



Firewall Integration Guide
Yubikey's mit privacyIDEA

Contents

1. Vorbereitung privacyIDEA	4
1.1. Erstellen einer virtuellen Maschine auf Microsoft Hyper-V	4
1.2. Installation von Ubuntu Server 16.04 (LTS).....	8
1.3. Ändern der Netzwerkeinstellungen	23
1.4. DNS Record hinzufügen	25
1.5. SSH Server auf Ubuntu Server installieren und konfigurieren	26
1.6. Verbindung via SSH Client (z.B. Putty) testen.....	27
1.7. Service Account in Active Directory anlagen	29
2. Installation privacyIDEA.....	31
2.1. Hinzufügen des privacyIDEA Ubuntu repository.....	31
2.2. Updaten der Ubuntu Repositories.....	31
2.3. Installation von privacyIDEA	32
2.4. Administrator Account hinzufügen	33
2.5. Erreichbarkeit des Webinterface testen	34
2.6. FreeRadius installieren	35
2.7. privacyIDEA Radius Plugin installieren.....	35
2.8. Konfigurieren von FreeRadius	35
2.9. Testen von FreeRadius und privacyIDEA kommunikation via radclient	37
3. Konfiguration privacyIDEA – Active Directory Anbindung	39
3.1. Standard Realm anlagen	39
3.2. ActiveDirectory Resolver anlagen.....	39
3.3. Neuen Realm anlagen	42
3.4. Überprüfen ob Benutzer in privacyIDEA angezeigt werden	43
3.5. Überprüfen ob Anmeldung mit Benutzer möglich ist	44
4. Konfiguration privacyIDEA – Richtlinien und Ereignisse	45
4.1. Erstellen einer Richtlinie für Active Directory Passwort + OTP	45
4.2. Hinzufügen eines SMTP Servers für Benachrichtigungen	46
4.3. Hinzufügen einer Ereignisregel (Benachrichtigung bei fehlerhaften Anmeldungen)	47
5. Zusätzliche Konfigurationen (optional)	50
5.1. Richtlinie für Self Enrollment auf bestimmte Tokentypen einschränken.....	50
5.2. E-Mail Token Konfiguration, Ausrollen und Testen	52
5.3. Überschreiben von Client IP Adresse über Radius erlauben	56
6. Yubikey's konfigurieren und ausrollen	58
6.1. Konfigurieren eines Yubikeys mit dem Yubico Personalization Tool.....	58

6.2.	Ausrollen und zuweisen eines Yubikeys in privacyIDEA	61
7.	Firewall's konfigurieren	65
7.1.	Sophos XG Firewall mit Radius	65
7.1.1.	Konfigurieren der Radius Anbindung	65
7.1.2.	Anmelden an User Portal mit Yubikey	69
7.1.3.	Anmelden via SSLVPN mit Yubikey	70
7.1.4.	Zeitbasiertes One Time Password	70
7.2.	Sophos UTM Firewall mit Radius.....	76
7.2.1.	Konfigurieren der Radius Anbindung	76
7.2.2.	Anmelden an User Portal mit Yubikey	78
7.2.3.	Anmelden via SSLVPN mit Yubikey	80
7.3.	Clavister Firewall mit Radius.....	81
7.3.1.	Konfigurieren der Radius Anbindung	81
7.3.2.	Anmelden an User Portal mit Yubikey	86
7.3.3.	Anmelden an SSLVPN mit Yubikey	86
7.4.	Rohde & Schwarz Firewall	88
7.4.1.	Konfigurieren der Radius Anbindung	88
7.5.	Untangle Firewall	90
7.5.1.	Konfigurieren der Radius Anbindung	90
7.5.2.	Anmelden an Captive Portal mit Yubikey.....	92
7.5.3.	Anmeldung via OpenVPN mit Yubikey	94
7.6.	pfSense Firewall.....	96
7.6.1.	Konfigurieren der Radius Anbindung	96
7.6.2.	Anmeldung an Captive Portal mit Yubikey	98
7.6.3.	Anmeldung via OpenVPN mit Yubikey	99
7.7.	Sonicwall NSA Firewall	102
7.7.1.	Konfigurieren der Radius Anbindung	102
7.7.2.	Konfigurieren von L2TP mit Yubikey.....	105
8.	privacyIDEA Protokolle und Berichte.....	106
8.1.	Protokolle (Audit).....	106
8.2.	Berichte	107

1. Vorbereitung privacyIDEA

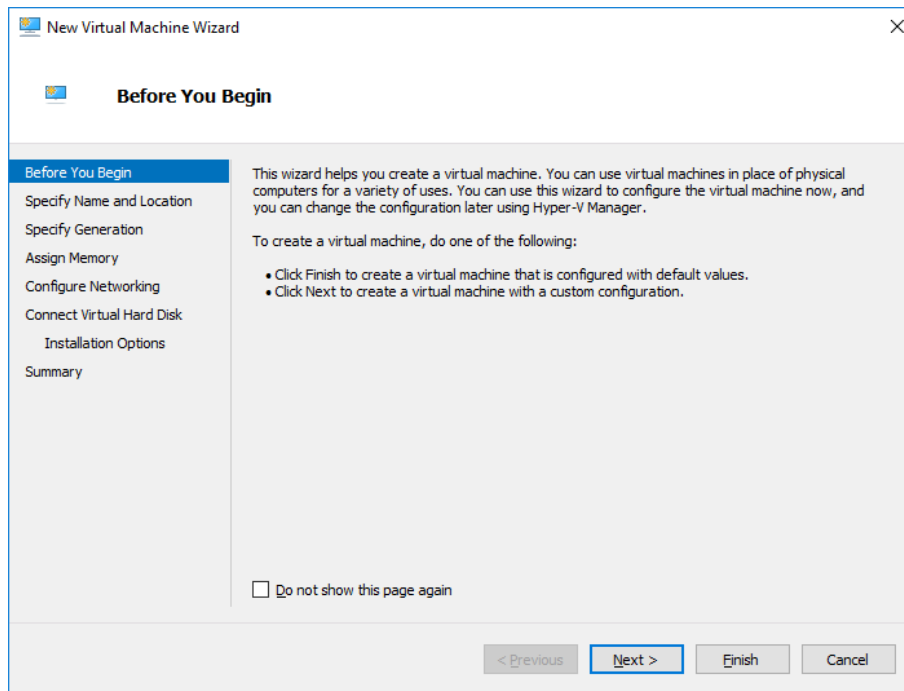
Um eine 2 Faktor Authentifizierung, an den in diesem Guide vorgestellten Sicherheitslösungen, zu realisieren, ist in den meisten Fällen eine Anbindung via Radius erforderlich. Yubico bietet ein Open Source Plugin für FreeRadius an, jedoch empfehlen wir in professionellen Umgebungen, eine einfacher verwaltbare 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 Plattform verwenden wir Microsoft Hyper-V 2016, Sie können jedoch auch einen physikalischen Server oder eine andere Virtualisierungsplattform verwenden.

Erstellen Sie nun eine neue Maschine in Microsoft Hyper-V



Vergeben Sie einen Namen und den Speicherort der virtuellen Maschine

The screenshot shows the 'Specify Name and Location' step of the 'New Virtual Machine Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains the following text: 'Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.' Below this, the 'Name' field is set to 'PrivacyIdea with FreeRadius'. The 'Location' field is set to 'D:\Virtual Machines\CFG\'. A checkbox labeled 'Store the virtual machine in a different location' is unchecked. A 'Browse...' button is next to the location field. A warning icon and text state: 'If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.' At the bottom, there are four buttons: '< Previous', 'Next >' (highlighted), 'Finish', and 'Cancel'.

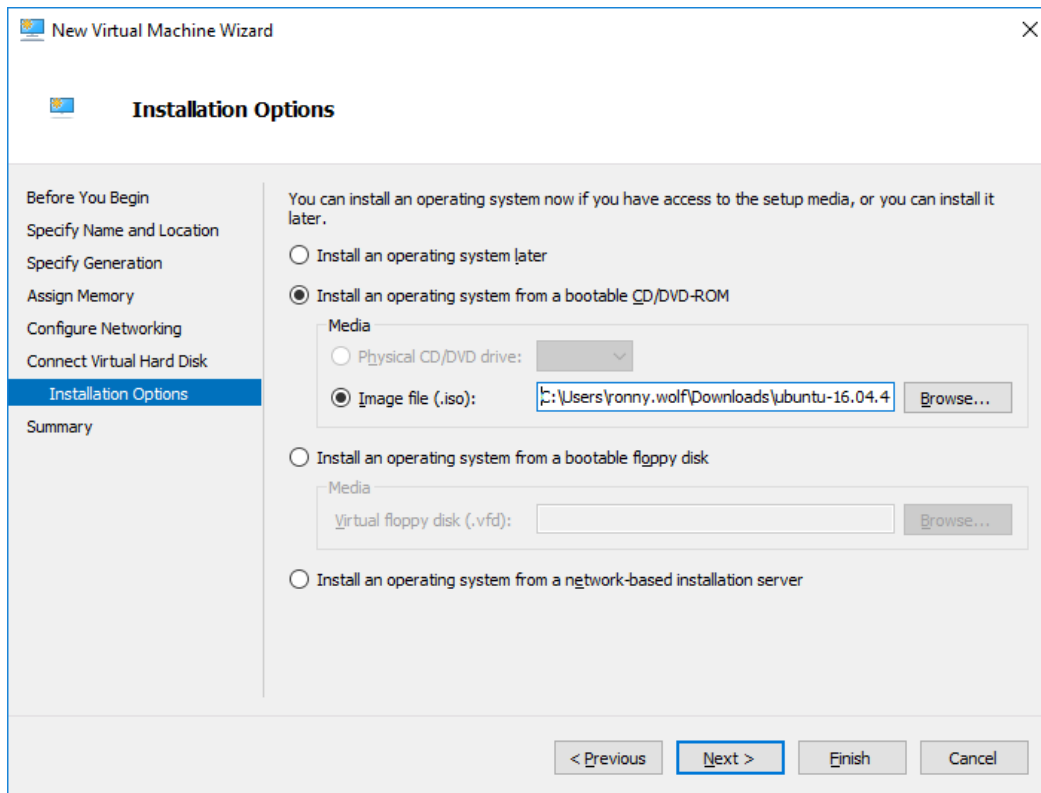
privacyIDEA ist in den meisten Szenarien sehr ressourcenschonend, jedoch empfehlen wir für einen reibungslosen und schnell Betrieb mindestens 4GB Arbeitsspeicher

The screenshot shows the 'Assign Memory' step of the 'New Virtual Machine Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation', 'Assign Memory' (highlighted), 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains the following text: 'Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.' Below this, the 'Startup memory' field is set to '4096' MB. A checkbox labeled 'Use Dynamic Memory for this virtual machine.' is unchecked. An information icon and text state: 'When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.' At the bottom, there are four buttons: '< Previous', 'Next >' (highlighted), 'Finish', and 'Cancel'.

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>)



New Virtual Machine Wizard

Installation Options

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

You can install an operating system now if you have access to the setup media, or you can install it later.

☐ Install an operating system later

☒ Install an operating system from a bootable CD/DVD-ROM

Media

☐ Physical CD/DVD drive: [v]

☒ Image file (.iso): C:\Users\ronny.wolf\Downloads\ubuntu-16.04.4 [Browse...]

☐ Install an operating system from a bootable floppy disk

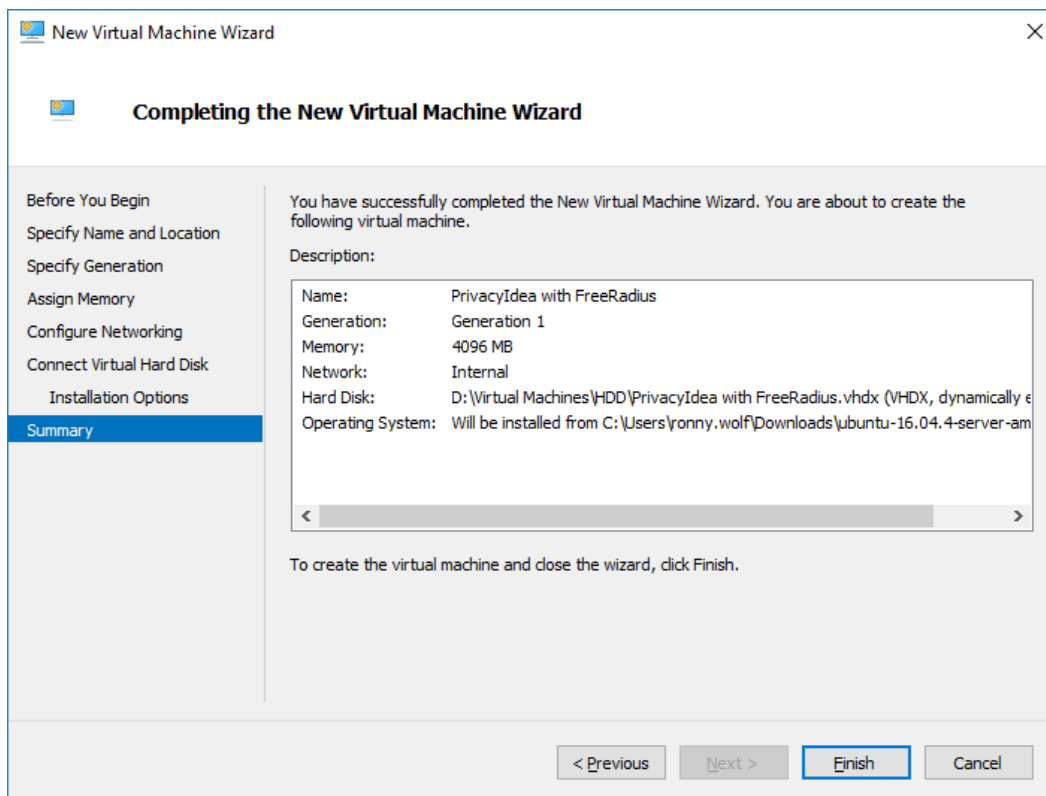
Media

☐ Virtual floppy disk (.vfd): [Browse...]

☐ Install an operating system from a network-based installation server

< Previous Next > Finish Cancel

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



New Virtual Machine Wizard

Completing the New Virtual Machine Wizard

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

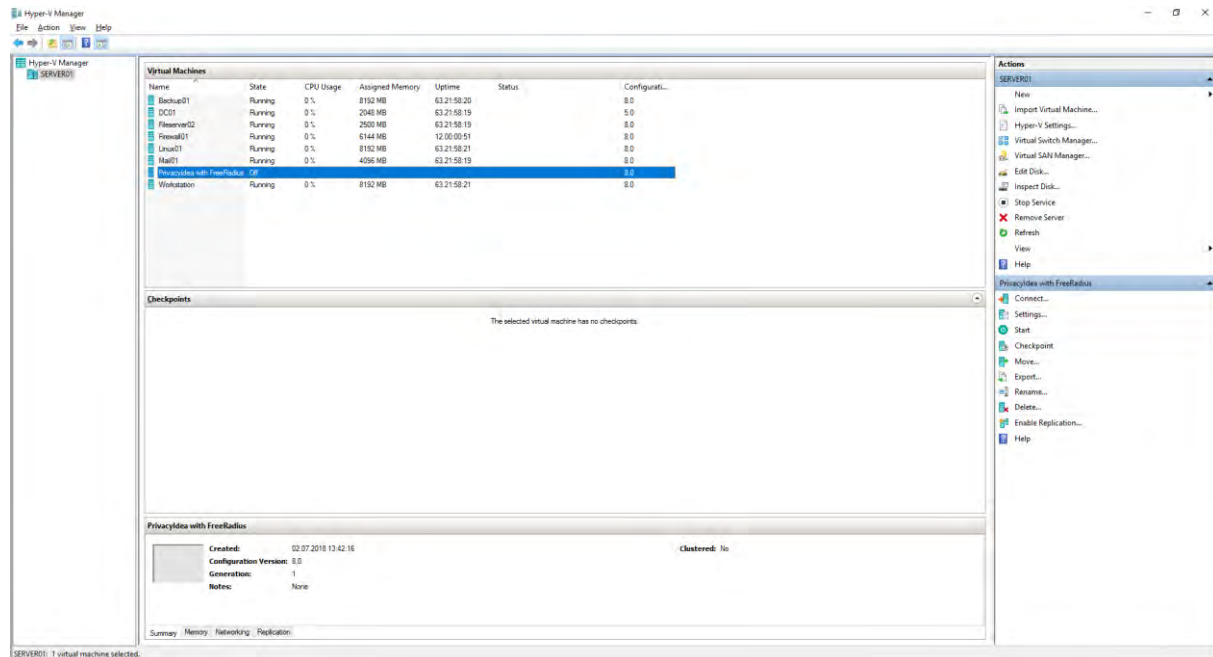
Name:	PrivacyIdea with FreeRadius
Generation:	Generation 1
Memory:	4096 MB
Network:	Internal
Hard Disk:	D:\Virtual Machines\HDD\PrivacyIdea with FreeRadius.vhdx (VHDX, dynamically e
Operating System:	Will be installed from C:\Users\ronny.wolf\Downloads\ubuntu-16.04.4-server-am

To create the virtual machine and close the wizard, click Finish.

< Previous Next > Finish Cancel

1.2. Installation von Ubuntu Server 16.04 (LTS)

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

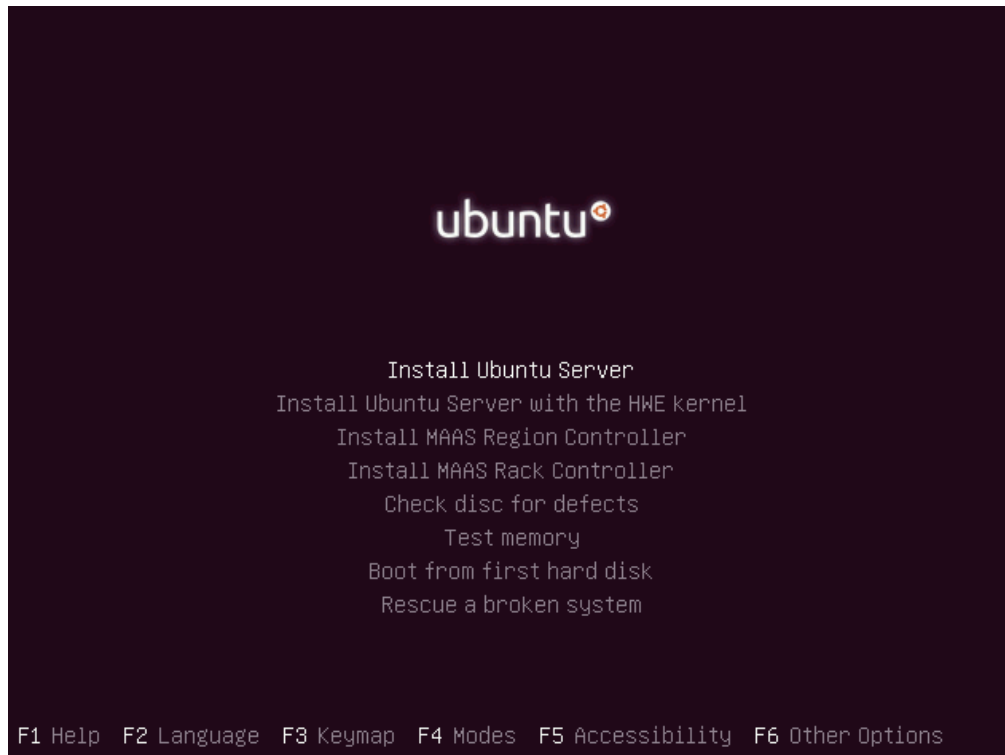


Die virtuelle Maschine starten nun vom verbundenen Ubuntu Server ISO.

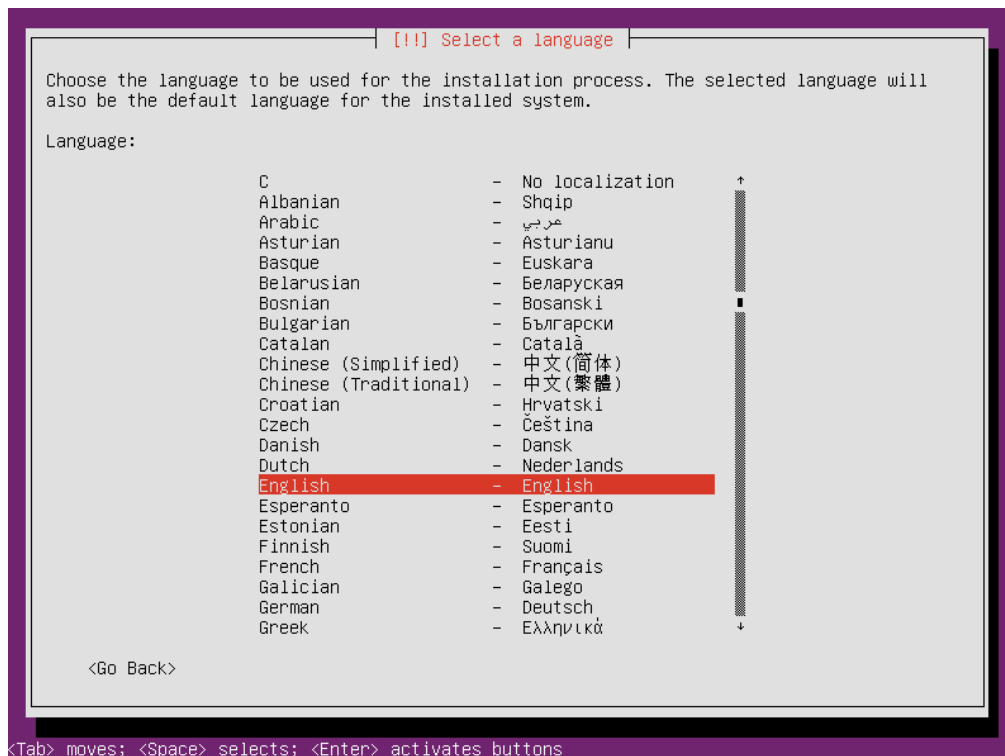
Wählen Sie als erstes die Sprache aus.



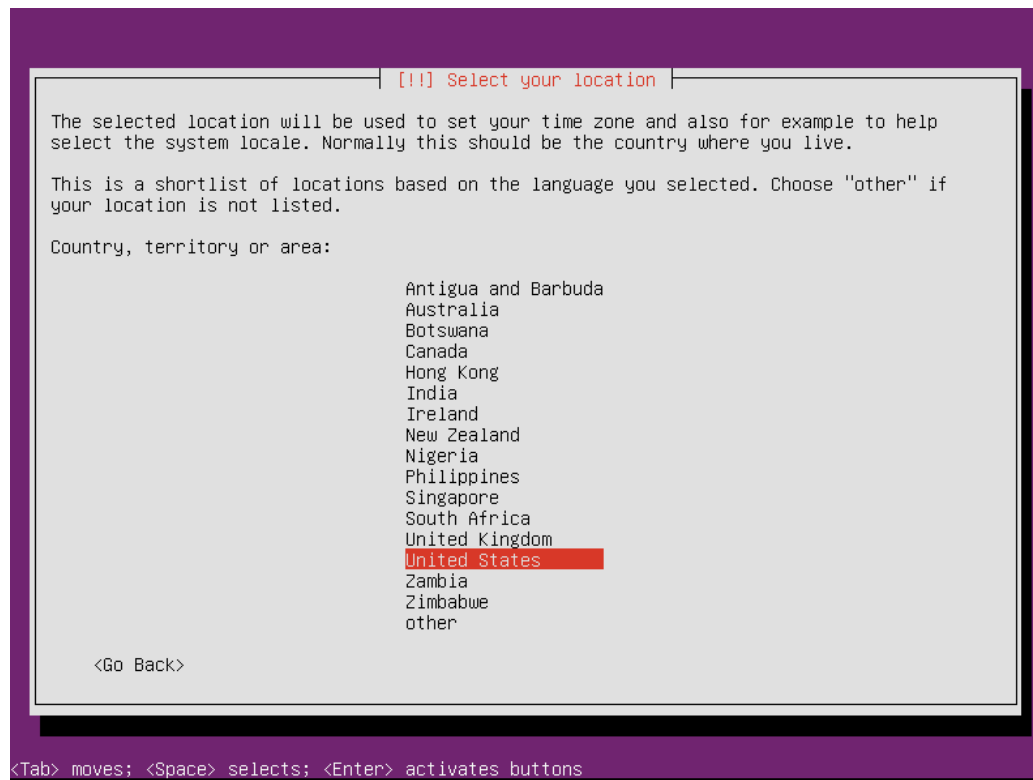
Und starten Sie die Installationsroutine



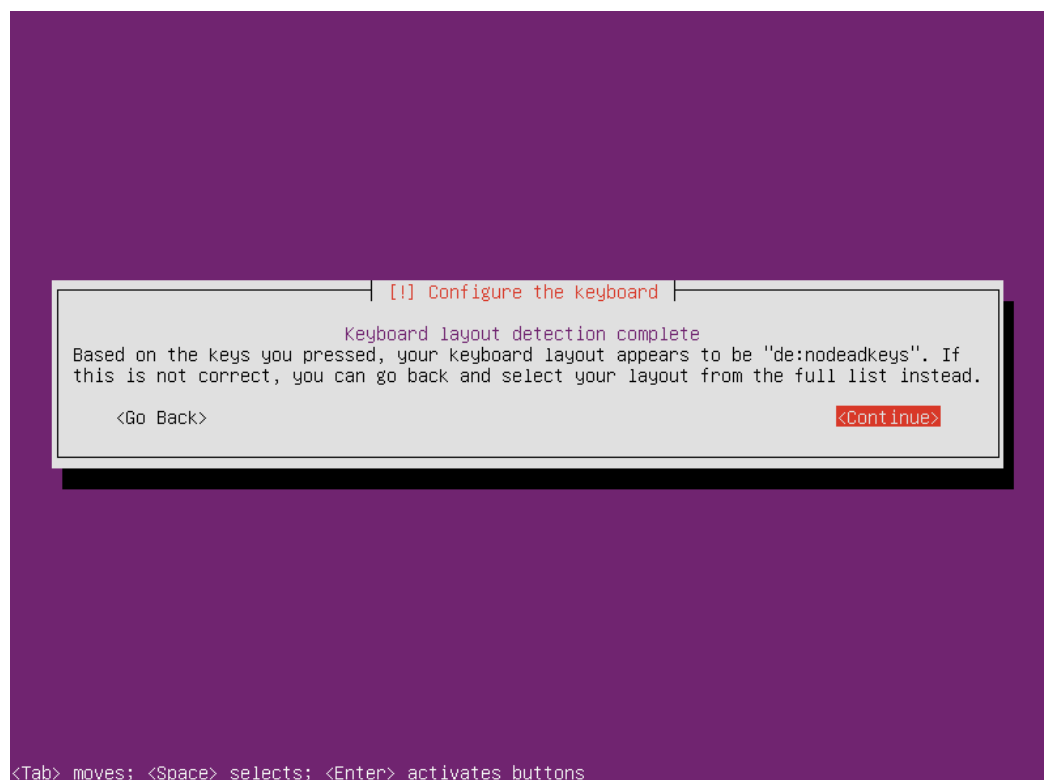
Wählen Sie nochmals die Sprache aus



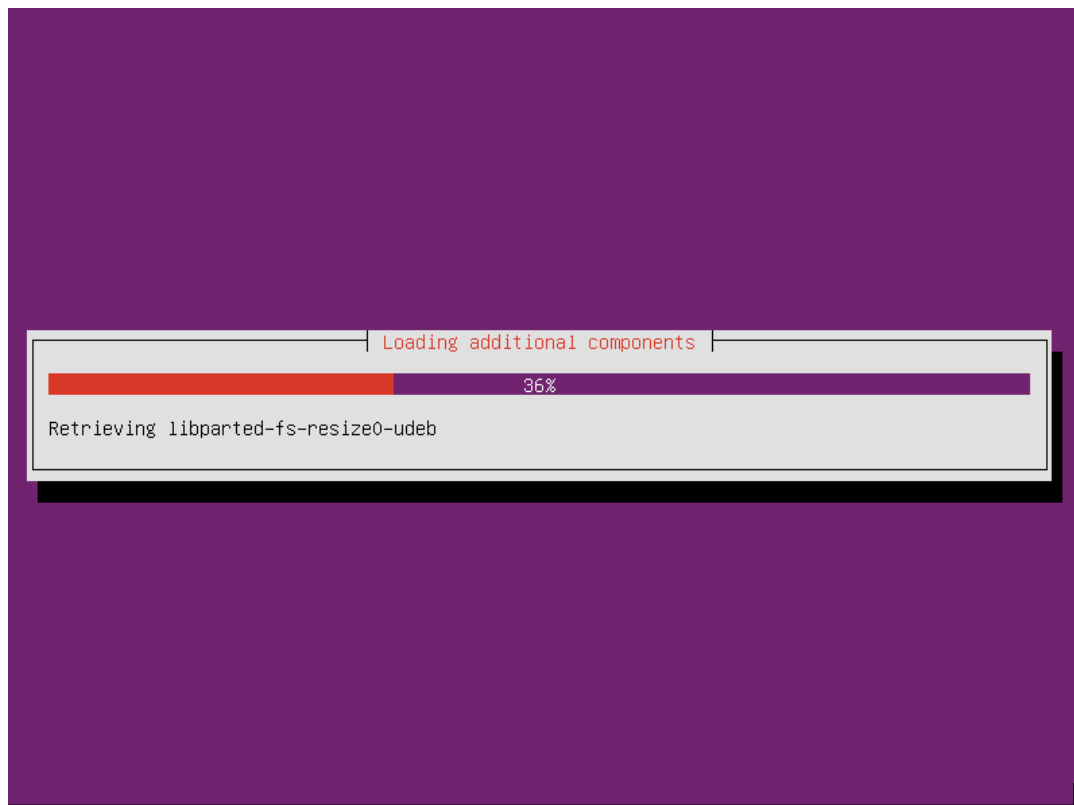
Nun wählen Sie Ihren Standort (benötigt für Zeitzone, Tastatur Layout...)



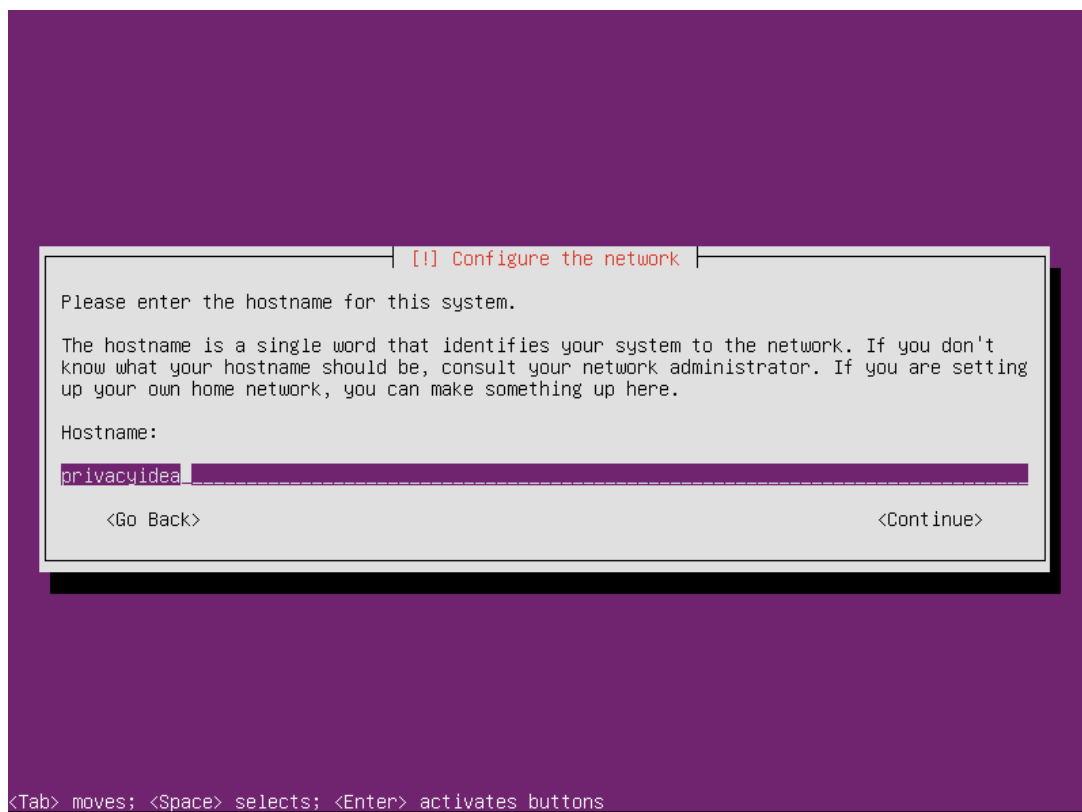
Nun wird der Assistent Sie auffordern einige Tasten auf der Tastatur zu betätigen, damit das richtige Tastaturlayout ausgewählt wird. Ist dies erfolgt und das Layout wurde richtig erkannt, fahren Sie mit der Installation fort.



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



Vergeben Sie nun den Hostnamen, welche wir später auch im DNS registrierten 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:

The screenshot shows a terminal window with a purple background. A dialog box titled "[!!] Set up users and passwords" is displayed. The dialog contains the following text: "A user account will be created for you to use instead of the root account for non-administrative activities. Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice. Full name for the new user:". Below this text is a text input field containing the word "administrator". At the bottom of the dialog are two buttons: "<Go Back>" and "<Continue>". At the bottom of the terminal window, a legend states: "<Tab> moves; <Space> selects; <Enter> activates buttons".

Benutzername:

The screenshot shows a terminal window with a purple background. A dialog box titled "[!!] Set up users and passwords" is displayed. The dialog contains the following text: "Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters. Username for your account:". Below this text is a text input field containing the word "administrator". At the bottom of the dialog are two buttons: "<Go Back>" and "<Continue>". At the bottom of the terminal window, a legend states: "<Tab> moves; <Space> selects; <Enter> activates buttons".

Vergeben Sie nun noch ein sicheres Passwort für den Benutzer:

Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

☐ Show Password in Clear

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

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

Set up users and passwords

Please enter the same user password again to verify you have typed it correctly.

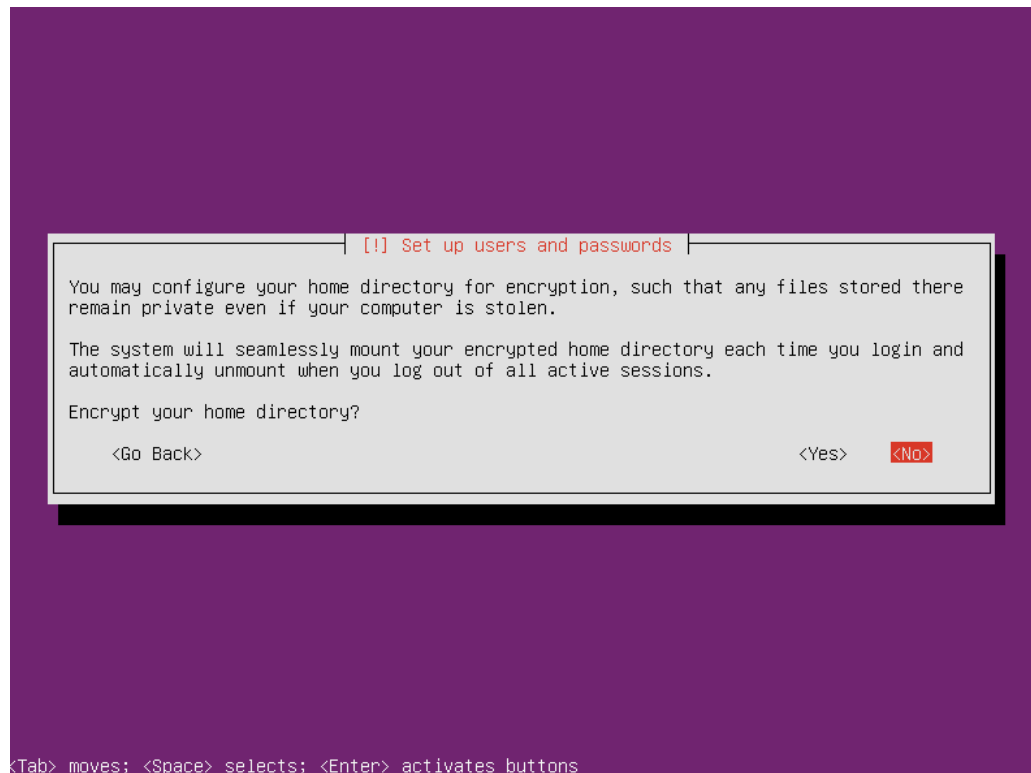
Re-enter password to verify:

☐ Show Password in Clear

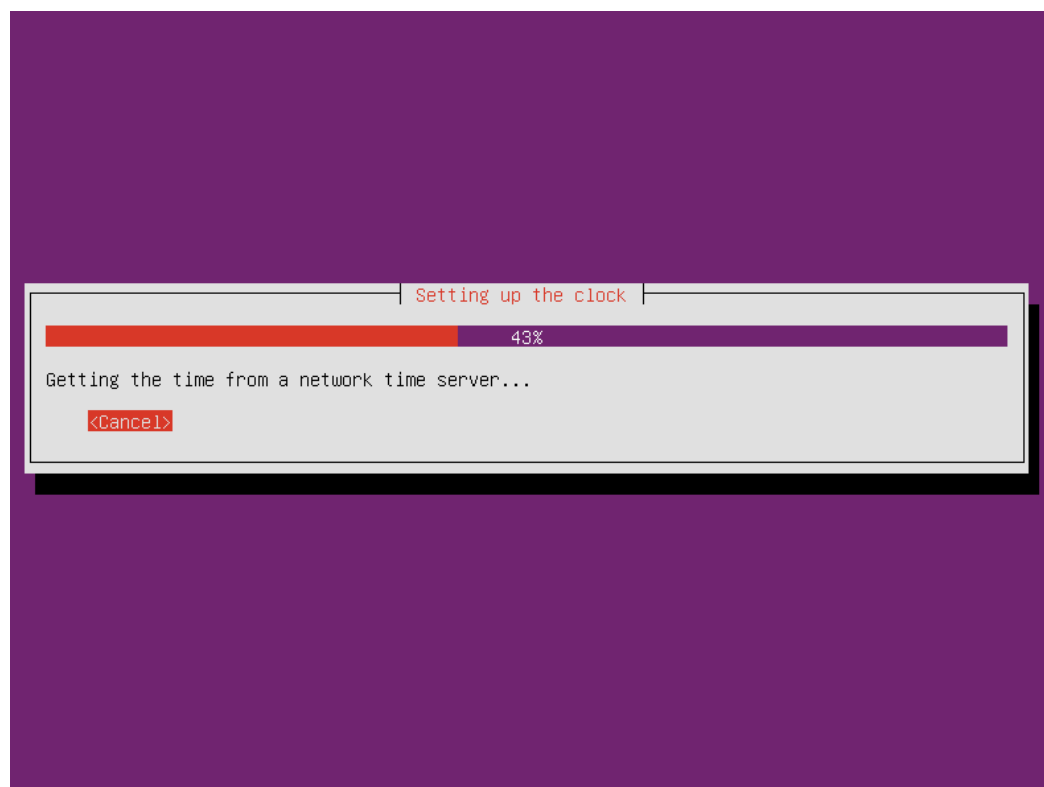
<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

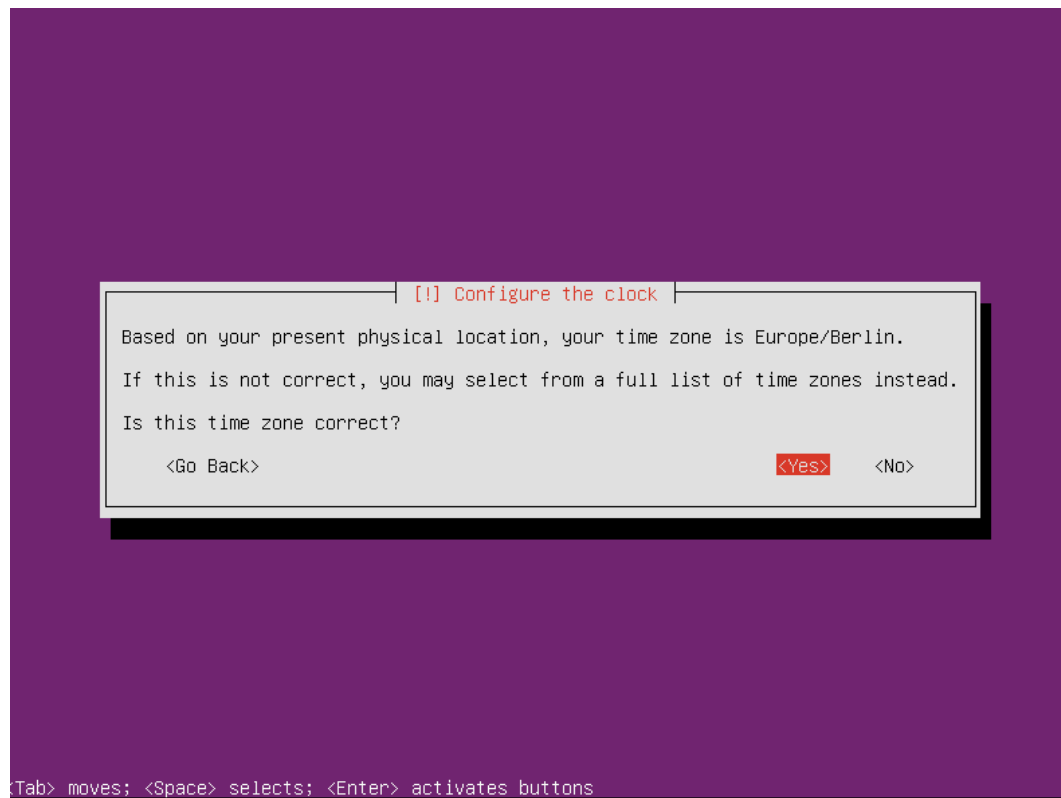
Der Assistent fragt nun, ob wir das Home Verzeichnis des Benutzers verschlüsseln wollen. In unserem Beispiel wählen wir: Nein



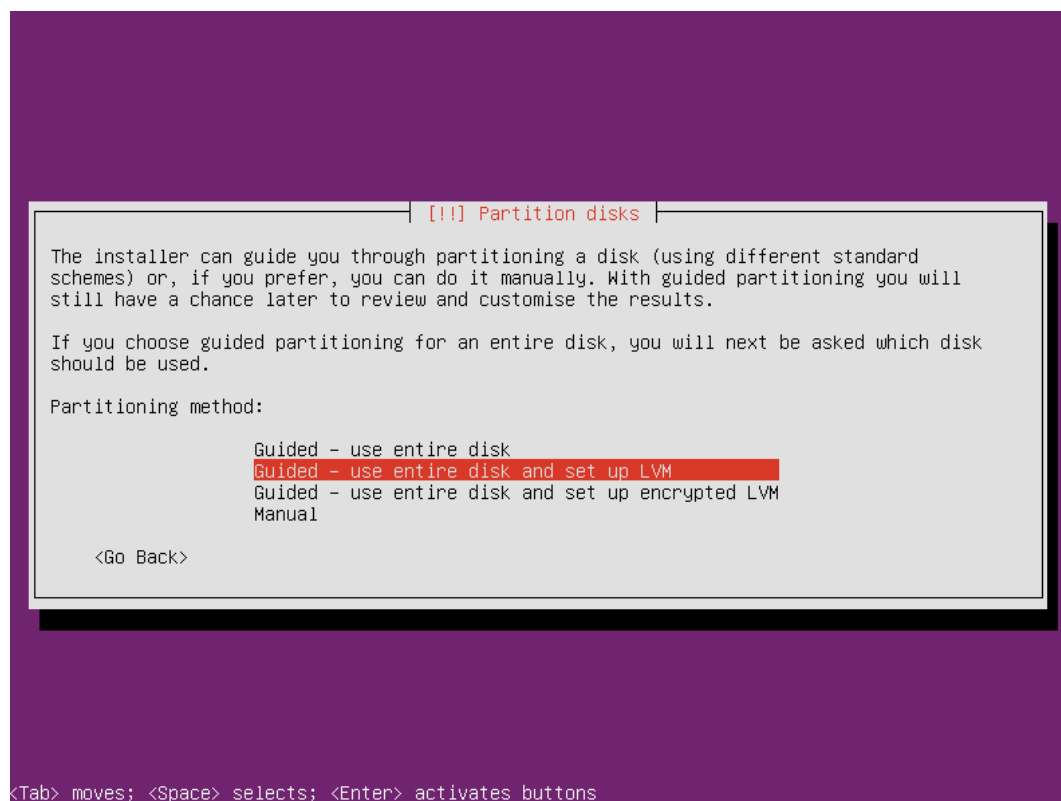
Nun versucht die Installation einen Netzwerkzeitserver zu erreichen, typischerweise ist dies Ihr Domänencontroller oder ein externer Zeitgeber.



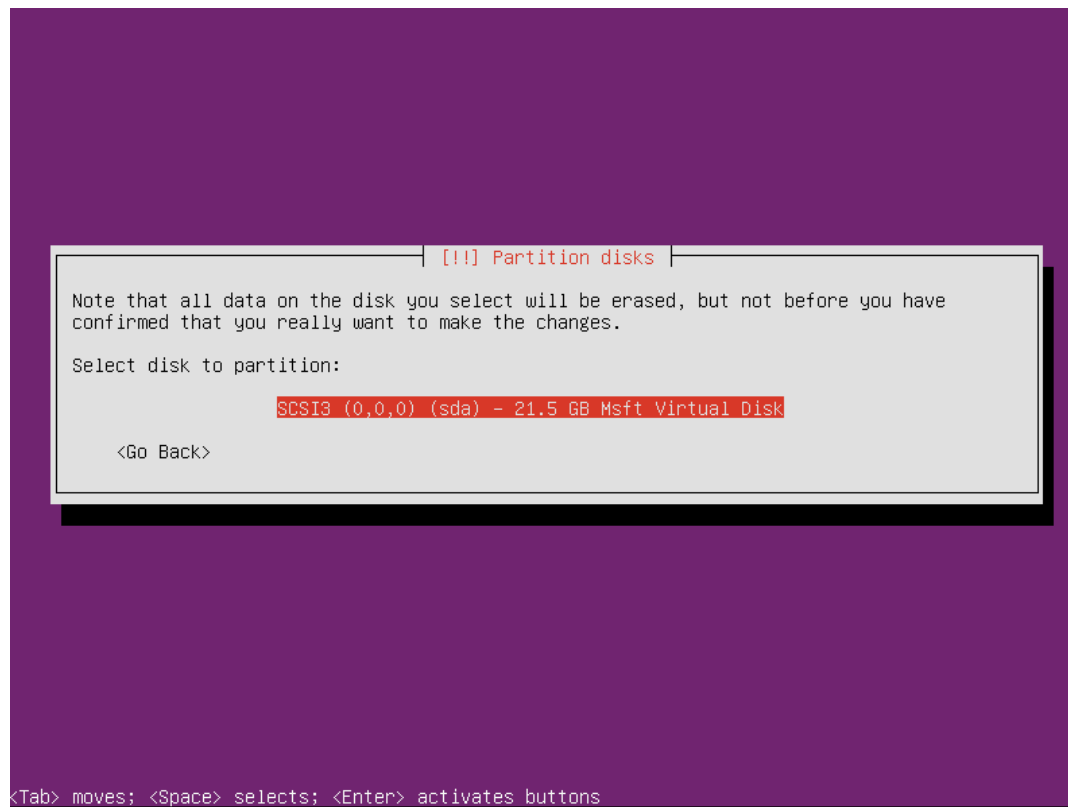
Wurde die Zeitzone richtig ermittelt, fahren Sie mit der Installation fort.



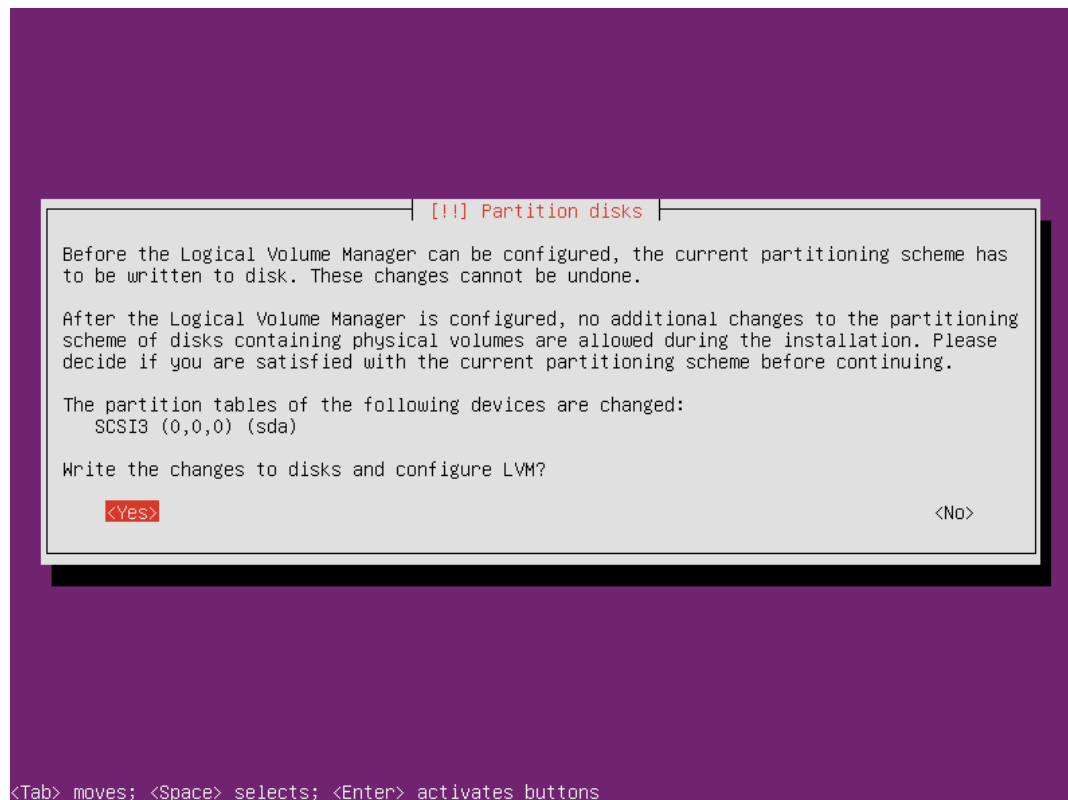
Da es sich bei uns um eine neue virtuelle Maschine handelt, lassen wir den Assistenten die Festplatten Partitionierung durchführen.



Wählen Sie nun die Festplatte auf Ubuntu installiert werden soll.



Und bestätigen die Eingabe



Geben Sie nun noch die Größe des Volumens an

[!] Partition disks

You may use the whole volume group for guided partitioning, or part of it. If you use only part of it, or if you add more disks later, then you will be able to grow logical volumes later using the LVM tools, so using a smaller part of the volume group at installation time may offer more flexibility.

The minimum size of the selected partitioning recipe is 1.9 GB (or 9%); please note that the packages you choose to install may require more space than this. The maximum available size is 21.0 GB.

Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage (e.g. "20%") to use that percentage of the maximum size.

Amount of volume group to use for guided partitioning:

21.0 GB

<Go Back>
<Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Und bestätigen das die Partitionierung nun durchgeführt wird.

[!] Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:

```

LVM VG privacyidea-vg, LV root
LVM VG privacyidea-vg, LV swap_1
SCSI3 (0,0,0) (sda)

```

The following partitions are going to be formatted:

```

LVM VG privacyidea-vg, LV root as ext4
LVM VG privacyidea-vg, LV swap_1 as swap
partition #1 of SCSI3 (0,0,0) (sda) as ext2

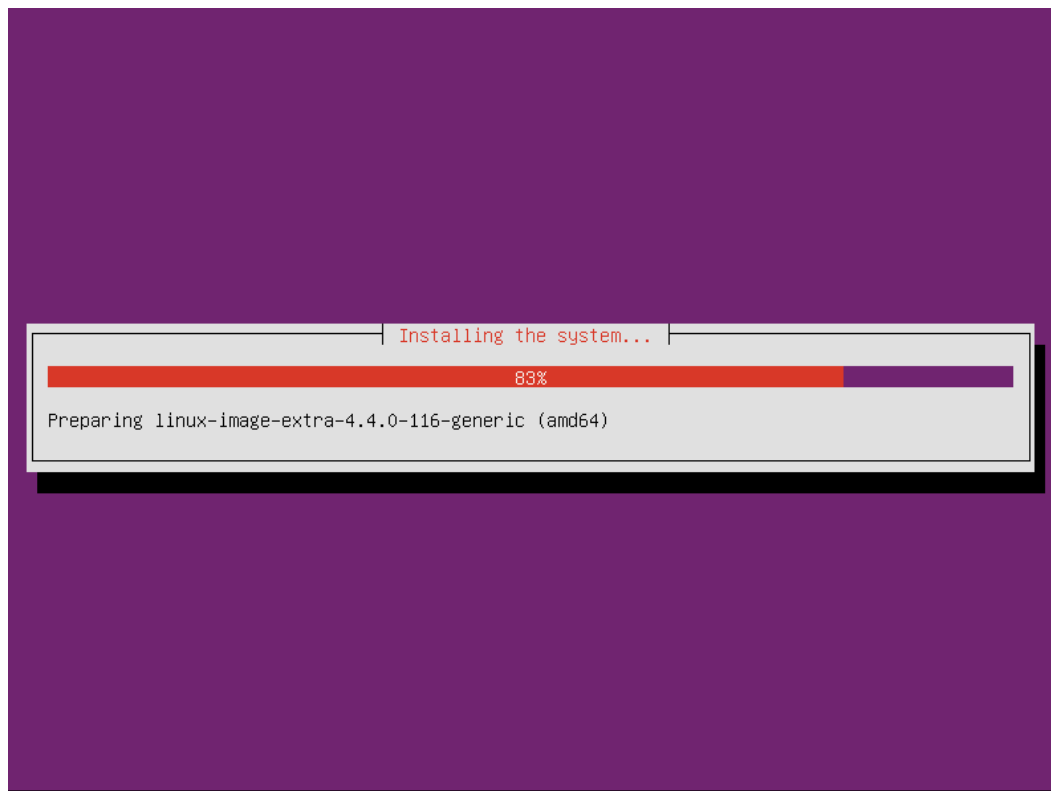
```

Write the changes to disks?

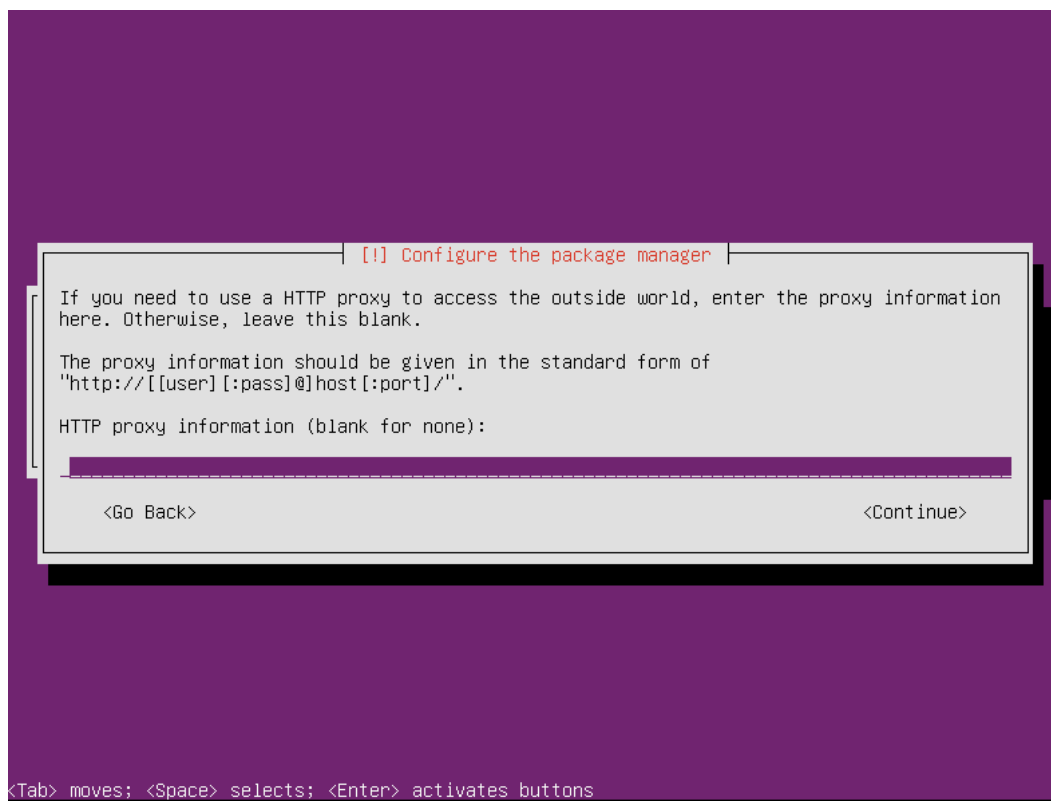
<Yes>
<No>

<Tab> moves; <Space> selects; <Enter> activates buttons

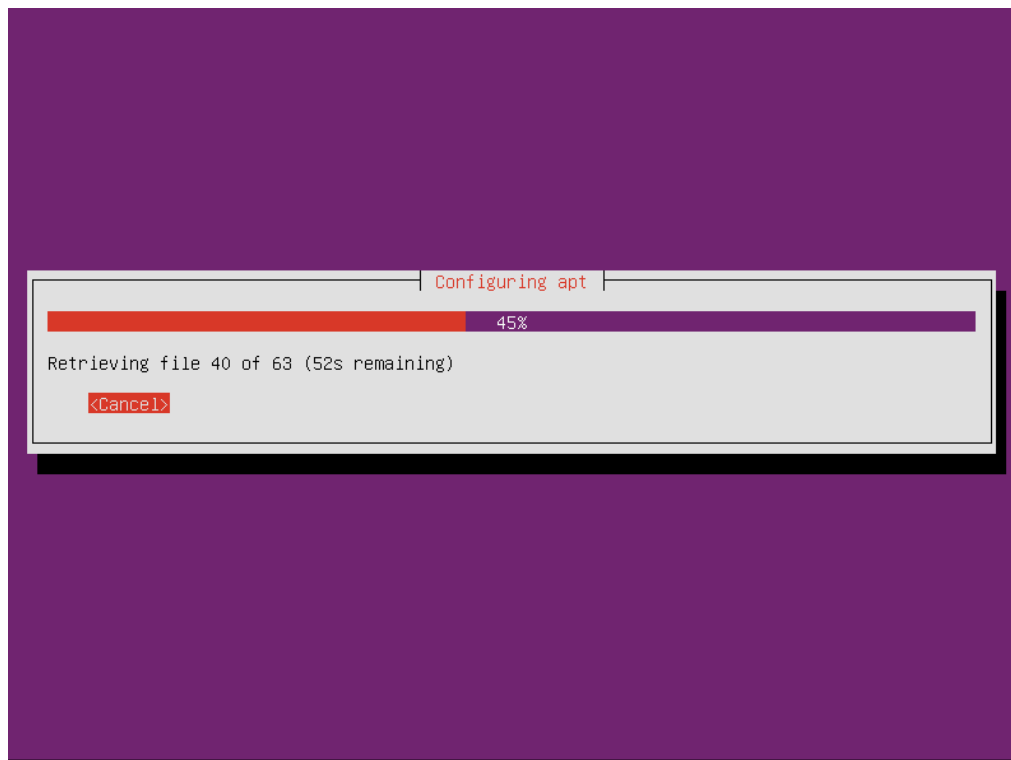
Ubuntu wird nun weitere Komponenten laden



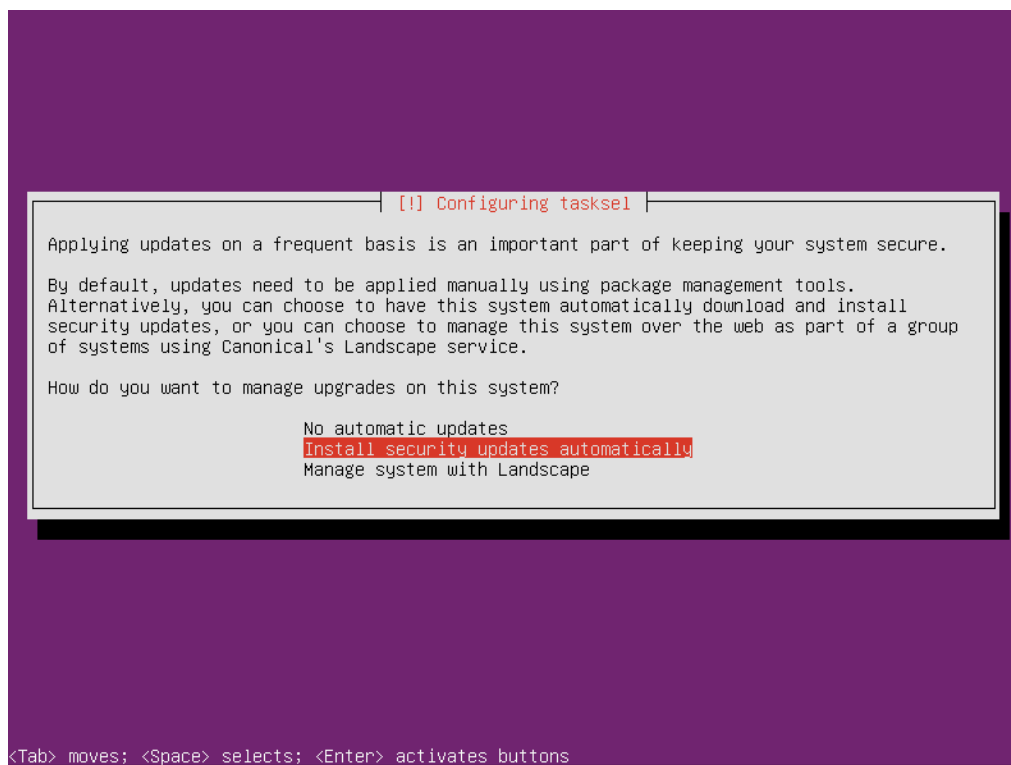
Für Updates und Pakete die nicht mit dem Installationsmedium ausgeliefert werden ist ggf. Eine Internetverbindung erforderlich. Sollte diese nur über einen HTTP Proxy bereitgestellt werden, geben Sie diesen nun ein.



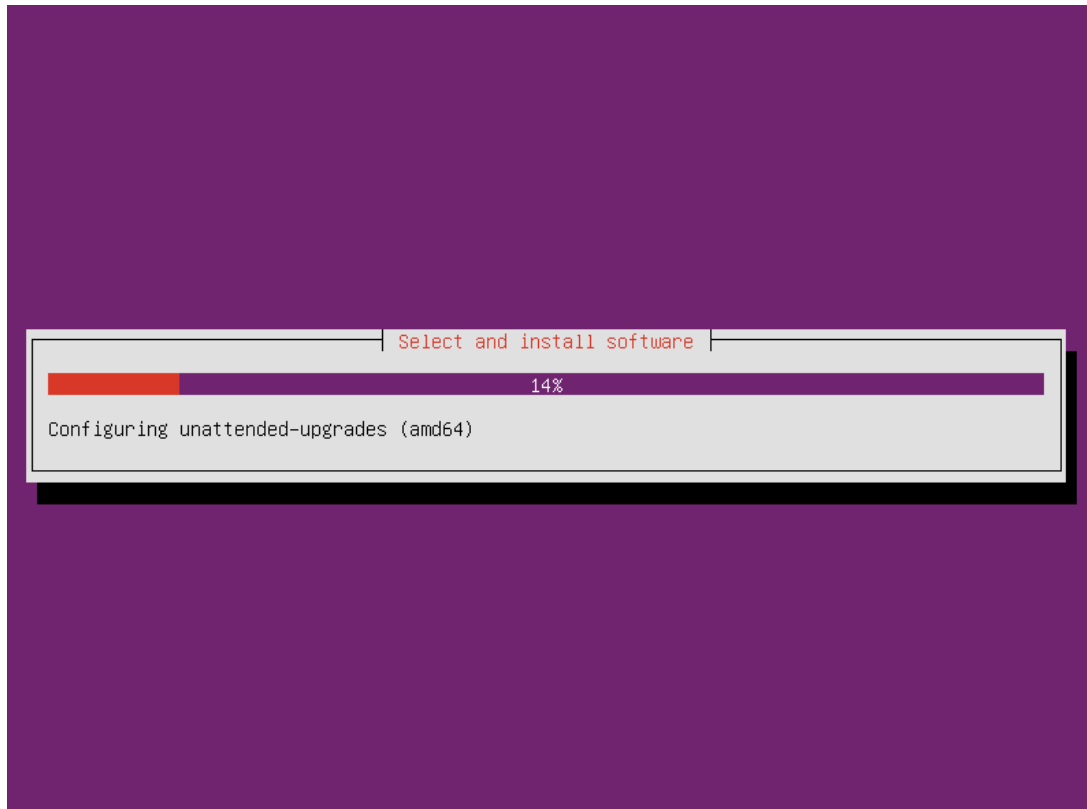
Die Internetverbindung wird nun überprüft und weitere Pakete und Updates nachgeladen.



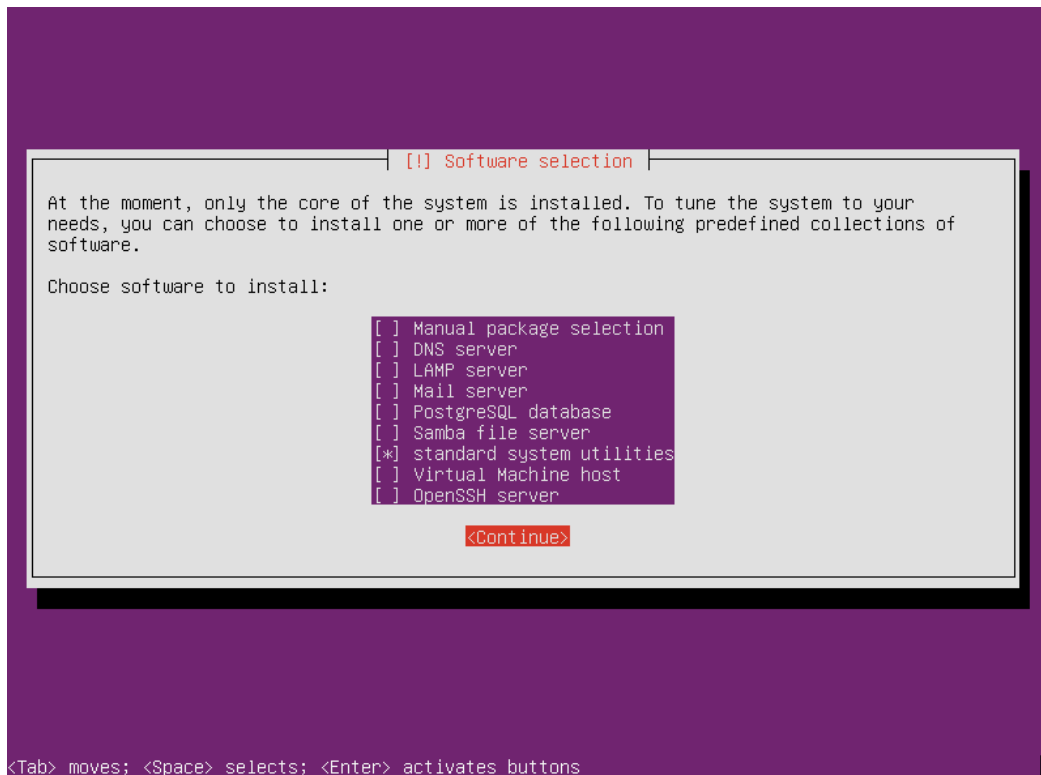
Sie können nun noch auswählen ob Updates automatisch installiert werden sollen. Beachten Sie das beim Installieren von Updates ggf. Ein Neustart von Diensten, Prozessen oder des gesamten Betriebssystems erforderlich ist.



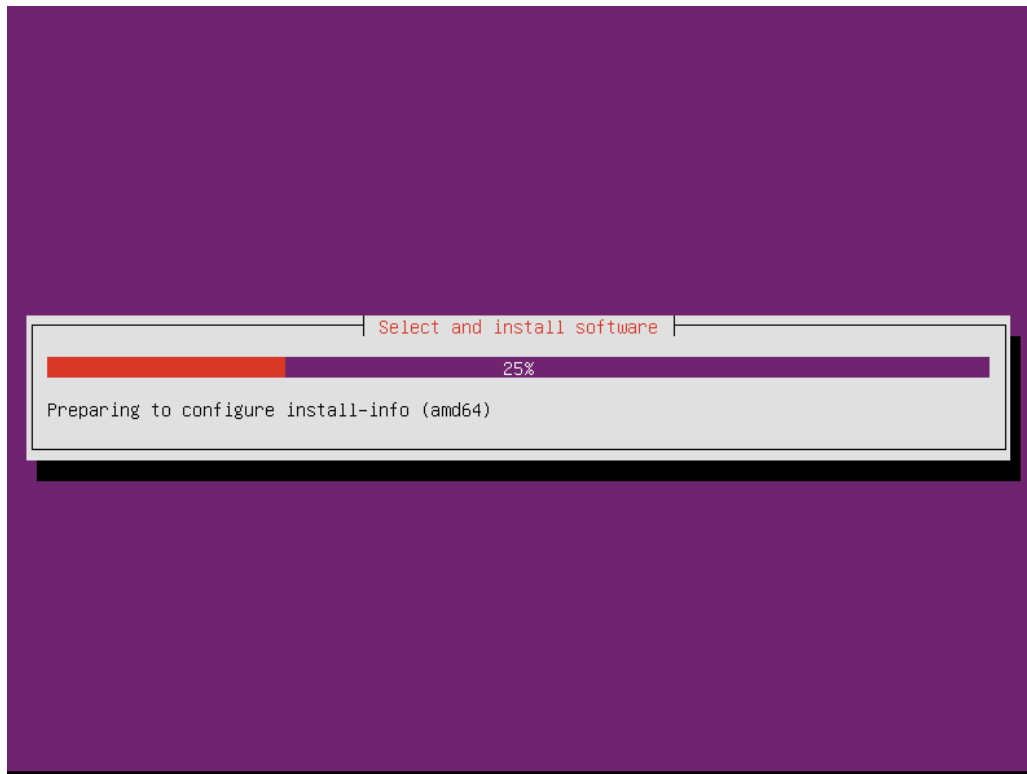
Da wir die automatische Installation von Sicherheitsupdates ausgewählt haben, wird dies nun konfiguriert.



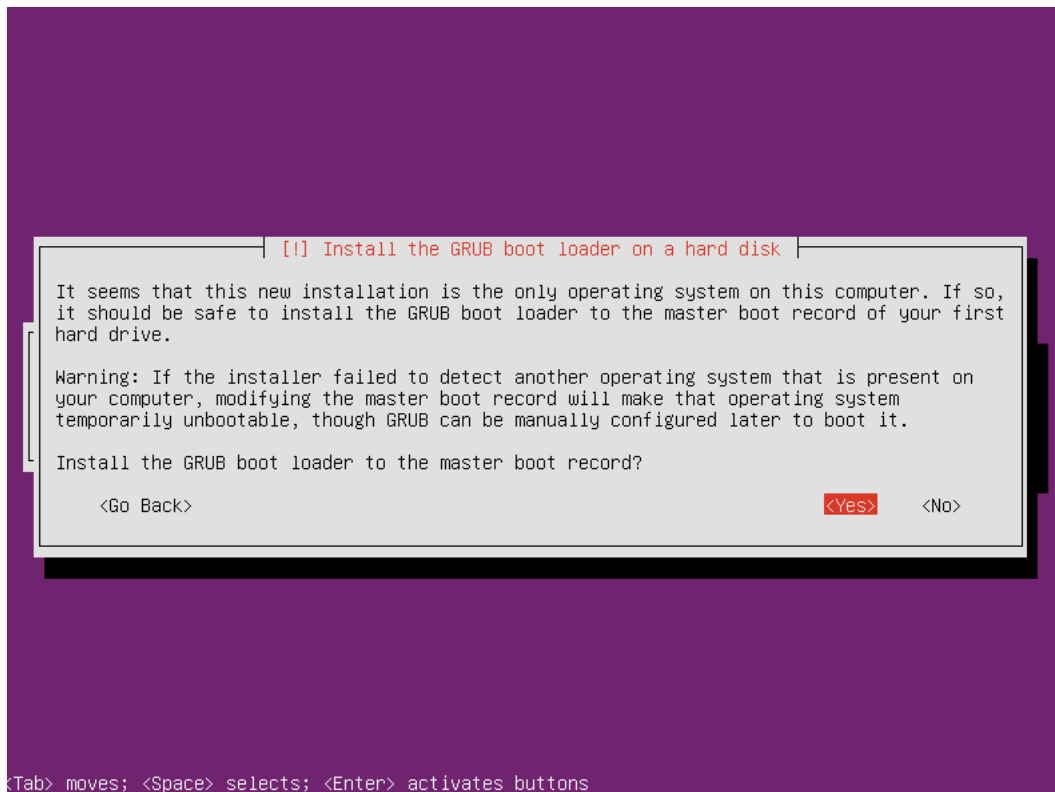
Da wir keine weiteren Komponenten zwingend benötigen können Sie ohne zusätzliche Auswahl von Paketen fortfahren. Optional können Sie den OpenSSH Server auswählen, dadurch muss Schritt 1.5. nicht vollständig beachtet werden.



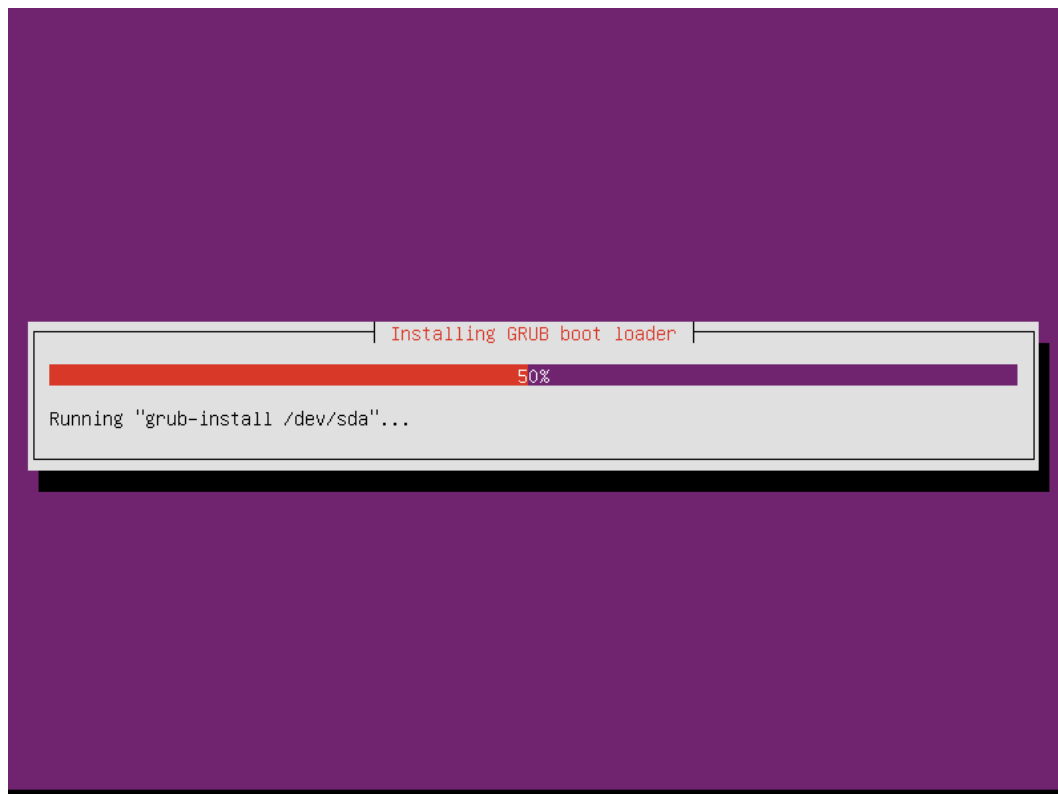
Nun wird Ubuntu auf die virtuelle Maschine installiert.



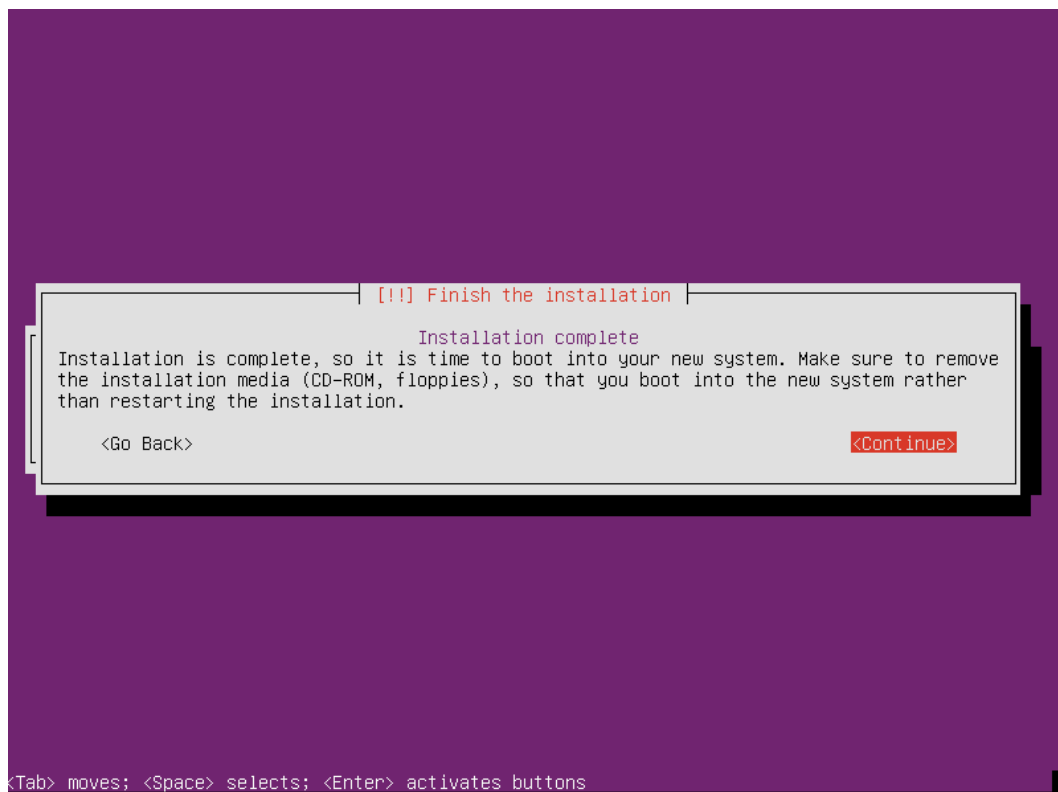
Nach Abschluss muss noch der Master Boot Record (MBR) geschrieben werden. Bestätigen Sie dies mit Ja, da sonst ggf. Das Betriebssystem nicht startet.



Der Assistent schließt nun die Installation ab

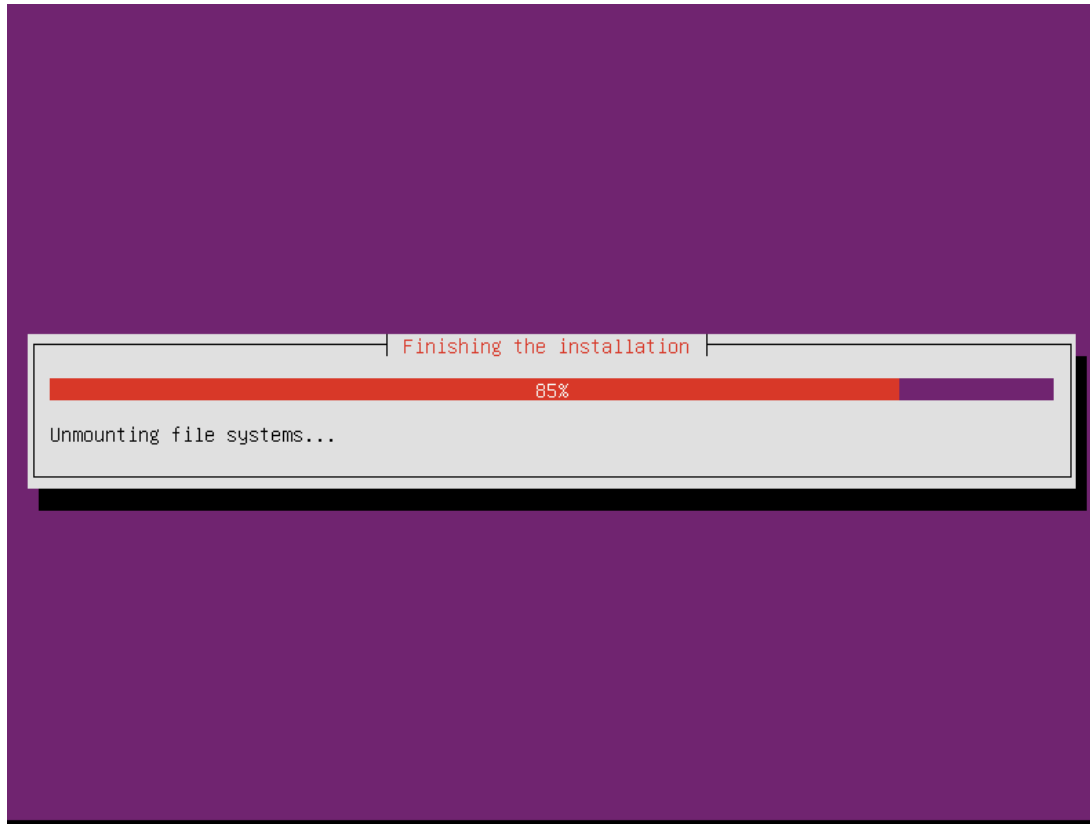


Damit nicht erneut die Installationsroutine von dem hinzugefügten ISO Image gestartet wird, Kann Ubuntu dieses automatisch entfernen und das System neustarten.



<Tab> moves; <Space> selects; <Enter> activates buttons

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 erstellten Benutzernamen an. Wir führen einige grundsätzliche Einstellungen durch, damit wir mit der Installation von privacyIDEA beginnen können.

Als erstes setzen wir eine statische IP Adresse. Selbstverständlich können Sie auch das Netzwerkinterface auf DHCP belassen, sollten jedoch sicherstellen, dass 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:

```
GNU nano 2.5.3 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
```

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:

```
GNU nano 2.5.3 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 172.17.7.205
netmask 255.255.255.0
gateway 172.17.7.1
dns-nameservers 172.17.7.10 172.17.7.1_
```

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.

The screenshot shows the Windows DNS console with a list of DNS records. The records are organized into a table with columns: Name, Typ, Daten, and Zeitstempel. The records include various hosts and services, such as dc01, firewall01, nas01, backup01, PC06, PC01, PC04, PC02, PC05, Dev01, Management01, management02, mail01, kinu01, ucs-ssn, FILESERVER02, Workstation, SERVER01, and Ginave. A dialog box titled 'Neuer Host' is open, showing the 'Name' field with 'privacyidea' and the 'IP-Adresse' field with '172.17.7.205'. The dialog also has checkboxes for 'Verknüpfen PTR-Eintrag erstellen' and 'Authentifizierte Benutzer können DNS-Einträge mit demselben Benutzeramen aktualisieren'.

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 Konfiguration des SSH Daemon fortfahren, in unserem Beispiel installieren wir diesen manuell.

Diesen können Sie mit folgender Zeile installieren.

Command: `sudo apt-get install ssh`

```

administrator@privacyidea:~$ sudo apt-get install ssh
[sudo] password for administrator:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  librap0 ncurses-term openssl-server openssl-sftp-server python3-requests python3-urllib3 ssh-import-id tcpd
Suggested packages:
  ssh-askpass rssh molly-guard monkeysphere python3-mdg-httpclient python3-openssl python3-pyasn1
The following NEW packages will be installed:
  librap0 ncurses-term openssl-server openssl-sftp-server python3-requests python3-urllib3 ssh-import-id tcpd
0 upgraded, 9 newly installed, 0 to remove and 82 not upgraded.
Need to get 822 kB of archives.
After this operation, 5,299 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 librap0 amd64 7.6.q-25 [46.2 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 openssl-sftp-server amd64 1:7.2p2-4ubuntu2.4 [39.7 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 openssl-server amd64 1:7.2p2-4ubuntu2.4 [335 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 ssh all 1:7.2p2-4ubuntu2.4 [7,076 B]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 ncurses-term all 6.0+20160213-1ubuntu1 [249 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 python3-urllib3 all 1.13.1-2ubuntu0.16.04.1 [57.3 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 python3-requests all 2.9.1-3 [55.4 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 tcpd amd64 7.6.q-25 [23.0 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 ssh-import-id all 5.5-0ubuntu1 [10.2 kB]
Fetched 822 kB in 1s (552 kB/s)
Unpacking previously unselected package librap0:amd64.
(Reading database ... 57183 files and directories currently installed.)
Preparing to unpack .../librap0_7.6.q-25_amd64.deb ...
Unpacking librap0:amd64 (7.6.q-25) ...
Selecting previously unselected package openssl-sftp-server.
Preparing to unpack .../openssl-sftp-server_1:3a7.2p2-4ubuntu2.4_amd64.deb ...
Unpacking openssl-sftp-server (1:3a7.2p2-4ubuntu2.4) ...
Selecting previously unselected package openssl-server.
Preparing to unpack .../openssl-server_1:3a7.2p2-4ubuntu2.4_amd64.deb ...
Unpacking openssl-server (1:3a7.2p2-4ubuntu2.4) ...
Selecting previously unselected package ssh.
Preparing to unpack .../ssh_1:3a7.2p2-4ubuntu2.4_all.deb ...
Unpacking ssh (1:3a7.2p2-4ubuntu2.4) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.0+20160213-1ubuntu1_all.deb ...
Unpacking ncurses-term (6.0+20160213-1ubuntu1) ...

```

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

```

GNU nano 2.5.3      File: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#PrivilegeSeparation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile      ~/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
IgnoreUserKnownHosts yes

```

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

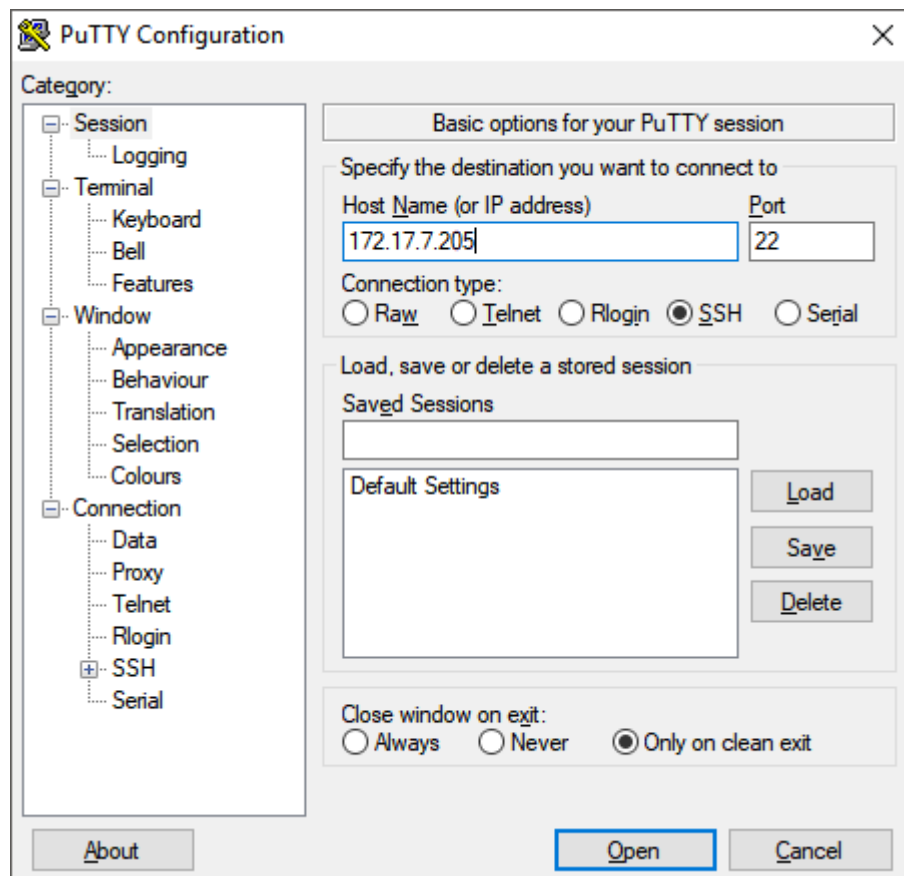
Command: `sudo service ssh restart`

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

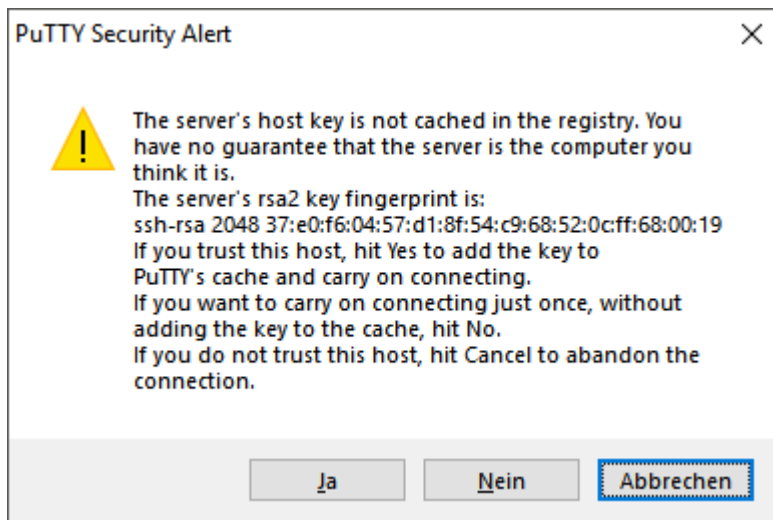
1.6. Verbindung via SSH Client (z.B. Putty) testen

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.



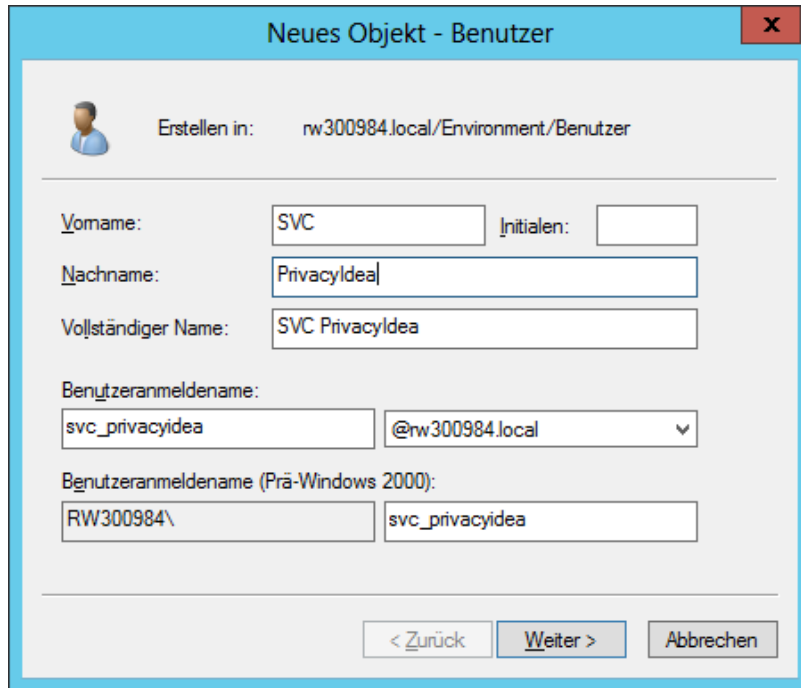
Anschliessend sehen Sie die Anmeldung am Ubuntu Server.



1.7. Service Account in Active Directory anlegen

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)



Neues Objekt - Benutzer

Erstellen in: nw300984.local/Environment/Benutzer

Vorname: SVC Initialen:

Nachname: PrivacyIdea

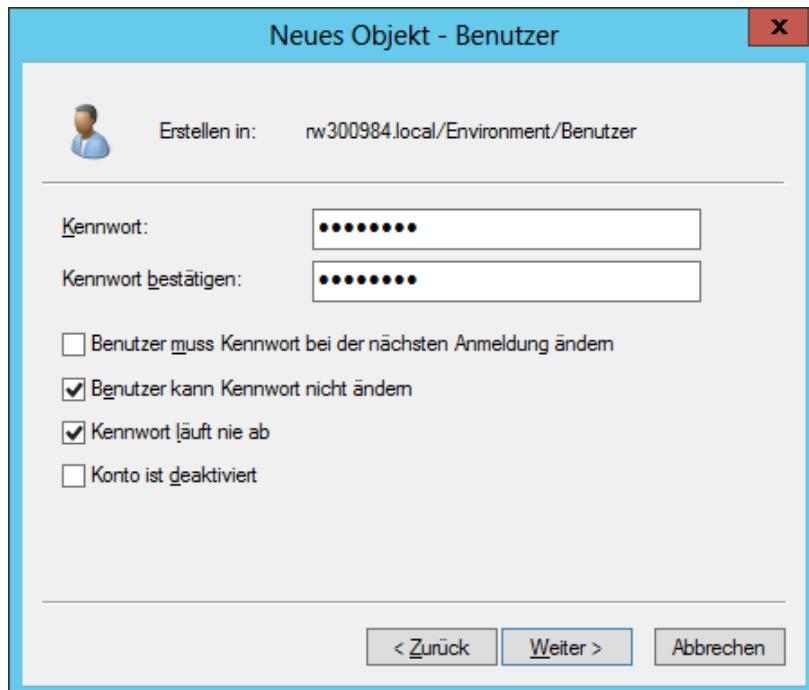
Vollständiger Name: SVC PrivacyIdea

Benutzeranmeldename: svc_privacyidea @nw300984.local

Benutzeranmeldename (Prä-Windows 2000): RW300984\svc_privacyidea

< Zurück Weiter > Abbrechen

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



Neues Objekt - Benutzer

Erstellen in: nw300984.local/Environment/Benutzer

Kennwort:

Kennwort bestätigen:

☐ Benutzer muss Kennwort bei der nächsten Anmeldung ändern

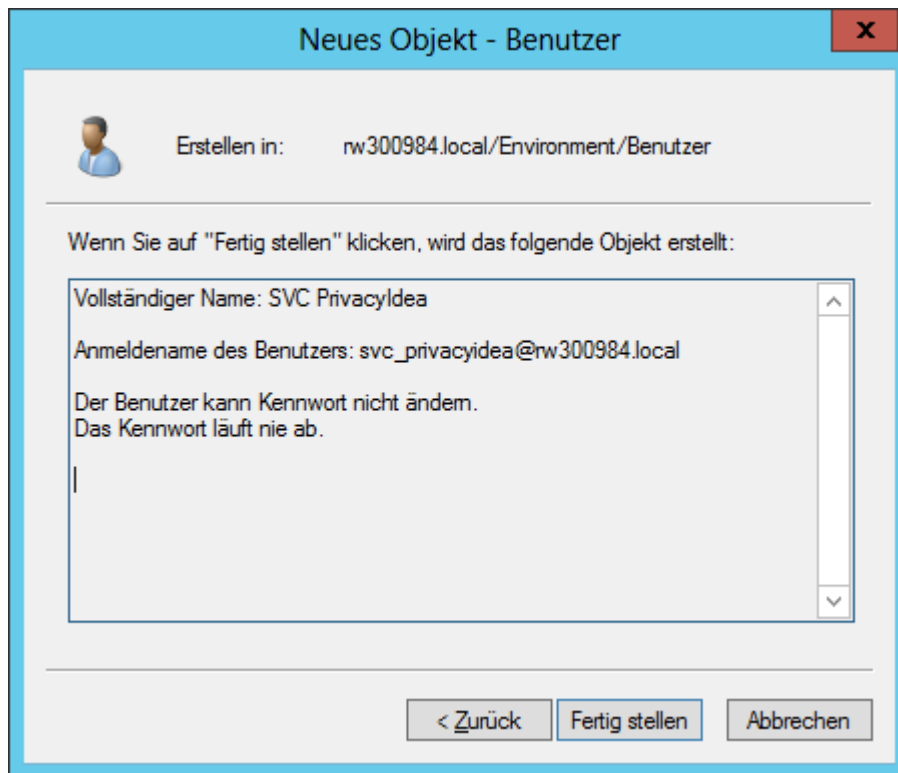
☒ Benutzer kann Kennwort nicht ändern

☒ Kennwort läuft nie ab

☐ Konto ist deaktiviert

< Zurück Weiter > Abbrechen

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



Neues Objekt - Benutzer

Erstellen in: rw300984.local/Environment/Benutzer

Wenn Sie auf "Fertig stellen" klicken, wird das folgende Objekt erstellt:

Vollständiger Name: SVC PrivacyIdea

Anmeldename des Benutzers: svc_privacyidea@rw300984.local

Der Benutzer kann Kennwort nicht ändern.
Das Kennwort läuft nie ab.

< Zurück Fertig stellen Abbrechen

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`

```
administrator@privacyidea: ~  
administrator@privacyidea:~$ sudo add-apt-repository ppa:privacyidea/privacyidea  
[sudo] password for administrator:  
This repository contains releases of privacyIDEA.  
privacyIDEA is a modular authentication system for two factor authentication. It  
runs on Linux and is completely opensource, licensed under the AGPLv3.  
  
You can install privacyidea via  
  
    apt-get install privacyidea-apache2  
  
Then you need to create your initial administrator via  
  
    pi-manage admin add administrator  
  
For more information see https://privacyidea.org  
More info: https://launchpad.net/~privacyidea/+archive/ubuntu/privacyidea  
Press [ENTER] to continue or ctrl-c to cancel adding it  
█
```

2.2. Updaten der Ubuntu Repositories

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

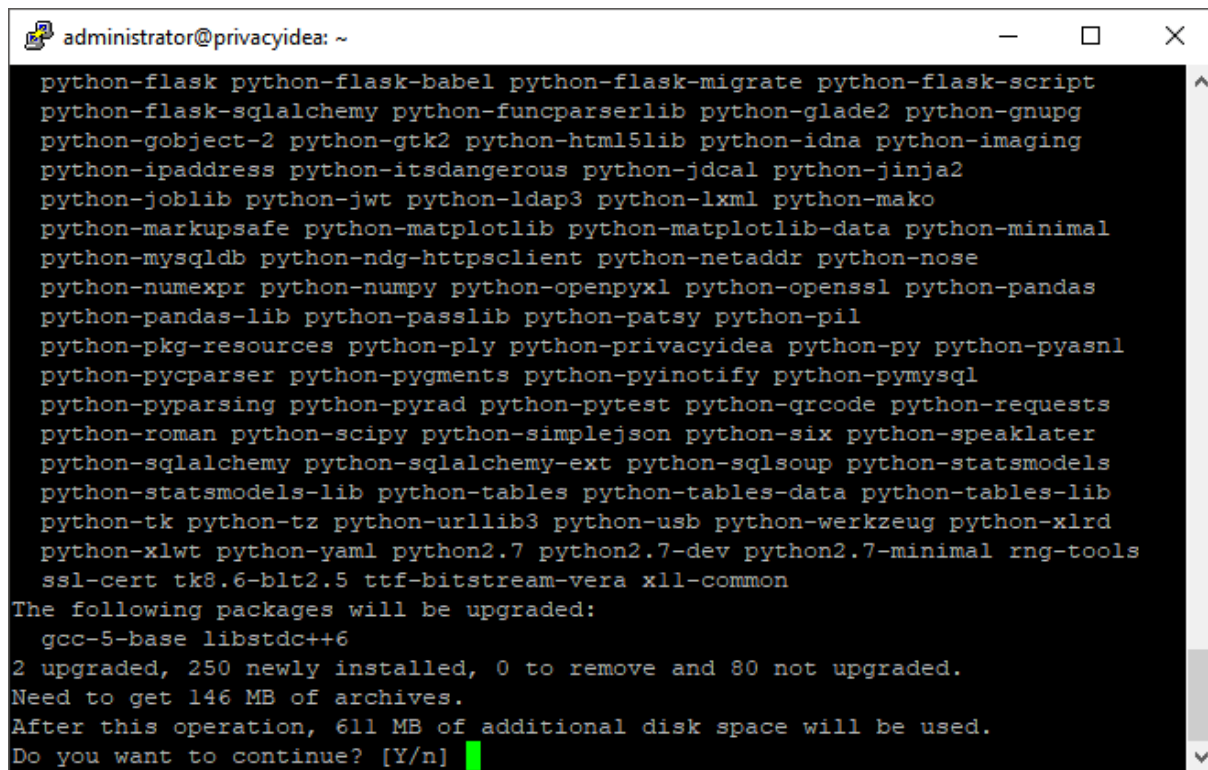
Command: `sudo apt-get update`

```
administrator@privacyidea: ~  
gpg: keyring `/tmp/tmpsp0e3l0k/secring.gpg' created  
gpg: keyring `/tmp/tmpsp0e3l0k/pubring.gpg' created  
gpg: requesting key C24DCF7D from hkp server keyserver.ubuntu.com  
gpg: /tmp/tmpsp0e3l0k/trustdb.gpg: trustdb created  
gpg: key C24DCF7D: public key "Launchpad PPA for privacyidea" imported  
gpg: Total number processed: 1  
gpg:      imported: 1 (RSA: 1)  
OK  
administrator@privacyidea:~$ sudo apt-get update  
Hit:1 http://security.ubuntu.com/ubuntu xenial-security InRelease  
Get:2 http://ppa.launchpad.net/privacyidea/privacyidea/ubuntu xenial InRelease [18.1 kB]  
Hit:3 http://us.archive.ubuntu.com/ubuntu xenial InRelease  
Hit:4 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease  
Hit:5 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease  
Get:6 http://ppa.launchpad.net/privacyidea/privacyidea/ubuntu xenial/main amd64 Packages [3,056 B]  
Get:7 http://ppa.launchpad.net/privacyidea/privacyidea/ubuntu xenial/main i386 Packages [3,056 B]  
Get:8 http://ppa.launchpad.net/privacyidea/privacyidea/ubuntu xenial/main Translation-en [1,944 B]  
Fetched 26.1 kB in 0s (27.1 kB/s)  
█
```

2.3. Installation von privacyIDEA

Nun starten wir die Installation mit folgendem Kommando.

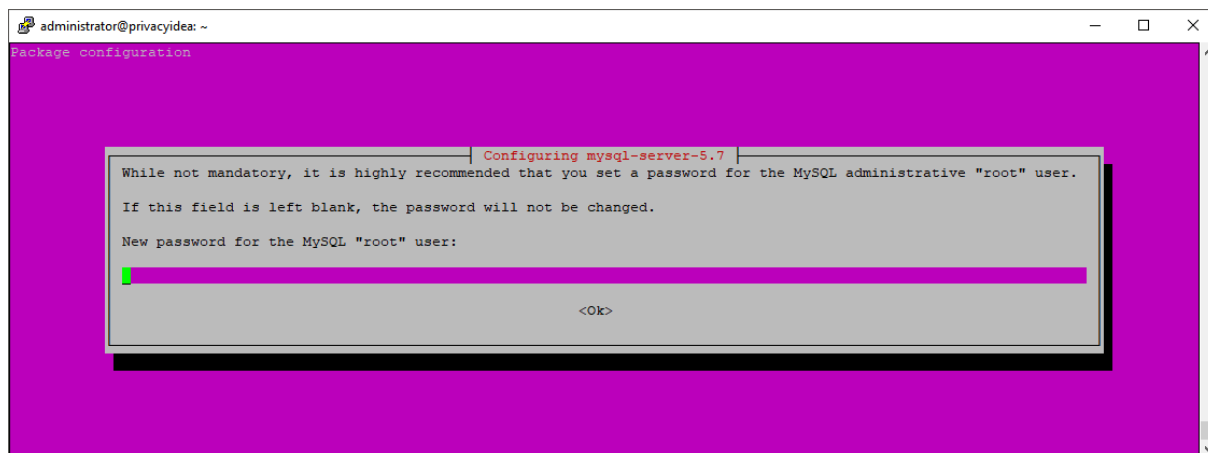
Command: `sudo apt-get install privacyIDEA-apache2`



```
administrator@privacyidea: ~  
python-flask python-flask-babel python-flask-migrate python-flask-script  
python-flask-sqlalchemy python-funcparserlib python-glade2 python-gnupg  
python-gobject-2 python-gtk2 python-html5lib python-idna python-imaging  
python-ipaddress python-itsdangerous python-jdcal python-jinja2  
python-joblib python-jwt python-ldap3 python-lxml python-mako  
python-markupsafe python-matplotlib python-matplotlib-data python-minimal  
python-mysqldb python-ndg-httpsclient python-netaddr python-nose  
python-numexpr python-numpy python-openpyxl python-openssl python-pandas  
python-pandas-lib python-passlib python-patsy python-pil  
python-pkg-resources python-ply python-privacyidea python-py python-pyasn1  
python-pyparser python-pygments python-pyinotify python-pymysql  
python-pyparsing python-pyrad python-pytest python-qrcode python-requests  
python-roman python-scipy python-simplejson python-six python-speaklater  
python-sqlalchemy python-sqlalchemy-ext python-sqlsoup python-statsmodels  
python-statsmodels-lib python-tables python-tables-data python-tables-lib  
python-tk python-tz python-urllib3 python-usb python-werkzeug python-xlrd  
python-xlwt python-yaml python2.7 python2.7-dev python2.7-minimal rng-tools  
ssl-cert tk8.6-blt2.5 ttf-bitstream-vera x11-common  
The following packages will be upgraded:  
gcc-5-base libstdc++6  
2 upgraded, 250 newly installed, 0 to remove and 80 not upgraded.  
Need to get 146 MB of archives.  
After this operation, 611 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

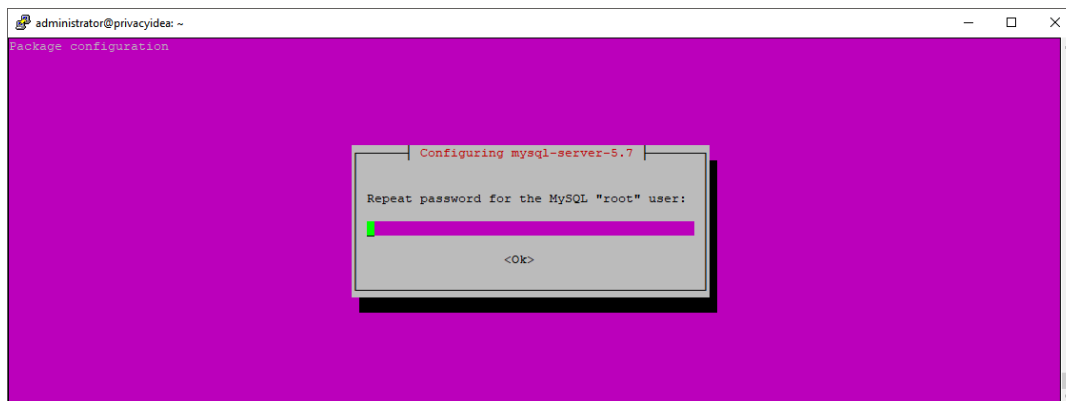
Benötigte Komponenten wie z.B. Apache Webserver oder MySQL Datenbank werden während der Installation automatisch installiert. Jedoch sind einige Eingabe erforderlich.

Vergeben Sie nun das Passwort für den MySQL Root Account:

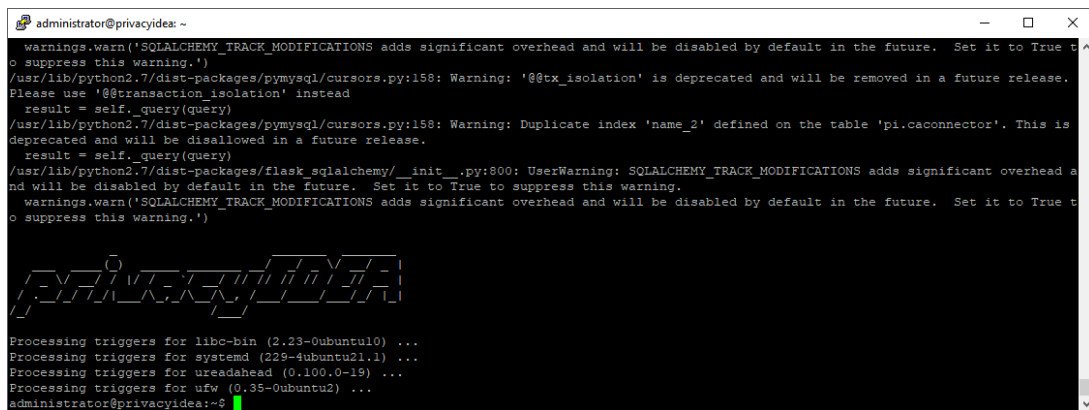


```
administrator@privacyidea: ~  
Package configuration  
Configuring mysql-server-5.7  
While not mandatory, it is highly recommended that you set a password for the MySQL administrative "root" user.  
If this field is left blank, the password will not be changed.  
New password for the MySQL "root" user:  
<Ok>
```


Bestätigen Sie dies durch nochmalige Eingabe:



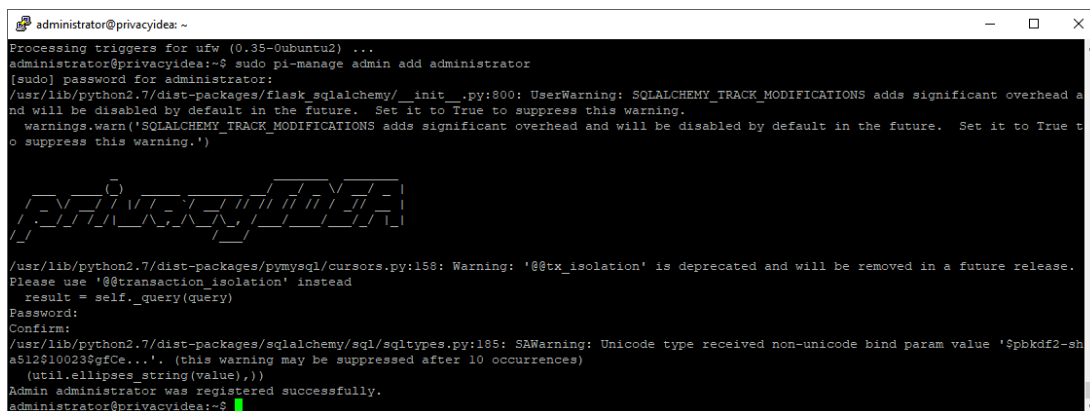
Wurde die Installation erfolgreich abgeschlossen. Sollten Sie wie im unteren Screenshot gezeigt aussehen.



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`



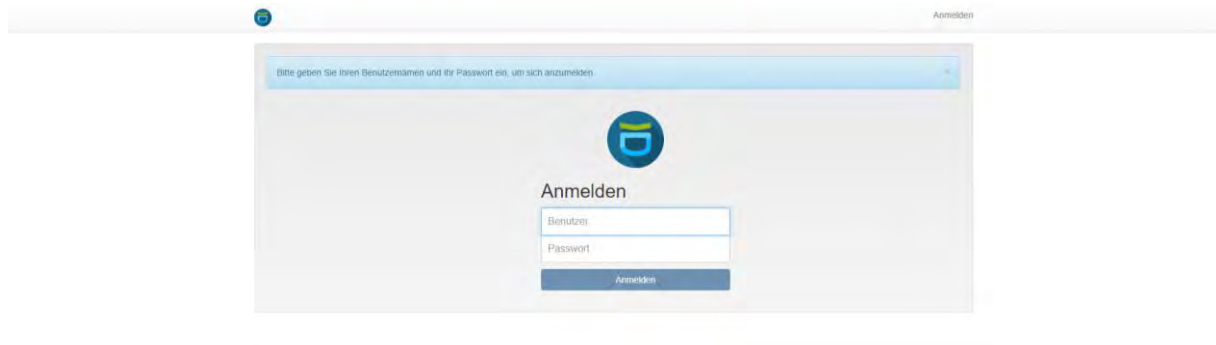
2.5. Erreichbarkeit des Webinterface testen

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).

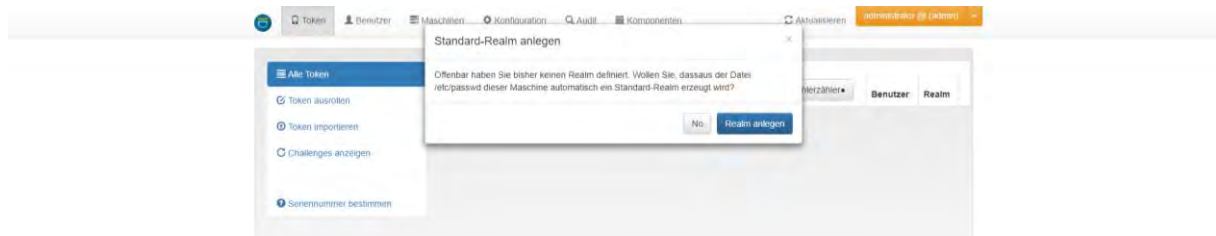
URL: <https://ip-address> oder <https://fgdn>

Benutzer: administrator

Password: bei der Installation des Betriebssystems 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 Authentifizierung 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`

```

administrator@privacyidea: ~
/usr/lib/python2.7/dist-packages/pymysql/cursors.py:158: Warning: '@@tx_isolation' is deprecated and will be removed in a future release.
Please use '@@transaction_isolation' instead
    result = self._query(query)
Password:
Confirm:
/usr/lib/python2.7/dist-packages/sqlalchemy/sql/sqltypes.py:185: SAWarning: Unicode type received non-unicode bind param value '$pbkdf2-sh
a5129100239gfCe...'. (this warning may be suppressed after 10 occurrences)
    (util.ellipses_string(value),))
Admin administrator was registered successfully.
administrator@privacyidea:~$ sudo apt-get install freeradius
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  freeradius-common freeradius-utils libdbi-perl libfreeradius2
Suggested packages:
  freeradius-ldap freeradius-postgresql freeradius-mysql freeradius-krb5 libclone-perl libmldbm-perl libnet-daemon-perl
  libsql-statement-perl
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-utils libdbi-perl libfreeradius2
0 upgraded, 5 newly installed, 0 to remove and 80 not upgraded.
Need to get 1,617 kB of archives.
After this operation, 5,843 kB of additional disk space will be used.
Do you want to continue? [Y/n]

```

2.7. privacyIDEA Radius Plugin installieren

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

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

```

administrator@privacyidea: ~
administrator@privacyidea:~$ sudo apt-get install privacyidea-radius
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libauthen-sasl-perl libcommon-sense-perl libconfig-inifiles-perl libdata-dump-perl libfile-listing-perl libfont-afm-perl
  libhtml-form-perl libhtml-format-perl libhtml-tree-perl libhttp-cookies-perl libhttp-daemon-perl libhttp-negotiate-perl
  libio-socket-ssl-perl libjson-perl libjson-xs-perl liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl
  libnet-ssleay-perl libtiny-perl libtypes-serializer-perl libwww-perl libwww-robotrules-perl
Suggested packages:
  libdigest-hmac-perl libgssapi-perl libcrypt-ssleay-perl libauthen-ntlm-perl
The following NEW packages will be installed:
  libauthen-sasl-perl libcommon-sense-perl libconfig-inifiles-perl libdata-dump-perl libfile-listing-perl libfont-afm-perl
  libhtml-form-perl libhtml-format-perl libhtml-tree-perl libhttp-cookies-perl libhttp-daemon-perl libhttp-negotiate-perl
  libio-socket-ssl-perl libjson-perl libjson-xs-perl liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl
  libnet-ssleay-perl libtiny-perl libtypes-serializer-perl libwww-perl libwww-robotrules-perl privacyidea-radius
0 upgraded, 25 newly installed, 0 to remove and 80 not upgraded.
Need to get 1,378 kB of archives.
After this operation, 4,626 kB of additional disk space will be used.
Do you want to continue? [Y/n]

```

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
```

```
}
```

```

root@privacyidea: /etc/freeradius
GNU nano 2.5.3      File: clients.conf      Modified
#
# The following two configurations are for future use.
# The 'naspasswd' file is currently used to store the NAS
# login name and password, which is used by checkrad.pl
# when querying the NAS for simultaneous use.
#
# login      = !root
# password   = someadminpas
#
# As of 2.0, clients can also be tied to a virtual server.
# This is done by setting the "virtual_server" configuration
# item, as in the example below.
#
# virtual_server = homel
#
# A pointer to the "home_server_pool" OR a "home_server"
# section that contains the CoA configuration for this
# client. For an example of a coa home server or pool,
# see raddb/sites-available/originate-coa
#
# coa_server = coa
#
# IPv6 Client
#client ::1 {
#    secret      = testing123
#    shortname   = localhost
#}
#
# All IPv6 Site-local clients
#client fe80::/16 {
#    secret      = testing123
#    shortname   = localhost
#}
#
#client some.host.org {
#    secret      = testing123
#    shortname   = localhost
#}
#
# You can now specify one secret for a network of clients.
# When a client request comes in, the BEST match is chosen.
# i.e. The entry from the smallest possible network.
#
client 172.17.7.0/24 {
    secret      = myownsecret
}
#
#client 192.168.0.0/16 {
#    secret      = testing123-2
#    shortname   = private-network-2
#}
#
#client 10.10.10.10 {
#    # secret and password are mapped through the "secrets" file.
#}
^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      ^Y Prev Page
^X Exit          ^R Read File    ^\ Replace      ^U Uncut Text   ^I To Spell     ^_ Go To Line    ^V Next Page

```

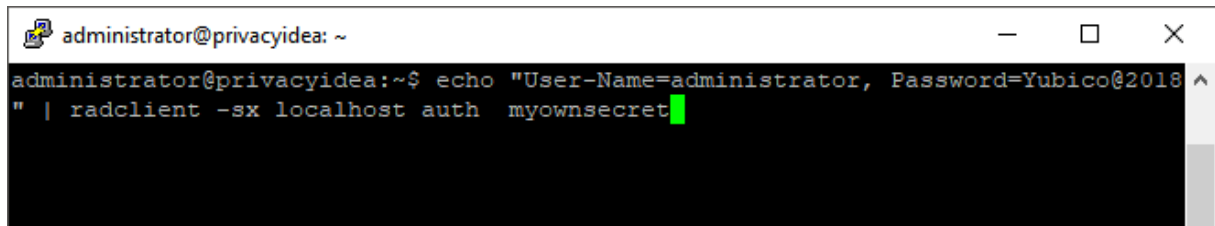
Damit die neue Konfiguration angewendet wird, müssen Sie den FreeRadius Server neustarten.

Command: `service freeradius restart`

2.9. Testen von FreeRadius und privacyIDEA kommunikation via radclient

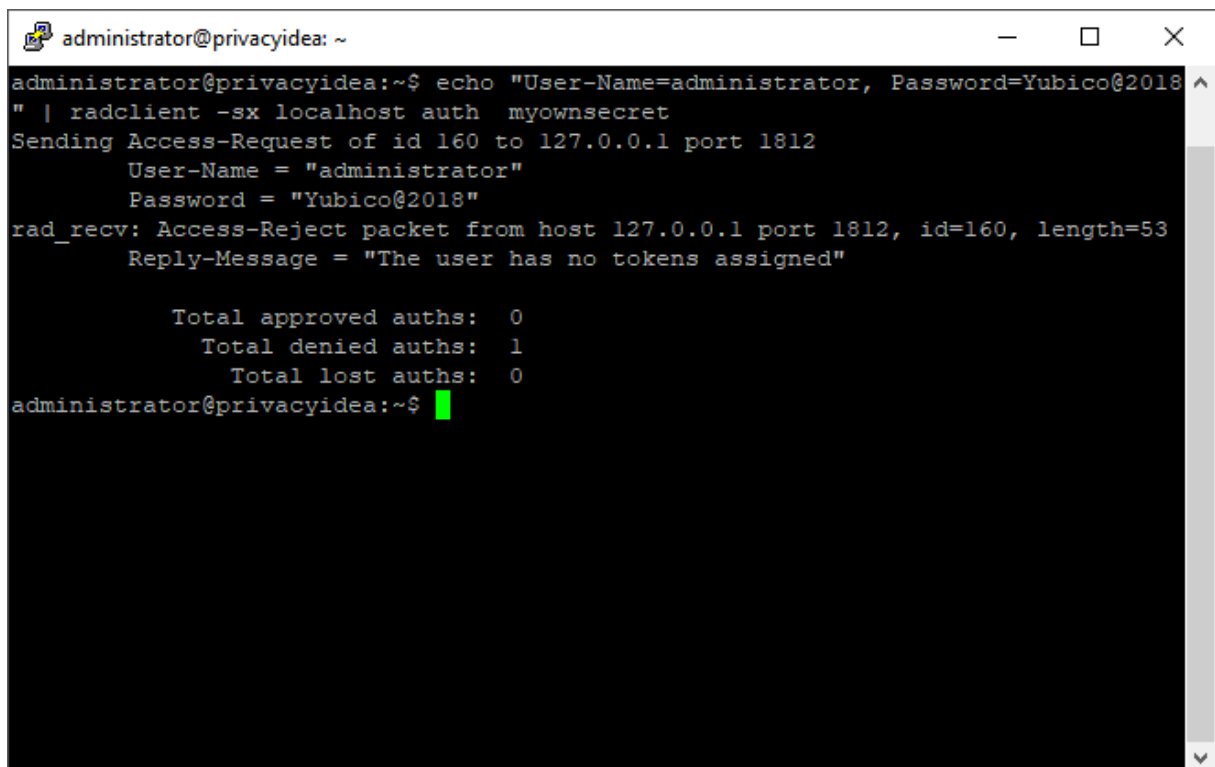
Nun können wir bereits anfangen die Radius Authentifizierung gegen das privacyIDEA Backend zu testen. Dies dient einerseits zu sehen ob der Radius Server auf Anfragen antwortet, sowie ob die Anfrage an privacyIDEA weitergeleitet wird.

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

A terminal window titled 'administrator@privacyidea: ~' showing the command `echo "User-Name=administrator, Password=Yubico@2018" | radclient -sx localhost auth myownsecret` being entered. The cursor is at the end of the command line.

```
administrator@privacyidea: ~  
administrator@privacyidea:~$ 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 folgende Meldung:

A terminal window titled 'administrator@privacyidea: ~' showing the output of the previous command. The output indicates that an Access-Request was sent to 127.0.0.1:1812, but it was rejected with the message 'The user has no tokens assigned'. It also shows summary statistics for the authentication attempt.

```
administrator@privacyidea: ~  
administrator@privacyidea:~$ echo "User-Name=administrator, Password=Yubico@2018"  
" | radclient -sx localhost auth myownsecret  
Sending Access-Request of id 160 to 127.0.0.1 port 1812  
  User-Name = "administrator"  
  Password = "Yubico@2018"  
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=160, length=53  
  Reply-Message = "The user has no tokens assigned"  
  
      Total approved auths: 0  
      Total denied auths:  1  
      Total lost auths:    0  
administrator@privacyidea:~$
```

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

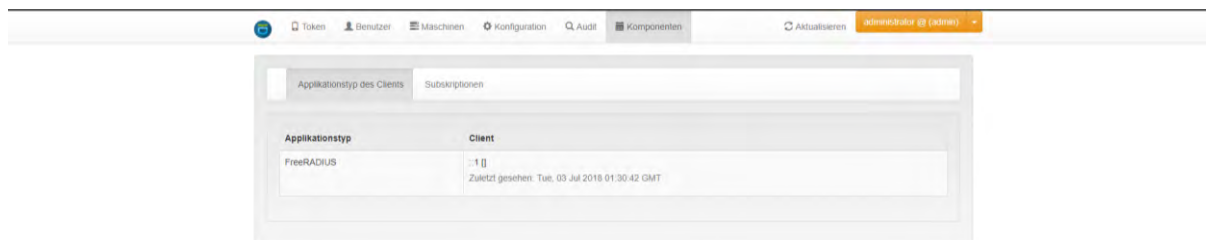
Sollte die Clients.conf falsch sein, d.h. z.B. Secret ist falsch, dann erhalten Sie folgende Meldung:

```

administrator@privacyidea: ~
administrator@privacyidea:~$ echo "User-Name=administrator, Password=Yubico@2018" | radclient -sx localhost auth myownsecret
Sending Access-Request of id 79 to 127.0.0.1 port 1812
    User-Name = "administrator"
    Password = "Yubico@2018"
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=79, length=53
rad_verify: Received Access-Reject packet from home server 127.0.0.1 port 1812 with invalid Response Authenticator! (Shared secret is incorrect.)
^C
administrator@privacyidea:~$
  
```

Sollte der Radius Server nicht auf Anfragen von der IP Adresse 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

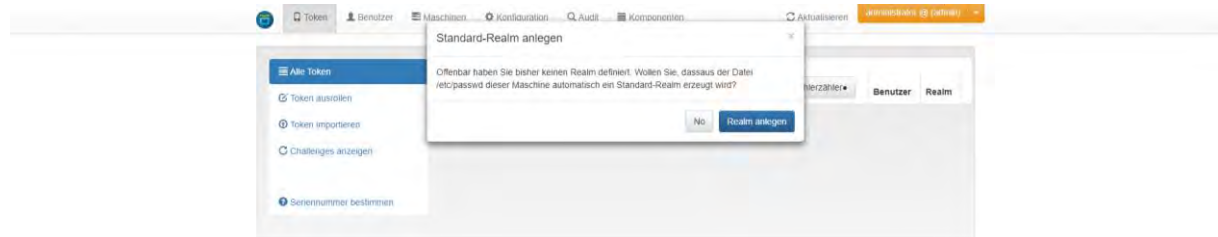
In unserer Beispielumgebung möchten wir erreichen das sich Benutzer mit Ihrem Active Directory Benutzernamen, dem Passwort und einem OTP (One Time Password) anmelden müssen. Damit privacyIDEA die Information des Active Directory erhält muss dies über einen sogenannten Realm und Resolver

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 authentifiziert 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.

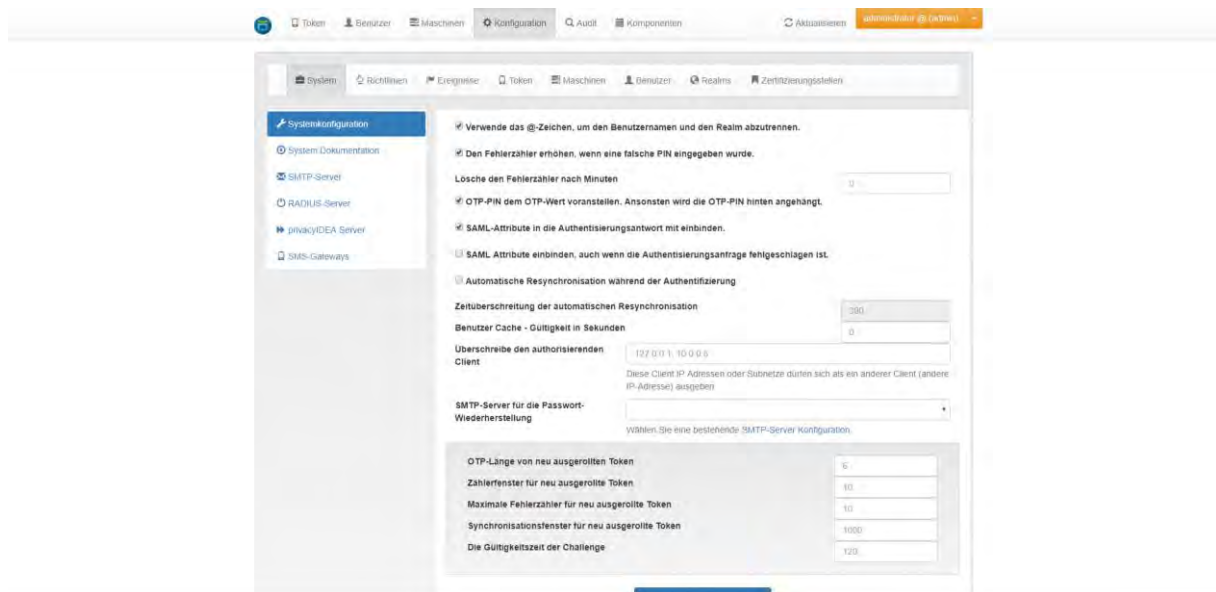
Der Assistent im privacyIDEA Webinterface legt automatisch einen Standard Realm an.



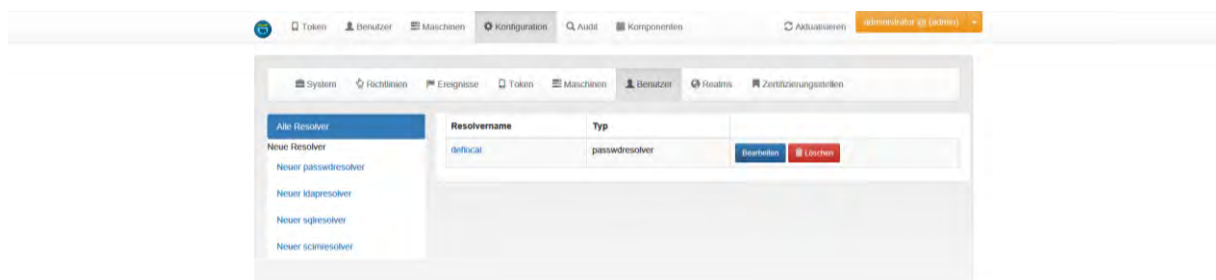
3.2. ActiveDirectory Resolver anlagen

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

Klicken Sie auf Konfiguration



Klicken Sie auf Resolver



Klicken Sie nun auf „Neuer LDAPResolver“

The screenshot shows the 'Erzeuge einen neuen LDAP-Resolver' (Create a new LDAP Resolver) form in the Yubico PrivacyIDE configuration tool. The form is titled 'Erzeuge einen neuen LDAP-Resolver' and contains the following fields and options:

- Resolvername:** resolver1
- Server-URI:** ldap://privacyidea.server1.ldap://privacyidea.server2
- TLS verifizieren:** ☒ Das TLS Zertifikat des LDAP Servers wird verifiziert.
- Die Datei mit dem CA-Zertifikat, das das LDAP-TLS-Zertifikat signiert hat:** /etc/privacyidea/ldap-ca.crt
- TLS Protokollversion:** (dropdown menu)
- Base-DN:** ou=users,dc=domain,dc=ld
- Geltungsbereich:** SUBTREE
- Bind-DN:** cn=admin,ou=users,dc=domain,dc=ld
- Bind-Passwort:** ldapsecret
- Bind-Typ:** Simple
- Time-out (Sekunden):** 5
- Cache-Zeitüberschreitung (Sekunden):** 120
- Serverpool Rundenanzahl:** 2
- Zeit, die ein nicht erreichbarer Server im Serverpool ignoriert wird (Sekunden):** 30

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.

The screenshot shows the 'LDAP-Resolver konfigurieren' (Configure LDAP Resolver) form in the Yubico PrivacyIDE configuration tool. The form is titled 'LDAP-Resolver konfigurieren' and contains the following fields and options:

- Bind-Passwort:** (password field)
- Bind-Typ:** Simple
- Time-out (Sekunden):** 5
- Cache-Zeitüberschreitung (Sekunden):** 120
- Serverpool Rundenanzahl:** 2
- Zeit, die ein nicht erreichbarer Server im Serverpool ignoriert wird (Sekunden):** 30
- Größenbeschränkung:** 500
- Benutzerquelle editierbar:** ☒ Die Benutzerdaten in der Datenbank können von privacyIDEA aus verwaltet werden.
- LDAP-Resolver konfigurieren:** (tab selected)
- Loginname Attribut:** sAMAccountName
- Suchfilter:** (&sAMAccountName=*)(objectClass=person)
- Attributzuordnung:** ["telephoneNumber", "mobile", "email", "mail", "surname", "sn", "givenName", "givenNameInitials"]
- Attribute mit mehreren Werten:** ["mobile"]
- UID Typ:** objectGUID
- Referrals werden nicht (anonym) verfolgt:** ☒
- Schema-Informationen werden nicht abgerufen:** ☒

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

The screenshot shows the 'Konfiguration' (Configuration) tab in the Yubico management interface. The 'Active Directory verbinden' (Connect Active Directory) section is active. It includes fields for 'Bind-Passwort' (Bind Password), 'Bind-Typ' (Bind Type) set to 'Simple', 'Time-out (Sekunden)' (5), 'Cache-Zeitüberschreitung (Sekunden)' (120), 'Serverpool-Rundenanzahl' (2), 'Zeit, die ein nicht erreichbarer Server im Serverpool ignoriert wird (Sekunden)' (30), and 'Größenbeschränkung' (500). There are checkboxes for 'Benutzerquelle editierbar' and 'Referrals werden nicht (anonym) verfolgt'. Below these are tabs for 'LDAP-Verbinden' and 'Active Directory verbinden'. The 'Active Directory verbinden' tab is selected, showing fields for 'Loginname Attribut' (sAMAccountName), 'Suchfilter' ((sAMAccountName=*)(objectClass=person)), 'Attributzusordnung' ({'phone', 'telephoneNumber', 'mobile', 'mobile', 'email', 'mail', 'surname', 'sn', 'gn', 'mobile'}), 'Attribute mit mehreren Werten' (mobile), and 'UID Typ' (objectGUID). At the bottom, there are buttons for 'Schlüssel (Resolver) testen', 'LDAP-Verbinden testen', and 'Resolver speichern'.

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 neuen Realm für die Active Directory.

Klicken Sie auf Konfiguration

The screenshot shows the 'Konfiguration' (Configuration) tab in the Yubico management interface, specifically the 'Systemkonfiguration' (System Configuration) section. It includes a sidebar with links to 'Systemkonfiguration', 'System Dokumentation', 'SMTP-Server', 'RADIUS-Server', 'privacyIDEA-Server', and 'SMS-Gateways'. The main area contains various configuration options for the system, including checkboxes for 'Verwende das @-Zeichen, um den Benutzernamen und den Realm abzutrennen', 'Den Fehlerzähler erhöhen, wenn eine falsche PIN eingegeben wurde', 'Löschen den Fehlerzähler nach Minuten', 'OTP-PIN dem OTP-Wert voranstellen', 'SAML-Attribute in die Authentifizierungsantwort mit einbinden', and 'SAML-Attribute einbinden, auch wenn die Authentifizierungsanfrage fehlgeschlagen ist'. There are also fields for 'Zeitüberschreitung der automatischen Resynchronisation' (300), 'Benutzer Cache - Gültigkeit in Sekunden' (0), 'Überschreibe den autorisierenden Client' (127.0.0.1, 10.0.0.8), 'SMTP-Server für die Passwort-Wiederherstellung', and several fields for token configuration: 'OTP-Länge von neu ausgerichteten Token' (6), 'Zählerfenster für neu ausgerollte Token' (10), 'Maximale Fehlerzähler für neu ausgerollte Token' (10), 'Synchronisationsfenster für neu ausgerollte Token' (1000), and 'Die Gültigkeitszeit der Challenge' (120).

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.

Benutzername	Nachname	Vorname	E-Mail	Telefon	Mobiletelefon	Beschreibung
service		ServiceAccount	serviceaccount@nc300984.local	9		
svc_privacyidea	Privacyidea	SVC				
ronny.wolf	Wolf	Ronny	ronny.wolf@nc300984.de	34567	1	
gina.velasquez	Velasquez	Gina	gina.velasquez@nc300984.local	31	2	

3.5. Überprüfen ob Anmeldung mit Benutzer möglich ist

Da die Benutzerauthentifizierung 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 detailliert darauf eingehen.

4. Konfiguration privacyIDEA – Richtlinien und Ereignisse

In privacyIDEA wird über Richtlinien definiert, wie sich das System verhalten soll bei Authentifizierungen 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>

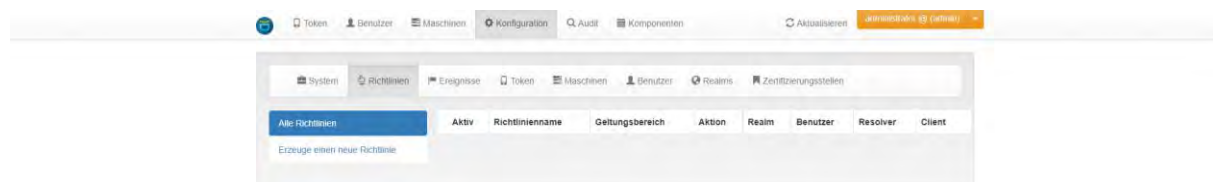
Darüber hinaus können Sie Ereignisse definieren. Diese Beschreiben was nach einem bestimmte Event (Ereignis) passieren soll z.B. wenn eine Benutzerauthentifizierung fehlgeschlagen ist. Weitere Informationen zu Ereignissen finden Sie hier:

<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 Richtlinie, 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

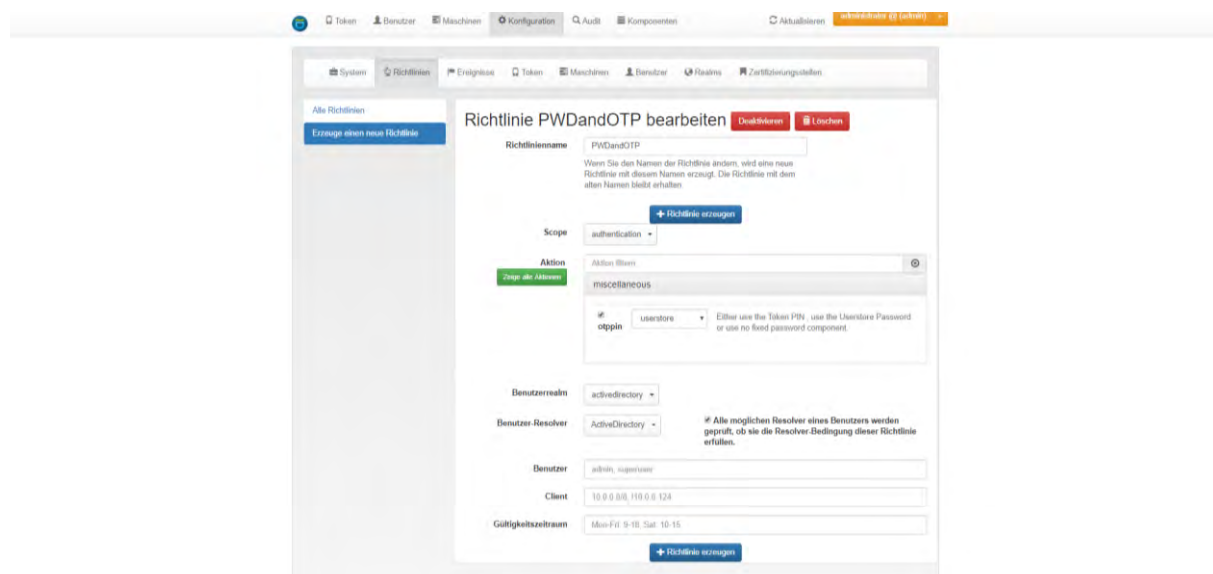
Scope: Authentication

Aktion: OTTPin

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 Authentifizierung an den Realm/Resolver schicken. Die Eingabe bei den meisten System (z.B. die im Guide vorstellten Firewalls)erfolgt hier:

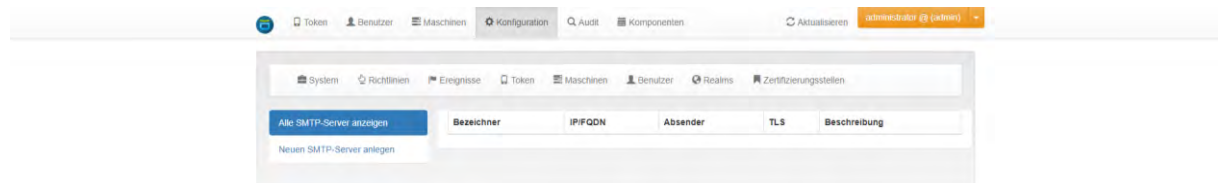
Benutzername: Active Directory Benutzername

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

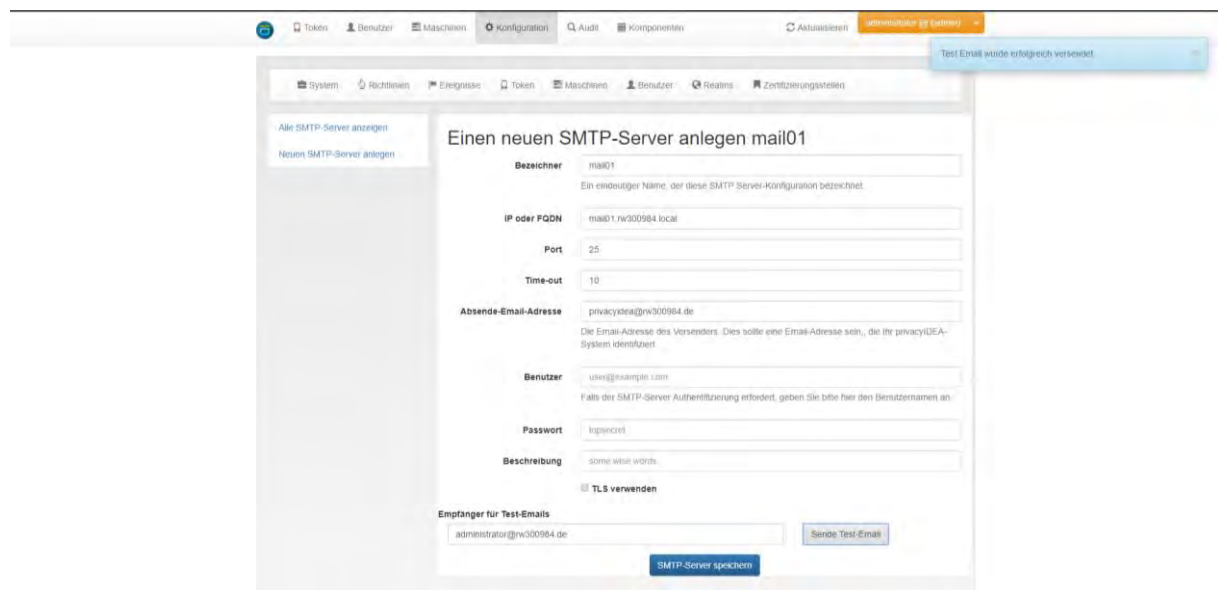
4.2. Hinzufügen eines SMTP Servers für Benachrichtigungen

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.



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 Emailadresse

Body: wie in unterem Screenshot gezeigt

Emailconfig: Ihr konfigurierter SMTP Server aus Kapitel 4, Abschnitt 2.

Reply to: frei definierbare Rückantwort Emailadresse

Subject: frei definierbar

Hinweis: Weitere Variablen finden Sie hier:

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

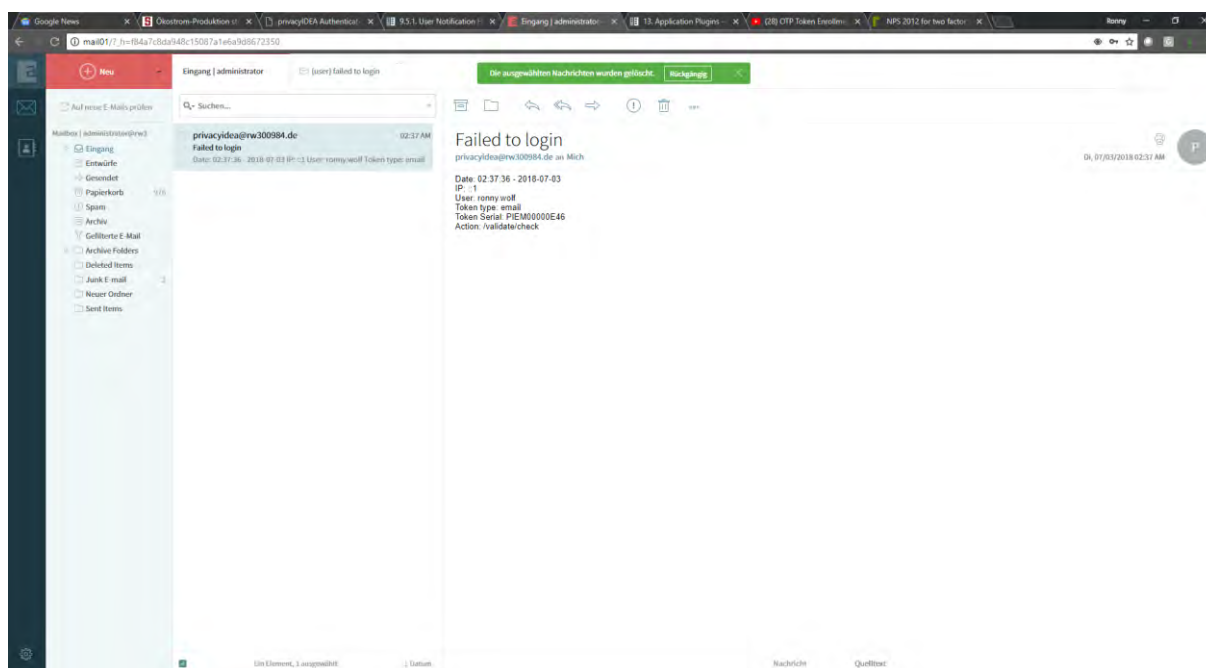
Speichern Sie nun das neue Ereignis ab.

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

Hierzu können wir direkt auf dem privacyIDEA Server mit folgendem Kommando 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)

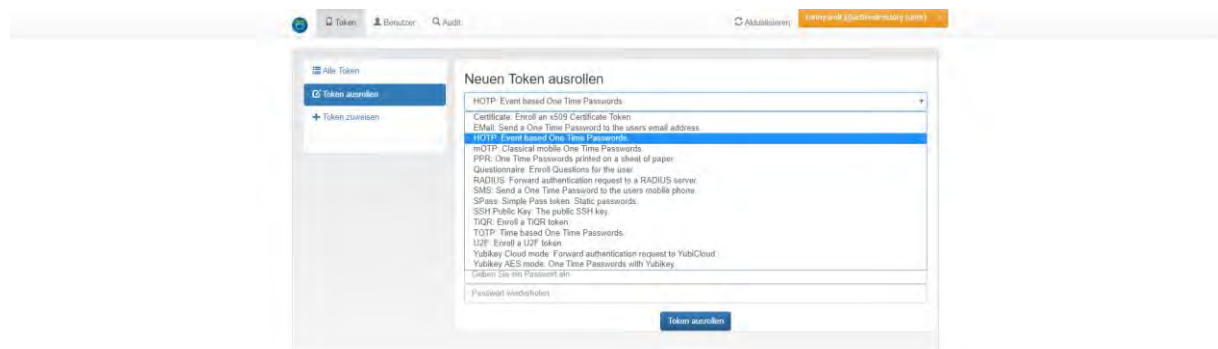
privacyIDEA hat sehr viele Möglichkeiten, die Anforderungen von Kunden zu erfüllen. Einen kleinen Teil von zusätzlichen Konfigurationen möchten wir Ihnen hier vorstellen.

5.1. Richtlinie für Self Enrollmet 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 authentifiziert wird.

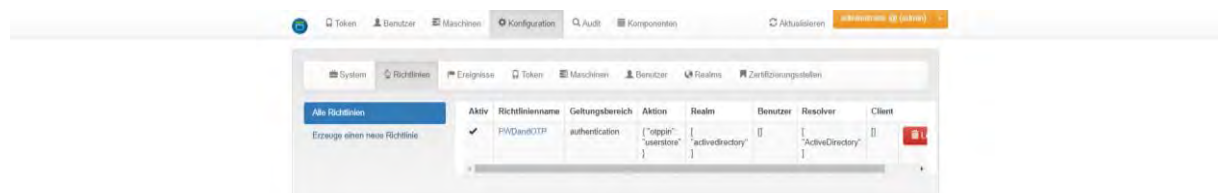
Dies dient einerseits der Übersicht für den Benutzer (Usability) und der Sicherheit (z.B. nur Hardware Token) und erleichtert die Verwaltung des Systems.

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



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 ist 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 Authentifizierungsmethode!

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 angegebenen Zeit eingeben ist die Eingabe ungültig.

The screenshot shows the 'Email-Token Einstellungen' (Email-Token Settings) page in the Yubico management console. The left sidebar contains a menu with options: System, Richtlinien, Ereignisse, Token, Maschienen, Benutzer, Reams, and Zertifizierungsstellen. The 'Token' menu is expanded, showing sub-options: HOTP, TOTP, U2F, RADIUS, Remote, SMS, TQR, Email (selected), Fragekatalog, Yubico, and Yubkey. The main content area is titled 'Email-Token Einstellungen' and includes a description: 'Der Email-Token ist ein Challenge-Response-Token, der - nachdem die richtige OTP-PIN eingegeben wurde - einen OTP-Wert an die hinterlegte E-Mail-Adresse sendet.' Below this, there is a section for 'SMTP-Server Konfiguration' with a dropdown menu showing 'mail01'. Another section, 'Gültigkeitszeitraum für OTP', has a text input field set to '300'. A 'Speichern' (Save) button is at the bottom right.

Speichern Sie diese Einstellungen ab.

Nun können wir einen Email Token unserem Benutzer zuweisen.

Klicken Sie hierzu auf Token – Token ausrollen

The screenshot shows the 'Neuen Token ausrollen' (Roll out new token) page. The left sidebar is the same as in the previous screenshot, but the 'Token' menu is expanded to show 'Token ausrollen' (selected), 'Token importieren', 'Challenges anzeigen', and 'Seriennummer bestimmen'. The main content area is titled 'Neuen Token ausrollen' and includes a dropdown menu for 'Email: Send a One Time Password to the users email address.' Below this, there is a section for 'Tokendaten' with a warning message: 'Damit Email-Token richtig funktionieren, müssen Sie die Email-Token Konfiguration setzen. Die Email-Adresse wird bei jeder Authentifizierung dynamisch aus der Benutzerquelle gelesen.' The 'Token einem Benutzer zuweisen' section has a 'Realm' dropdown set to 'activedirectory', a 'Benutzer' text input field with 'ronny.wolf', and a 'PIN' section with two masked input fields. An 'Erweiterte Attribute' section is also present. A 'Token ausrollen' button is at the bottom right.

Wählen Sie nun Email aus. Wählen einen Benutzer aus (bei Eingabe in das Textfeld erfolgt 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.

Neuen Token ausrollen

Email: Send a One Time Password to the users email address.

Der Email-Token sendet einen OTP-Wert an die Email-Adresse des Benutzers.

Tokenarten

Damit Email-Token richtig funktionieren, müssen Sie die Email-Token Konfiguration setzen.

☒ Die Email-Adresse wird bei jeder Authentifizierung dynamisch aus der Benutzerquelle gelesen.

Token einem Benutzer zuweisen

Realm

active directory

Benutzer

ronny wolf

PIN

Erweiterte Attribute

Token ausrollen

Der Email Token ist nun erstellt und dem Benutzer zugewiesen

Anzahl der Tokens: 1

Seriennummer	Typ	aktiv	Beschreibung	Fehlerzähler	Benutzer	Realm
PHEM00000E46	email	aktiv		0	ronny wolf	active directory

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.

Anmelden

Bitte geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich anzumelden.

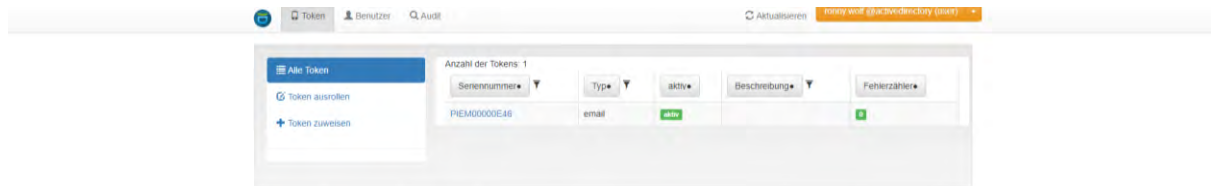
Anmelden

ronny wolf

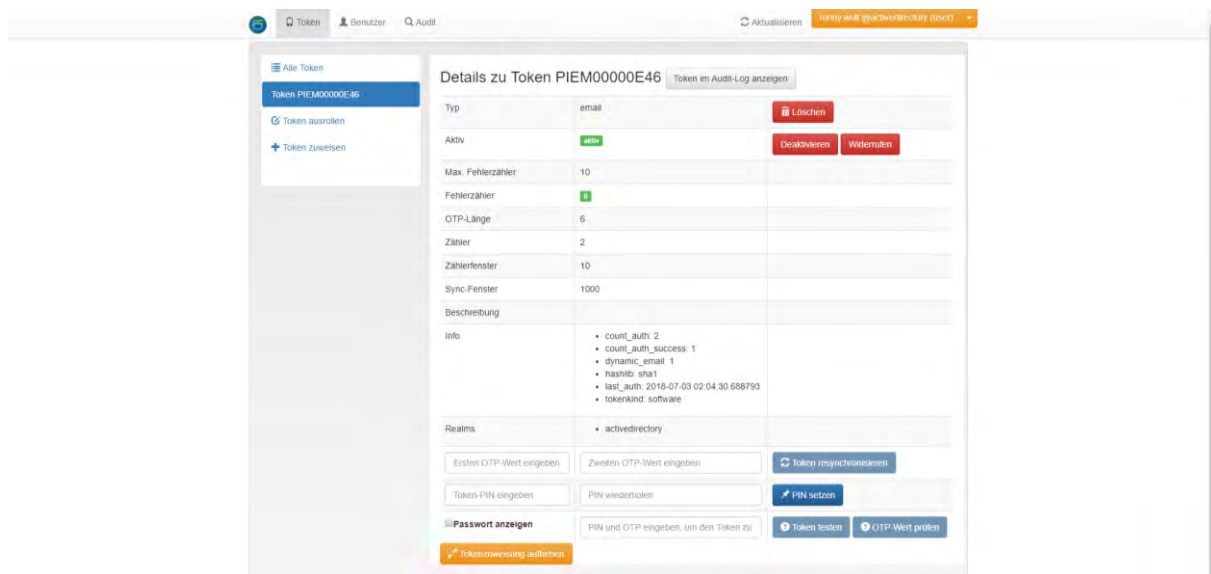
Passwort

Anmelden

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

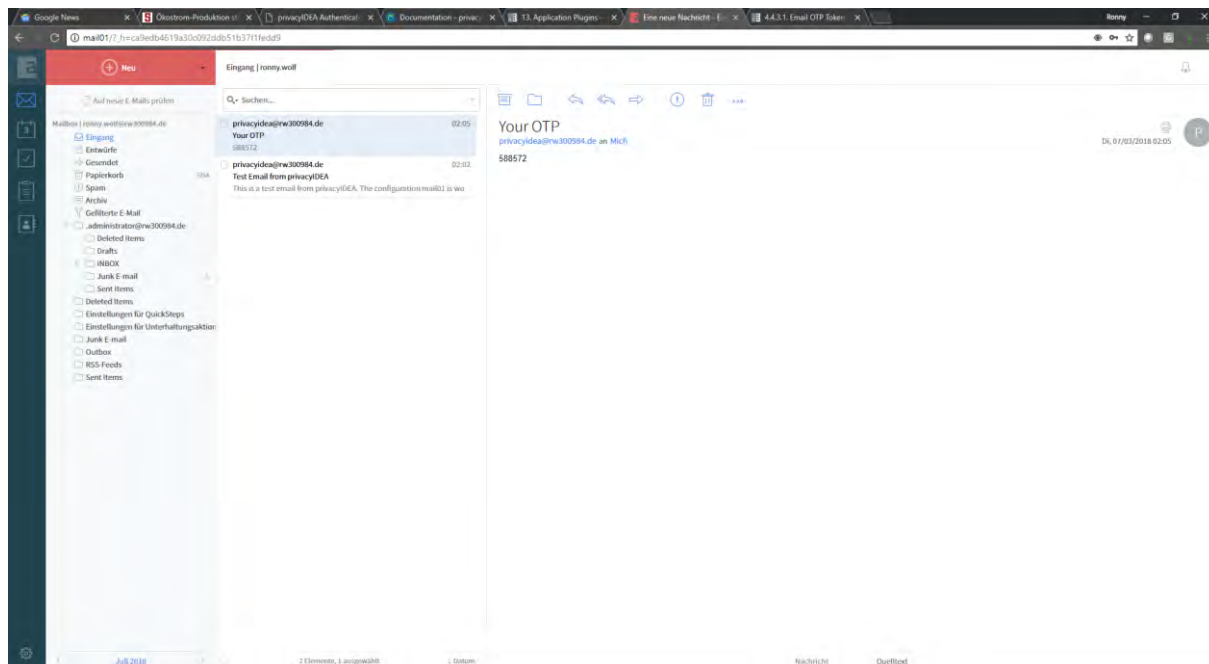


Anders als bei einem Hardware oder Software (z.B. Google Authenticator) basierten OTP, muss bei einem Email Token der erste Anmeldeversuch mit Active Directory Benutzer + Passwort erfolgen. Ist dies richtig eingegeben, sendet privacyIDEA über den Radius Server eine Rückantwort an den Client (z.B. Ihre 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 eingegeben 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 Benutzernamen und Passwort ein. Sie erhalten nun die Meldung „Enter the OTP from Email“.

The screenshot shows the Yubico web interface. On the left, there's a sidebar with 'Alle Token' and a list of tokens, including 'Token PIEM00000E46'. The main area displays 'Details zu Token PIEM00000E46'. The token is of type 'email' and is active. It has a maximum number of failed attempts of 10, a current failed attempt count of 0, an OTP length of 6, a counter of 3, a window size of 10, and a sync window of 1000. The description includes a list of attributes: count_auth: 2, count_auth_success: 1, dynamic_email: 1, hashlib: sha1, last_auth: 2016-07-03 02:04:30 668793, and tokenkind: software. The realms section shows 'activeDirectory'. At the bottom, there are input fields for 'Erster OTP-Wert eingeben', 'Zweiter OTP-Wert eingeben', 'Token-PIN eingeben', and 'PIN wiederholen', along with buttons for 'Token synchronisieren', 'PIN setzen', 'Token testen', and 'OTP-Wert prüfen'. A red notification banner at the top right says 'Enter the OTP from the 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 authentifizieren.

5.3. Überschreiben von Client IP Adresse 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 Authentifizierungsanfrage kommt.

Um dies zu umgehen, können Sie in den Einstellungen von privacyIDEA definieren, welche Quelladressen vom Radius Server/privacyIDEA überschrieben werden dürfen. Dadurch wird nicht die IP Adresse 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 autorisierenden Client, das Netz und/oder die lokale IP Adresse des FreeRadius Servers (in unserem Beispiel ist dies der 127.0.0.1 = IPv4 und ::1 = IPv6 an)

Speichern Sie diese Einstellung.

Bei zukünftigen Authentifizierungsanfragen sehen Sie nun die originäre Quelle.

Vorher:

Aktion	Erfolg	Aktionsdetail	Seriennummer	Token typ	Administrator	Benutzer	Realm	Resolver	Client	Info	Signatur	Fehler
POST /validate/check	0				administrator	administrator	defrealm	deflocal	-1	The user has no tokens assigned	OK	0
POST /validate/check	0				administrator	administrator	defrealm	deflocal	-1	The user has no tokens assigned	OK	0
POST /validate/check	0				administrator	administrator	defrealm	deflocal	-1	The user has no tokens assigned	OK	0

Nachher (mit neuen Einstellungen):

Aktion	Erfolg	Aktionsdetail	Seriennummer	Token typ	Administrator	Benutzer	Realm	Resolver	Client	Info
GET /resolver/	1				administrator				172.17.7.104	
GET /realm/	1				administrator				172.17.7.104	
GET /token/	1				administrator				172.17.7.104	realm: [\"*\"]
GET /realm/	1				administrator				172.17.7.104	
GET /realm/	1				administrator				172.17.7.104	
POST /auth	1				administrator				172.17.7.104	internal admin
GET /register	1								172.17.7.104	0
POST /validate/check	0		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	192.168.178.40	matchir 1 token
POST /validate/check	0		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	192.168.178.40	Enter the OTP from the Email: matchir 1 token
POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	192.168.178.40	matchir 1 token

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.

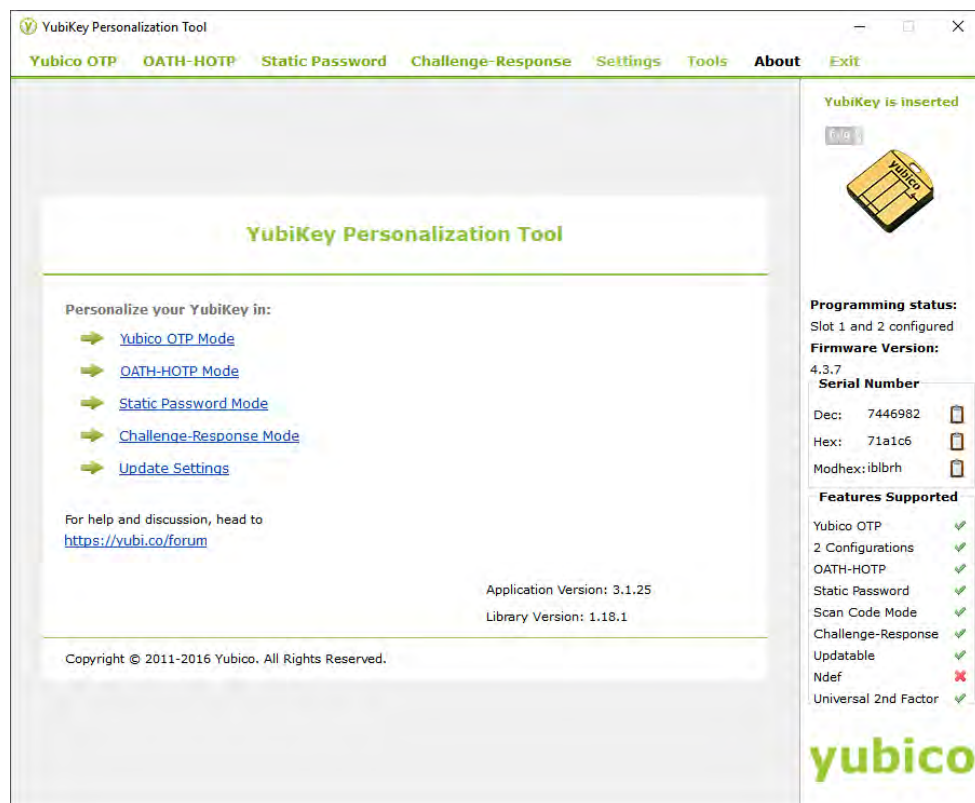
Weitere Informationen über die Möglichkeiten des Ausrollen von Yubikeys finden Sie hier:

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

6.1. Konfigurieren eines Yubikeys mit dem Yubico Personalization Tool

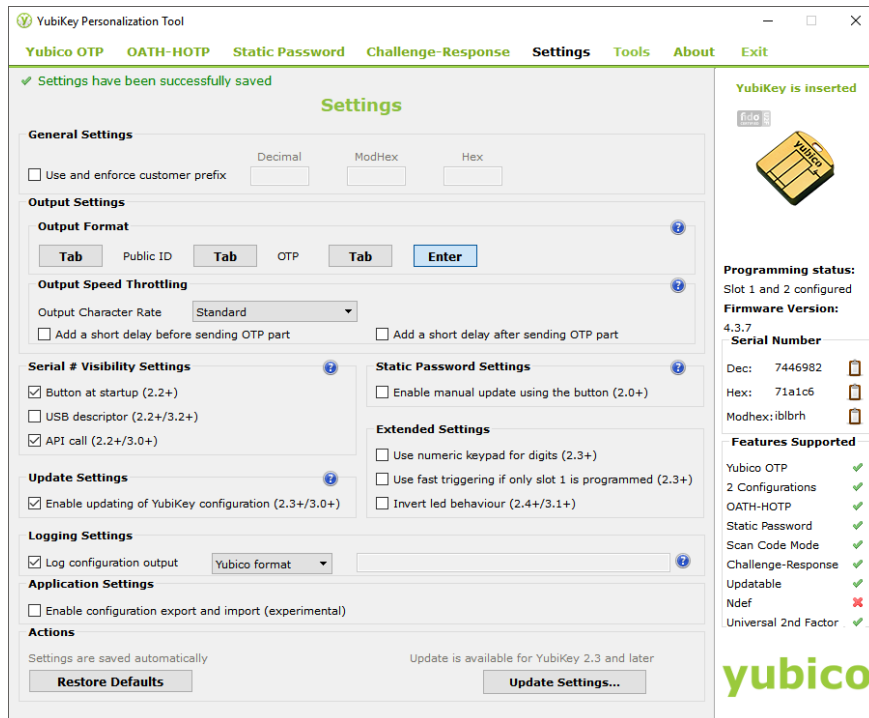
Alle Yubikeys unterstützen verschiedene OTP Protokolle (TOTP, HOTP und YubiOTP). In diesem Beispiel verwenden wir das Protokoll YubiOTP.

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

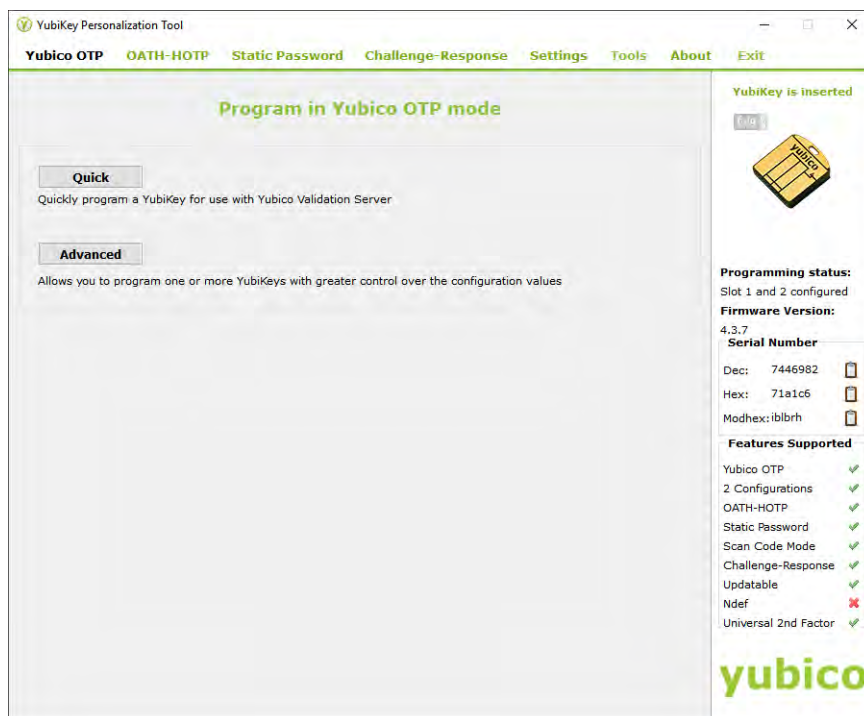


Klicken Sie nun auf Settings und konfigurieren Sie unter Logging Settings, folgendes:

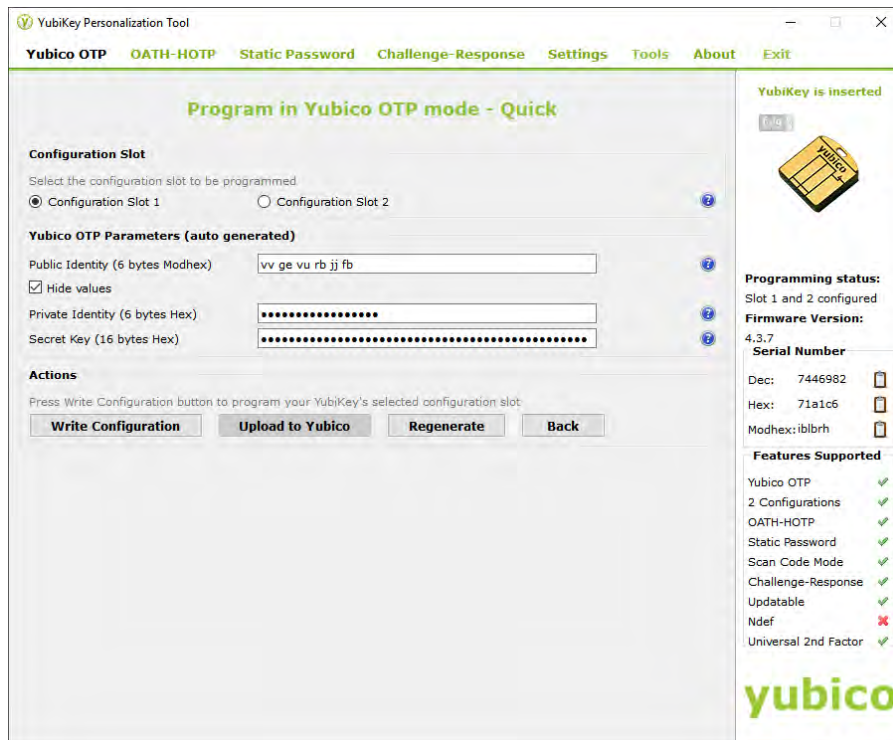
Log configuration output = aktiviert
Wert: Yubico Format



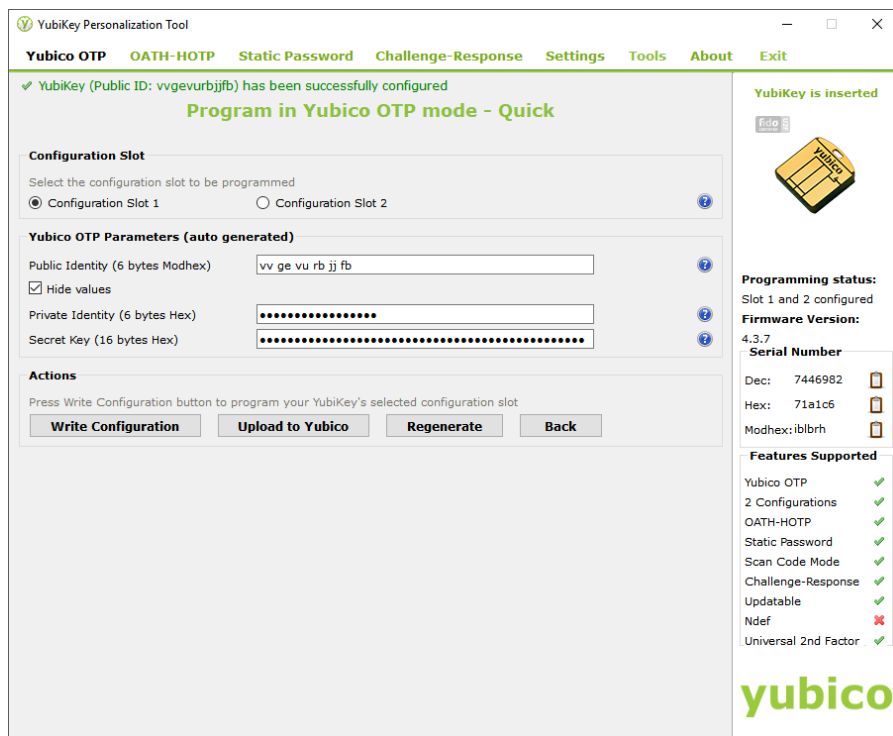
Klicken Sie nun auf Yubico OTP



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

Unbenannt - Editor

Datei Bearbeiten Format Ansicht ?

vvgevurbjffbritjtcfereujgurrv1chukrivkcrrvkn

Ihr Yubikey ist nun erfolgreich für PrivacyIDEA konfiguriert.

6.2. Ausrollen und zuweisen eines Yubikeys in privacyIDEA

Öffnen Sie nun das privacyIDEA Webinterface und klicken auf

The screenshot shows the 'Token' management interface in privacyIDEA. The top navigation bar includes 'Token', 'Benutzer', 'Maschinen', 'Konfiguration', 'Audit', and 'Komponenten'. The main content area shows a table of tokens. The table has columns for 'Seriennummer', 'Typ', 'aktiv', 'Beschreibung', 'Fehlerzähler', 'Benutzer', and 'Realm'. One token is listed: 'PIEM00000E46' with type 'email' and status 'aktiv'. The left sidebar contains a menu with 'Alle Token' and several actions: 'Token ausrollen', 'Token importieren', 'Challenges anzeigen', and 'Seriennummer bestimmen'.

Klicken Sie auf Token importieren

The screenshot shows the 'Tokendatei importieren' (Import token file) page in privacyIDEA. The page has a dropdown menu set to 'OATH CSV'. Below it, there is a text area for the PGP key, which contains 'PGP-Schlüssel 740E2E023969FDDE'. The 'Datei auswählen und importieren' button is visible at the bottom. The left sidebar is the same as in the previous screenshot.

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

Tokendatei importieren

Yubikey CSV

Hier können Sie eine CSV-Datei mit Yubikey-Token hochladen. Diese Datei enthält einen Token pro Zeile.

Wenn Sie den Yubikey im HOTP-Modus initialisieren, sollten Sie in neueren Yubikey-Personalisierungs-GUIs das PSKC-Dateiformat wählen.

Hier wählen Sie den Realm, in den die Token importiert werden. Sie können später die Realms der Token ändern.

activedirectory

PGP-Schlüssel 740E2E023969FDDE

Datei auswählen und importieren

Fortschritt: 100%
Hochgeladene Datei: YubiOTP.csv
Hochgeladene Token: 1

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

Anzahl der Tokens: 2

Seriennummer	Typ	aktiv	Beschreibung	Fehlerzähler	Benutzer	Realm
PIEM00000E46	email	aktiv		0	ronny.wolf	activedirectory
UBAM7446982_X	yubikey	aktiv	vvgevurbijfb	0		

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

The screenshot shows the Yubico Admin Console interface. The left sidebar contains navigation links: 'Alle Token', 'Token UBAM7446982_X', 'Token ausrollen', 'Token importieren', 'Challenges anzeigen', 'Verlorener Token', and 'Seriennummer bestimmen'. The main content area is titled 'Details zu Token UBAM7446982_X' and includes a 'Token im Audit-Log anzeigen' link. The token details are as follows:

Typ	yubikey	Löschen
Aktiv	aktiv	Deaktivieren, Widerrufen
Max. Fehlerzähler	10	Bearbeiten
Fehlerzähler	0	
OTP-Länge	44	
Zähler	0	
Zählerfenster	10	Bearbeiten
Sync-Fenster	1000	Bearbeiten
Beschreibung	vvgeurbjftb	Bearbeiten
Info	• tokenkind: hardware	Bearbeiten
Realms	• activedirectory	Bearbeiten

Below the details, there are input fields for 'Ersten OTP-Wert eingeben', 'Zweiten OTP-Wert eingeben', 'Token-PIN eingeben', and 'PIN wiederholen'. There are also buttons for 'Token resynchronisieren', 'PIN setzen', 'Token testen', and 'OTP-Wert prüfen'. A 'Passwort anzeigen' checkbox is present. The 'Benutzer zuweisen' section includes a 'Realm' dropdown menu, a 'Benutzer' input field, and a 'PIN' input field. The 'Benutzer' field contains the text: 'Fangen Sie an, einen Benutzernamen zu tippen.' The 'PIN' field contains the text: 'Geben Sie ein Passwort ein.' and 'Passwort wiederholen'.

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

The screenshot shows the Yubico Admin Console interface with the 'Benutzer zuweisen' form filled out. The 'Realm' dropdown is set to 'activedirectory'. The 'Benutzer' field contains the text: '[3ede0b5e-436b-46f8-f7ba-e00b30446352] ronny.wolf (Ronny Wolf)'. The 'PIN' field is empty. The 'Benutzer zuweisen' button is visible at the bottom.

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

Details zu Token UBAM7446982_X

Typ	yubikey	Löschen
Aktiv	aktiv	Deaktivieren Widerrufen
Max. Fehlerzähler	10	Bearbeiten
Fehlerzähler	0	
OTP-Länge	44	
Zähler	0	
Zählerfenster	10	Bearbeiten
Sync-Fenster	1000	Bearbeiten
Beschreibung	vvgevvubjfb	Bearbeiten
Info	tokenkind: hardware	Bearbeiten
Realms	activedirectory	Bearbeiten

Ersten OTP-Wert eingeben: Zweiten OTP-Wert eingeben:

Token-PIN eingeben: PIN wiederholen:

☒ Passwort anzeigen: Yubico@2018vvgevvubjfbttuuu

[Token resynchronisieren](#) [PIN setzen](#) [Token testen](#) [OTP-Wert prüfen](#)

Klicken Sie nun auf Token testen

Details zu Token UBAM7446982_X

Typ	yubikey	Löschen
Aktiv	aktiv	Deaktivieren Widerrufen
Max. Fehlerzähler	10	Bearbeiten
Fehlerzähler	0	
OTP-Länge	44	
Zähler	258	
Zählerfenster	10	Bearbeiten
Sync-Fenster	1000	Bearbeiten
Beschreibung	vvgevvubjfb	Bearbeiten
Info	- count_auth: 1 - count_auth_success: 1 - last_auth: 2018-07-17 16:18:02.575458 - tokenkind: hardware - yubico.prefix: vvgevvubjfb - yubico.tokenid: 627559e0511	Bearbeiten
Realms	activedirectory	Bearbeiten

Ersten OTP-Wert eingeben: Zweiten OTP-Wert eingeben:

Token-PIN eingeben: PIN wiederholen:

☒ Passwort anzeigen: Yubico@2018vvgevvubjfbttuuu

[Token resynchronisieren](#) [PIN setzen](#) [Token testen](#) [OTP-Wert prüfen](#)

Erfolgreich authentisiert

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

Details zu Token UBAM7446982_X

Typ	yubikey	Löschen
Aktiv	aktiv	Deaktivieren Widerrufen
Max. Fehlerzähler	10	Bearbeiten
Fehlerzähler	1	Fehlerzähler zurücksetzen

wrong otp value

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

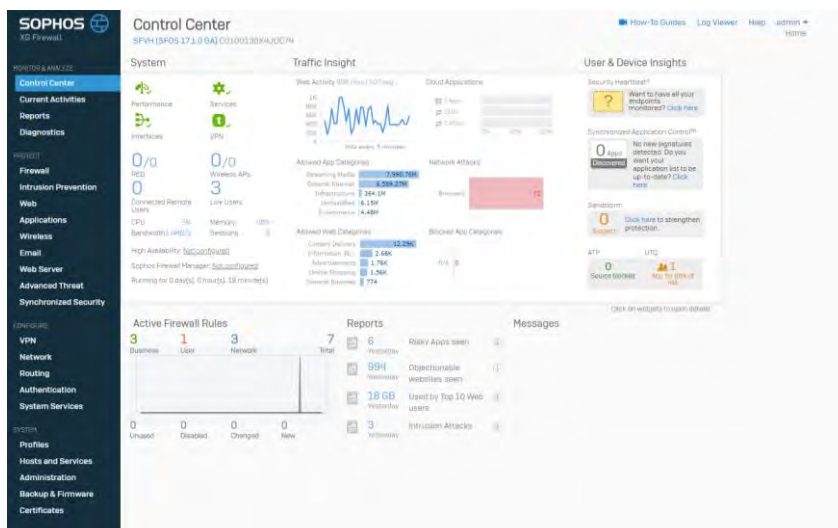
Die Firewalls von der Firma Sophos bieten verschieden Möglichkeiten eine Zwei Faktor Authentifizierung durchzuführen. Hierbei gibt es die Variante TOTP, welche ohne zusätzliches Authentifizierungs Backend funktioniert, als auch die Anbindung an einen Radius Server. Im Guide verwenden wir Version 17.x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

7.1.1. Konfigurieren der Radius Anbindung

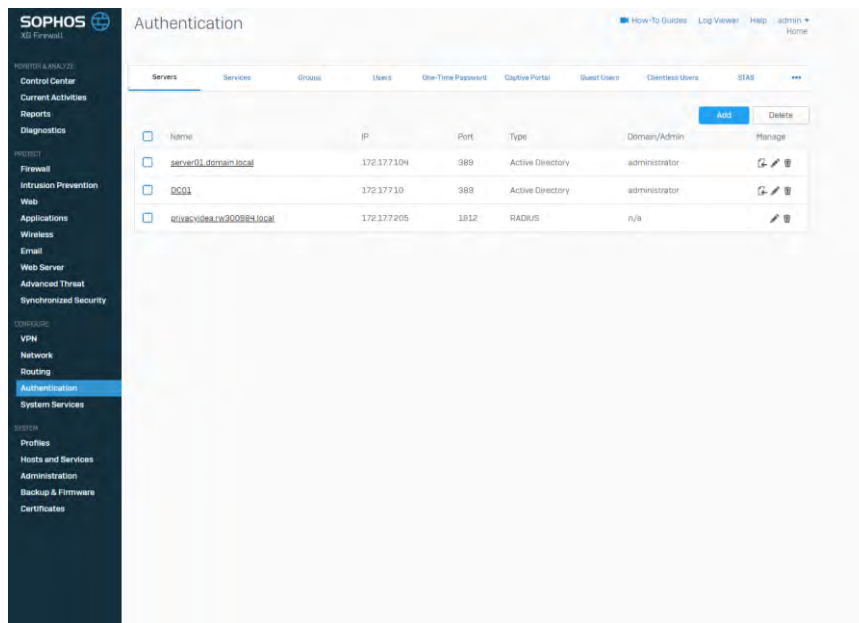
Melden Sie sich an Ihrer Sophos XG Appliance als Administrator an.



Nach erfolgreicher Anmeldung, klicken auf Configure -> Authentication



Klicken Sie nun auf „Add“

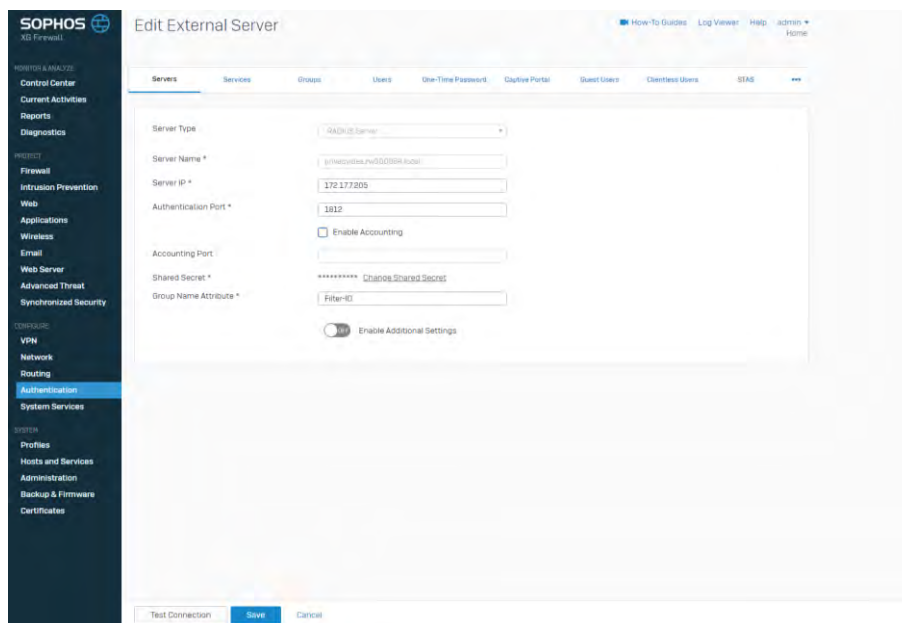


Definieren Sie wie im unteren Screenshot gezeigt die Radius Server Anbindung.

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

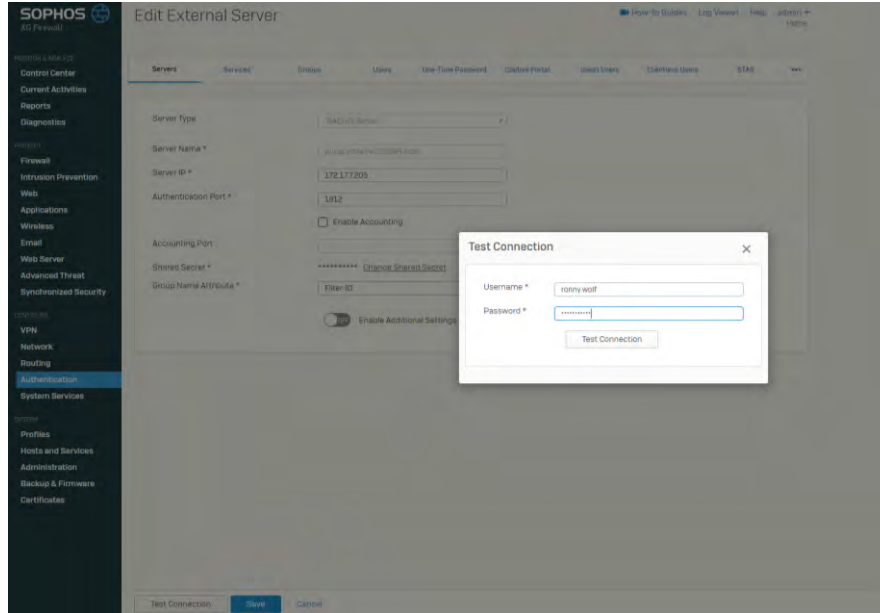


Testen Sie nun die Radius Authentifizierung mit einem Benutzer der einen Yubikey zugewiesen hat

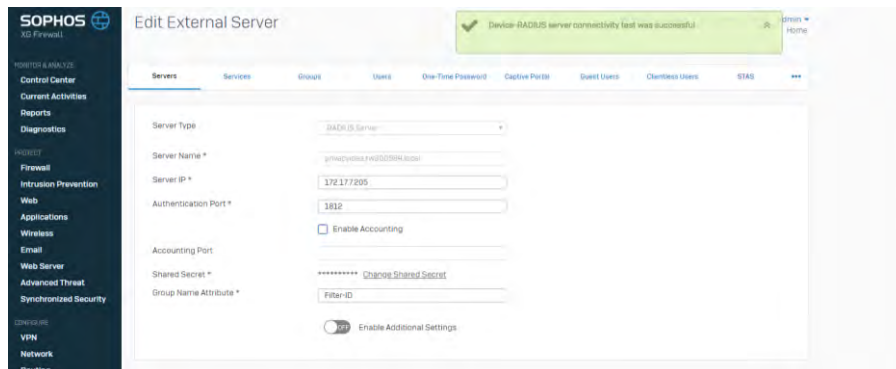
In unserem Beispiel:

Username: ronny.wolf

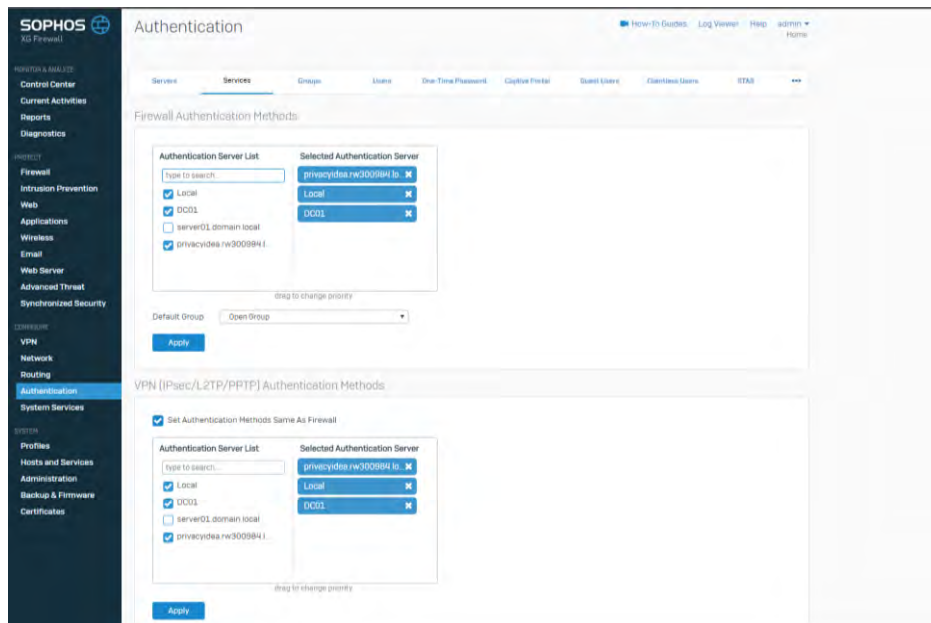
Password: Active Directory Passwort + Yubikey OTP



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



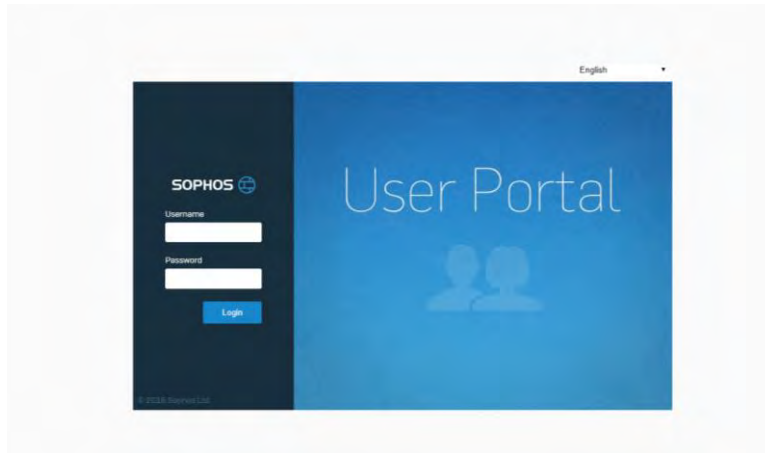
Nun müssen Sie die Radius Authentifizierung, den unterschiedlichen Dienste (VPN, User Portal...) der Sophos XG zuweisen.



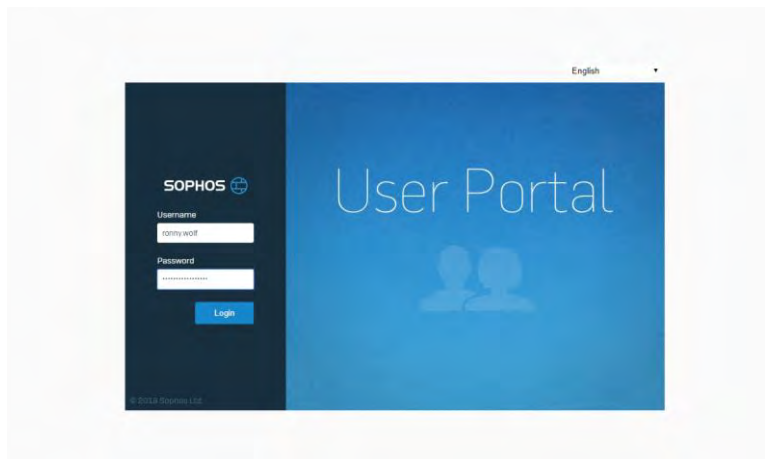
Hinweis: Sollten Sie weitere Authentifizierungsbackends in Ihrer Sophos XG definiert haben, empfehlen wir die Reihenfolge (Drag & Drop) zu ändern, damit der privacyIDEA Server als erste Quelle angegeben ist.

7.1.2. Anmelden an User Portal mit Yubikey

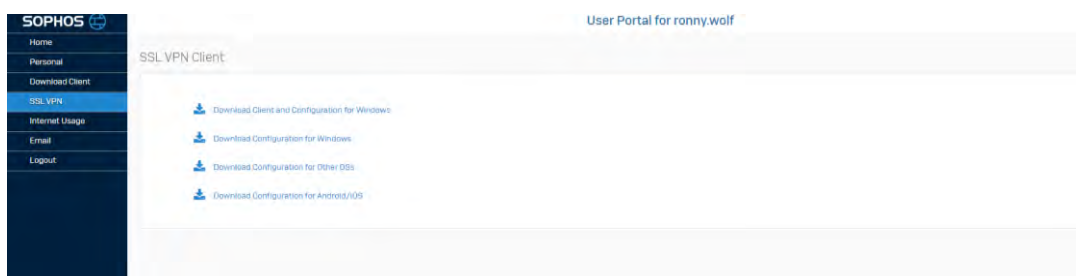
Öffnen Sie nun das User Portal der Sophos XG (Webinterface)



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

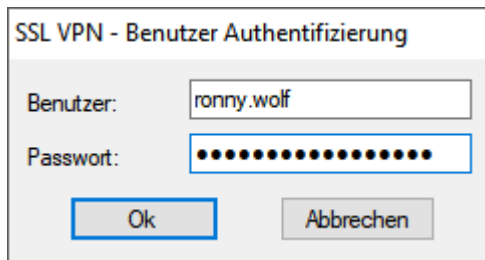


War die Anmeldung erfolgreich, sehen Sie nun das User Portal des Benutzers



7.1.3. Anmelden via SSLVPN mit Yubikey

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

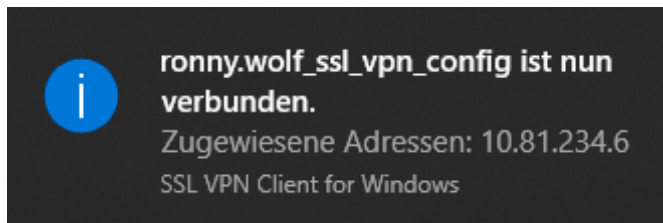


SSL VPN - Benutzer Authentifizierung

Benutzer:

Passwort:

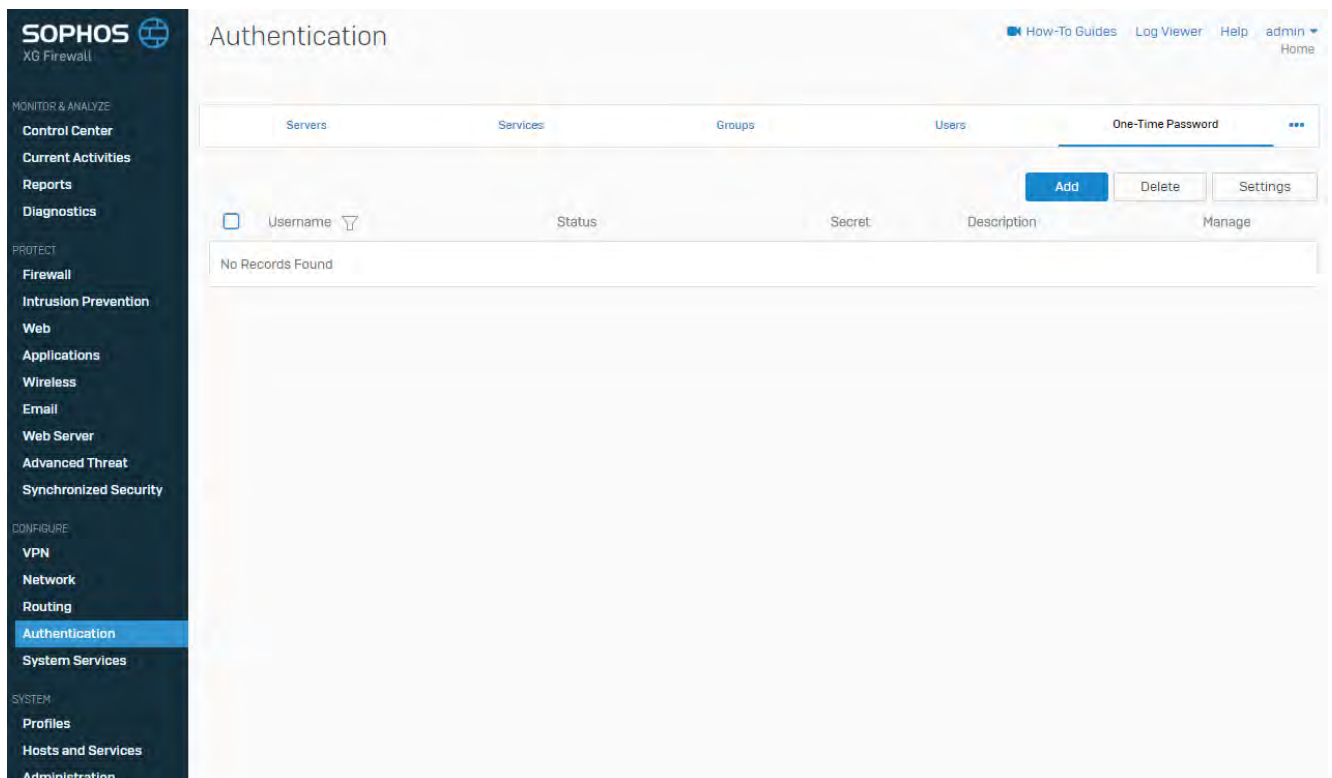
War die Anmeldung erfolgreich, wird eine VPN Verbindung aufgebaut.



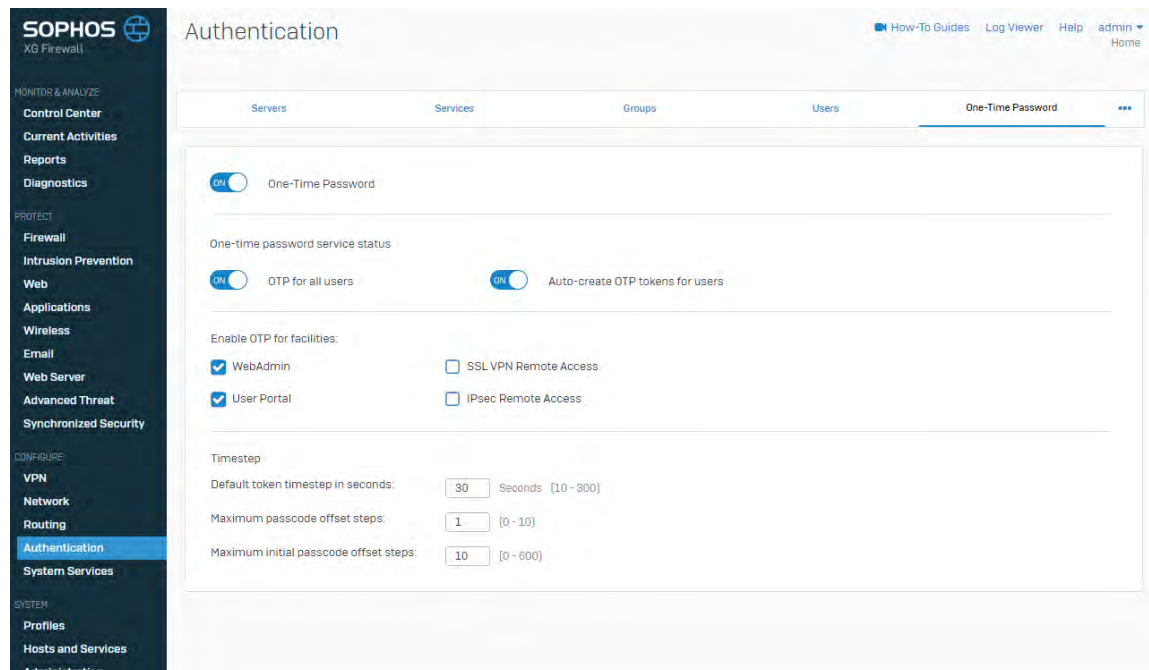
7.1.4. Zeitbasiertes One Time Password

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

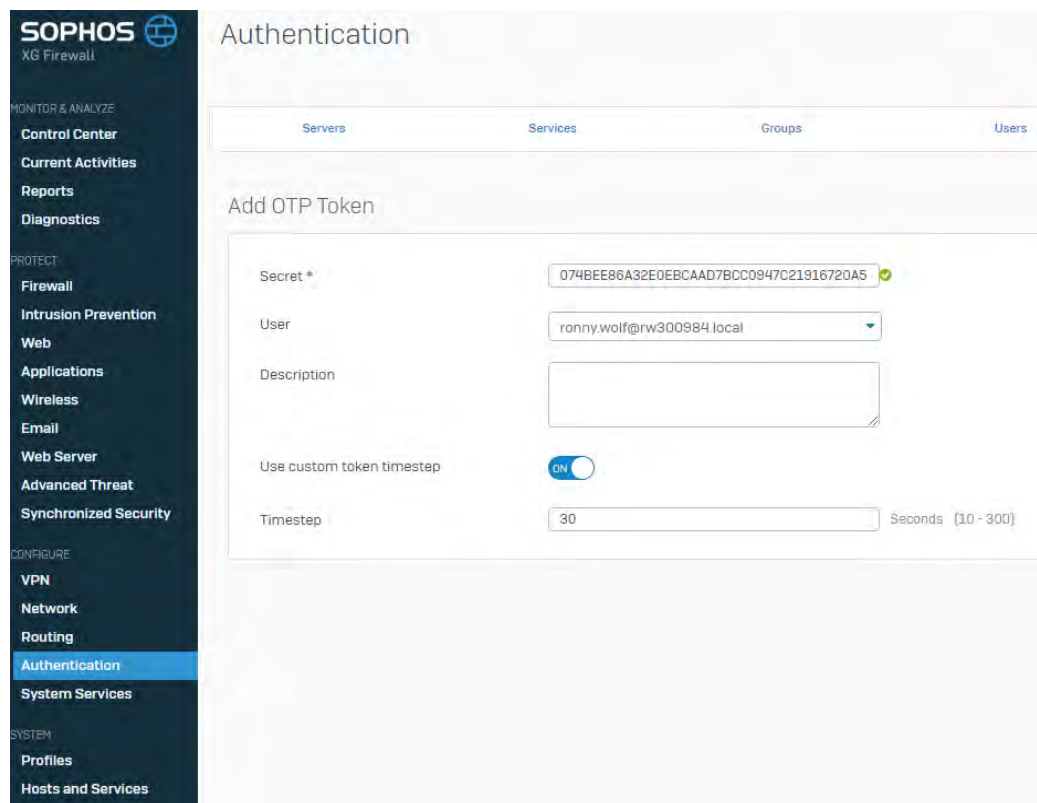


Klicken Sie nun auf Add und geben folgende Parameter ein:

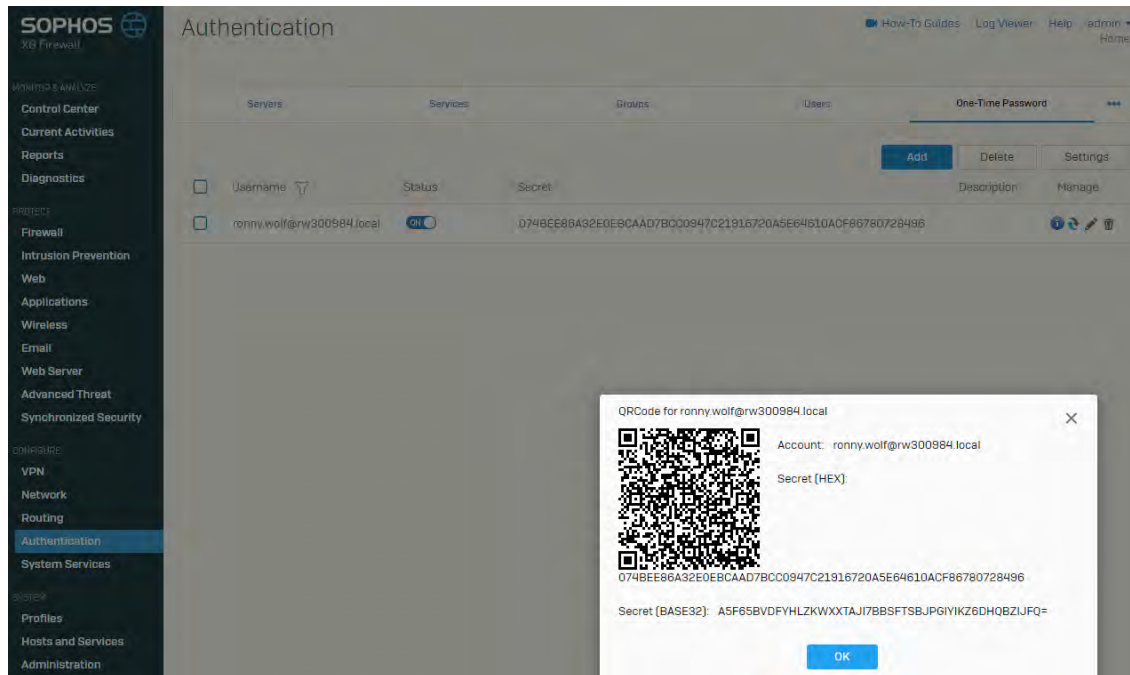
Secret: Zufälliges Secret in HEX Format mit min. 32 Zeichen (z.B. Sie können Sie hier ein random Hex Wert generieren: http://rumkin.com/tools/password/pass_gen.php)

User: Benutzer welche auf der Sophos XG vorhanden ist

Custom timestamp: 30 Sekunden

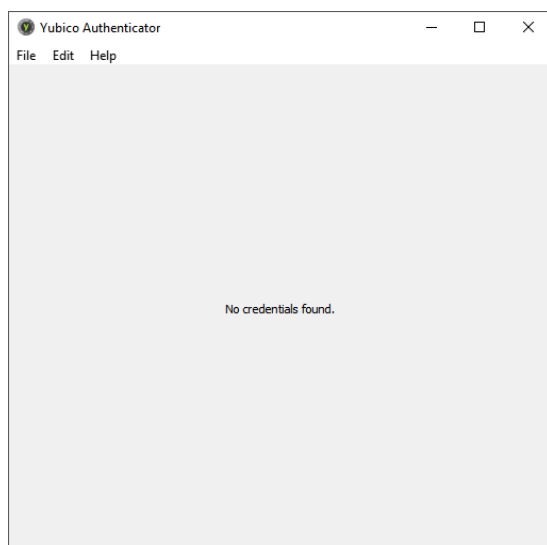


Klicken Sie nun auf das Ausrufezeichen (!) neben dem generierten TOTP Token um einen QR Code zu generieren

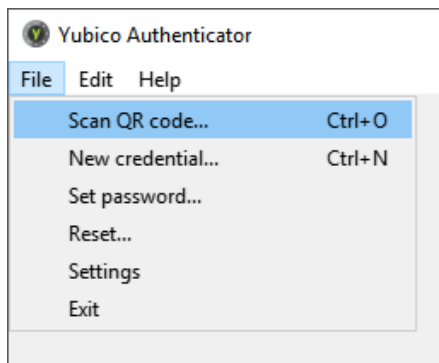


Lassen Sie nun dieses Fenster (mit QR Code sichtbar) geöffnet und öffnen den Yubico Authenticator

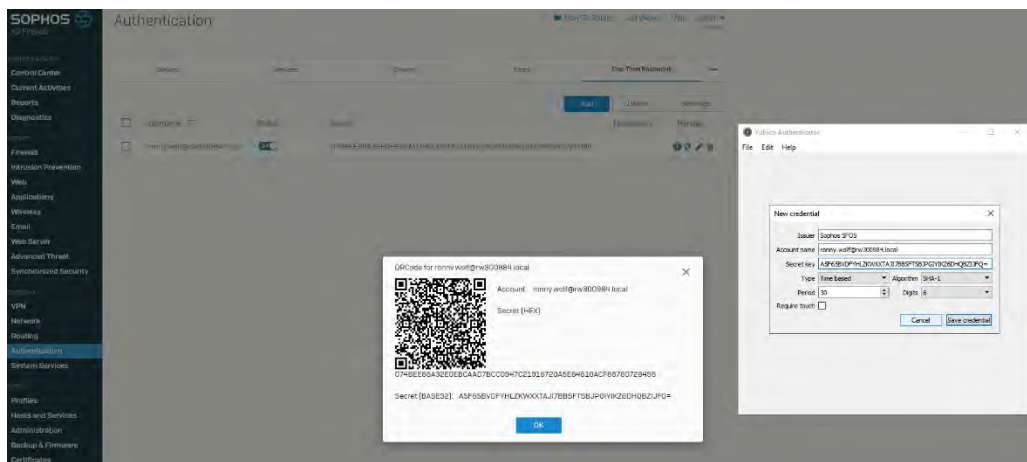
Download: (<https://www.yubico.com/products/services-software/download/yubico-authenticator/>)



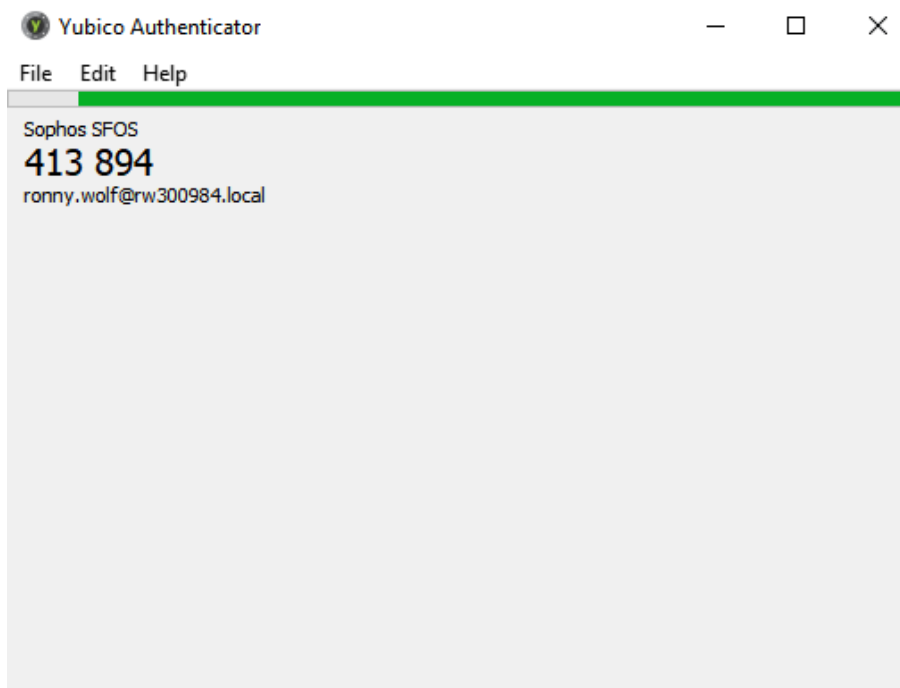
Klicken Sie auf File – Scan QR Code



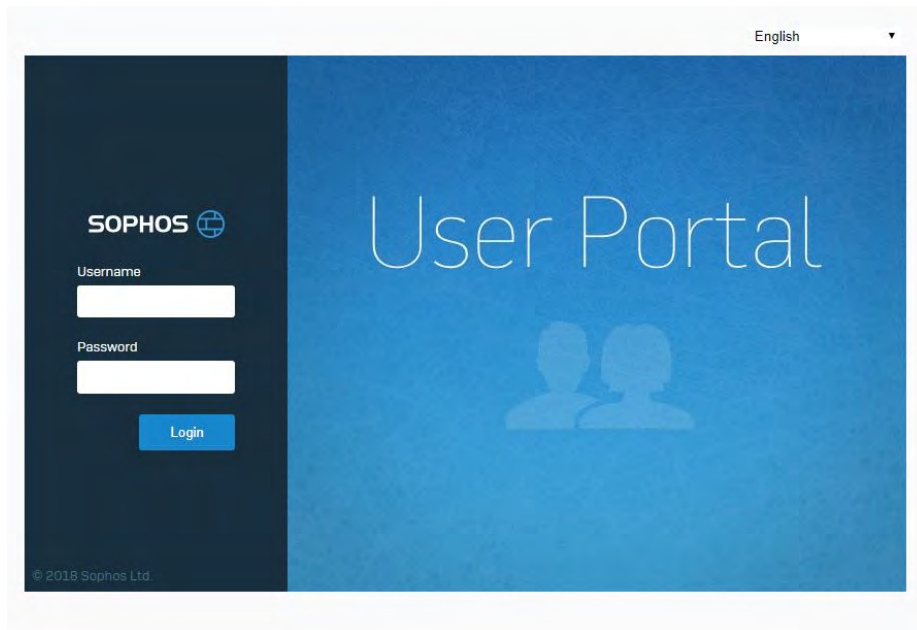
Nun wird automatisch das Secret erfasst:



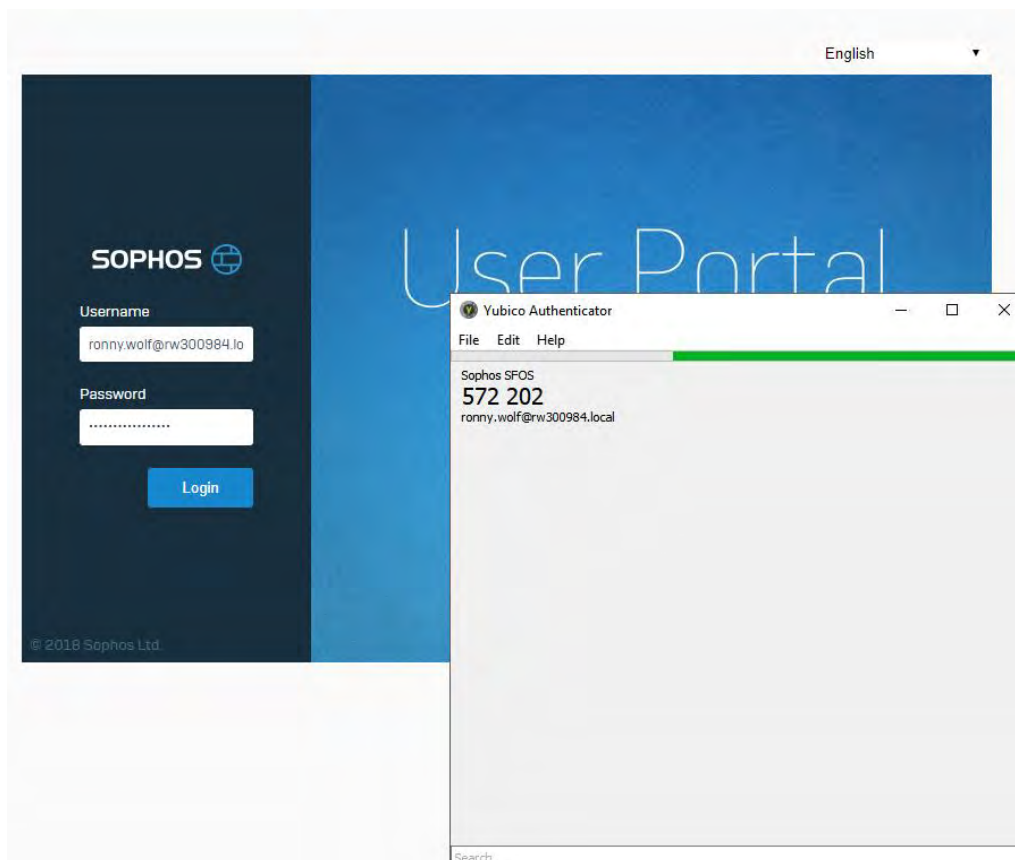
Speichern Sie die Credentials nun ab. Nun wird automatisch (solange der Yubico Authenticator geöffnet ist) ein zeitbasierter OTP generiert



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



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



Sie sind nun erfolgreich am User Portal angemeldet

SOPHOS 

Home

Personal

Download Client

SSL VPN

Internet Usage

Email

Logout

User Portal for ronny.wolf@rw300984.local

SSL VPN Client

 Download Client and Configuration for Windows

 Download Configuration for Windows

 Download Configuration for Other OSs

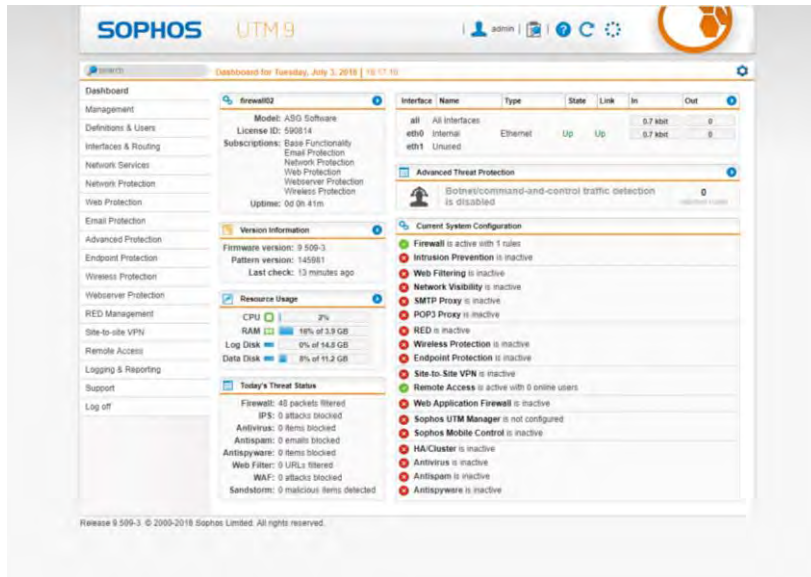
 Download Configuration for Android/iOS

7.2. Sophos UTM Firewall mit Radius

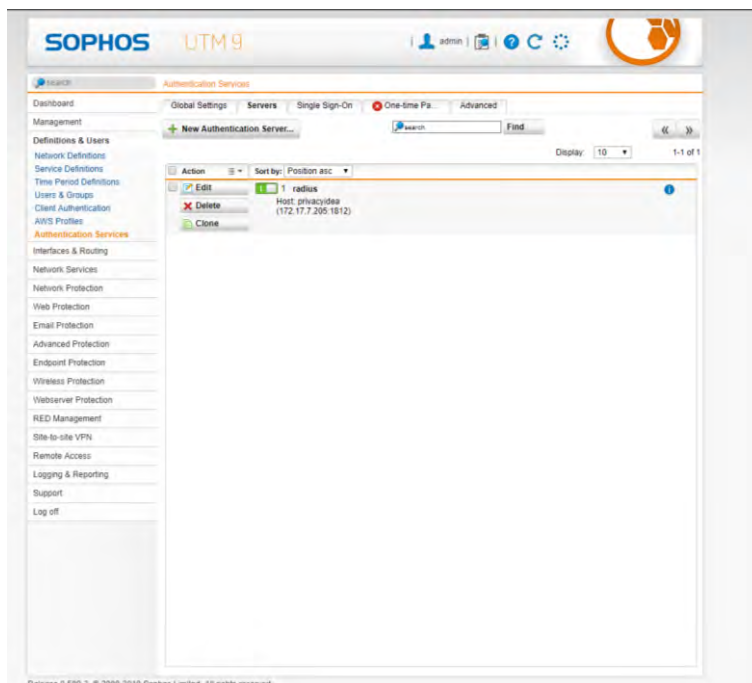
Der Sicherheitshersteller Sophos bietet noch eine weitere Firewall Lösung. In unserem Guide verwenden wir die Version 9.3xx. Auch hier gibt es verschiedene Möglichkeiten Benutzer zu authentifizieren.

7.2.1. Konfigurieren der Radius Anbindung

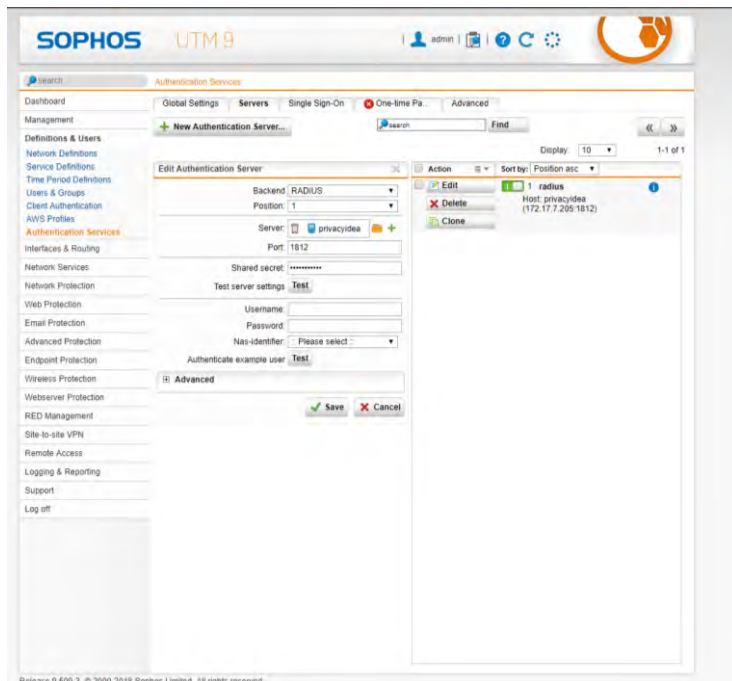
Als erstes konfigurieren wir die Radius Anbindung, so dass eine Kommunikation mit dem privacyIDEA Server möglich ist. Hierzu melden Sie sich am Sophos Webinterface als Administrator an.



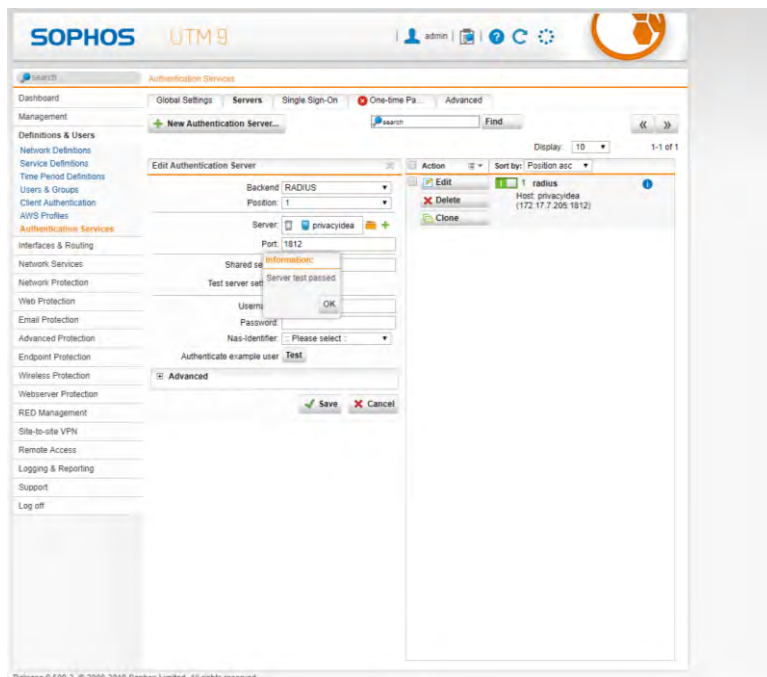
Klicken Sie nun auf Definitions & Users – Authentication Services



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.



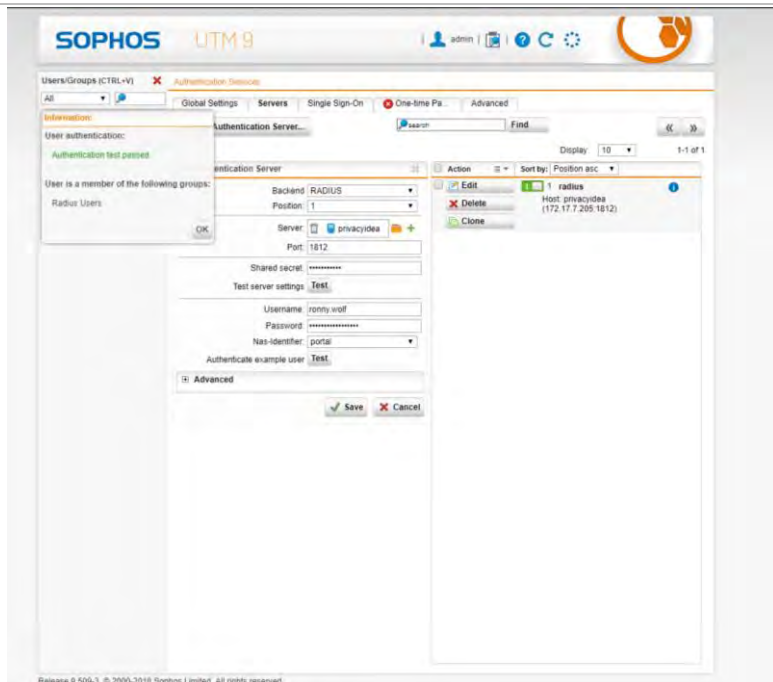
Bevor Sie fortfahren testen Sie die Verbindung zum Radius Server



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

Username: Active Directory Benutzer

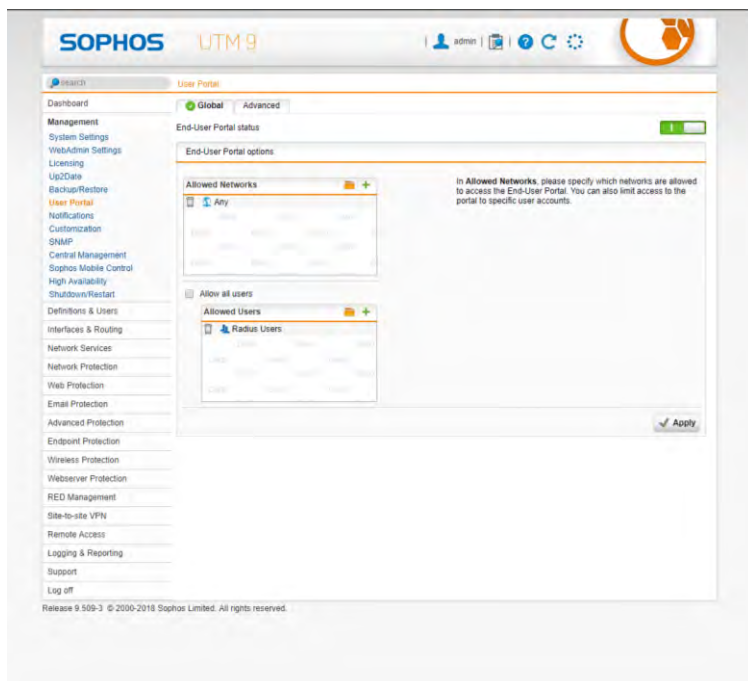
Password: Active Directory Passwort + Yubikey OTP



Die Radius Server Konfiguration ist nun abgeschlossen.

7.2.2. Anmelden an User Portal mit Yubikey

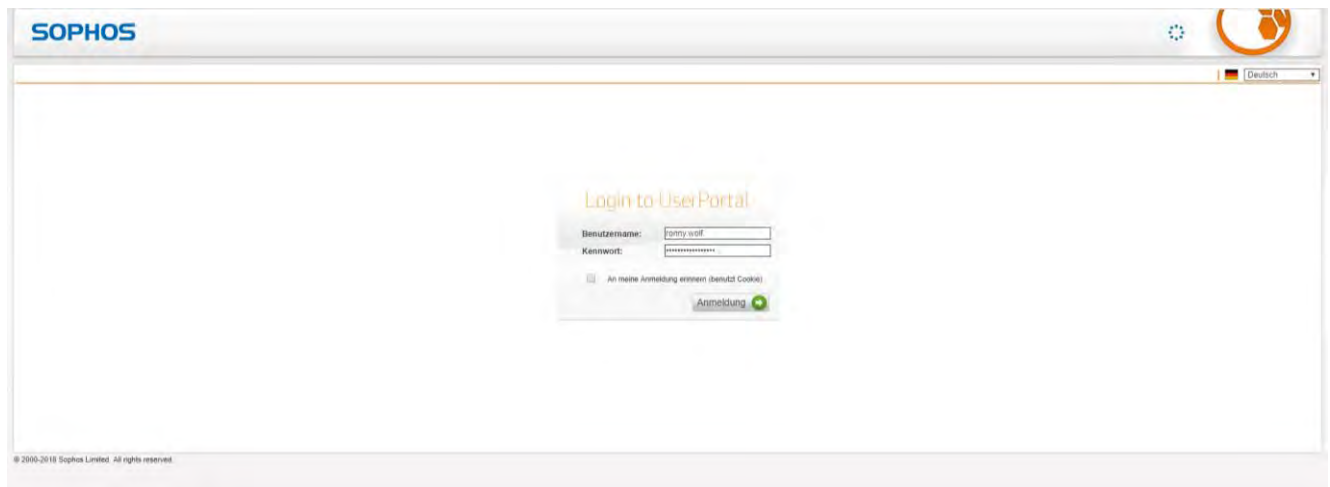
Damit Benutzer sich am User Portal der Sophos UTM mit den Radius Anmeldedaten authentifizieren können, müssen Sie die Gruppe Radius Uses, unter Management – User Portal – Global hinzufügen



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

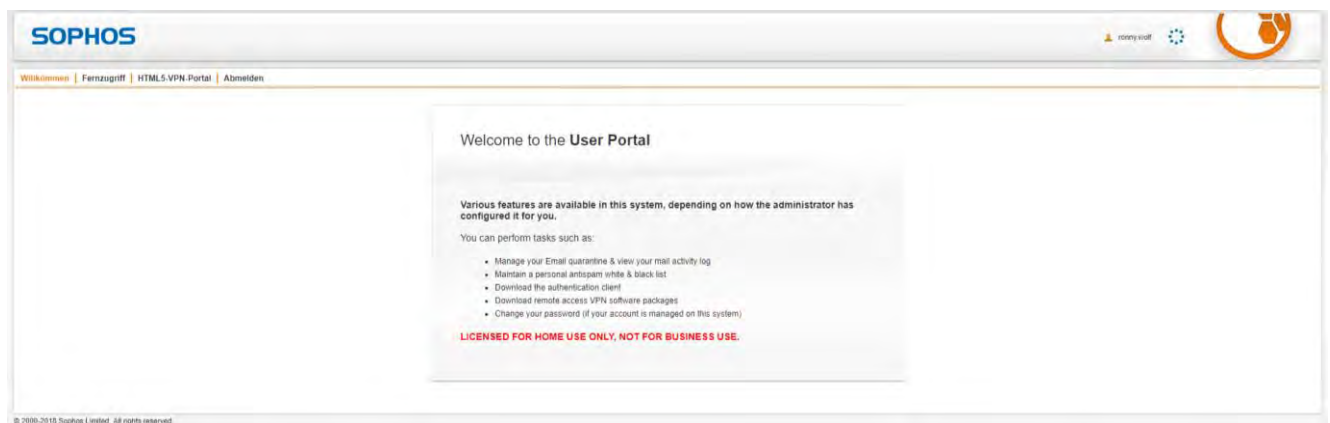
Benutzername: Active Directory Benutzer mit Yubikey zugewiesen

Passwort: Active Directory Passwort + Yubikey OTP



The screenshot shows the Sophos User Portal login interface. At the top, the 'SOPHOS' logo is on the left, and a language dropdown menu is on the right, currently set to 'Deutsch'. The main content area is titled 'Login to User Portal' and contains a login form with fields for 'Benutzername:' (username) and 'Kennwort:' (password). Below the password field is a checkbox labeled 'An meine Anmeldung erinnern (benutzt Cookies)'. A green 'Anmeldung' button with a key icon is at the bottom right of the form. The footer of the page reads '© 2000-2018 Sophos Limited. All rights reserved.'

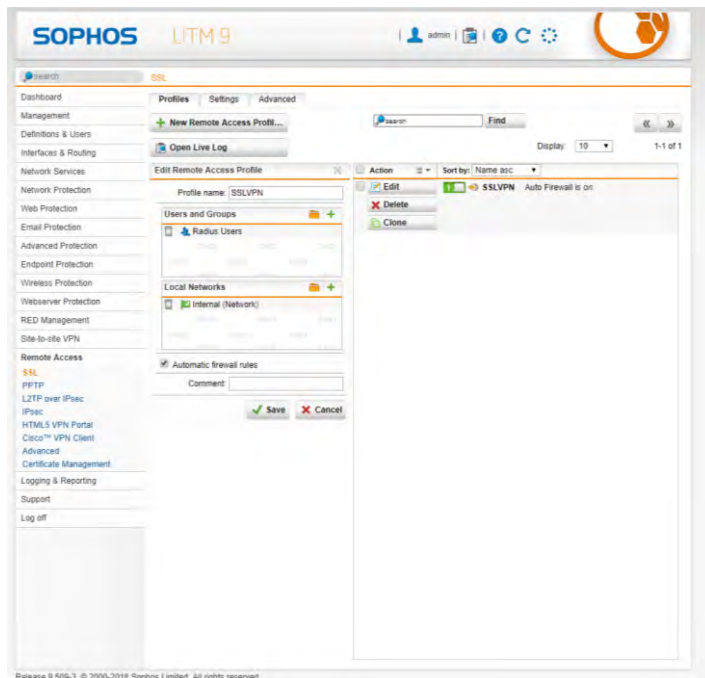
Sie sind nun erfolgreich am User Portal der Sophos UTM angemeldet



The screenshot shows the Sophos User Portal welcome page. At the top, the 'SOPHOS' logo is on the left, and a user profile icon labeled 'johannes.wolf' is on the right. Below the logo is a navigation bar with links: 'Willkommen', 'Fernzugriff', 'HTML5-VPN-Portal', and 'Abmelden'. The main content area is titled 'Welcome to the User Portal' and contains a list of features available in the system. The features are: 'Manage your Email quarantine & view your mail activity log', 'Maintain a personal antispam white & black list', 'Download the authentication client', 'Download remote access VPN software packages', and 'Change your password (if your account is managed on this system)'. Below the list is a red warning: 'LICENSED FOR HOME USE ONLY, NOT FOR BUSINESS USE.'. The footer of the page reads '© 2000-2018 Sophos Limited. All rights reserved.'

7.2.3. Anmelden via SSLVPN mit Yubikey

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



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

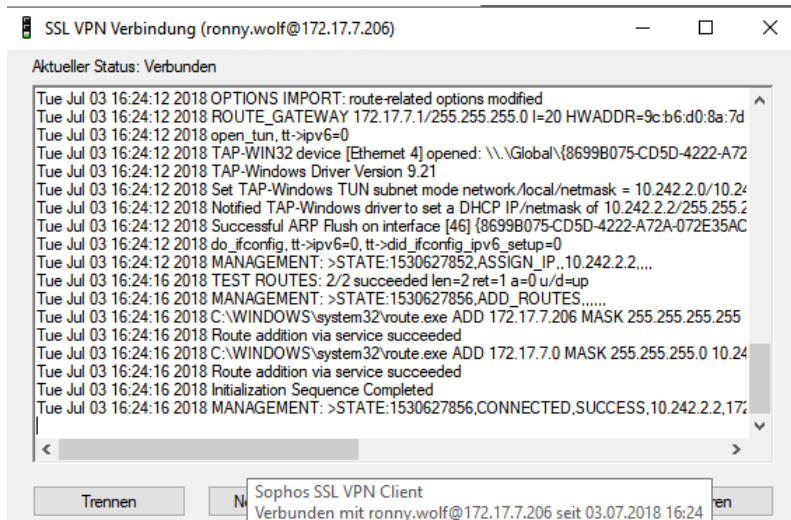
Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
Passwort: Active Directory Passwort + Yubikey OTP

SSL VPN - Benutzer Authentifizierung

Benutzer:

Passwort:

Sie sind nun erfolgreich via SSL VPN verbunden.



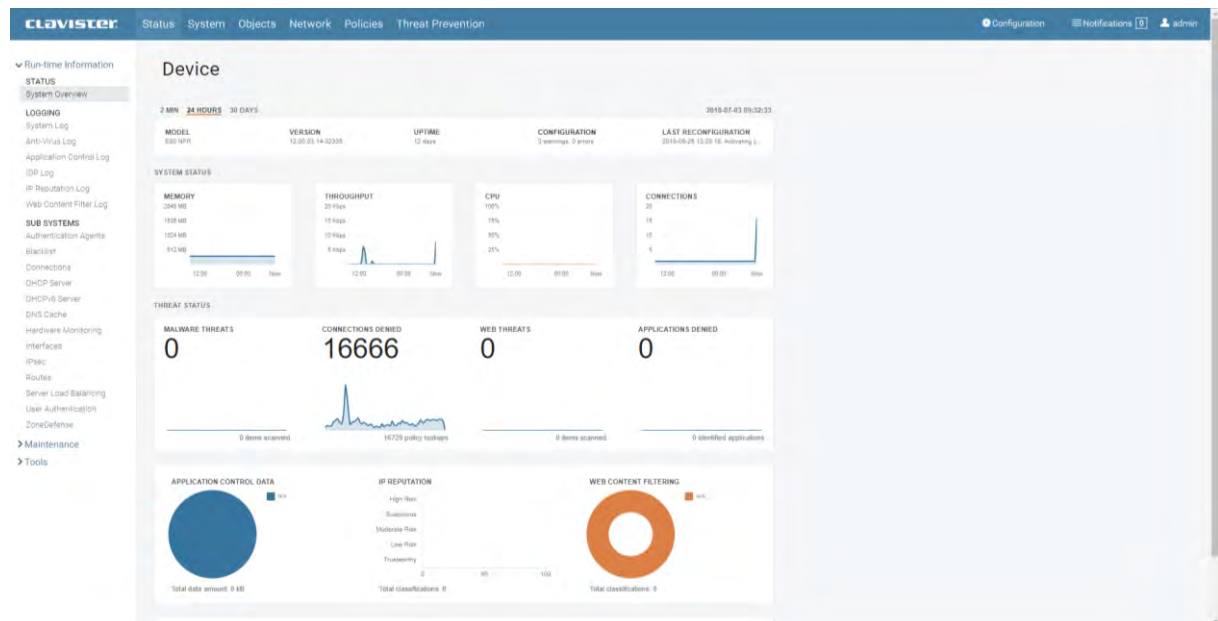
7.3. Clavister Firewall mit Radius

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

Getestet 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

The screenshot shows the 'Address Book' configuration page in the Clavister Firewall web interface. The page title is 'Address Book' and it includes a description: 'The Address Book contains symbolic names for various types of addresses, including IP networks and Ethernet MAC addresses.' There is a 'Filter' input field and a table with columns: '#', 'Name', 'Address', 'User Auth Groups', and 'Comments'. The table contains 11 entries, including 'InterfaceAddresses', 'all-nets', 'all-mbld', 'localhost', 'VMWare_Gateway', 'DNS1', 'DNS2', 'my_address', 'Radius_Server', and 'VPNPool'. A note at the bottom right says 'Right-click on a row for additional options.'

#	Name	Address	User Auth Groups	Comments
1	InterfaceAddresses			
2	all-nets	0.0.0.0/0		All possible networks
3	all-mbld	::/0		All possible IPv6 networks
4	localhost	127.0.0.1 (127.0.0.1)		Localhost, for non-management high Availability d...
5	localhost6	::1 (::1)		Localhost, for non-management high Availability d...
6	VMWare_Gateway	172.17.1.1		
7	DNS1	172.17.1.1		
8	DNS2	172.17.1.1		
9	my_address	172.17.1.222		
10	Radius_Server	172.17.1.205		
11	VPNPool	10.40.1.0/24		

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

Wechseln Sie nun in Policies – User Directories - Radius

#	Name	IP address	Port	Retry timeout	Comments
1	Radius_domain_local	Radius_Server	1812	2	

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 Authentifizierung zum Einsatz kommt. Hierfür sind die sogenannten Authentication Rules der Clavister Firewall zuständig.

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

#	Name	Authentication agent	Authentication source	Interface	Comments
1	Radius_Http	HTTPS	RADIUS	any	
2	Radius_SSH	L2TP/IPsec/SSL/VPN	RADIUS	any	

Klicken Sie auf Add und erstellen eine neue Regel für HTTP/HTTPS Authentifizierung

The screenshot shows the 'Radius_http' configuration page in the Clavister interface. The 'General' tab is selected, displaying fields for Name, Authentication agent, Authentication Source, Interface, Originator IP, and Terminator IP. The 'Add' button is located at the bottom of the form.

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

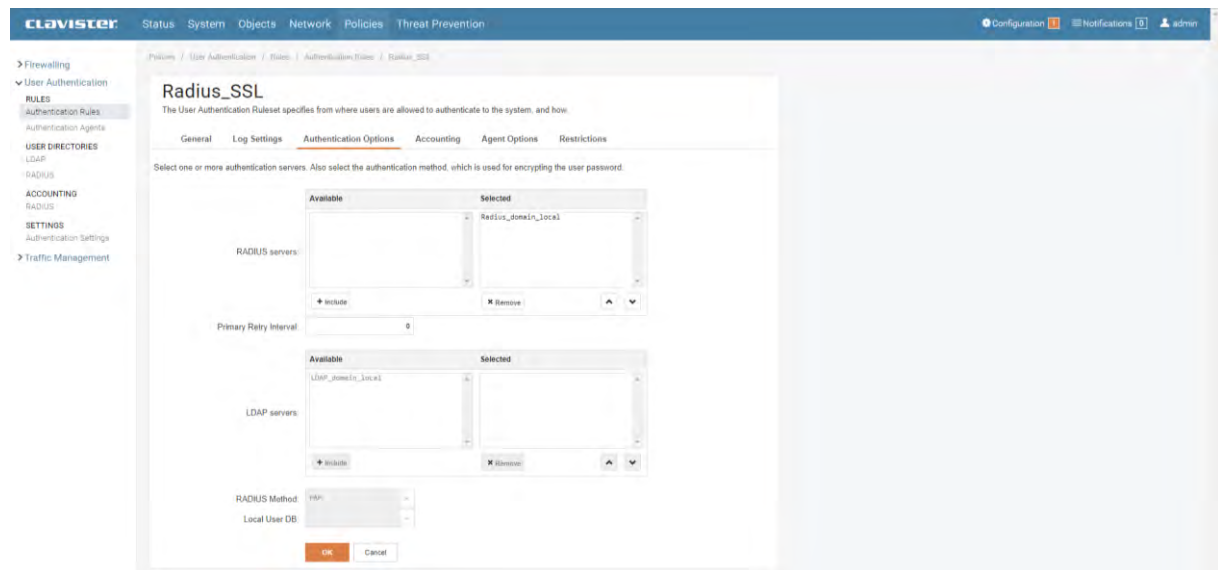
The screenshot shows the 'Radius_http' configuration page in the Clavister interface, with the 'Authentication Options' tab selected. It displays fields for RADIUS servers, Primary Retry Interval, LDAP servers, RADIUS Method, and Local User DB. The 'Add' button is at the bottom.

Unter Agent Options, müssen Sie grundsätzlich keine Einstellungen vornehmen, wichtig ist das PAP Authentication unter PPP Agent Options aktiviert ist. Eventuell müssen Sie noch ein HTTPs Host Zertifikat auswählen, diese Einstellung betrifft aber nicht die eigentlich Radius Authentifizierung, 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.

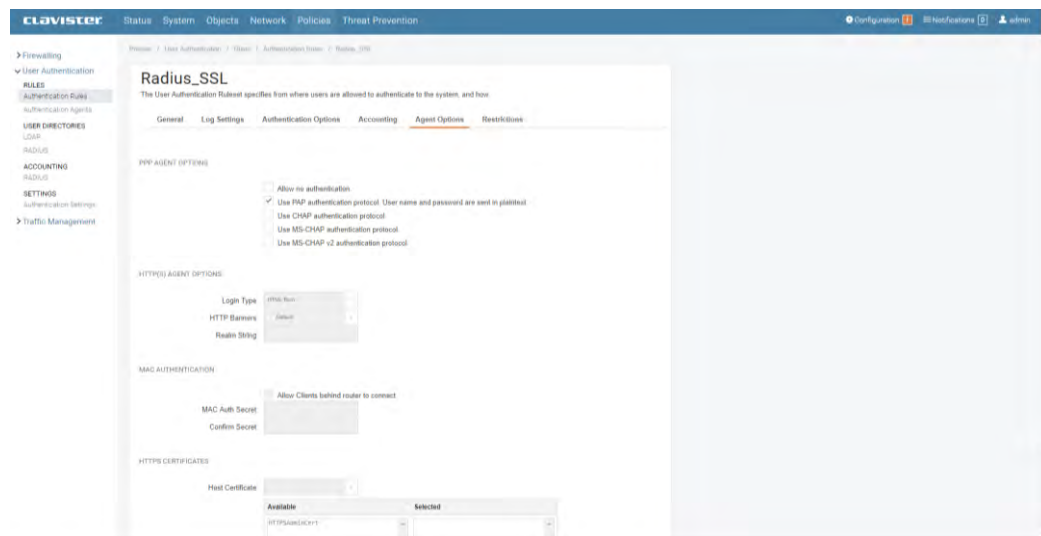
Die Einstellungen hierbei sind identisch mit der HTTP/HTTPs Authentifizierung.

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

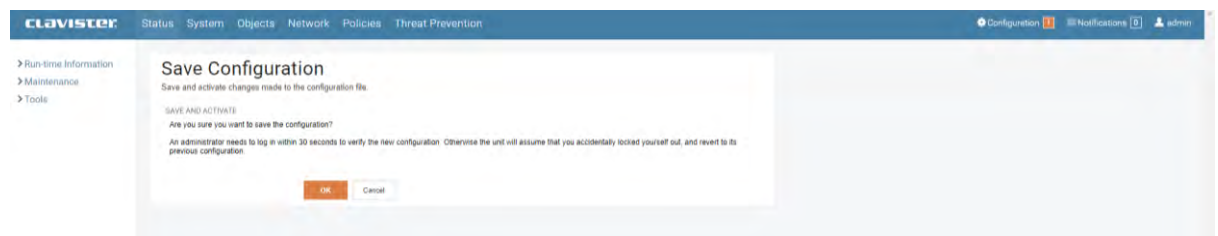


Die Radius Method ist ausgegraut, sollte jedoch bereits auf PAP eingestellt sein.

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.



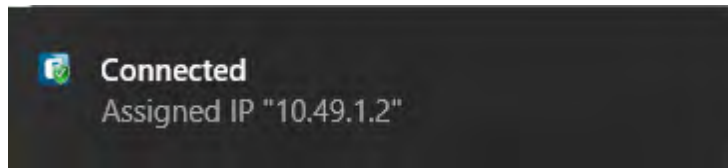
7.3.3. Anmelden an SSLVPN mit Yubikey

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 Adresse. 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.



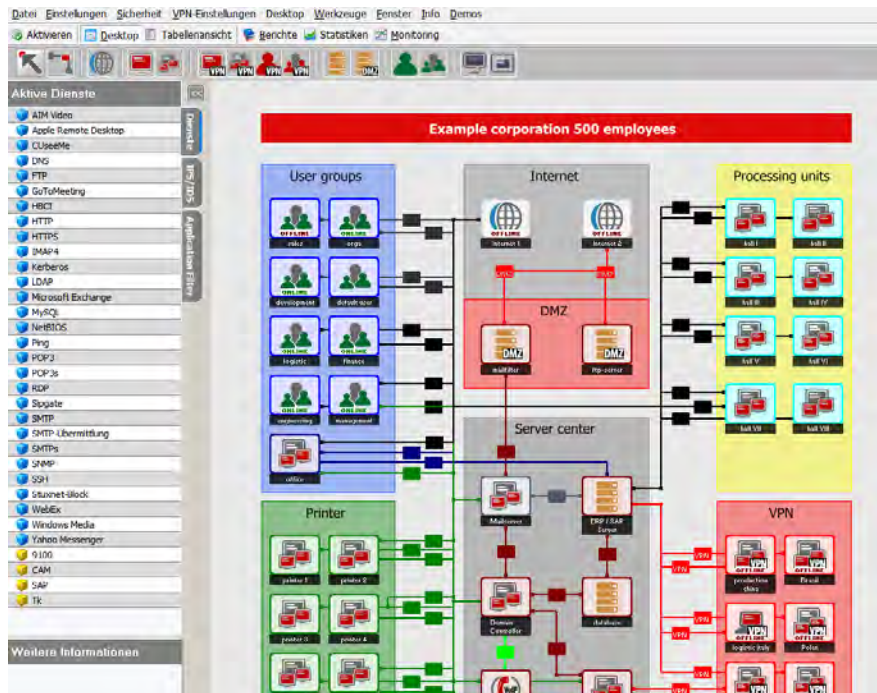
7.4. Rohde & Schwarz Firewall

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

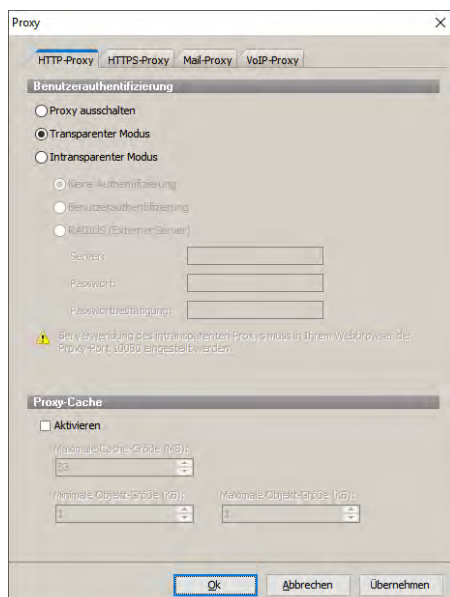
Wir verwenden die Rohde & Schwarz Unified Firewall Version 9.8

7.4.1. Konfigurieren der Radius Anbindung

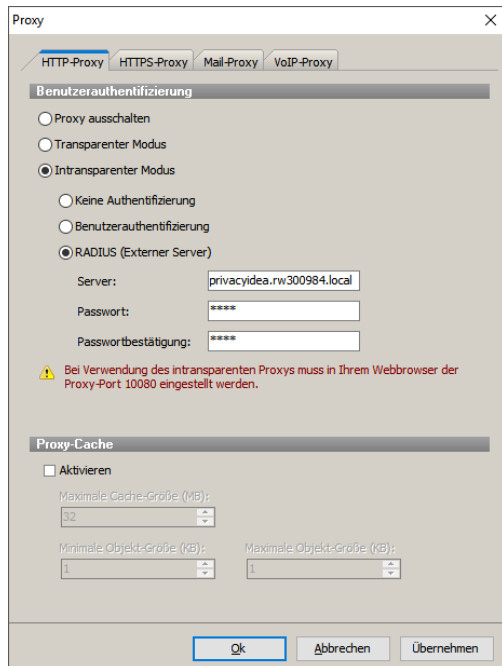
Öffnen Sie den Administrationsclient



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 Adresse 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



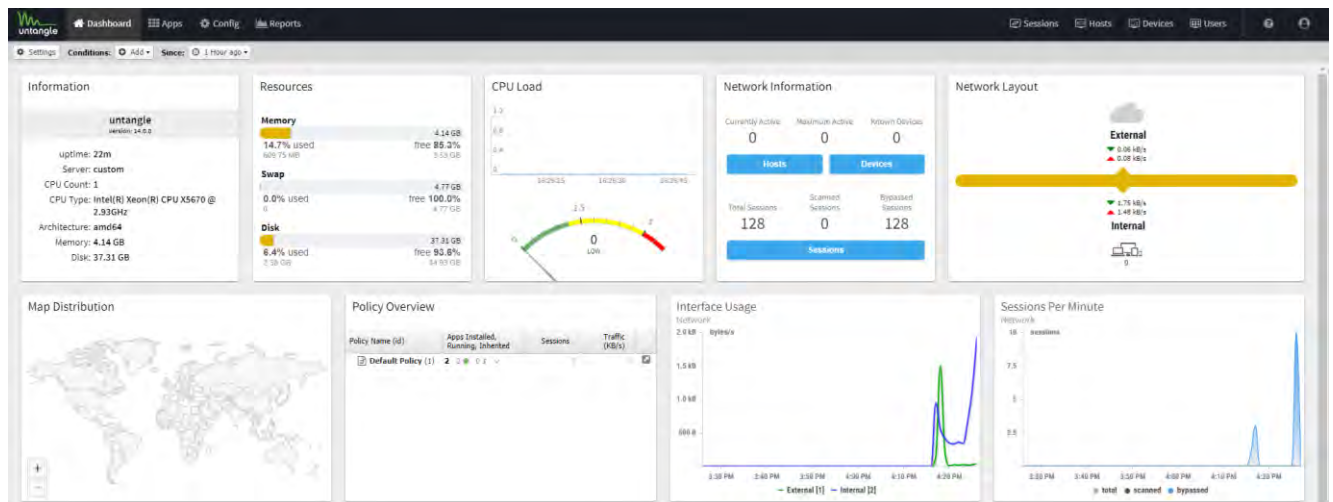
7.5. Untangle Firewall

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

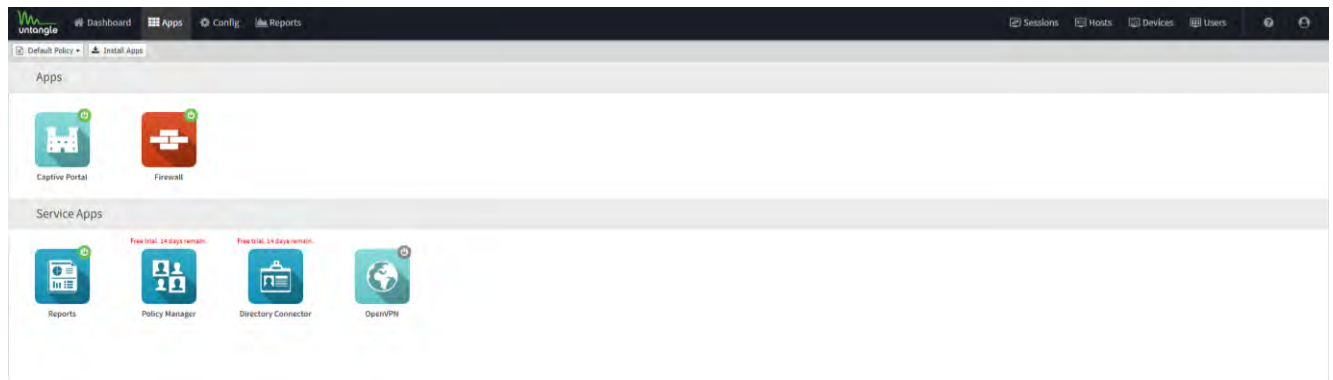
Der Guide wurde erstellt mit der Untangle Version 14.

7.5.1. Konfigurieren der Radius Anbindung

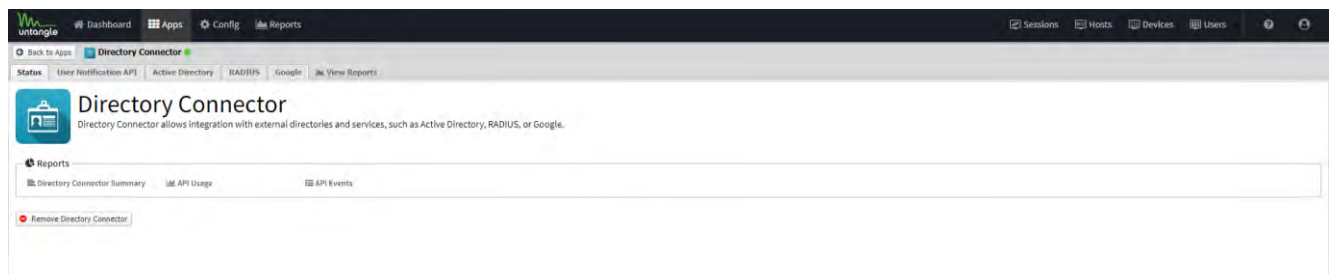
Öffnen Sie das Untangle Webinterface als Administrator



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

The screenshot shows the 'Directory Connector' configuration window in Windows Firewall. The 'RADIUS' tab is selected. The 'Enable RADIUS Connector' checkbox is checked. The configuration fields are as follows:

- RADIUS Server IP or Hostname: 172.17.7.205
- Authentication Port: 1812
- Accounting Port: 1813
- Shared Secret: myownsecret
- Authentication Method: PAP

Below the configuration fields, there is a 'RADIUS Test' section. It includes a 'Test' button and a 'RADIUS Test' checkbox. The test parameters are:

- Username: ronny.wolf
- Password: yubico@2018952474

Sie können nun die Radius Authentifizierung testen. Geben Sie hierzu

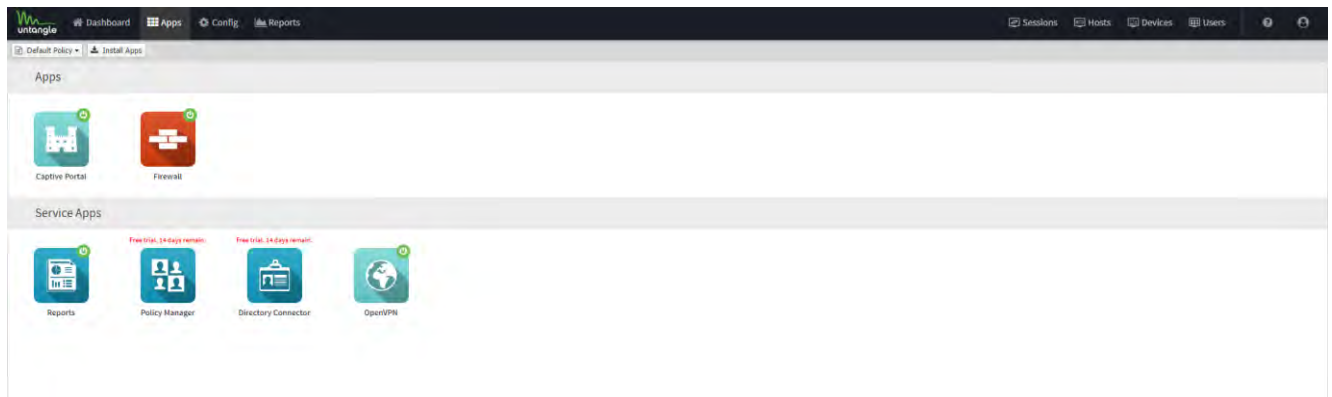
Benutzer: Active Directory Benutzer mit Yubikey zugewiesen
 Passwort: Active Directory Passwort + Yubikey OTP

This screenshot shows the same 'Directory Connector' configuration window as before, but with a small dialog box overlaid in the center. The dialog box is titled 'RADIUS Test' and contains the message 'RADIUS authentication successful!'. There is an 'OK' button at the bottom of the dialog box.

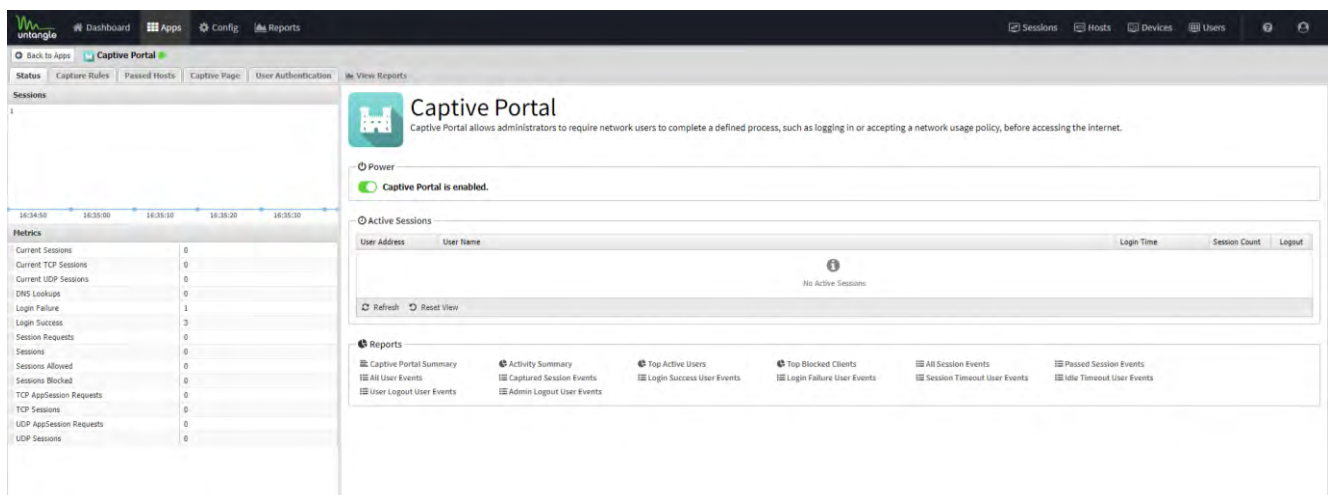
Sie haben sich nun erfolgreich die Radius Server Anbindung konfiguriert.

7.5.2. Anmelden an Captive Portal mit Yubikey

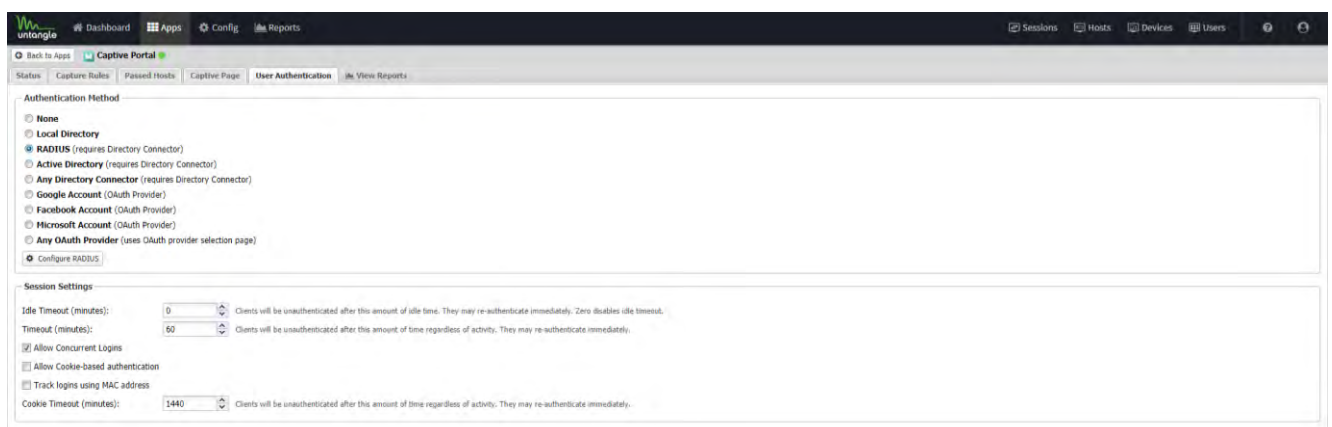
Um eine Zwei Faktor Authentifizierung am Captive Portal von Untangle zu erreichen. Klicken Sie auf Apps – Captive Portal



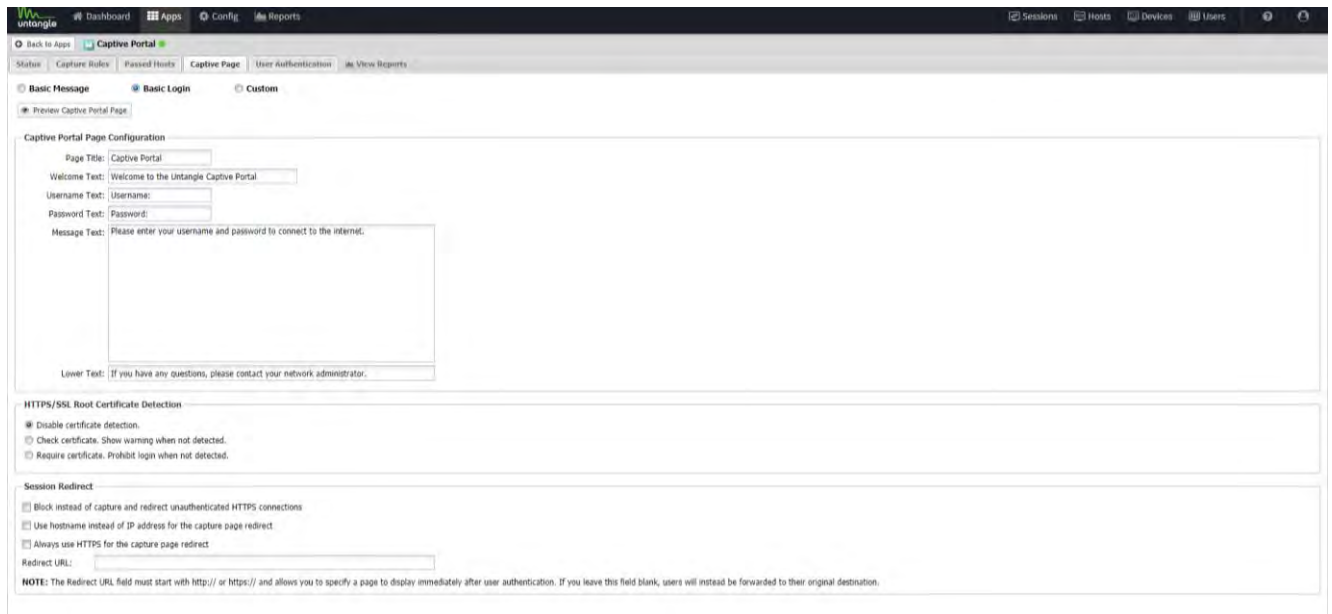
Wählen Sie nun User Authentication



Selektieren Sie unter Authentication = Radius



Damit eine Benutzerauthentifizierung (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

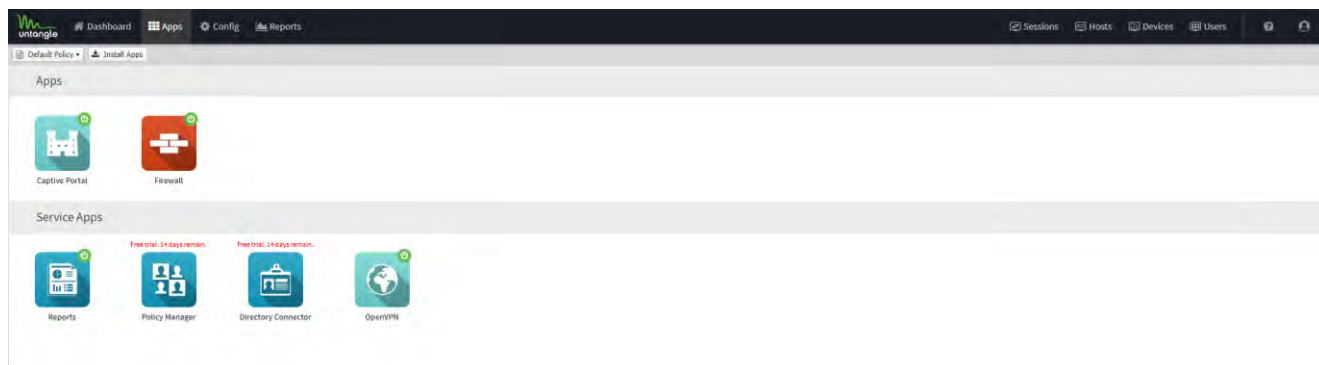


War die Anmeldung erfolgreich, erhalten Sie folgende Meldung

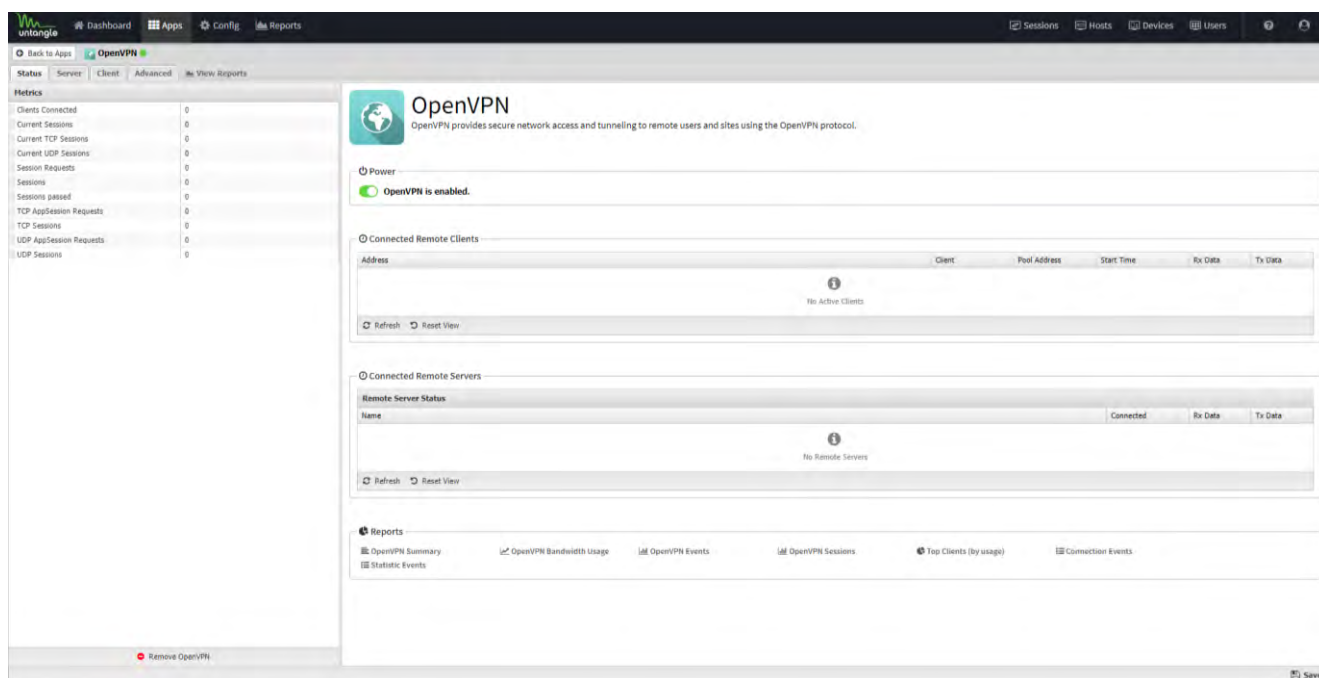
Login Success

7.5.3. Anmeldung via OpenVPN mit Yubikey

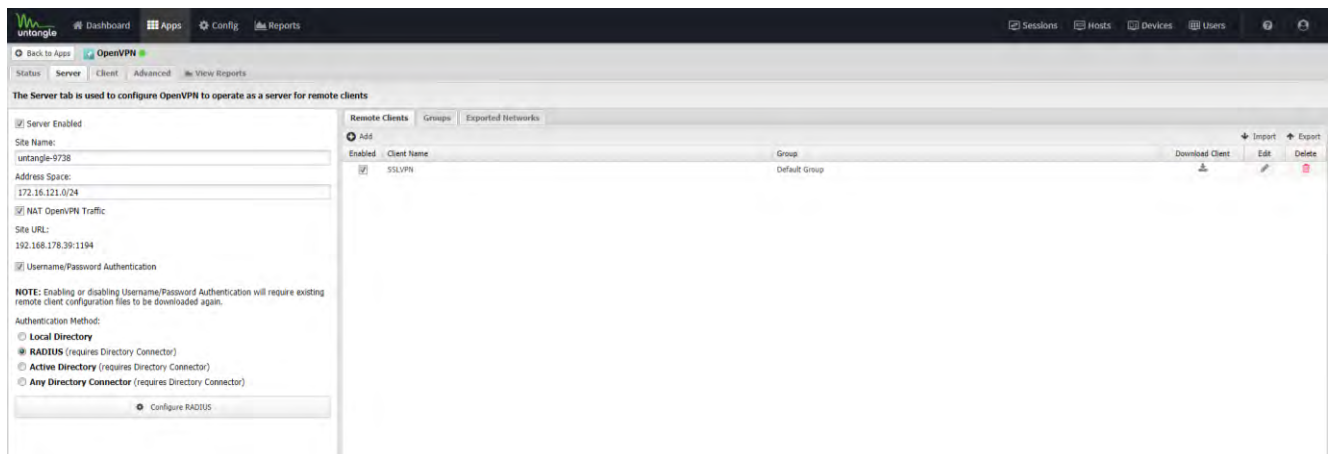
Um eine SSL VPN (OpenVPN) Anmeldung mit einem zweiten Faktor zu realisieren. Klicken Sie auf Apps – OpenVPN



Klicken Sie auf Server



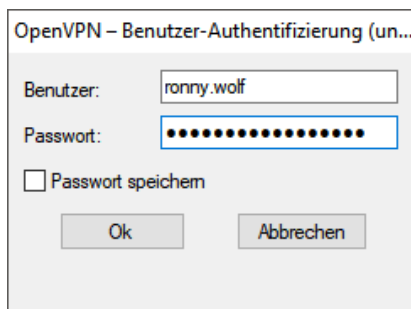
Aktivieren Sie den OpenVPN Server und wählen als Authentication Method: Radius



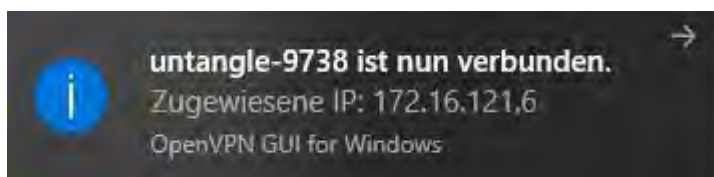
Nachdem Sie den OpenVPN Client von Untangle erfolgreich installiert haben, können Sie sich wie folgt anmelden:

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.

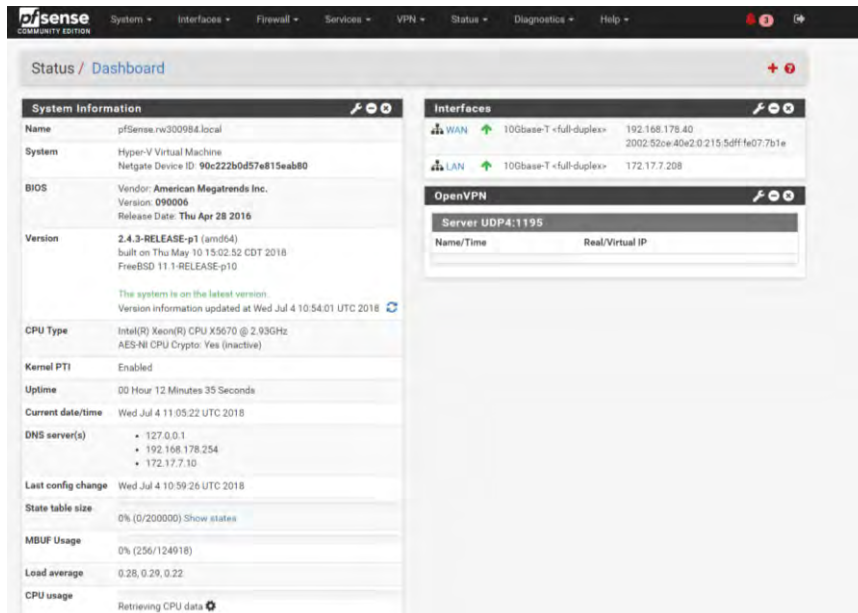


7.6. pfSense Firewall

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

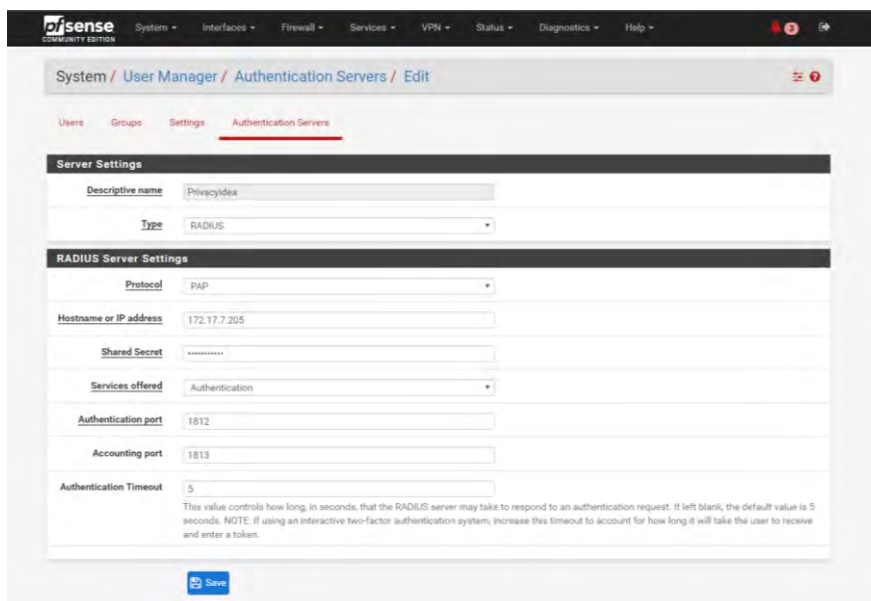
Definieren Sie folgende Parameter:

Type: Radius

Protocol: PAP

Hostname or IP address: privacyIDEA Server

Shared Secret: Shared Secret aus Kapitel 2, Absatz 8

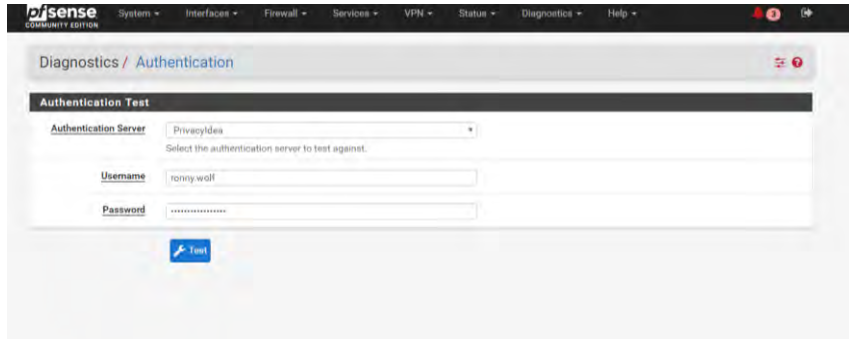


Testen Sie nun die Authentifizierung am Radius Server über Diagnostics – Authentication

Geben Sie hierzu folgende Benutzerdaten ein:

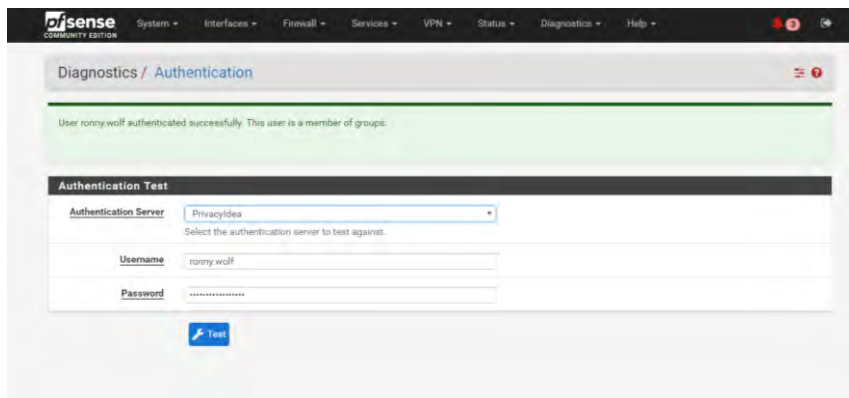
Benutzer: Active Directory Benutzer mit Yubikey zugewiesen

Passwort: Active Directory Passwort + Yubikey OTP



The screenshot shows the Pfsense web interface, specifically the 'Diagnostics / Authentication' section. The 'Authentication Test' form is visible, with the following fields: 'Authentication Server' set to 'PrivacyIDEA', 'Username' set to 'ronny.wolf', and 'Password' masked with dots. A 'Test' button is located below the password field.

Die Zwei Faktor Authentifizierung am privacyIDEA Server war erfolgreich

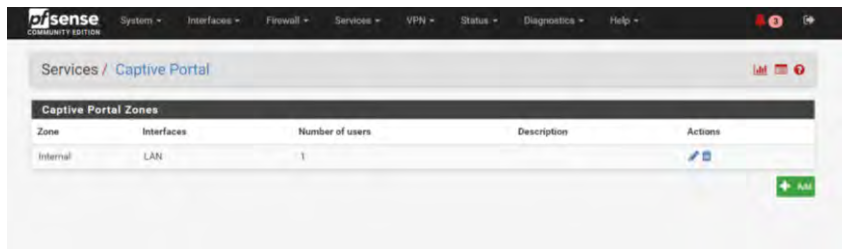


The screenshot shows the same Pfsense web interface, but now with a green success message at the top: 'User ronny.wolf authenticated successfully. This user is a member of groups:'. The 'Authentication Test' form is still visible below the message.

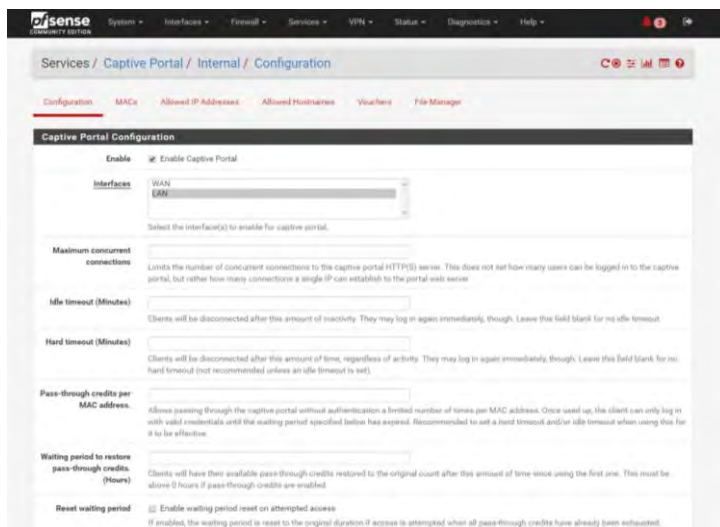
Die Radius Server Anbindung ist nun vollständig konfiguriert.

7.6.2. Anmeldung an Captive Portal mit Yubikey

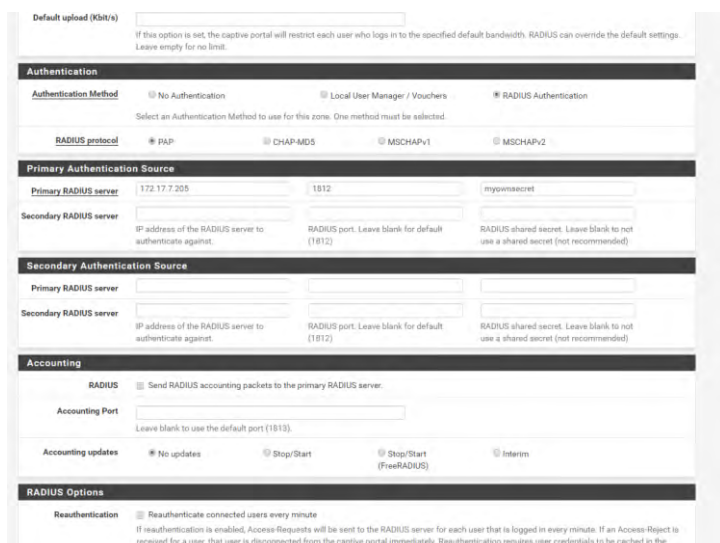
Um sich am Captive Portal anmelden zu können, müssen wir dieses konfigurieren. Klicken Sie hierzu auf Services – Captive Portal



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

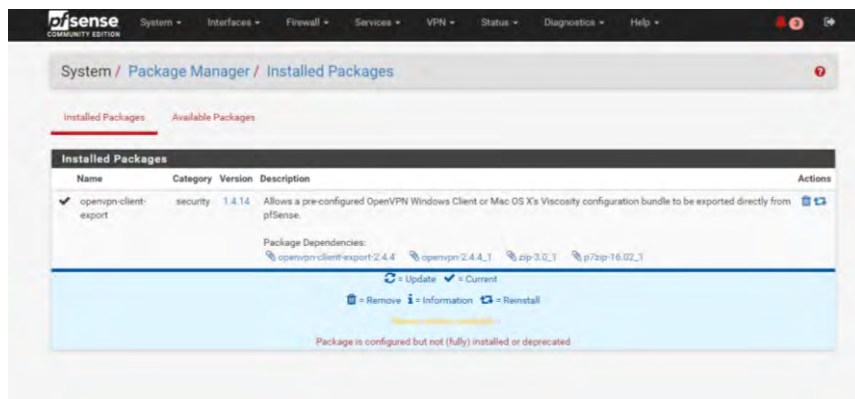


Die Anmeldung mit einem zweiten Faktor war erfolgreich.

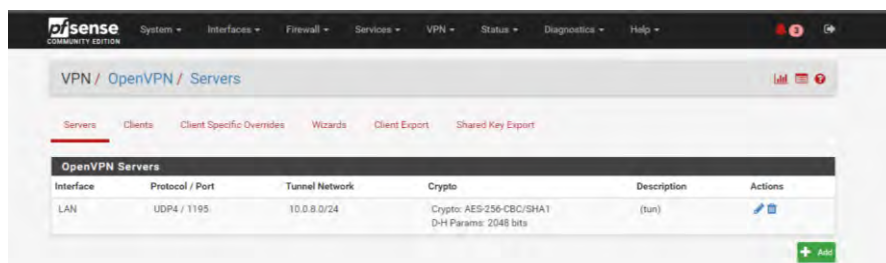
7.6.3. Anmeldung via OpenVPN mit Yubikey

Sie können ebenfalls eine OpenVPN (SSL VPN) Verbindung über eine zwei Faktor Authentifizierung 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

VPN / OpenVPN / Servers / Edit

General Information

Disabled ☐ Disable this server
Set this option to disable this server without removing it from the list.

Server mode Remote Access (User Auth)

Backend for authentication Radius

Protocol UDP on IPv4 only

Device mode tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2)

Interface LAN
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port 1195
The port used by OpenVPN to receive client connections.

Description
A description may be entered here for administrative reference (not parsed).

Cryptographic Settings

TLS Configuration ☒ Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake.
This layer of "MMA" authentication allows remote channel markets without the need for a common key to be derived, restricting the name from attack or

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

Additional configuration options

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote random;

[Save as default](#)

Search

Search term [Search](#) [Clear](#)

Enter a search string or fnix regular expression to search.

OpenVPN Clients

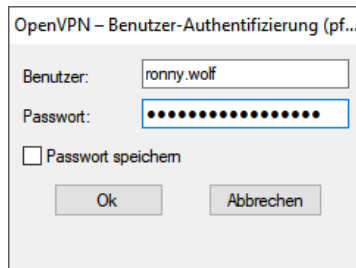
User	Certificate Name	Export
Authentication Only (No Cert)	none	Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) Bundled Configurations: Archive Config File Only Current Windows Installer (2.4.4-1x01): Windows Vista and Later Old Windows Installers (2.3.18-1x01): x86-32 x86-64 x86-64-32bit x86-64-64bit Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

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



OpenVPN - Benutzer-Authentifizierung (pf...)

Benutzer:

Passwort:

☐ Passwort speichern

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

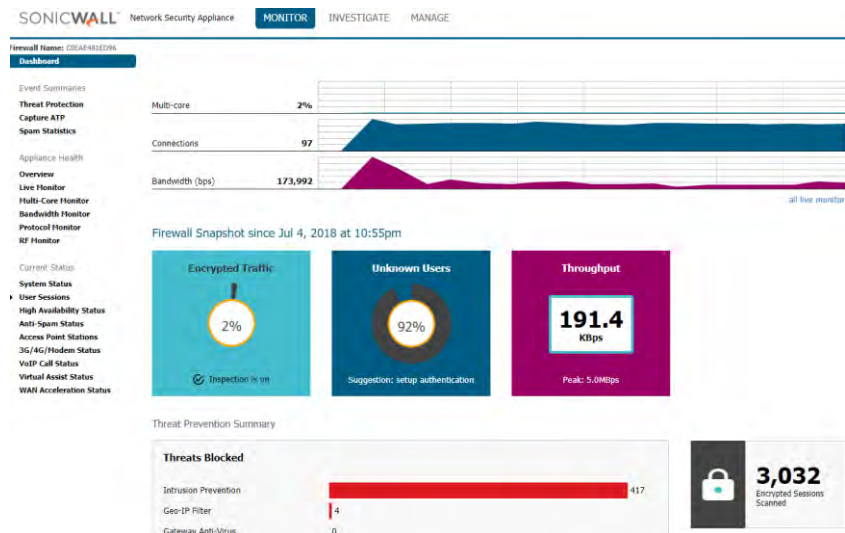


7.7. Sonicwall NSA Firewall

Der Hersteller Sonicwall bietet die Möglichkeit eine Zwei Faktor Authentifizierung 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

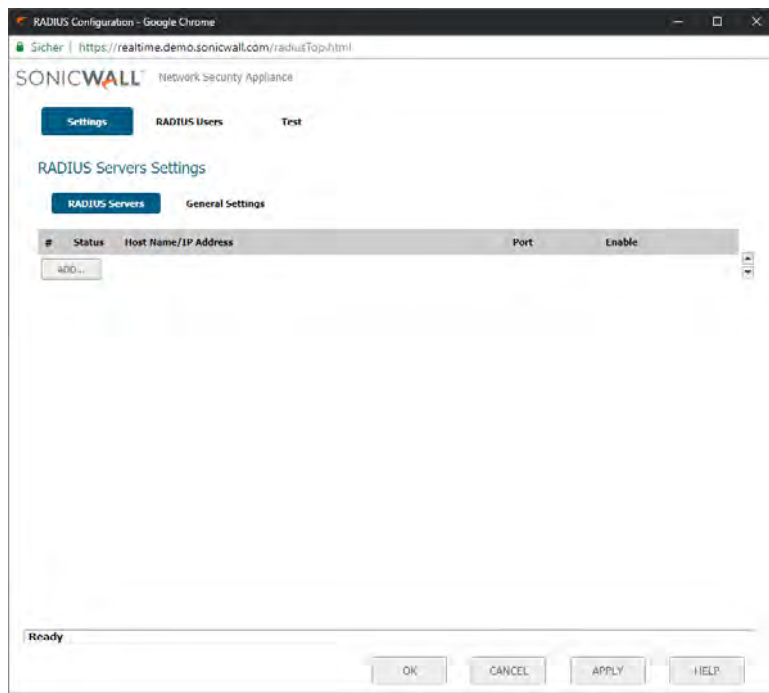
Öffnen Sie das Sonicwall NSA Webinterface als Administrator.



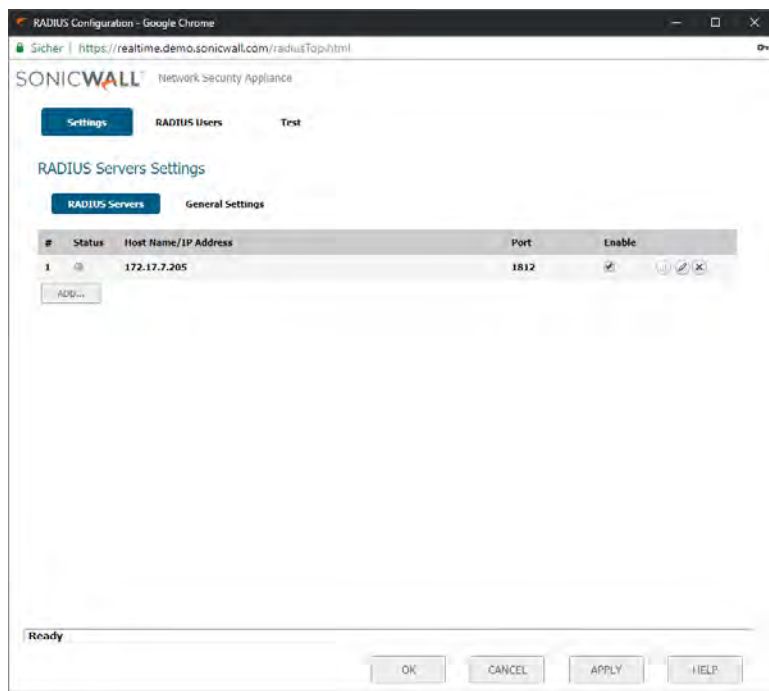
Wechseln Sie nun zu Manage – System Setup – Settings

The screenshot shows the 'User Authentication Settings' configuration page in the 'MANAGE' section. The left sidebar shows the navigation tree with 'Settings' selected under 'System Setup'. The main content area is titled 'User Authentication Settings' and includes tabs for 'Authentication', 'Web Login', 'Authentication Bypass', 'User Sessions', 'Accounting', and 'Customization'. The 'Authentication' tab is active, showing the 'User authentication method' set to 'LDAP + Local Users'. Below this, the 'Single-sign-on method(s)' section lists various authentication methods, including 'SSO Agent', 'Terminal Services Agent', 'RADIUS Accounting', '3rd-Party API', and 'Browser NTLM Authentication'. The 'One-Time Password' section is expanded, showing options for 'Enforce password complexity for One-Time Password', 'One-time password E-mail format' (set to 'Plain Text'), 'One Time Password Format' (set to 'Characters'), and 'One Time Password Length' (set to '10' characters). A 'Password Strength' indicator shows 'Good'. At the bottom, there are 'ACCEPT' and 'CANCEL' buttons.

Klicken Sie auf Configure Radius



Fügen Sie einen neuen Radius Server hinzu, verwenden Sie hierbei die IP Adresse 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

RADIUS Configuration - Google Chrome

Sicher | <https://realtime.demo.sonicwall.com/radiusTop.html>

SONICWALL Network Security Appliance

Settings RADIUS Users **Test**

Test RADIUS Settings

To test the RADIUS settings select the test, enter a user name and password that is valid on the RADIUS server if relevant, and then click the Test button. Note that this will apply any changes that have been made.

Select server to test: 172.17.7.205

Test: ☒ Connectivity ☐ Password authentication ☐ CHAP ☐ MSCHAP ☐ MSCHAPV2

TEST

Test Status:
Ready

Returned User Attributes:

Ready

OK CANCEL APPLY HELP

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

SONICWALL Network Security Appliance MONITOR INVESTIGATE **MANAGE**

Firewall Name: CREAN81ED96 Help | Close Mode: Non-Config

Updates Licenses Firmware & Backups WXA Firmware Restart

Connectivity

VPN VPN SSL VPN Access Points 3G/4G/HSDPA

Policies Rules Objects

System Setup

Apppliance Users

Partitions Local Users & Groups Guest Services Guest Accounts

Network Switching High Availability WAN Acceleration VOIP Virtual Asset

Security Configuration

Firewall Settings Security Services Decryption Services Anti-spam

Loss & Reporting

User Authentication Settings

User authentication method: RADIUS + Local Users CONFIGURE RADIUS CONFIGURE LDAP CONFIGURE TACACS+

Single-sign-on method(s): SSO Agent Terminal Services Agent RADIUS Accounting 3rd Party API Browser NTLM Authentication CONFIGURE SSO

☐ Case-sensitive user names
☐ Enforce login uniqueness
☒ Force relogin after password change
☒ Display user login info since last login

One-Time Password:
☐ Enforce password complexity for One-Time Password
One-time password E-mail format: Plain Text HTML
One Time Password Format: Characters
One Time Password Length: 10 - 10 characters Password Strength: Good

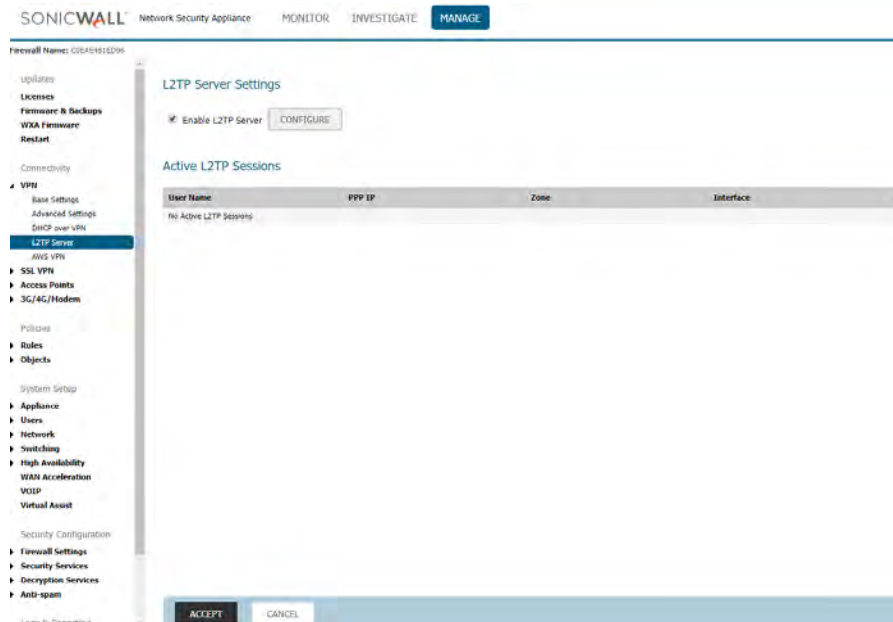
ACCEPT CANCEL

Sie haben nun die Grundkonfiguration des Radius Server abgeschlossen

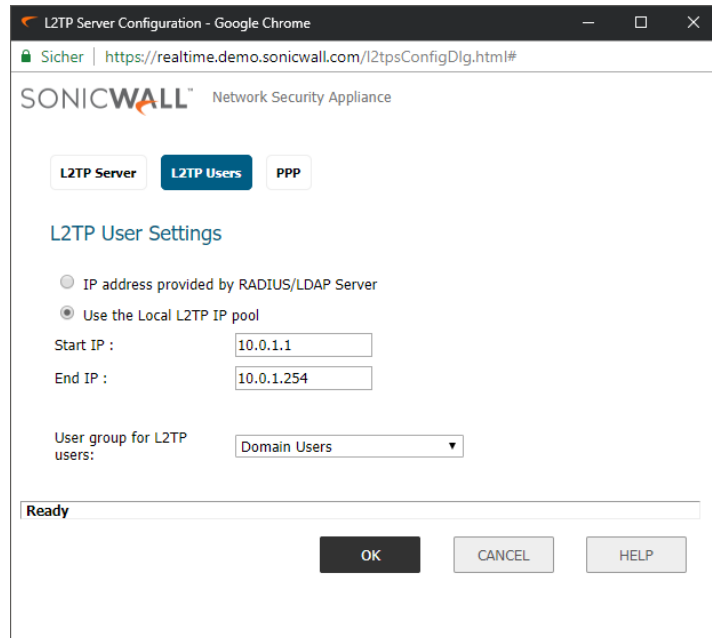
7.7.2. Konfigurieren von L2TP mit Yubikey

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 Authentifizierungsversuche, 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.

Nr.	Datum	Aktion	Erfolg	Aktionsdetail	Seriennummer	Tokentyp	Administrator	Benutzer	Realm	Resolver	Client
683	3.7.18 02:07:05	GET /realm/	1				administrator				172.17.7.
682	3.7.18 02:07:05	GET /token/	1				administrator				172.17.7.
681	3.7.18 02:07:05	GET /realm/	1				administrator				172.17.7.
680	3.7.18 02:07:05	POST /auth/	1				administrator				172.17.7.
679	3.7.18 02:06:43	GET /token/	1		PIEM00000E46	email		ronny.wolf	activedirectory	ActiveDirectory	172.17.7.
678	3.7.18 02:06:43	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	172.17.7.
677	3.7.18 02:05:58	GET /token/	1		PIEM00000E46	email		ronny.wolf	activedirectory	ActiveDirectory	172.17.7.
676	3.7.18 02:05:57	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	172.17.7.
675	3.7.18 02:05:34	GET /token/	1		PIEM00000E46	email		ronny.wolf	activedirectory	ActiveDirectory	172.17.7.
674	3.7.18 02:05:34	GET /system/	1					ronny.wolf	activedirectory	ActiveDirectory	172.17.7.

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

Nr.	Datum	Aktion	Erfolg	Aktionsdetail	Seriennummer	Tokentyp	Administrator	Benutzer	Realm	Resolver	Client
1485	17.7.18 16:19:03	POST /validate/check	1		UBAM7446982_X						172.1
1413	4.7.18 13:13:55	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	192.1
1411	4.7.18 13:12:29	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	192.1
1409	4.7.18 13:08:10	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	0.0.0.
1407	4.7.18 13:03:46	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	192.1
1373	3.7.18 19:52:13	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	192.1
1370	3.7.18 19:12:37	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	0.0.0.
1350	3.7.18 16:50:31	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	172.1
1347	3.7.18 16:39:27	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	172.1
1344	3.7.18 16:33:30	POST /validate/check	1		PIEM00000E46			ronny.wolf	activedirectory	ActiveDirectory	172.1

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

audit.csv - Excel																			
File Home Insert Page Layout Formulas Data Review View Tell me what you want to do...																			
From Access From Web From Other Sources Recent Sources Refresh All Edit Links Sort Filters Reapply Text to Columns Flash Fill Remove Duplicates Validation Data Consolidate Links Worksheets Manage Data Model What-If Analysis Forecast Group Ungroup																			
Get & Transform Get & Transform Connections Sort & Filter Data Tools																			
1266																			
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	'	'None'	'None'	'None'	'None'	'privac'	'FAIL'	'None'	'172.17.7.104'	'None'	'GET /rs/1/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'None'	'None'
2	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'264'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
3	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'265'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
4	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'266'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
5	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'268'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
6	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'290'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
7	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'307'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
8	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'309'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
9	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'310'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
10	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'311'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
11	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'312'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
12	'The user has no tokens assign	'None'	'default'	'None'	'V'	'localhost'	'OK'	'313'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'administr'	'default'	'None'	'2018-07-0'	'None'	'None'	'None'
13	'wrong otp pin'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'713'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'None'	'None'
14	'Enter the OTP from the Email'	'None'	'None'	'None'	'V'	'privacyid'	'OK'	'667'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
15	'matching 1 tokens'	'None'	'None'	'None'	'V'	'privacyid'	'OK'	'669'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
16	'Enter the OTP from the Email'	'None'	'None'	'None'	'V'	'privacyid'	'OK'	'676'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
17	'matching 1 tokens'	'None'	'None'	'None'	'V'	'privacyid'	'OK'	'678'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
18	'wrong otp pin'	'None'	'None'	'None'	'V'	'privacyid'	'OK'	'711'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
19	'Enter the OTP from the Email'	'None'	'None'	'None'	'V'	'privacyid'	'OK'	'713'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
20	'matching 1 tokens'	'None'	'None'	'None'	'V'	'privacyid'	'OK'	'715'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'None'	'None'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
21	'Enter the OTP from the Email'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'772'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
22	'matching 1 tokens'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'773'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
23	'Enter the OTP from the Email'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'789'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
24	'matching 1 tokens'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'791'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
25	'Enter the OTP from the Email'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'949'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
26	'matching 1 tokens'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'956'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
27	'Enter the OTP from the Email'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'959'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'PIEM000000E46'	'None'
28	'None'	'None'	'activedi'	'None'	'V'	'localhost'	'OK'	'960'	'172.17.7.104'	'None'	'POST /val/OK'	'None'	'Yonny.w'	'ActiveDir'	'None'	'2018-07-0'	'None'	'None'	'None'

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 Authentifizierungsanfragen und damit einen Statistischen Überblick.

Klicken Sie hierzu auf Audit – Statistik

Token
 Benutzer
 Maschinen
 Konfiguration
 Audit
 Komponenten

Aktualisieren

administrator @ (admin)

Logbuch
 Statistik

Statistik für die zurückliegenden Tage...

30

Statistik von

Statistik bis

Aktualisieren

Validate-Requests pro Benutzer

Validate-Requests pro Token

Fehlgeschlagene Authentisierungen pro Token

Fehlgeschlagene Authentisierungen pro Benutzer

Administrative Aktionen

Allgemeine Tokennutzung

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

