server liegen die neuen *ready2go*-Pakete unterhalb der bisherigen Pakete im Verzeichnis:

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

anstelle von

/var/www/readytogo/<username>/

Hinweis: Diese Abweichung ist ausschließlich mit Version 1.1.21 gegeben! Später mit *OpenVPN4UCS* 2.0 erstellte Pakete nutzen erneut die alten Namensgebung und Pfade.

Fallunterscheidung:

- a) Wurde *OpenVPN4UCS* auf dem Primary DC (Master) installiert, so werden die neuen *ready2go*-Pakete zusammen mit den alten *ready2go*-Paketen über dasselbe Downloadportal bereitgestellt.
- b) Wurde *OpenVPN4UCS* auf einer anderen Serverrolle installiert, so wird der Download der neuen *ready2go*-Pakete auf eben jenem Server angeboten. Im *UCS-Portal* ist eine weitere Kachel hinzugefügt (*new ready2go packages*), welche auf das entsprechende System zeigt. Auf dem Primary DC (Master) stehen weiterhin die alten *ready2go*-Pakete im alten Downloadportal bereit.

Sollten vor Durchführung der nachfolgenden Schritten weitere Benutzer mit einem VPN-Zugang versorgt werden, so wird auch für diese das zweite *ready2go*-Paket bereitgestellt.

5.2.2 Neue *ready2go*-Pakete verteilen

Versorgen Sie VPN-Nutzer mit den neuen *ready2go*-Paketen und weisen Sie diese an ihre VPN-Clients **NOCH NICHT** auf die Nutzung der neuen *ready2go*-Pakete umzustellen.

Definieren Sie einen Zeitpunkt, wann ein Upgrade auf *UCS 5.0* mit Wechsel auf *OpenVPN4UCS 2.0* stattfinden soll und informieren Sie Ihre Nutzer, dass ab diesem Zeitpunkt auf die neuen *ready2go*-Paketen umgestellt werden muss.

Hinweis: Die neuen *ready2go*-Pakete enthalten all-in-one Konfigurationen für die Clients (vgl. Kapitel 3.3). Diese bestehen jeweils aus einer Datei, die alle benötigten Einstellungen, Zertifikate und Schlüssel in sich vereint. In *OpenVPN4UCS 1.1* wurden diese Komponenten separiert in den *ready2go*-Paketen ausgeliefert.

5.2.3 Upgrade auf *UCS 5.0* durchführen

!WARNUNG! Ein unter *UCS 4.4* erstelltes VPN und die dafür erstellten *ready2go*-Pakete können unter *UCS 5.0* noch genutzt werden. **Das VPN kann jedoch nicht mehr über die UMC konfiguriert werden!**

Hinweis: Dieser Schritt sollte möglichst erst dann durchgeführt werden, wenn Sie auch die nachfolgenden Schritte im direkten Anschluss erledigen können. Dies wiederum setzt voraus, dass VPN-Nutzer mit den neuen *ready2go*-Pakete versorgt wurden.

Führen Sie ein Upgrade auf *UCS 5.0* durch.

5.2.4 Upgrade auf *OpenVPN4UCS* 2.0

Hinweis: Dieser Schritt sollte möglichst unmittelbar nach einem Upgrade auf *UCS* 5.0 durchgeführt werden.

Fallunterscheidung:

a) Wurde *OpenVPN4UCS* auf einem Primary DC (Master) installiert, so kann ein Upgrade auf Version 2.0 unmittelbar im Anschluss an das Upgrade auf *UCS* 5.0 erfolgen.

b) Wurde *OpenVPN4UCS* auf einer anderen Serverrolle installiert, so sollte auf dem Primary DC (Master) das Skript

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

DIREKT VOR dem Upgrade ausgeführt werden. Dieses entfernt die verbliebenen Pakete von *OpenVPN4UCS* 1.1. Erst im Anschluss kann ein Upgrade auf *OpenVPN4UCS* erfolgen.

Führen Sie das Upgrade auf *OpenVPN4UCS* 2.0 je nach Fall durch.

Hinweis: Ab diesem Zeitpunkt sind nur noch die neuen *ready2go*-Pakete funktional.

Hinweis: Ab diesem Zeitpunkt werden die alten *ready2go*-Pakete nicht länger auf dem Primary DC (Master) zum Download angeboten.

Hinweis: Die alten *ready2go*-Pakete werden nicht länger benötigt und sollten zeitnah manuell entfernt werden. Sie liegen im Verzeichnis:

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

Beachten Sie hierbei die Hinweise in Abschnitt 5.2.1! Sollte *OpenVPN4UCS* auf einem Primary DC (Master) installiert worden und vor dem Löschen bereits neue *ready2go*-Pakete erstellt worden seien, so kann es hilfreich sein sich an den Zeitstempeln der Dateien oder deren Inhalt zu orientieren. Enthalten die zip-Dateien lediglich zwei Dateien, so wurde der Inhalt mit der neuen Public Key Infrastruktur erstellt.