yubico

Trust the Net

Firewall Integration Guide

Yubikey's mit privacyIDEA

Contents

1. Vorbereitung privacyIDEA

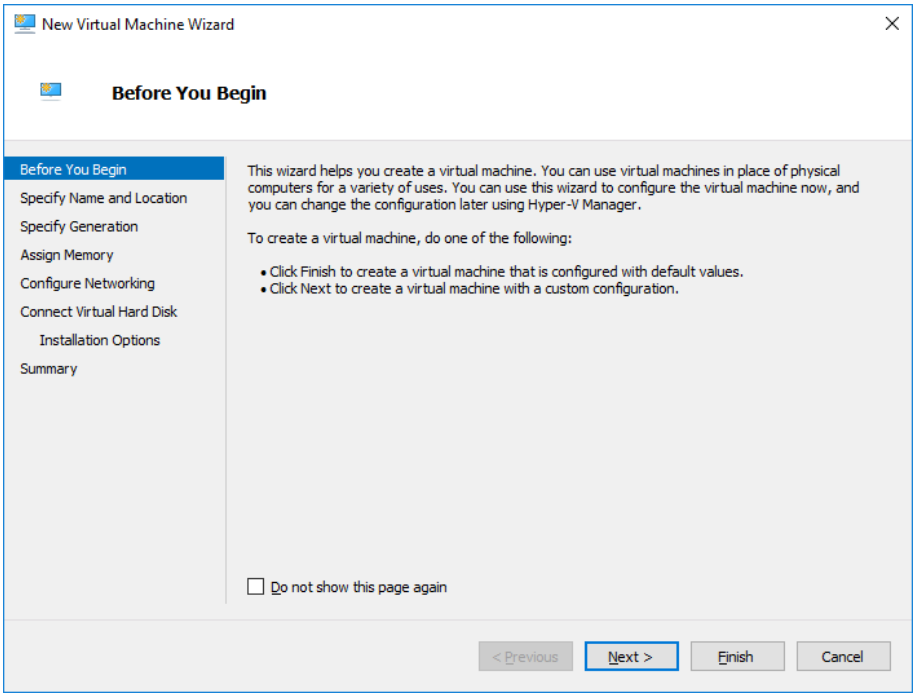
Um eine 2 Faktor Authentifizierung, an den in diesem Guide vorgestellten Sicherheitslösungen, zu realisieren, ist in den meisten Fällen eine Anbindung via Radius erforderlich. Yubico bietet ein Open Source Plugin für FreeRadius an, jedoch empfehlen wir in professionellen Umgebungen, eine einfacher verwaltbare und skalierbare Lösung die mehrere Authentifizierungsprotokolle neben Radius unterstützt. In diesem Guide verwenden wir das Authentifizierungs Backend privacyIDEA welche ebenfalls als Open Source verfügbar ist. Für weitere Informationen zu privacyIDEA empfehlen wir https://www.privacyIDEA.org

Als Betriebssystem für privacyIDEA verwenden wir einen Ubuntu Server in Version 16.04 LTS (http://releases.ubuntu.com/16.04/ubuntu-16.04.4-server-amd64.iso)

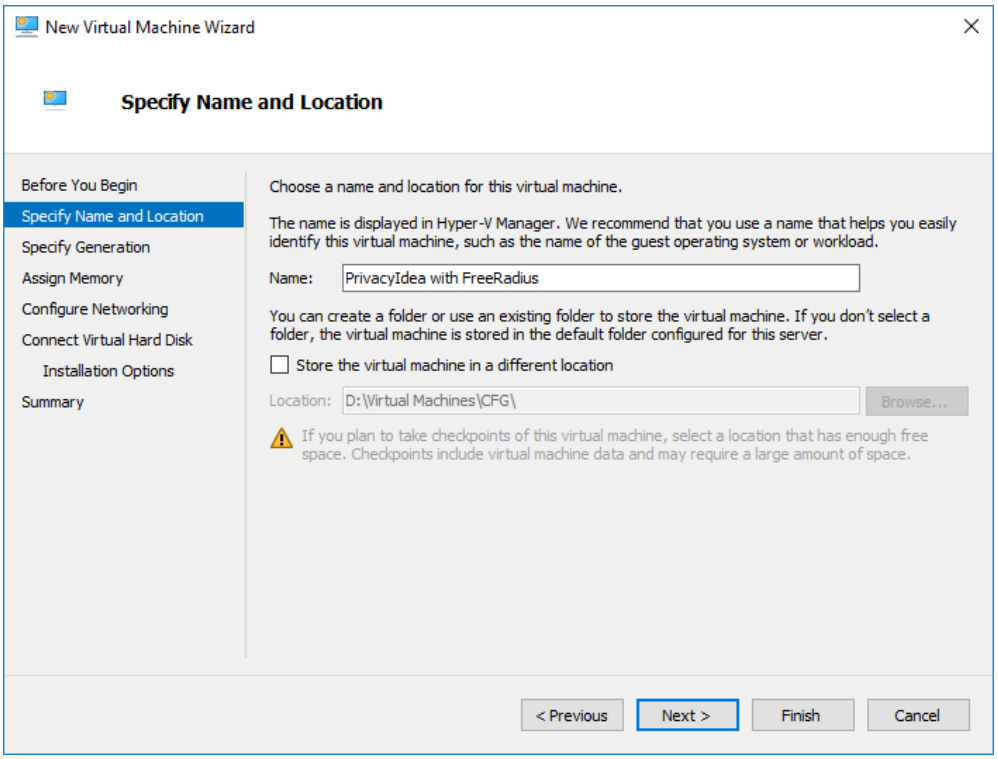
1.1. Erstellen einer virtuellen Maschine auf Microsoft Hyper-V

Als Platform verwenden wir Microsoft Hyper-V 2016, Sie können jedoch auch einen physikalischen Server oder eine andere Virtualisierungsplatform verwenden.

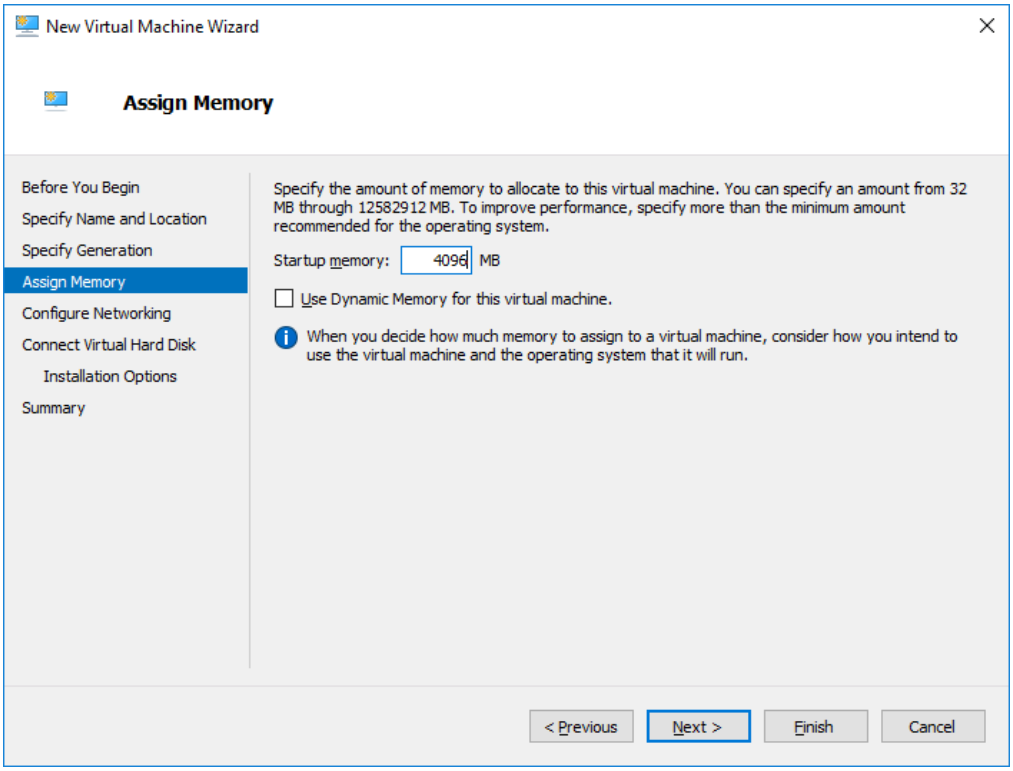
Erstellen Sie nun eine neue Maschine in Microsoft Hyper-V



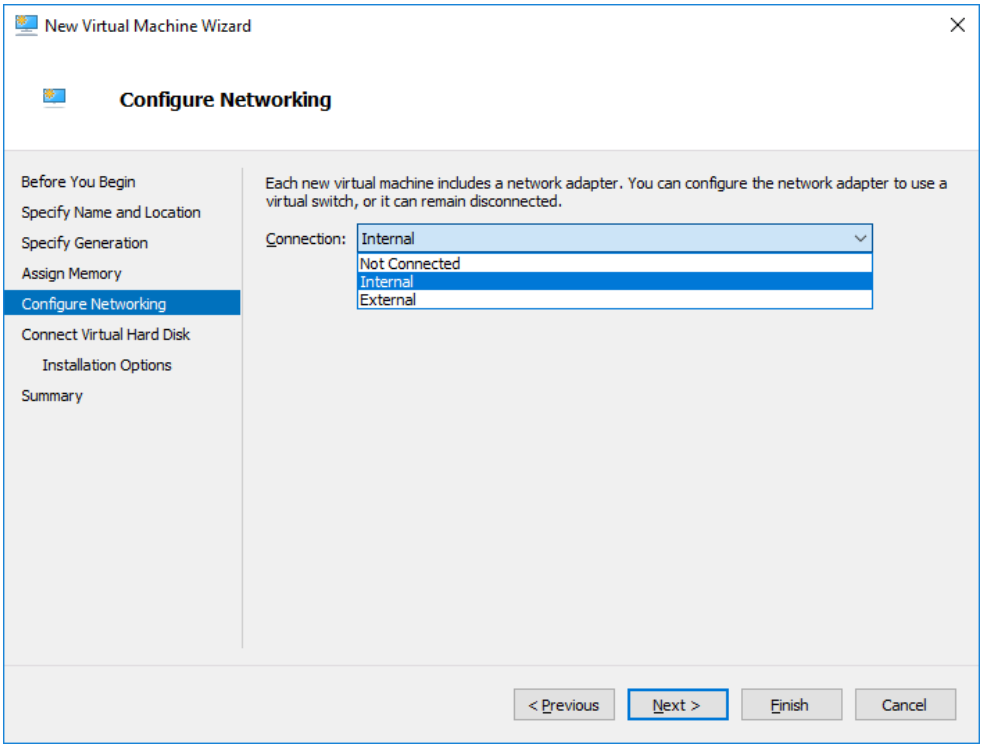
Vergeben Sie einen Namen und den Speicherort der virtuellen Maschine



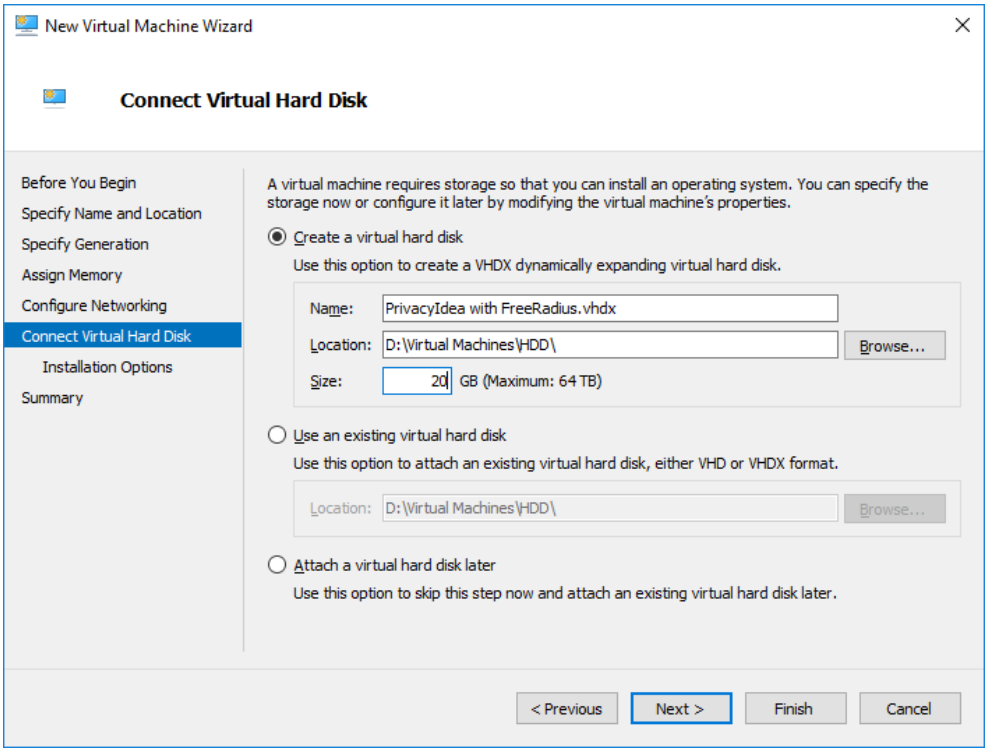
privacyIDEA ist in den meisten Szenarien sehr ressourcenschonend, jedoch empfehlen wir für einen reibungslosen und schnell Betrieb mindestens 4GB Arbeitspeicher



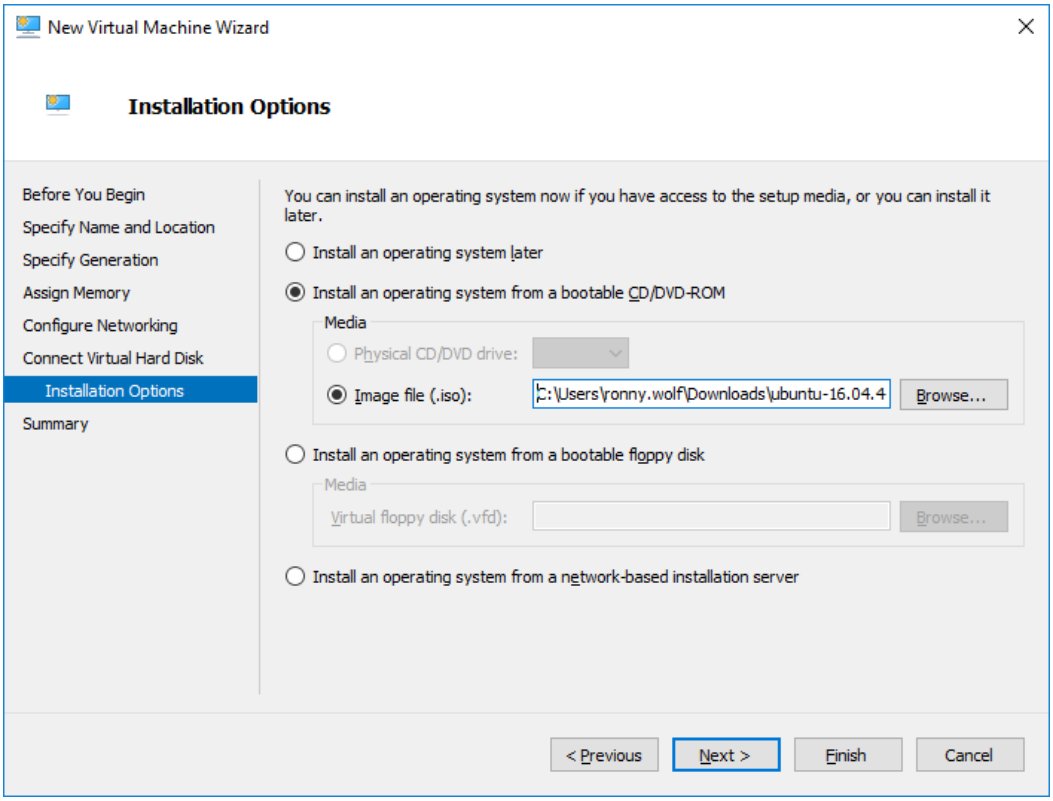
Fügen Sie eine (1) Netzwerkkarte hinzu und verbinden Sie diese mit dem virtuelle Switch für das interne Netzwerk, so dass die Firewalls diesen Server erreichen können.



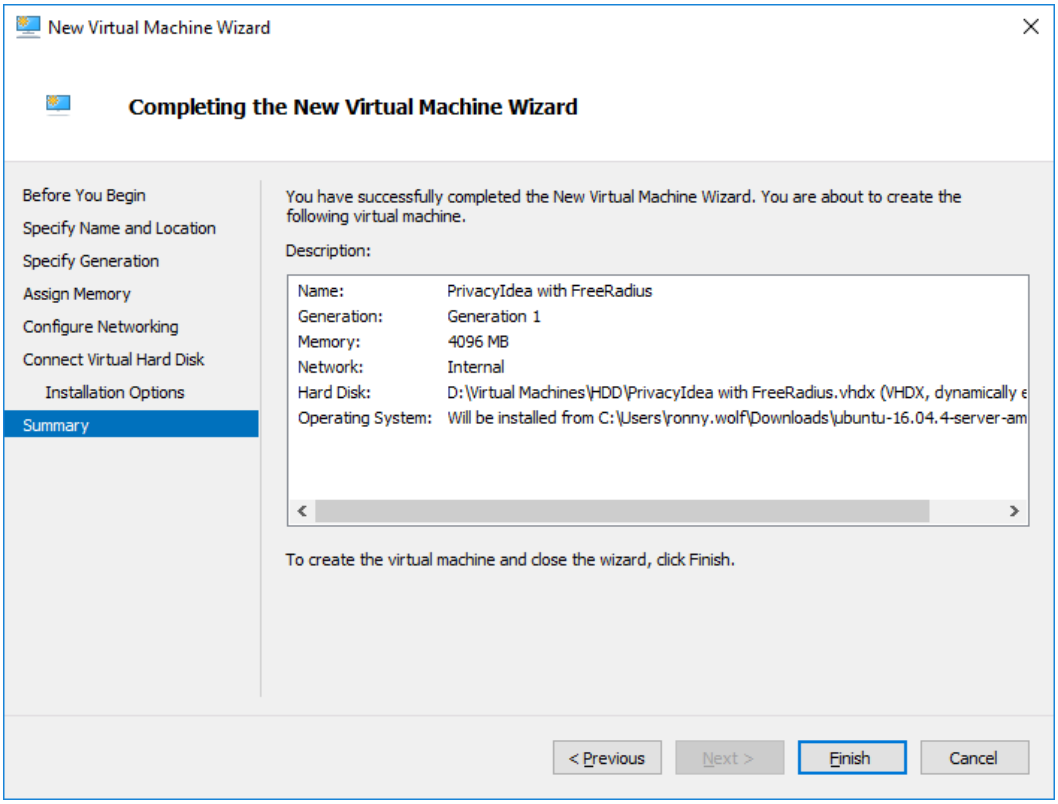
Wir vergeben eine virtuelle Festplatte mit 20GB Speicherkapazität. Sollten Sie eine Langzeitaufbewahrung für Berichte und Protokolle anstreben, empfiehlt sich eventuell mehr Speicherplatz zu vergeben.



Wählen Sie nun das ISO Image des Ubuntu Server 16.04 LTS, welches Sie zuvor heruntergeladen haben, aus (http://releases.ubuntu.com/16.04/ubuntu-16.04.4-server-amd64.iso)

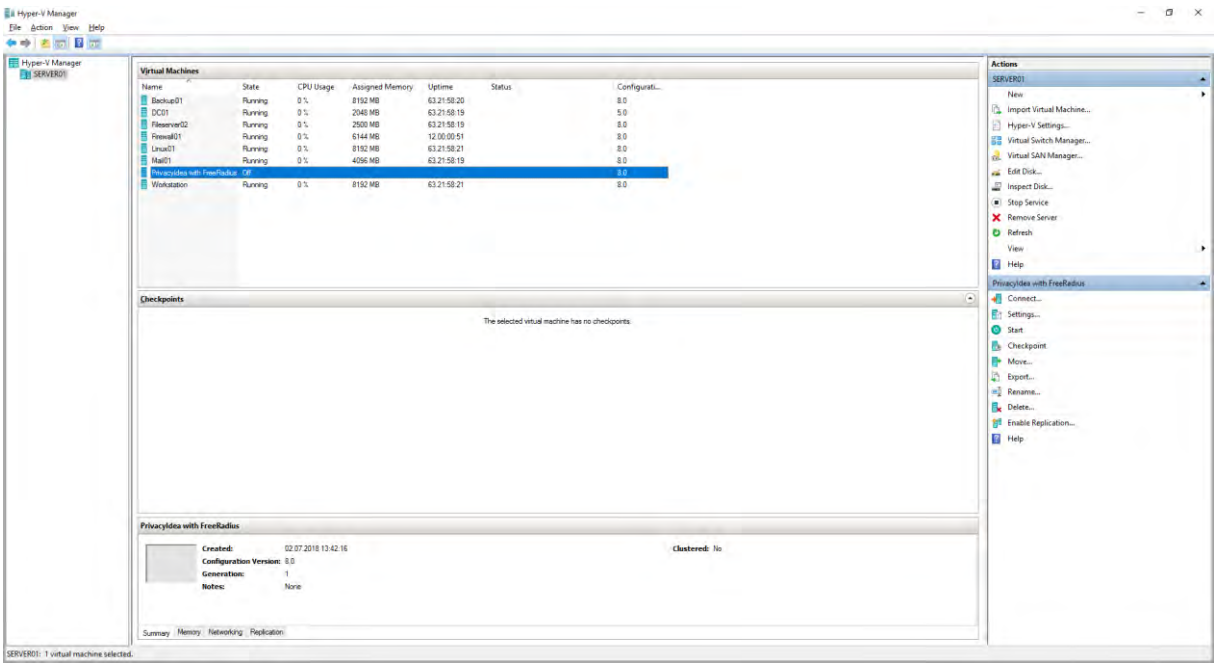


Nun sind die EInstellungen der virtuellen Maschine vollständig und Sie können mit dem Abschliessen des Assistenten die virtuellle Maschine erstellen.



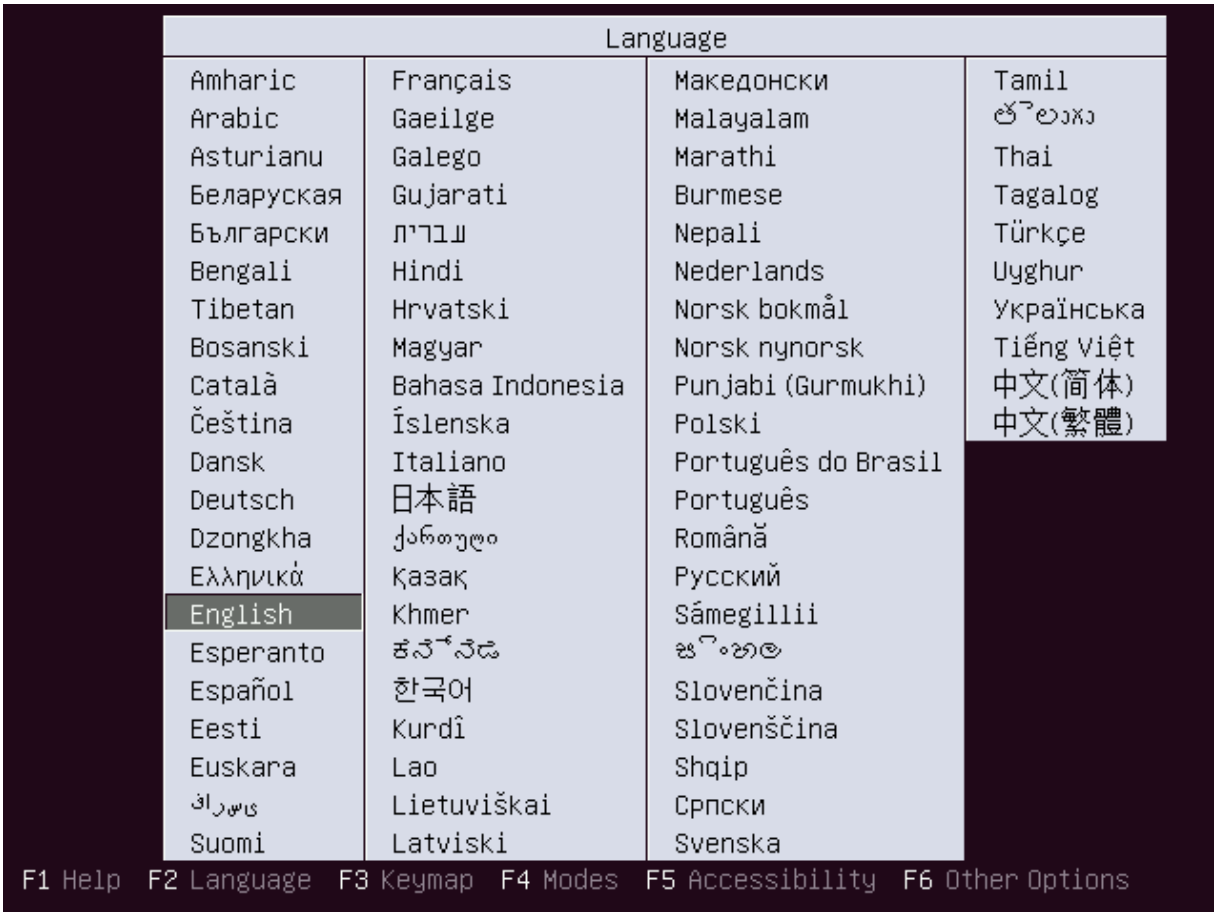
1.2. Installation von Ubuntu Server 16.04 (LTS)

Starten Sie nun die virtuelle Maschine über den Microsoft Hyper-V Manager.

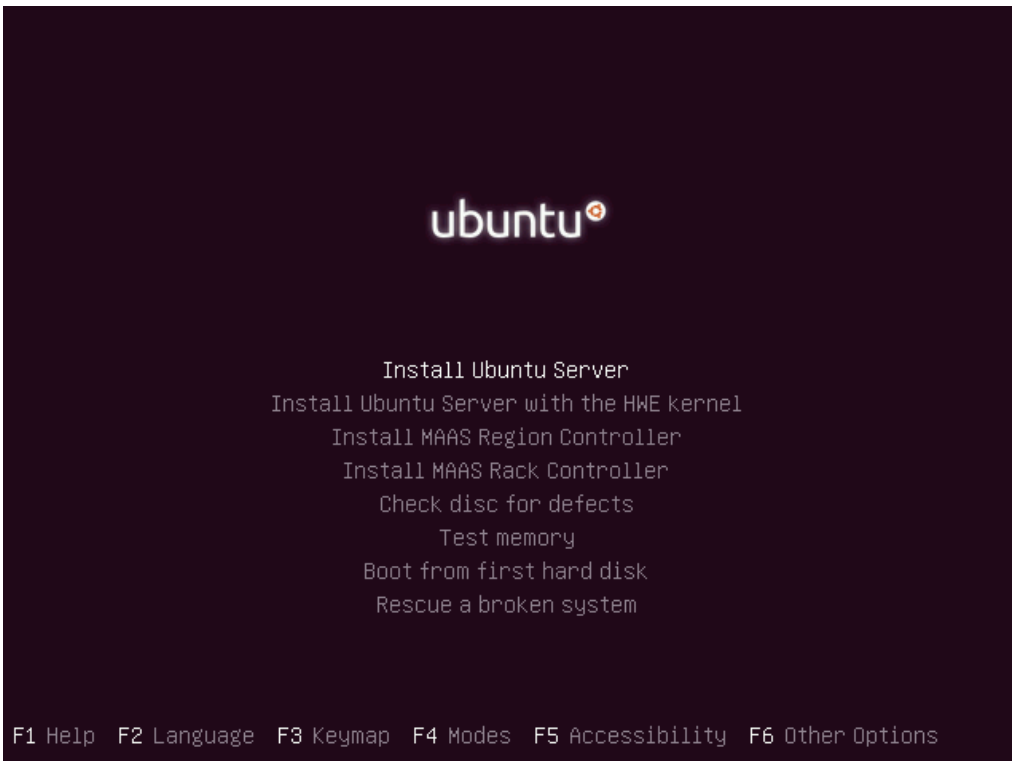


Die virtuelle Maschine starten nun vom verbunden Ubuntu Server ISO.

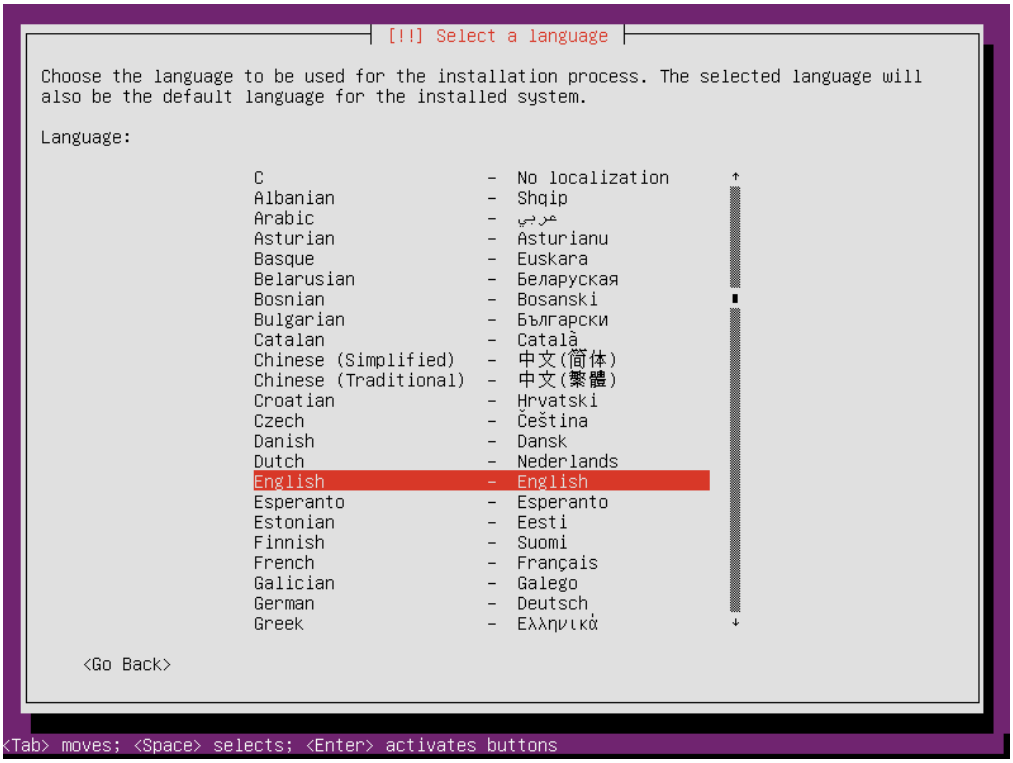
Wählen Sie als erstes die Sprache aus.



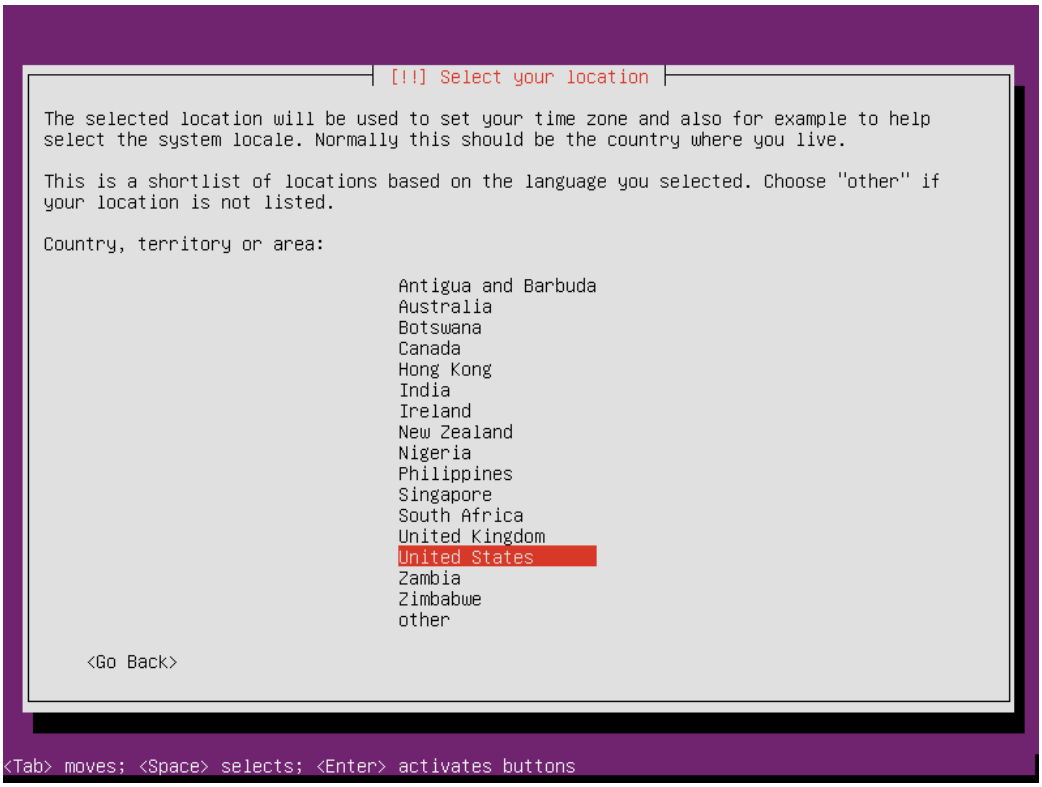
Und starten Sie die Installationsroutine



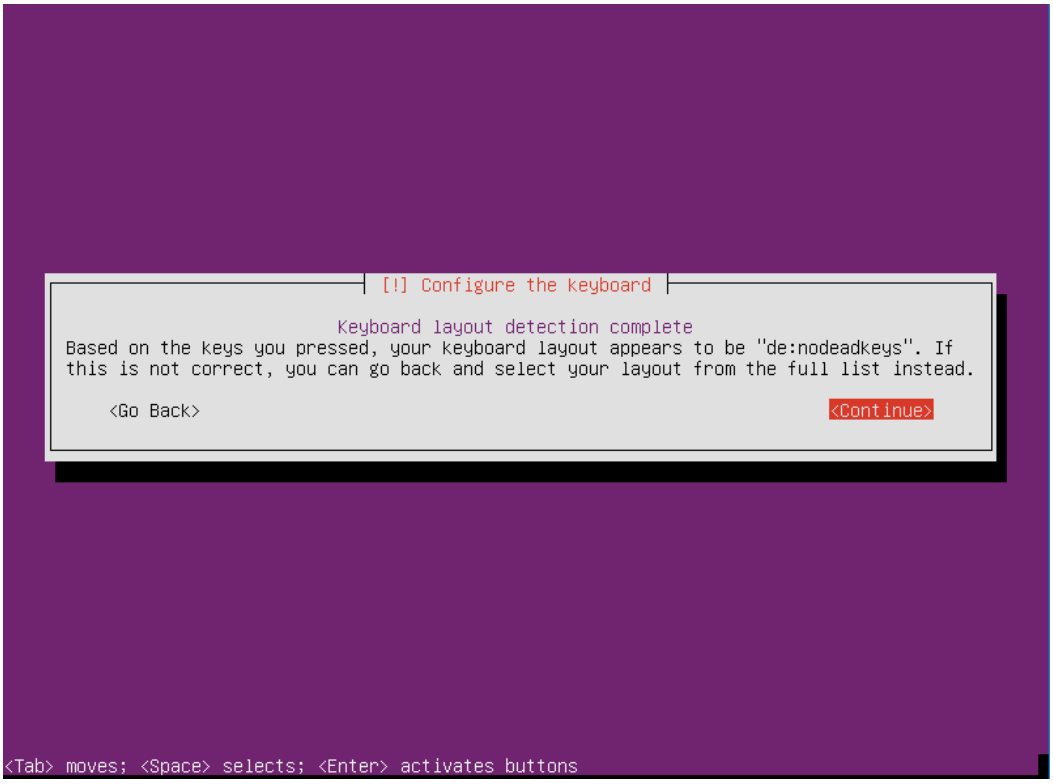
Wählen Sie nochmals die Sprache aus



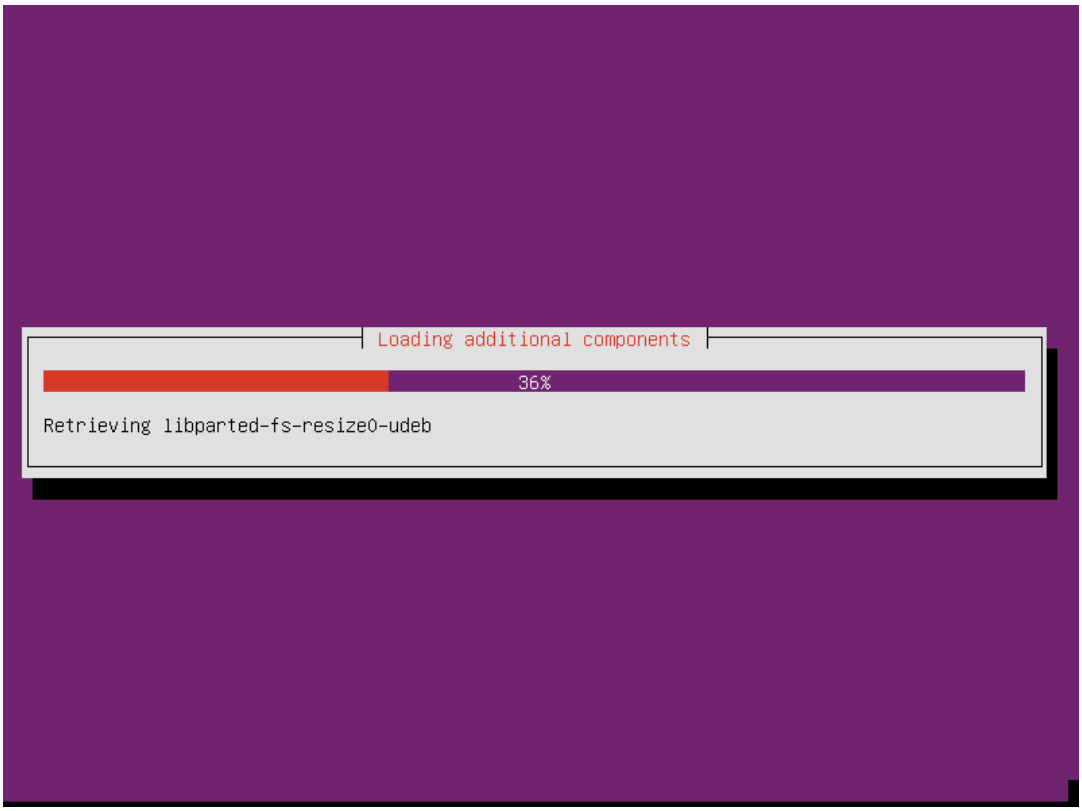
Nun wählen Sie Ihren Standort (benötigt für Zeitzone, Tastatur Layout...)



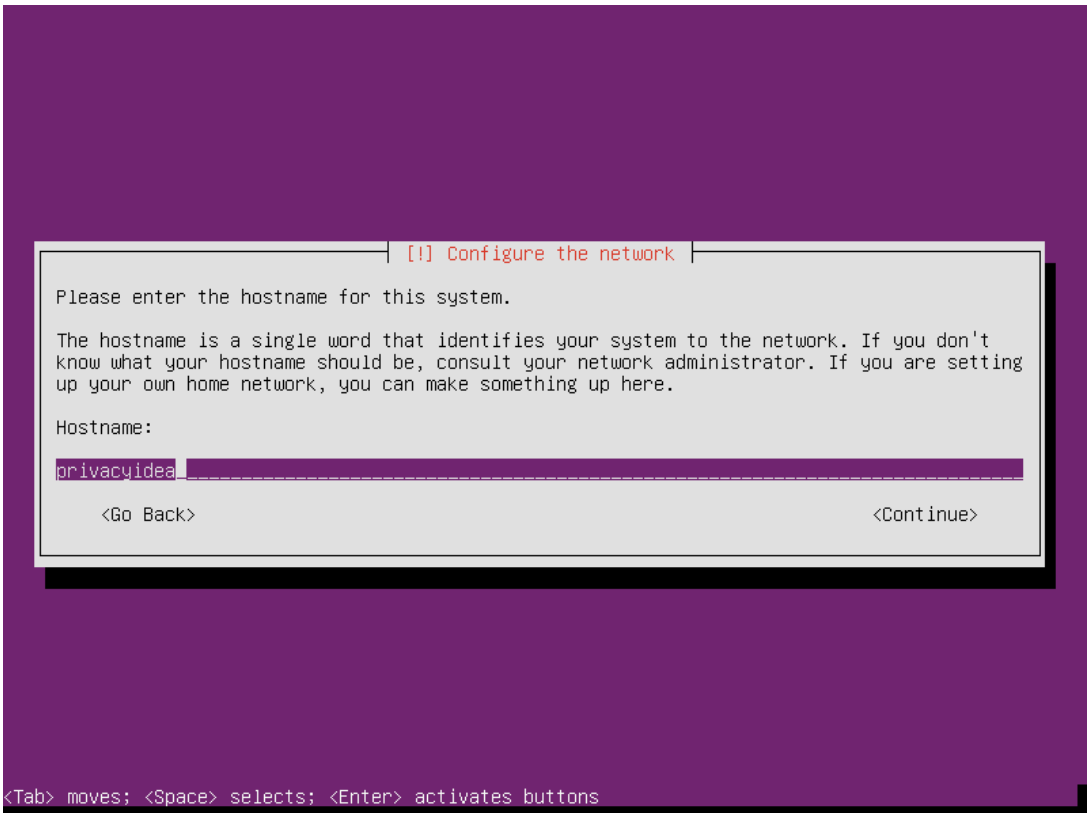
Nun wir der Assistent Sie auffordern einige Tasten auf der Tastatur zu betätigen, damit das richtige Tastaturlayout ausgewählt wird. Ist dies erfolgt und das Layout wurde richtig erkannt, fahren Sie mit der Installation fort.



Nun werden notwendige Komponenten für die Installation vom Assistenten automatisch nachgeladen.

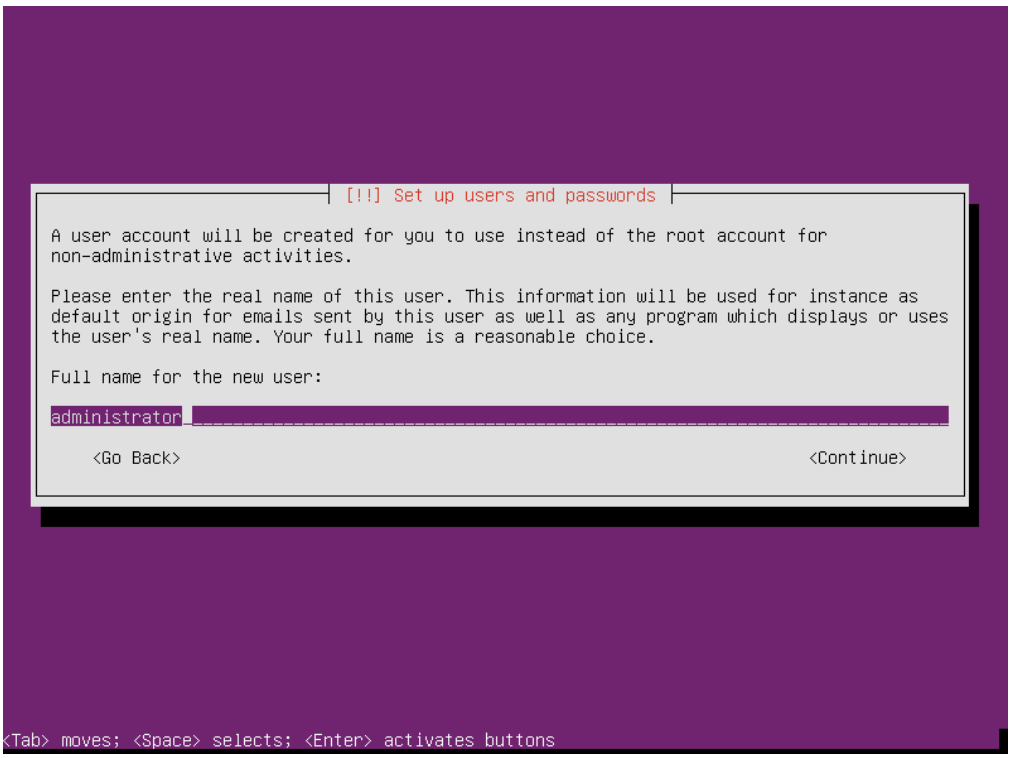


Vergeben Sie nun den Hostnamen, welche wir später auch im DNS registierten werden und unter dem der privacyIDEA Server erreichbar sein soll. In unserem Beispiel privacyIDEA

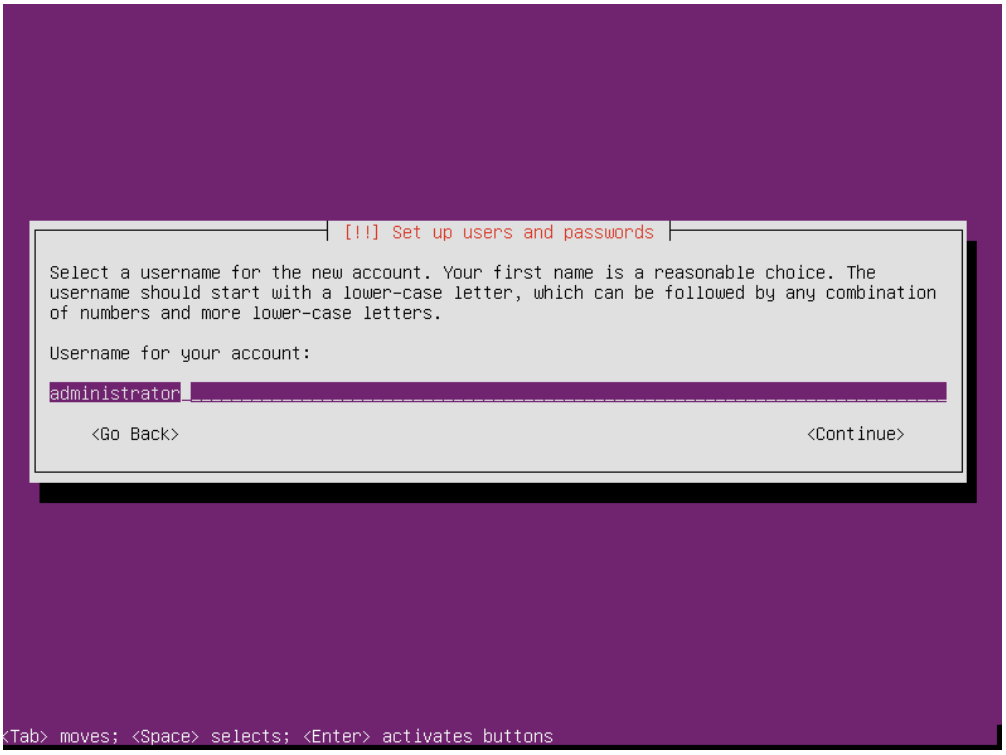


Nun müssen wir einen neuen Benutzer anlegen. In unserem Beispiel: administrator (beachten Sie bei Linux/Unix System gilt Groß-/Kleinschreibung)

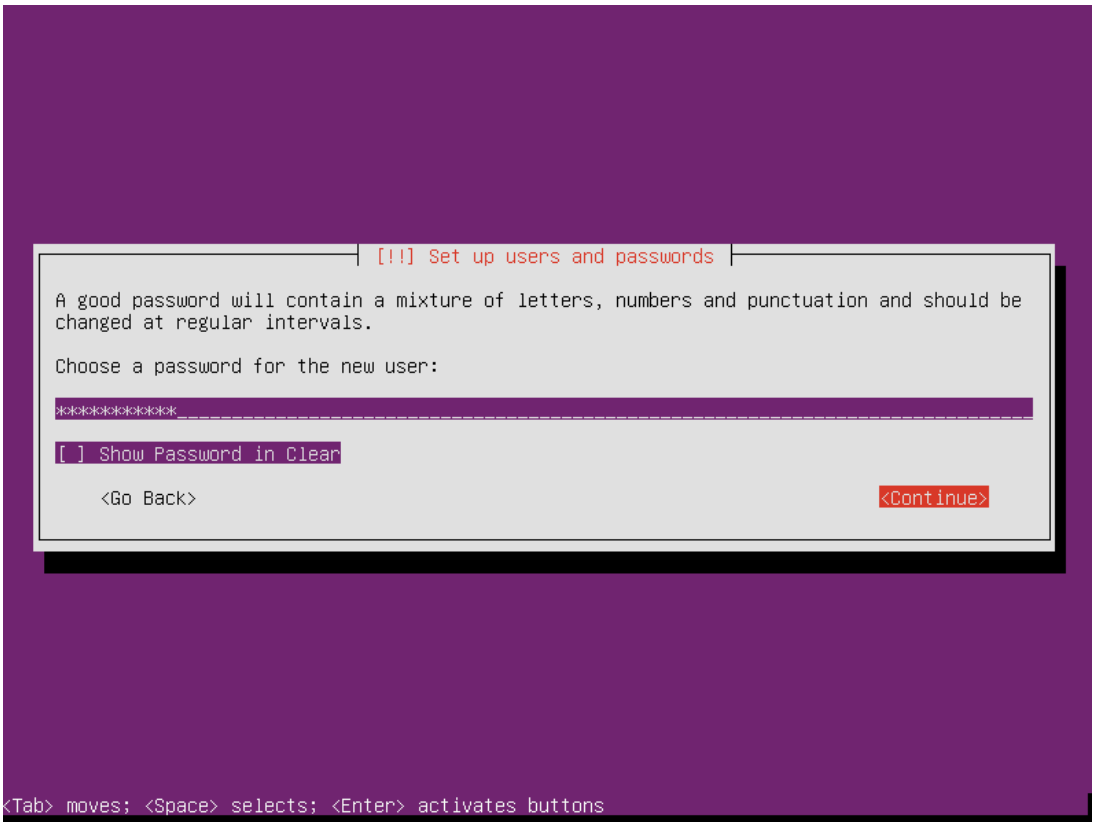
Vollständiger Name:



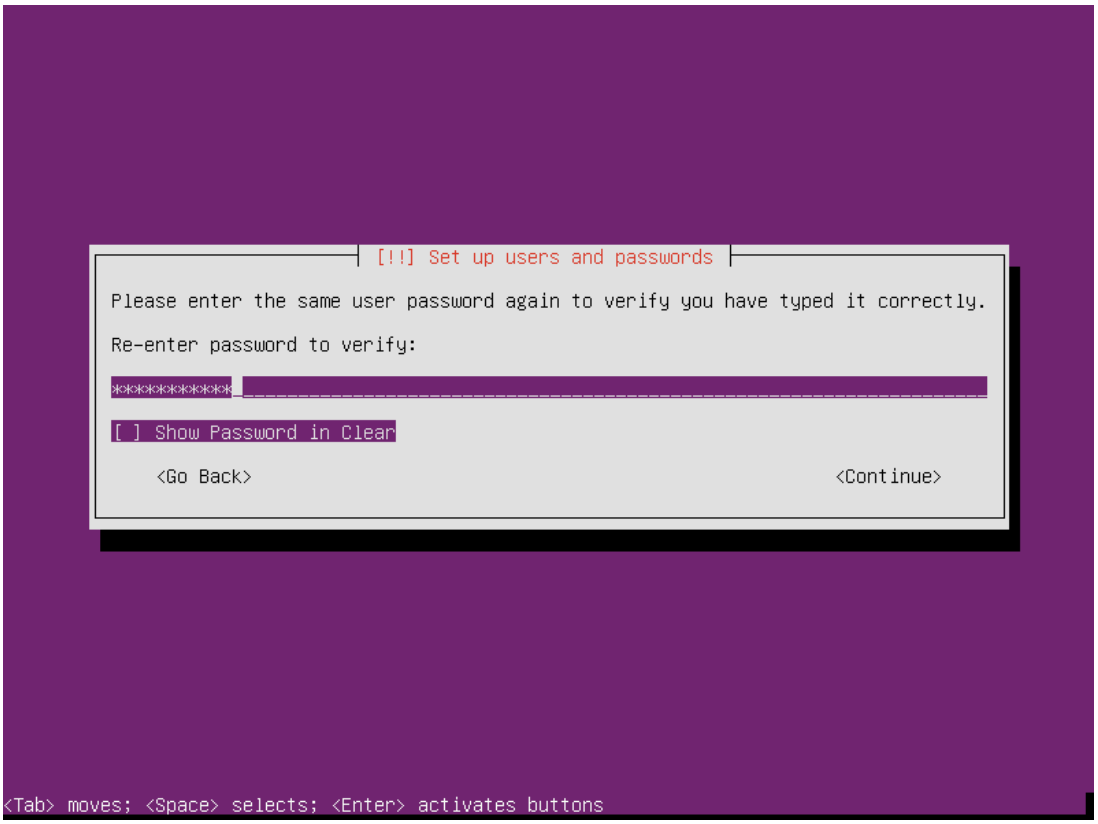
Benutzername:



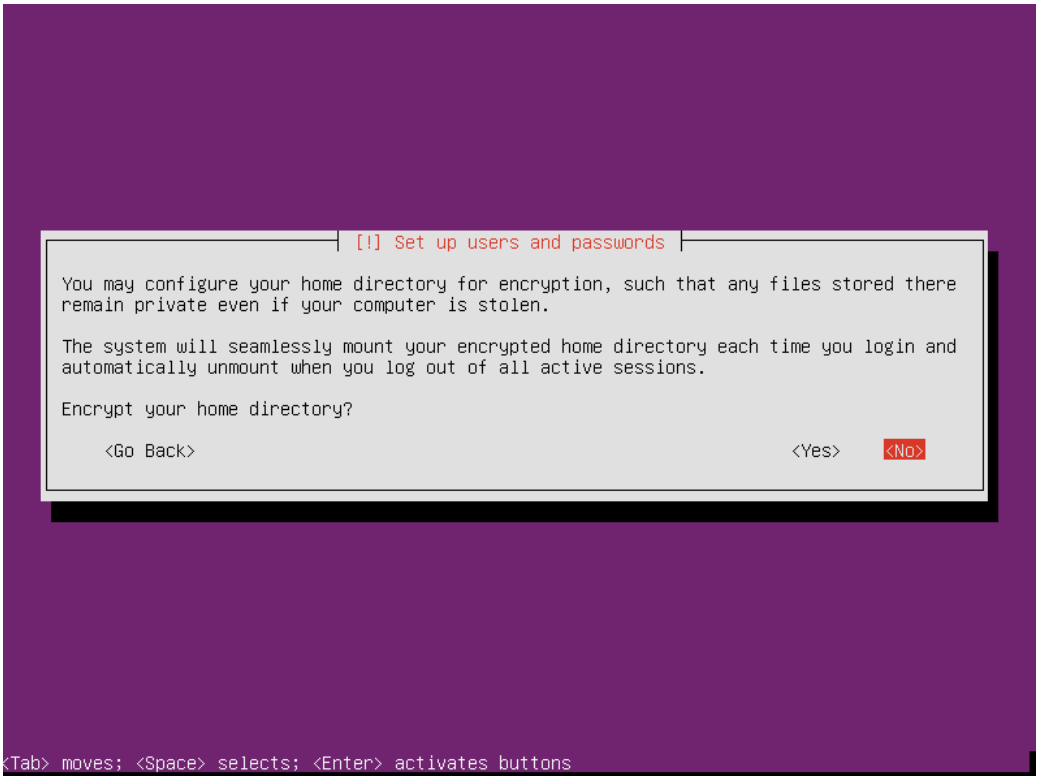
Vergeben Sie nun noch ein sicheres Passwort für den Benutzer:



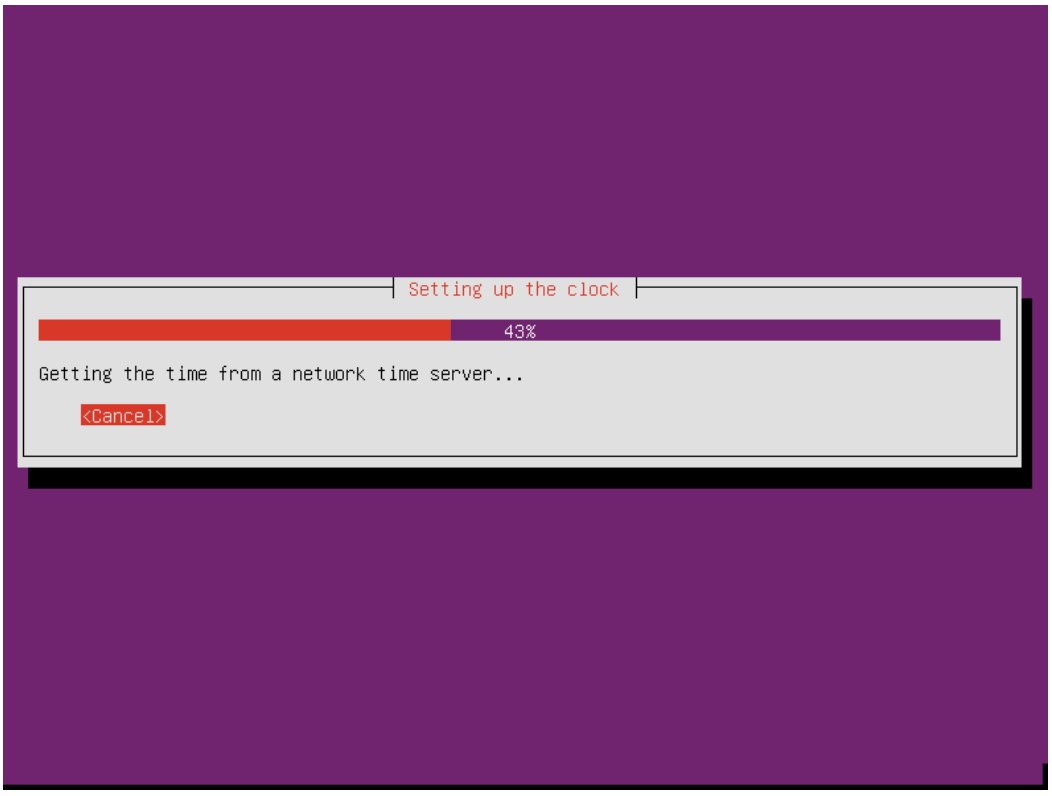
Um Fehleingaben zu vermeiden, fragt Sie der Assistent ein weiteres Mal das Passwort einzugeben.



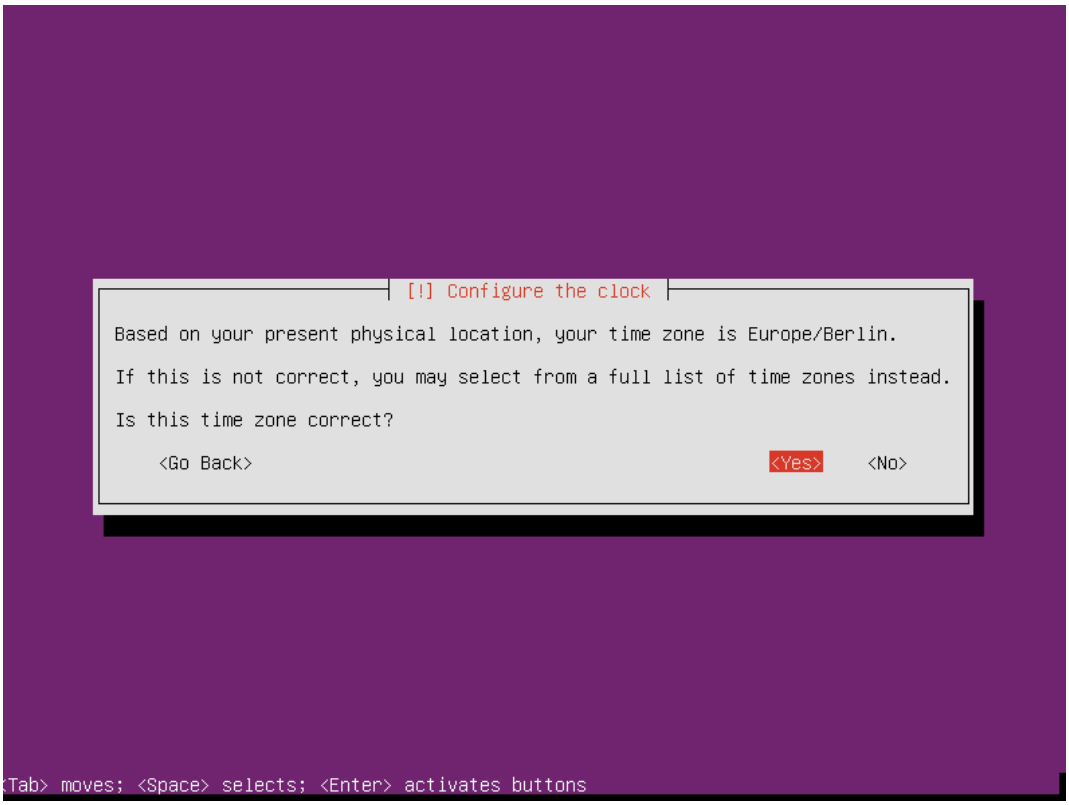
Der Assistent erfragt nun, ob wir das Home Verzeichnis des Benutzers verschlüssel wollen. In unserem Beispiel wählen wir: Nein



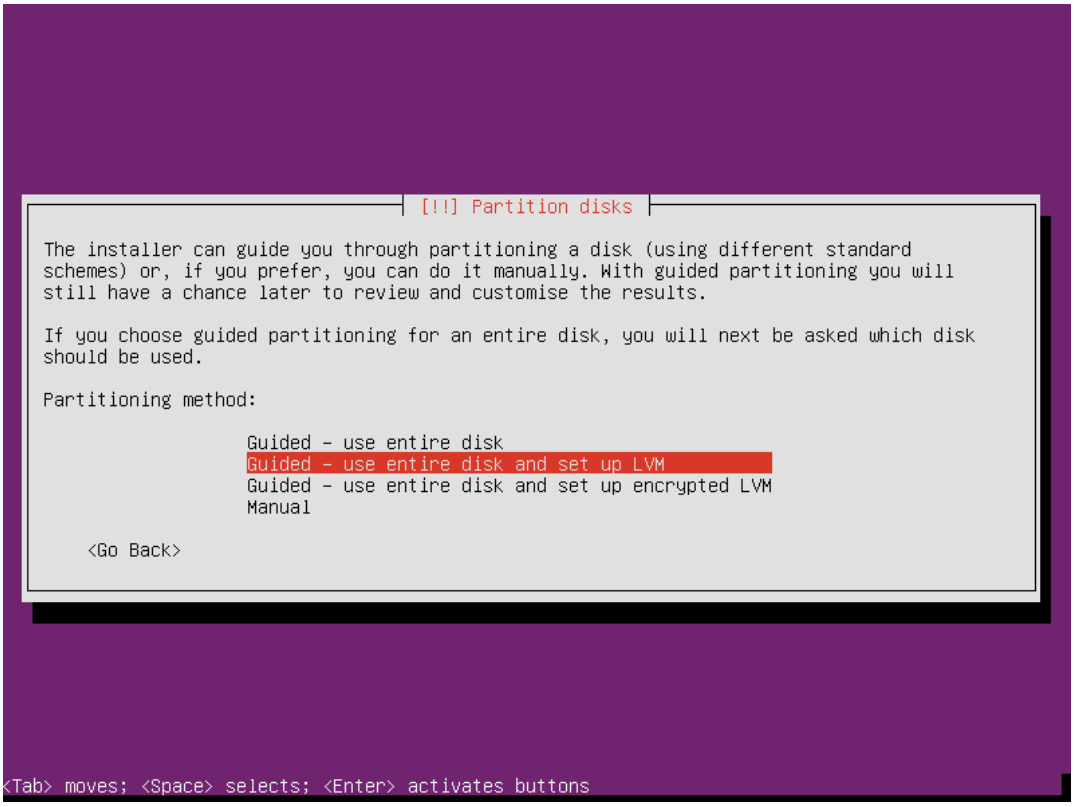
Nun versucht die Installation einen Netzwerkzeitserver zu erreichen, typischerweise ist dies Ihr Domänencontroller oder ein externer Zeitgeben.



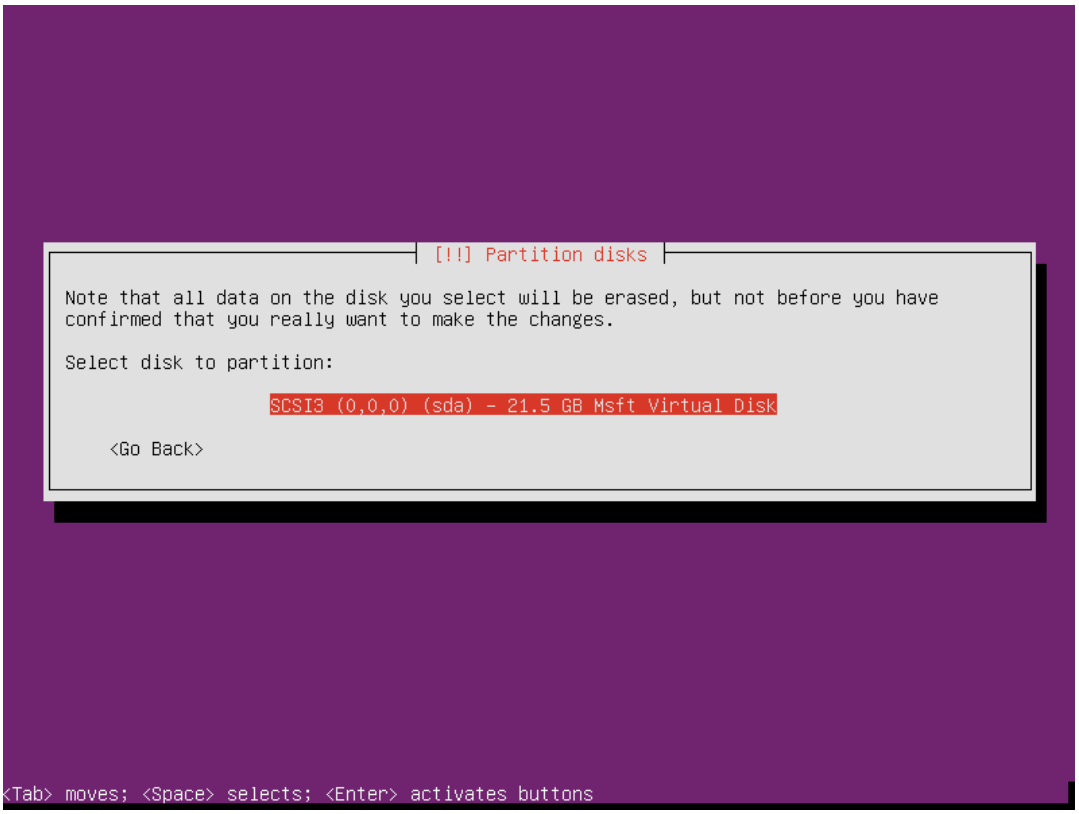
Wurde die Zeitzone richtig ermittelt, fahren Sie mit der Installation fort.



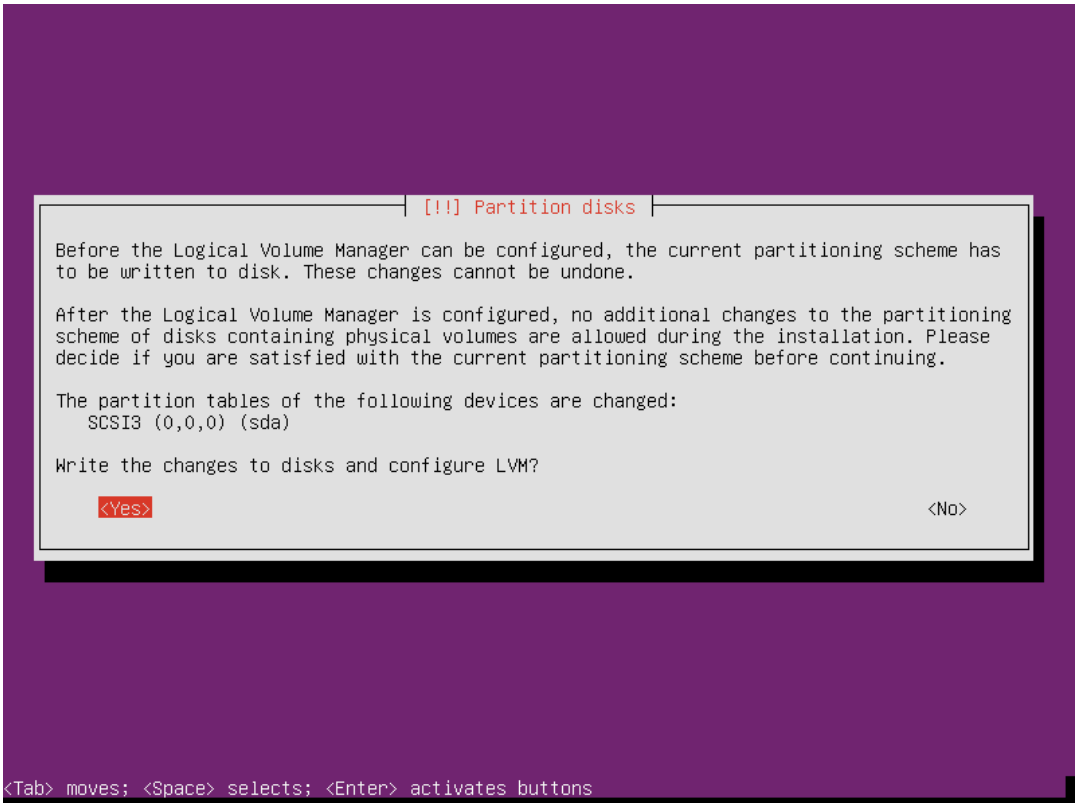
Da es sich bei uns um eine neue virtuelle Maschine handelt, lassen wir den Assistenten die Festplatten Partitionierung durchführen.



Wählen Sie nun die Festplatte auf Ubuntu installiert werden soll.

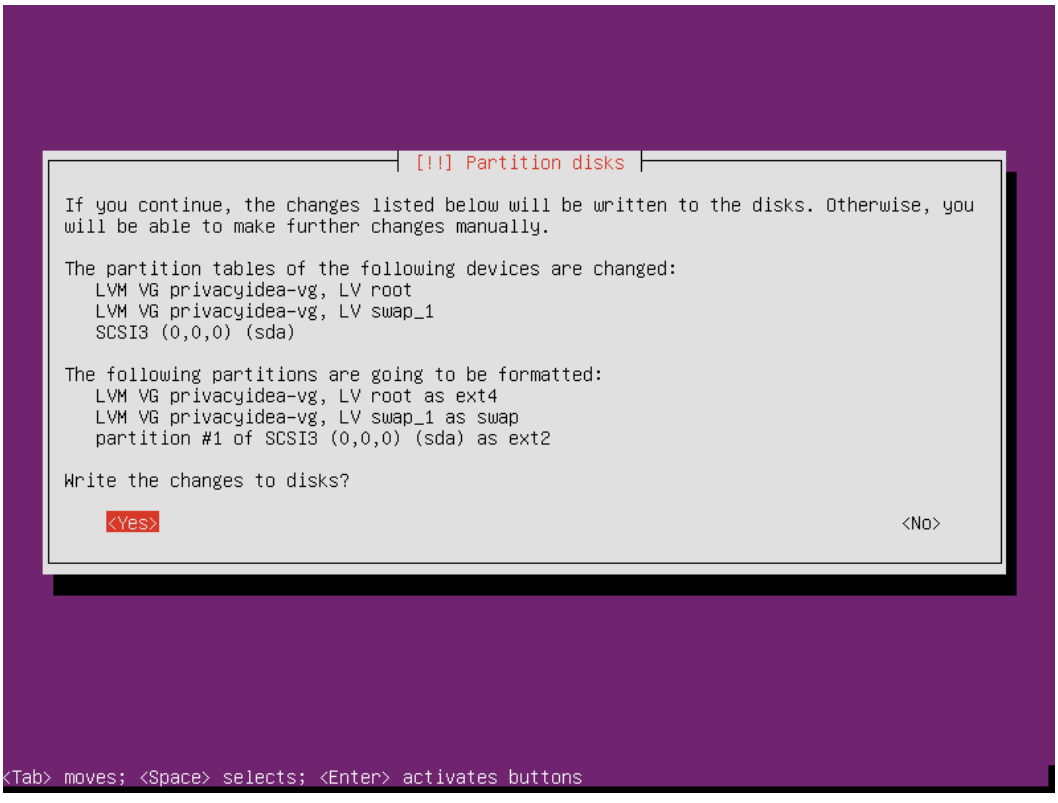


Und bestätigen die Eingabe

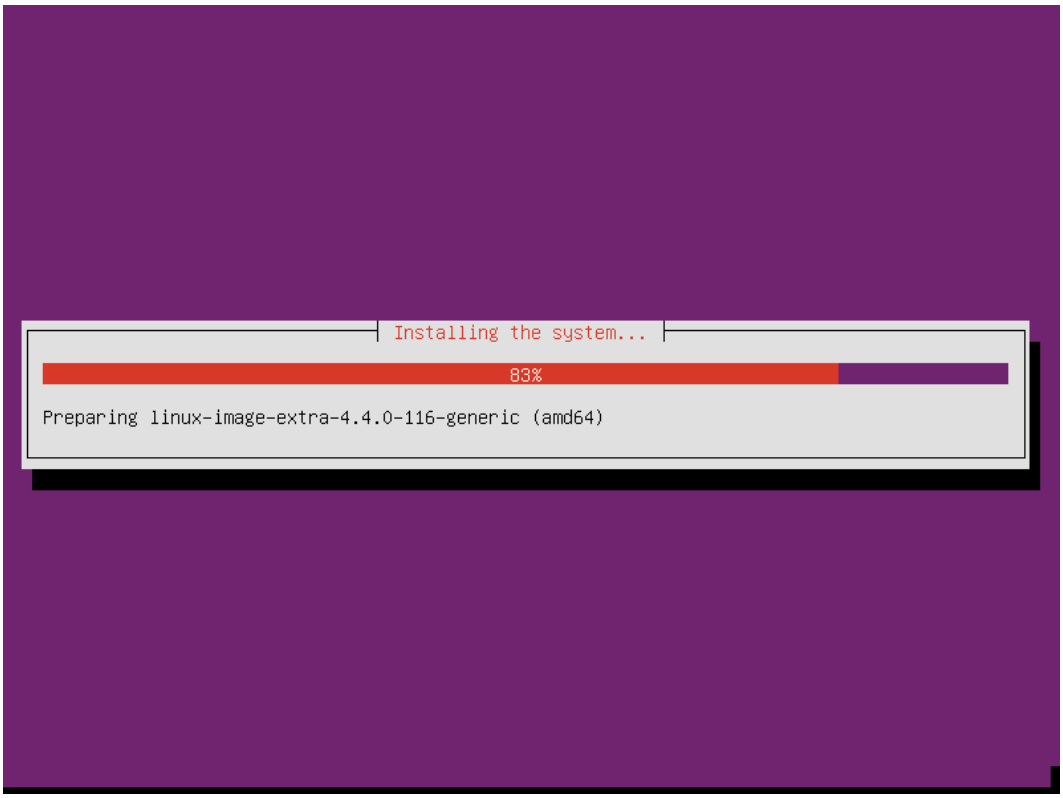


Geben Sie nun noch die Größe des Volumens an

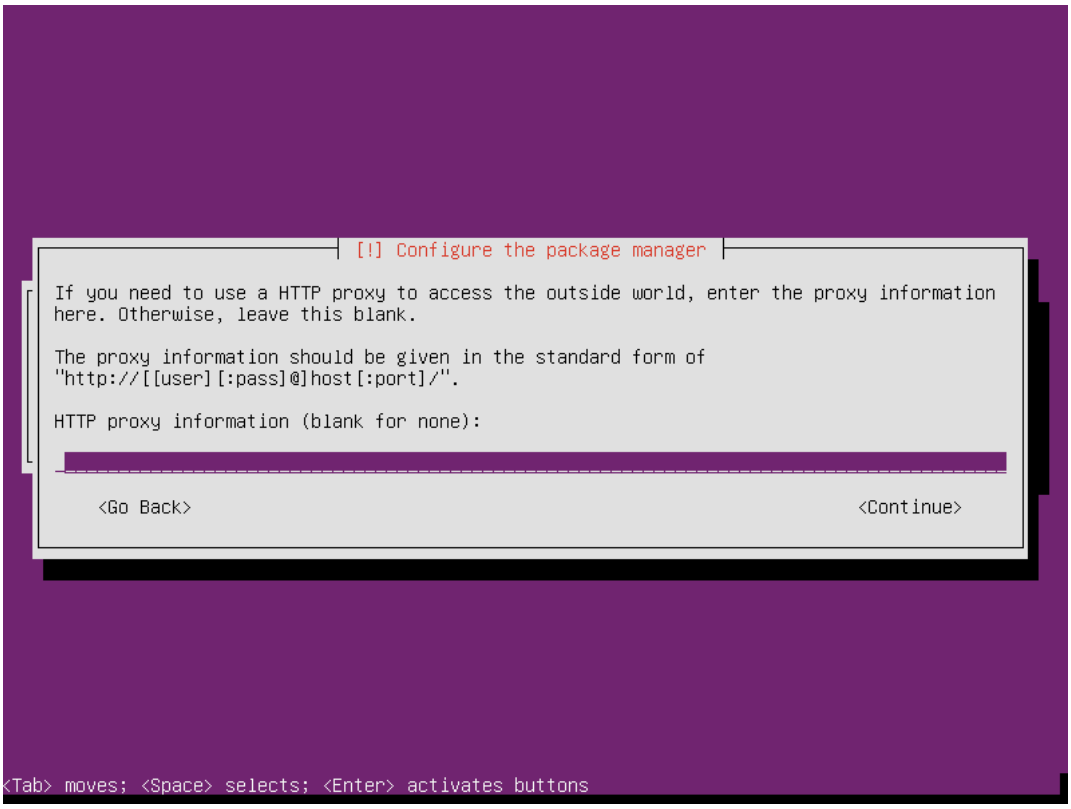
Und bestätigen das die Partitionierung nun durchgeführt wird.



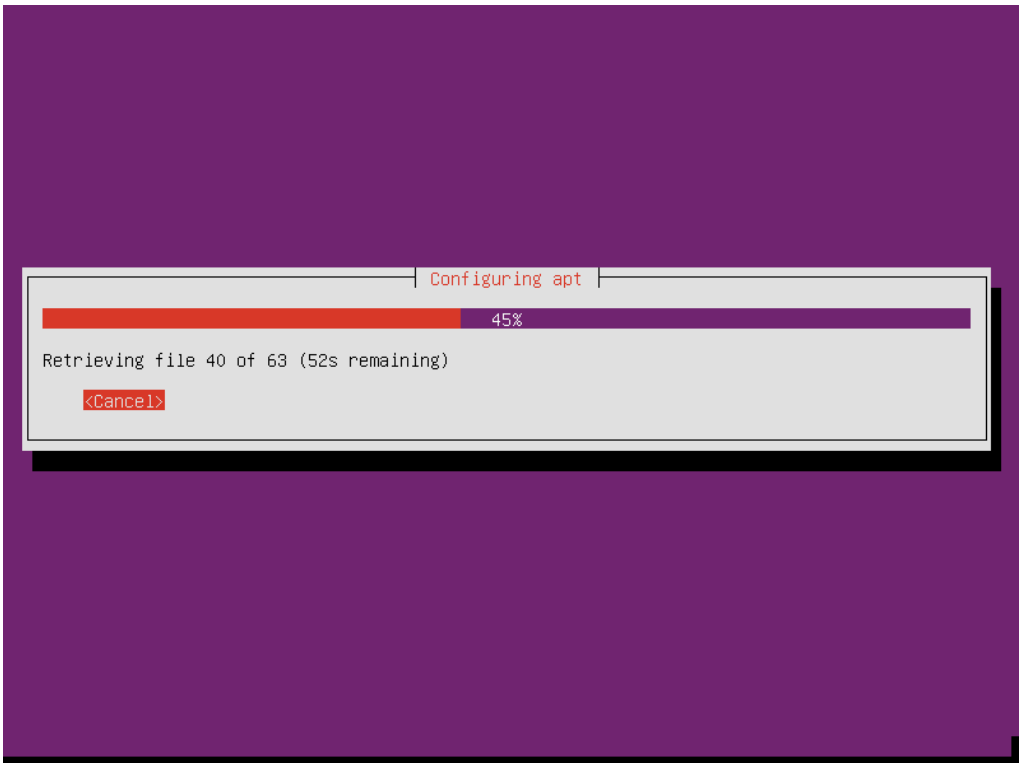
Ubuntu wird nun weitere Komponenten laden



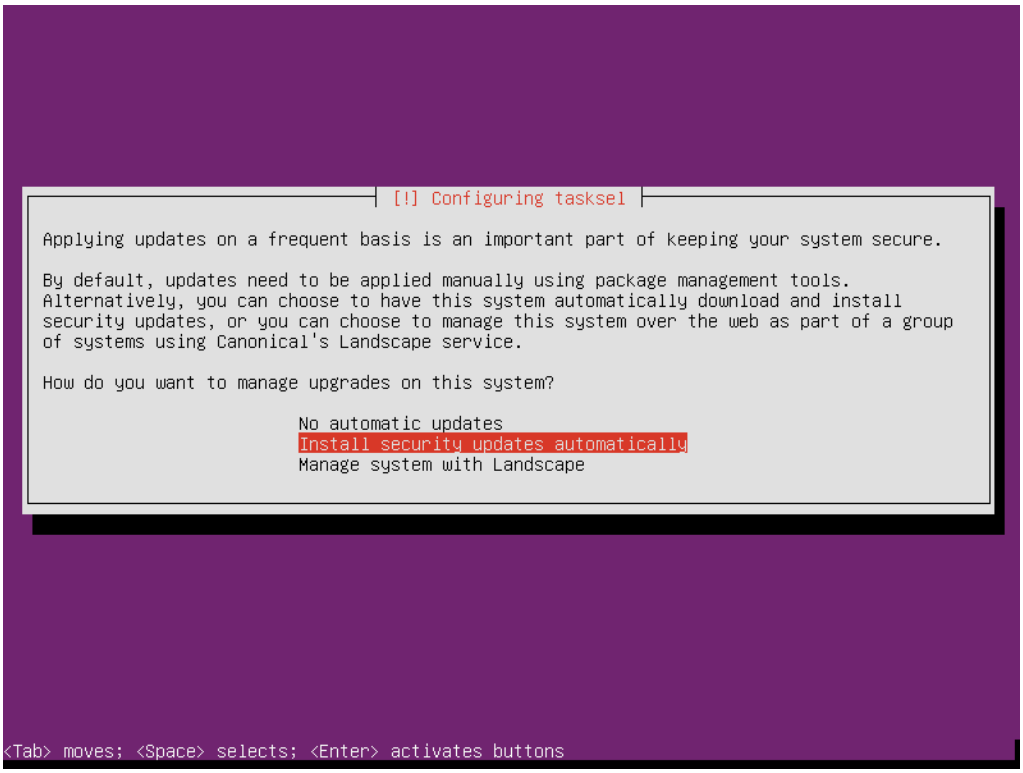
Für Updates und Pakete die nicht mit dem Installationsmedium ausgeliefert werden ist ggf. Eine Internetverbindung erforderlich. Sollte diese nur über einen HTTP Proxy bereitgestellt werden, geben Sie diesen nun ein.



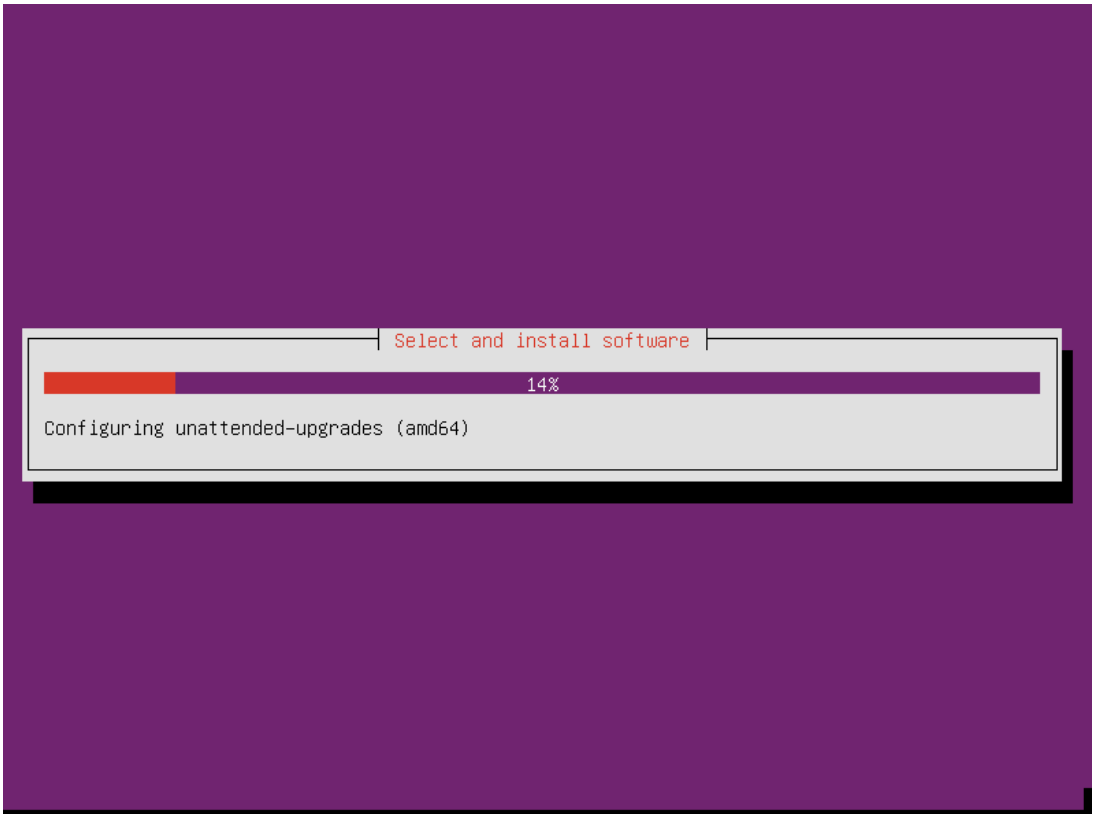
Die Internetverbindung wird nun überprüft und weitere Pakete und Updates nachgeladen.



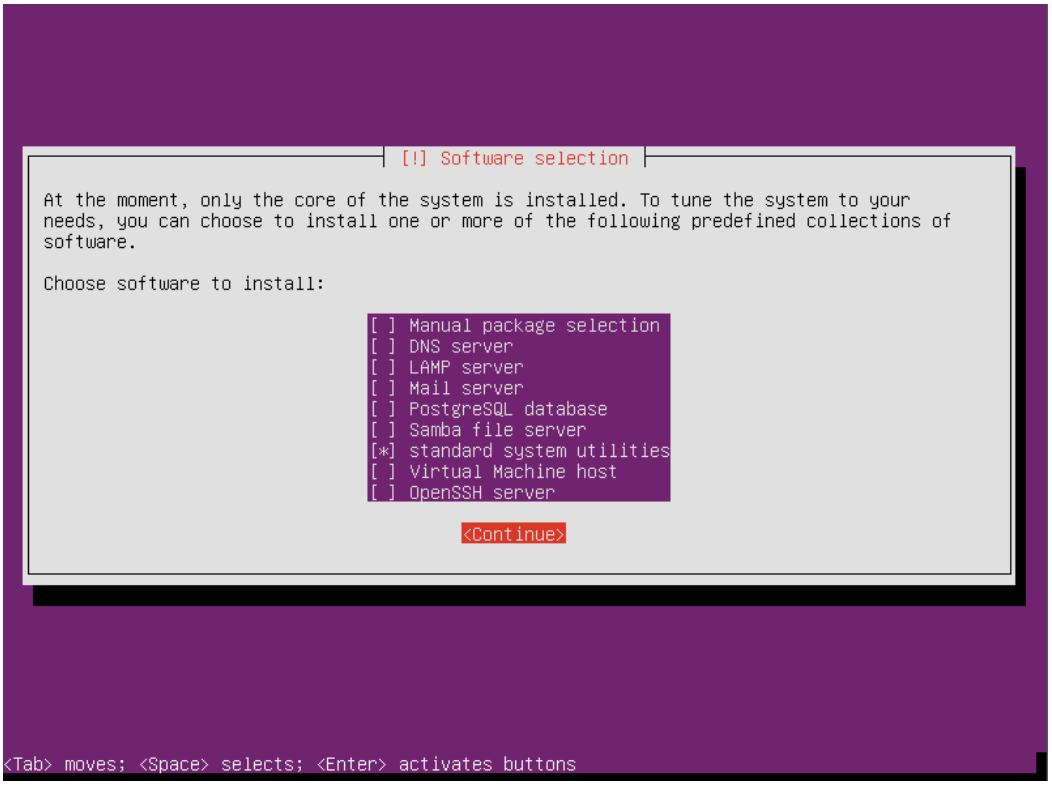
Sie können nun noch auswählen ob Updates automatisch installiert werden solen. Beachten Sie das beim Installieren von Updates ggf. Ein Neustart von Diensten, Prozessen oder des gesamten Betriebssystems erforderlich ist.



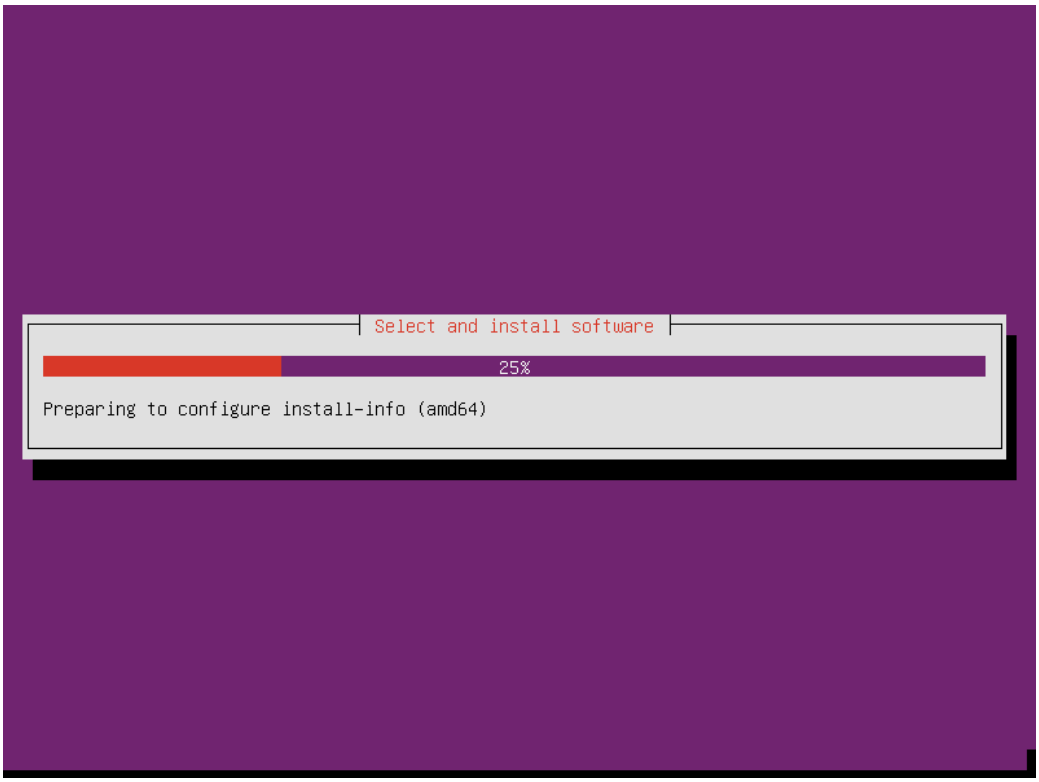
Da wir die automatische Installation von Sicherheitsupdates ausgewählt haben, wird dies nun konfiguriert.



Da wir keine weiteren Komponenten zwingend benötigen können Sie ohne zusätzliche Auswahl von Paketen fortfahren. Optional können Sie den OpenSSH Server auswählen, dadurch muss Schritt 1.5. nicht vollständig beachtete werden.

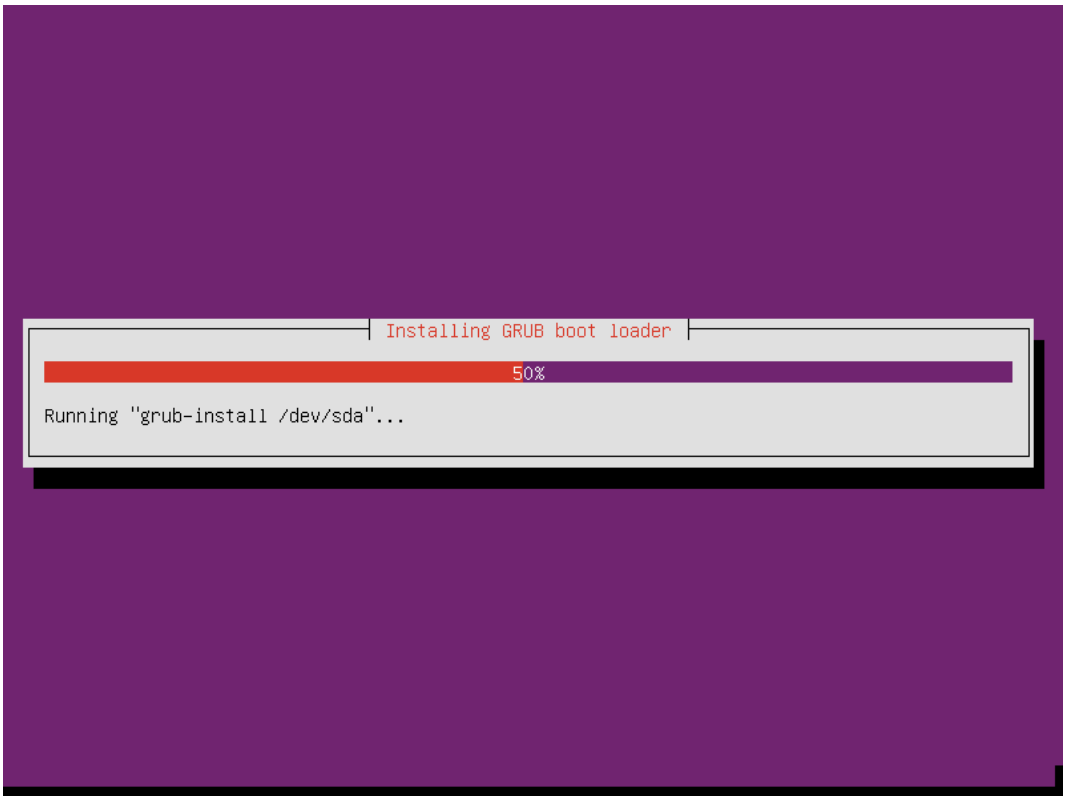


Nun wird Ubuntu auf die virtuelle Maschine installiert.

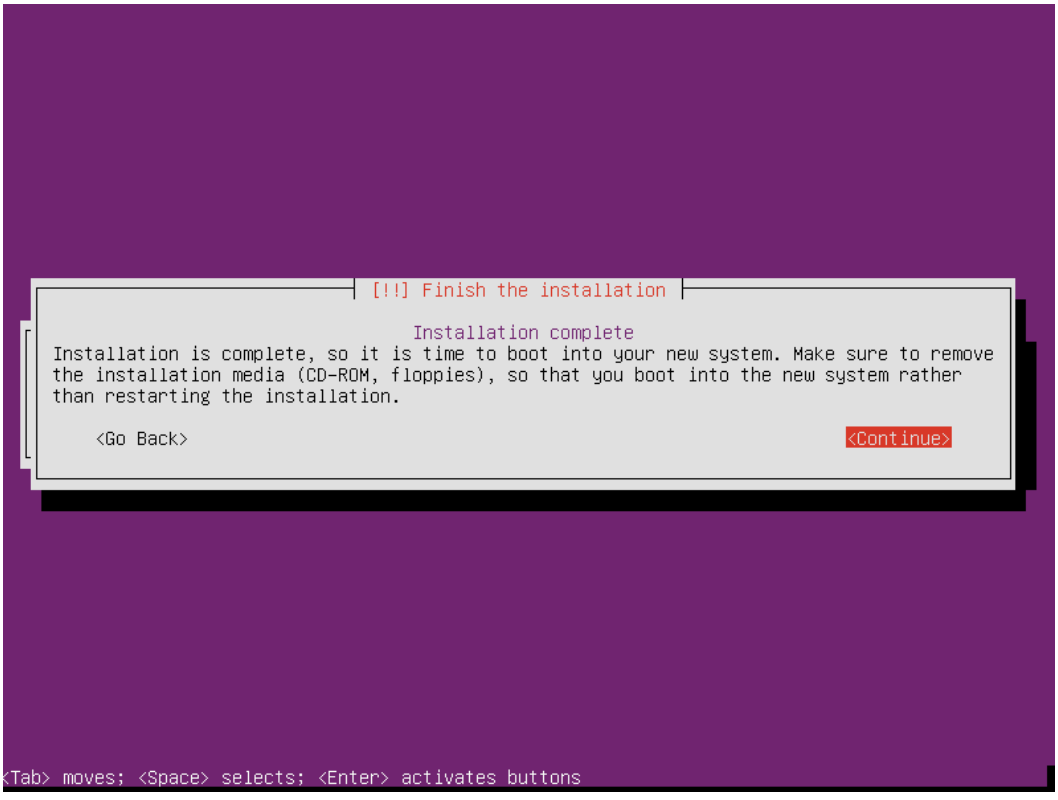


Nach Abschluss muss noch der Master Boot Record (MBR) geschrieben werden. Bestätigen Sie dies mit Ja, da sonst ggf. Das Betriebssystem nicht startet.

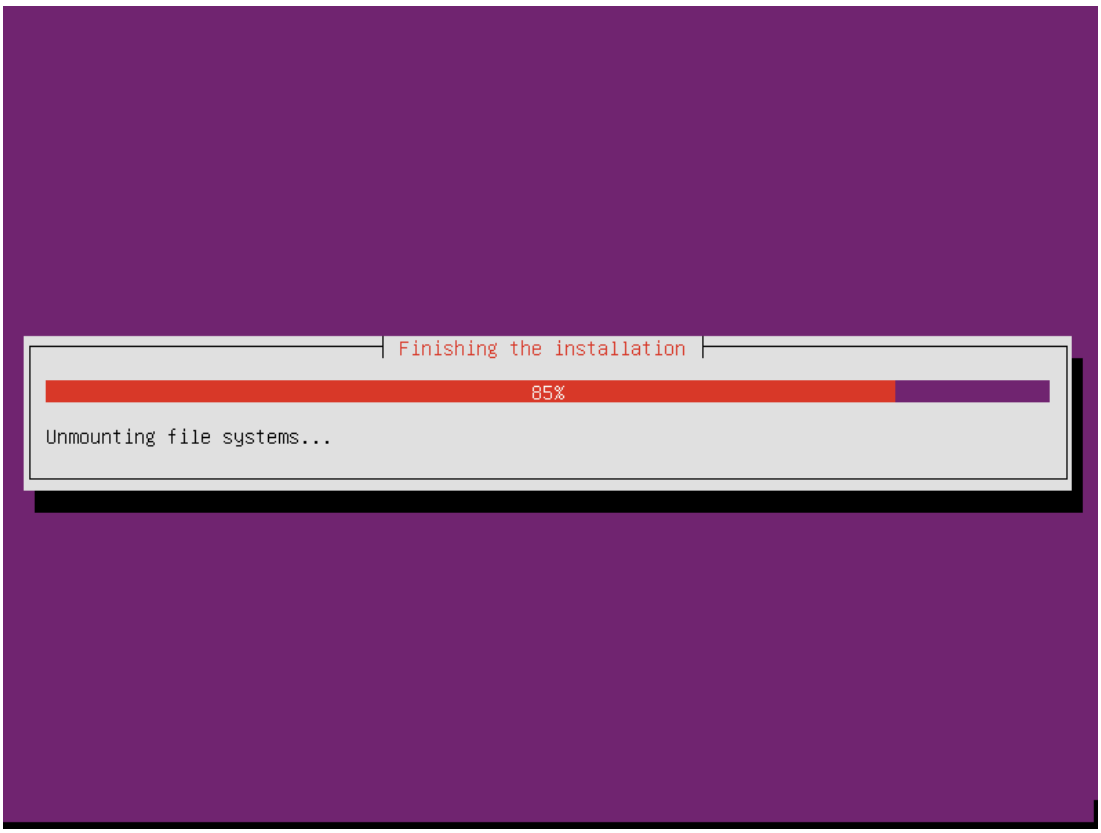
Der Assistent schließt nun die Installation ab



Damit nicht erneut die Installationsroutine von dem hinzugefügten ISO Image gestartet wird, Kann Ubuntu dieses automatisch entfernen und das System neustarten.



Das System wird nun neu gestartet



1.3. Ändern der Netzwerkeinstellungen

Nachdem die Installation abgeschlossen ist und Ubuntu 16.04 erfolgreich installiert wurde, melden Sie sich mit dem zuvor erstellen Benutzername an. Wir führen einige grundsätzliche Einstellungen durch, damit wir mit der Installation von privacyIDEA beginnen können.

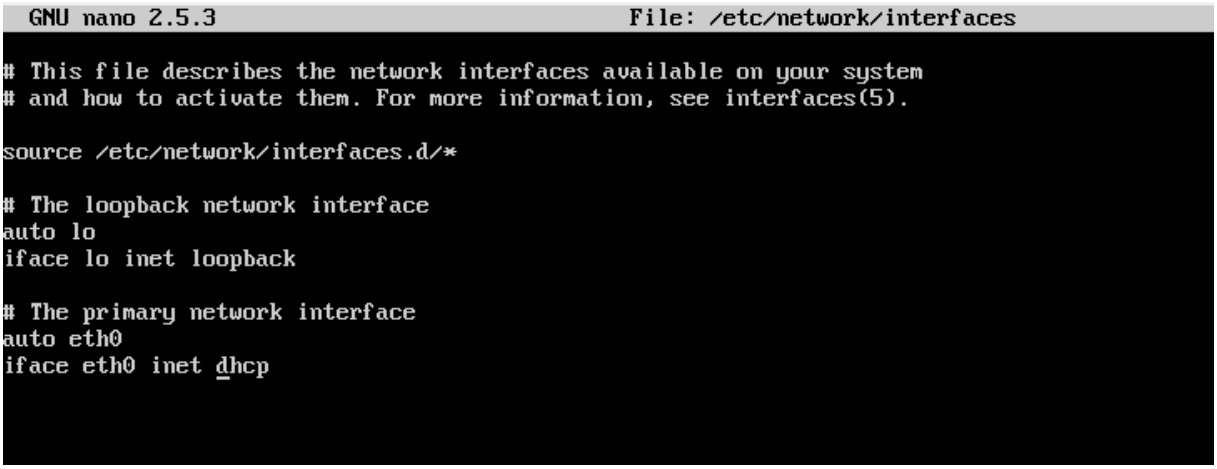
Als erstes setzen vergeben wir eine statische IP Adresse. Selbstverständlich können Sie auch das Netzwerkinterface auf DHCP belassen, sollten jedoch sicherstellen das eine feste IP Adresse zugewiesen wird.

Hierzu öffnen wir die Konfigurationsdatei für die Netzwerkschnittstellen mit einem Texteditor (Nano)

Command: sudo nano /etc/network/interfaces

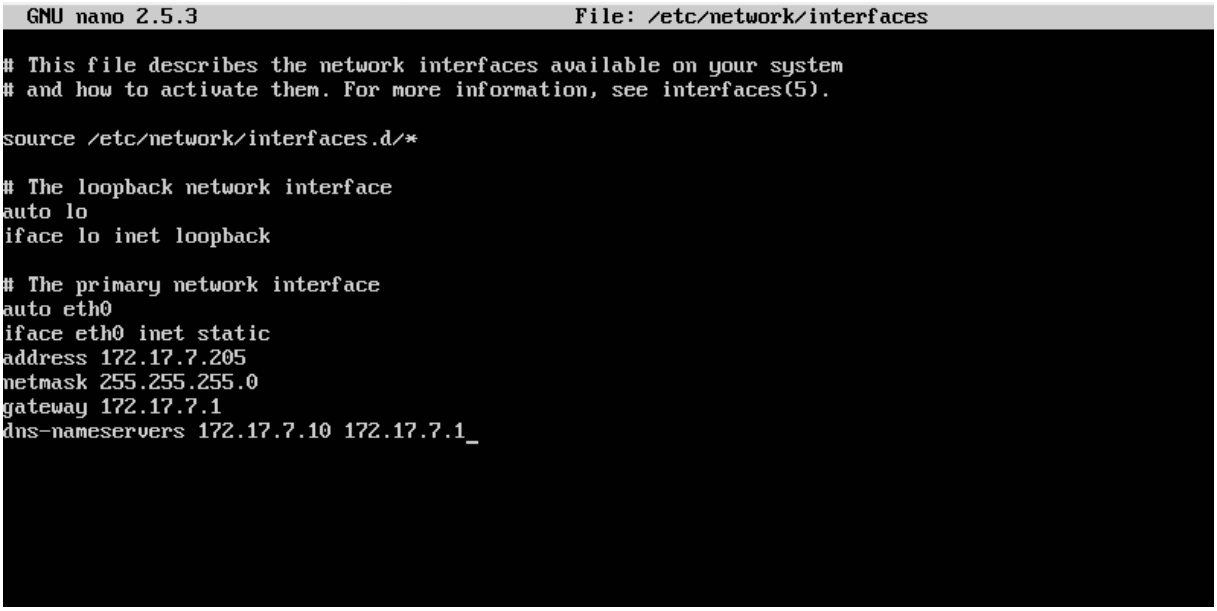
Die Netzwerkschnittstellen sollte ähnlich wie im Bild (original) aussehen.

Original:



Ändern Sie nun die Datei wie folgt ab. Bitte verwenden Sie die entsprechenden Parameter für Ihr Netzwerk (Netzmaske, Gateway, DNS Server und eine IP Adresse aus dem selben Addressbereich) Unsere Beispielkonfiguration sieht nun wie folgt aus

Neu:



Um die Änderungen zu speichern, drücken Sie STRG + X und bestätigen das Speichern mit JA/Yes

Damit die Einstellungen ohne Neustart übernommen werden, „reseten“ wir die Netzwerkschnittstelle.

Zuerst entfernen wir die zuvor vergebene IP Adresse des Adapters

Kommando: sudo ip addr flush eth0

```
administrator@privacyidea:~$ sudo ip addr flush eth0_
```

Nun starten wir den Netzwerk Dienst neu

Command: sudo systemctl restart networking.service

```
administrator@privacyidea:~$ sudo systemctl restart networking.service
administrator@privacyidea:~$ _
```

Damit wir sicherstellen das die von uns vergebene IP Adresse auch auf dem Adapter zugewiesen ist, überprüfen wir die Einstellungen mit folgendem Kommando:

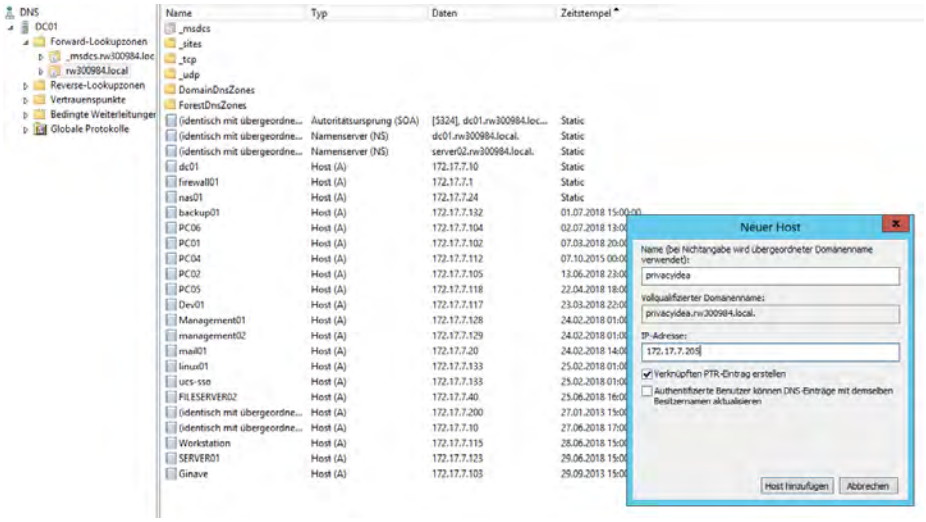
Command: ip add

```
administrator@privacyidea:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:15:5d:07:7b:14 brd ff:ff:ff:ff:ff:ff
    inet 172.17.7.205/24 brd 172.17.7.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe07:7b14/64 scope link
       valid_lft forever preferred_lft forever
administrator@privacyidea:~$ _
```

Nun sollte der privacyIDEA Server bereits via IP Adresse über das Netzwerk verfügbar sein. Damit der Server auch über den FQDN/Hostname erreichbar ist, müssen wir noch einen DNS Eintrag erstellen.

1.4. DNS Record hinzufügen

Damit der privacyIDEA auch über den Hostname/FQDN erreichbar ist, fügen wir einen DNS A Record in unserem Microsoft DNS Server hinzu.

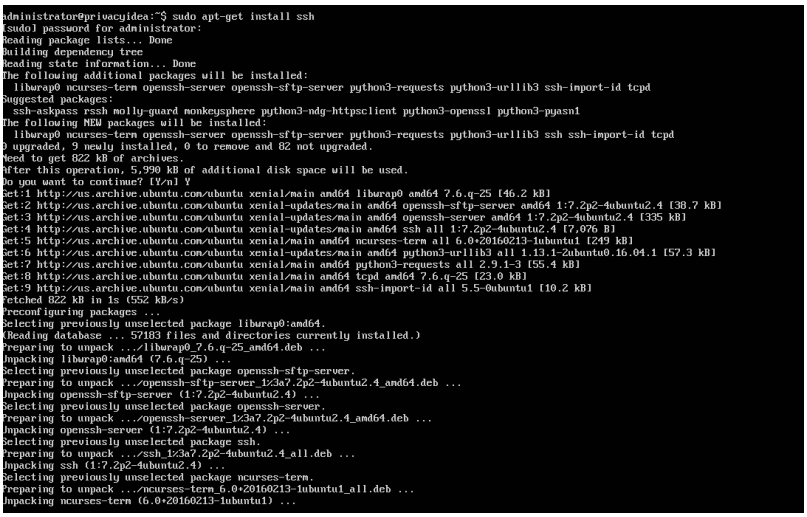


1.5. SSH Server auf Ubuntu Server installieren und konfigurieren

Sollten Sie bereits während der Installation des Ubuntu Betriebssystems den OpenSSH Server installiert haben, können Sie direkt mit der Konfiguriation des SSH Daemon fortfahren, in unserem Beispielt installieren wir diesen manuell.

Diesen können Sie mit folgender Zeile installieren.

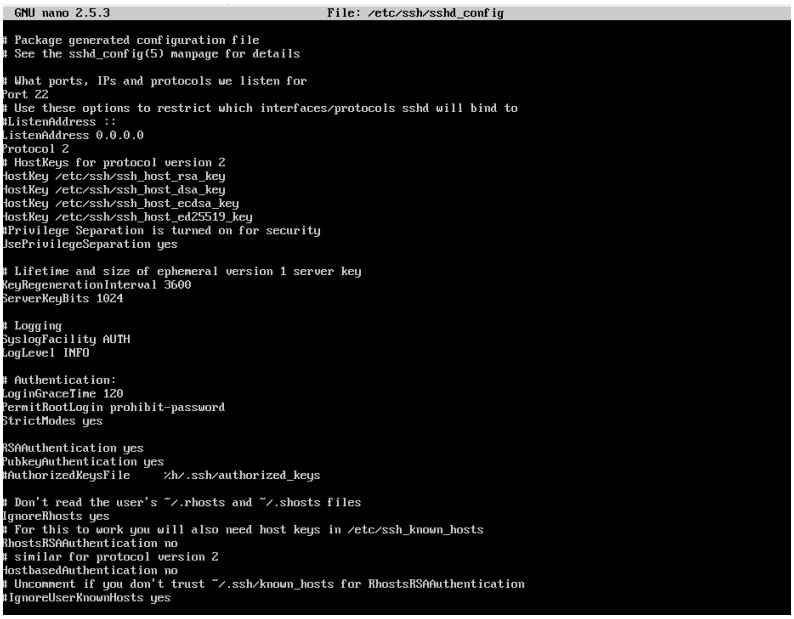
Command: sudo apt-get install ssh



Ist die Installation erfolgreich gewesen, müssen wir den SSH Server konfigurieren. Hierzu öffnen wir die Konfigurationsdatei in einem Texteditor (Nano)

Command: sudo nano /etc/ssh/sshd_config

Kommentieren Sie die ListenAddress aus oder geben Sie die IP Adresse des Servers an. Speichern Sie nun die Konfiguration mit STRG + X und bestätigen Sie mit Ja/Yes



Damit die Konfigurationsänderungen aktiv warden, starten Sie den SSH Dienst neu.

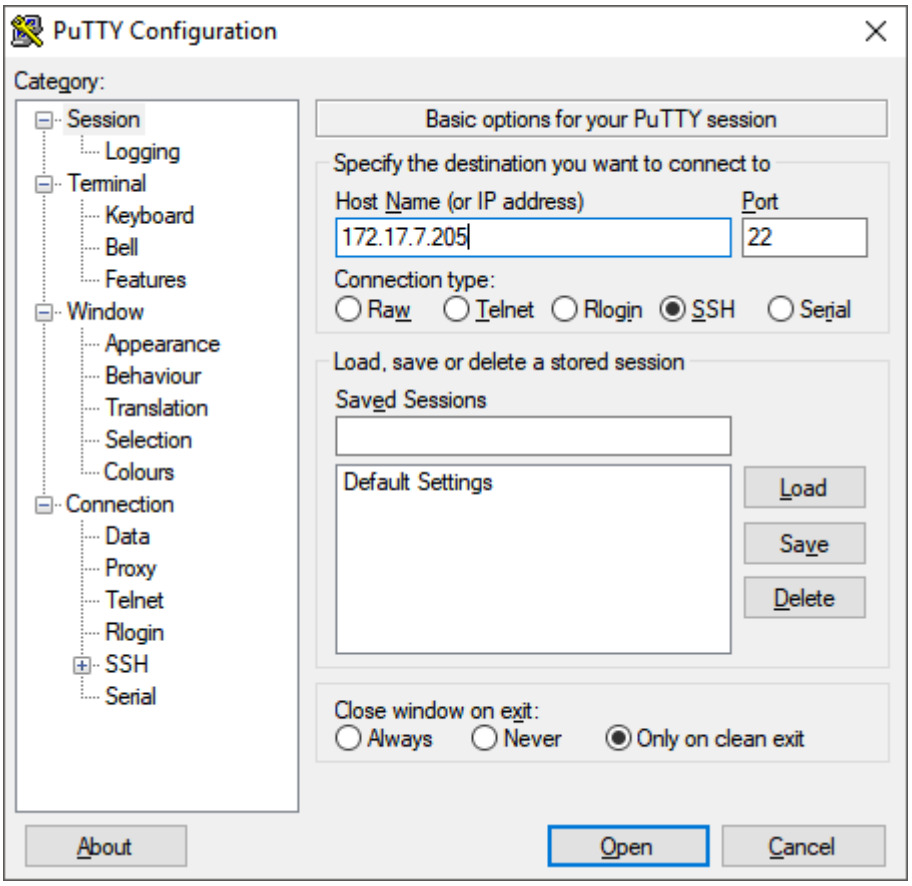
Command: sudo service ssh restart

```
administrator@privacyidea:~$ sudo service ssh restart
administrator@privacyidea:~$ _
```

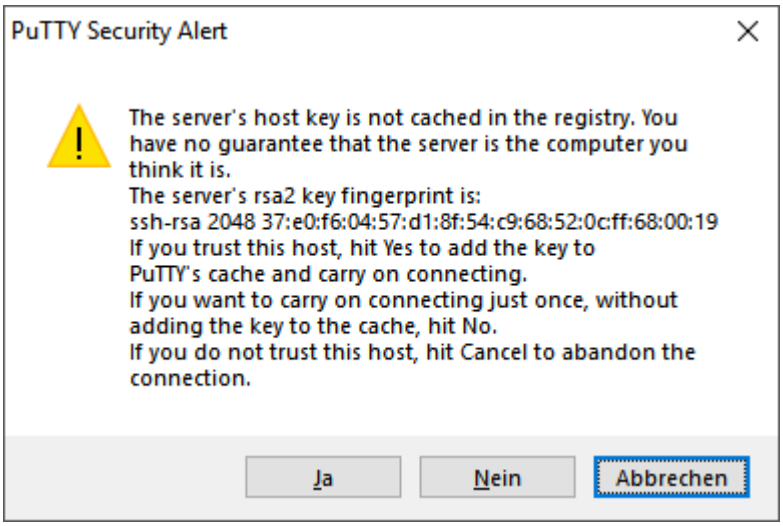
1.6. Verbindung via SSH Client (z.B. Putty) testen

Nun können Sie mit einem SSH Client direkt von Ihrem Computer auf den privacyIDEA Server zugreifen. Wir verwenden in unserem Beispiel: Putty (https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html)

Im Putty Client geben Sie nun den Hostname oder die IP Adresse des Servers ein, wählen den SSH Port (Standard: 22) und als Connection Type wählen Sie SSH. Anschliessend klicken Sie auf Open, um eine Verbindung herzustellen.



Sie werden nun gefragt ob Sie den Schlüssel des Servers für zukünftige Verbindungen speichern möchte.

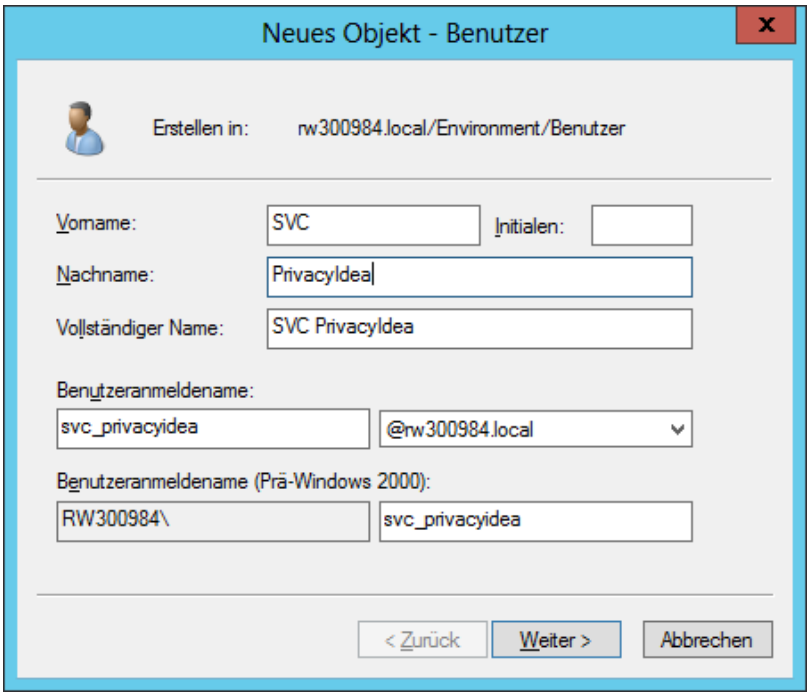


Anschliessend sehen Sie die Anmeldung am Ubuntu Server.

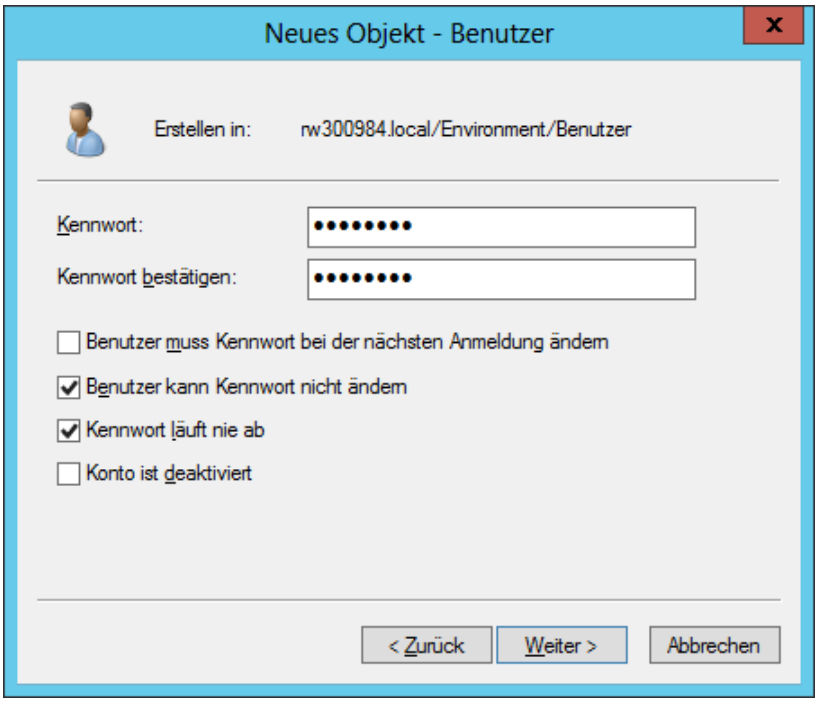
1.7. Service Account in Active Directory anlagen

Damit wir nach der Installation von privacyIDEA nicht nochmal auf ein anderes System wechseln müssen, legen wir bereits jetzt einen Service Account an. Dieser ist erforderlich um die Benutzer aus einem Active Directory zu synchronisieren und Passwörter zu validieren.

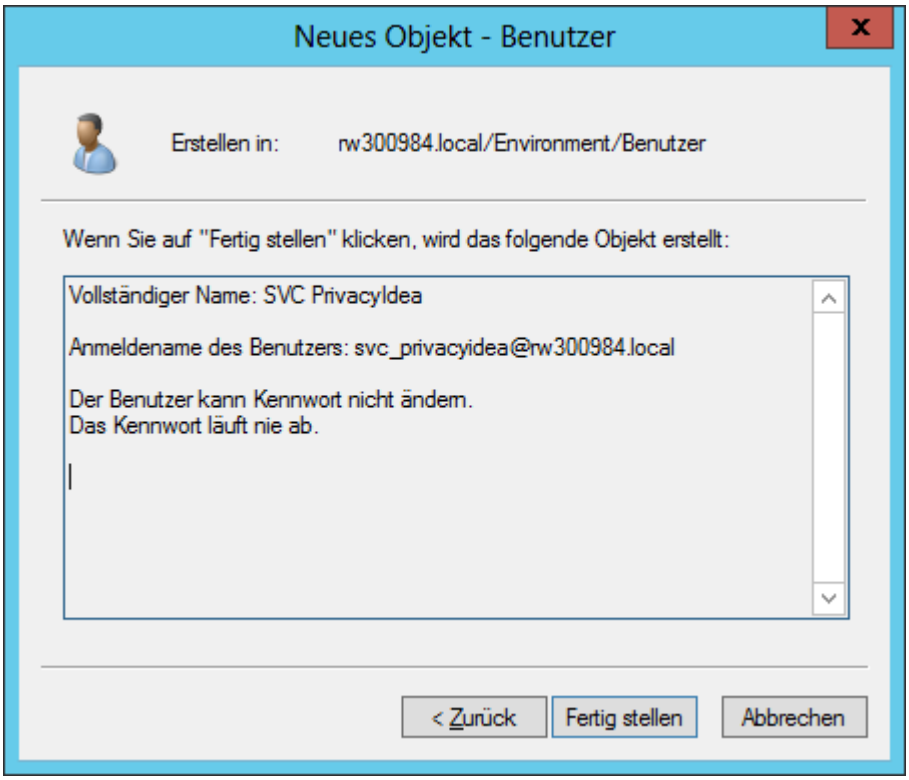
Wir legen einen Standardbenutzer an (er benötigt keine administrativen Rechte, muss jedoch auf das zu synchronisierende Verzeichnis lesend zugreifen können)



Vergeben Sie ein sicheres Passwort und stellen sicher das dieses Kennwort nicht abläuft.



Mit klick auf “Fertig stellen” wird der Benutzer im Active Directory erstellt.



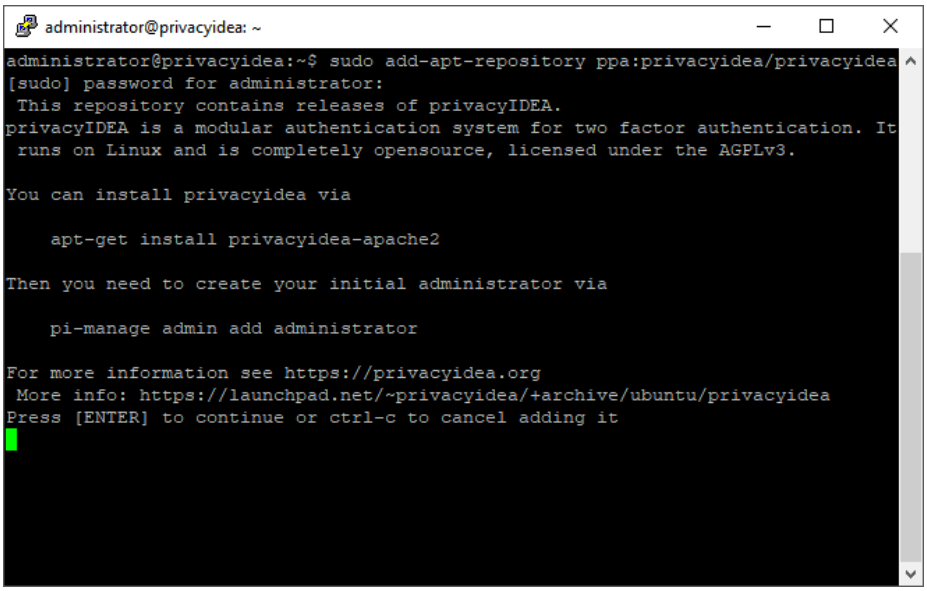
2. Installation privacyIDEA

Nachdem wir alle Vorbereitungen in Kapitel 1 dieses Guides durchgeführt haben, können wir mit der Installation des privacyIDEA Servers beginnen.

2.1. Hinzufügen des privacyIDEA Ubuntu repository

Für privacyIDEA existiert ein eigenes Ubuntu Repository, welches wir auf dem Server hinzufügen müssen. Dies ermöglicht uns eine einfache Installation und zukünftige Updates.

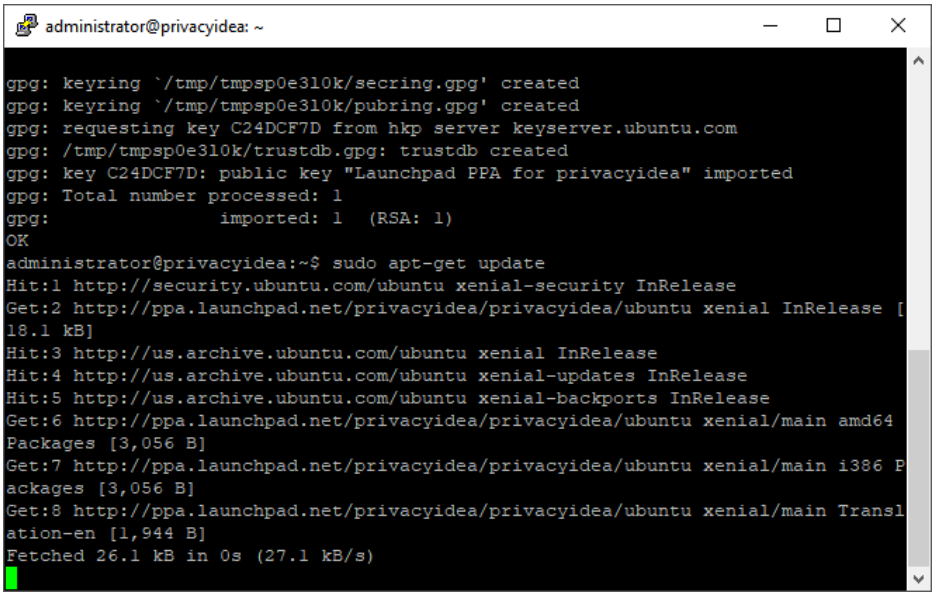
Command: `sudo add-apt-repository ppa:privacyIDEA/privacyIDEA`



2.2. Updaten der Ubuntu Repositories

Wurde das Repository hinzugefügt, müssen wir nun den lokalen Cache aktualisieren, damit wir mit der Installation starten können

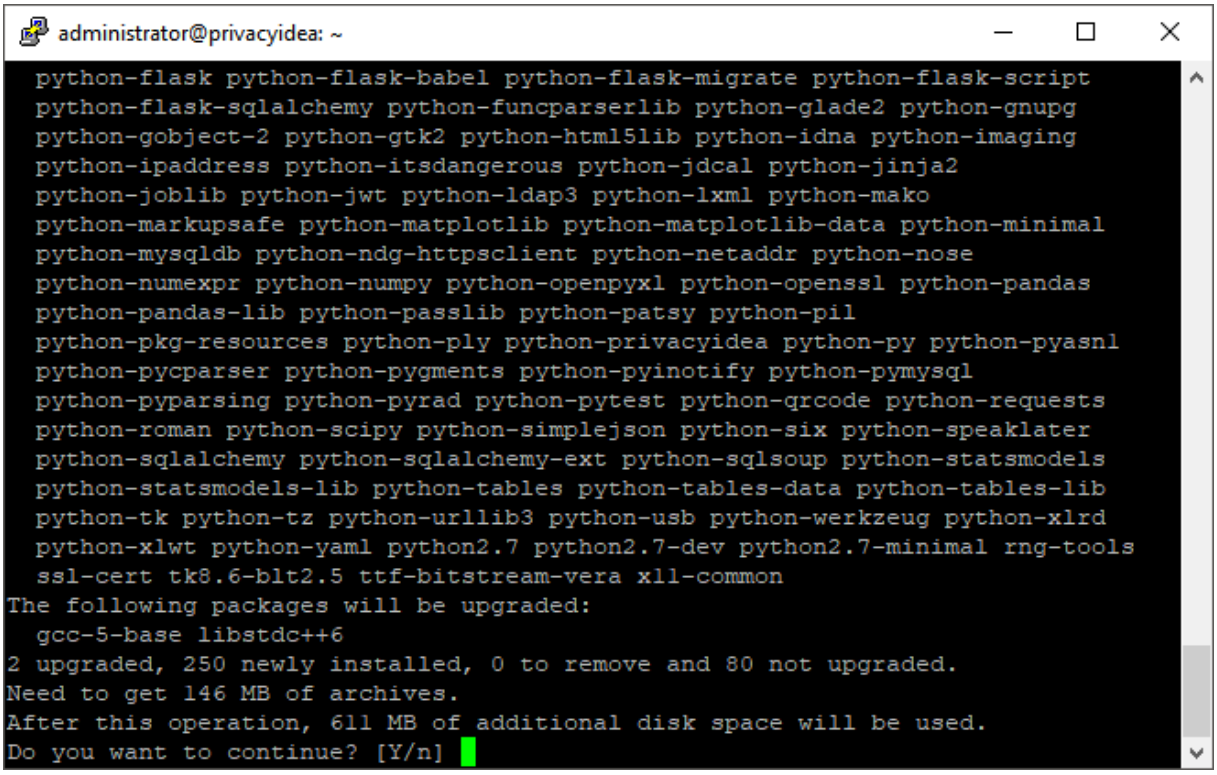
Command: sudo apt-get update



2.3. Installation von privacyIDEA

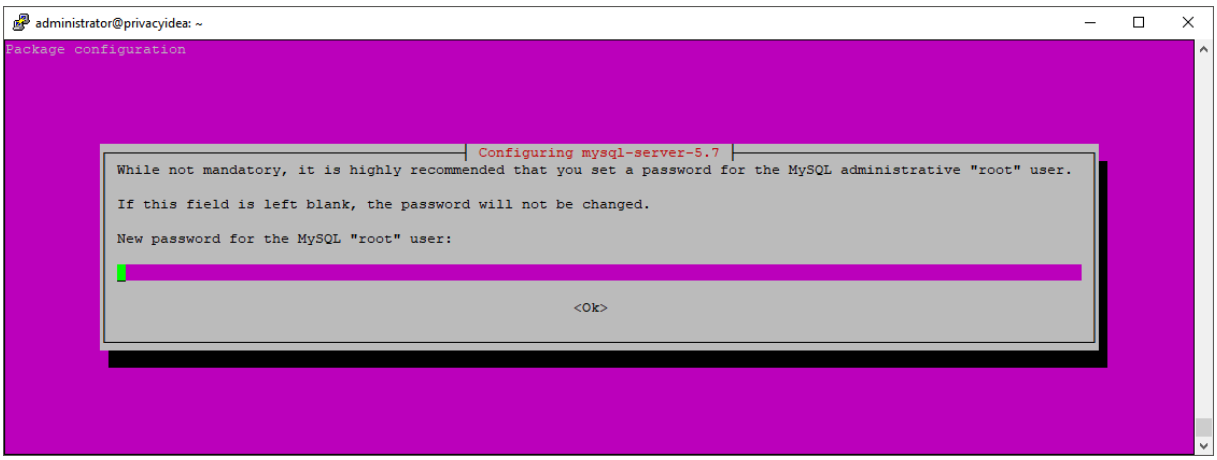
Nun starten wir die Installation mit folgendem Kommando.

Command: sudo `apt-get install privacyIDEA-apache2`

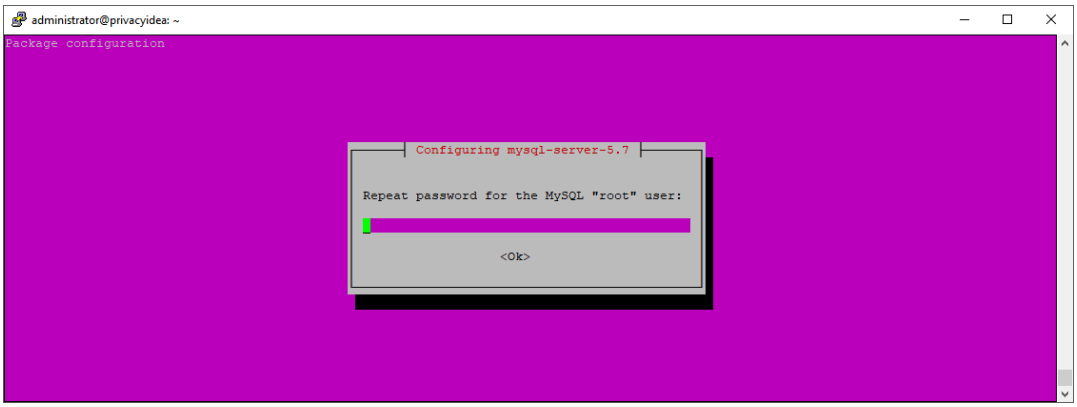


Benötigte Komponenten wie z.B. Apache Webserver oder MySQL Datenbank werden während der Installation automatisch installiert. Jedoch sind einige Eingabe erforderlich.

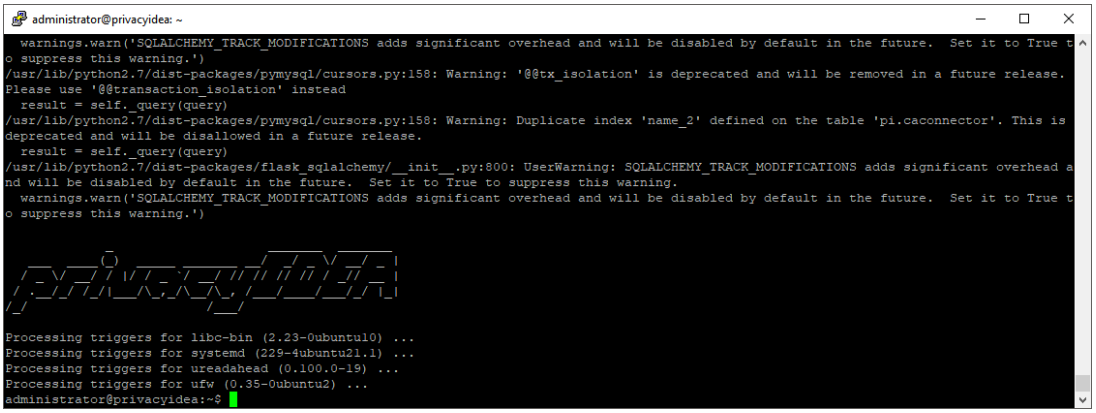
Vergeben Sie nun das Passwort für den MySQL Root Account:



Bestätigen Sie dies durch nochmalige Eingabe:



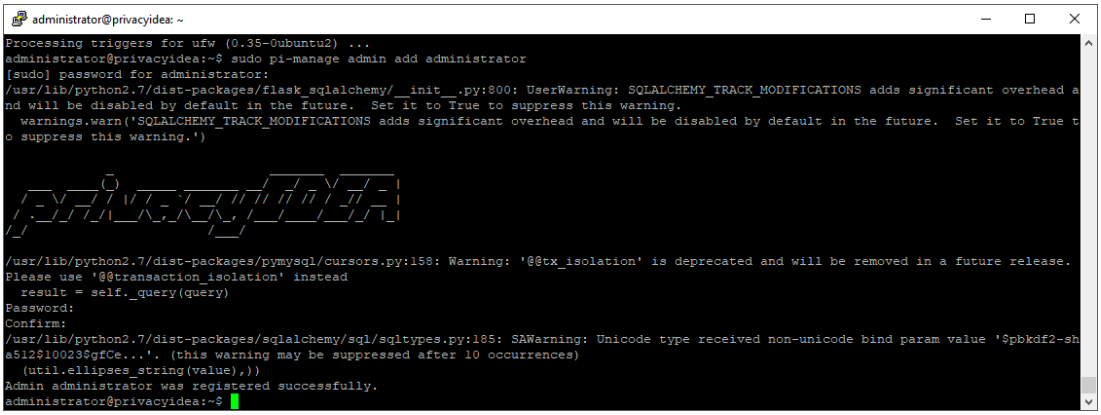
Wurde die Installation erfolgreich abgeschlossen Sollten Sie wie im unteren Screenshot gezeigt aussehen.



2.4. Administrator Account hinzufügen

Damit Sie sich an privacyIDEA anmelden können, müssen Sie nun noch den Benutzeraccount hinzufügen. Wichtig dieser muss auf dem lokalen System (Ubuntu Betriebssystem) vorhanden sein. In unserem Fall fügen wir den „administrator“ Benutzer hinzu und geben die Rolle „Admin“.

Command: sudo pi-manage admin add administrator



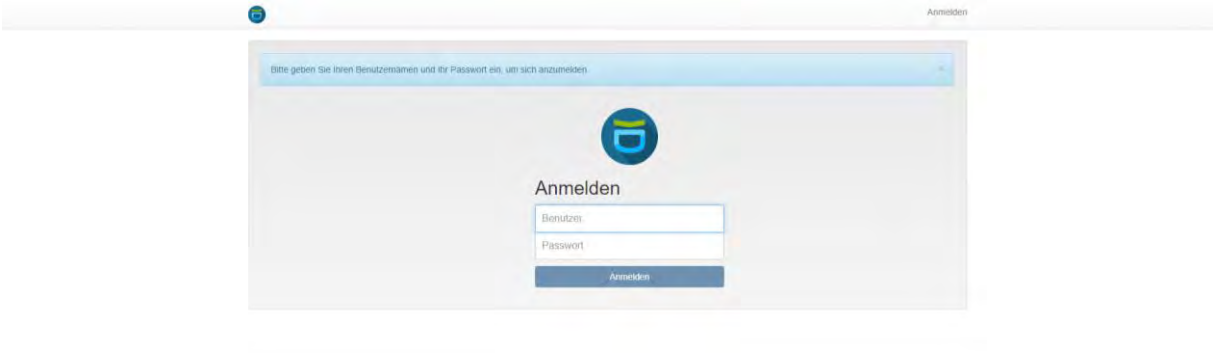
2.5. Ereichbarkeit des Webinterface testen

Nun können wir schonmal einen ersten Blick auf das Webinterface werfen. So stellen wir sicher das der Server über HTTP/HTTPs erreichbar ist und die Anmeldung mit dem zuvor hinzugefügten Benutzer funktioniert. Öffnen Sie einen Browser Ihrer Wahl (am Besten Chrome oder Firefox).

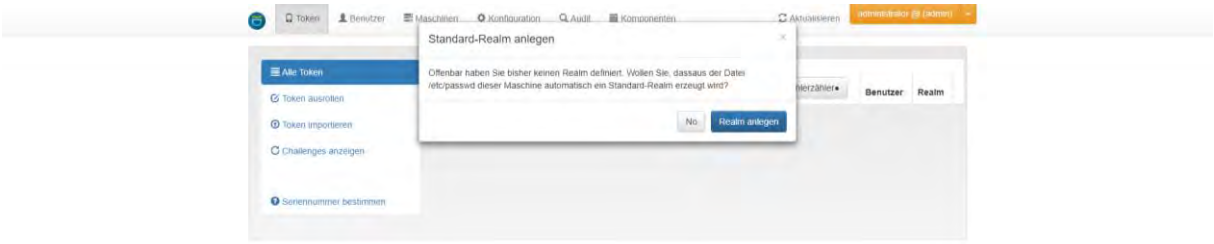
URL: https://ip-address oder https://fqdn

Benutzer: administrator

Password: bei der Installation des Betriebssystem gewähltes



War die Anmeldung erfolgreich, sollte Sie einen Assistenten und den Startbildschirm von privacyIDEA sehen.

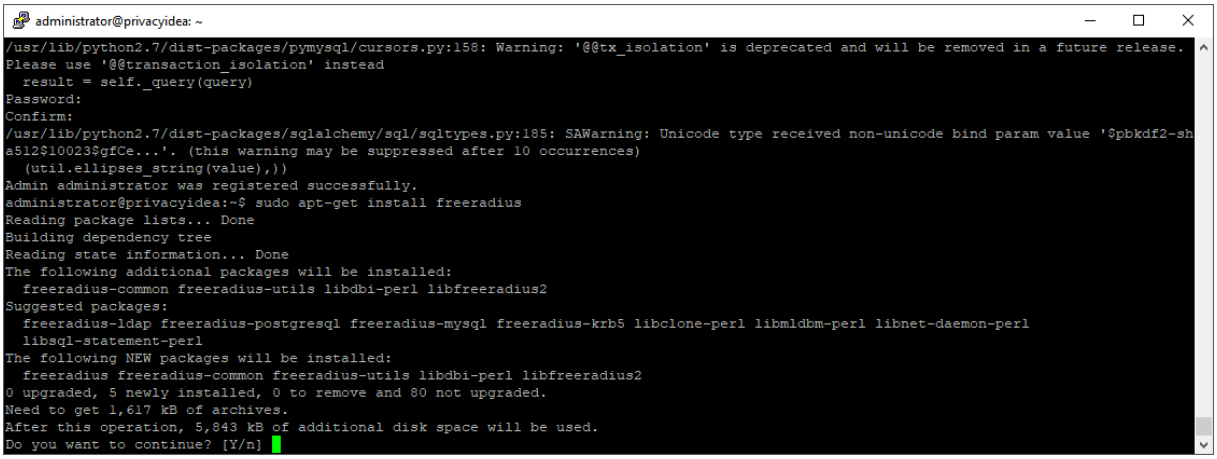


2.6. FreeRadius installieren

privacyIDEA ist in erster Linie ein Authentifizierungsframework, d.h. es kann mit vielen unterschiedlichen Protokollen (Radius, die Authentifzierung und Authorisierung durchführen. Damit privacyIDEA mit einem Radius kommunizieren kann, benötigt es einen Radius Server. In unserem Fall verwenden wir den OpenSource Radius Server: FreeRadius.

Diesen installieren wir mit folgendem Kommando

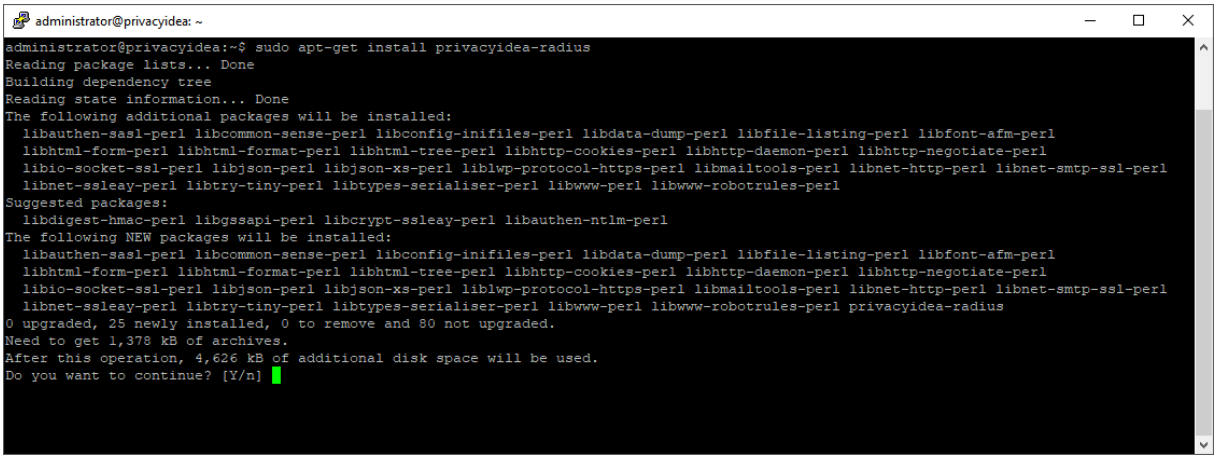
Command: sudo apt-get install freeradius



2.7. privacyIDEA Radius Plugin installieren

Ist der Radius Server installiert, muss nun noch das privacyIDEA Plugin installiert warden. Hierbei wird auch bereits eine Grundkonfiguration von einige Konfigurationdateien für FreeRadius durchgeführt.

Command: sudo apt-get install privacyIDEA-radius



2.8. Konfigurieren von FreeRadius

Damit FreeRadius Anfragen von externen Client (z.B. eine Firewall) akzeptiert, muss dies noch in der Radius Konfiguration eingestellt werden. Für weitere Informationen zur Konfiguration von FreeRadius oder dem privacyIDEA Plugin für FreeRadius finden Sie hier:

FreeRadius: https://wiki.freeradius.org/config/Configuration-files

FreeRadius Plugin: http://privacyIDEA.readthedocs.io/en/latest/application_plugins/rlm_perl.html#rlm-perl

In unserem Beispiel passen wir nur die Clients.conf Konfigurationsdatei an

Command: sudo nano /etc/freeradius/clients.conf

Fügen Sie den Localhost und die Systeme (z.B. Firewall) hinzu, welche mit FreeRadius kommunizieren sollen. In unserm Beispiel fügen wir das gesamte Netzwerk hinzu (172.17.7.0/24). Bitte wählen Sie ein sicheres Passwort als Secret.

client localhost {

secret = myownsecret

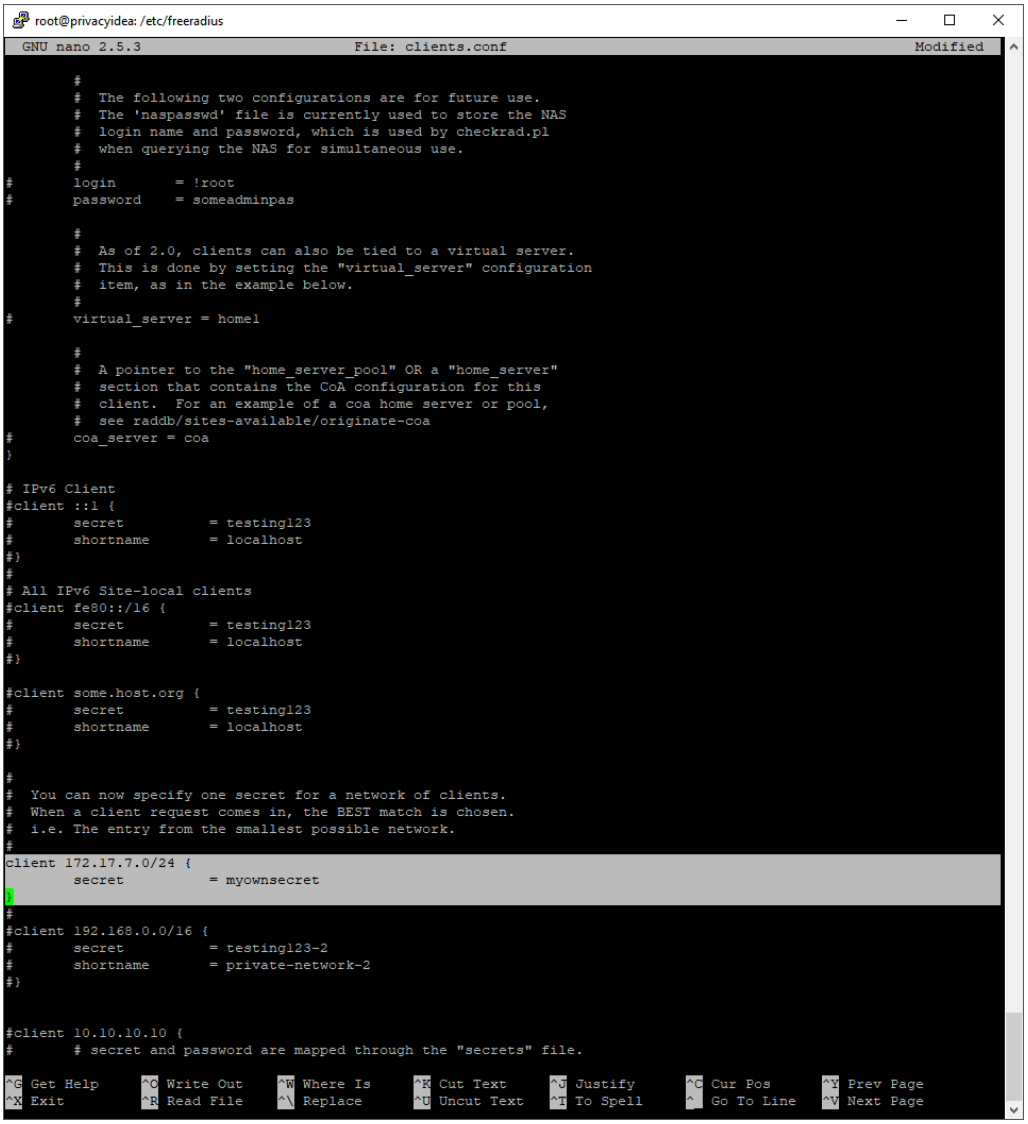
}

und

client 172.17.7.0/24 {

secret = myownsecret

}



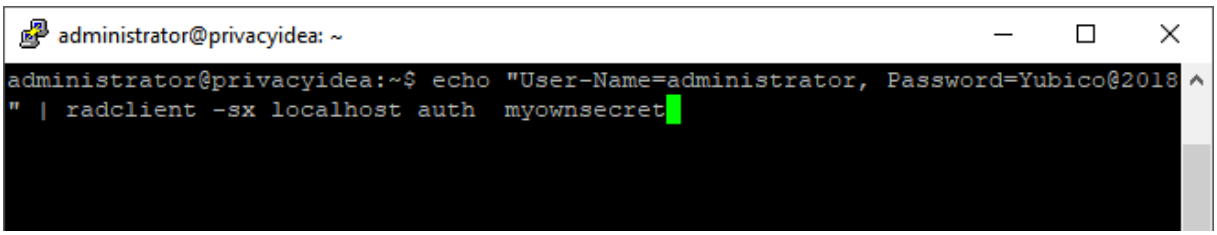
Damit die neue Konfiguration angewendet wird, müssen Sie den FreeRadius Server neustarten.

Command: service freeradius restart

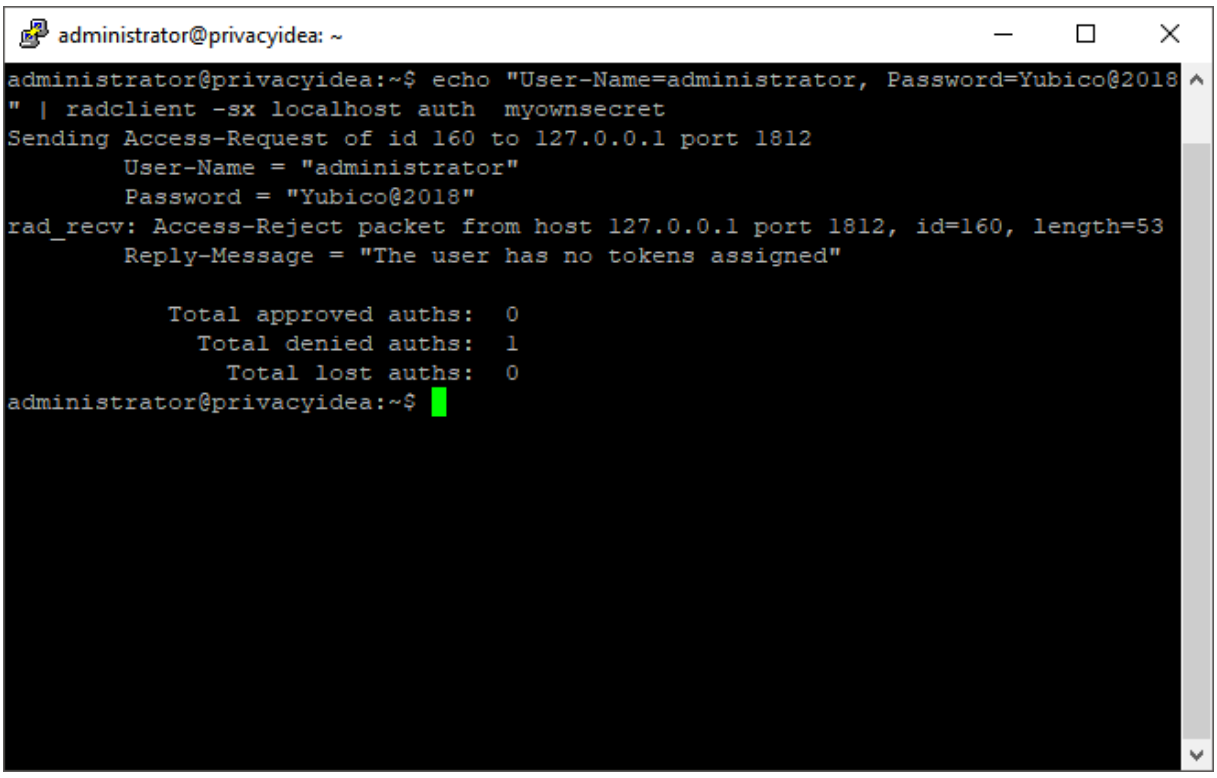
2.9. Testen von FreeRadius und privacyIDEA kommunikation via radclient

Nun können wir bereits anfangen die Radius Authentifzierung gegen das privacyIDEA Backend zu testen. Dies dient einerseits zu sehen ob der Radius Server auf Anfragen antwortet, sowie ob die Anfrage an privacyIDEA weitergeleitet wird.

Command: echo "User-Name=administrator, Password=Yubico@2018" | radclient -sx localhost auth myownsecret

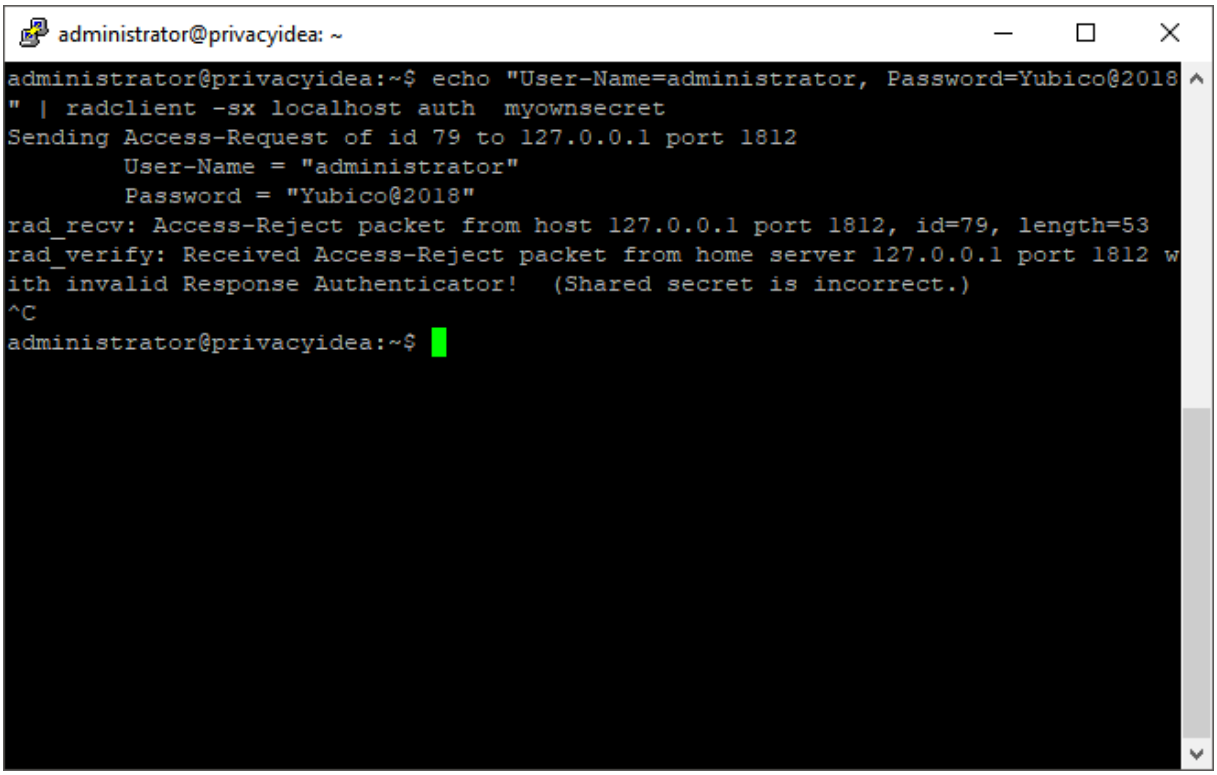


Wenn das Senden der Anfrage an den Radius Server, sowie das weiterleiten erfolgreich war, erhalten Sie folgene Meldung:



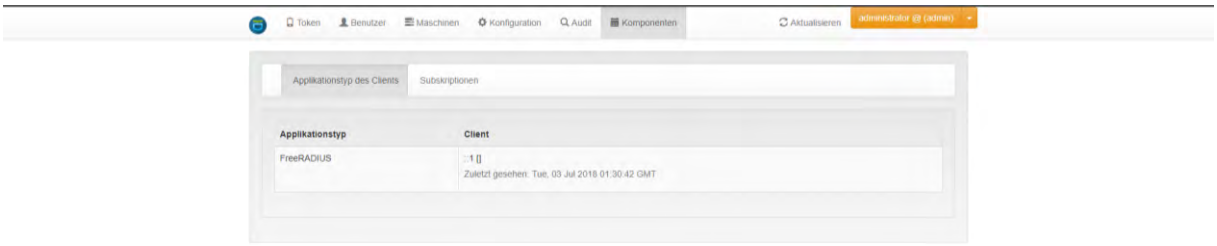
Bitte lassen Sie sich nicht von einer fehlgeschlagenen Authentifzierung irritieren, da dies ein normales Verhalten ist, solang wir keinen Token (Yubikey) dem Benutzer zugewiesen haben.

Sollte die Clients.conf falsch sein, d.h. z.b. Secret ist falsch, dann erhalten Sie folgende Meldung:



Sollte der Radius Server nicht auf Anfragen von der IP Addresse reagieren, erhalten Sie ein Connection Timeout Fehler.

Sobald die Anfragen erfolgreich bearbeitet und weitergeleitet werden, sehen Sie den Radius Server im privacyIDEA Webinterface unter -> Komponenten – Applikationstyp des Clients



Haben Sie den FreeRadius mit privacyIDEA Plugin erfolgreich getestet, können Sie mit Kapitel 3 fortfahren.

3. Konfiguration privacyIDEA – Active Directory Anbindung

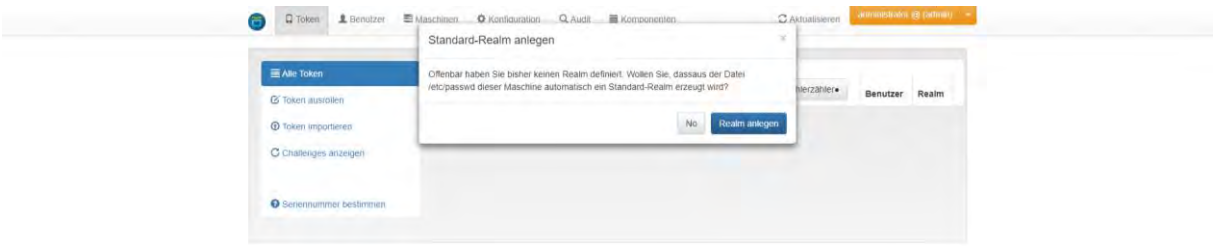
In unserer Beispielumgebung möchten wir erreichen das sich Benutzer mit Ihrem Active Directory Benutzernamen, dem Passwort und einem OTP (One Time Password) anmelden müssen. Damit privacyIDEA die Information des Active Directory erhält muss dies über einen sogenannten Realm und Resolver

3.1. Standard Realm anlagen

Ein Realm in privacyIDEA ist vergleichbar mit einem Bereich oder ferner „Domäne“, gegen den authentifiziert wird. Innerhalb eines Realms können mehrere externe Quellen (z.B. Active Directory) angegeben werden. Ein unterscheidet hierbei gegen welche externe Quelle der anzumeldende Benutzer authentiziert wird. Es gibt einen Standard/Default Realm, mit dem die Benutzer nicht mit Ihrem Benutzernamen anmelden können. Ist ein Benutzer nicht im Standard Realm, muss der Benutzer sich mit benutzername@realmname anmelden.

Sind mehrere externe Authentifizierungsquellen in einem Realm angelegt, werden diese nach einander bis zu einer erfolgreichen Anmeldung durchgegangen.

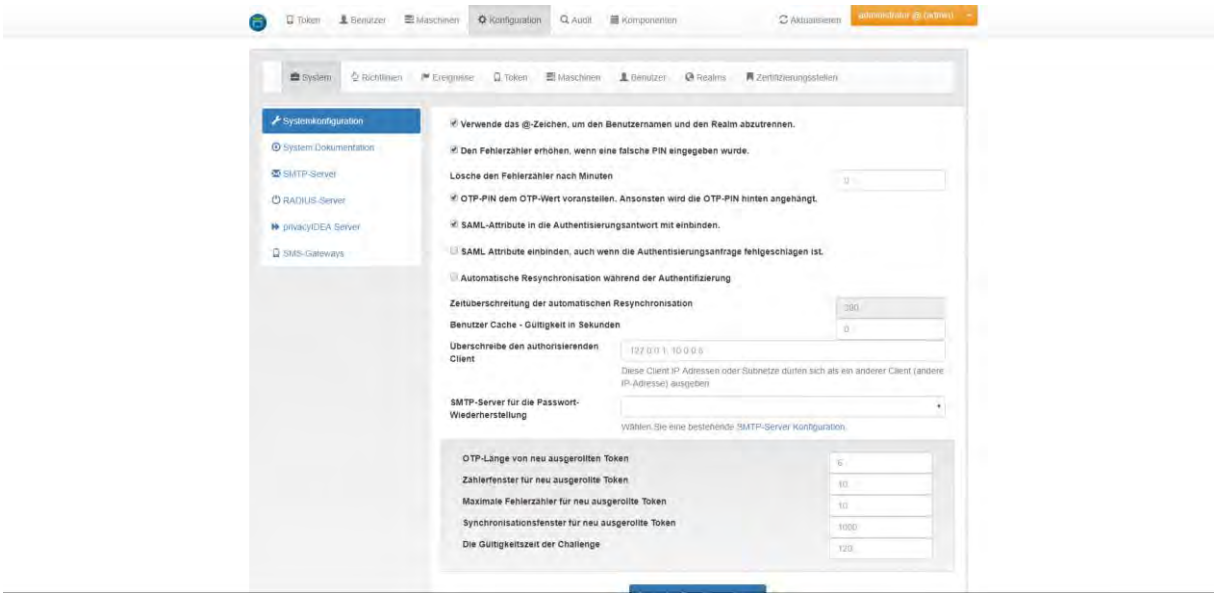
Der Assistent im privacyIDEA Webinterface legt automatisch einen Standard Realm an.



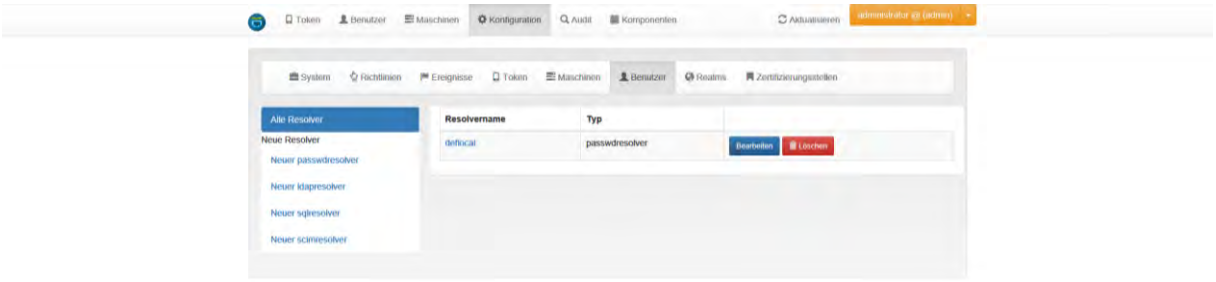
3.2. ActiveDirectory Resolver anlagen

Der Standard Realm wird angelegt um gegen lokale auf dem Linux Betriebssystem vorhandene Benutzer zu authentifizieren. Damit wir gegen einen existierenden Verzeichnisdienst authentifzieren können, legen wir nun einen Active Directory Resolver an. Ein Resolver beschreibt das externe Backend an den die Authentifzierung weitergeleitet wird.

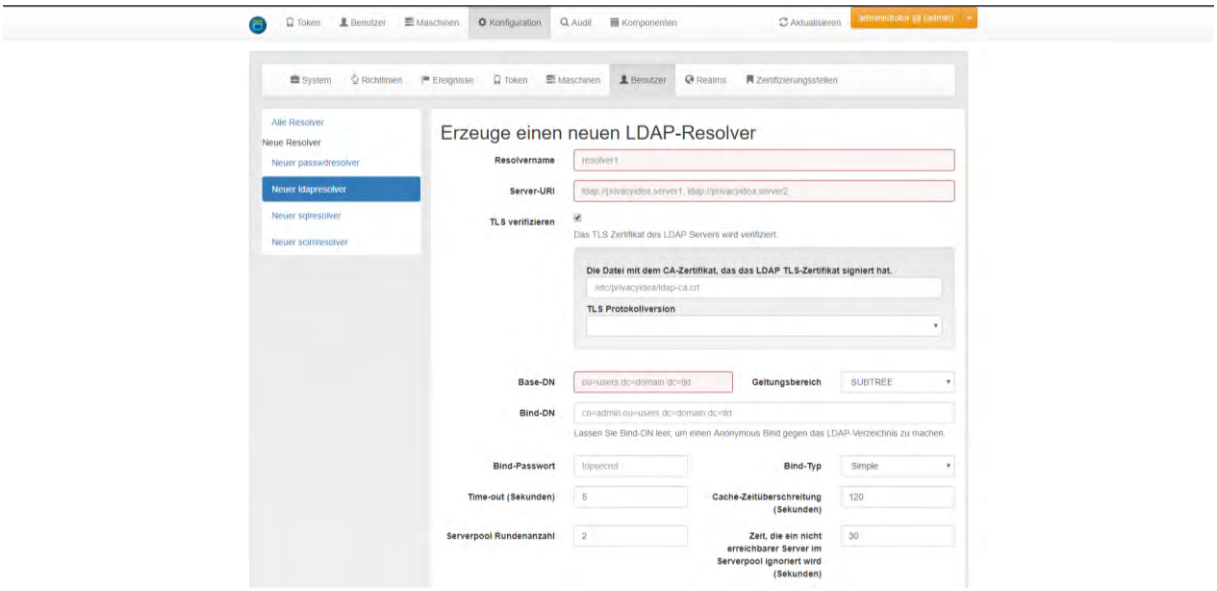
Klicken Sie auf Konfiguration



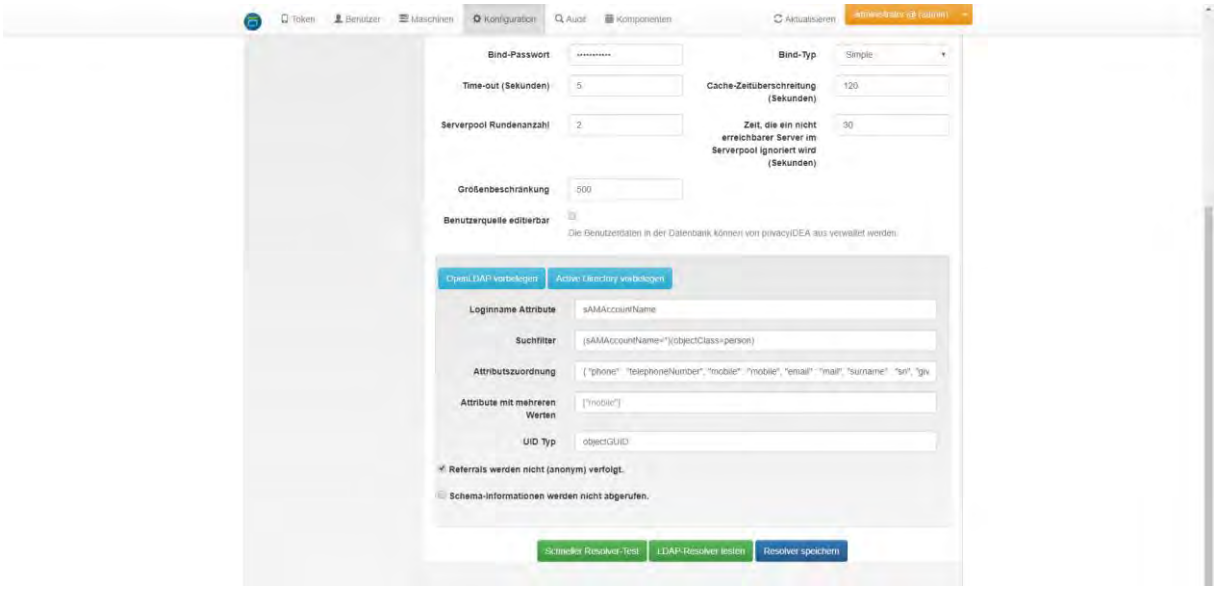
Klicken Sie auf Resolver



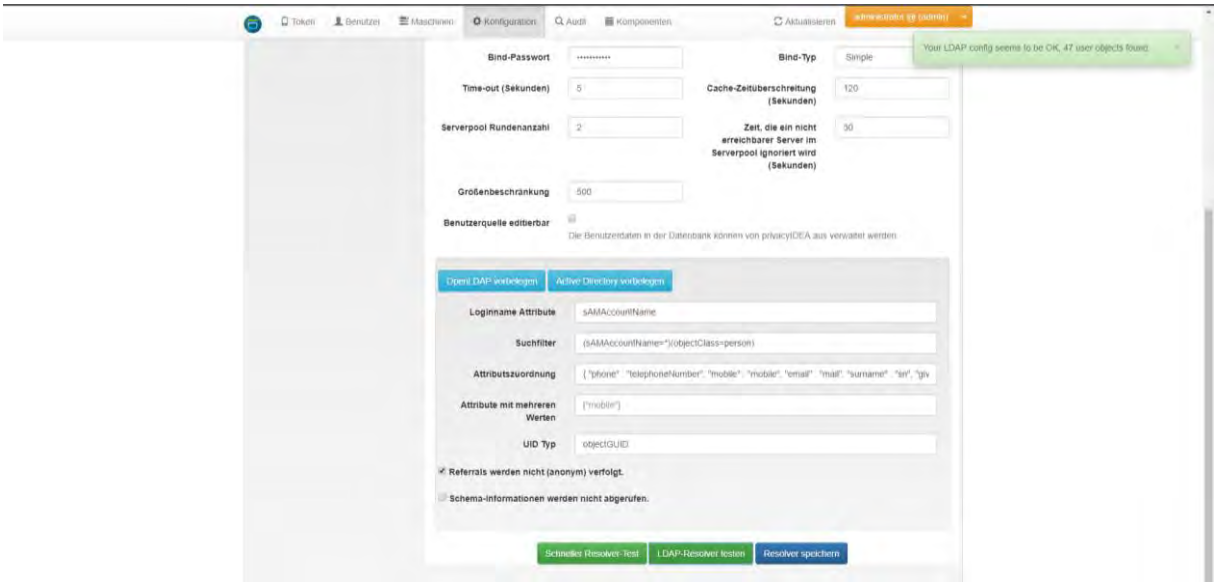
Klicken Sie nun auf „Neuer LDAPResolver“



Konfigurieren Sie nun den Resolver mit den Parametern Ihres Active Directory. Hierzu ist ein LDAP Browser (z.B. ADSI Edit oder Softerra LDAP Browser - https://www.ldapadministrator.com/download.htm?download=browser) empfehlenswert, um Parameter wie Base DN und Bind zu ermitteln. Bitte verwenden Sie als Benutzer den zuvor angelegten Service Account aus Kapitel 1, Absatz 7.



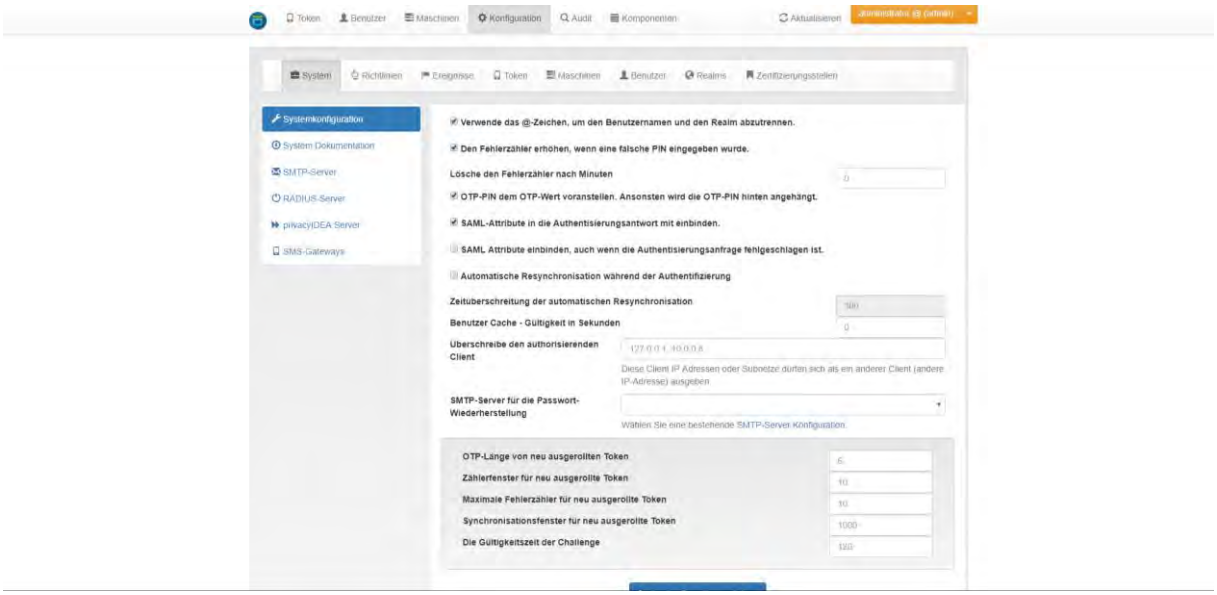
Nach Eingabe der Parameter können Sie die Verbindung mit Ihrem Active Directory testen.



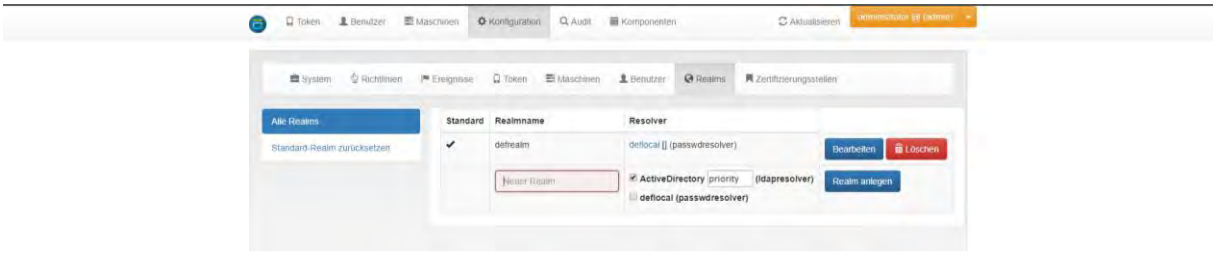
3.3. Neuen Realm anlagen

Wir haben nun den Resolver für unser Active Directory angelegt, jedoch noch nicht einem Realm hinzugefügt. In unserem Beispiel legen wir einen neue Realm für die Active Directory.

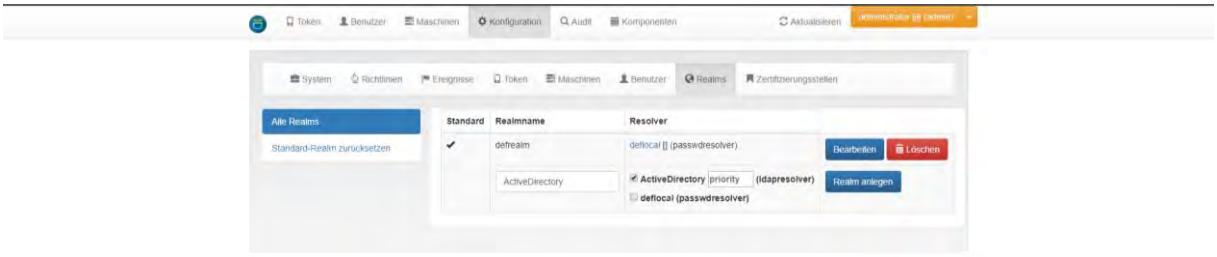
Klicken Sie auf Konfiguration



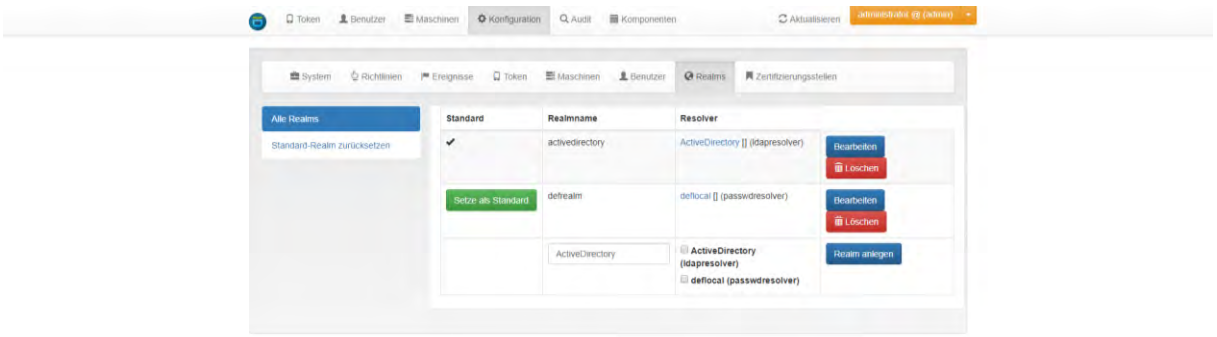
Vergeben Sie einen Namen und wählen Ihren ActiveDirectory Resolver aus



Klicken Sie nun auf Realm anlegen

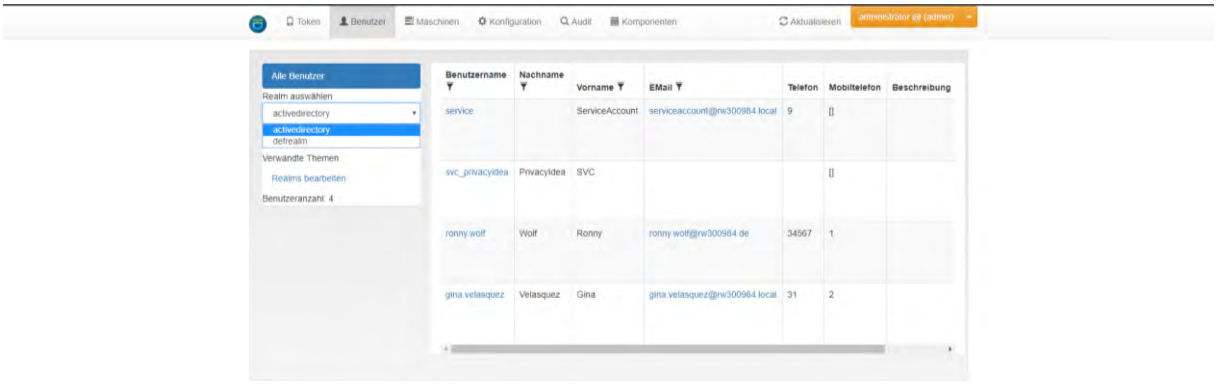


Damit unsere Benutzer nicht benutzername@realm eingeben müssen, empfiehlt es sich den neu angelegten Realm, als Standard Realm zu setzen.



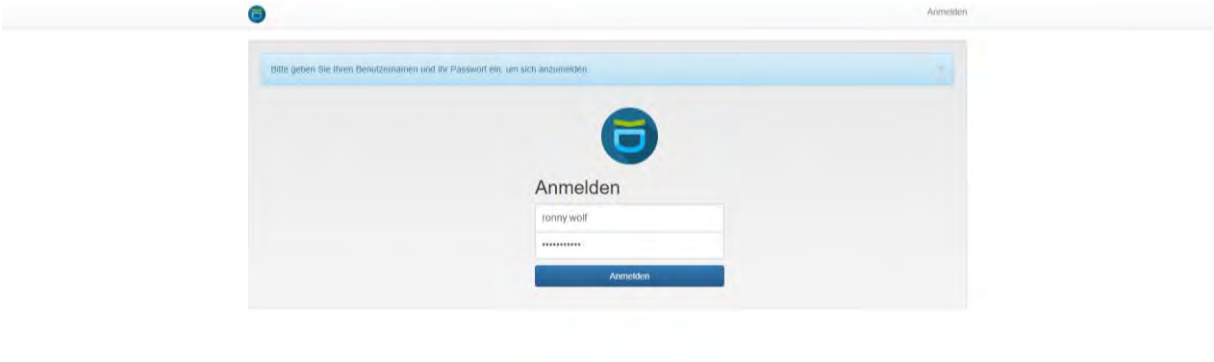
3.4. Überprüfen ob Benutzer in privacyIDEA angezeigt werden

Nun werden uns die Benutzer im privacyIDEA – Benutzer Interface angezeigt. Eventuell müssen Sie auf der rechten Seite den entsprechenden Realm auswählen.



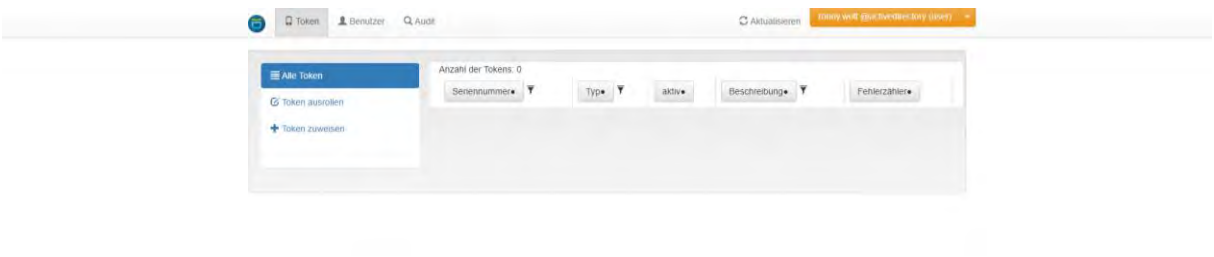
3.5. Überprüfen ob Anmeldung mit Benutzer möglich ist

Da die Benutzerauthentifzierung nicht nur für Radius und andere externe Services gilt, können wir nun mit einem Demo Benutzer uns an das Webinterface (Self Service) von privacyIDEA anmelden.



Bitte verwenden Sie hier den Active Directory Benutzername und das entsprechende Passwort.

War die Authentifizierung erfolgreich, sehen Sie nun ein Webinterface mit beschränkten Rechten, d.h. Benutzer können standardmässig einen neuen Token für sich ausrollen und Ihre eigenen Protokolle (Audit) sehen.



Soll dies eingeschränkt werden, kann dies über die privacyIDEA Richtlinien durchgeführt werden. Hierzu konsultieren Sie bitte das privacyIDEA Handbuch, da wir in diesem Guide nicht detailiert darauf eingehen.

4. Konfiguration privacyIDEA – Richtlinien und Ereignisse

In privacyIDEA wird über Richtlinien definiert, wie sich das System verhalten soll bei Authentifzierungen oder Authorisierungen, aber auch welche Rechte Benutzer haben oder welche Token (z.B. nur Yubikey) diese ausrollen können. Weitere Informationen über Richtlinien finden Sie hier:

https://privacyIDEA.readthedocs.io/en/master/policies/index.html

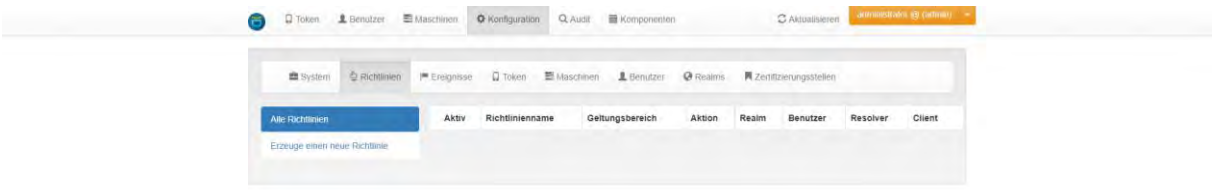
Darüber hinaus können Sie Ereignisse definieren. Diese Beschreiben was nach einem bestimmte Event (Ereignis) passieren soll z.B. wenn eine Benutzerauthentifzierung fehlgeschlagen ist. Weitere Informationen zu Ereignissen finden Sie hier:

https://privacyIDEA.readthedocs.io/en/master/eventhandler/index.html

4.1. Erstellen einer Richtlinie für Active Directory Passwort + OTP

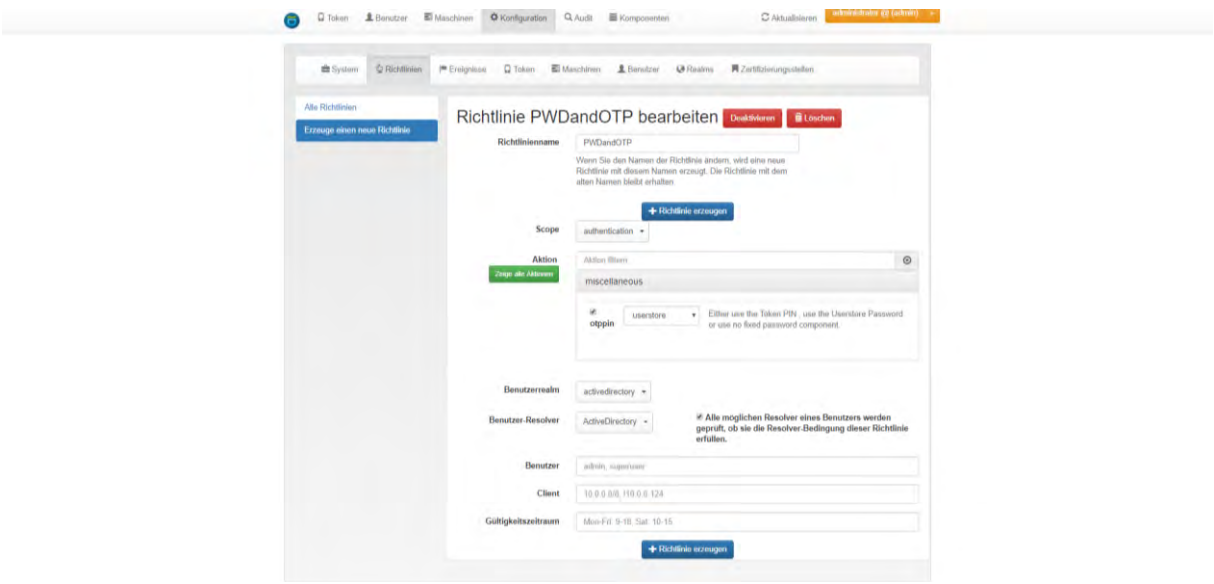
In unserem Beispiel wollen wir definieren wir eine Richtinie, welche das Active Directory Passwort und einen OTP erfordert. Ist diese Richtlinie nicht definiert, müssen sich Benutzer mit einer Token Pin (wird beim Ausrollen vergeben) und dem OTP anmelden.

Hierzu klicken wir auf Konfiguration - Richtlinien



Legen Sie nun eine Richtlinie an

Richtlinienname: frei wählbar
Scope: Authentication
Aktion: OTPPin
Wert: Userstore
Benutzerrealm: Active Directory
Benutzerresolver: Active Directory



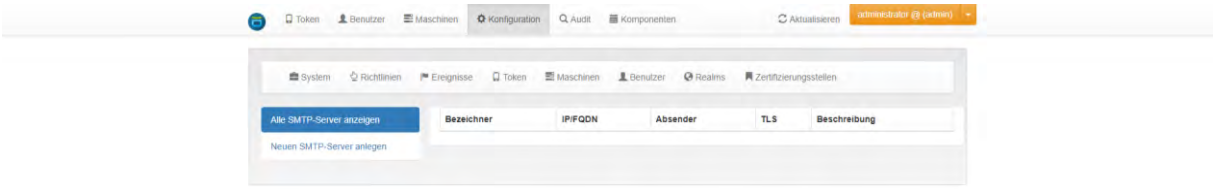
Nun ist es erforderlich das Benutzer sich mit Active Directory und OTP anmelden, da der Wert Userstore bedeutet das wir die Authentifzierung an den Realm/Resolver schicken. Die Eingabe bei den meisten System (z.B. die im Guide vorstellten Firewalls)erfolgt hier:

Benutzername: Active Directory Benutzername
Passwort: adpasswordotp (Active Directory Passwort und OTP werden direkt hintereinander eingeben)

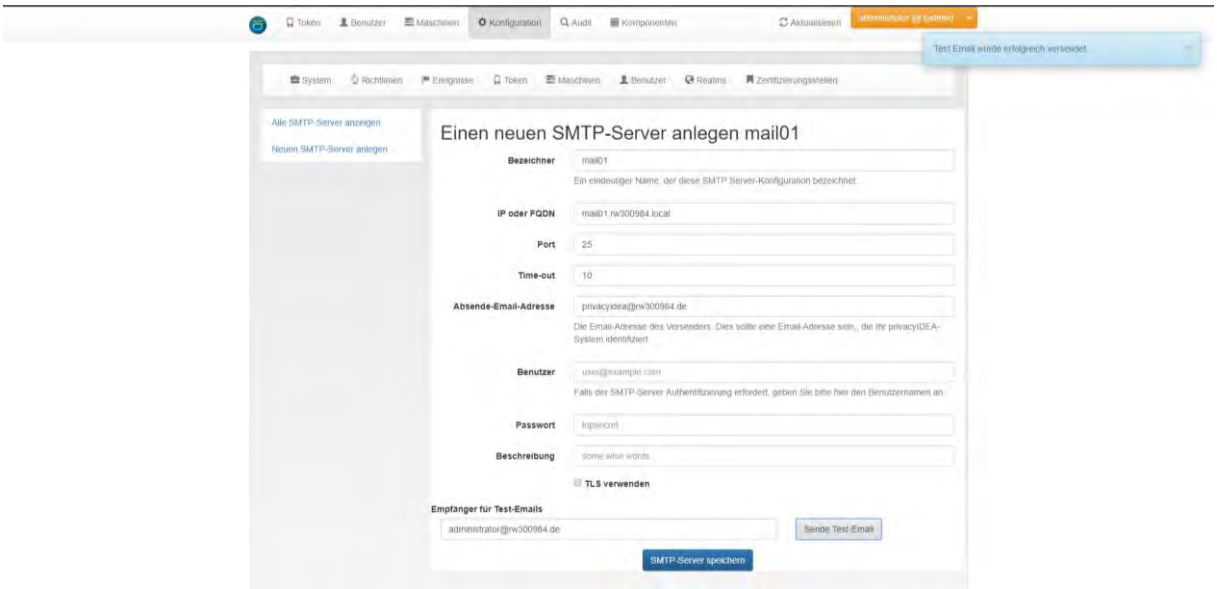
4.2. Hinzufügen eines SMTP Servers für Benachrichtigungen

Damit unsere Administratoren über fehlgeschlagene Anmeldungen via Email informiert werden können, müssen wir noch einen Email Server definieren.

Klicken Sie auf Konfiguration – System – SMTP Server



Klicken Sie nun auf neuen SMTP Server anlegen und konfigurieren die Parameter. Nun können Sie die Einstellungen testen. War dies erfolgreich sollten Sie eine Testemail von privacyIDEA in Ihrem Email Postfach vorfinden.

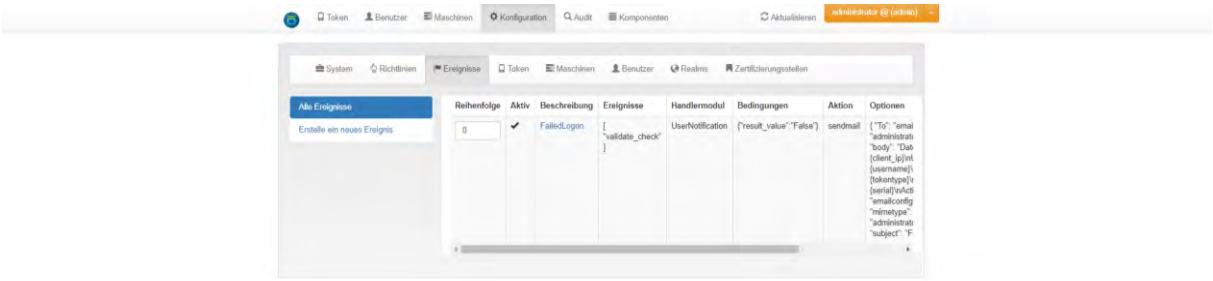


War der Email Server Test erfolgreich, können wir die Konfiguration abspeichern.

4.3. Hinzufügen einer Ereignisregel (Benachrichtigung bei fehlerhaften Anmeldungen)

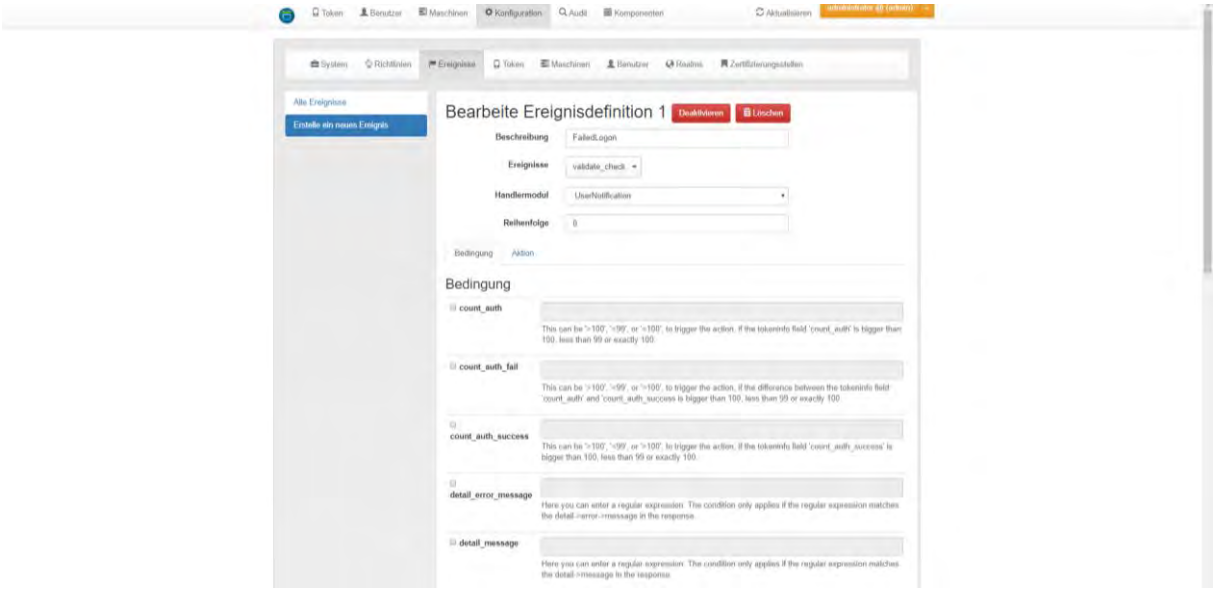
Da in privacyIDEA keine Ereignisregel definiert sind, erhalten wir keine Benachrichtigung für fehlgeschlagene Anmeldungen. Um eine E-Mail Benachrichtigung zu erhalten müssen wir ein neues Ereignis definieren.

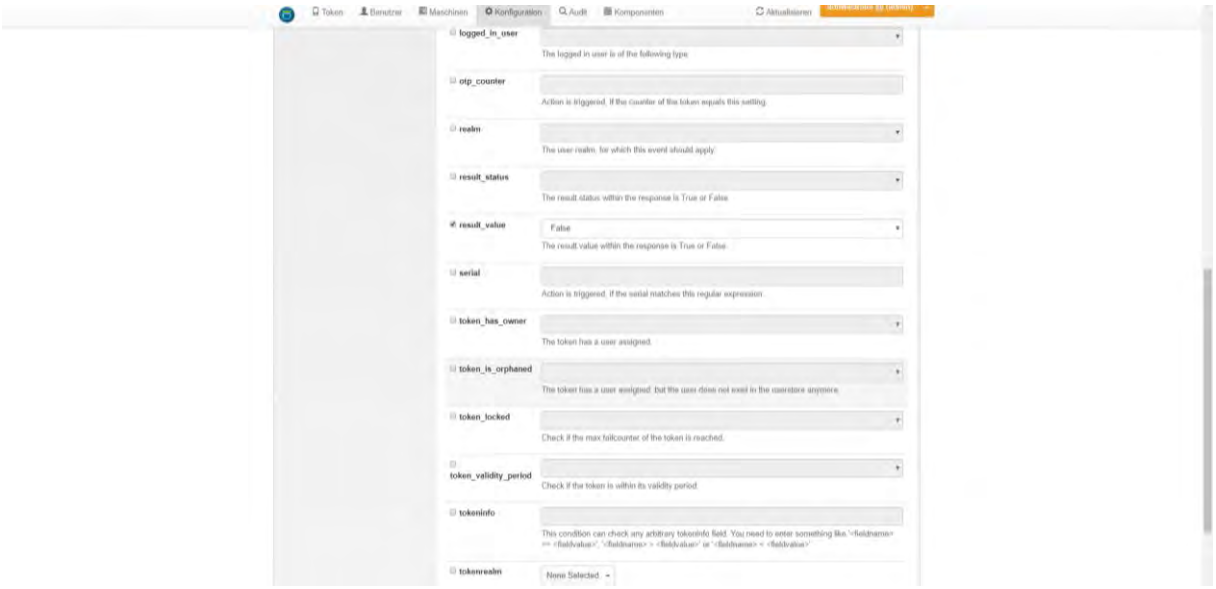
Klicken Sie auf Konfiguration - Ereignisse



Erstellen Sie nun eine neue Regel

Beschreibung: frei wählbar
Ereignisse: validate_check
Handlermodule: UserNotification
Reihenfolge: 0
Bedingung: result_value
Wert: false





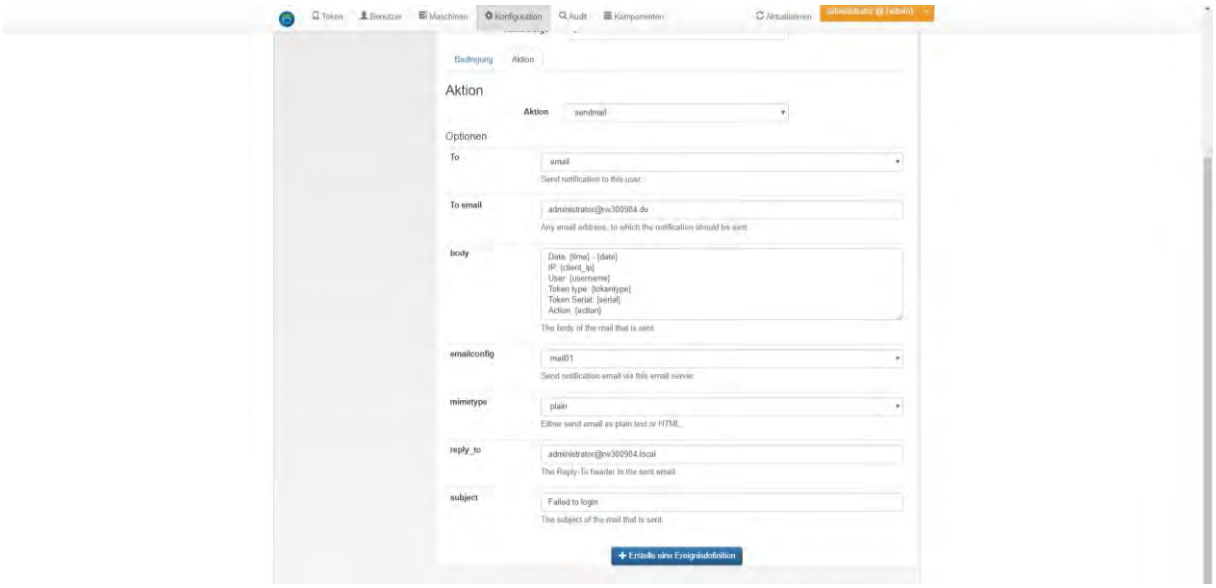
Neben der Bedingung für das Ereignis, muss nun auch eine Aktion erfolgen. In unserem Beispiel möchten wir eine Email Benachrichtigung erhalten.

Klicken Sie auf Aktion

Aktion: sendmail
To: email
To email: administrative Emailaddresse
Body: wie in unterem Screenshot gezeigt
Emailconfig: Ihr konfigurierter SMTP Server aus Kapitel 4, Abschnitt 2.
Reply to: frei definierbare Rückantwort Emailaddresse
Subject: frei definierbar

Hinweis: Weitere Variablen finden Sie hier:

https://privacyIDEA.readthedocs.io/en/master/eventhandler/usernotification.html)



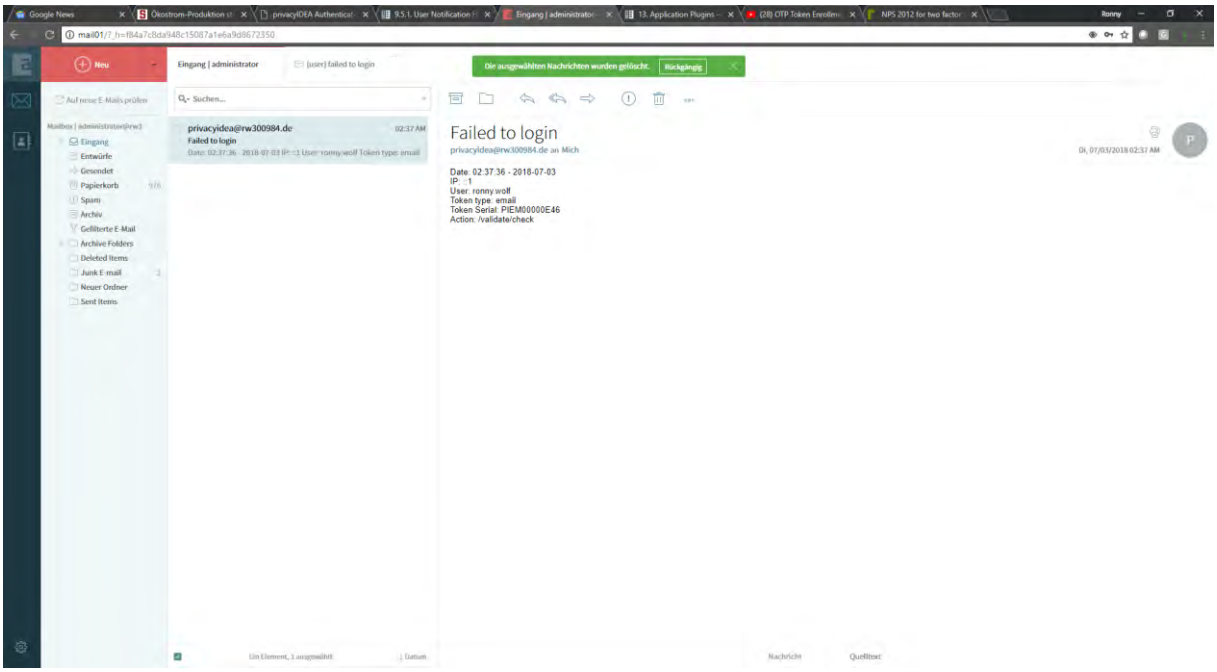
Speichern Sie nun das neue Ereignis ab.

Da wir noch keine Token einem Benutzer zugewiesen haben, werden alle Authentifzierungen fehlschlagen, d.h. wir können mit einem Benutzer direkt die Benachrichtigung testen.

Hierzu können wir direkt auf dem privacyIDEA Server mit folgendem Kommand die Authentifizierung testen:

Command: echo "User-Name=administrator, Password=Yubico@2018" | radclient -sx localhost auth myownsecret

Wechseln Sie nun in das Postfach des administrativen Benutzers, welches die Benachrichtigung erhalten soll und überprüfen ob Sie eine Email von privacyIDEA erhalten haben.



Nun sind wir mit den Basis Konfigurationen in privacyIDEA fertig und können neue Tokens ausrollen. Einige weitere Konfigurationen für privacyIDEA finden Sie unter Kapitel 5 in diesem Guide. Diese sind jedoch optional und nicht zwingend erforderlich. Möchten Sie keine zusätzlichen Konfigurationen durchführen fahren Sie mit Kapitel 6 fort.

5. Zusätzliche Konfigurationen (optional)

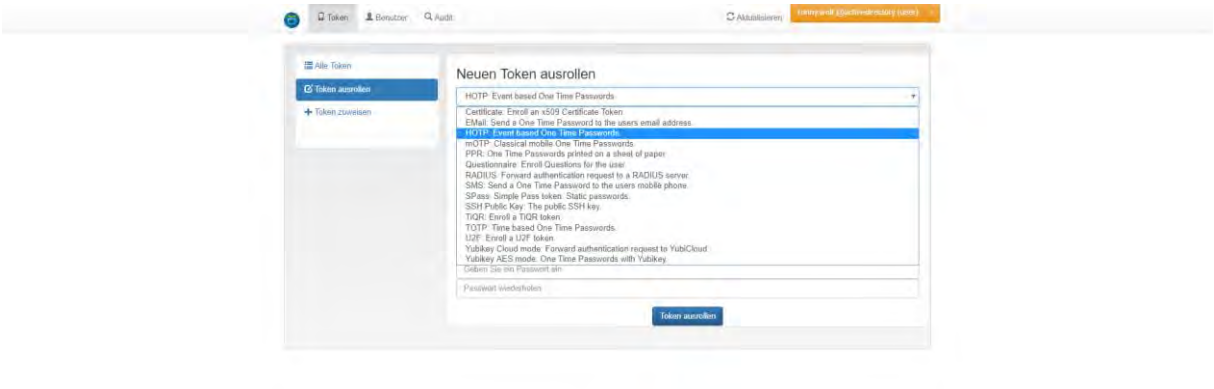
privacyIDEA hat sehr viele Möglichkeiten, die Anforderungen von Kunden zu erfüllen. Einen kleinen Teil von zusätzlichen Konfigurationen möchten wir Ihnen hier vorstellen.

5.1. Richtlinie für Self Enrollment auf bestimmte Tokentypen einschränken

Standardmässig gibt es für Benutzer keine Einschränkung welche Token ausgerollt werden können. In der Regel möchten Unternehmen jedoch sicherstellen das sich nur mit einem bestimmten Typ von Tokens authentifziert wird.

Dies dient einerseits der Übersicht für den Benutzer (Usability) und der Sicherheit (z.B. nur Hardware Token) und erleichtert die Verwaltung des Systems.

Per Default sieht die Auswahl der auszurollenden Tokens wie folgt aus:

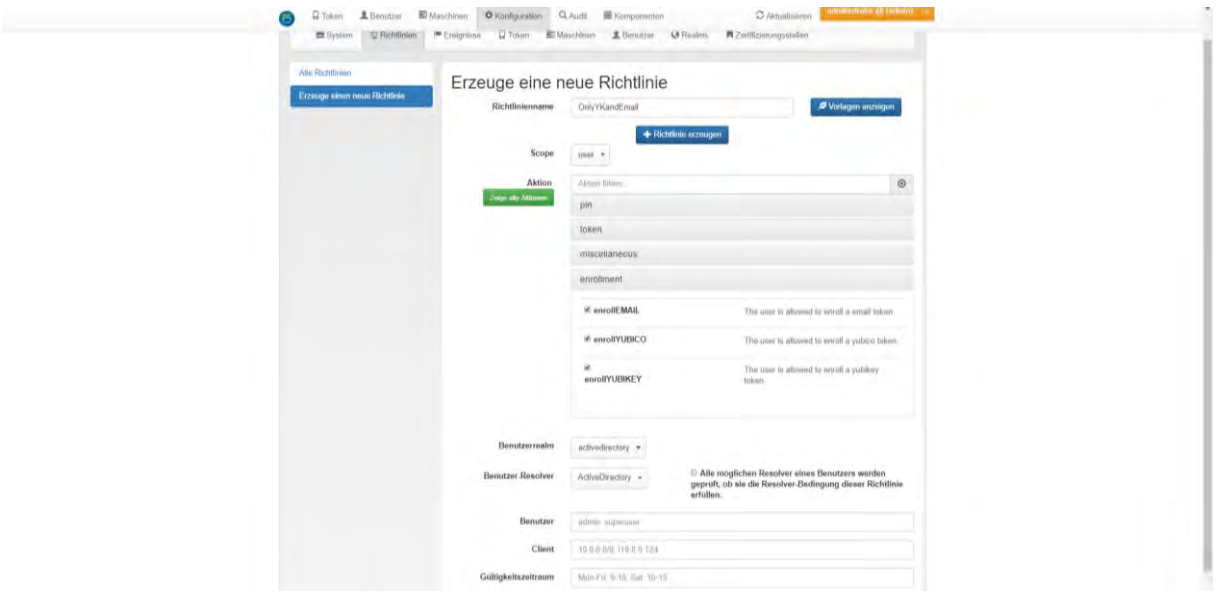


Damit wir diese Auswahl einschränken können, erzeugen wir eine neue Richtlinie. In unserem Beispiel wollen wir nur Yubikeys und falls nicht verfügbar einen Email OTP erlauben.

Klicken Sie auf Konfiguration - Richtlinien

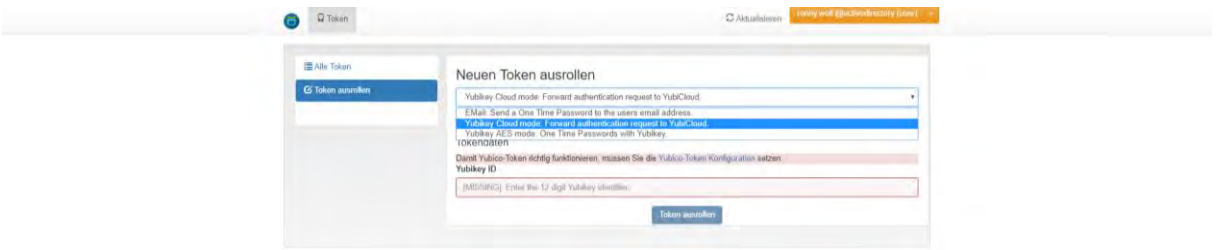
Erstellen Sie folgende Richtlinie:

Richtlinienname: frei wählbar
Scope: User
Aktion: Enrollment
Wert: enrollEmail = aktiviert
enrollYubico = aktiviert
enrollYubikey = aktiviert
Benutzerrealm: Active Directory
Benutzer Resolver: Active Directory



Speichern Sie nun die neue Richtlinie ab.

Wenn Sie sich nun mit einem Benutzer anmelden und einen Token ausrollen möchten, erhalten Sie folgende limitierte Auswahl:



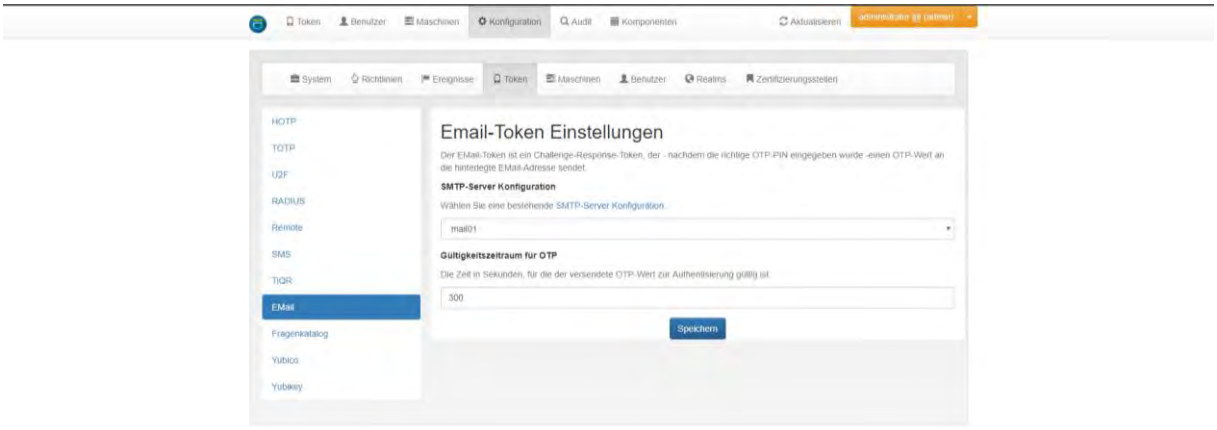
5.2. E-Mail Token Konfiguration, Ausrollen und Testen

Da wir in Kapitel 5, Abschnitt 1, auch Email Tokens für Benutzer freigegeben haben, müssen Sie diese nun noch konfigurieren, ausrollen und testen.

E-Mail Tokens eignen sich besonders in der Testphase sollte der Kunde noch keine Hardware Token (Yubikeys) haben oder aber als Fallback, sollte der Benutzer seinen Hardware Token vergessen haben. Die Sicherheit, als auch die Zuverlässigkeit von E-Mail Tokens in beschränkt, da einerseits E-Mail potentiell von Dritten gelesen werden können, als auch der E-Mail Token von einem AntiSpam System blockiert wird. Wir empfehlen dies nicht als Primäre Authentifzierungsmethode!

Klicken Sie auf Konfiguration – Token – Email

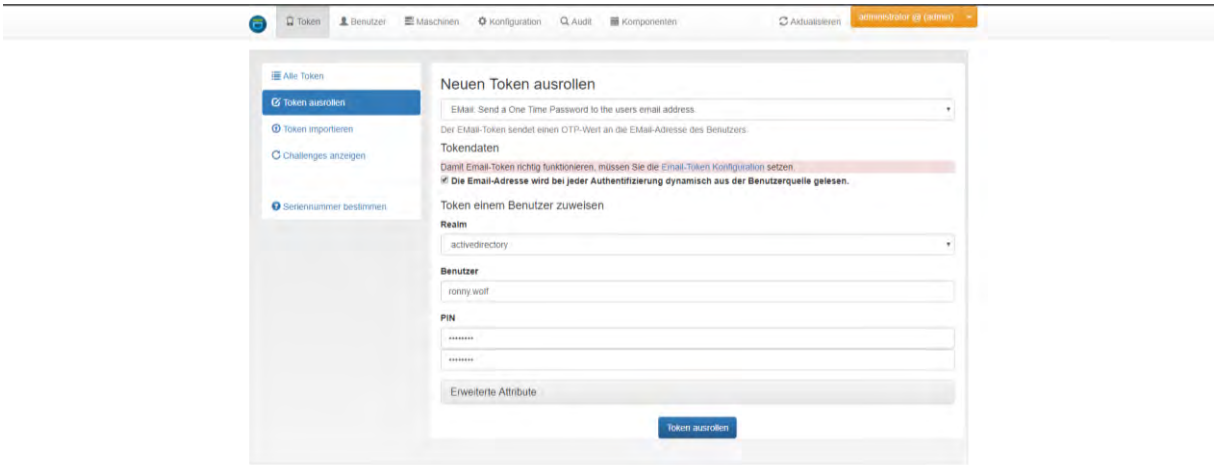
Wählen Sie Ihren SMTP Server aus und die Gültigkeit eines einzelnen OTP's. Sollte der Benutzer den OTP nach der angegeben Zeit eingeben ist die Eingabe ungültig.



Speichern Sie diese Einstellungen ab.

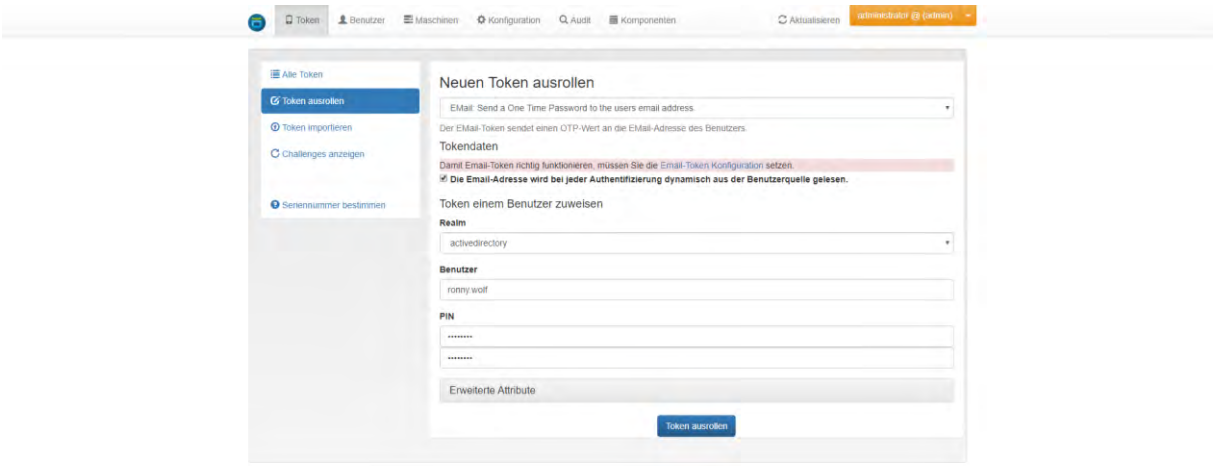
Nun können wir einen Email Token unserem Benutzer zuweisen.

Klicken Sie hierzu auf Token – Token ausrollen

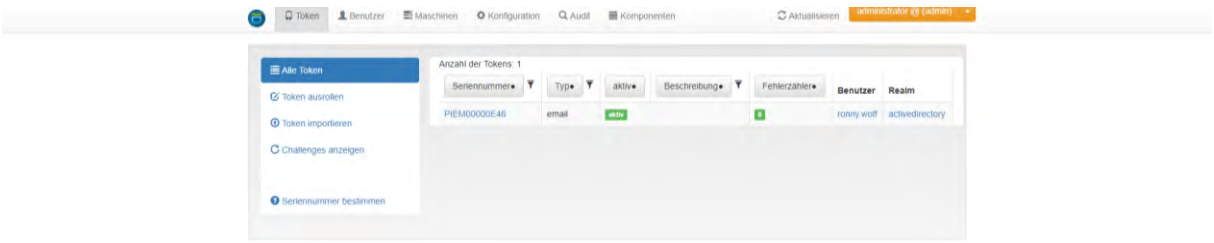


Wählen Sie nun Email aus. Wählen einen Benutzer aus (bei Eingabe in das Textfeld erfolg die Autovervollständigung) und vergeben eine Pin (die Token Pin verwenden wir in unserem Beispiel nicht, da wir die Richtlinie Active Directory Passwort + OTP erstellt haben).

Klicken Sie abschliessend auf Token ausrollen.

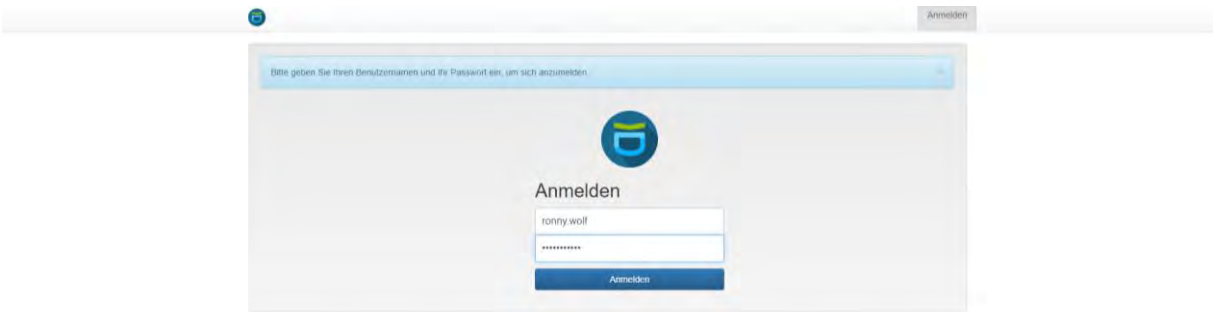


Der Email Token ist nun erstellt und dem Benutzer zugewiesen

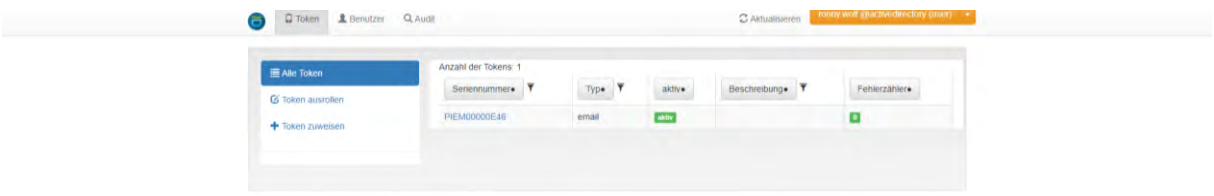


Wenn sich der Benutzer am privacyIDEA Webinterface anmeldet sieht dieser nun das ein Token für Ihr zugewiesen ist.

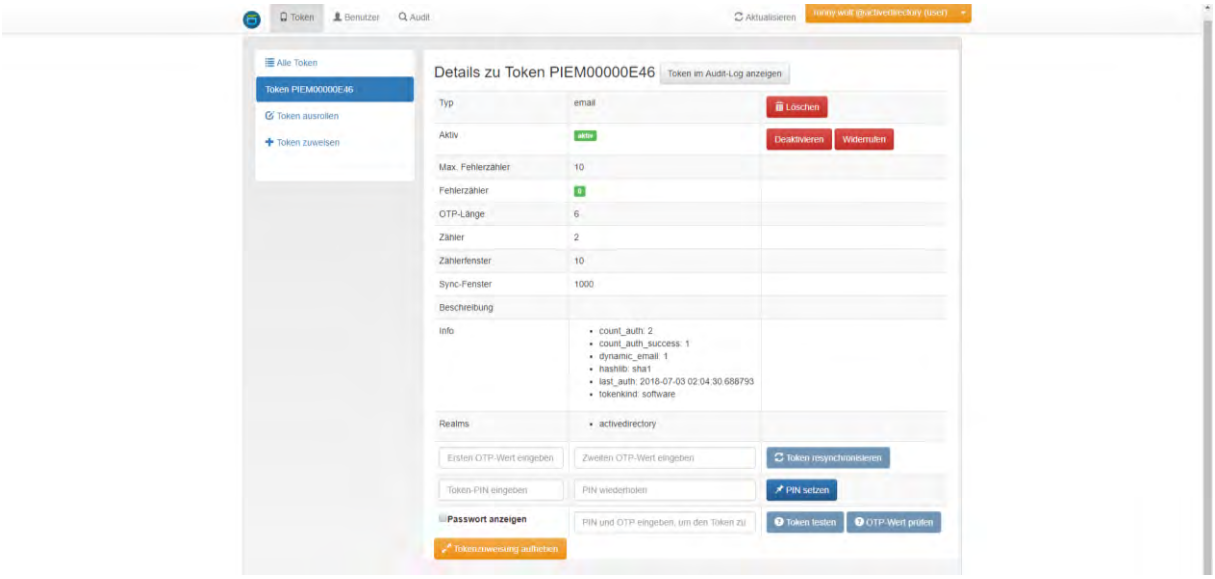
Melden Sie sich als Benutzer am Webinterface an.



Nun sieht der Benutzer den oder die zugewiesenen Token, grundsätzlich kann der Benutzer, sofern nicht in einer Richtlinie definiert, mehrere Token zugewiesen haben.

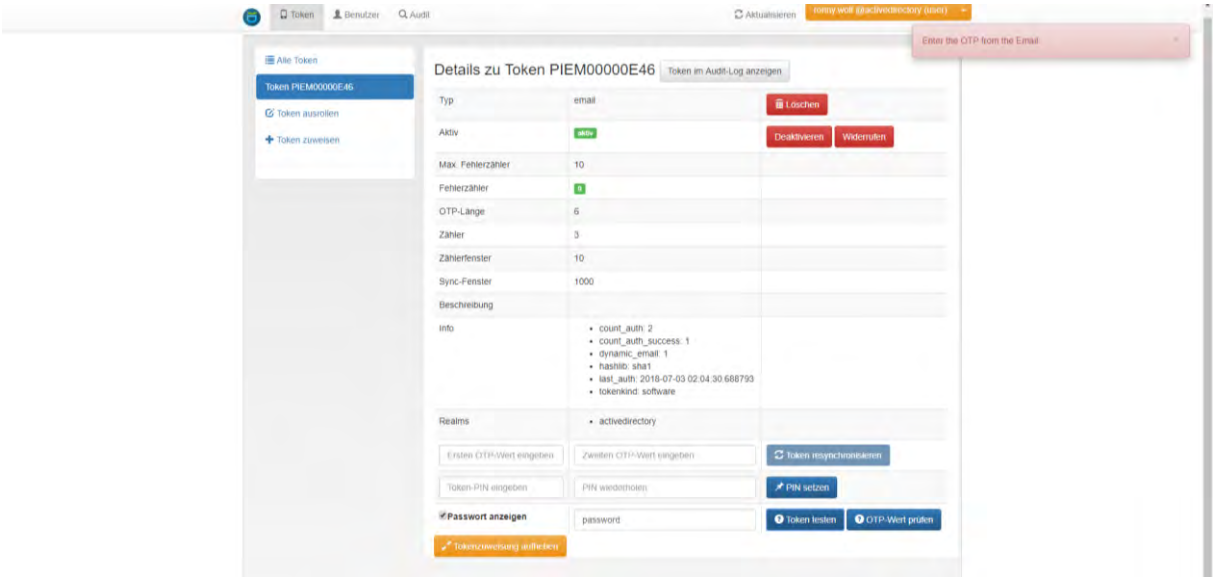


Durch klick auf die Token ID kann die Funktionsfähigkeit getestet werden

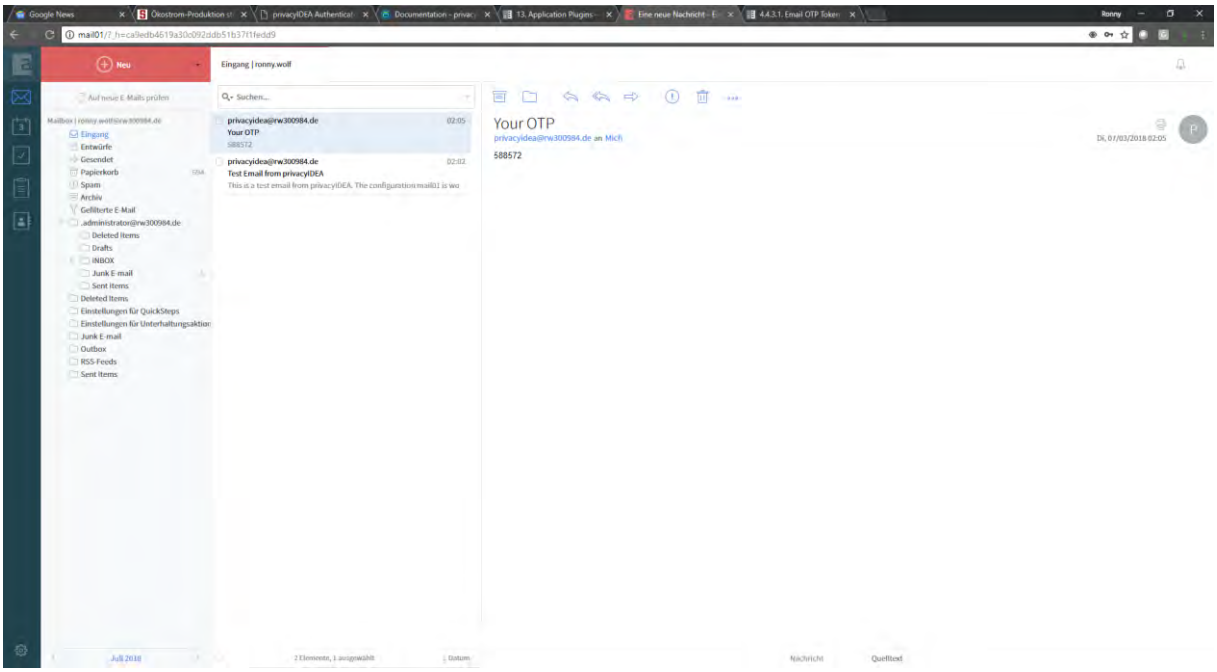


Anders als bei einem Hardware oder Software (z.B. Google Authenticator) basierten OTP, muss bei einem Email Token der erste Anmeldeversuch mit Active Directory Benutzer + Passwort erfolgen. Ist dies richtig eingeben, sendet privacyIDEA über den Radius Server eine Rückantwort an den Client (z.B. Ihre Firewall) mit der Meldung das ein OTP via Email an den Benutzer zugesendet wurde. Beim zweiten Anmeldeversuch innerhalb des konfigurierten OTP Zeitfensters, muss nun Benutzername + Active Directory und Email Token OTP eingeben werden. D.h. der erste Anmeldeversuch scheint immer fehlzuschlagen, jedoch wird dadurch die Generierung angetriggert.

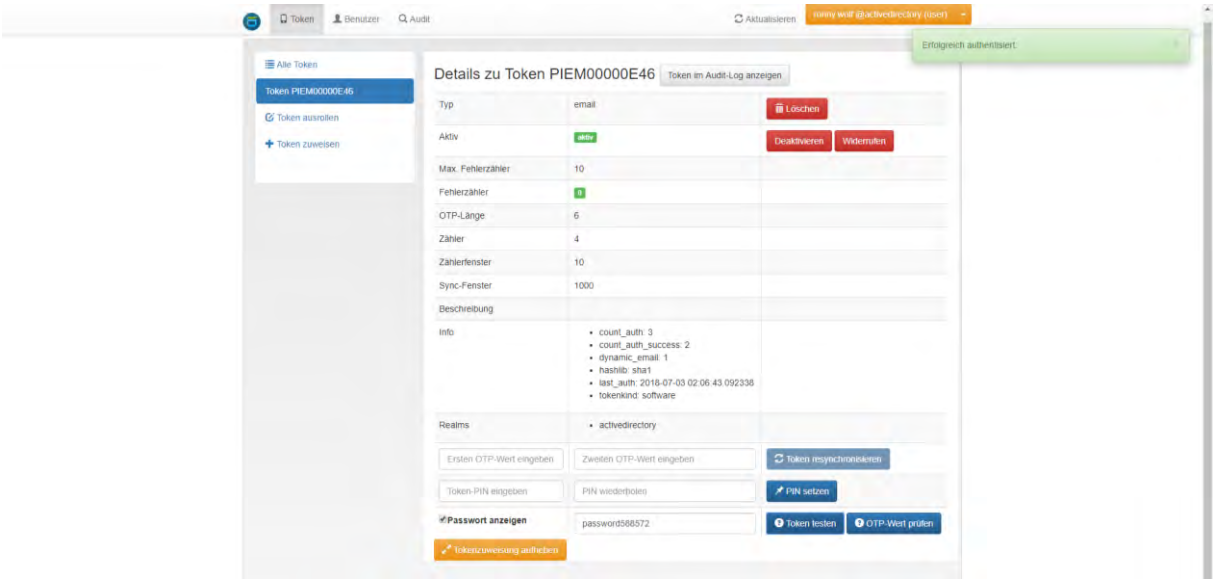
Um nun die Funktion zu testen geben wir als erstes Benutzername und Passwort ein. Sie erhalten nun die Meldung „Enter the OTP from Email“.



Sehen Sie nun in Benutzerpostfach nach ob Sie von privacyIDEA eine Email mit dem OTP erhalten haben.



Nun geben Sie das Active Directory Passwort und den OTP in der Email an.



Wie im oberen Screenshot zu erkennen, konnten wir uns erfolgreich authentifzieren.

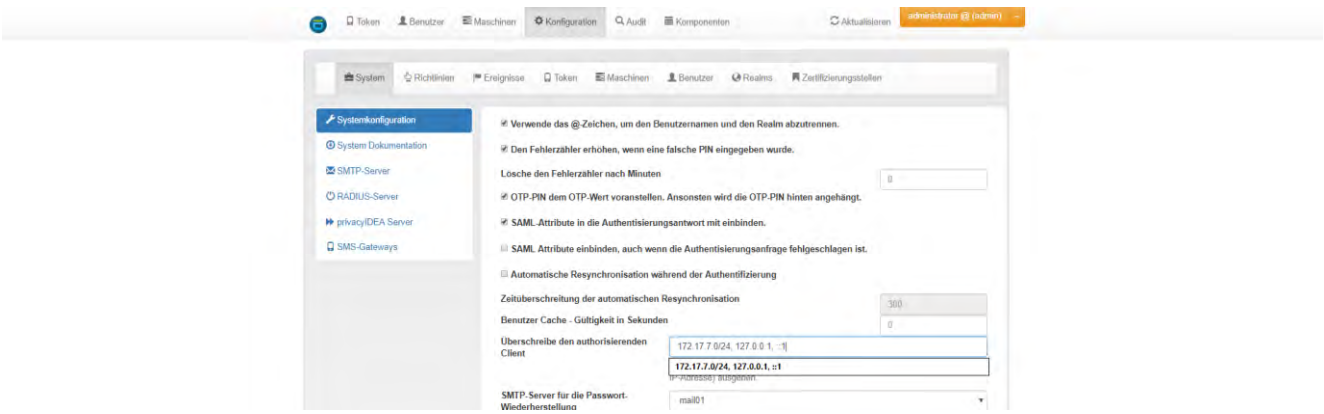
5.3. Überschreiben von Client IP Addresse über Radius erlauben

Wenn Sie individuelle Richtlinien für einzelne Radius Clients (z.B. Ihre Firewalls), als auch ein genaueres Berichtswesen möchte, besteht in der Standardkonfiguration die Herausforderung das der installierte Radius Server (FreeRadius) mit dem privacyIDEA Server auf „Localhost“ kommunizieren. Dies bedeutet das Sie privacyIDEA nicht erkennen woher die Authentifzierungsanfrage kommt.

Um dies zu umgehen, können Sie in den Einstellungen von privacyIDEA definieren, welche Quelladdressen vom Radius Server/privacyIDEA überschrieben werden dürfen. Dadurch wird nicht die IP Addresse des Radius Server (Localhost = 127.0.0.1), sondern der richtige Client (z.B. die IP ihrer Firewall) angezeigt.

Klicken Sie hierzu auf Konfiguration – System

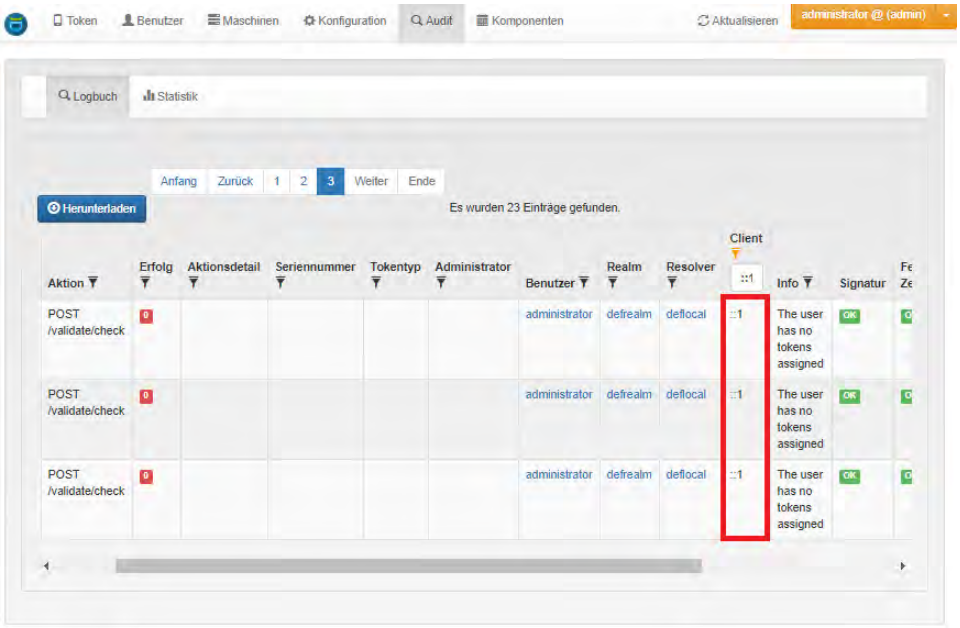
Geben Sie unter Überschreibe den authorisierenden Client, das Netz und/oder die lokale IP Addresse des FreeRadius Servers (in unserem Beispiel ist dies der 127.0.0.1 = IPv4 und ::1 = IPv6 an)



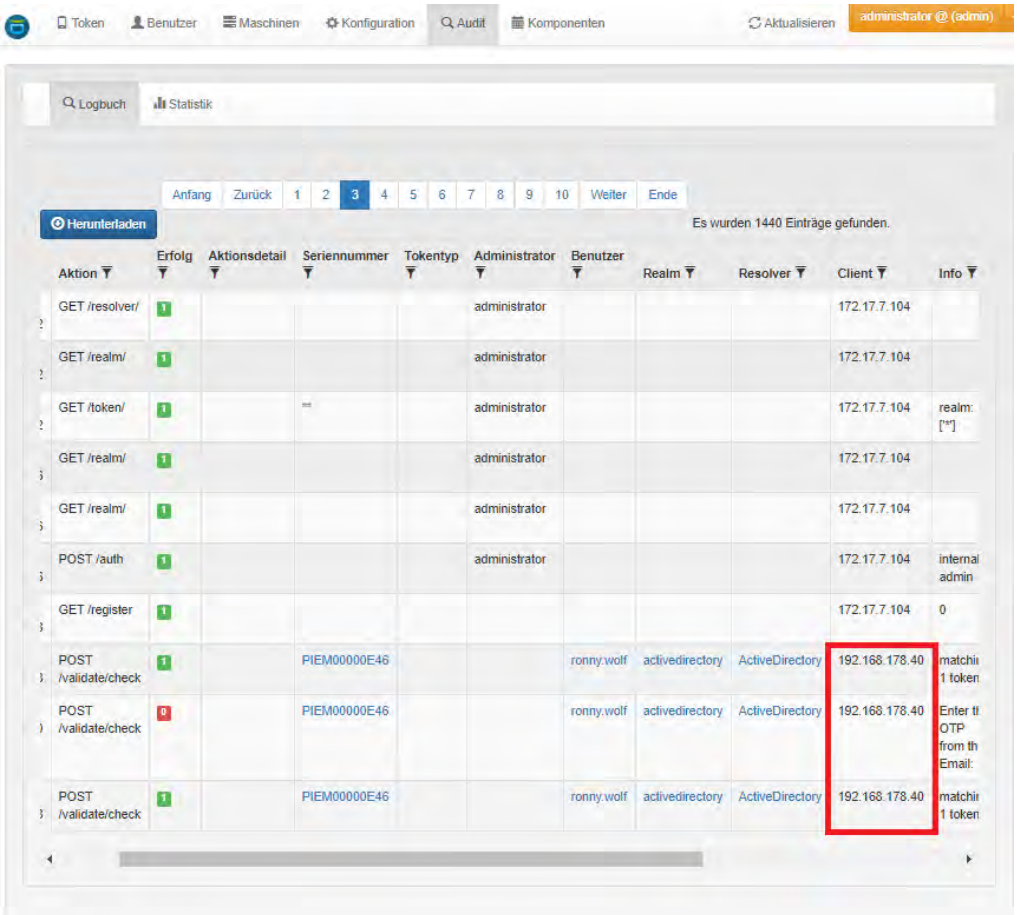
Speichern Sie diese Einstellung.

Bei zukünftigen Authentifzierungsanfragen sehen Sie nun die originäre Quelle.

Voher:



Nachher (mit neuen Einstellungen):



6. Yubikey's konfigurieren und ausrollen

Da privacyIDEA eine native Unterstützung für Yubikeys anbietet, ist es besonders einfach neue Yubikeys auszurollen. Während Sie zwar die Möglichkeit haben direkt am privacyIDEA Server Yubikeys zu konfigurieren, zeigen wir in diesem Kapitel die Konfiguration anhand des Personalization Tools von Yubico.

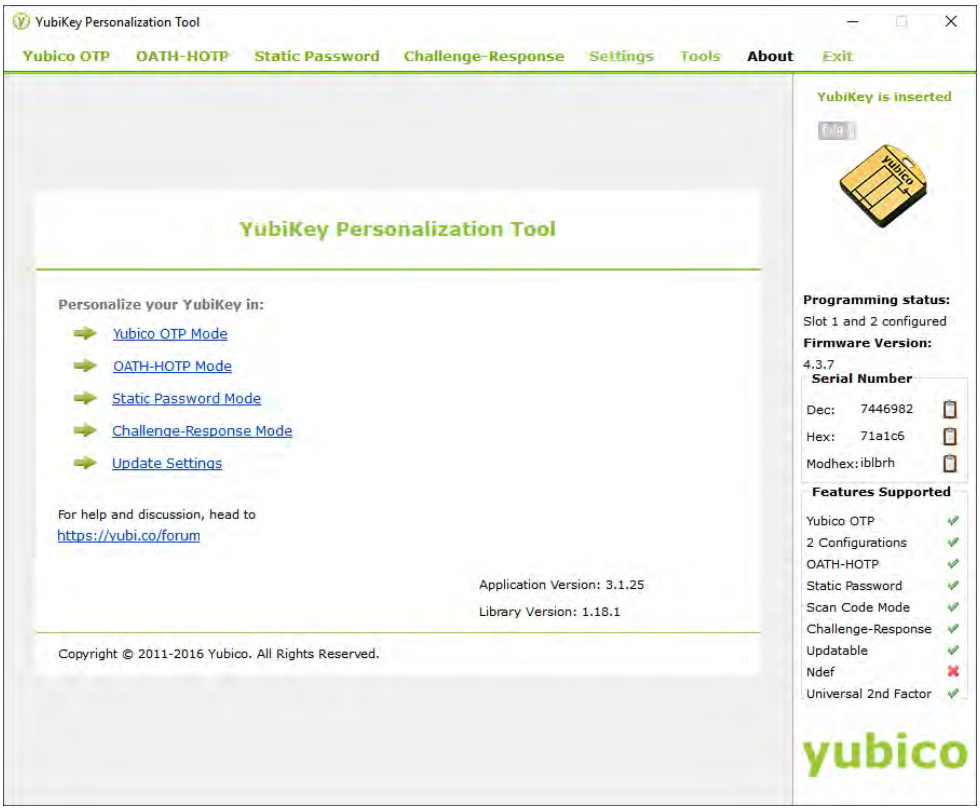
Weitere Informationen über die Möglichkeiten des Ausrollen von Yubikeys finden Sie hier:

https://privacyIDEA.readthedocs.io/en/master/configuration/tokens/yubikey.html

6.1. Konfigurieren eines Yubikeys mit dem Yubico Personalization Tool

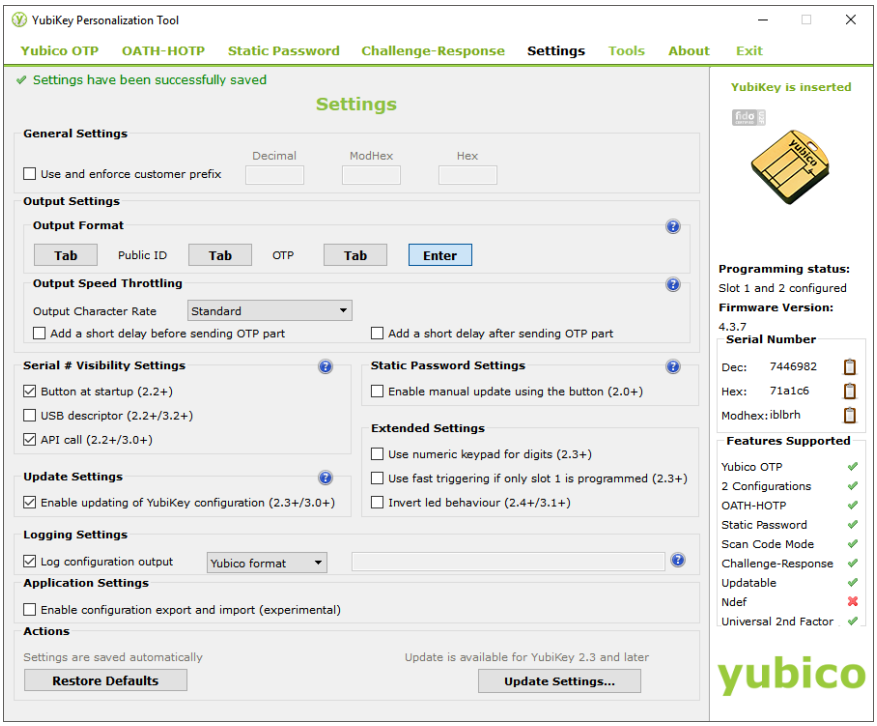
Alle Yubikeys unterstützen verschiedene OTP Protokolle (TOTP, HOTP und YubiOTP). In diesem Beispiel verwenden wir das Protokoll YubiOTP.

Stecken Sie nun den Yubikey an öffnen Sie das Personalisierungs Tool von Yubico (https://www.yubico.com/products/services-software/download/yubikey-personalization-tools/)

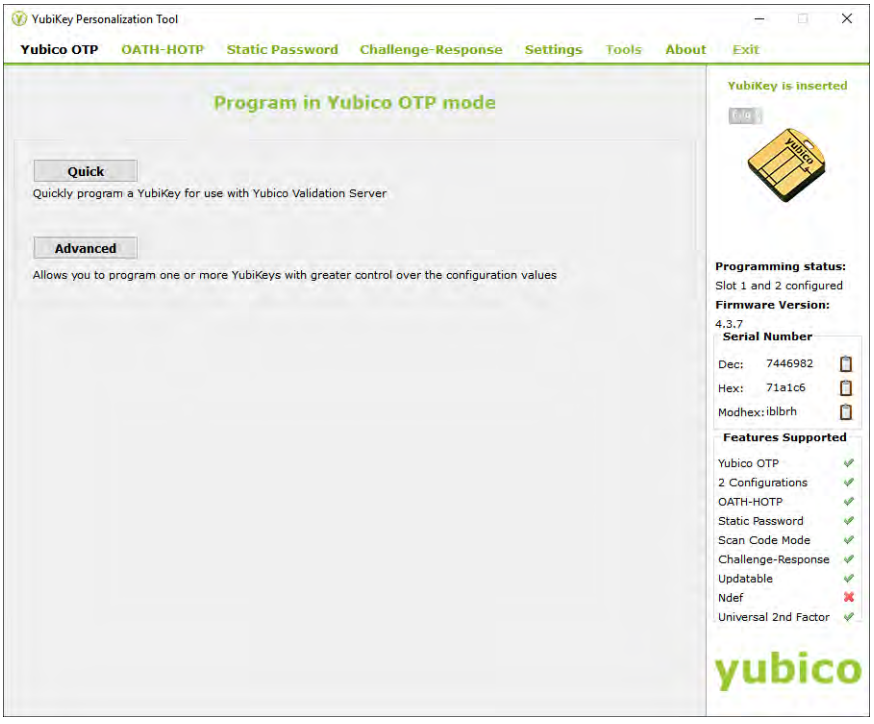


Klicken Sie nun auf Settings und konfigurieren Sie unter Logging Settings, folgendes:

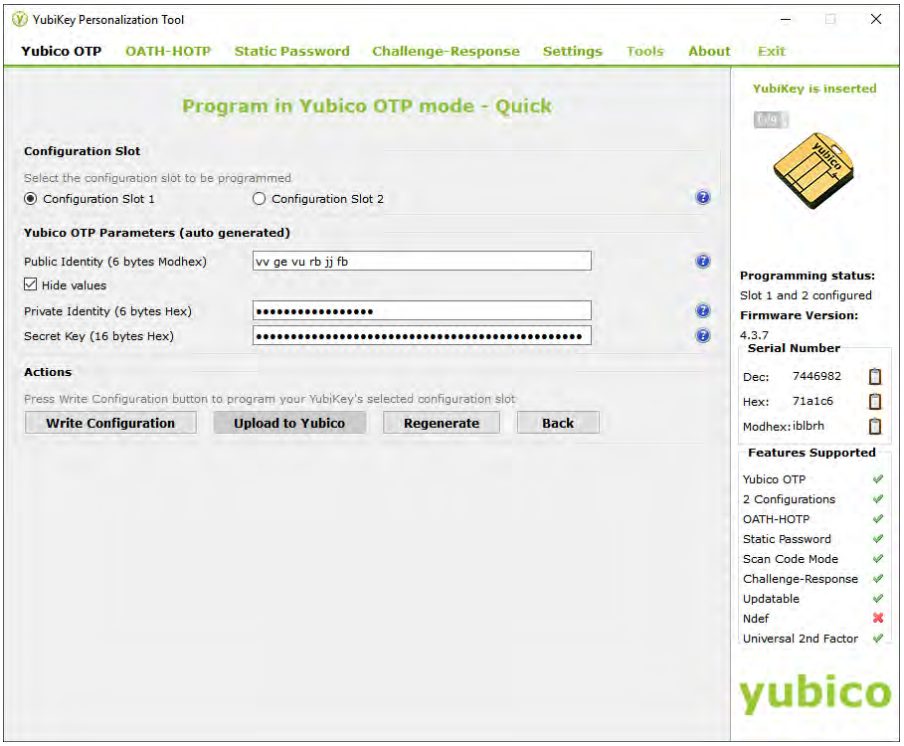
Log configuration output = aktiviert
Wert: Yubico Format



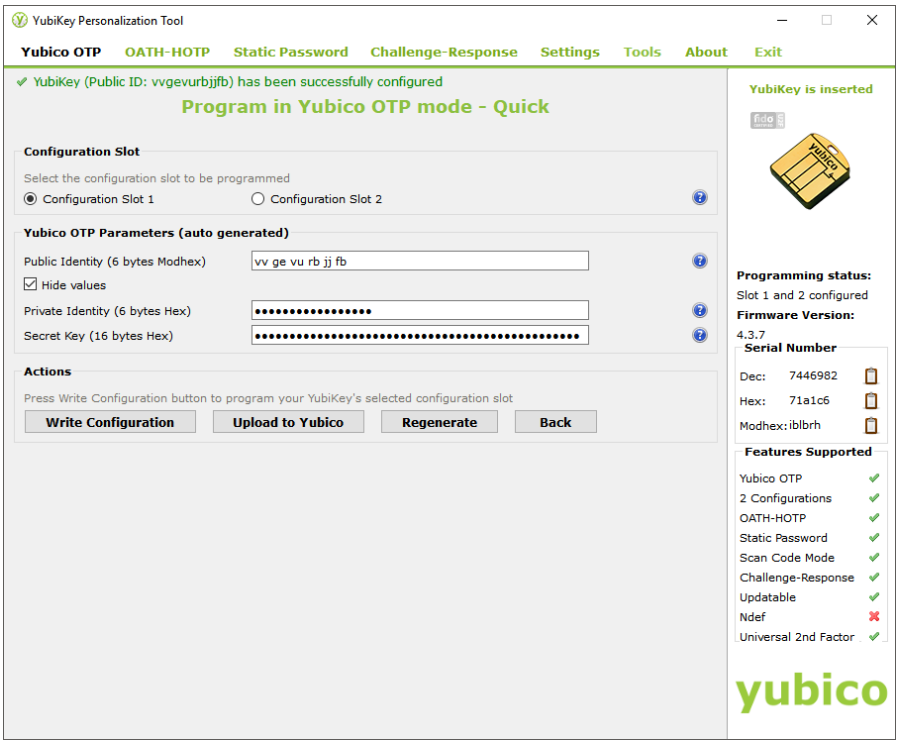
Klicken Sie nun auf Yubico OTP



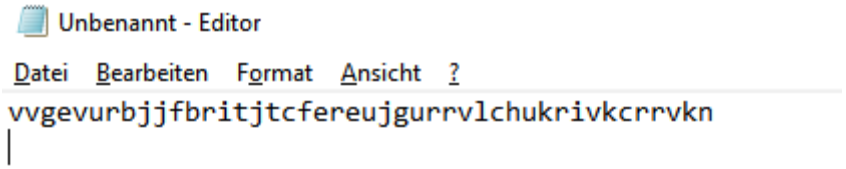
Wählen Sie nun Quick und klicken einmal auf Regenerate. Wählen Sie nun den Konfigurationsslot (Slot 1 = Kurze Berührung | Slot 2 = Lange Berührung).



Schreiben Sie die Konfiguration auf den Yubikey und wählen eine Speicherort für die Logdatei



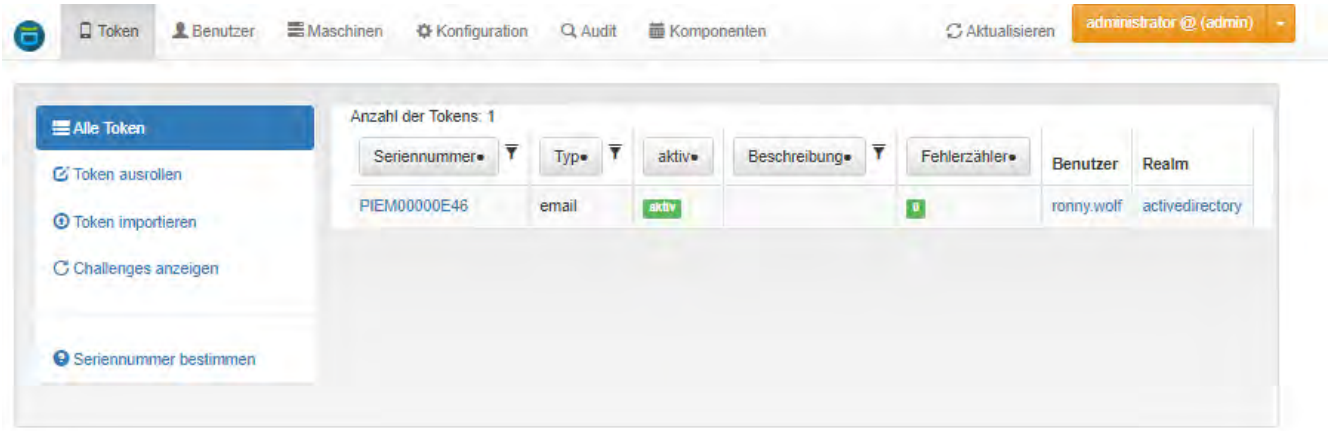
Testen Sie nun den Yubikey z.B. in einem Texteditor ob ein OTP durch berühren des Yubikeys generiert wird



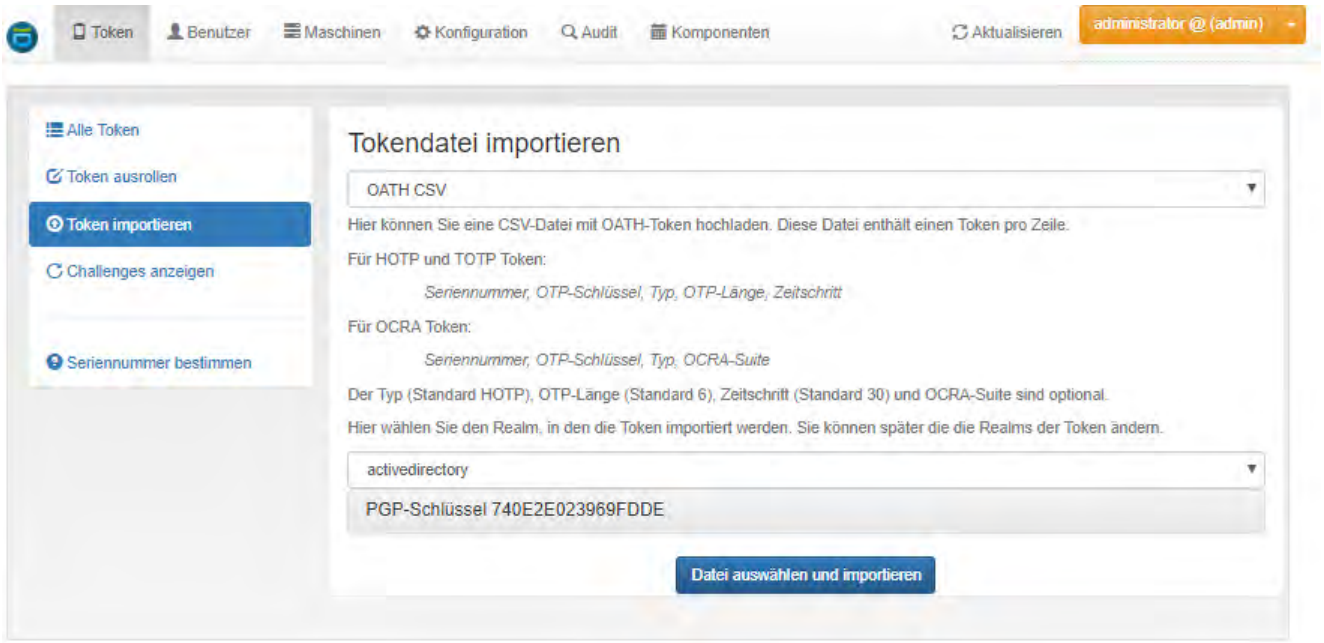
Ihr Yubikey ist nun erfolgreich für Privcayldea konfiguriert.

6.2. Ausrollen und zuweisen eines Yubikeys in privacyIDEA

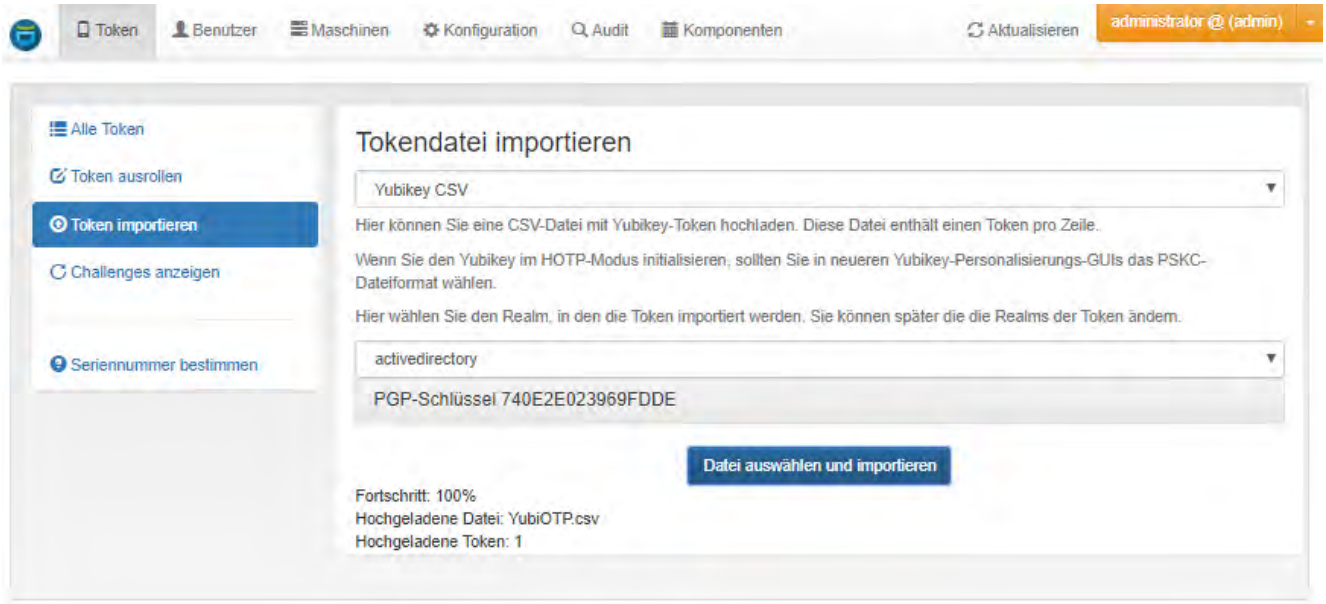
Öffnen Sie nun das privacyIDEA Webinterface und klicken auf



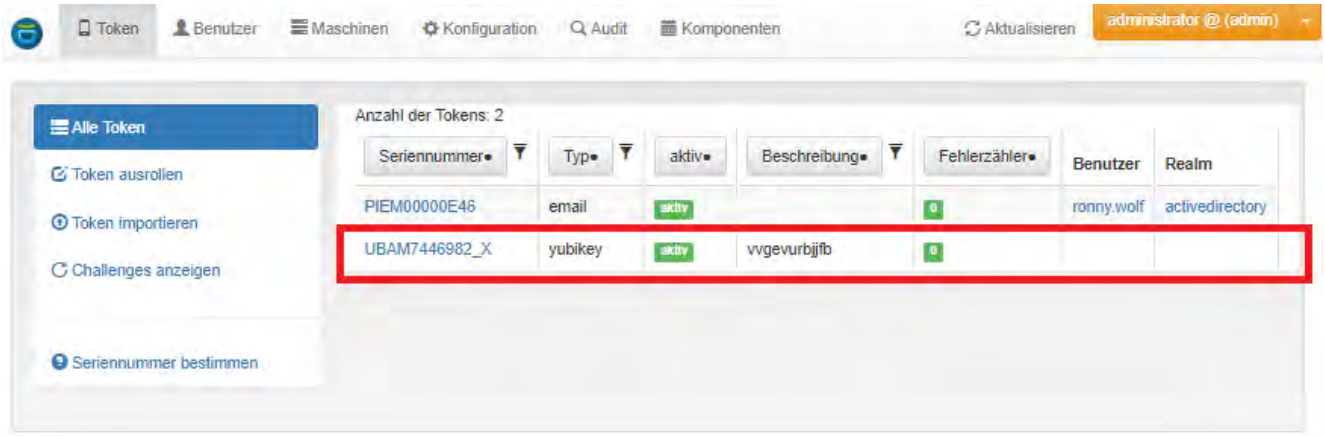
Klicken Sie auf Token importieren



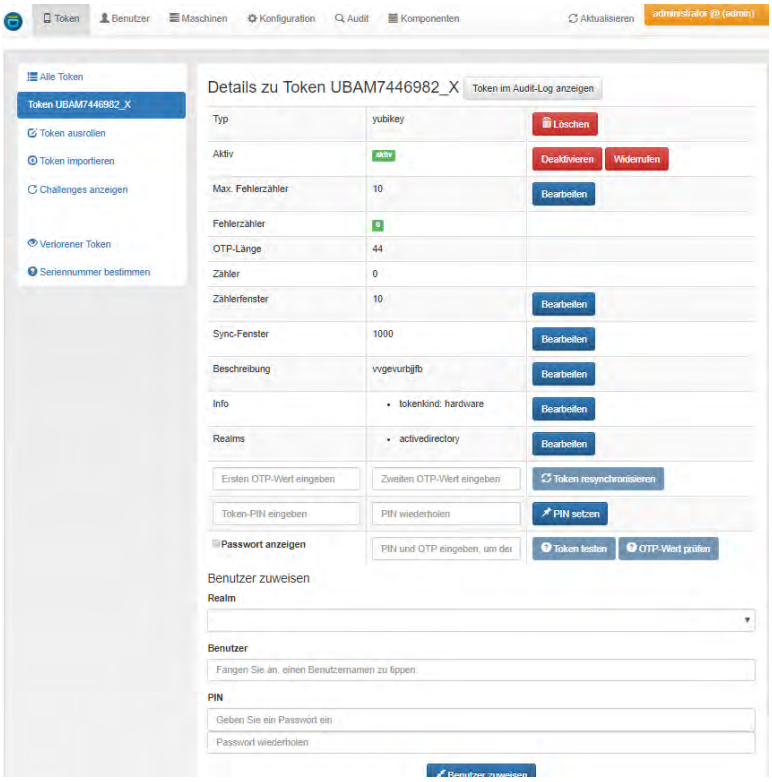
Wählen Sie als Import Format Yubikey CSV, den Active Directory Realm und die in Kapitel 6, Abschnitt 1 gespeicherte Logdatei aus



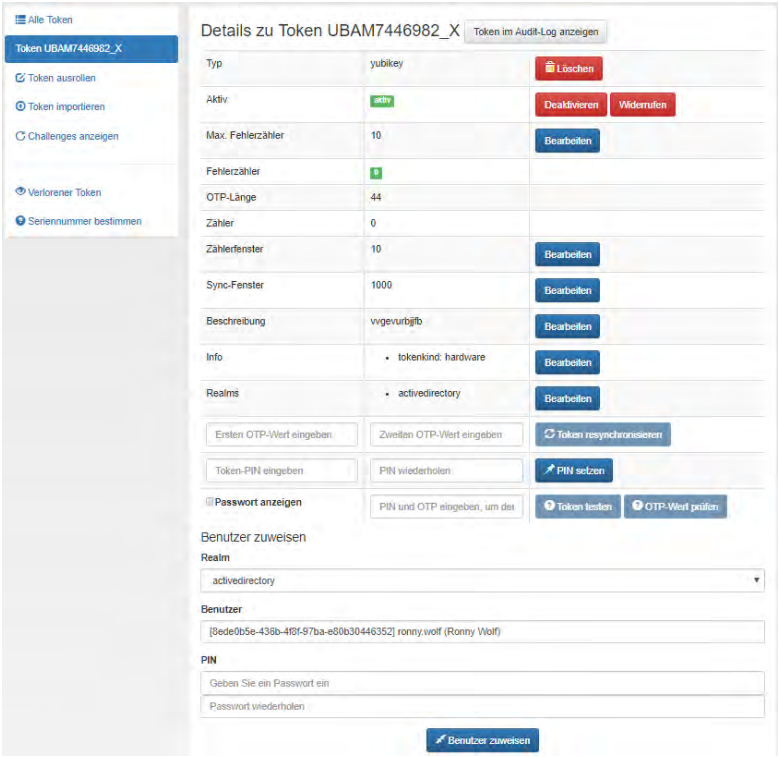
Nun sollte der Yubikey erfolgreich importiert sein. Klicken Sie hierzu auf „Alle Token“



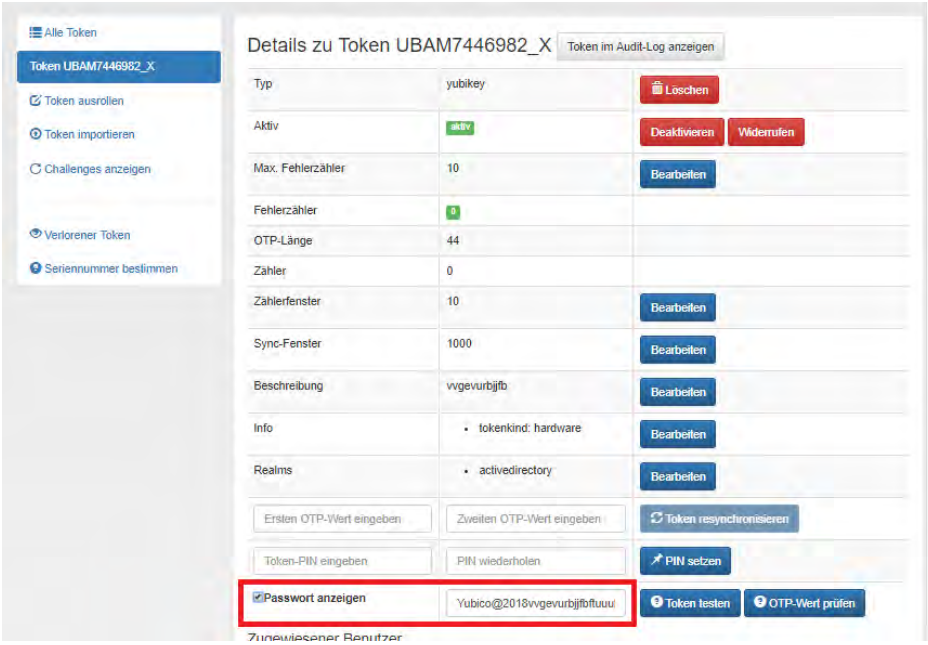
Nun können Sie den Yubikey einem Benutzer zuweisen. Klicken Sie hierzu auf die Seriennummer (Token ID):



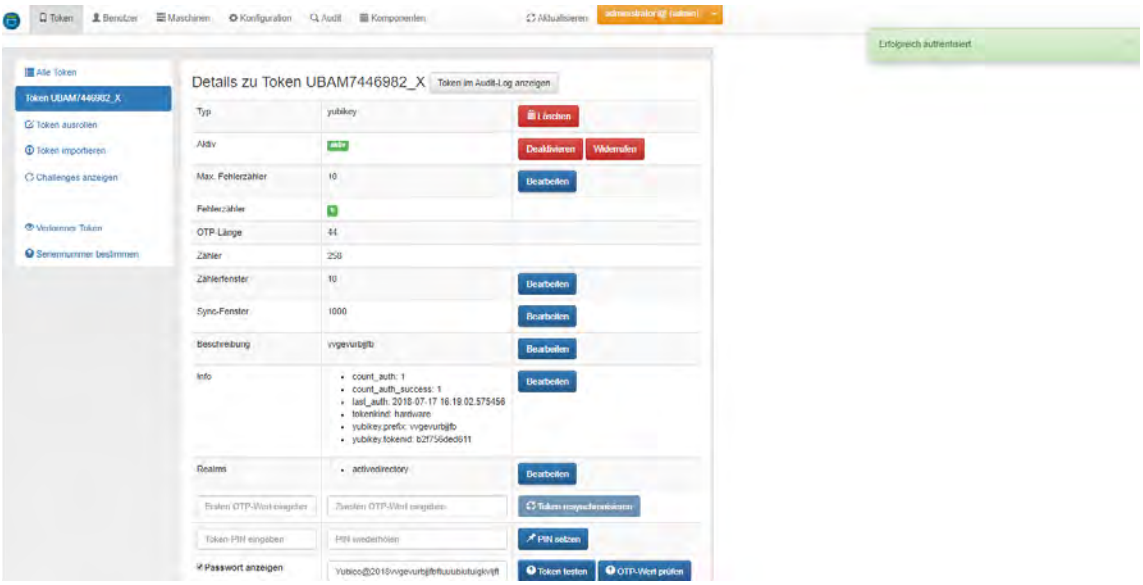
Definieren Sie nun unter Realm = Active Directory und Benutzer, den Benutzer der sich zukünftig mit dem Yubikey anmelden soll



Sie können nun den die Authentifzierung testen. Geben Sie hierzu das Passwort des Benutzers und berühren direkt im Anschluss (im selben Feld) den Yubikey, damit ein OTP generiert wird



Klicken Sie nun auf Token testen



Sollten Sie zweimal auf Token testen klicken, kann es passieren das der OTP bereits wieder ungültig ist (Einmalpasswort!)

7. Firewall's konfigurieren

In unserem Guide behandelt wir nur verschiedene Firewall Backends, beachten Sie das grundsätzlich jedes Radius fähige System angebunden werden kann. Wichtig ist lediglich das der Radius Client das Protokoll „PAP“ unterstützt. Andere Protokolle wie CHAP (Challenge/Response), EAP oder MSCHAP können nicht verwendet werden.

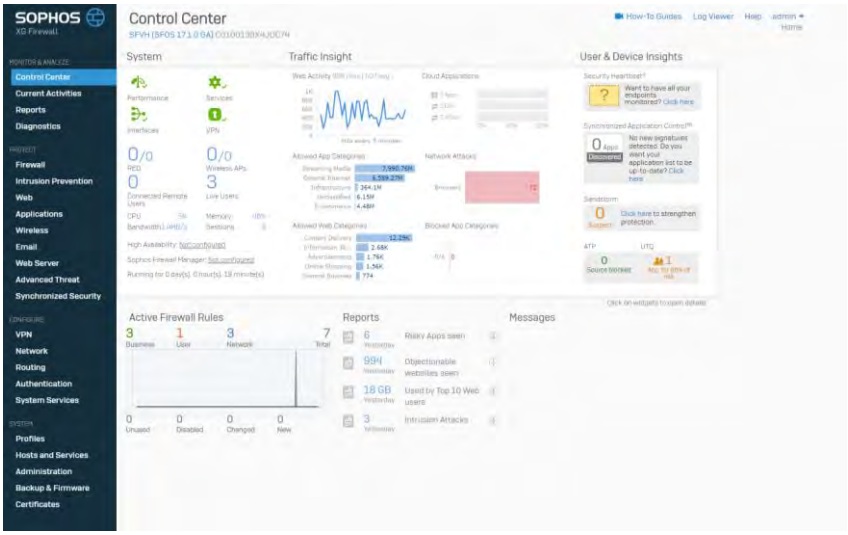
7.1. Sophos XG Firewall mit Radius

Die Firewalls von der Firma Sophos bieten verschieden Möglichkeiten eine Zwei Faktor Authentifzierung durchzuführen. Hierbei gibt es die Variante TOTP, welche ohne zusätzliches Authentifierungs Backend funktioniert, als auch die Anbindung an einen Radius Server. Im Guide verwenden wir Version 17.x von Sophos XG

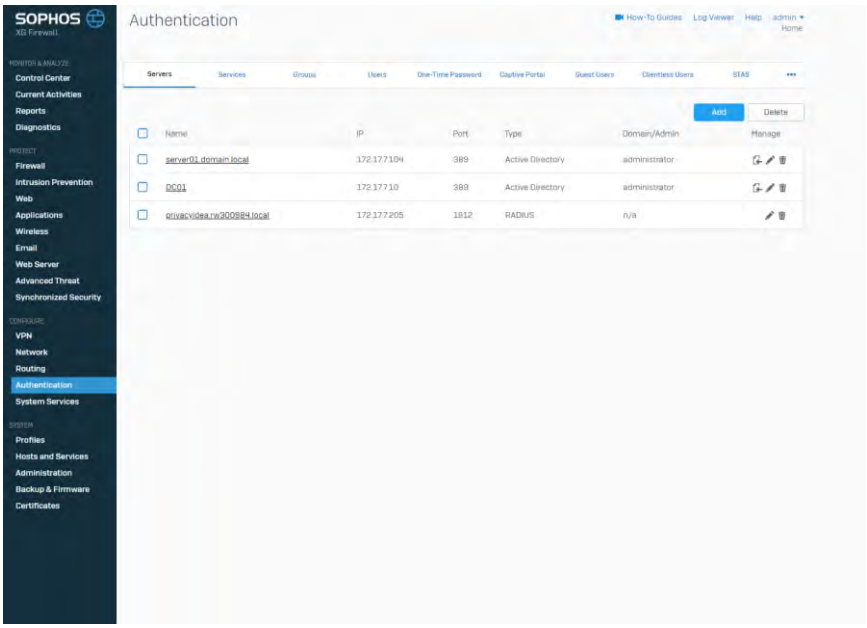
7.1.1. Konfigurieren der Radius Anbindung

Melden Sie sich an Ihrer Sophos XG Appliance als Administrator an.

Nach erfolgreicher Anmeldung, klicken auf Configure -> Authentication

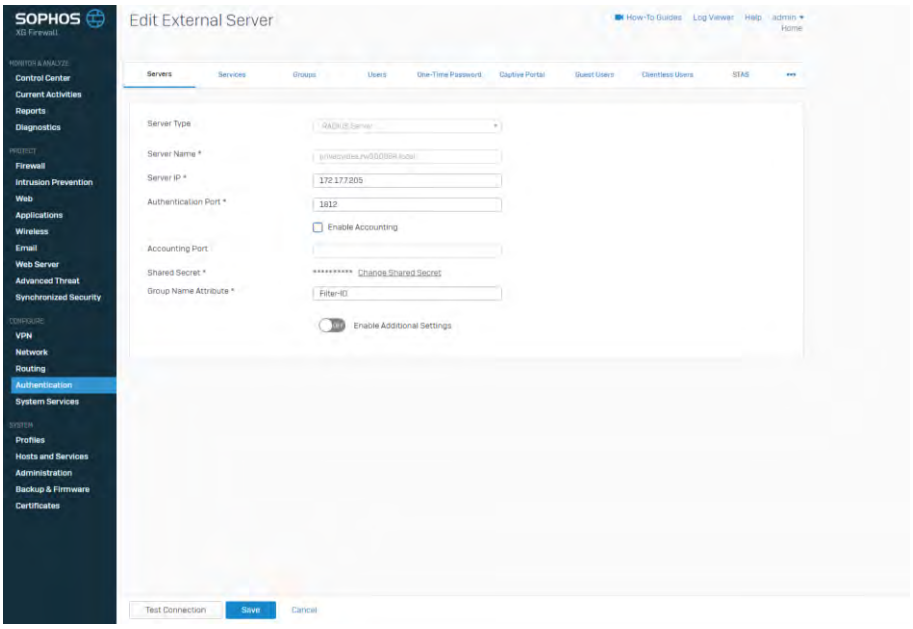


Klicken Sie nun auf „Add“



Definieren Sie wie im unteren Screenshot gezeigt die Radius Server Anbindung.

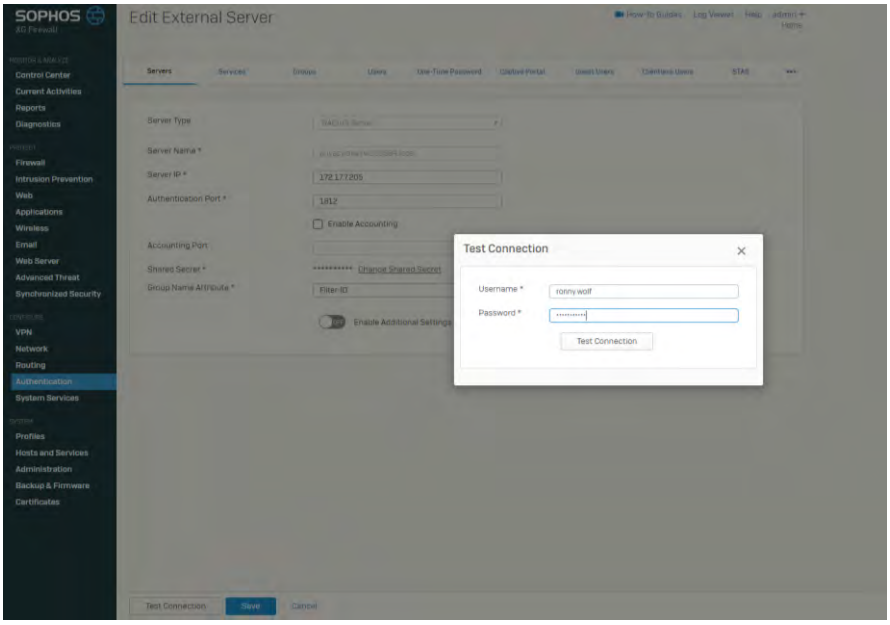
Server Name: FQDN des privacyIDEA Server
Server IP: IP des privacyIDEA Server
Shared Secret: Das in Kapitel 2, Absatz 8, definierte Secret für den Radius Client



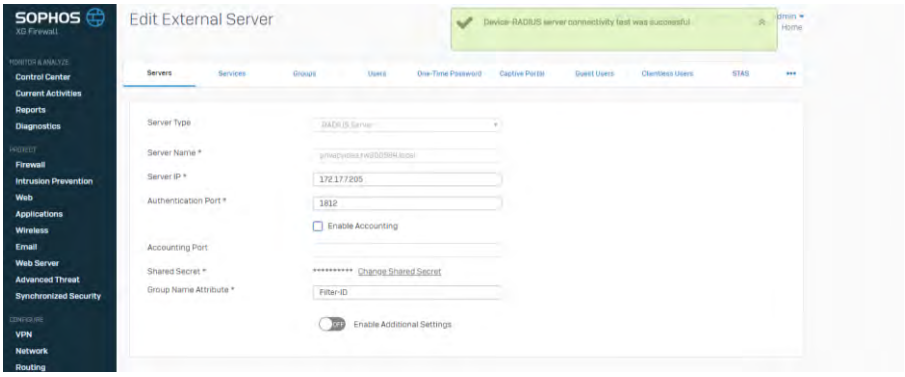
Testen Sie nun die Radius Authentifzierung mit einem Benutzer der einen Yubikey zugewiesen hat

In unserem Beispiel:

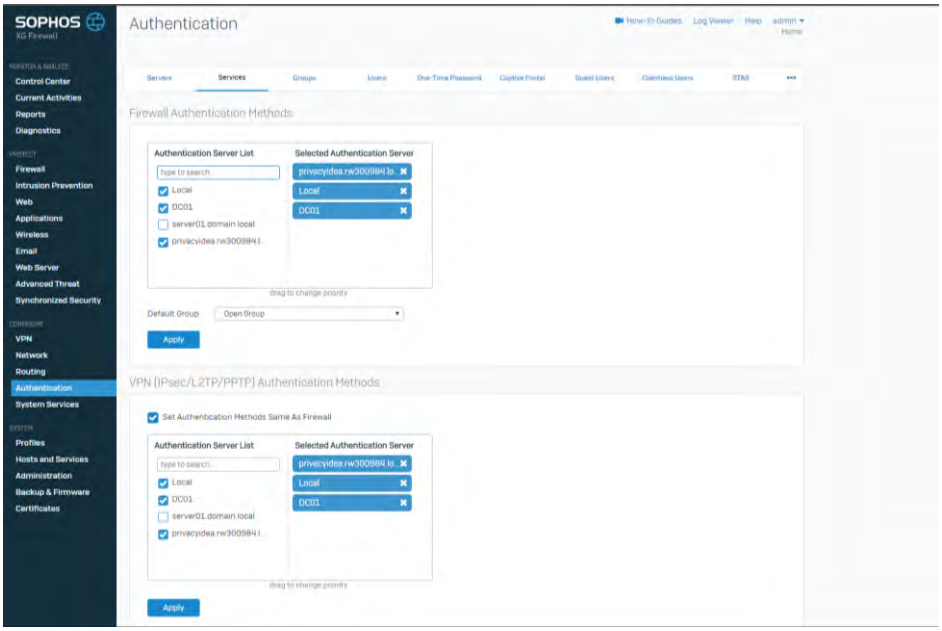
Username: ronny.wolf
Password: Active Directory Passwort + Yubikey OTP



Ist die Authentifzierung erfolgreich, erhalten sie direkt im Webinterface der Sophos XG Appliance eine Rückmeldung.



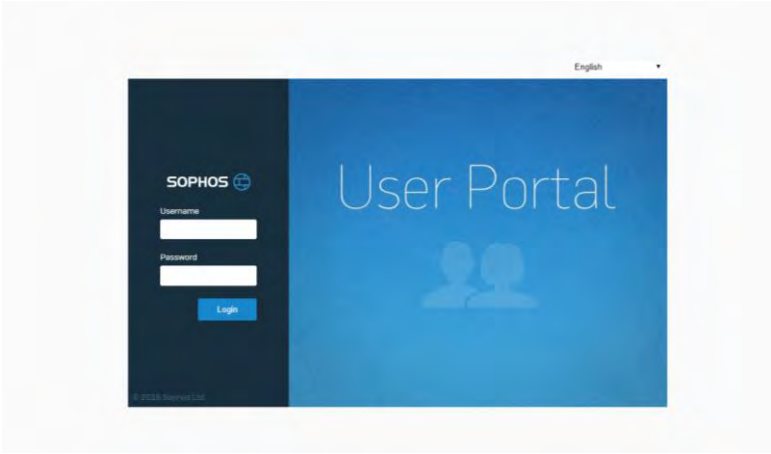
Nun müssen Sie die Radius Authentifizierung, den unterschiedlichen Dienste (VPN, User Portal...) der Sophos XG zuweisen.



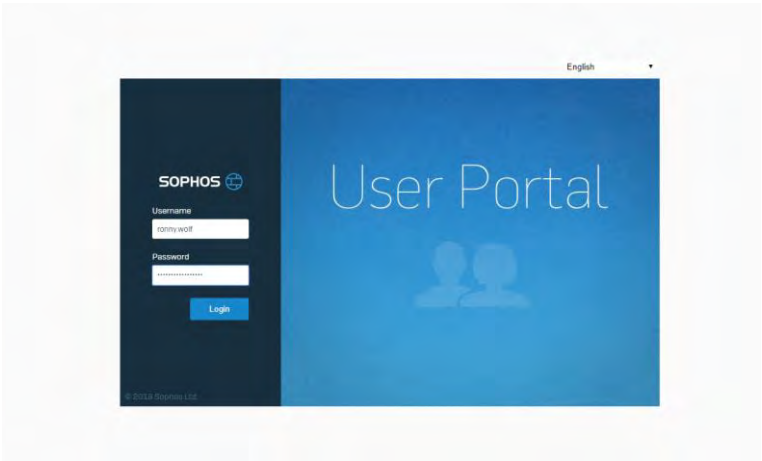
Hinweis: Sollten Sie weitere Authentifzierungsbackends in Ihrer Sophos XG definiert haben, empfehlen wir die Reihenfolge (Drag & Drop) zu ändern, damit der privacyIDEA Server als erste Quelle angegeben ist.

7.1.2. Anmelden an User Portal mit Yubikey

Öffnen Sie nun das User Portal der Sophos XG (Webinterface)



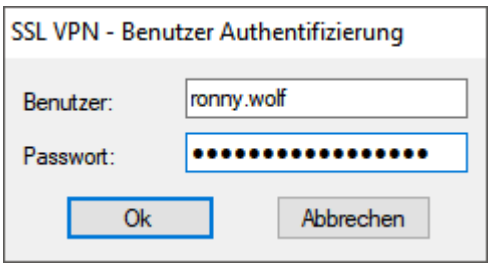
Geben Sie den Benutzer welcher einen Yubikey zugeordnet hat ein, und geben das Active Directory Passwort gefolgt von Yubikey OTP ein.



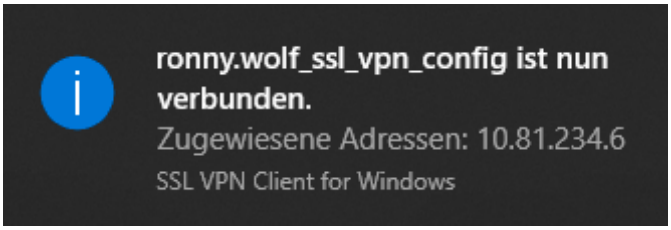
War die Anmeldung erfolgreich, sehen Sie nun das User Portal des Benutzers

7.1.3. Anmelden via SSLVPN mit Yubikey

Die Anmeldung via SSL VPN (OpenVPN Client) erfolg ebenfalls durch Eingabe des Benutzers, sowie dem Active Directory Passwort + Yubikey OTP



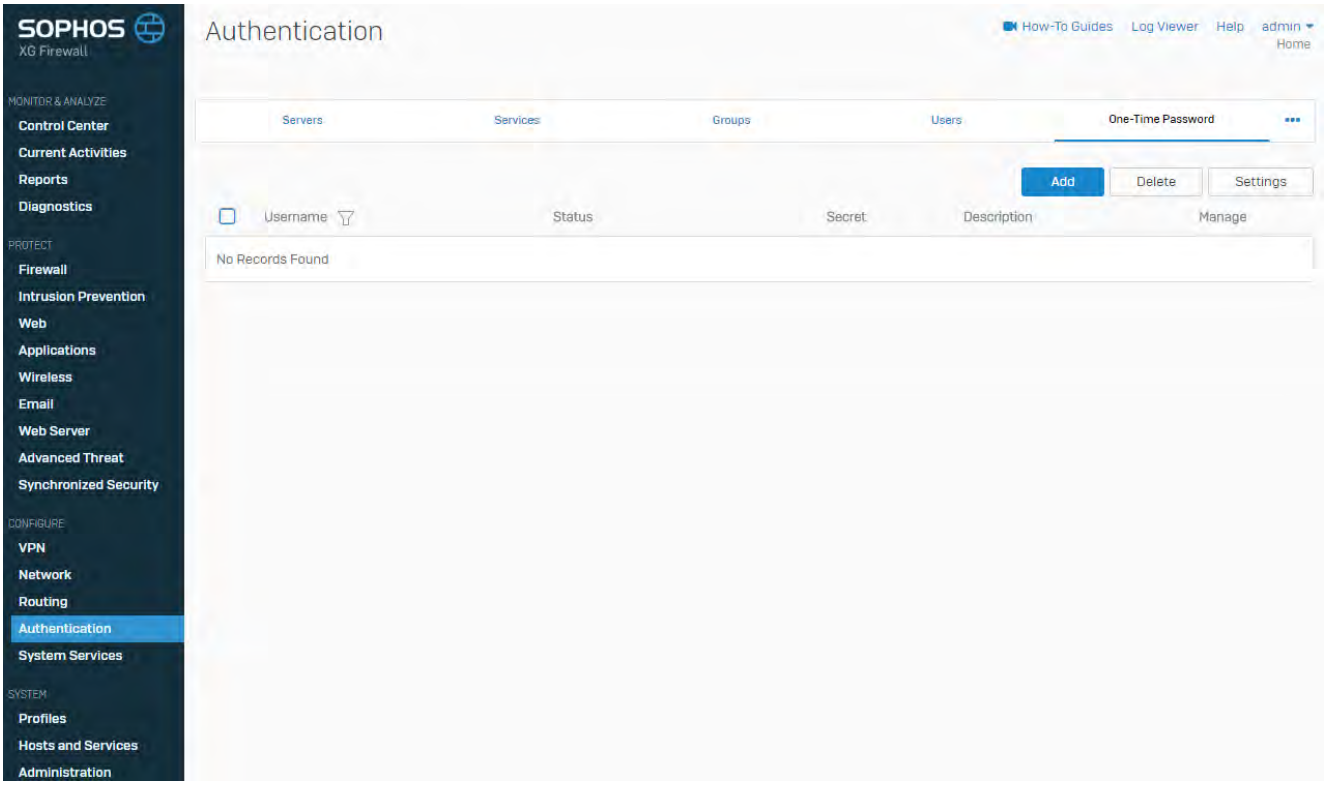
War die Anmeldung erfolgreich, wird eine VPN Verbindung aufgebaut.



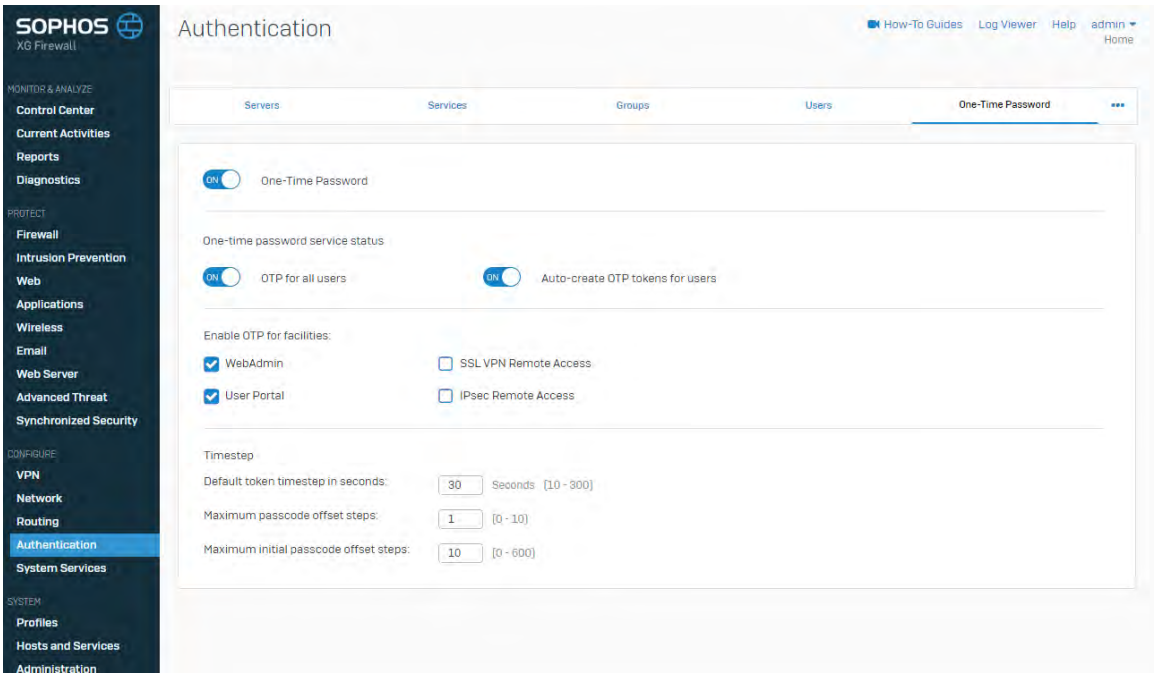
7.1.4. Zeitbasiertes One Time Password

Sophos XG bietet ein natives TOTP Backend, d.h. es ist kein Radius Server (FreeRadius + privacyIDEA) notwendig.

Klicken Sie im Sophos XG Webinterface auf Configure – Authentication – One Time Password

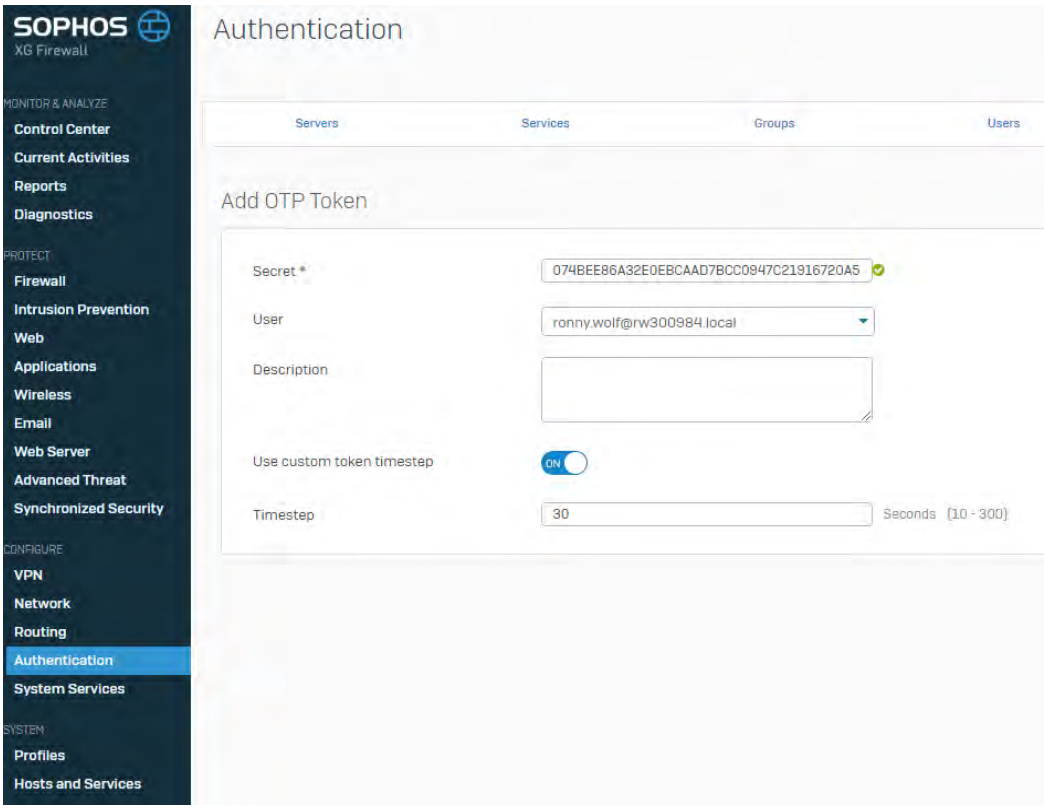


Klicken Sie auf Settings und aktivieren OTP, sowie die Dienste für die OTP verwendet werden soll

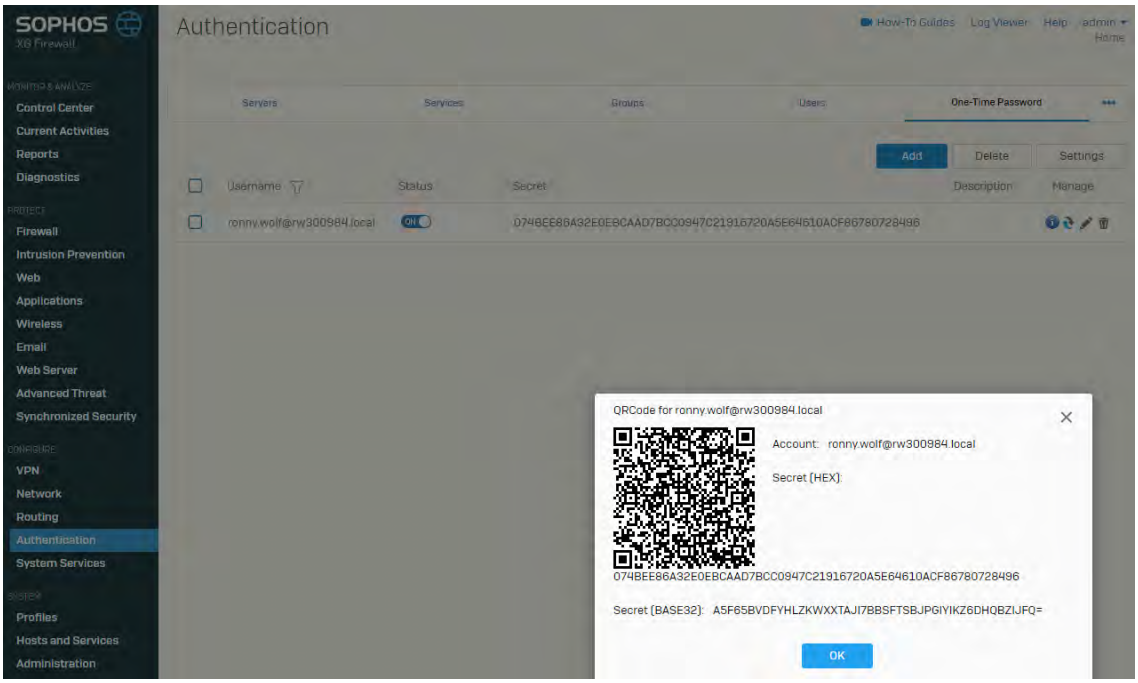


Klicken Sie nun auf Add und geben folgende Parameter ein:

Secret: Zufälliges Secret in HEX Format mit min. 32 Zeichen (z.B. Sie können Sie hier ein random Hex Wert generieren: http://rumkin.com/tools/password/pass_gen.php)
User: Benutzer welche auf der Sophos XG vorhanden ist
Custom timestamp: 30 Sekunden

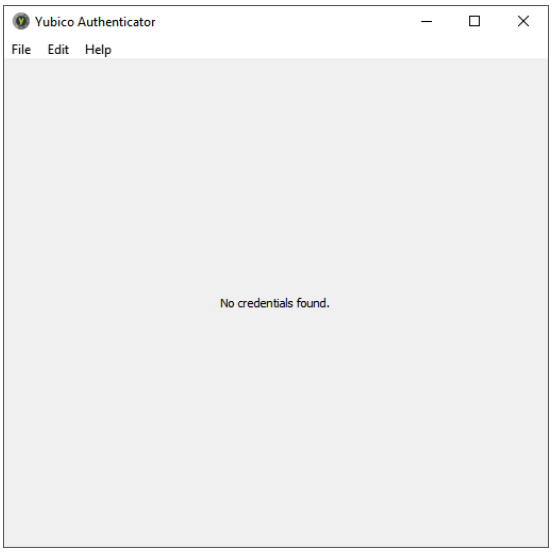


Klicken Sie nun auf das Ausrufezeichen (!) neben dem generierten TOTP Token um einen QR Code zu generieren

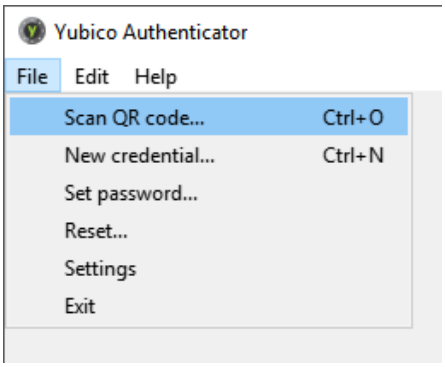


Lassen Sie nun dieses Fenster (mit QR Code sichtbar) geöffnet und öffnen den Yubico Authenticator

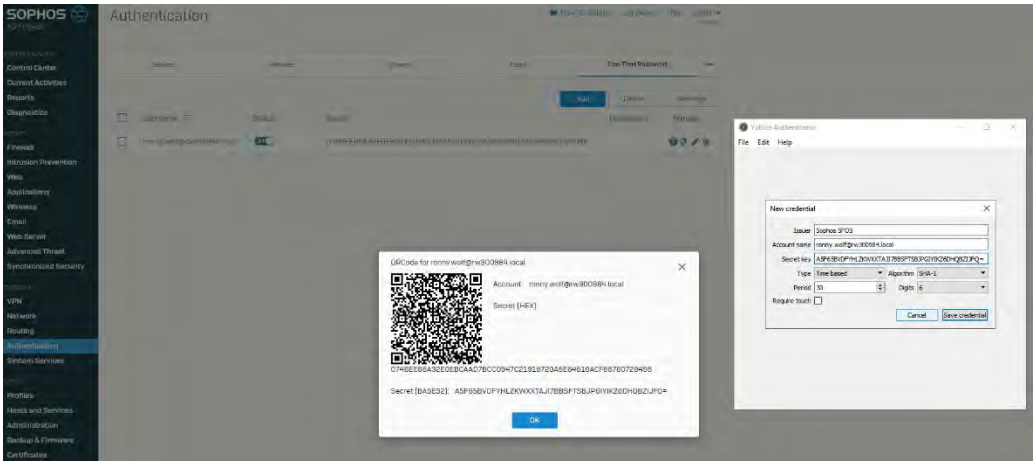
Download: (https://www.yubico.com/products/services-software/download/yubico-authenticator/)



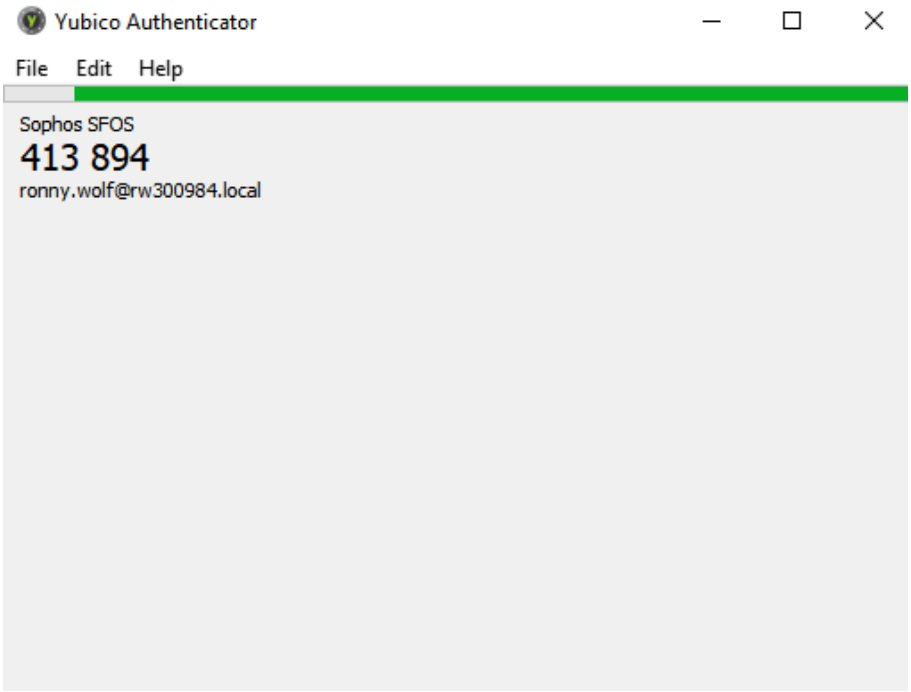
Klicken Sie auf File – Scan QR Code



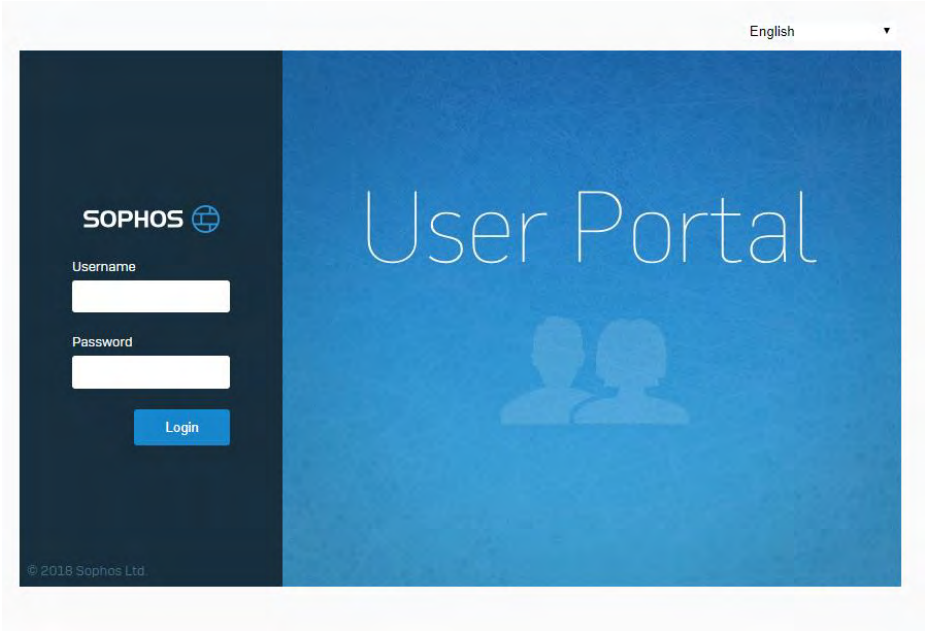
Nun wird automatisch das Secret erfasst:



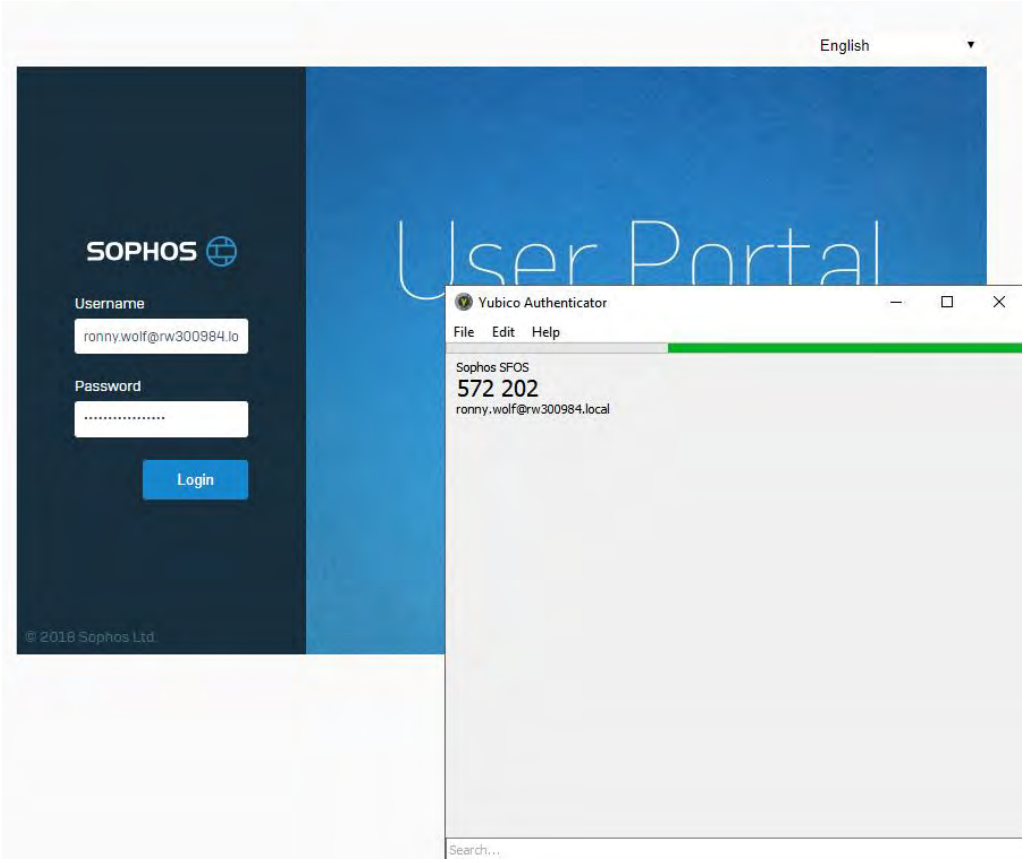
Speichern Sie die Credentials nun ab. Nun wird automatisch (solang der Yubico Authenticator geöffnet ist) ein zeitbasierter OTP generiert



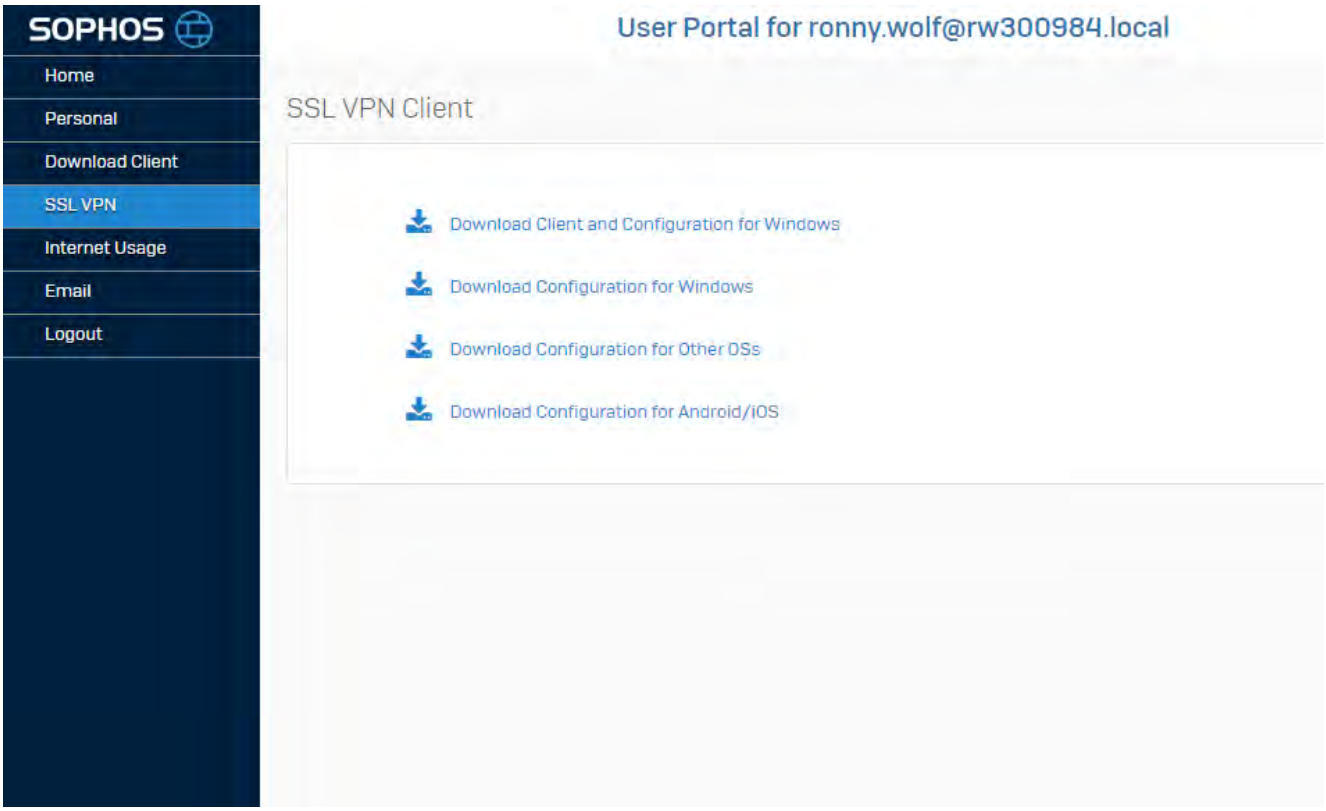
Nun können Sie die Authentifizierung von OTP z.B. am User Portal testen



Geben Sie hier den Benutzername, sowie das Passwort und den TOTP aus dem Yubico Authenticator ein.



Sie sind nun erfolgreich am User Portal angemeldet

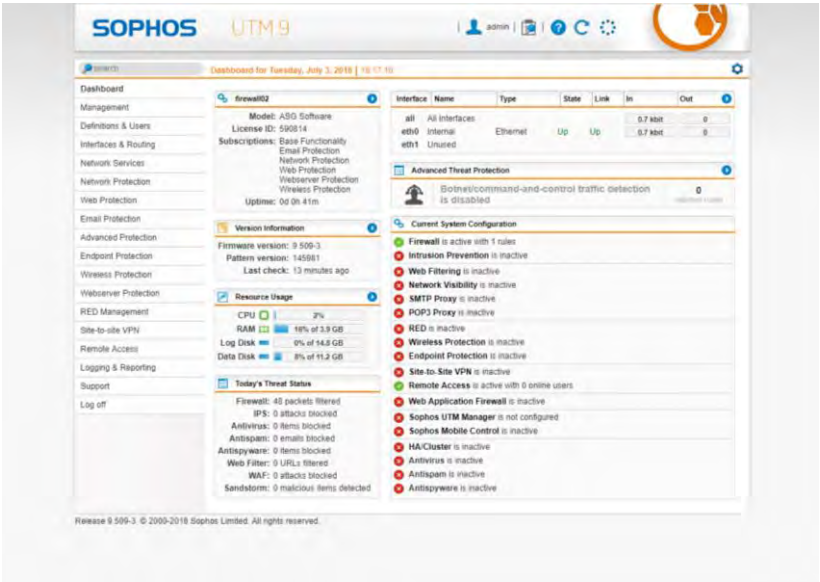


7.2. Sophos UTM Firewall mit Radius

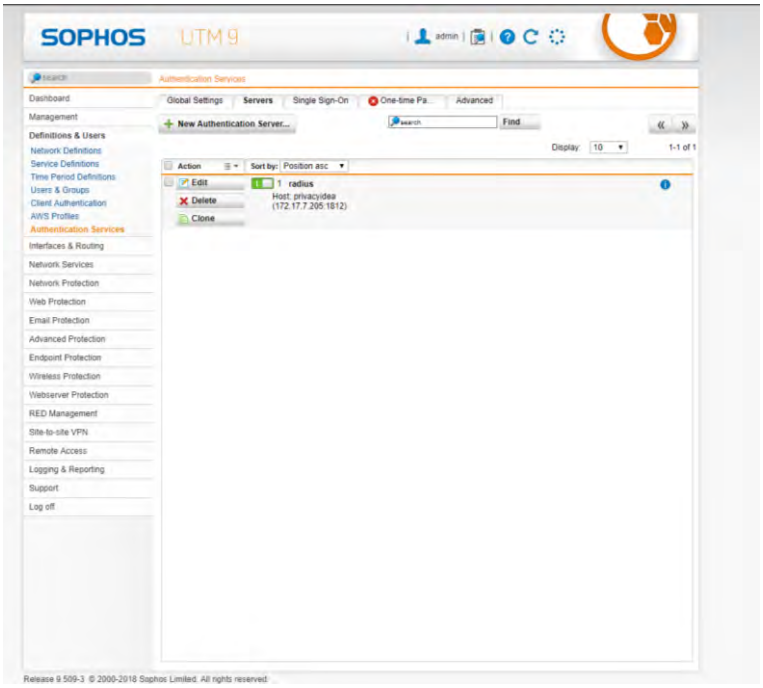
Der Sicherheitshersteller Sophos bietet noch eine weitere Firewall Lösung. In unserem Guide verwenden wir die Version 9.3xx. Auch hier gibt es verschiedene Möglichkeiten Benutzer zu authentifizieren.

7.2.1. Konfigurieren der Radius Anbindung

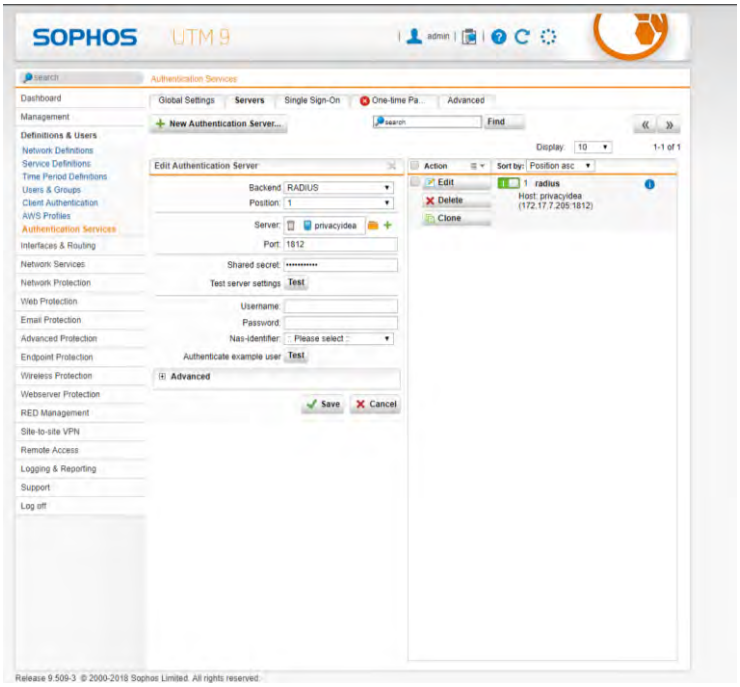
Als erstes konfigurieren wir die Radius Anbindung, so dass eine Kommunikation mit dem privacyIDEA Server möglich ist. Hierzu melden Sie sich am Sophos Webinterface als Administrator an.



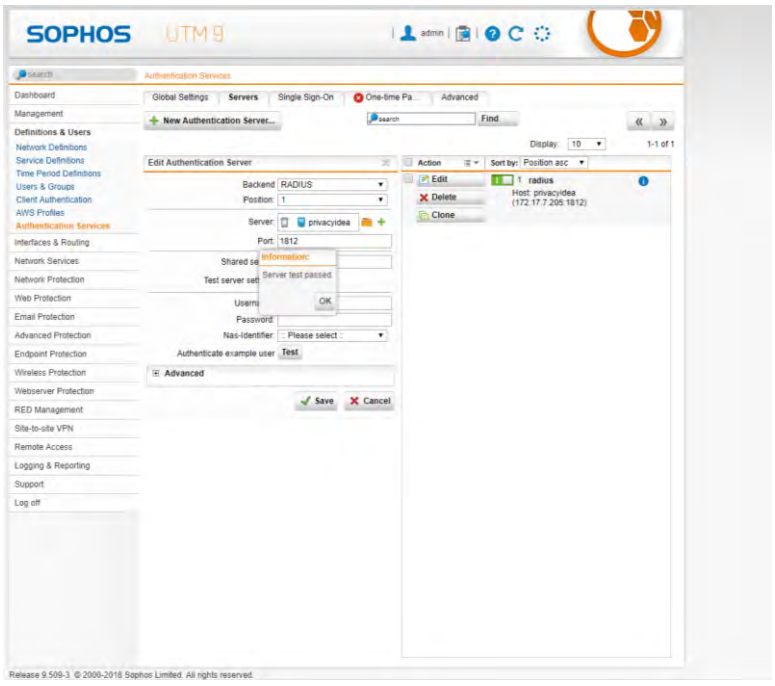
Klicken Sie nun auf Definitions & Users – Authentication Services



Definieren Sie nun wie im Screenshot unten gezeigt, den Radius Server. Das Shared Secret muss identisch mit dem in Kapitel 2, Abschnitt 8 konfigurierten sein.

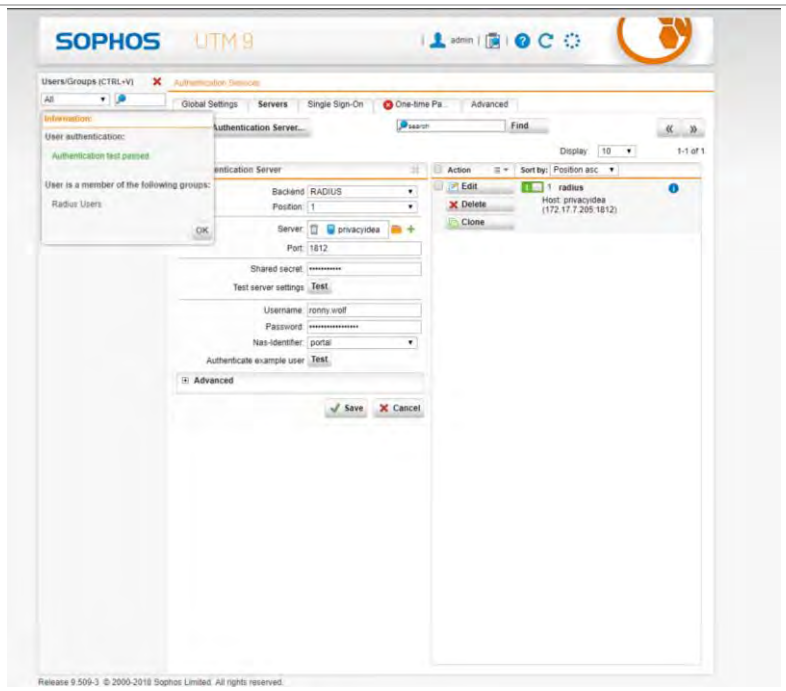


Bevor Sie fortfahren testen Sie die Verbindung zum Radius Server



Auch können Sie die Benutzerauthentifzierung testen. Geben Sie hier folgendes ein:

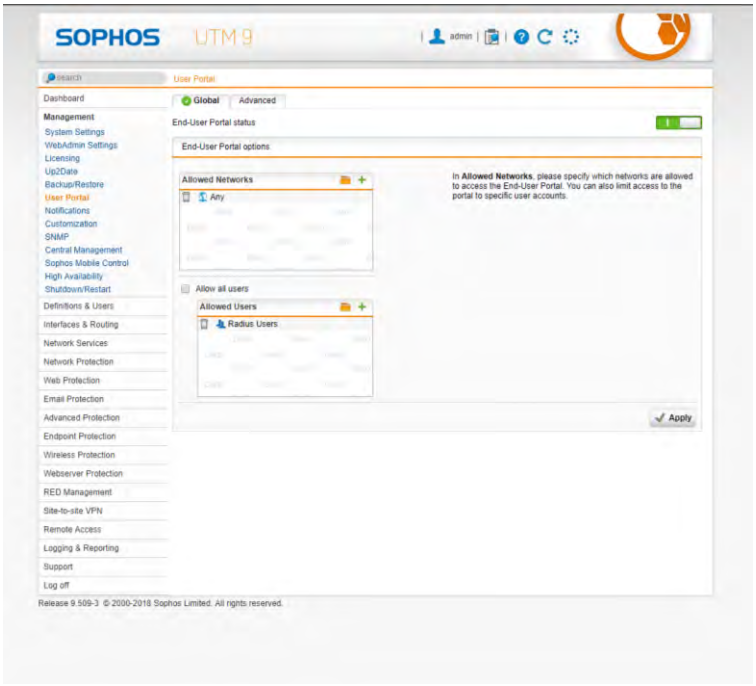
Username: Active Directory Benutzer
Password: Active Directory Passwort + Yubikey OTP



Die Radius Server Konfiguration ist nun abgeschlossen.

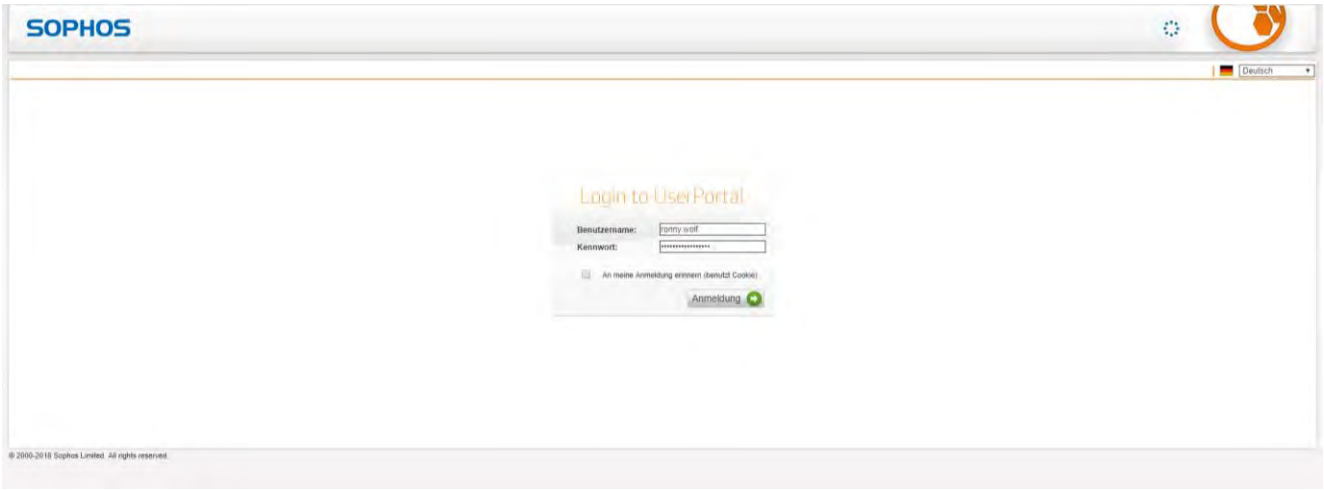
7.2.2. Anmelden an User Portal mit Yubikey

Damit Benutzer sich am User Portal der Sophos UTM mit den Radius Anmeldedaten authentifzieren können, müssen Sie die Gruppe Radius Uses, unter Management – User Portal – Global hinzufügen

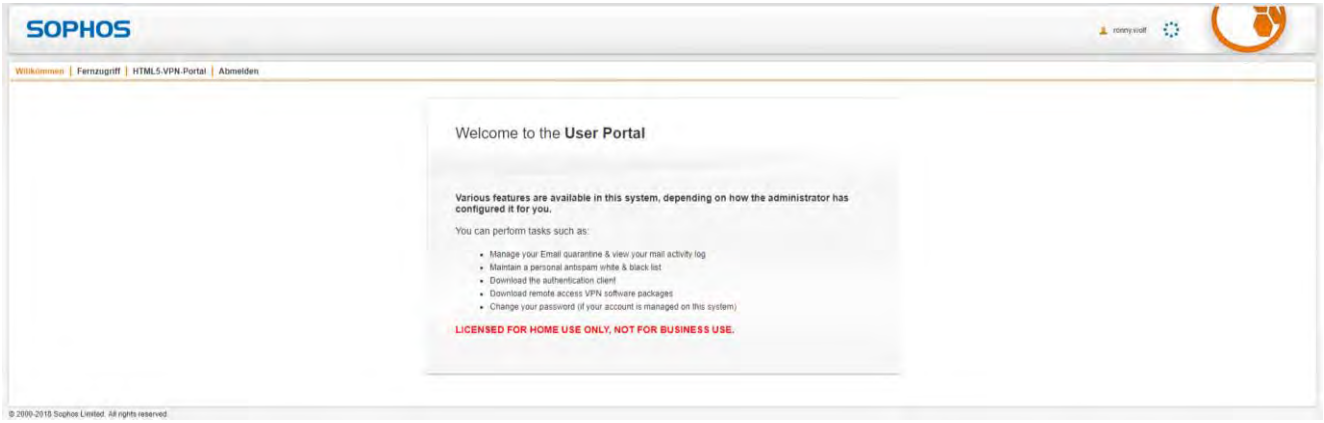


Nun können Sie die Anmeldung am Sophos User Portal testen. Hierbei geben Sie folgendes ein:

Benutzername: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP

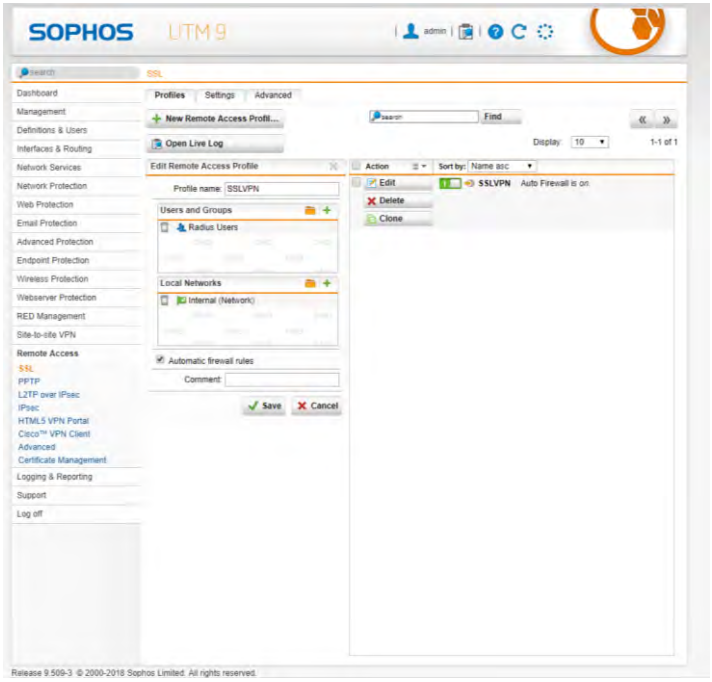


Sie sind nun erfolgreich am User Portal der Sophos UTM angemeldet



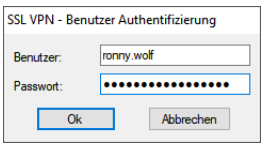
7.2.3. Anmelden via SSLVPN mit Yubikey

Möchten Sie SSL VPN mit einer 2 Faktor Authentifzierung absichern, müssen Sie unter Remote Access – SSL – Profiles, die Radius Users Gruppe hinzufügen

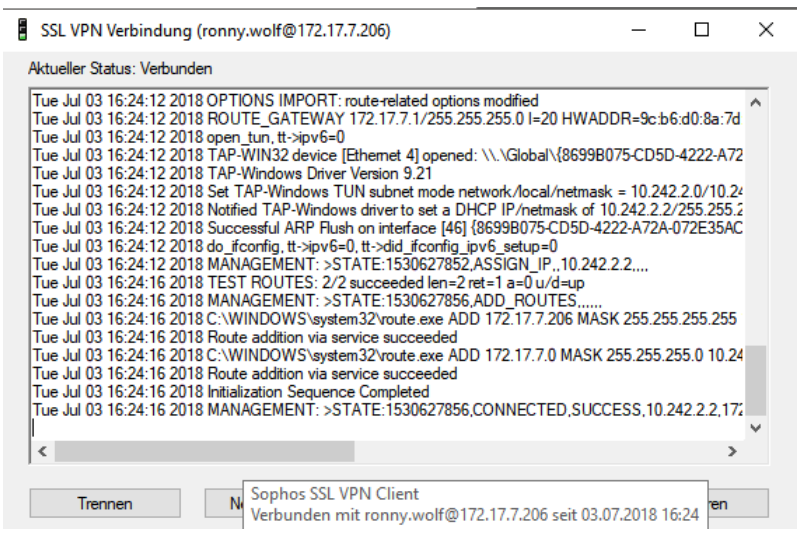


Nun können Sie die Radius Authentifzierung am Sophos SSL VPN Client (OpenVPN) testen. Geben Sie hierzu folgndes ein:

Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP



Sie sind nun erfolgreich via SSL VPN verbunden.



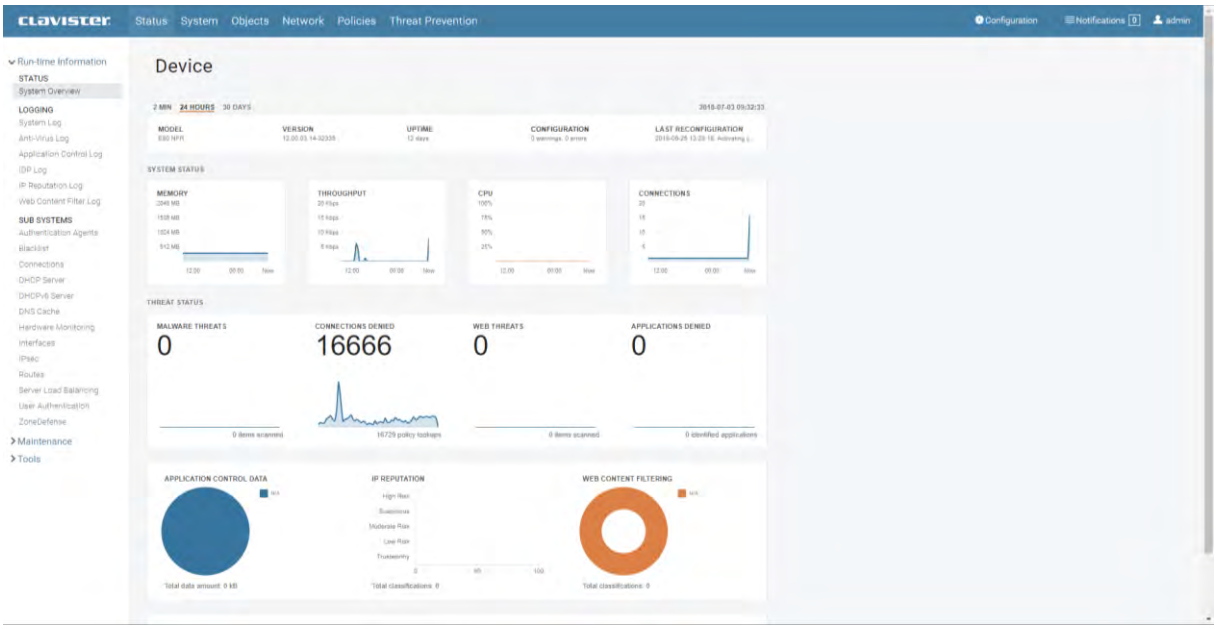
7.3. Clavister Firewall mit Radius

Die Firewalls von der Firma Clavister bieten die Möglichkeit eine Zwei Faktor Authentifzierung über eine Radius Anbindung zu realisieren.

Getested wurde die Clavister Firewall Version 12.

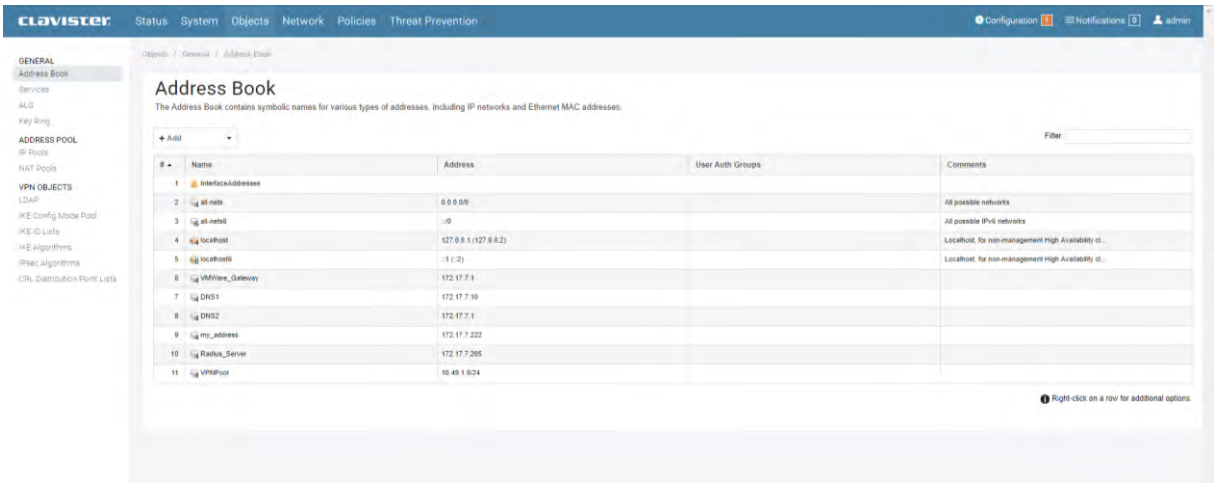
7.3.1. Konfigurieren der Radius Anbindung

Öffnen Sie das Clavister Webinterface als Administrator

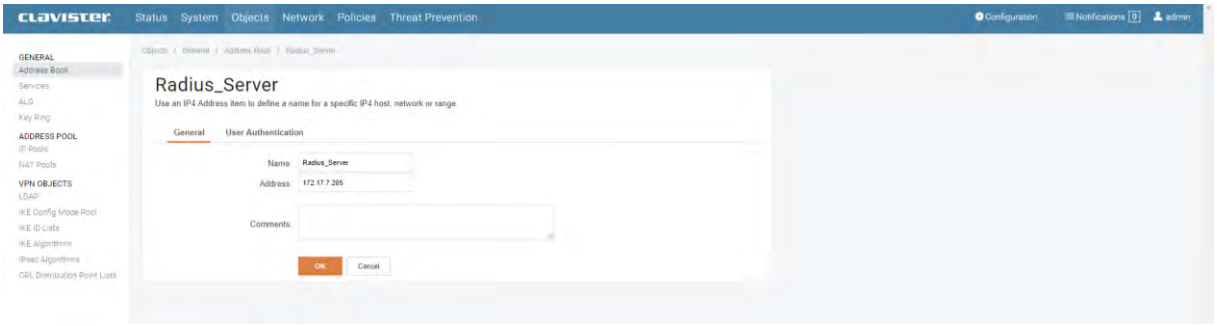


Legen Sie nun eine neue Definition im Address Book für den Radius Server an.

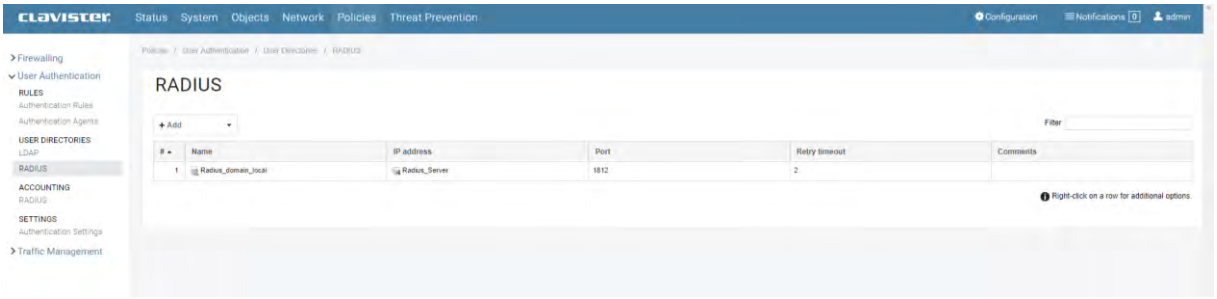
Klicken Sie hierzu auf Objects – Address Book



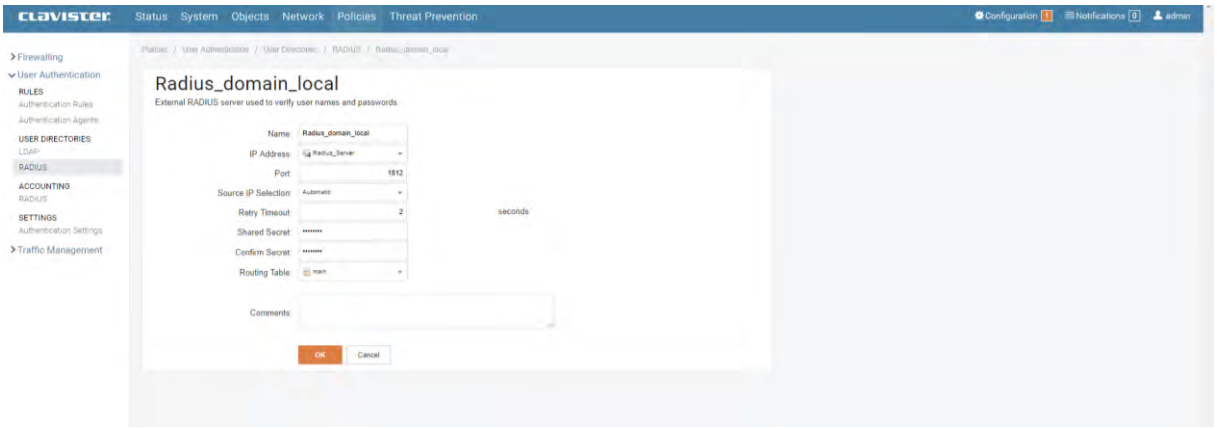
Klicken Sie auf Add und vergeben einen Namen, sowie die IP Addresse des Radius Servers (privacyIDEA)



Wechseln Sie nun in Policies – User Directories - Radius

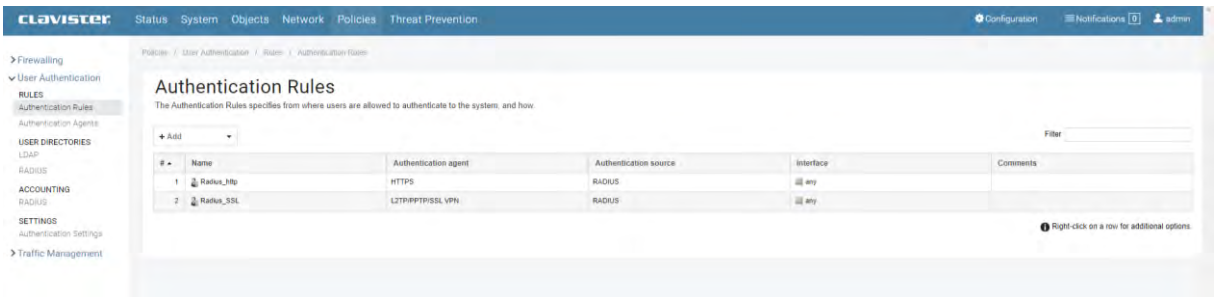


Klicken Sie auf Add und wählen das zuvor im Address Book erstellte Object des Radius Server aus und geben das Shared Secret, welches wir in Kapitel 2, Abschnitt 8 definiert haben.

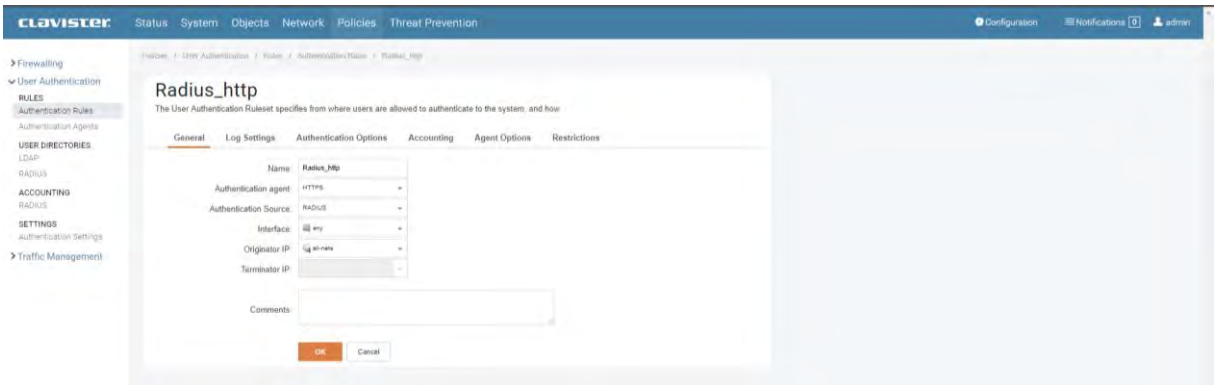


Nun müssen Sie definieren wo die Radius Authentifzierung zum Einsatz kommt. Hierfür sind die sogenannten Authentication Rules der Clavister Firewall zuständig.

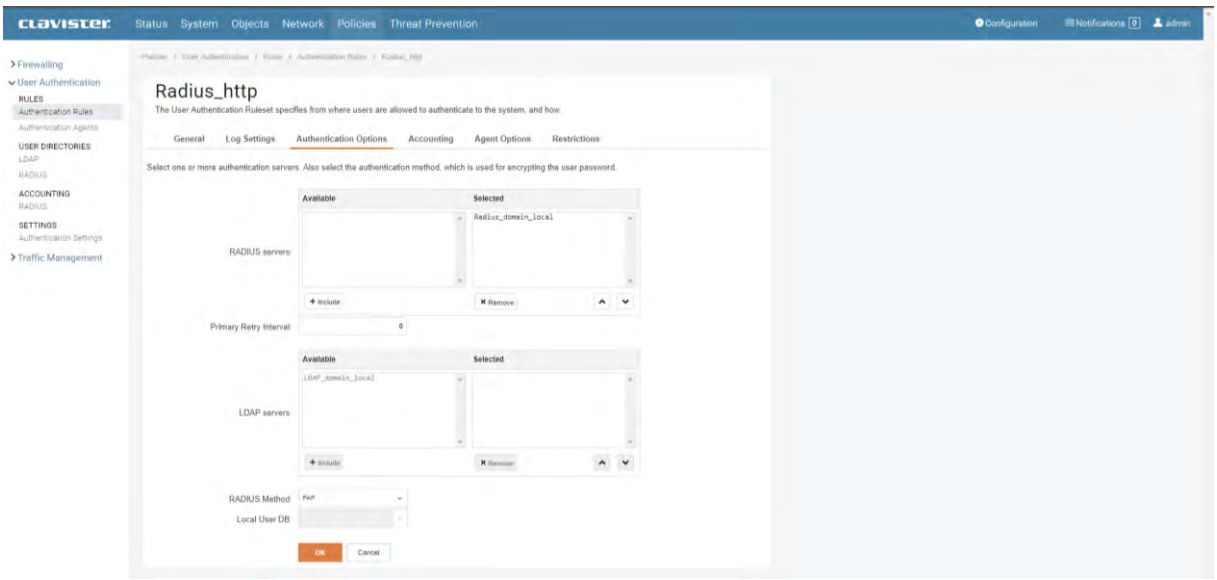
Klicken Sie auf Policies – User Authentication – Rules – Authentication Rules



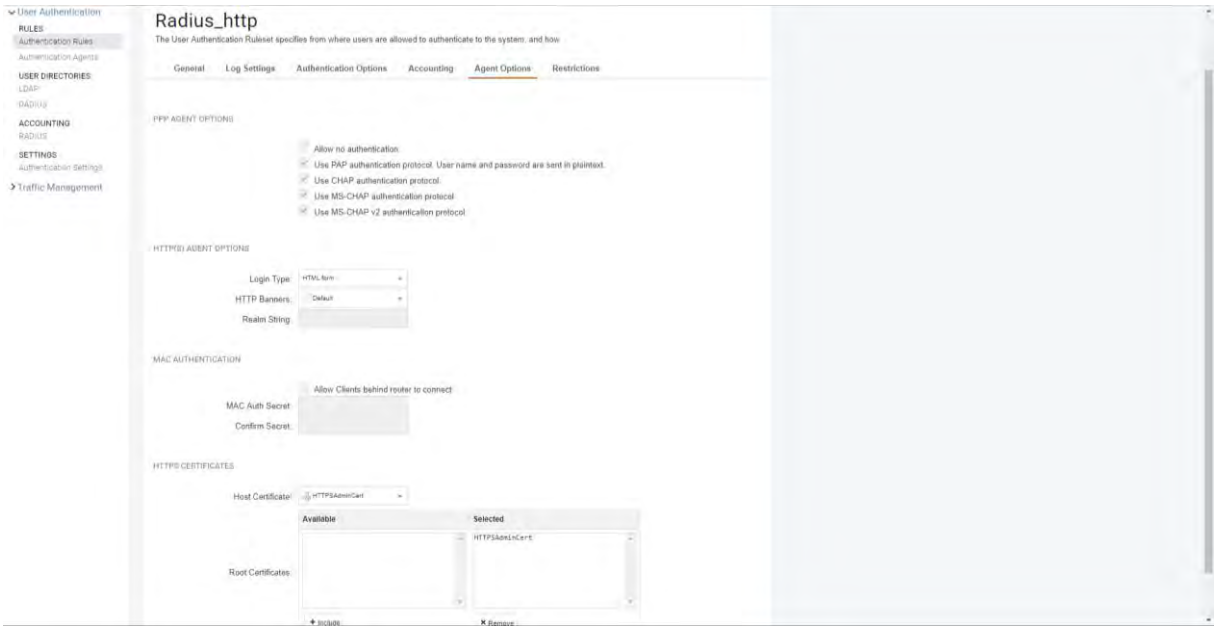
Klicken Sie auf Add und erstellen eine neue Regel für HTTP/HTTPs Authentifzierung



Wählen Sie nun unter Authentication Options den Radius Server, welchen wir zuvor konfiguriert haben aus. Als Radius Method wählen Sie PAP.

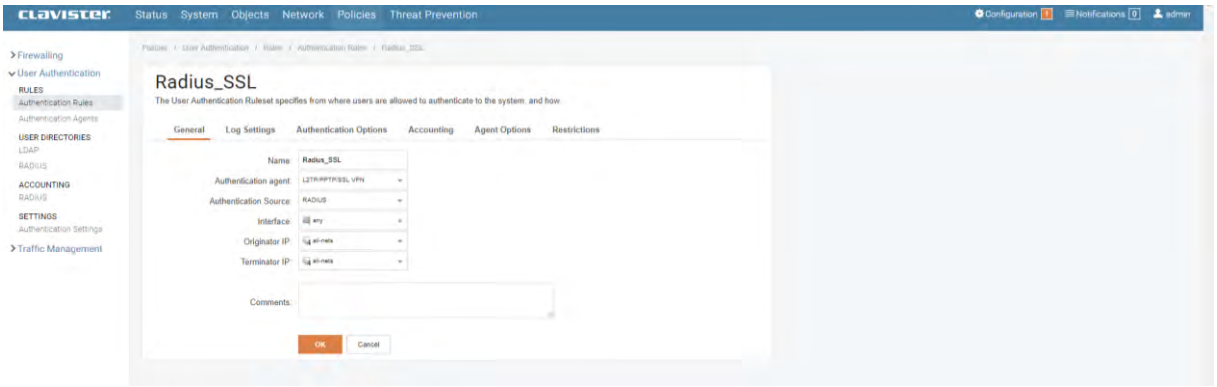


Unter Agent Options, müssen Sie grundsätzlich keine Einstellungen vornehmen, wichtig ist das PAP Authentication under PPP Agent Options aktiviert ist. Eventuell müssen Sie noch ein HTTPs Host Zertifikat auswählen, diese Einstellung betrifft aber nicht die eigentlich Radius Authentifzierung, sondern ist nur wichtig, wenn Sie eine Verbindung via HTTPs aufbauen möchten.

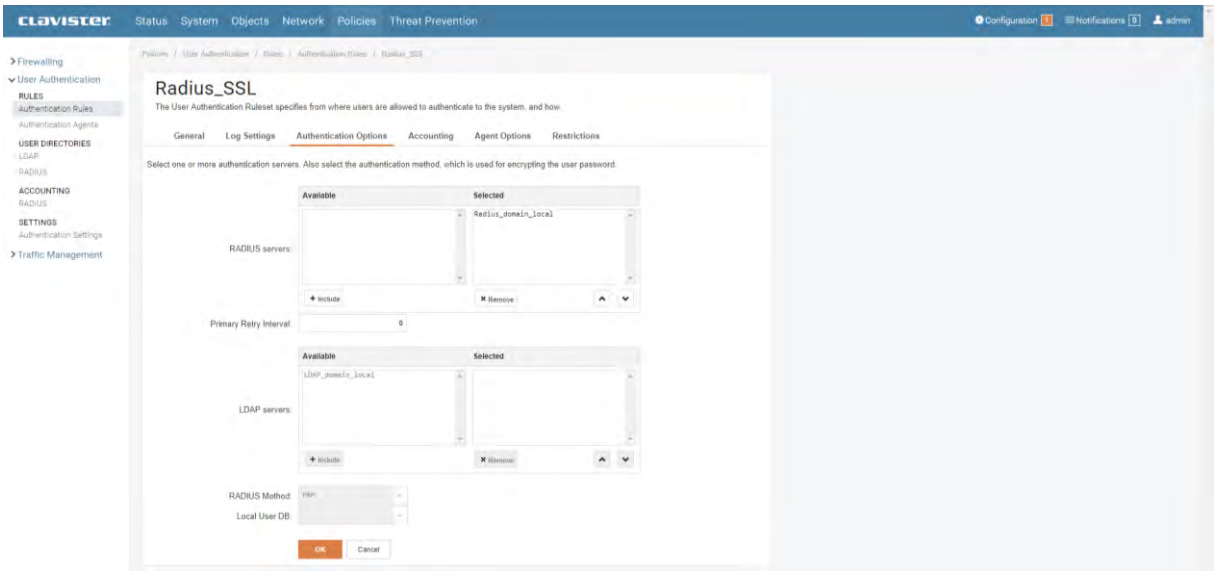


Damit wir die Zwei Faktor Authentifizierung auch über SSL VPN durchführen können, müssen wir eine zweite Authentication Rule erstellen.

Die Einstellungen hierbei sind identisch mit der HTTP/HTTPs Authentifzierung.

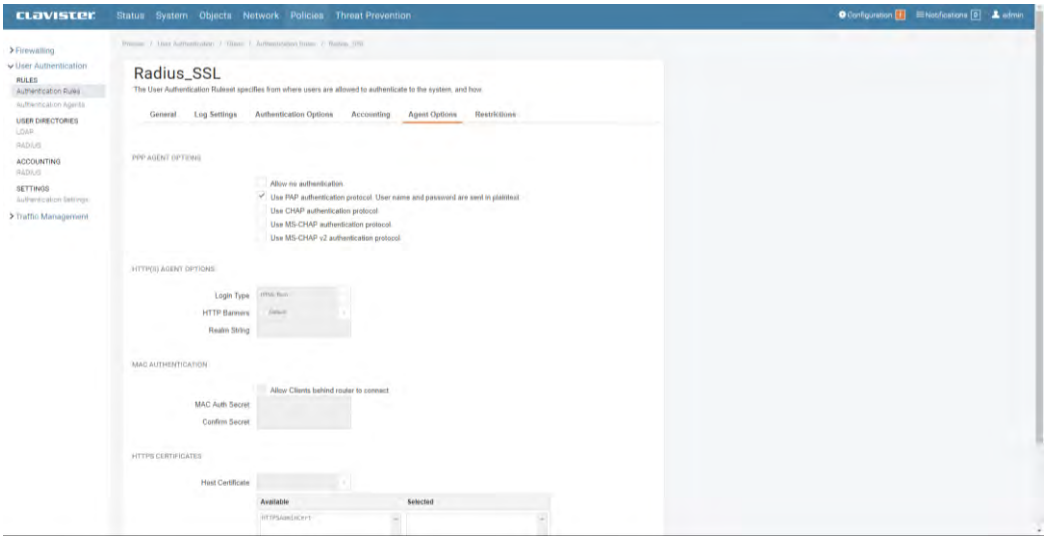


Wählen Sie auch hier den Radius Server, welchen wir zuvor konfiguriert haben aus.



Die Radius Method ist ausgegraut, sollte jedoch bereits auf PAP eingestellt sein.

Wählen Sie nun unter PPP Agent Options „Use PAP Authentication protocol“ und wählen alle anderen Protokolle ab.



Speichern und Übernehmen Sie nun die Konfiguration

Sie haben nun erfolgreich die Radius Server Anbindung für SSL VPN, das User Portal, sowie die HTTP Authentifizierung konfiguriert.

7.3.2. Anmelden an User Portal mit Yubikey

Öffnen Sie nun das SSL VPN User Portal über Ihren Webbrowser und geben folgende Benutzerdaten ein:

Username: Active Directory Benutzer mit Yubikey zugewiesen
Password: Active Directory Passwort + Yubikey OTP

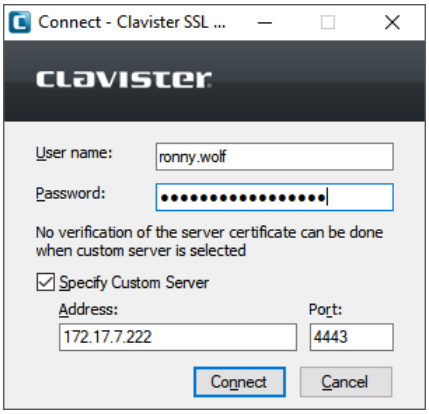
Sie sind nun erfolgreich am SSL VPN User Portal angemeldet.

7.3.3. Anmelden an SSLVPN mit Yubikey

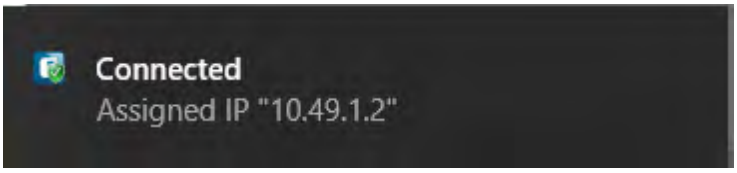
Installieren Sie nun den SSL VPN Client der Clavister Firewall und geben folgende Daten in das Anmeldefenster

Username: Active Directory Benutzer mit Yubikey zugewiesen
Password: Active Directory Passwort + Yubikey OTP

In unserem Beispiel müssen wir noch die Clavister Firewall via IP Addresse. Dies ist in einem produktiven Betrieb nicht notwendig.



Wir konnten uns nun erfolgreich mit einer 2 Faktor Authentifizierung anmelden und einen SSL VPN Tunnel aufbauen.



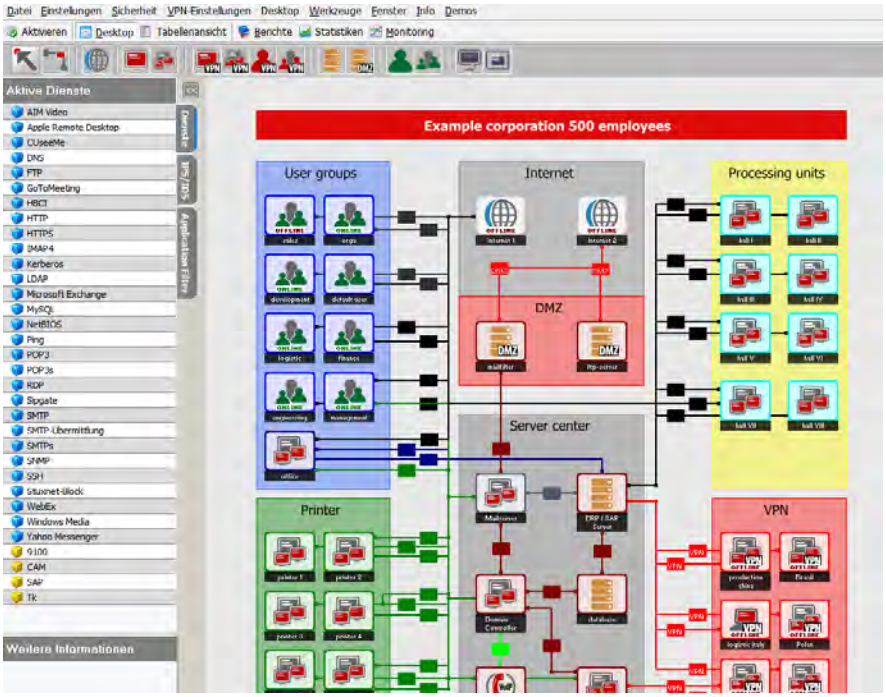
7.4. Rohde & Schwarz Firewall

Die Möglichkeiten der Radius Authentifzierung an einer Rohde & Schwarz Unified Firewall begrenzt, weshalb lediglich die HTTP Proxy Authentifzierung über Radius möglich ist. Deshalb wird nur die generelle Anbindung an den HTTP Proxy in diesem Guide behandelt.

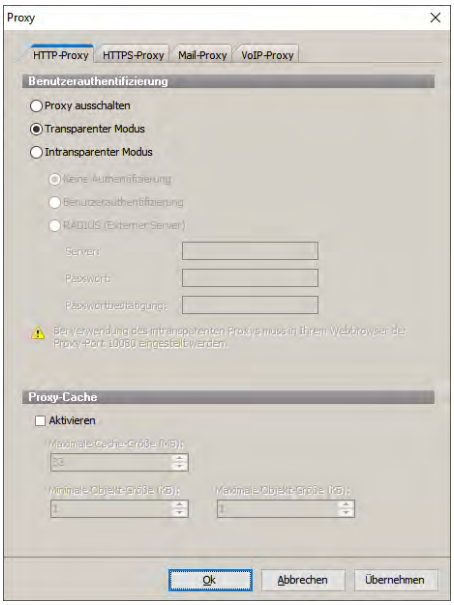
Wir verwenden die Rohde & Schwarz Unified Firewall Version 9.8

7.4.1. Konfigurieren der Radius Anbindung

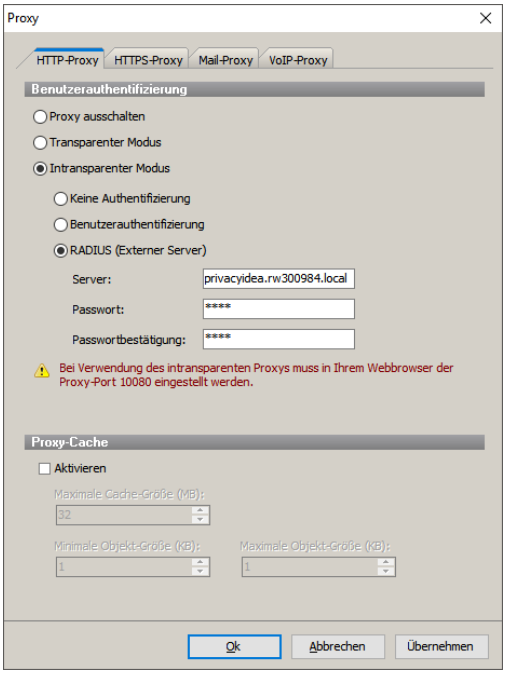
Öffnen Sie den Administrationsclient



Klicken Sie nun auf Einstellungen – Proxy



Die Radius Server Anbindung ist nur im Intransparenten Modus (Standard Proxy) möglich, aktivieren Sie den intransparenten Proxy und wählen Radius (Externer Server) aus. Geben Sie die IP Addresse oder FQDN des privacyIDEA Servers ein und geben das Shared Secret aus Kapitel 2, Absatz 8 ein



Wenn Benutzer nun über den HTTP Proxy ins Internet gelangen, müssen Sie folgende Daten eingeben

Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP

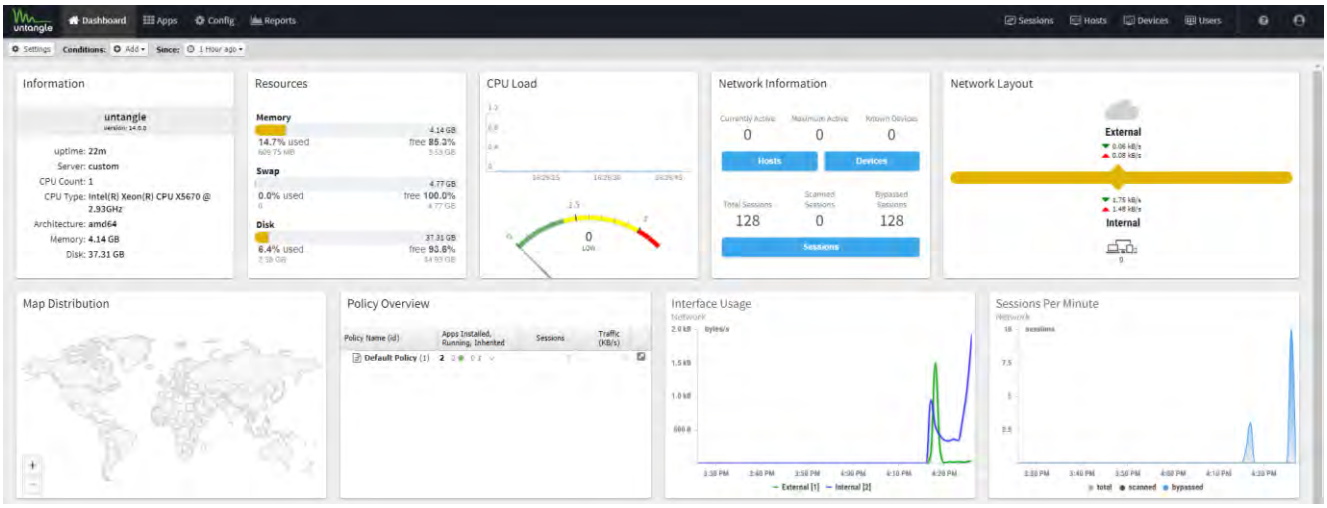
7.5. Untangle Firewall

Der Sicherheitshersteller Untangle bietet eine Plugin basierte Unified Threat Management Appliance an. Hierbei muss eine Zwei Faktor Authentifzierung über eine Radius Anbindung erfolgen.

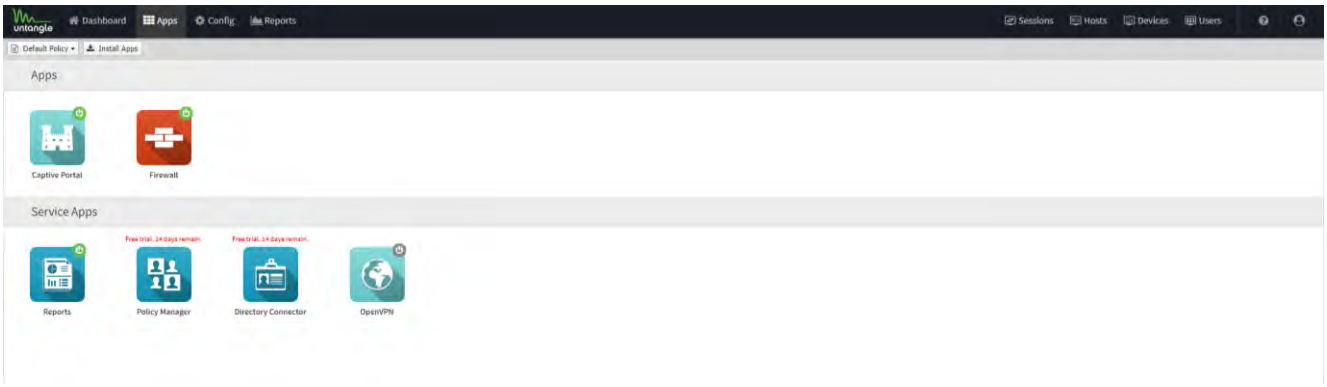
Der Guide wurde erstellt mit der Untangle Version 14.

7.5.1. Konfigurieren der Radius Anbindung

Öffnen Sie das Untangle Webinterface als Administrator



Klicken Sie auf Apps

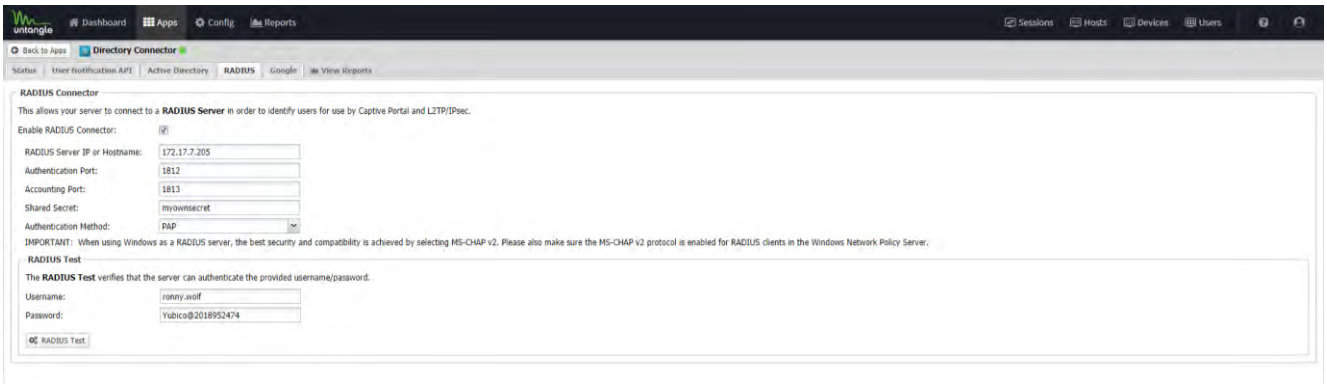


Klicken Sie auf Directory Connector

Im Directory Connector wählen Sie nun Radius und aktivieren diesen.

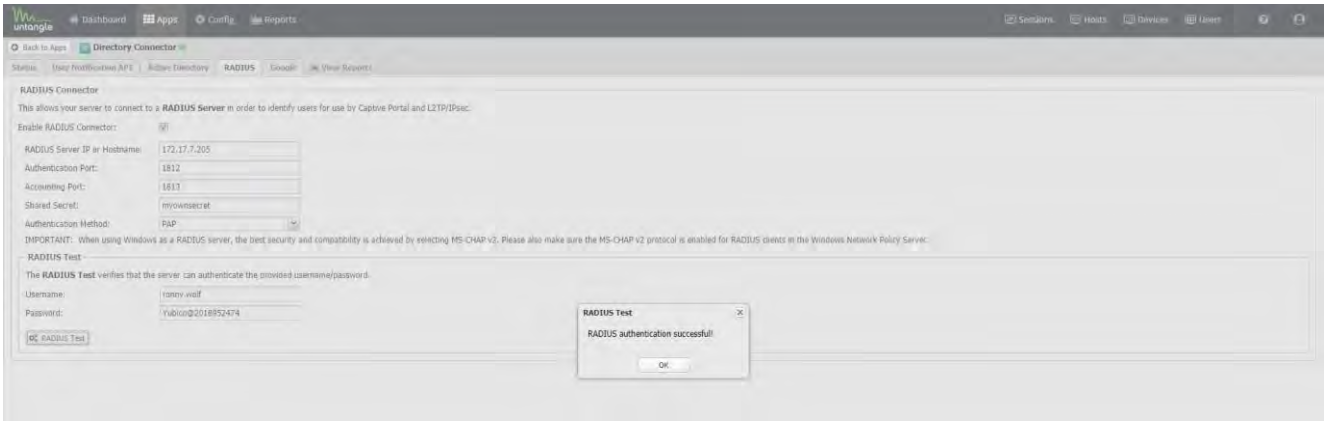
Bitte geben Sie nun die Parameter des privacyIDEA Radius Servers ein.

Radius Server IP or Hostname: privacyIDEA Server
Shared Secret: Shared Secret aus Kapitel 2, Absatz 8
Authentication Method: PAP



Sie können nun die Radius Authentifzierung testen. Geben Sie hierzu

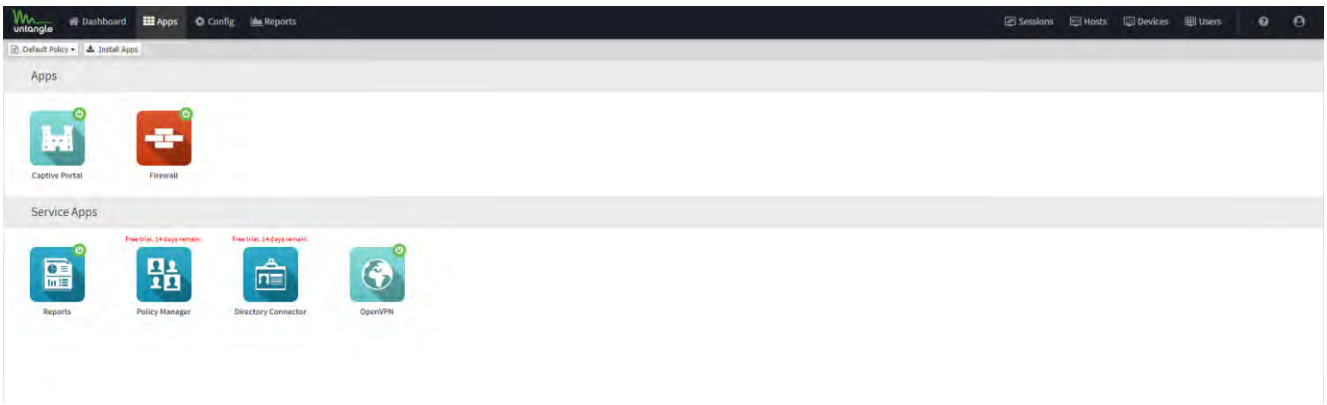
Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP



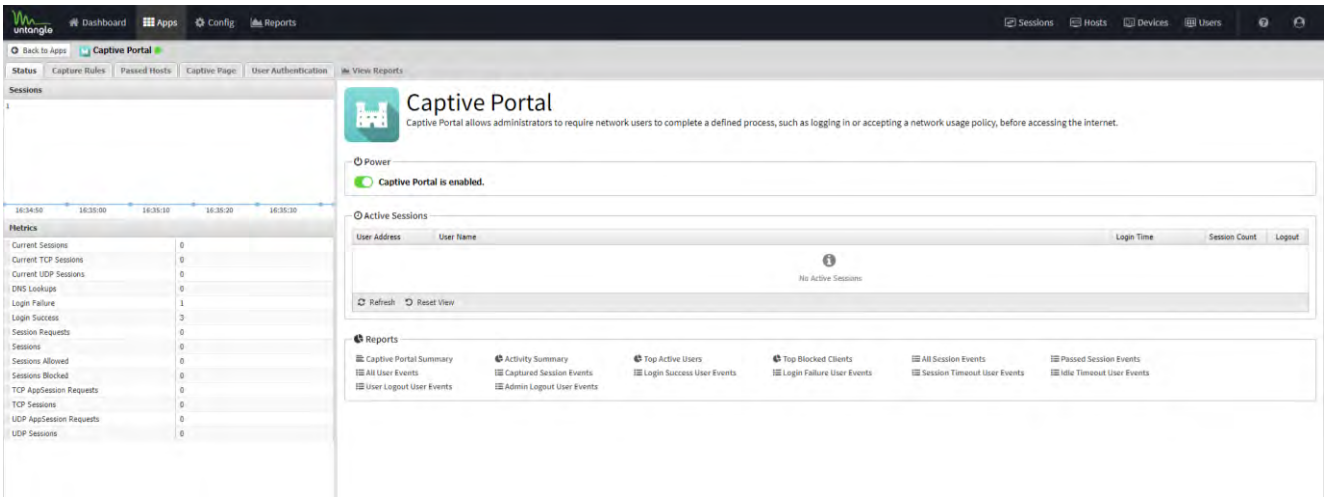
Sie haben sich nun erfolgreich die Radius Server Anbindung konfiguriert.

7.5.2. Anmelden an Captive Portal mit Yubikey

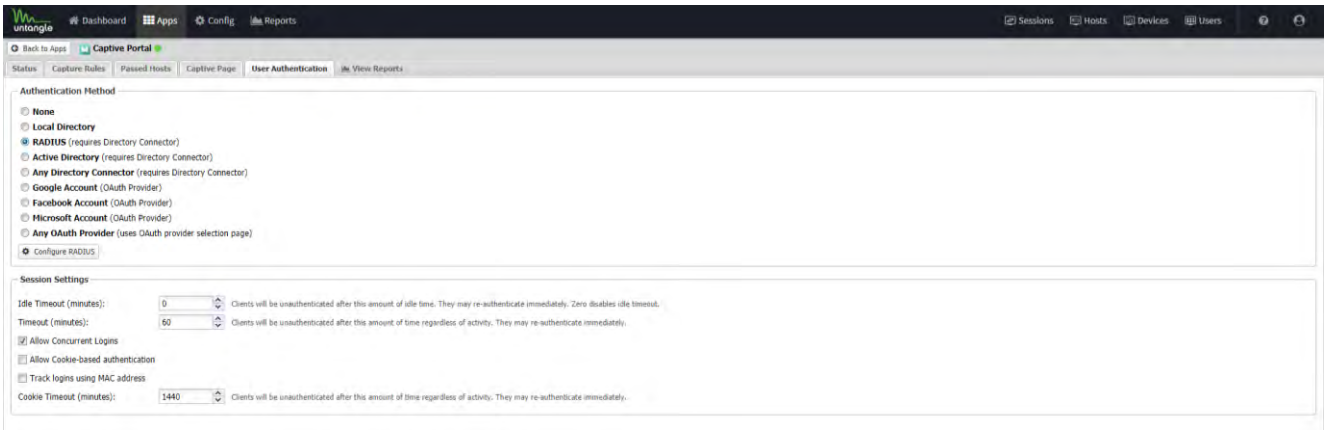
Um eine Zwei Faktor Authentifzierung am Captive Portal von Untangle zu erreichen. Klicken Sie auf Apps – Captive Portal



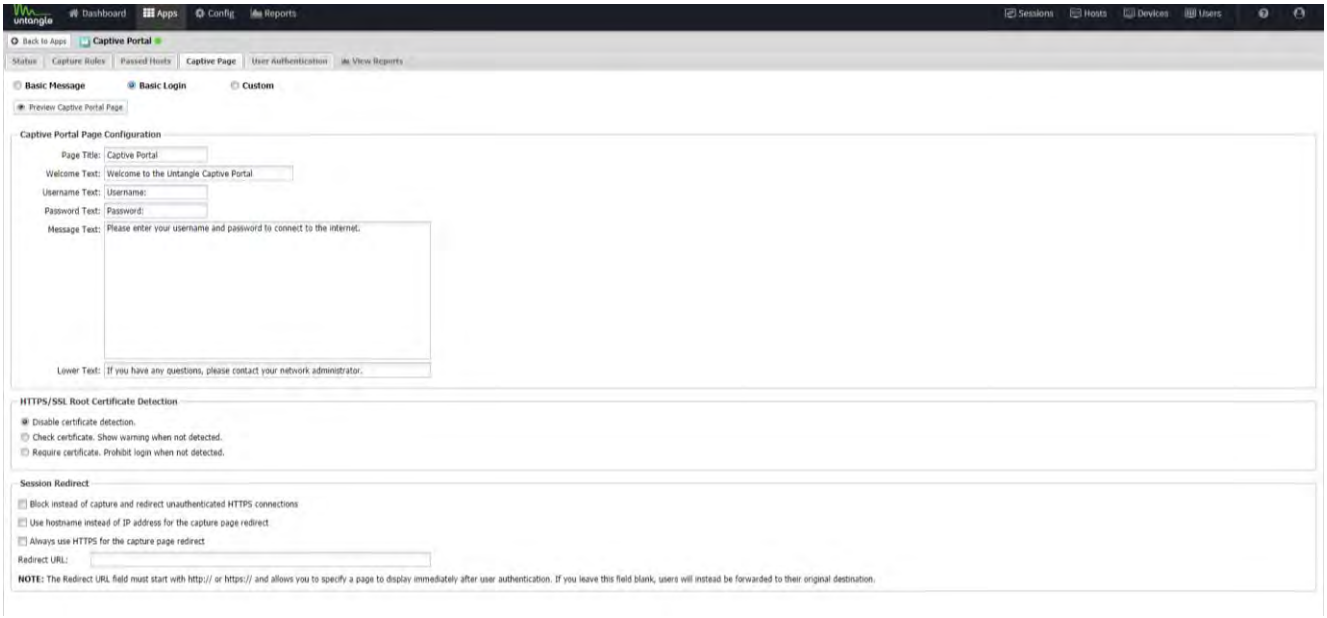
Wählen Sie nun User Authentication



Selektieren Sie unter Authentication = Radius

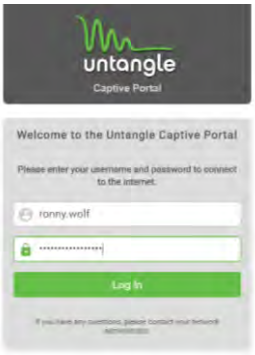


Damit eine Benutzerauthentifzierung (Username + Passwort) am Captive Portal erforderlich ist, müssen Sie noch die Captive Page, auf Basic Login konfigurieren.



Sie können nun das Captive Portal testen, in dem Sie folgende Benutzerdaten eingeben.

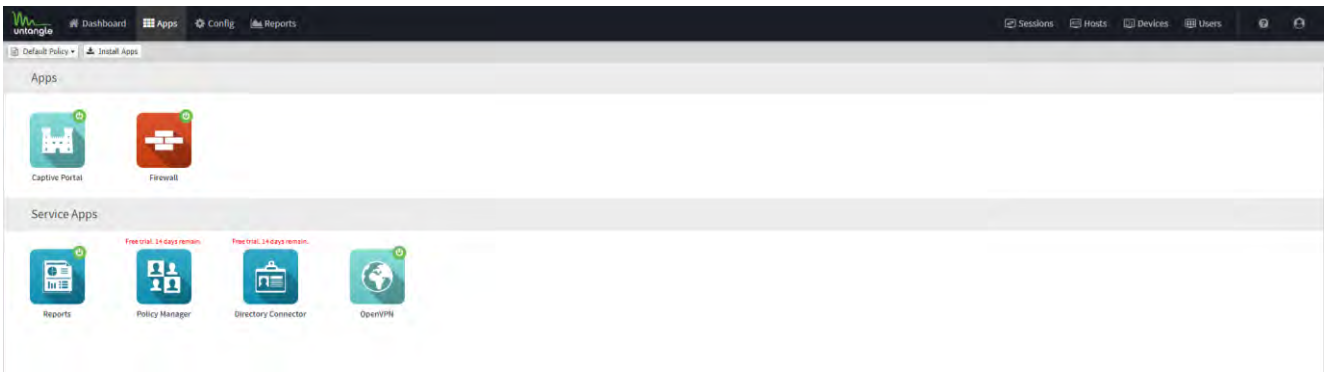
Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP



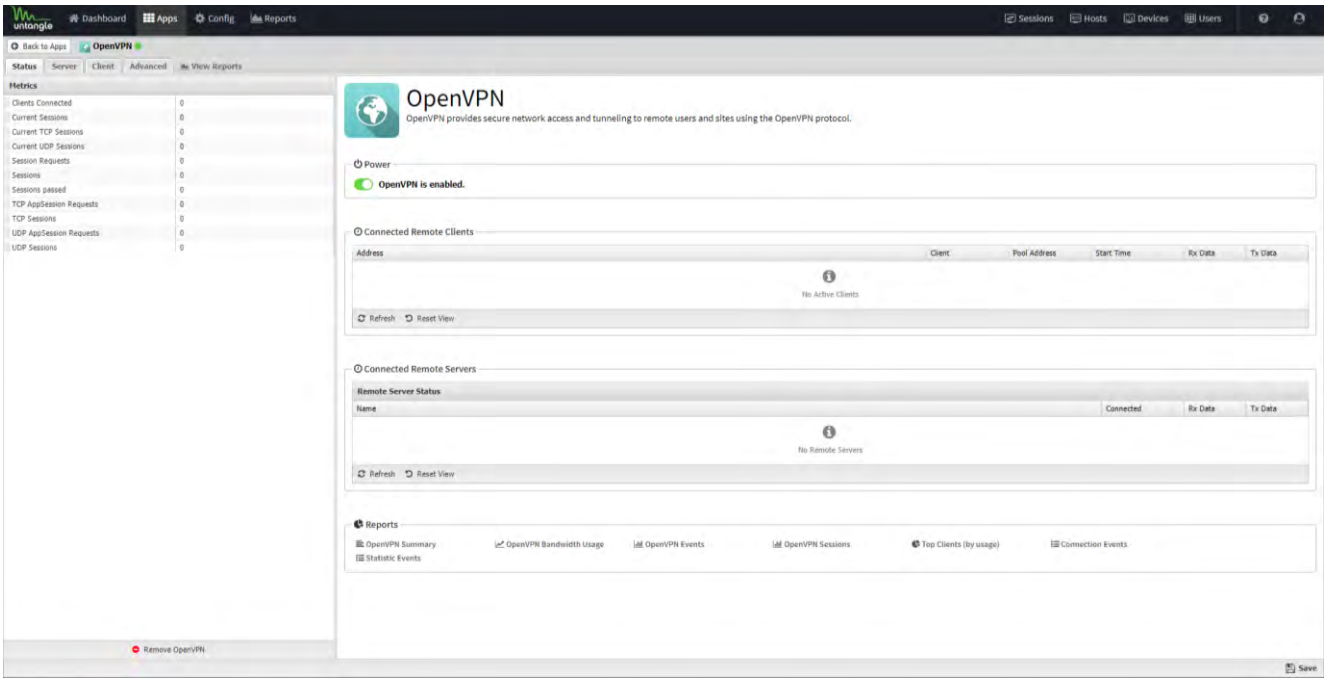
War die Anmeldung erfolgreich, erhalten Sie folgende Meldung

7.5.3. Anmeldung via OpenVPN mit Yubikey

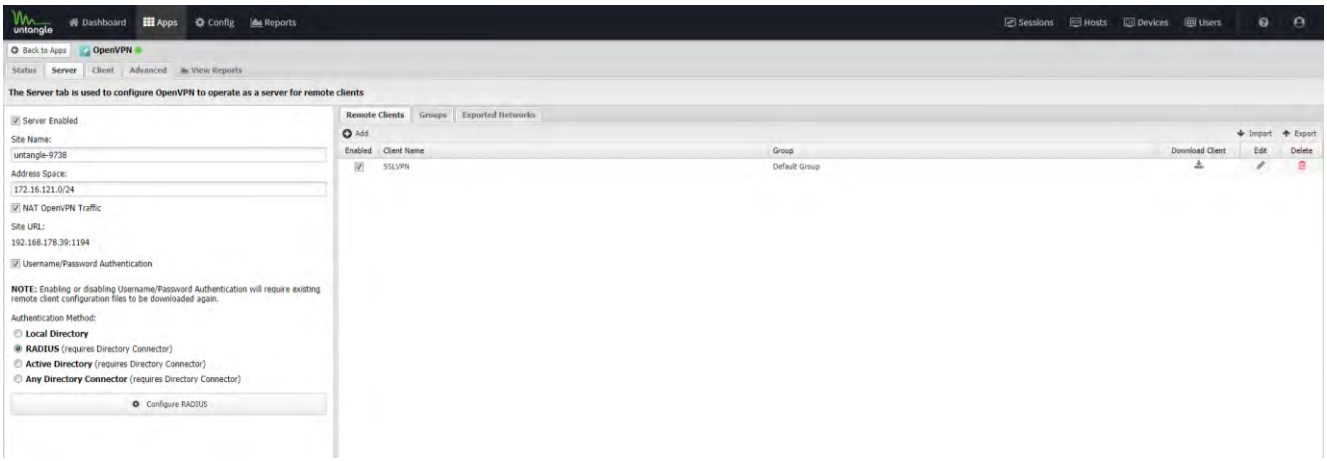
Um eine SSL VPN (OpenVPN) Anmeldung mit einem zweiten Faktor zu realisieren. Klicken Sie auf Apps – OpenVPN



Klicken Sie auf Server

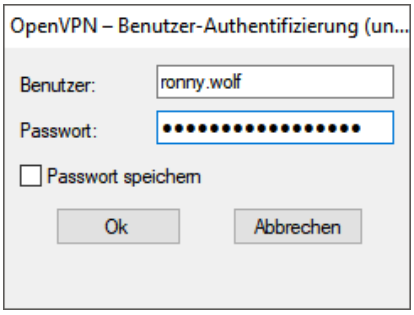


Aktivieren Sie den OpenVPN Server und wählen als Authentication Method: Radius

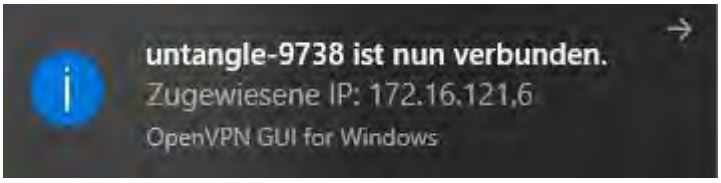


Nachdem Sie den OpenVPN Client von Untangle erfolgreich installiert haben, können Sie sich wie folgt anmelden:

Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP



Wir haben uns nun erfolgreich am OpenVPN Server der Untangle Appliance angemeldet und einen VPN Tunnel aufgebaut.

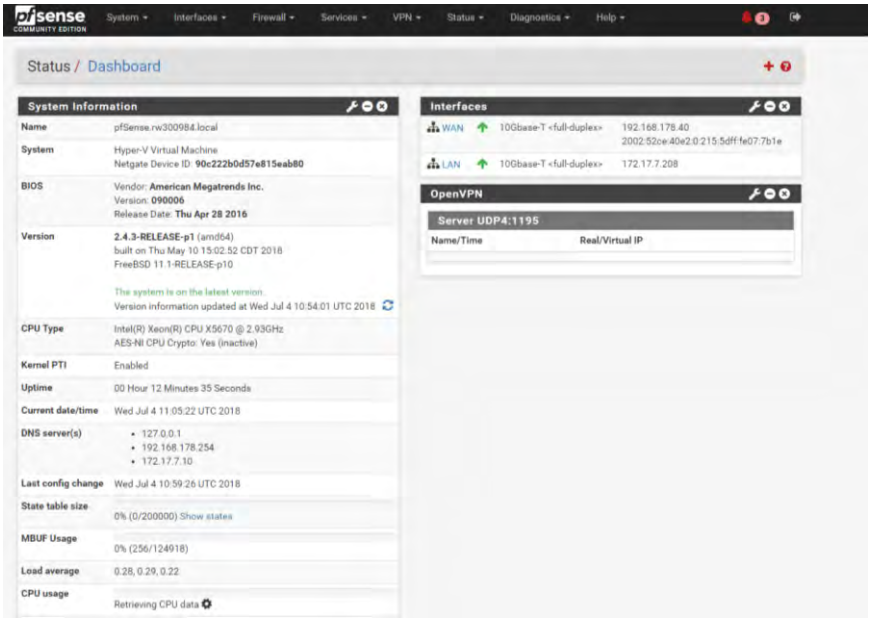


7.6. pfSense Firewall

Die OpenSource Firewall pfSense bietet die Möglichkeit eine Zwei Faktor Authentifizierung via Radius. In diesem Guide kommt die pfSense Version 2.4.x zum Einsatz.

7.6.1. Konfigurieren der Radius Anbindung

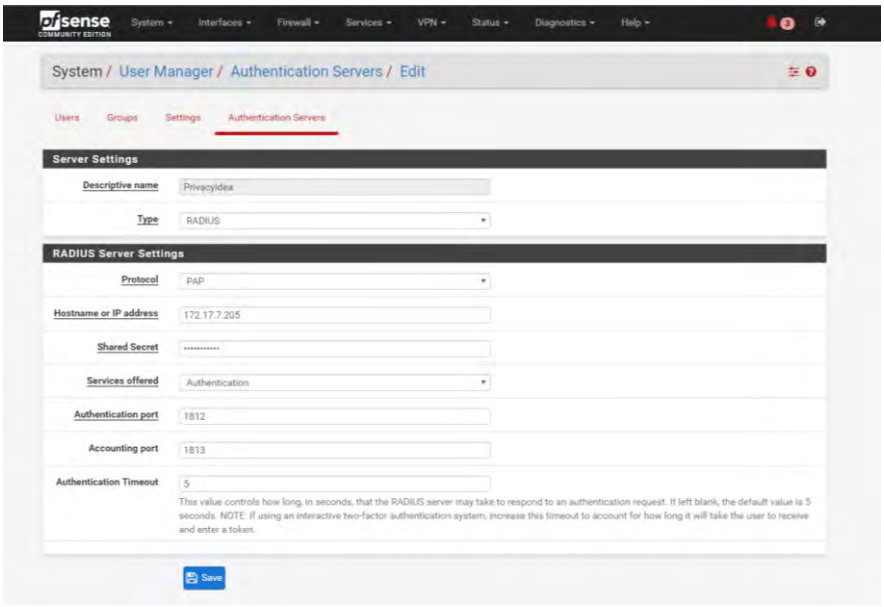
Melden Sie sich am pfSense Webinterface als Administrator an.



Klicken Sie nun auf System – User Manager - Authentication Servers

Definieren Sie folgende Parameter:

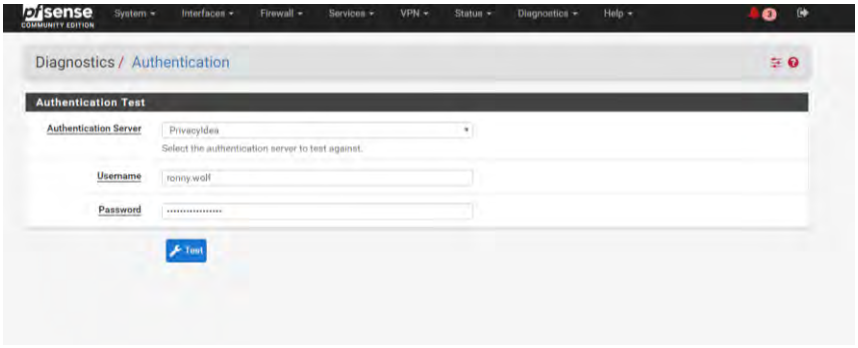
Type: Radius
Protocol: PAP
Hostname or IP address: privacyIDEA Server
Shared Secret: Shared Secret aus Kapitel 2, Absatz 8



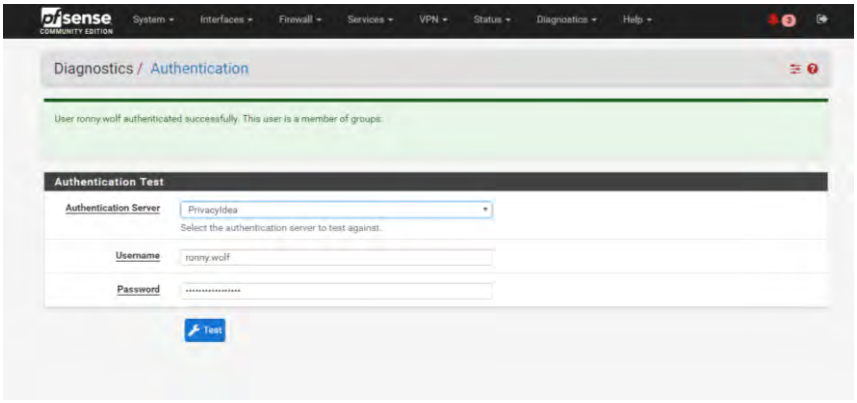
Testen Sie nun die Authentifizierung am Radius Server über Diagnostics – Authentication

Geben Sie hierzu folgende Benutzerdaten ein:

Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP



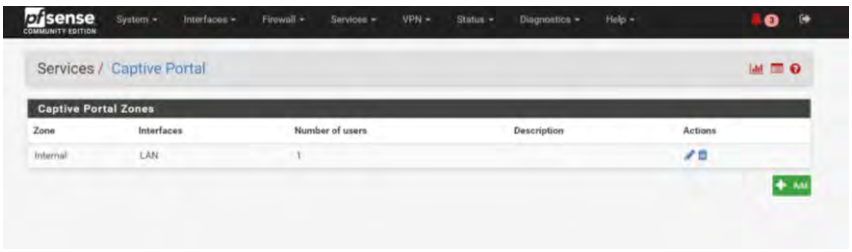
Die Zwei Faktor Authentifzierung am privacyIDEA Server war erfolgreich



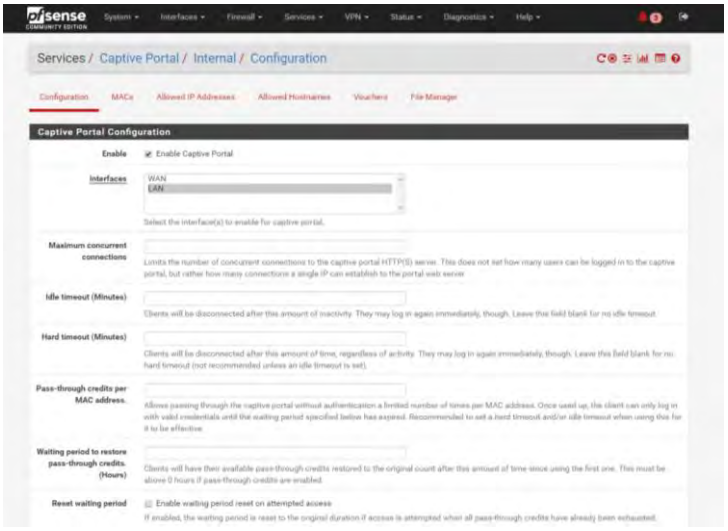
Die Radius Server Anbindung ist nun vollständig konfiguriert.

7.6.2. Anmeldung an Captive Portal mit Yubikey

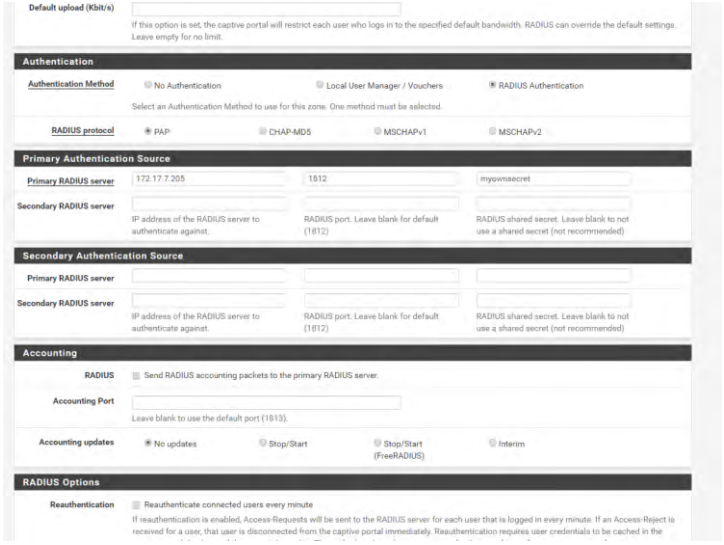
Um sich am Captive Portal anmelden zu können, müssen wir dieses konfigurieren. Klicken Sie hierzu auf Services – Captive Portal



Alle Einstellungen können Sie gemäß Ihren Anforderungen konfigurieren



Unter Authentication wählen Sie Radius Authentication und als Radius Protocol wählen Sie PAP. Darüberhinaus geben Sie unter Primary Radius Server die IP Adresse oder FQDN des privacyIDEA Servers ein, sowie das Shared Secret aus Kapitel 2, Absatz 8.



Sie können nun die Captive Portal Anmeldung testen. Geben Sie hierzu folgende Anmeldedaten ein:

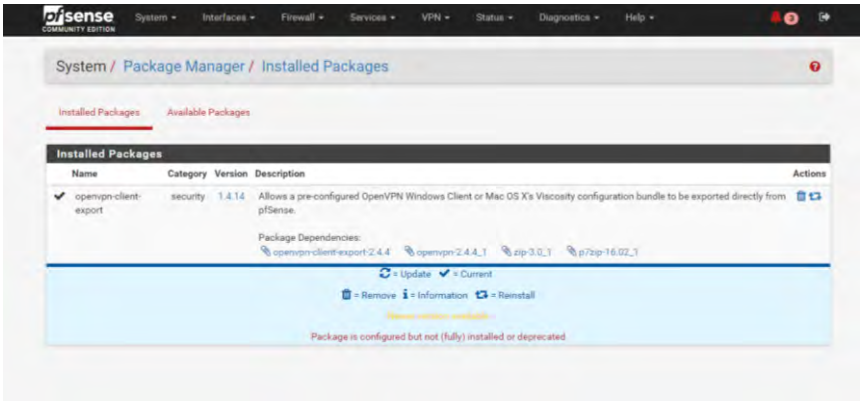
Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP

Die Anmeldung mit einem zweiten Faktor war erfolgreich.

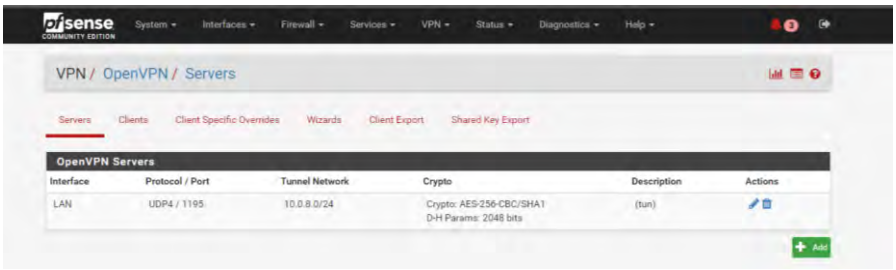
7.6.3. Anmeldung via OpenVPN mit Yubikey

Sie können ebenfalls eine OpenVPN (SSL VPN) Verbindung über eine zwei Faktor Authentifzierung absichern. Um die Konfiguration des OpenVPN Client zu vereinfachen, installieren wir ein zusätzliches Paket.

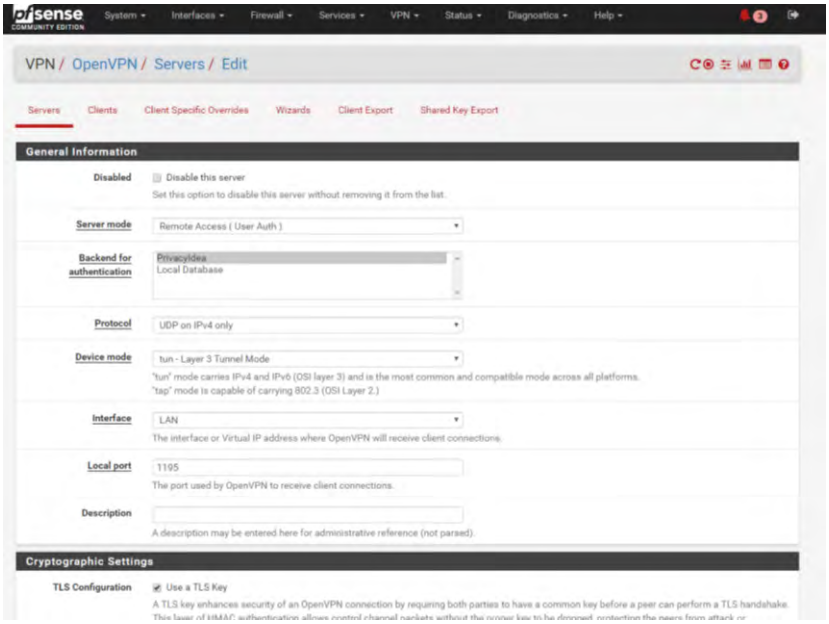
Klicken Sie auf System – Package Manager und installieren das OpenVPN-Client-Export Paket.



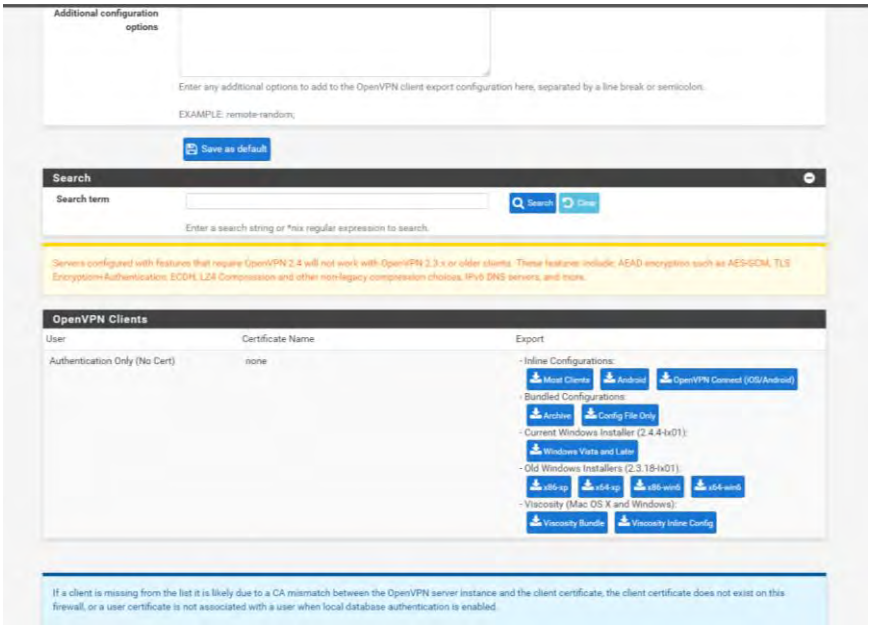
Wechseln Sie nun zu VPN – OpenVPN – Servers und fügen einen neuen Server hinzu oder editieren einen bestehenden



Wählen Sie in den Einstellungen des OpenVPN Servers als Backend for authentication den zuvor definierten Radius Server

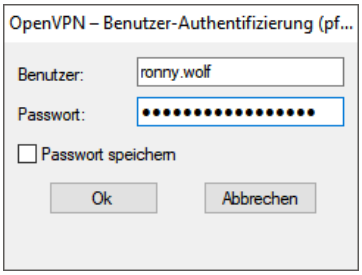


Unter VPN – OpenVPN – Client Export können Sie nun die Installationsdateien und/oder OpenVPN Konfiguration herunterladen

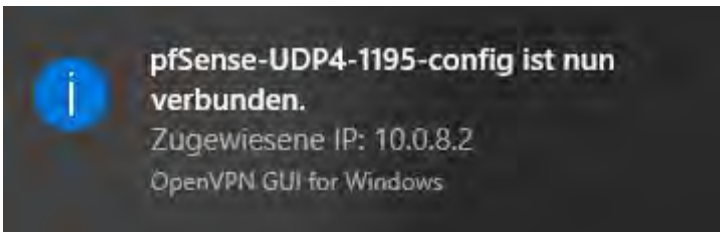


Nachdem Sie den OpenVPN Client erfolgreich installiert haben, können Sie einen VPN Tunnel aufbauen. Hierzu geben Sie folgende Anmeldedaten ein:

Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP



Wir haben nun eine OpenVPN Verbindung mit einer zwei Faktor Authentifzierung erfolgreich aufgebaut.

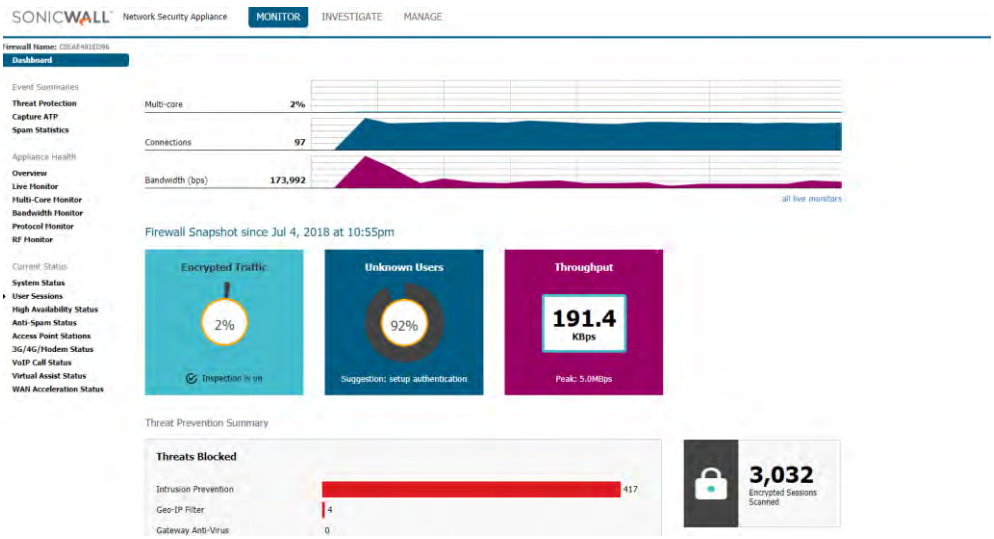


7.7. Sonicwall NSA Firewall

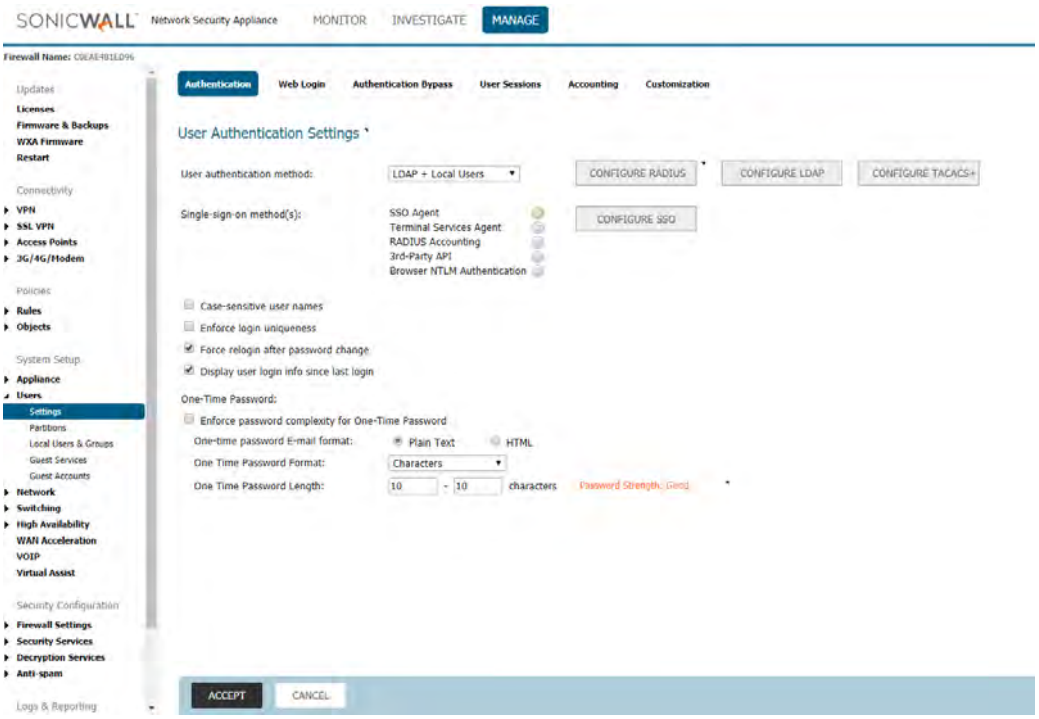
Der Hersteller Sonicwall bietet die Möglichkeit eine Zwei Faktor Authentifzierung anhand von Radius oder einem integrierten TOTP (zeitbasiert) zu realisieren. In diesem Guide behandeln wir nur die Radius Anbindung.

7.7.1. Konfigurieren der Radius Anbindung

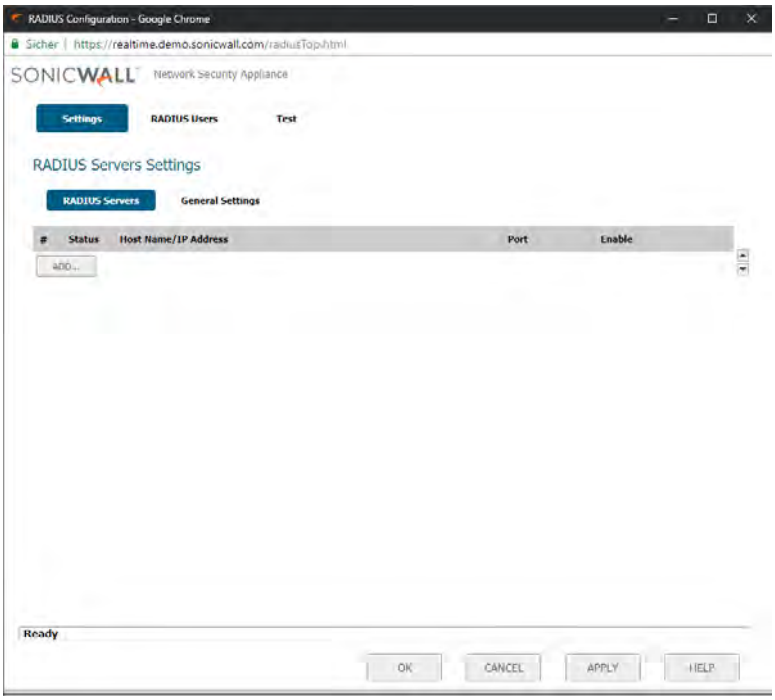
Öffnen Sie das Sonicwall NSA Webinterface als Administrator.



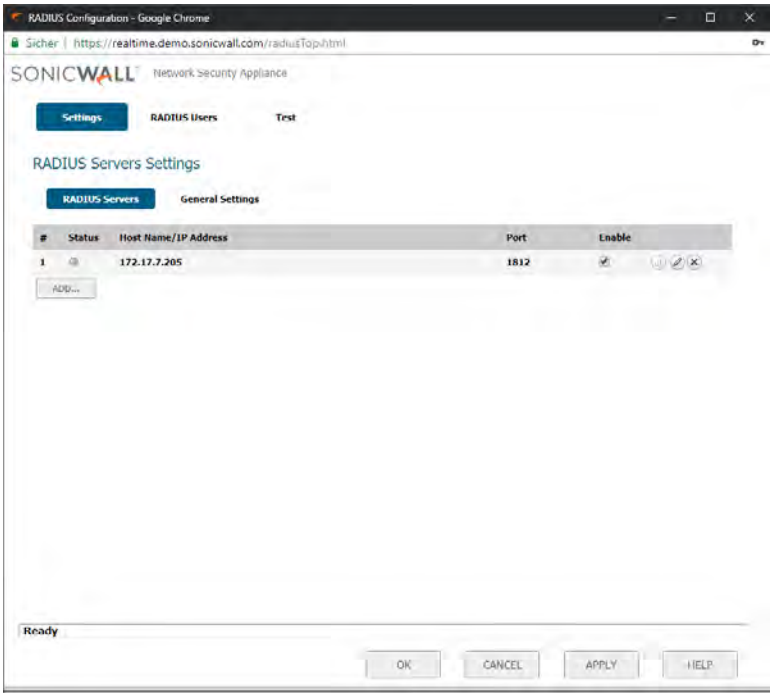
Wechseln Sie nun zu Manage – System Setup – Settings



Klicken Sie auf Configure Radius

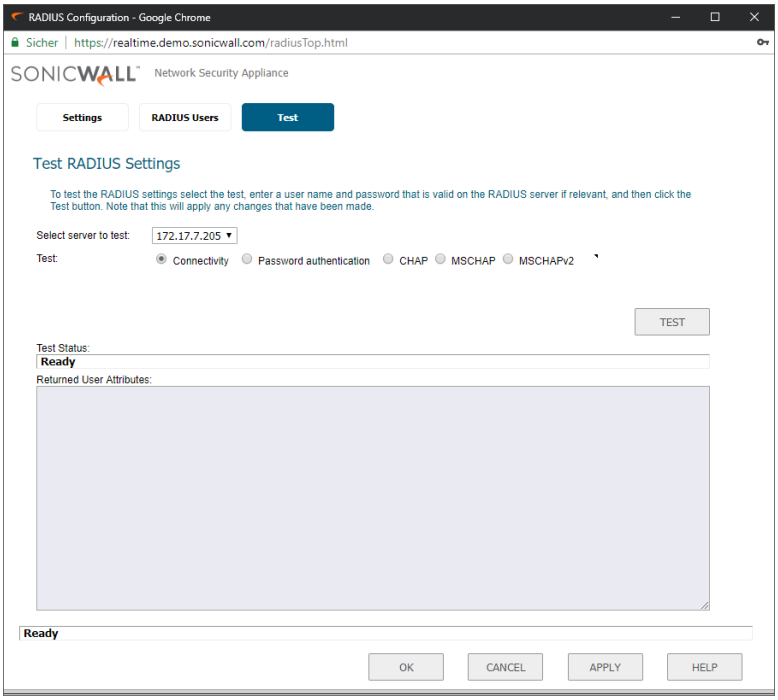


Fügen Sie einen neuen Radius Server hinzu, verwenden Sie hierbei die IP Addresse des privacyIDEA Servers und das Shared Secret aus Kapitel 2, Absatz 8

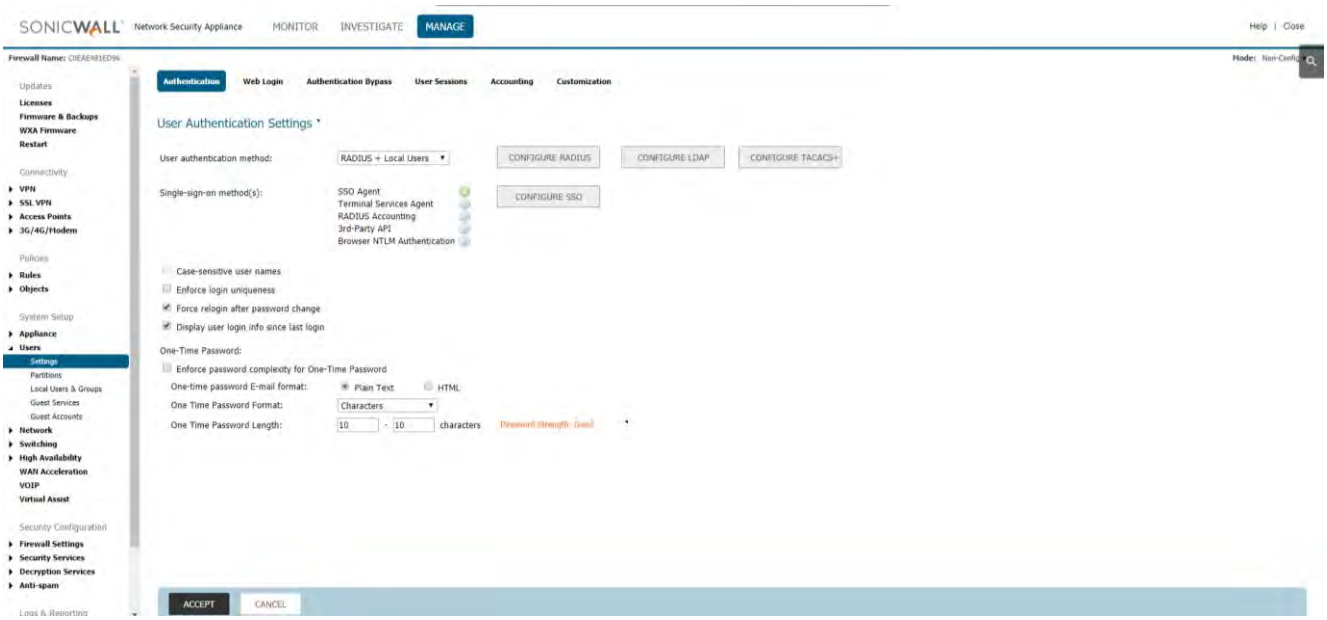


Standardmässig werden alle über Radius Authentifizierten Benutzer der Gruppe Domain Users hinzugefügt, möchten Sie dies ändern, können Sie unter Radius Users dies ändern.

Haben Sie den Radius Server erfolgreich angelegt, testen Sie die Verbindung, sowie die „Password Authentication“ mit Klick auf Test



Wählen Sie nun unter User Authentication Method: Radius + Local User aus

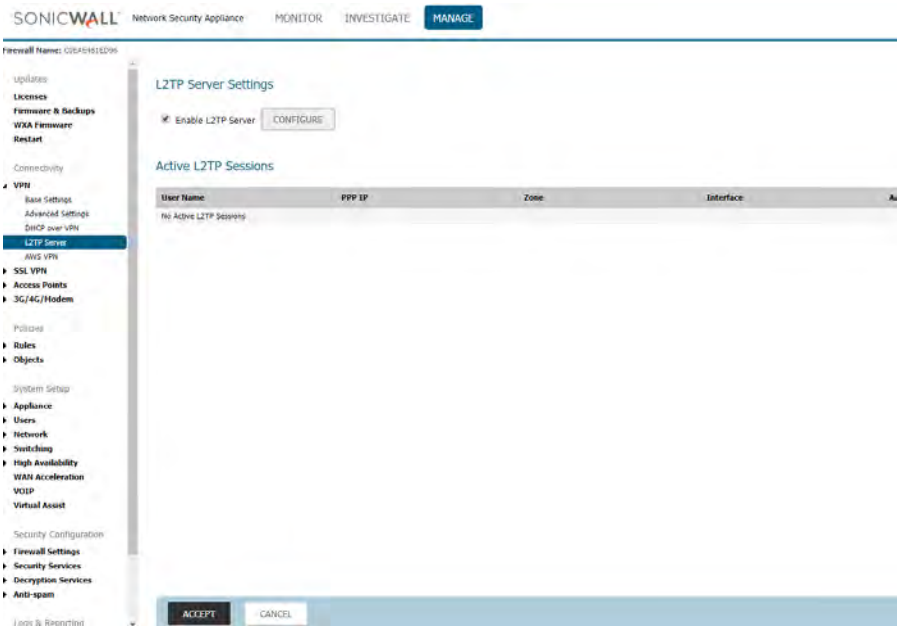


Sie haben nun die Grundkonfiguration des Radius Server abgeschlossen

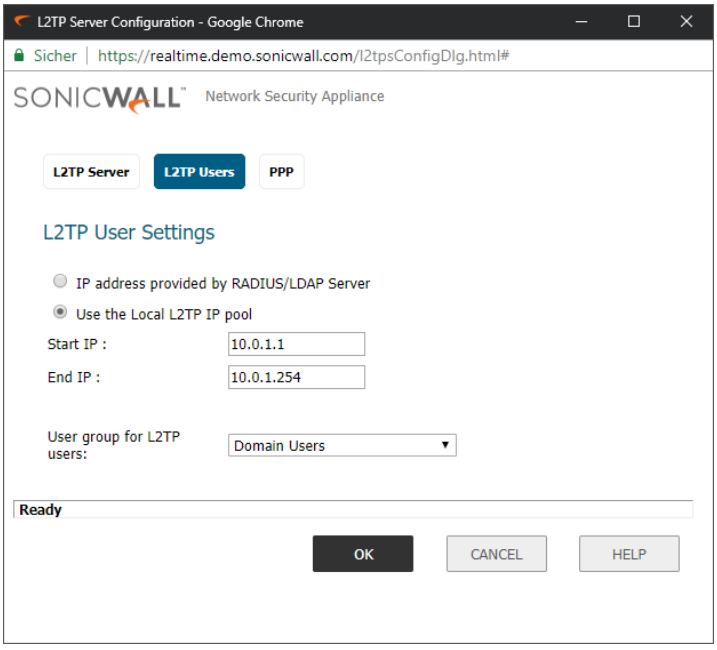
7.7.2. Konfigurieren von L2TP mit Yubikey

In unserem Beispiel zeigen wir die Konfiguration für ein L2TP VPN Tunnel.

Klicken Sie auf Manage – VPN – L2TP Server. Aktivieren Sie den Server und klicken auf Configure



Wählen Sie einen L2TP IP Pool, sowie die Gruppe (Standardmäßig werden all Radius Benutzer der Domain Users Gruppe hinzugefügt).



Sie können nun über einen L2TP Client (z.B Microsoft Windows) die Verbindung aufbauen. Hierbei wählen Sie als Benutzerdaten:

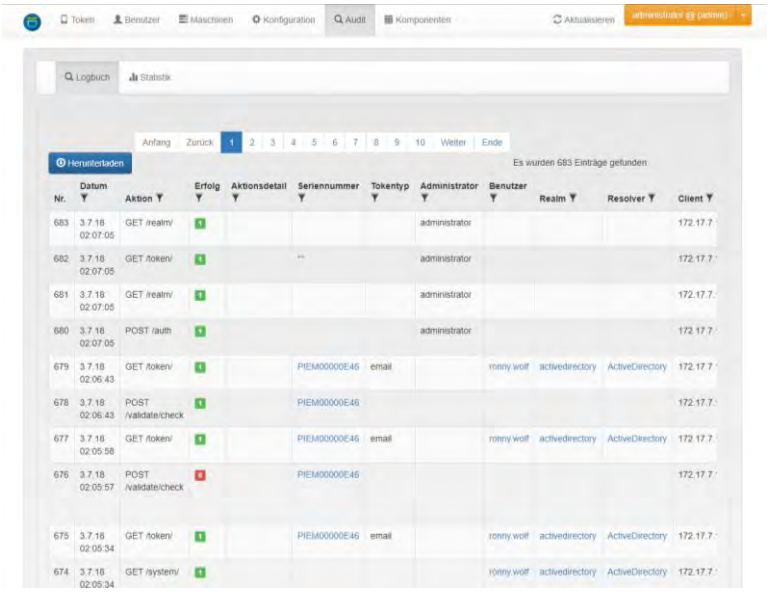
Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP

8. privacyIDEA Protokolle und Berichte

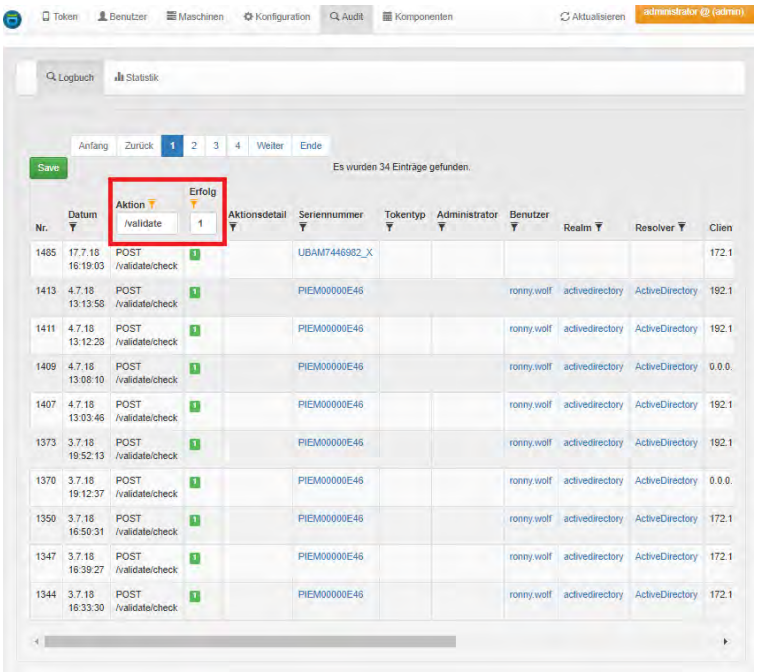
privacyIDEA bietet umfangreiche Möglichkeiten den Status des gesamten Systems anzuzeigen. Besonders die erfolgten Authentifzierungsversuche, können hilfreiche Daten über die Verwendung des Systems zeigen.

8.1. Protokolle (Audit)

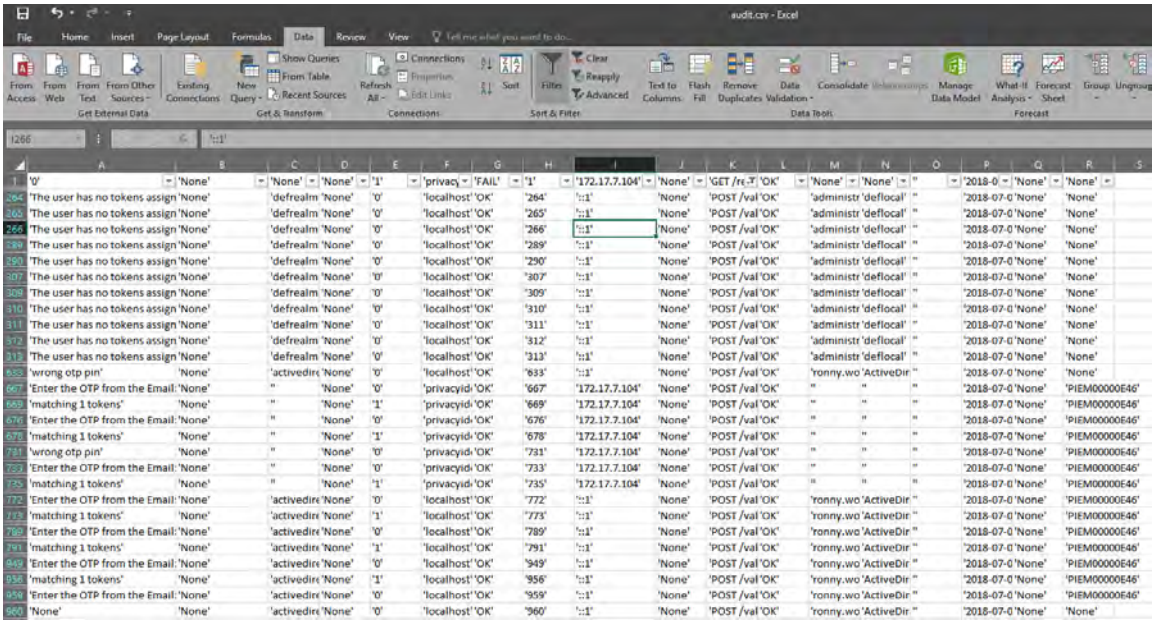
Um die Protokolle in privacyIDEA aufzurufen, melden Sie sich als Administrator am Webinterface an. Klicken Sie nun auf Audit.



Im Audit Log, werden alle Aktivitäten (Webinterface, Authentifzierung...) protokolliert. Durch die Filtersymbole in den jeweiligen Spalten können Sie Einträge filtern, um bestimmte Ereignisse zu finden.



Auch können Sie für eine externe Bearbeitung (z.B. Microsoft Excel) die Logs als CSV Datei exportieren. Klicken Sie hierzu auf „Save“

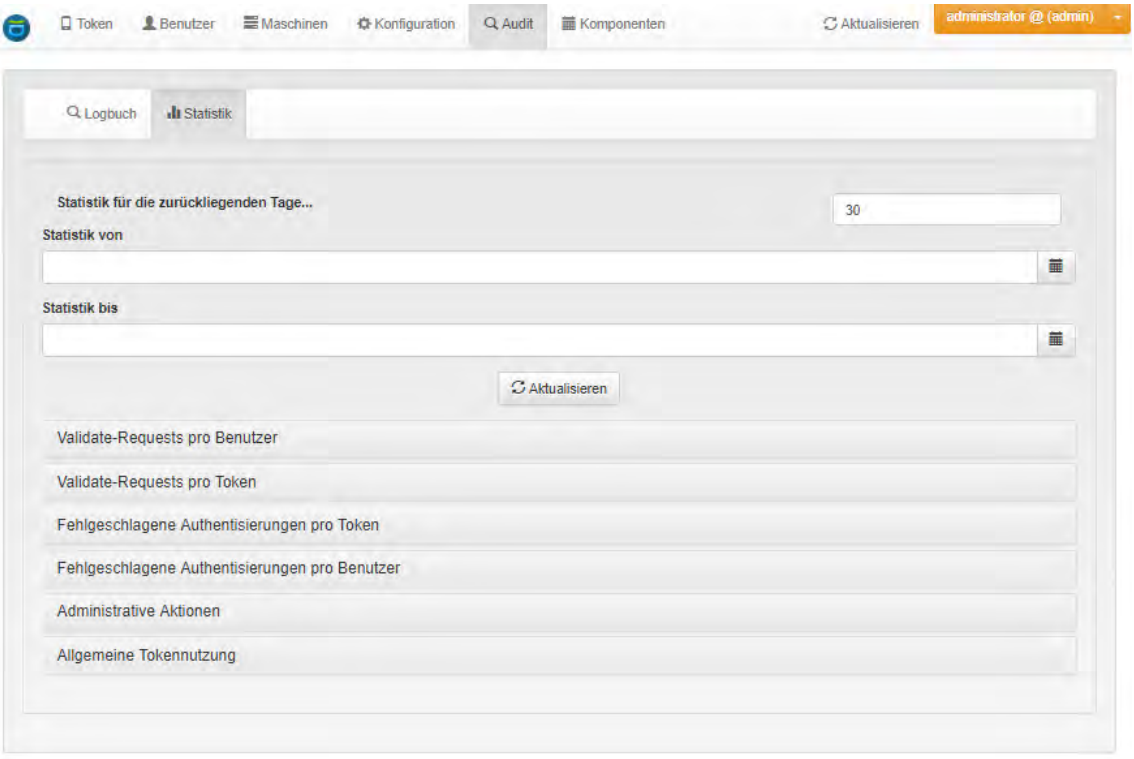


Weitere Details zu den Audit Logs, können Sie im privacyIDEA Handbuch nachlesen: https://privacyIDEA.readthedocs.io/en/master/audit/index.html

8.2. Berichte

Das Berichtswesen in privacyIDEA bieten Ihnen eine grafische Aufbereitung der Authentizfierungsanfragen und damit einen Statistischen Überblick.

Klicken Sie hierzu auf Audit – Statistik



Wählen Sie nun einen Zeitraum aus, für den die Berichte erstellt werden sollen und klicken auf aktualisieren