EINRICHTUNG NETZWERK UND WLAN

für Schulen ohne pädagogischen Landes-Breitbandanschluss

Letzte Änderung: **15.03.2024**

Diese Anleitung beschreibt die Einrichtung der Netzwerk- und WLAN-Komponenten für die Musterlösung Grundschule SH. Es werden die notwendigen Einrichtungsschritte für Schulen aufgezeigt, die anstelle des pädagogischen Landes-Breitbandzugangs eine **alternative Internetanbindung** nutzen.

Wichtig: Für Schulen, die den pädagogischen Landes-Breitbandzugang nutzen, wird die Einrichtung in der Anleitung „Musterlösung Grundschule SH_Einrichtung Netzwerk und WLAN (mit Landes-Breitbandanschluss).pdf“ beschrieben.

Änderung vom 15.03.2024:

- Die Einbindung von WLAN-Access Points funktioniert nur, wenn bereits WLAN-Netze angelegt wurden. Daher wurde die Reihenfolge im Kapitel WLAN einrichten geändert.

Änderung vom 14.03.2024:

- Ein UniFi-Account zur Registrierung eines bzw. mehrerer Cloudkeys soll zukünftig maximal die Geräte der Schule(n) eines Schulträgers enthalten. Für weitere zu betreuende Schulträger soll jeweils ein neuer UniFi-Account mit einer neuen E-Mail-Adresse angelegt werden. Dadurch soll sichergestellt werden, dass im Falle eines Dienstleisterwechsels, der UniFi-Account problemlos an den neuen Dienstleister übergeben werden kann (siehe Kapitel E-Mail-Benachrichtigung aktivieren).

Änderung vom 07.02.2024:

- Durch die Aktualisierung der UniFi Network Application haben sich einige Screenshots im Kapitel Controller einrichten geändert.

Änderung vom 29.11.2023:

- Durch die Aktualisierung der UniFi Network Application haben sich einige Screenshots im Kapitel Controller einrichten geändert. So gibt es im Systemmenü zur Einrichtung der UniFi-Komponenten nun z. B. einen eigenen Menüpunkt zum Einstellen der Switch-Ports.

Ältere Änderungen sind in der Änderungshistorie am Ende der Anleitung zu finden.

1 Kurzbeschreibung

Neben den Netzen für Endgeräte der Lernenden und Dienstgeräte der Lehrkräfte soll ein Netz für die Nutzung persönlicher Endgeräte von Lehrkräften, Mitarbeitern, Mitarbeiterinnen und Gästen eingerichtet werden. Die Netze werden über unterschiedliche WLAN-SSIDs bereitgestellt.

Das **Netz für die schuleigenen Endgeräte der Schülerinnen und Schüler** hat folgende Merkmale:

- Das WLAN wird über ein festes Kennwort (WPA 2 AES) abgesichert, das in den mobilen schuleigenen Endgeräten hinterlegt wird. Die Anmeldung am WLAN erfolgt dann automatisch.
- Der Zugriff aus diesem Netz auf das Internet ist gefiltert.
- Der Zugriff auf die gemeinsame Datenablage ist möglich.

Das **Netz für die Dienstgeräte der Lehrkräfte** hat folgende Merkmale:

- Das WLAN wird über ein festes Kennwort (WPA 2 AES) abgesichert.
- Der Zugriff aus diesem Netz auf das Internet ist ungefiltert.
- Der Zugriff auf die gemeinsame Datenablage ist möglich.

Das **Netz für private Endgeräte z.B. von Lehrkräften, Mitarbeitern und Gästen** hat folgende Merkmale:

- Die Anmeldung am WLAN ist ohne Passwort (offenes WLAN) möglich.
- Die Internetnutzung wird im Anschluss über ein Portal (Captive Portal) geregelt. Dabei wird ein Gutschein-Code abgefragt, der zur Nutzung des Internets berechtigt. Die Gutscheine können über den Controller generiert und mit unterschiedlichen Laufzeiten (z.B. 5 Jahre für Lehrkräfte und 1 Tag für Gäste) ausgegeben werden. Für die Bereitstellung des Portals wird ein Hardware-Controller benötigt.
- Der Zugriff aus diesem Netz auf das Internet ist ungefiltert.
- Der Zugriff auf die gemeinsame Datenablage ist nicht möglich.

Hinweis: Nach Möglichkeit soll ein **VPN-Zugriff** von außen auf das Unterrichtsnetz eingerichtet werden. Auf diesem Wege soll zum Beispiel die Fernwartung des Systems über den Dienstleister bzw. den Schulträger möglich sein. Dadurch entfällt dann die Anschaffung eines Wartungsrechners. Das **VPN** hat folgende Merkmale:

- Die Verbindung zum Netzwerk wird über IPSec/L2TP mit Pre-shared Key hergestellt.
- Das VPN wird über ein festes Kennwort abgesichert.

Über eine **Dienstanweisung (siehe Vorlage „Musterlösung Grundschule SH_Dienstanweisung)** sollte eine **Nutzungsordnung** u.a. für das eingerichtete WLAN in Kraft gesetzt werden. Daraus sollte hervorgehen, dass das WLAN nur für dienstliche Zwecke genutzt werden darf und das Kennwort nicht weitergegeben werden darf. Personen, die der Dienstanweisung nicht unterliegen, sollten die Nutzungsordnung unterschreiben.

Hinweis: Die Einrichtung wird exemplarisch anhand von Ubiquiti- und Draytek-Hardware beschrieben.

Für die Einrichtung des Netzwerks (inkl. WLAN) werden folgende Geräte benötigt:

- Draytek-Router (Modell Vigor 2927)
- Ubiquiti-UniFi-Controller Cloudkey (2. Generation)
- Ubiquiti-UniFi-POE-Switch
- Ubiquiti-UniFi-Access Points
- Admin-Endgerät (zum Beispiel Notebook des Dienstleisters)

2 Router einrichten

Als Router soll der Draytek-Dual-WAN-Router Vigor 2927 verwendet werden. Das WLAN-Modul wird nicht benötigt. Bei Bedarf kann zusätzlich zum Landes-Breitbandanschluss über die zweite WAN-Schnittstelle ein weiterer Internetanschluss als Backup-Leitung genutzt werden.

Für Schulen ohne Landes-Breitbandanschluss soll der Router um eine Webfilterung (Global View Web Content Filter) ergänzt werden. Dafür fällt eine jährliche Lizenzgebühr an. Einstellungen an den schuleigenen Endgeräten für Schülerinnen und Schüler (fester Proxy) sind nicht notwendig, da es sich um eine DNS-Filterung handelt.

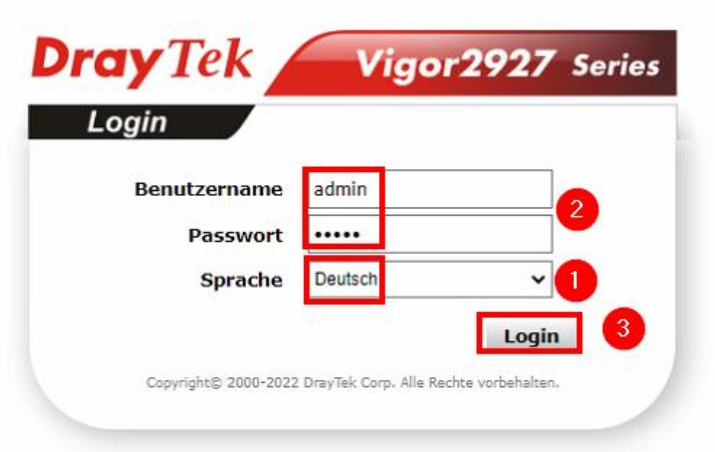
2.1 Erstkonfiguration und Firmware-Aktualisierung

Zunächst für das Admin-Endgerät eine IP aus dem Bereich 192.168.1.x vergeben.

Admin-Gerät an LAN-Port 1 („P1“) des Routers anschließen.

Die Weboberfläche des Routers über https://192.168.1.1 aufrufen.

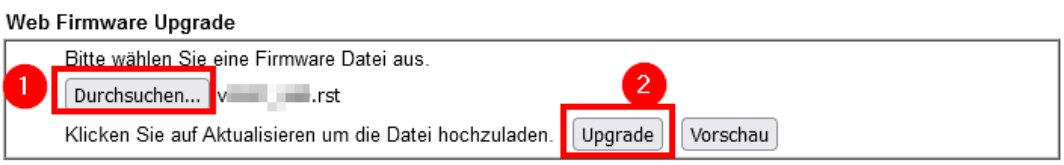
Sprache auf „Deutsch“ einstellen (1), beim ersten Login als User „admin“ sowie ebenfalls als Passwort „admin“ eingeben (2) und mit „Login“ bestätigen (3):



Hinweis: Ggf. ist die Sprachoption an dieser Stelle noch nicht vorhanden, da diese erst bei neueren Firmware-Versionen auftaucht. Spätestens nach dem Firmware-Update (siehe unten) sollte die Sprachwahl jedoch möglich sein.

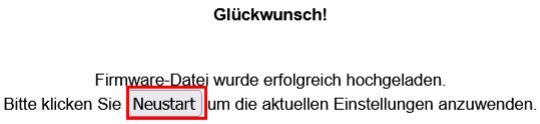
https://www.draytek.com/support/latest-firmwares die aktuelle Firmware für den verwendeten Draytek-Router herunterladen (STD-Variante) und die ZIP-Datei entpacken.

Über den Menüeintrag „Systemmanagement“ („System Maintenance“) – „Firmware aktualisieren“ („Firmware Upgrade“) und „Durchsuchen“ die heruntergeladene RST-Datei auswählen (1) und mit „Upgrade“ installieren (2):

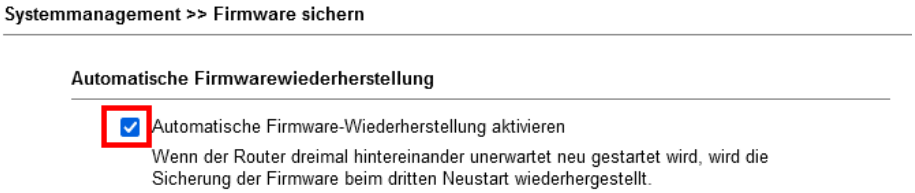


Wichtig: Mit der RST-Datei wird das Gerät komplett zurückgesetzt, bei späteren Updates sollte daher die ALL-Datei verwendet werden.

Gerät nach dem Firmware-Update über „Neustart“ bzw. „Restart“ und „OK“ neu starten:

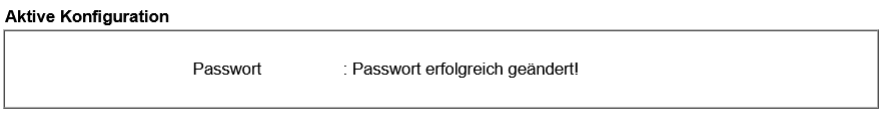


Erneut einloggen (Benutzername/Passwort = admin, Sprachwahl = „Deutsch“) und Frage nach Aktivierung der automatischen Firmware-Wiederherstellung mit „Ja“ beantworten. Falls diese Frage nicht auftaucht, diese Einstellung über „Systemmanagement“ („System Maintenance“) – „Firmware sichern“ („Firmware Backup“) selbst aktivieren:



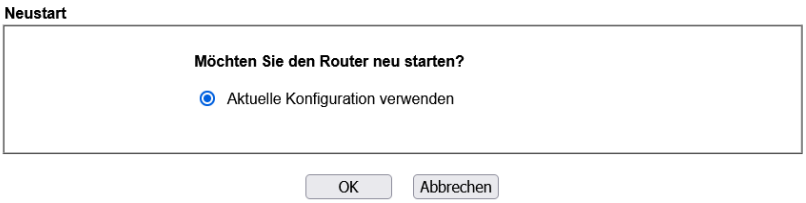
Menüeintrag „Systemmanagement“ – „Administrator Passwort“ wählen (1), den bisherigen Benutzernamen individuell z. B. auf den Nachnamen des Administrators bzw. der Administratorin anpassen (2), das Passwort auf ein starkes Kennwort ändern (3) und mit „OK“ bestätigen:

Die erfolgreiche Zugangsdaten-Änderung wird nachfolgend bestätigt:



Die Zugangsdaten in der IT-Dokumentation der Schule hinterlegen.

Hinweis: In den folgenden Schritten der Anleitung wird man nach bestimmten Änderungen immer wieder aufgefordert, den Router neu zu starten:



Anstatt den Neustart sofort durchzuführen, kann man auch auf „Abbrechen“ klicken und zunächst mit der Einrichtung weiterer Punkte fortfahren. Später kann dann ein Neustart gleich für mehrere vorgenommene Einstellungen durchgeführt werden. Dies kann über den Menüpunkt „Systemmanagement – „Neustart“ – „Jetzt neu starten“ vorgenommen werden.

2.2 Internet-Schnittstelle konfigurieren

Der vorhandene Router im Unterrichtsnetz der Schule soll durch den Draytek-Router ersetzt werden. Wenn in der Schule noch ein weiterer Internetanschluss vorhanden ist (zum Beispiel ein kostenloser T@School-Zugang), soll dieser Anschluss nach Möglichkeit ebenfalls über die zweite WAN-Schnittstelle genutzt werden, um eine Ausfallsicherheit herzustellen.

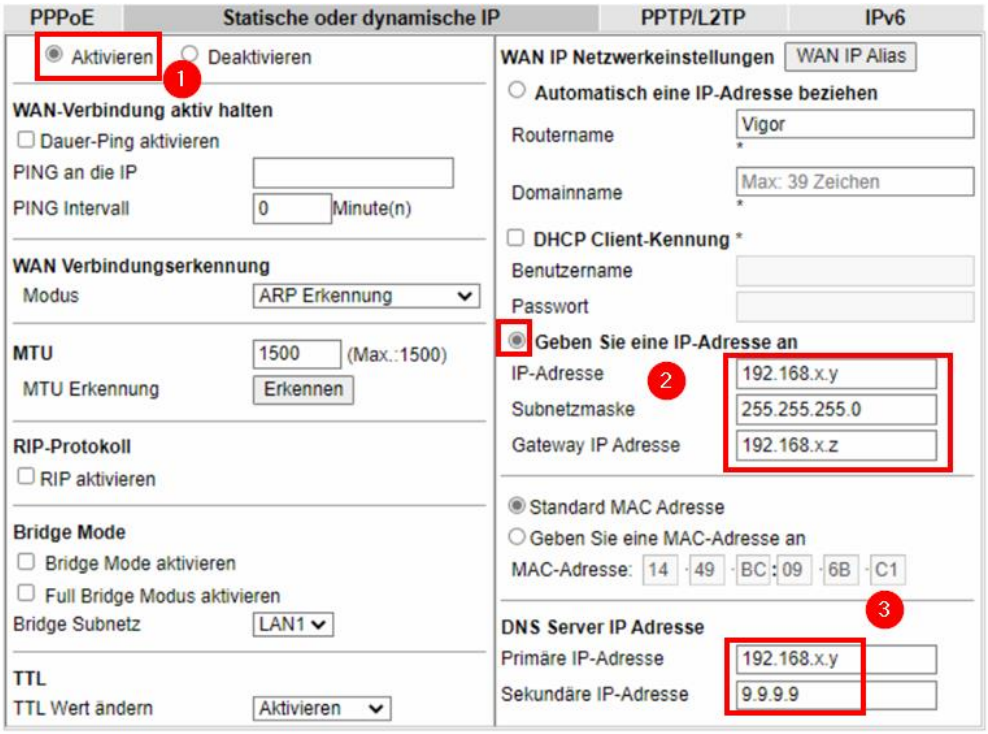
2.2.1 Internetverbindung herstellen

„WAN1“ mit dem Internetzugang der Schule verbinden.

Im Menü „WAN“ - „Interneteinwahl“ wählen.

„WAN 1“ auf „Statische oder dynamische IP“ umstellen (1) und im Anschluss „Details“ wählen (2):

WAN-Schnittstelle aktivieren (1), feste IP-Adresse für die WAN-Schnittstelle (je nach Internetanbindung) (2) sowie den DNS-Server (Router-IP und sekundären DNS z. B. 9.9.9.9) einstellen (3) und mit „OK“ bestätigen:



Hinweis: Je nach Anbieter müssen ggf. noch Anmeldedaten im Reiter „PPPoE“ hinterlegt werden:

Nach der Konfiguration der WAN-Schnittstelle den Router neu starten und die Internetverbindung überprüfen.

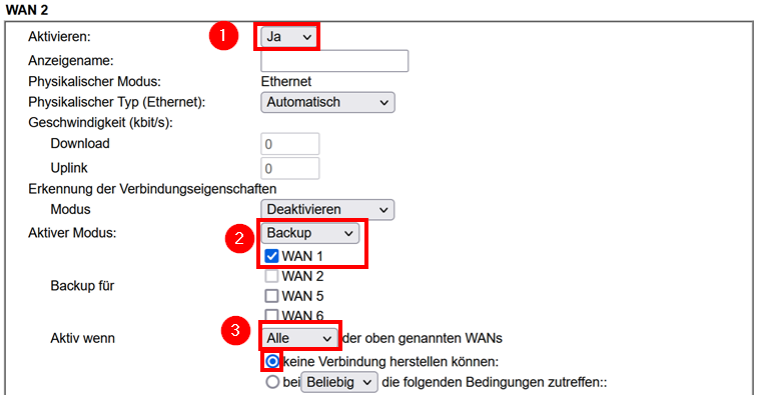
2.2.2 Sekundäre Internetschnittstelle einrichten (optional)

Die zweite WAN-Schnittstelle kann wie die erste Schnittstelle nur als Ethernet-Schnittstelle verwendet werden, eine Einwahl per Modem ist nicht möglich.

Im Menü „WAN“ - „Grundeinstellung“ wählen.

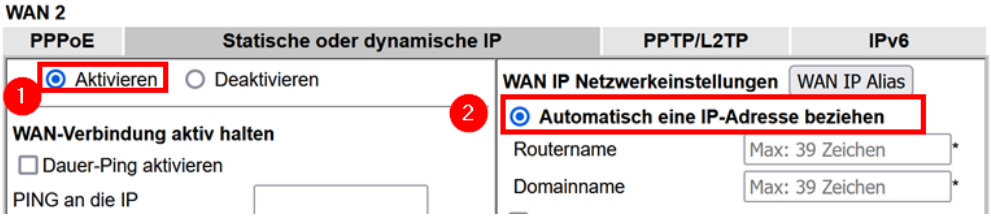
„WAN 2“ wählen:

Die WAN-Schnittstelle aktivieren (1), WAN 1 als Backup einstellen (2), Option „Aktiv, wenn alle der oben genannten WANs keine Verbindung herstellen können“ (3) und mit „OK“ bestätigen:

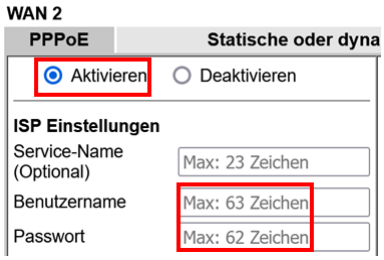


Im Menü „WAN“ - „Interneteinwahl“ – „Details“ für WAN 2 wählen.

Dort die Schnittstelle aktivieren und die IP-Adresse automatisch beziehen (2) bzw. nach Vorgabe des Providers einrichten:



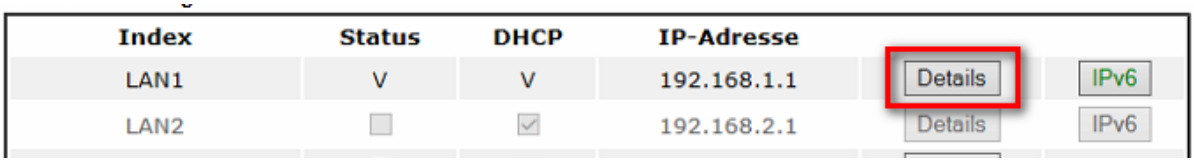
Hinweis: Je nach Anbieter müssen ggf. noch Anmeldedaten im Reiter „PPPoE“ hinterlegt werden:



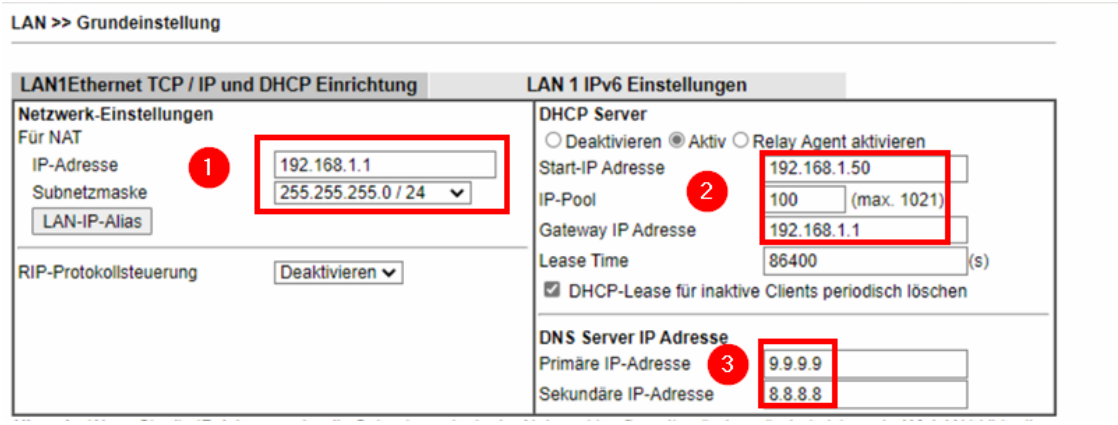
2.3 LAN-Schnittstelle konfigurieren

Im Menü „LAN“ - „Grundeinstellung“ wählen.

Für „LAN1“ „Details“ wählen:



Die feste IP-Adresse 192.168.1.1 für die LAN-Schnittstelle (Admin-Netz) belassen (1), DHCP auf 192.168.1.50-150, Gateway auf 192.168.1.1 (2) und DNS-Server auf 9.9.9.9 und 8.8.8.8 einstellen (3). Abschließend mit „OK“ bestätigen:



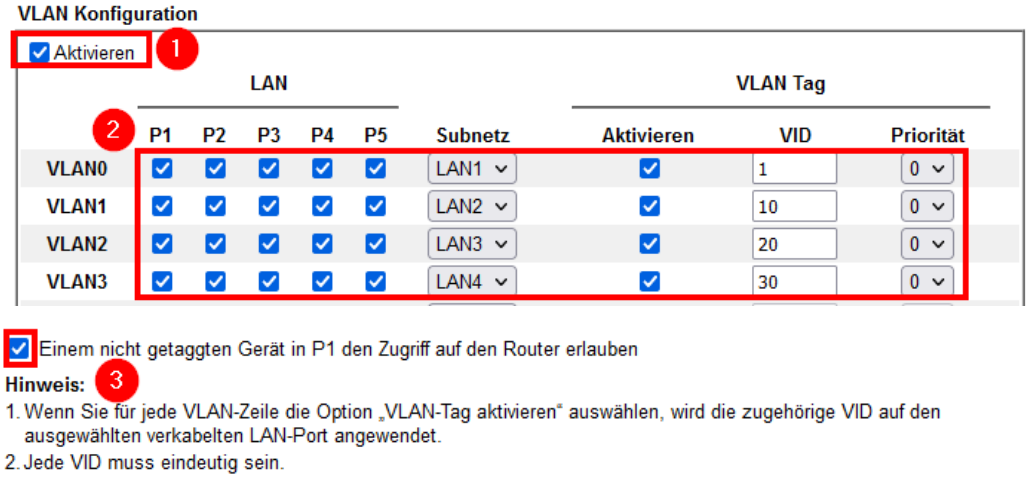
Wichtig: Wenn sich zwischen Internetanschluss und Draytek-Router ein weiterer Router (z. B. eine Fritzbox) befindet, muss - wie oben im Beispiel gezeigt - eine öffentliche IP-Adresse (z. B. 9.9.9.9 oder 8.8.8.8) als DNS-Server verwendet werden. Andernfalls kann auch die IP-Adresse des Draytek-Routers (192.168.1.1) als DNS-Server verwendet werden.

2.4 Weitere Netzwerke konfigurieren

Wichtig: Bevor die folgenden Schritte durchgeführt werden, sollte überprüft werden, ob das Admin-Endgerät, mit dem diese Einstellungen vorgenommen werden, am Router-Port 1 angeschlossen ist. Nur an diesem Port erhält man nach Aktivierung der VLANs noch eine ungetaggte Verbindung zum Router.

Im Menü „LAN“ - „VLAN“ wählen.

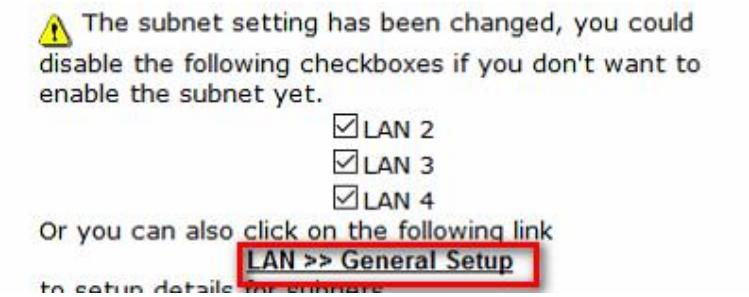
VLAN aktivieren (1) und folgende Port-Einstellungen vornehmen (2+3):



Hinweis: Das native Netz (VLAN-ID 1/LAN1) ist für die Geräte wie Access Points, Switches, Router usw. vorgesehen, das VLAN1/LAN2 ist für die schuleigenen Endgeräte für Schülerinnen

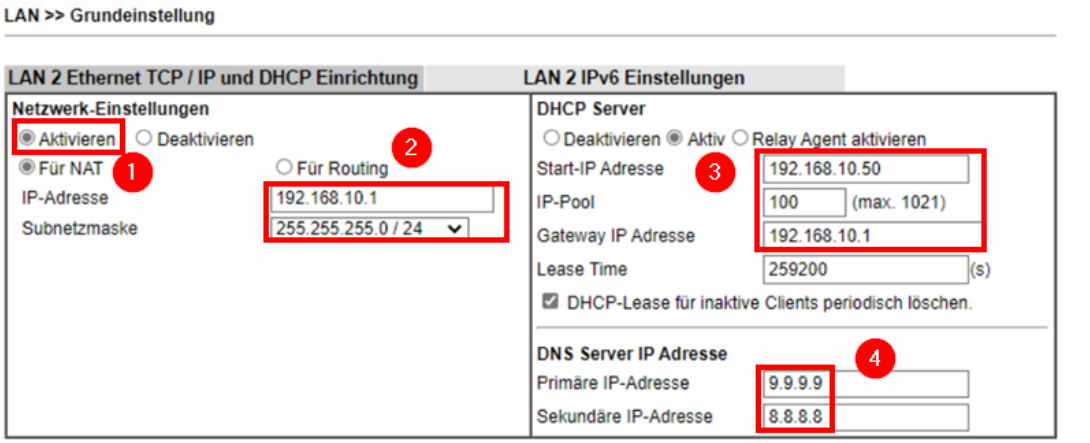
und Schüler, das VLAN2/LAN3 für die Dienstgeräte der Lehrkräfte und das VLAN3/LAN4 für die privaten Endgeräte vorgesehen.

Mit „OK“ bestätigen und im anschließenden Hinweis auf „LAN >> Grundeinstellung“ klicken:



In den LAN-Einstellungen (im Menü unter „LAN“ – „Grundeinstellung“) für LAN2 „Details“ wählen.

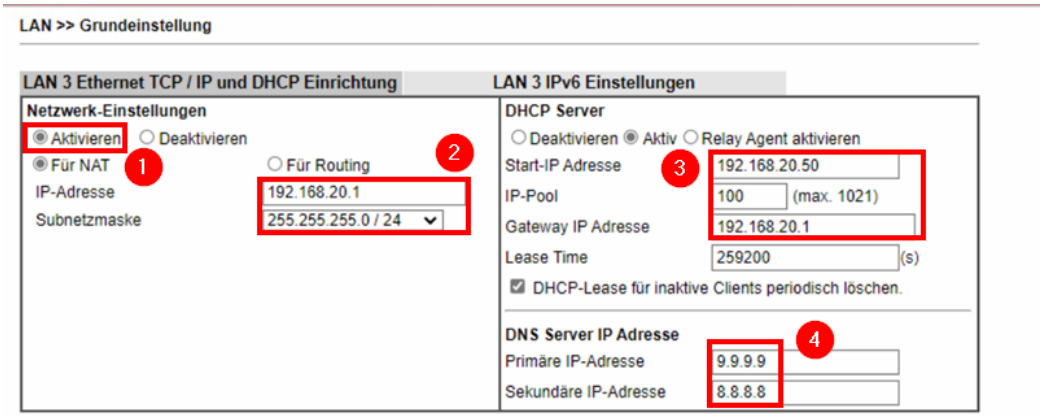
LAN2 – das **Netz für schuleigene Endgeräte von Schülerinnen und Schülern** – aktivieren (1), die IP-Adresse auf 192.168.10.1 (2) anpassen, DHCP auf 192.168.10.50-150, Gateway auf 192.168.10.1 (3) und DNS-Server auf 9.9.9.9 und 8.8.8.8 einstellen (4). Abschließend mit „OK“ bestätigen:



Wichtig: Wenn sich zwischen Internetanschluss und Draytek-Router ein weiterer Router (z. B. eine Fritzbox) befindet, muss - wie oben im Beispiel gezeigt - eine öffentliche IP-Adresse (z. B. 9.9.9.9 oder 8.8.8.8) als DNS-Server verwendet werden. Andernfalls kann auch die IP-Adresse des Draytek-Routers (192.168.10.1) als DNS-Server verwendet werden.

Im Menü unter „LAN“ – „Grundeinstellung“ für LAN3 „Details“ wählen.

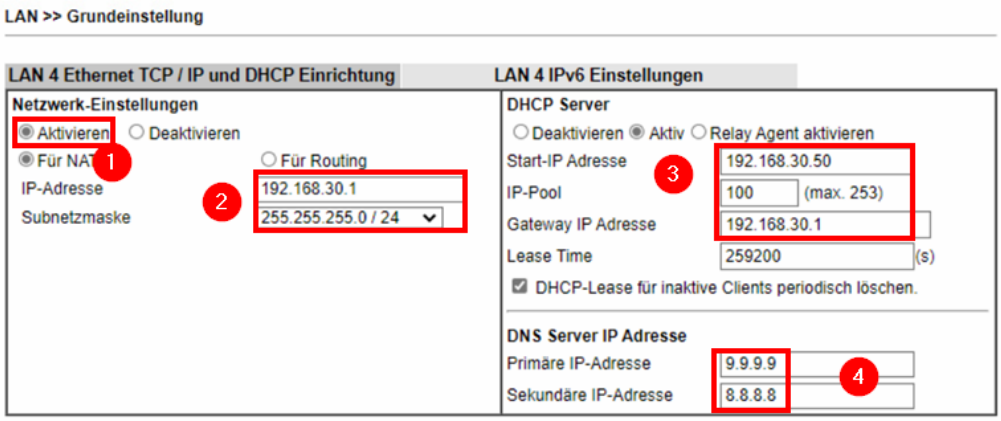
LAN3 – das **Netz für Dienstgeräte der Lehrkräfte** – aktivieren (1), die IP-Adresse auf 192.168.20.1 (2) anpassen, DHCP auf 192.168.20.50-150, Gateway auf 192.168.20.1 (3) und DNS-Server auf 9.9.9.9 und 8.8.8.8 einstellen (4). Abschließend mit „OK“ bestätigen:



Wichtig: Wenn sich zwischen Internetanschluss und Draytek-Router ein weiterer Router (z. B. eine Fritzbox) befindet, muss - wie oben im Beispiel gezeigt - eine öffentliche IP-Adresse (z. B. 9.9.9.9 oder 8.8.8.8) als DNS-Server verwendet werden. Andernfalls kann auch die IP-Adresse des Draytek-Routers (192.168.20.1) als DNS-Server verwendet werden.

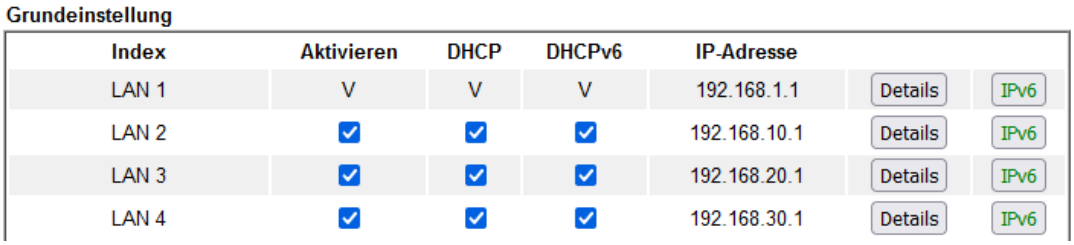
Im Menü unter „LAN“ – „Grundeinstellung“ für LAN4 „Details“ wählen.

LAN4 – das **Netz für private Endgeräte** – aktivieren (1), die IP-Adresse auf 192.168.30.1 (2) anpassen, DHCP auf 192.168.30.50-150, Gateway auf 192.168.30.1 (3) und und DNS-Server auf 9.9.9.9 und 8.8.8.8 einstellen (4). Abschließend mit „OK“ bestätigen:

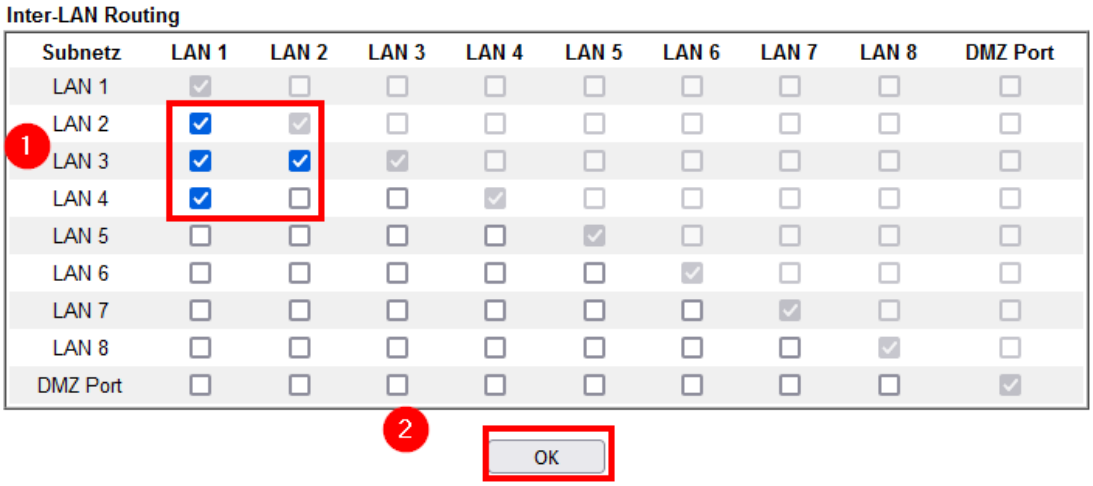


Wichtig: Wenn sich zwischen Internetanschluss und Draytek-Router ein weiterer Router (z. B. eine Fritzbox) befindet, muss - wie oben im Beispiel gezeigt - eine öffentliche IP-Adresse (z. B. 9.9.9.9 oder 8.8.8.8) als DNS-Server verwendet werden. Andernfalls kann auch die IP-Adresse des Draytek-Routers (192.168.30.1) als DNS-Server verwendet werden.

Erneut im Menü auf „LAN“ und „Grundeinstellung“ wechseln. Es sollten nun folgende Netze aktiviert sein:



Es soll eine Kommunikation zwischen LAN1 und allen anderen Netzen sowie zwischen LAN2 (schuleigene Endgeräte der Schülerinnen und Schüler) und LAN3 (Dienstgeräte der Lehrkräfte) möglich sein. Dazu müssen unter „LAN“ und „Grundeinstellung“ für die Einstellungen „Inter-LAN Routing“ folgende Häkchen gesetzt werden (1) und mit „OK“ (2) bestätigt werden:

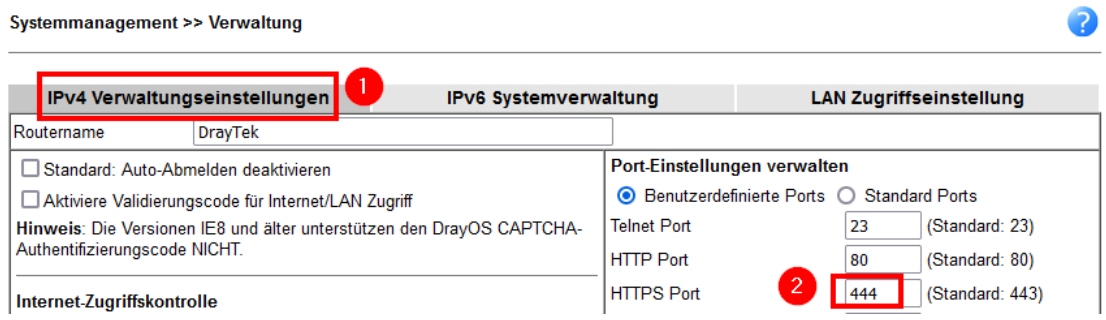


Hinweis: Es ist nun z.B. ein Zugriff auf den Controller (LAN1) und damit die Nutzung des Gastportals aus dem Netz LAN4 möglich oder die Nutzung der Datenablage (LAN2) aus dem Netz LAN3.

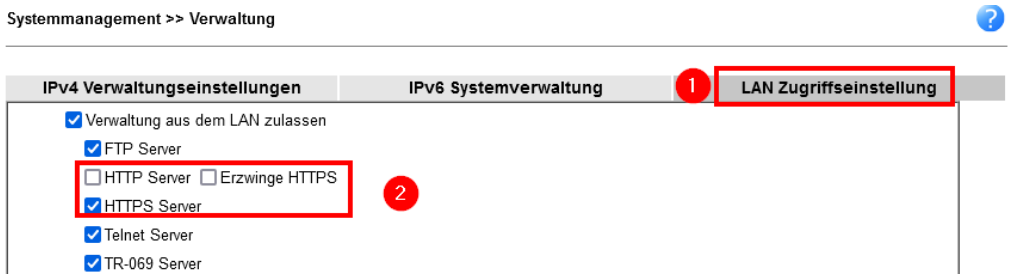
2.5 HTTPS-Port ändern und Webinterface auf HTTPS umleiten

Hinweis: Die Weboberfläche des Draytek-Routers soll immer auf HTTPS umgeleitet werden. Da der Port 443 im nächsten Kapitel für die Portweiterleitung auf die Datenablage benötigt wird, soll zudem der Standard-HTTPS-Port auf 444 geändert werden.

Im Hauptmenü „Systemmanagement“ - „Verwaltung“ wählen und dort im Reiter „IPv4 Verwaltungseinstellungen“ (1) den HTTPS-Standard-Port auf 444 abändern (2):



Im Reiter „LAN Zugriffseinstellung“ (1) die Häkchen für „HTTP Server“ und „Erzwinge HTTPS“ entfernen (2):



Beide Einstellungen mit „OK“ bestätigen.

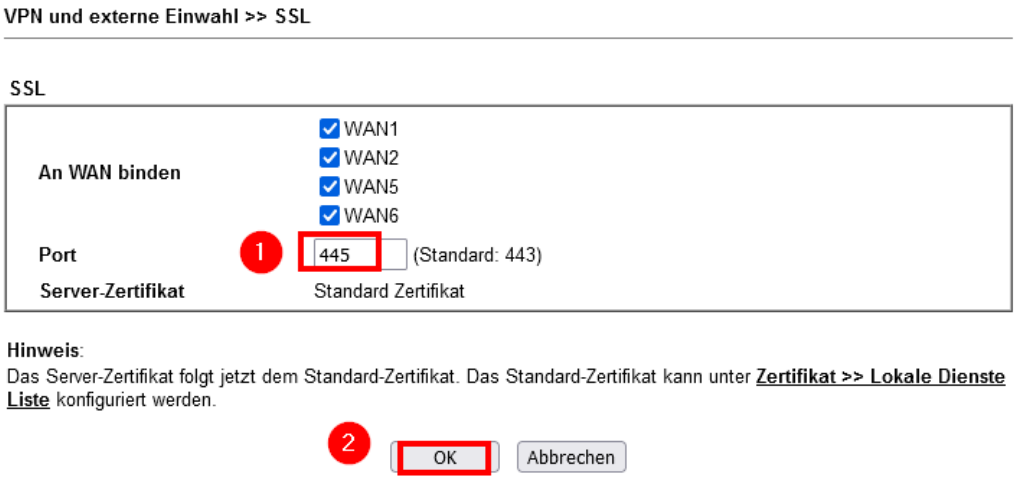
Im Anschluss den Router neu starten.

Hinweis: Der Aufruf der Administrationsoberfläche funktioniert nun nur noch per HTTPS und Portangabe: https://192.168.1.1:444. Sollte der Aufruf nicht funktionieren, sollte der Router nochmals über den An- und Ausschalter am Gerät neu gestartet werden.

2.6 Portweiterleitung einrichten

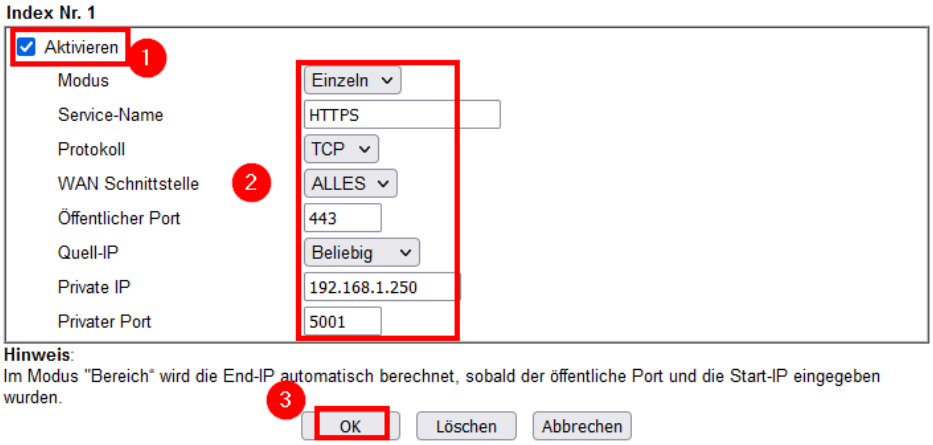
Damit die NAS der Musterlösung (Synology-Diskstation) von außen erreichbar ist, soll eine Weiterleitung von Port 443 auf die IP-Adresse der NAS (192.168.1.250) und den verwendeten Port 5001 eingerichtet werden. Zusätzlich soll zur Nutzung des Protokolls WebDAV auch eine Weiterleitung für den Port 5006 eingerichtet werden.

Da der Port 443 bereits für den SSL-VPN-Zugang verwendet wird, muss dieser zunächst auf einen anderen Port umgestellt werden. Dazu im Menü auf „VPN und externe Einwahl“ – „SSL““ wechseln, Port auf „445“ ändern (1) und mit „OK“ bestätigen (2):



Im Abschluss im Hauptmenü „NAT“ - „Portumleitung“ wählen und dort per Klick auf „1.“ Eine neue Regel anlegen:

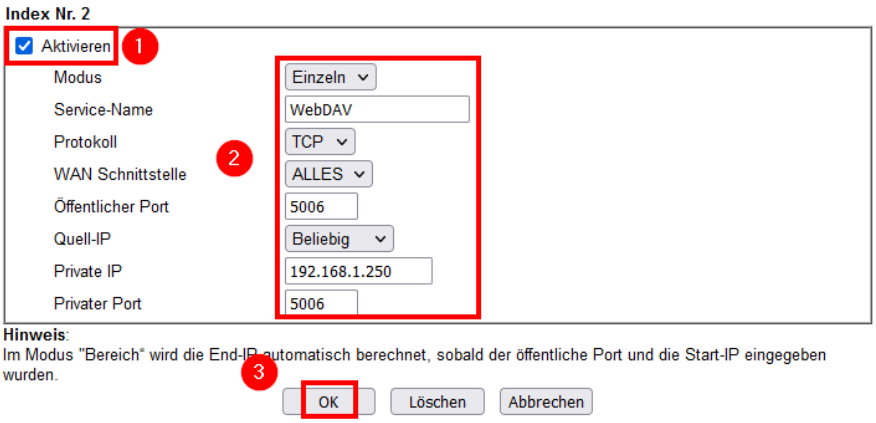
Regel aktivieren (1), mit „HTTPS“ benennen, folgende Einstellungen vornehmen (2) und mit „OK“ bestätigen (3):



Hinweis: Bei Aufruf der öffentlichen IP der Schule bzw. der DDNS-Hostadresse sollte man nun auf das Webinterface der Datenablage (192.168.1.250:5001) weitergeleitet werden.

Im Abschluss über „NAT“ - „Portumleitung“ und dort per Klick auf „2.“ eine weitere Regel anlegen:

Regel aktivieren (1), mit „WebDAV“ benennen, folgende Einstellungen vornehmen (2) und mit „OK“ bestätigen (3):



Hinweis: Ordner auf der Datenablage lassen sich nun mit Hilfe des WebDAV-Protokolls auf Endgeräten einbinden.

2.7 Zeitzone einstellen

Im Menü dazu „Systemmanagement“ - „Uhrzeit und Datum“ wählen.

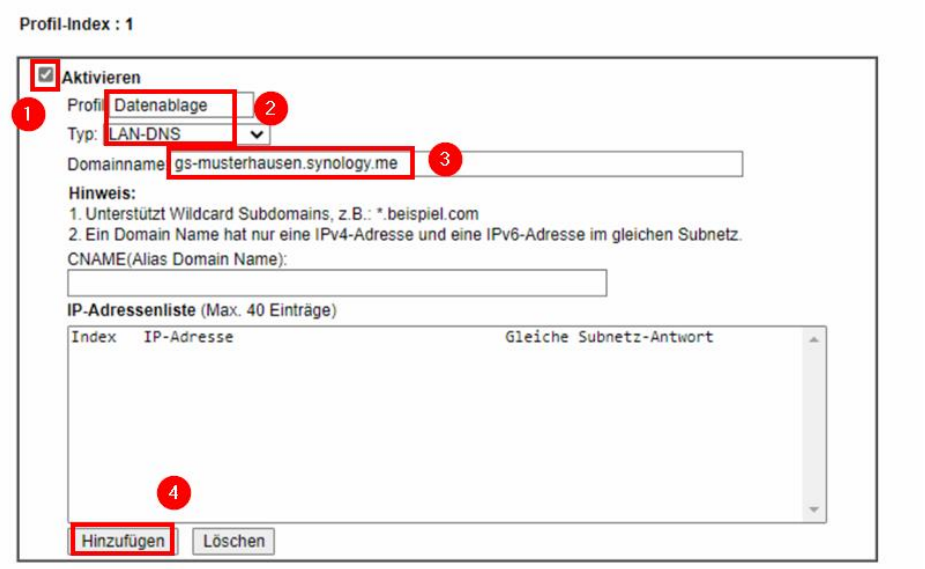
Folgende Einstellungen (1-3) vornehmen und mit „OK“ bestätigen (4):

2.8 Internen DNS-Eintrag anlegen

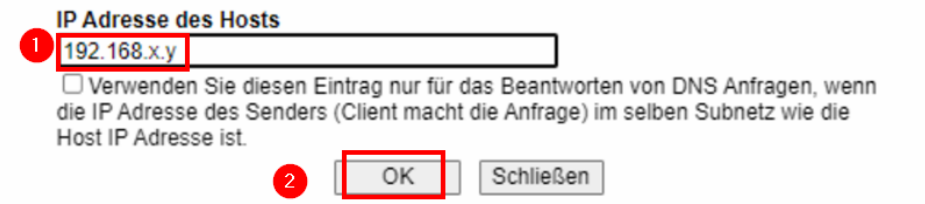
Hinweis: Wenn für die oben eingerichteten LAN-Schnittstellen als primärer DNS-Server die IP-Adresse des Routers genutzt wird (siehe Kapitel LAN-Schnittstelle konfigurieren), muss wie nachfolgend beschrieben ein interner DNS-Eintrag angelegt werden, damit man auch innerhalb des Unterrichtsnetzes auf die öffentliche Webadresse der Datenablage zugreifen kann. Sind als primärer und sekundärer DNS öffentliche IP-Adresse (z.B. 9.9.9.9 und 8.8.8.8) eingerichtet, so ist diese Einstellung nicht notwendig.

Dazu im Menü „Anwendungen“ – „LAN-DNS / DNS Weiterleitung“ auswählen und unter „Index“ den ersten Eintrag öffnen:

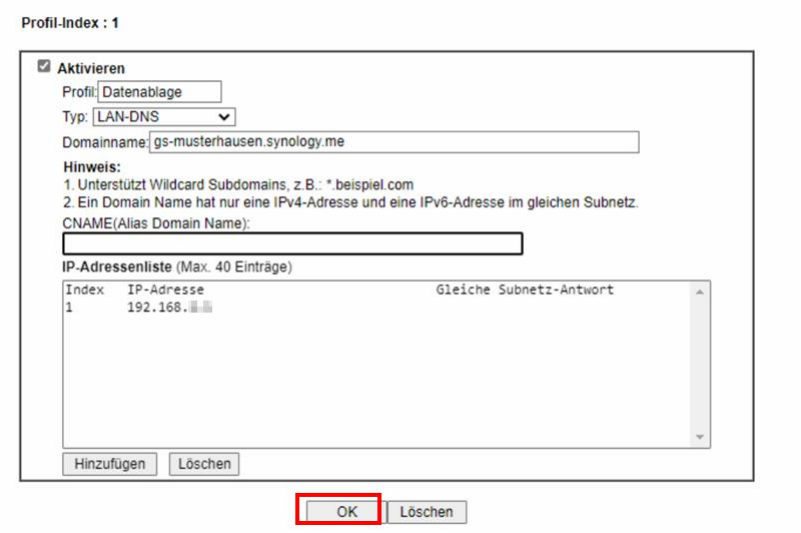
Den Eintrag aktivieren (1), einen Profilnamen vergeben und Typ „LAN DNS“ belassen“ (2), als Domain-Namen die Webadresse der unterrichtlichen Datenablage (xyz.synology.me) eingeben (3) sowie mit „Hinzufügen“ (4) die Maske für den IP-Adresseneintrag öffnen:



Als IP-Adresse die WAN-Adresse des Draytek-Routers eintragen (1) und mit „OK“ (2) bestätigen:



Danach den angelegten internen DNS-Eintrag mit „OK“ bestätigen:



Im Anschluss innerhalb des Unterrichtsnetzes den browserbasierten Zugriff über die oben verwendete Adresse auf die Datenablage überprüfen.

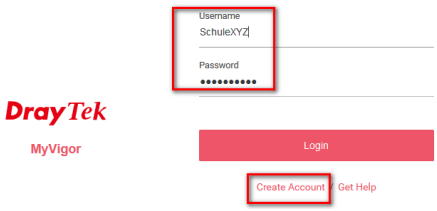
2.9 Internetfilterung einrichten

Wird der Breitbandanschluss des Landes nicht genutzt, soll der Jugendmedienschutz direkt über den Draytek-Router aktiviert werden. Dazu muss zunächst das Gerät online registriert und eine Filterlizenz erworben werden.

2.9.1 Gerät registrieren

Im Draytek-Menü „Produkt Registrierung“ wählen.

Im Anschluss wird man auf die Webseite https://myvigor.draytek.com weitergeleitet. Dort den Loginnamen und das Passwort eingeben bzw. falls kein Zugang vorhanden über „Create Account“ einen neuen Zugang anlegen:

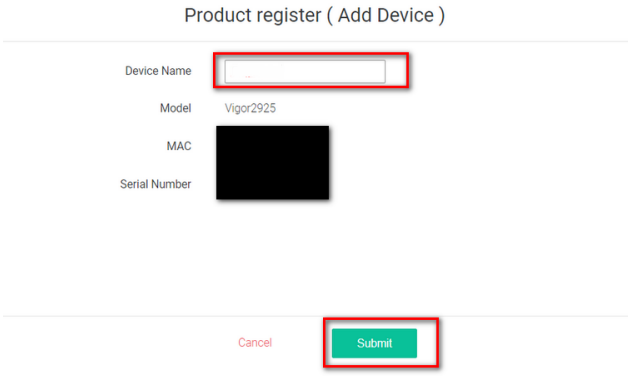


Hinweis: Wenn die Weiterleitung nicht funktioniert ggf. erneut mit einem anderen Browser versuchen.

Die Zugangsdaten in der IT-Dokumentation der Schule vermerken.

Im Menü der Webseite „My Information“ – „My Product“ wählen.

Den neuen Router auswählen, einen Namen für den Router vergeben und mit „Submit“ das Gerät hinzufügen:

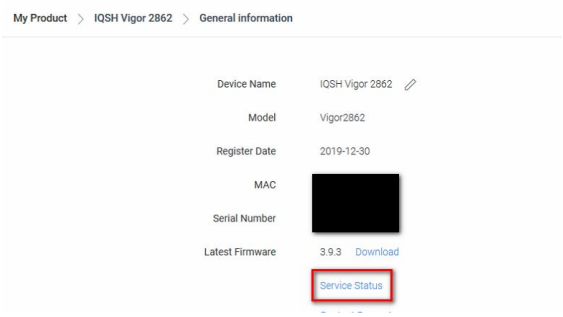


2.9.2 Filterlizenz aktivieren

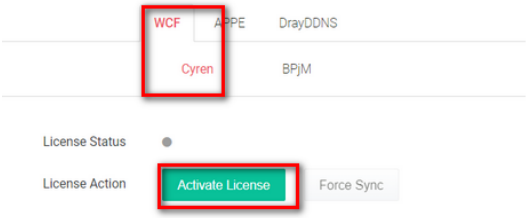
Hinweis: Für die oben genannten Draytek-Modelle wird die Filterlizenz „DrayTek Globalview WCF“ (A Package) benötigt. Sie kostet für die Laufzeit von einem Jahr je nach Anbieter ca. 90 Euro.

Im Menü der Webseite „My Product“ wählen.

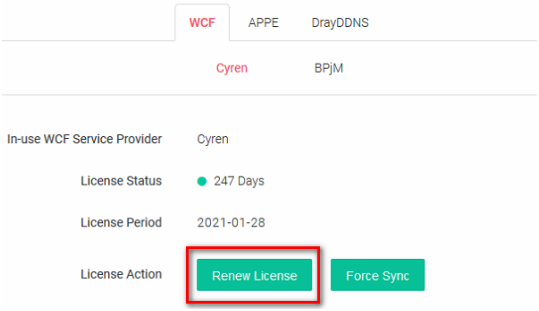
Gerät auswählen und „Service Status“ wählen:



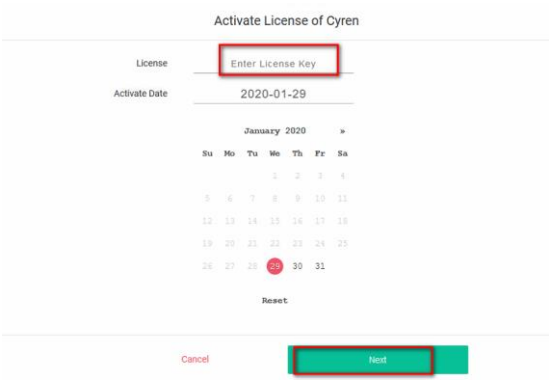
Den Reiter „WCF“ (Web-Content-Filter), den Anbieter „Cyren“ und den Button „Activate License“ wählen:



Hinweis: Bei der ersten Aktivierung erhält man zunächst einen kostenlosen Probemonat. Im Anschluss für die gleiche Lizenz „Renew“ wählen:



Im Anschluss die Lizenznummer eingeben, das vorgeschlagene Aktivierungsdatum (direkt im Anschluss an die Probelizenz) belassen, mit „Next“ bestätigen:

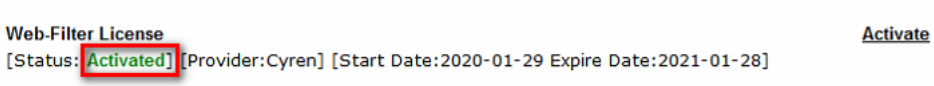


Im Anschluss die Lizenzbedingungen akzeptieren. Es sollte nun neben der Probelizenz auch die noch nicht aktive einjährige Lizenz in der Liste auftauchen.

Zurück auf die Weboberfläche des Routers wechseln.

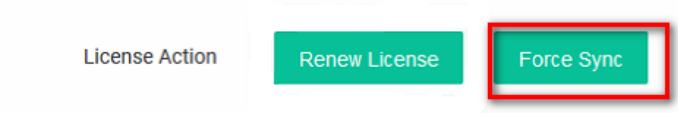
Im Menü „CSM“ – „Web Content Filter“ wählen.

Dort sollte die gekaufte Lizenz nun mit dem Status „Aktiviert“ auftauchen:

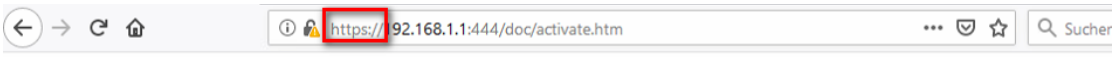


Hinweis: Ist dies nicht der Fall, so kann über den Button „Aktiviert“ erneut die Webseite https://myvigor.draytek.com aufgerufen werden. Im Anschluss dann folgende Schritte durchführen:

- Button „Force Sync“ wählen.



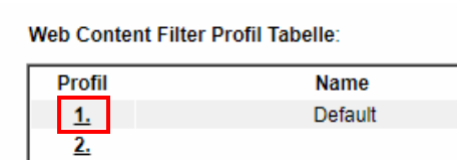
- Es sich öffnet ein neues Browserfenster mit der Bestätigung. Bei bestimmten Firmware-Versionen kann es sein, dass die Seite nicht korrekt geladen wird. In diesem Fall muss der Linkadresse aus der Adresszeile ein „https“ vorweggestellt werden:



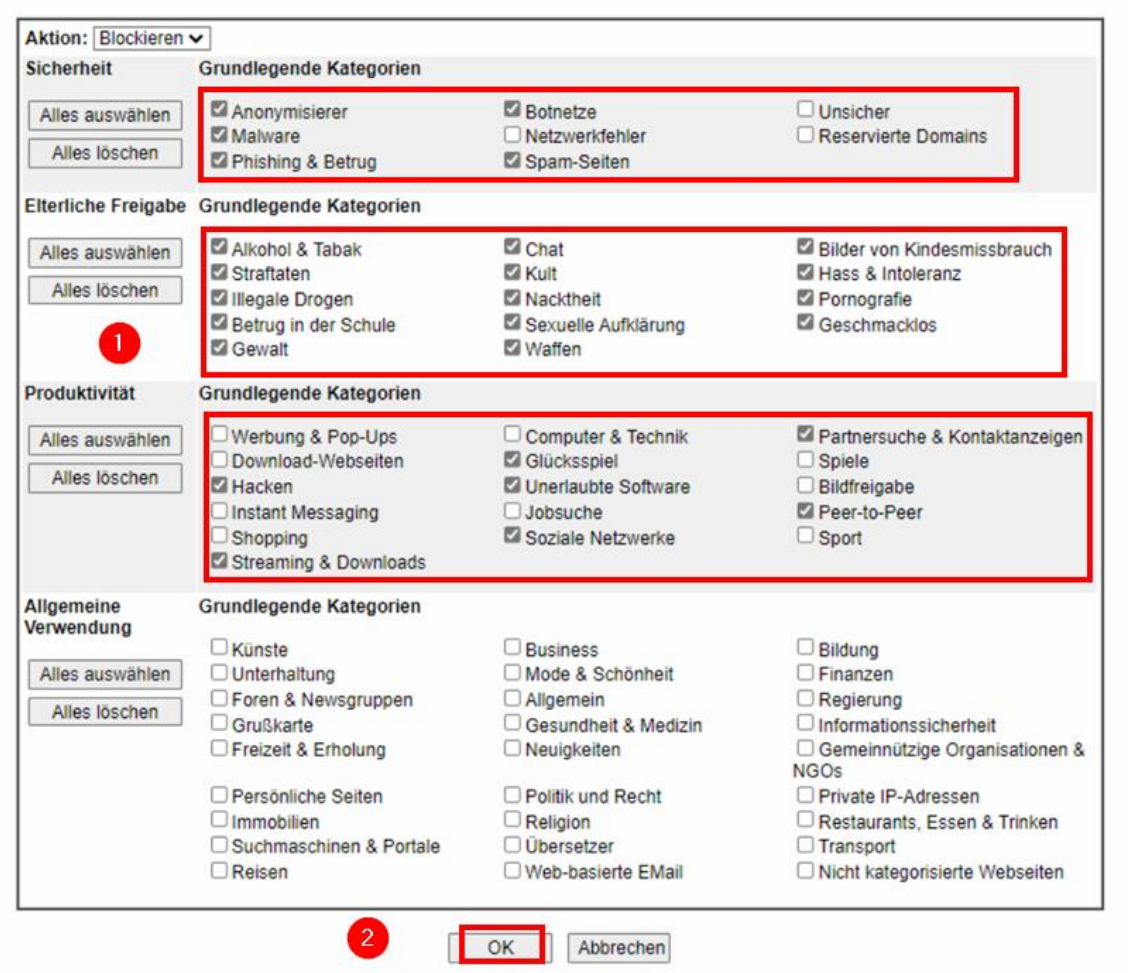
2.9.3 Filtereinstellungen vornehmen

Im Menü des Draytek-Routers „CSM“ - „Web Content Filter“ wählen.

Profil „Default“ wählen:



Folgende Kategorie-Einstellungen vornehmen (1) und mit „OK“ bestätigen (2):

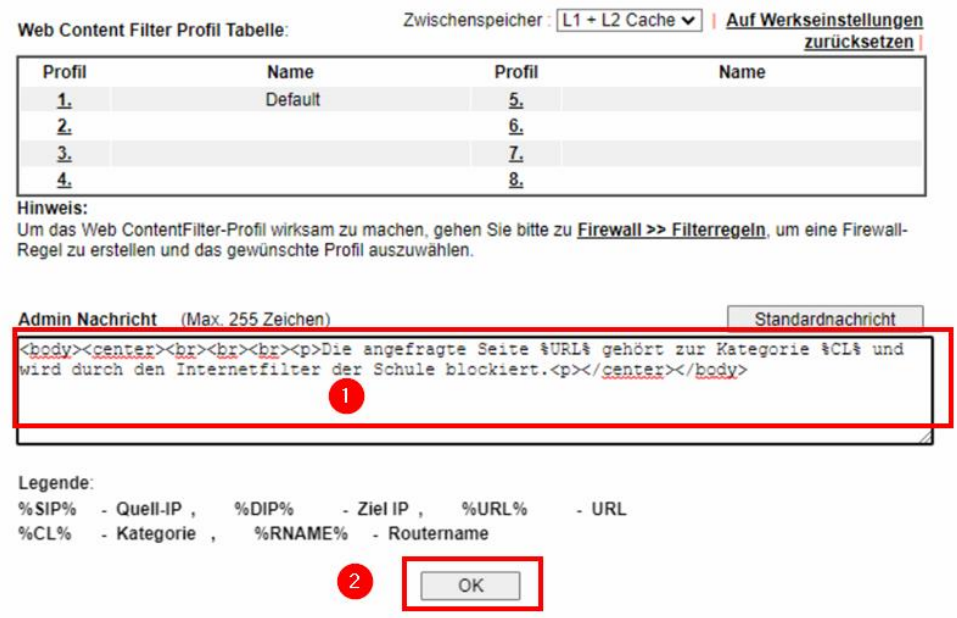


Wichtig: Wird ein Mobile-Device-Management verwendet, verhindert die Sperrung der Kategorie „Streaming & Downloads“ die Verteilung von Apps. In diesem Falle sollte die Kategorie in Absprache mit der Schule freigegeben werden. Alternativ müsste sonst bei jeder Verteilung von Apps die Kategorie kurzzeitig deaktiviert werden.

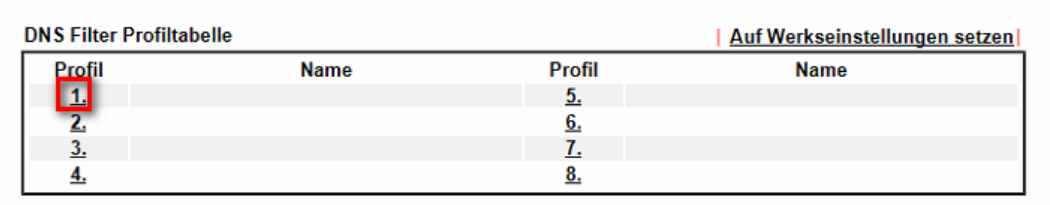
Im Anschluss den Filter-Hinweis des Webcontent-Filters ändern. Dazu folgenden Text kopieren, unter „CSM“ - „Web Content Filter“ in das Feld „Admin Nachricht“ einfügen und im Anschluss mit „OK“ bestätigen:

*<body>

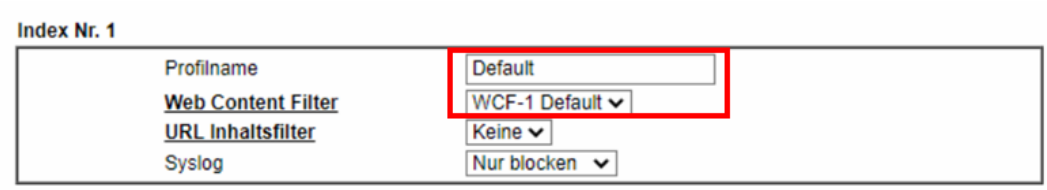
<p>Die angefragte Seite %URL% gehört zur Kategorie %CL% und wird durch den Internetfilter der Schule blockiert.<p> </body>*



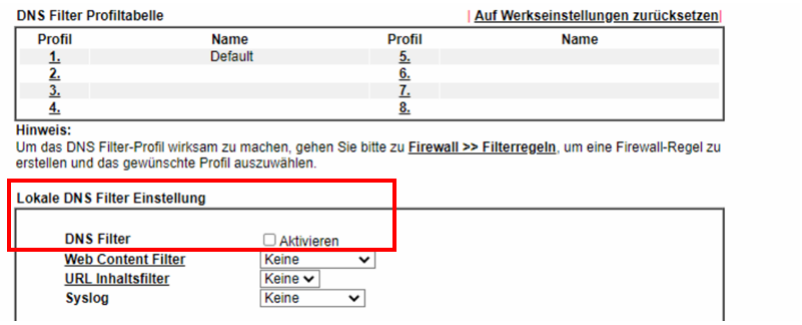
Im Hauptmenü „CSM“ - „DNS Filter“ wählen und dort das Profil 1 wählen:



Als Profilnamen „Default“ wählen, für den Contentfilter „WCF-1 Default“ auswählen und mit „OK“ bestätigen:



In der anschließenden Übersicht zum DNS-Filter unter „CSM“ - „DNS Filter“ überprüfen, ob der lokale DNS-Filter für den Punkt „Lokale DNS Filter Einstellung“ deaktiviert ist:



Im Anschluss den Filter-Hinweis des DNS-Filters ändern. Dazu folgenden Text kopieren, unter „CSM“ - „DNS Filter“ in das Feld „Admin Nachricht“ einfügen (1) und im Anschluss mit „OK“ bestätigen (2):

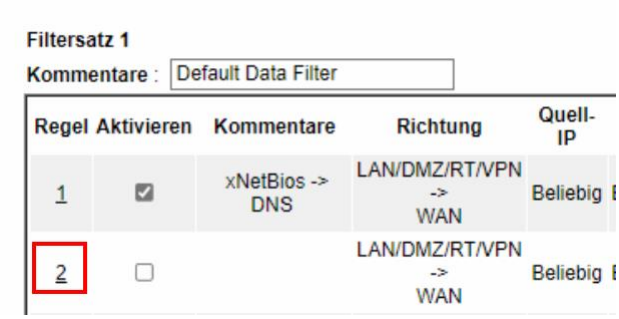
*<body>

<p>Die angefragte Seite %URL% wird durch den Internetfilter der Schule blockiert.<p> </body>*

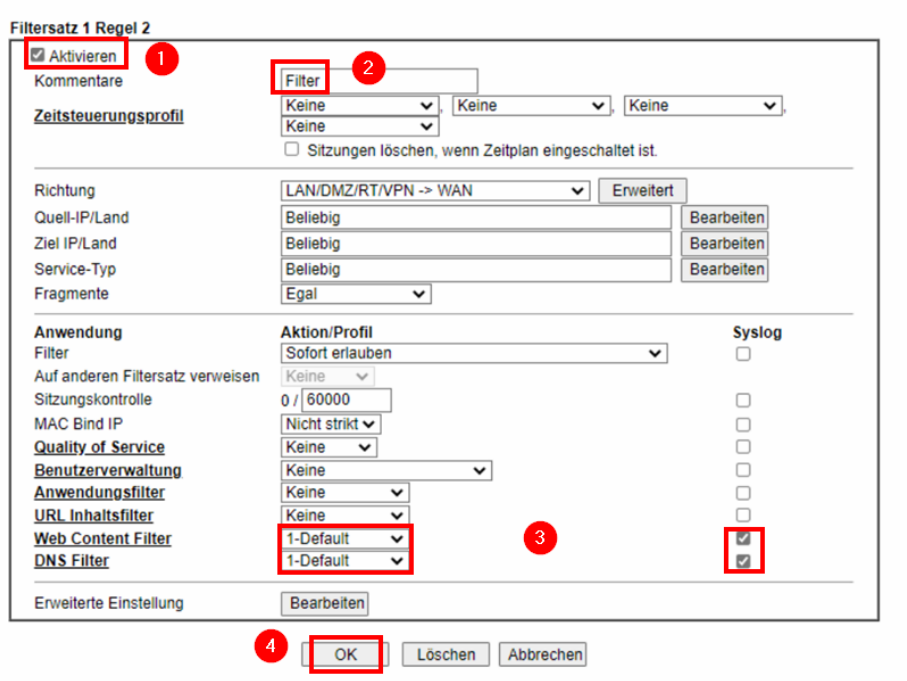
Im Menü „Firewall“ - „Filterregeln“ wählen.

„Default Data Filter“ wählen:

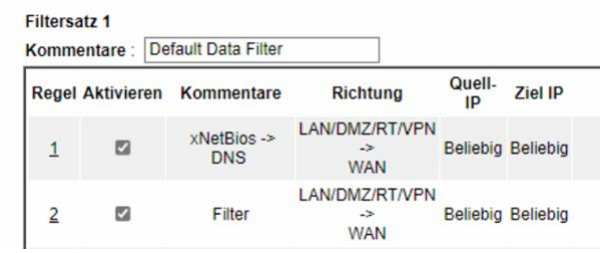
Anschließend Regel „2“ wählen:



Die Regel aktivieren (1), mit „Filter“ benennen (2), Web Content Filter und DNS-Filter jeweils auf „1-Default“ umstellen und Syslog aktivieren (3) sowie mit „OK“ bestätigen (4):



Die Übersicht der Filterregeln sollte nun so aussehen:



Mit „OK“ bestätigen.

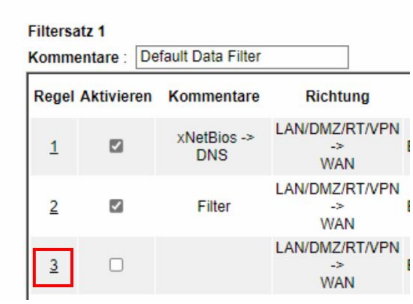
2.9.4 Ungefilterte Netzwerke einrichten

Die Filterung soll lediglich für das Netz für schuleigene Endgeräte der Schülerinnen und Schüler gelten. Alle anderen Netze werden aus der Filterung herausgenommen.

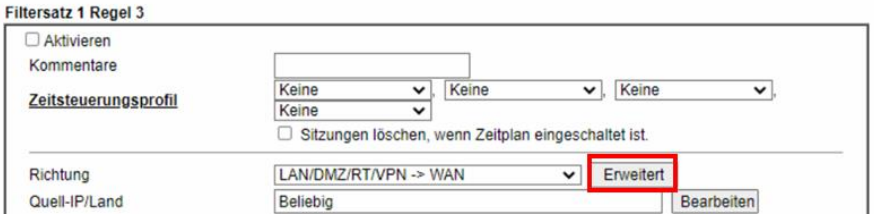
Im Menü „Firewall“ - „Filterregeln“ wählen.

„Default Data Filter“ wählen:

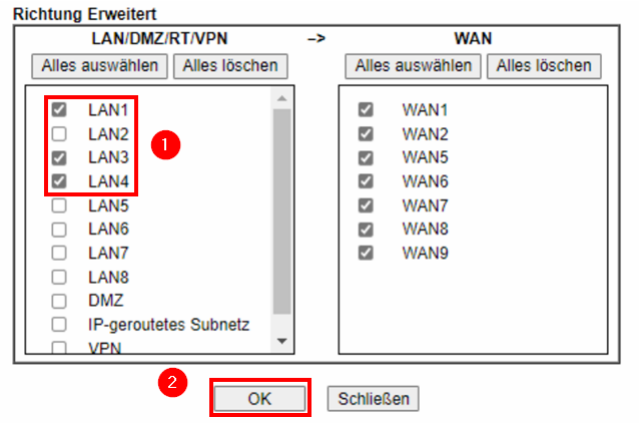
Neue Filterregel wählen:



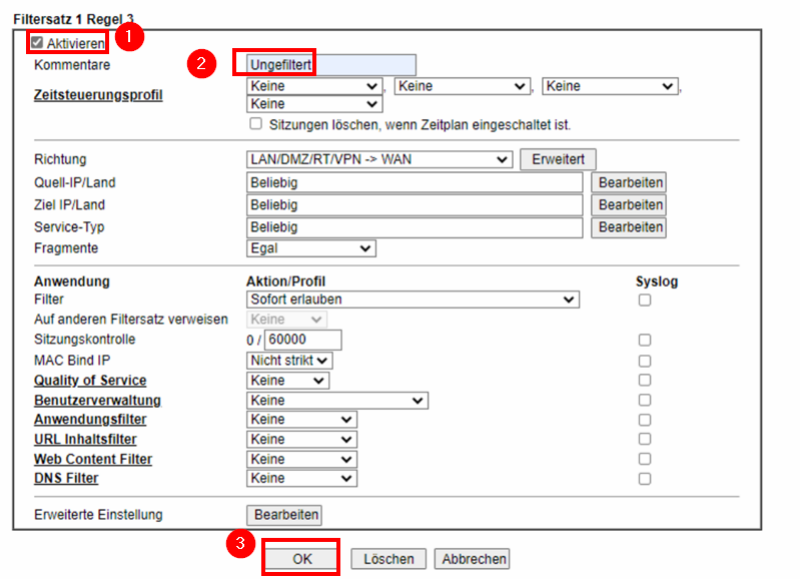
„Erweitert“ wählen:



Als Quelle nur LAN1, LAN3 und LAN4 auswählen (1) und mit „OK“ bestätigen (2):

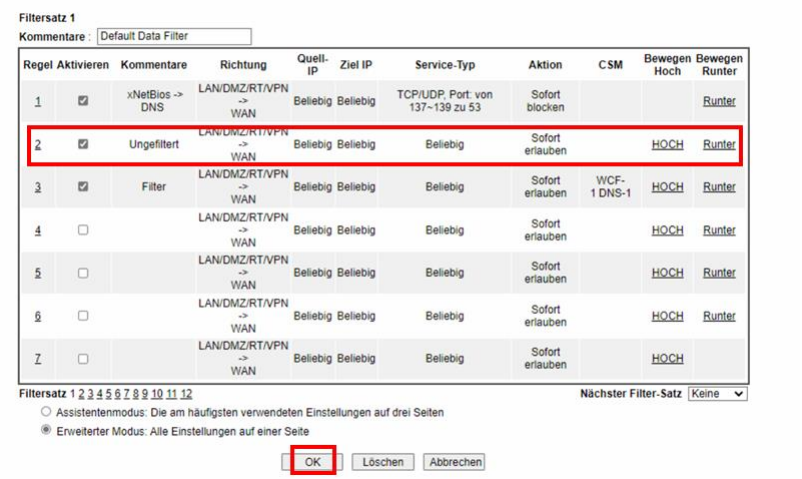


Die Filterregel aktivieren (1), mit „Ungefiltert“ benennen (2) und mit „OK“ bestätigen (3):



Im Anschluss die die Regel „Ungefiltert“ über die Regel „Filter“ verschieben. Dazu für die Regel „Ungefiltert“ auf „HOCH“ klicken:

Danach mit „OK“ bestätigen:



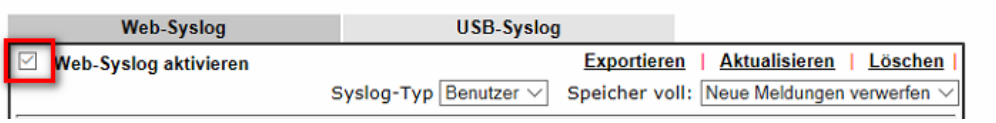
Hinweis: Alle Geräte in den Netzen LAN1, LAN3 und LAN4 sind nun ungefiltert.

2.9.5 Filter-Protokollierung aktivieren (optional)

Hinweis: Bei Aktivierung der Filter-Protokollierung soll dauerhaft ein USB-Stick an den Router angeschlossen werden.

Im Menü „Diagnose“ - „Syslog Explorer“ wählen.

Häkchen für „Enable Web Syslog“ setzen:



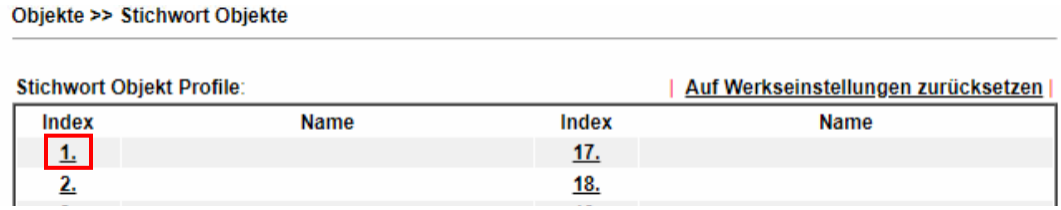
Da der Speicher auf dem Router begrenzt ist, sollen die Protokolldateien automatisch auf einem angeschlossenen USB-Stick abgelegt werden.

Im Menü dazu „Systemmanagement“ - „SysLog/ EMail Alarm“ wählen, SysLog aktivieren (1), USB-Stick als Speicherort mit Speicherobergrenze festlegen (2) und mit „OK“ bestätigen:

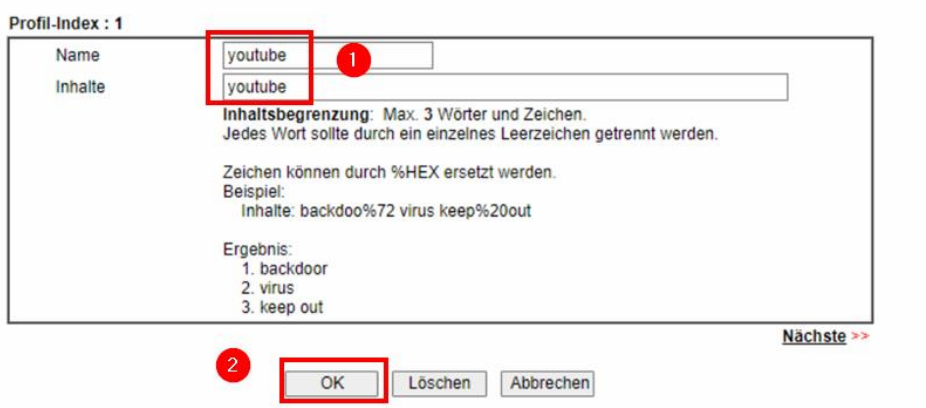
2.9.6 Filterausnahmen hinzufügen (optional)

Soll eine bestimmte Kategorie durch den Webcontent-Filter gesperrt werden, jedoch eine bestimmte Seite aus dieser Kategorie freigegeben werden (zum Beispiel die Seite „youtube.de“ aus der Kategorie „Streaming & Downloads“), kann dies bei Bedarf über eine Filterausnahme ermöglicht werden.

Zunächst ein Keyword-Objekt anlegen. Dazu im Menü „Objekte“ – „Stichwort Objekte“ wählen und dort das erste Profil öffnen:



Einen passenden Namen wählen, Filterbegriff eintragen (1) und mit „OK“ bestätigen:



Hinweis: Beim angegebenen Beispiel werden alle Domains mit dem Filterbegriff „youtube“ (zum Beispiel „youtube.de“, „youtube.com“) zur Ausnahme hinzugefügt. Alternativ kann man als Filterbegriff jedoch auch eine bestimmte Domain (z.B. „youtube.com“) eingeben. In diesem Fall wird dann nur diese Domain bei den Ausnahmen erfasst.

Im Menü „CSM“ - „Web Content Filter“ und dort das Profil „Default“ wählen.

Dort unter „Black/White List“ den Button „Bearbeiten“ wählen:

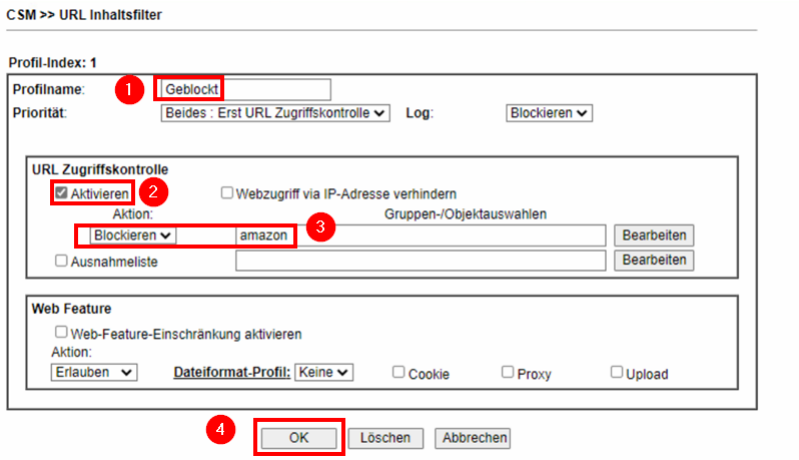
Das vorher angelegte Stichwort-Objekt auswählen und mit „OK“ bestätigen:

Im Anschluss im Bereich „Black/White List“ die Ausnahme aktivieren (1) und je nach Bedarf auf „Erlauben“ oder „Blockieren“ stellen:

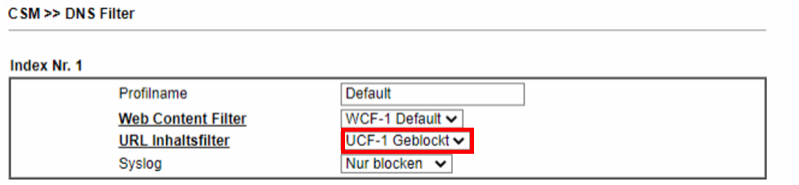
Abschließend mit „OK“ bestätigen. Auch die nachfolgenden beiden Meldungen mit „OK“ bestätigen.

Hinweis: Im angegebenen Beispiel sind alle Seiten der Kategorie „Streaming & Downloads“ gesperrt mit der Ausnahme von Youtube. Es können über weitere Stichwort-Objekte bzw. Stichwort-Gruppen weitere Ausnahmen hinzugefügt werden. Für alle Ausnahmen gilt jedoch entweder „Erlauben“ oder „Blockieren“. Will man jedoch einige Ausnahmen blockieren und andere zulassen, muss man dies über ein zusätzlich angelegtes URL-Filter-Profil regeln:

- Dazu wie oben beschrieben ein weiteres Stichwort-Objekt für die neue Ausnahme (zum Beispiel für das Stichwort „Amazon“) einrichten.
- Im Menü „CSM“ – „URL Inhaltsfilter“ ein neues Profil für das zusätzlich eingerichtete Stichwort-Objekt erstellen (1-3) und mit „OK“ bestätigen (4):



- Unter „CSM“ - „DNS Filter“ – „Default“ das eben eingerichtete URL-Content-Filter-Profil aktivieren und mit „OK“ bestätigen:



Hinweis: Im Beispiel werden nun zusätzlich zu den zugelassenen Youtube-Domains die Domains von Amazon gesperrt.

2.10 VPN-Einrichtung

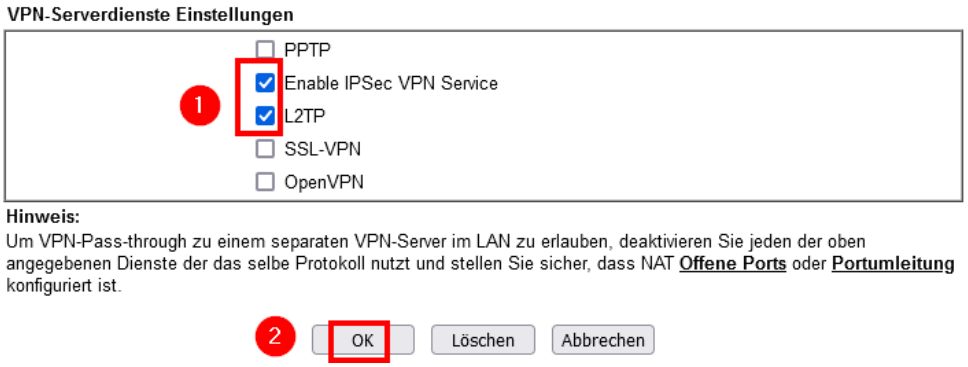
Für Fernwartungszugriffe des Dienstleisters bzw. Schulträgers soll eine VPN-Einwahl in die Schule eingerichtet werden.

Hinweis: Zunächst muss geprüft werden, ob eine VPN-Einrichtung für die vorhandene Internetanbindung möglich ist. Anschlüsse mit DS-Lite-Technik unterstützen VPN zum Beispiel nicht. In diesem Fall kann ggf. als zweite Internetleitung ein kostenloser T@School-Anschluss verwendet werden, um einen VPN-Zugriff zu ermöglichen. Am jeweils verwendeten Router müssen die Ports für VPN freigeben werden: für die verwendete IPSec/L2TP-Lösung sind dies die Ports 500, 1701, 4500 und 8443. Sollte eine VPN-Einrichtung nicht möglich sein, kann ein Außenzugriff über einen Wartungsrechner mit Remotesoftware stattfinden.

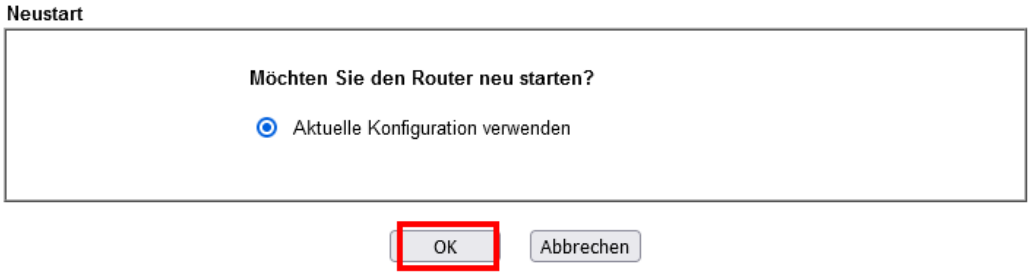
2.10.1 VPN-Einrichtung

Über die Draytek-Weboberfläche (192.168.1.1) einloggen.

Im Menü „VPN und externe Einwahl“ sowie „VPN-Serverdienste“ wählen und dort die Felder „Enable IPsec VPN Service“ und „L2TP“ markieren (1) und mit „OK“ bestätigen (2):

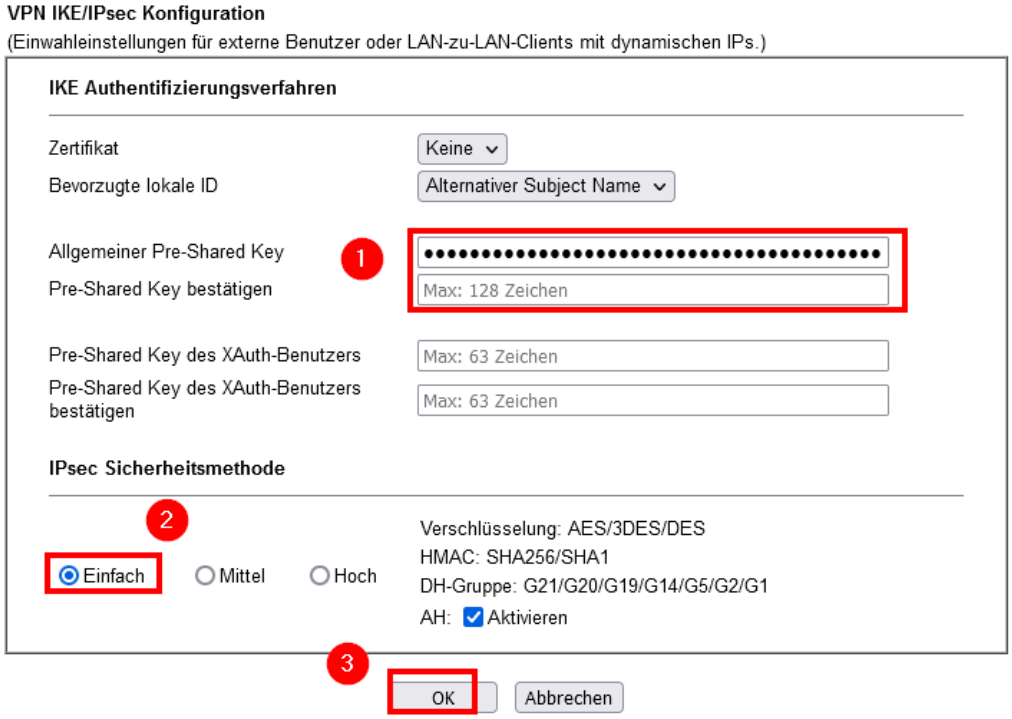


Im Anschluss einen Neustart des Routers bestätigen:



Im Anschluss neu einloggen und im Menü „VPN und externe Einwahl“ und „IPsec“ wählen.

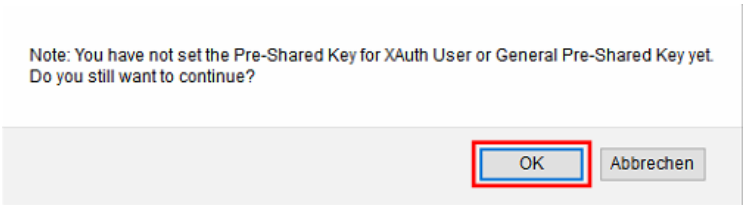
Pre-Shared Key (siehe Hinweis unten) eingeben (1), als Sicherheitsmethode „Einfach“ wählen (2) und mit „OK“ bestätigen (3):



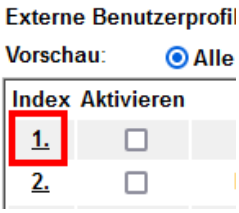
Hinweis: Der Pre-Shared Key muss sowohl dem Server als auch jedem Client, der eine VPN-Verbindung aufbauen will, mitgeteilt werden. Da über diesen Key die gesamte Kommunikation verschlüsselt wird, muss ein sehr sicherer Key gewählt werden. Seiten wie https://www.uni-muenster.de/IT-Sicherheit/passwortgenerator.html berechnen einen Code, der entsprechend sicher ist.

Den vorinstallierten Schlüssel in der IT-Dokumentation der Schule vermerken.

Anschließende Warnung, dass es keinen Key für den XAuth-Nutzer gibt, mit „OK“ bestätigen:

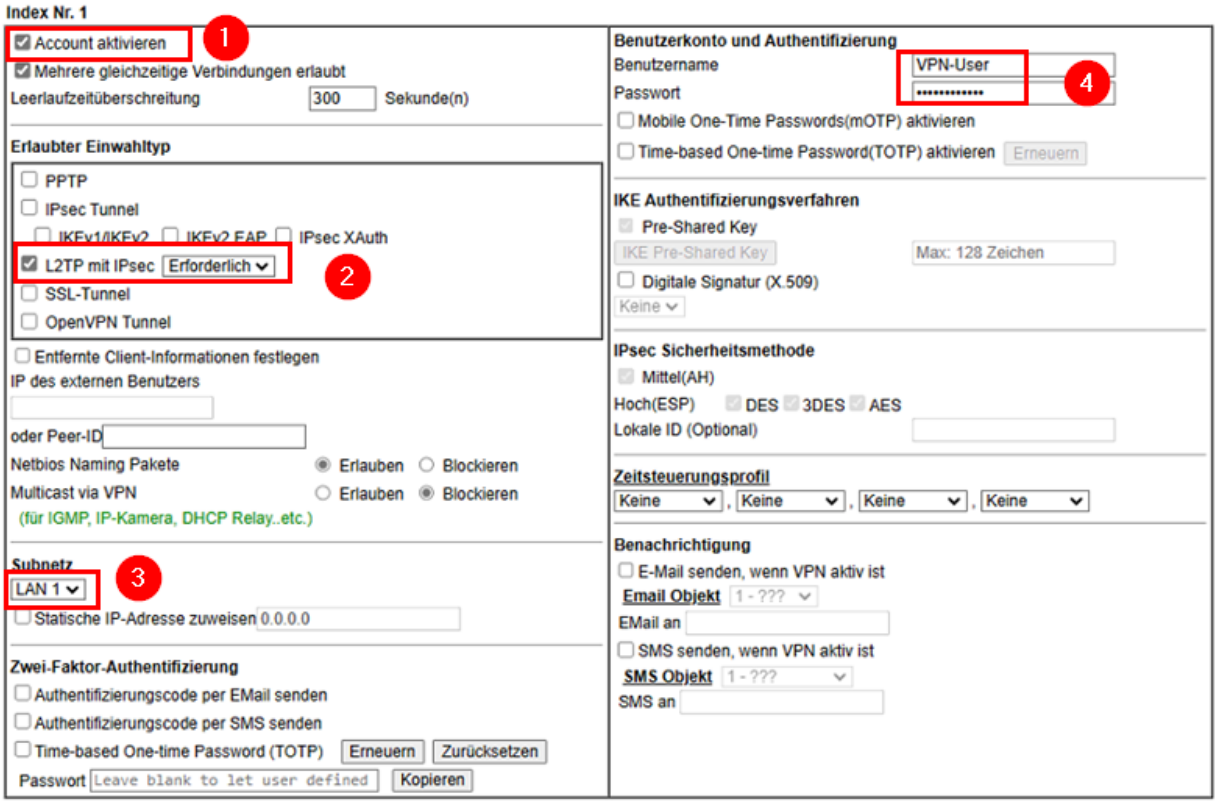


Nutzer für den administrativen VPN-Zugriff erstellen. Dazu im Menü „VPN und externe Einwahl“ sowie „Externe Benutzer“ auswählen und die erste Index-Zahl wählen:



Hinweis: Es sind auch mehrere gleichzeitige VPN-Verbindungen über einen Nutzer-Account möglich.

Das Benutzerkonto aktivieren (1), „L2TP mit IPsec“ auf „Erforderlich“ setzen (2), als Subnetz „LAN1“ auswählen (3) sowie einen individuellen Nutzernamen und ein sicheres Passwort festlegen (4) und mit „OK“ bestätigen:



Im Anschluss alle oben gewählten Zugangsdaten in der IT-Dokumentation der Schule abspeichern.

Hinweis: Sofern auch ein VPN-Zugriff von den dienstlichen Lehrkräfte-Endgeräten ins Unterrichtsnetz ermöglicht werden soll, ein neues gemeinsames Konto für das Kollegium bzw. Einzel-Accounts für Lehrkräfte wie oben gezeigt anlegen. Die Schritte zur VPN-Einrichtung auf dem LK-Endgerät werden in der Anleitung „Musterlösung Grundschule SH_VPN-Verbindung herstellen.pdf“ beschrieben.

2.10.2 Dynamischen DNS-Eintrag erzeugen

Hinweis: Um von außen auf die Schule zugreifen zu können, wird die öffentliche IP-Adresse der Schule benötigt. Da sich diese im Normalfall regelmäßig ändert, muss ein DynDNS-Dienst verwendet werden. Für diese Anleitung wird beispielhaft einer der von Draytek selbst vorgeschlagenen Dienste verwendet. Alternativ wäre auch ein benutzerdefinierter Dienst wie der bereits auf der Datenablage eingerichtete DNS-Dienst von Synology nutzbar.

Wichtig: Wenn ein kostenloser Dienst in Anspruch genommen wird, sollte darauf geachtet werden, dass kein regelmäßiges Update des Accounts erforderlich ist.

Die Schule auf der Webseite www.twodns.de registrieren. Es stehen fünf kostenlose Domains zur Verfügung. Ein späteres Update des Accounts ist nicht erforderlich.

Nach der Registrierung wird eine E-Mail versendet. Dort das Konto durch das Anklicken eines Links final aktivieren.

Im Anschluss auf www.twodns.de einloggen und über „Add new host“ einen passenden Domainnamen (z.B. Beispielschule.dd-dns.de) vergeben und erneut mit „Add new host“ den Vorgang abschließen:

Hinweis: Auf dem Dashboard kann der Status des registrierten Hostnamens angezeigt werden. Zu jedem Hostnamen wird der Name, die aktuell registrierte IP sowie das letzte Update angezeigt.

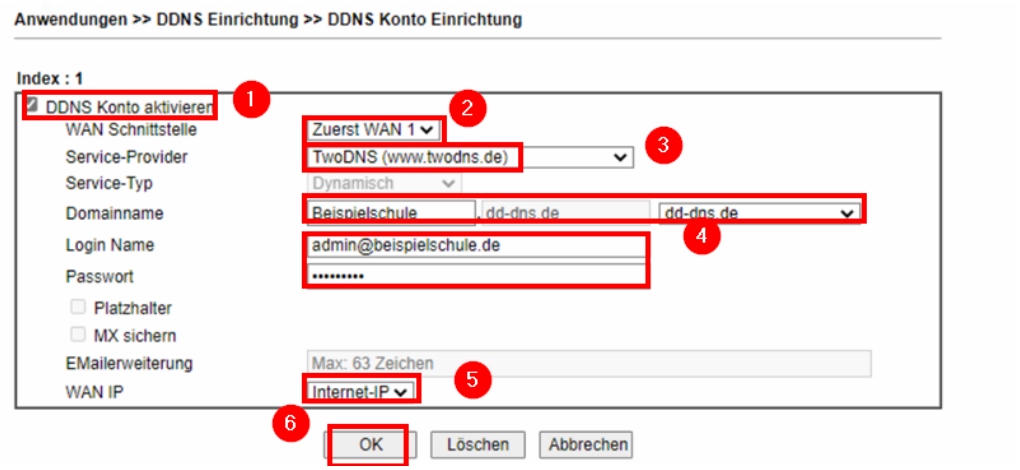
2.10.3 Einrichtung Dyn-DNS Draytek-Router

Login in die Administrationsoberfläche des Draytek-Routers (192.168.10.1).

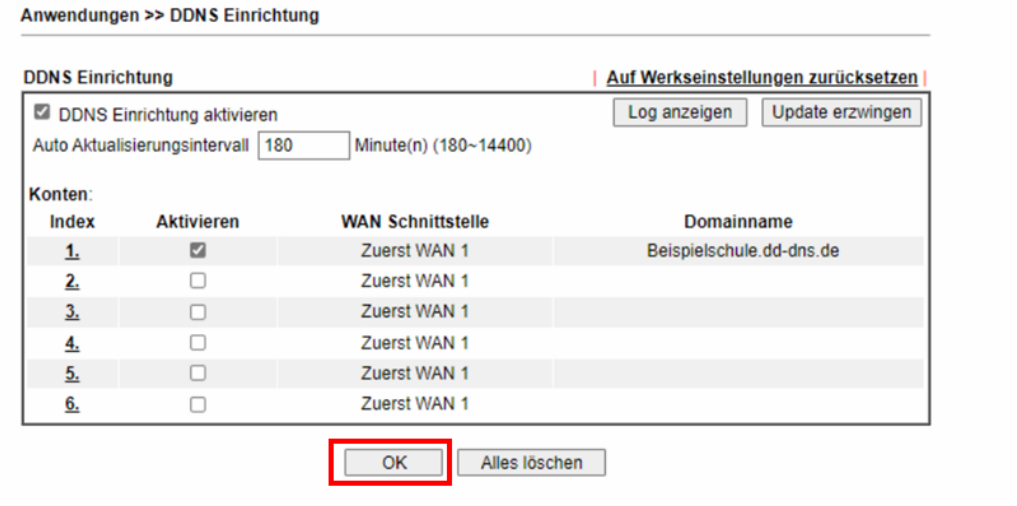
Im Menü „Anwendungen“ und „DDNS“ wählen.

In der Übersicht ein Häkchen für „DDNS Einrichtung aktivieren“ setzen (1), das „Auto-Aktualisierungsintervall“ auf 180 Minuten festlegen (2) und den ersten Listeneintrag wählen (3):

Häkchen für „DDNS Konto aktivieren“ setzen (1), die WAN-Schnittstelle auf „Zuerst WAN1“ einstellen (2), den verwendeten Service-Provider auswählen (3), die Domain- und Zugangsdaten des DynDNS-Anbieters eingetragen (4), „WAN IP“ auf den Wert „Internet IP“ stellen (5) und mit „OK“ bestätigen (6):



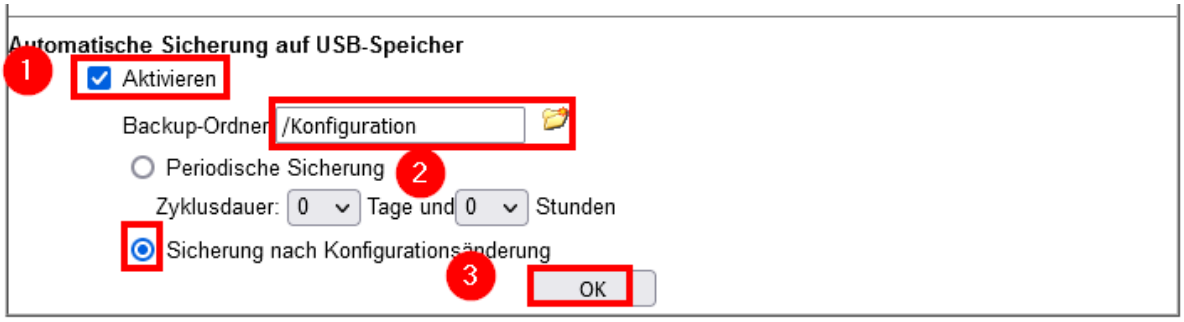
Auf der Übersichtseite der dynamischen DNS-Verwaltung über den Button „OK“ alles final bestätigen:



Auf der Webseite des Dyn-DNS-Anbieters noch überprüfen, ob die aktuelle öffentliche IP-Adresse der Schule übermittelt wurde.

2.11 Router-Konfiguration speichern

Die Konfiguration des Routers soll automatisiert auf einem am Router angeschlossenen USB-Stick gespeichert werden. Im Menü dazu „Systemmanagement“ - „Konfigurationssicherung“ wählen und das Auto-Backup aktivieren (1), folgende Einstellungen vornehmen (2) und mit „OK“ bestätigen (3):



Im Anschluss überprüfen, ob nach Änderung der Konfiguration, diese in einer CFG-Datei im Ordner „Konfiguration“ auf dem USB-Stick abgespeichert wird.

Hinweis: Bei Konfigurationen, die innerhalb derselben volle Stunde vorgenommen werden, wird die vorhandene Konfiguration überschrieben. Für jede spätere Änderung wird eine neue Datei angelegt.

3 Controller einrichten

Hinweis: Die Anleitung bezieht sich auf die Controller-Version ab 7.4.156 und die Firmware-Version ab 3.1.9 für den Cloudkey (2. Generation).

Cloudkey (2. Generation) mit einer Micro-SD-Karte (mind. 8 GB) ausstatten.

Admin-Endgerät und Cloudkey an einen unkonfigurierten UniFi-POE-Switch anschließen.

Hinweis: Router und Access Points werden erst später angeschlossen. Es sollte darauf geachtet werden, dass am Switch kein Gerät angeschlossen ist, das IP-Adressen per DHCP vergibt (z. B. der Router). In diesem Fall ist der Cloudkey dann ggf. nicht mehr unter der unten genannten Adresse erreichbar.

Zunächst für das Admin-Endgerät eine IP aus dem Bereich 192.168.1.x vergeben.

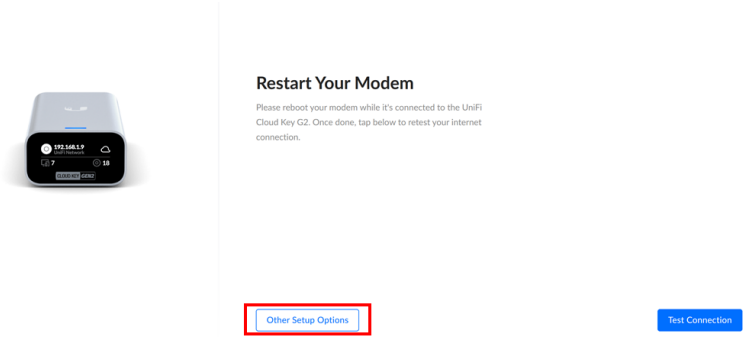
Die Weboberfläche des Cloudkeys aufrufen. Dazu die Startseite (https://192.168.1.30) laden und die Cloudkey-Konfiguration öffnen.

Hinweis: Falls der Cloudkey nicht über 192.168.1.30 erreichbar sein, lässt sich die korrekte IP-Adresse über das Mini-Display auf der Vorderseite des Cloudkey herausfinden.

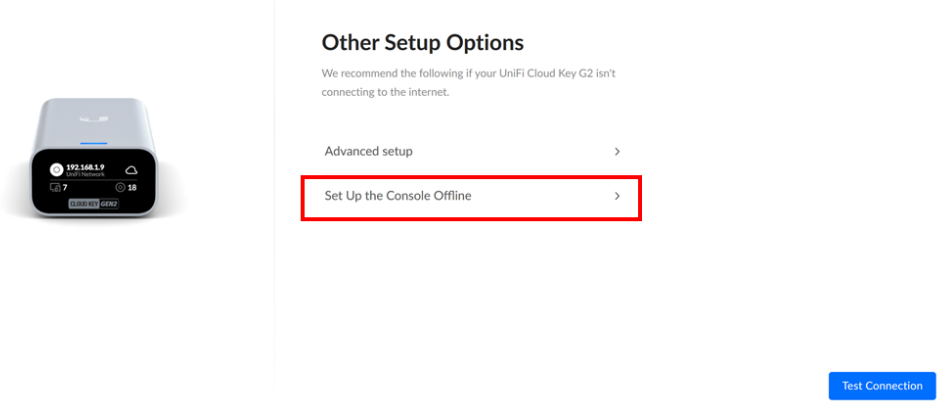
Den Setupprozess über „Setup UCK G2“ starten:

Hinweis: Der Cloudkey versucht zunächst eine Internetverbindung herzustellen. Um die Einrichtung eine UI.com-Accounts und die Cloud-Anbindung des Gerätes zu umgehen, soll zunächst keine Internetverbindung bereitgestellt werden und stattdessen eine **Offline-Einrichtung** vorgenommen werden. Sollte dennoch bereits eine Internetverbindung bestehen, soll die Account-Einrichtung zu Beginn über den Menüpunkt „Proceed without UI-Account“ umgangen werden. Ein Account wird später für die E-Mail-Benachrichtigung (siehe Kapitel E-Mail-Benachrichtigung aktivieren) noch eingerichtet, die Anbindung daran jedoch wieder deaktiviert.

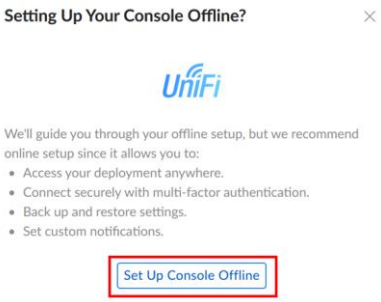
Den Button „Other Setup Options“ wählen:



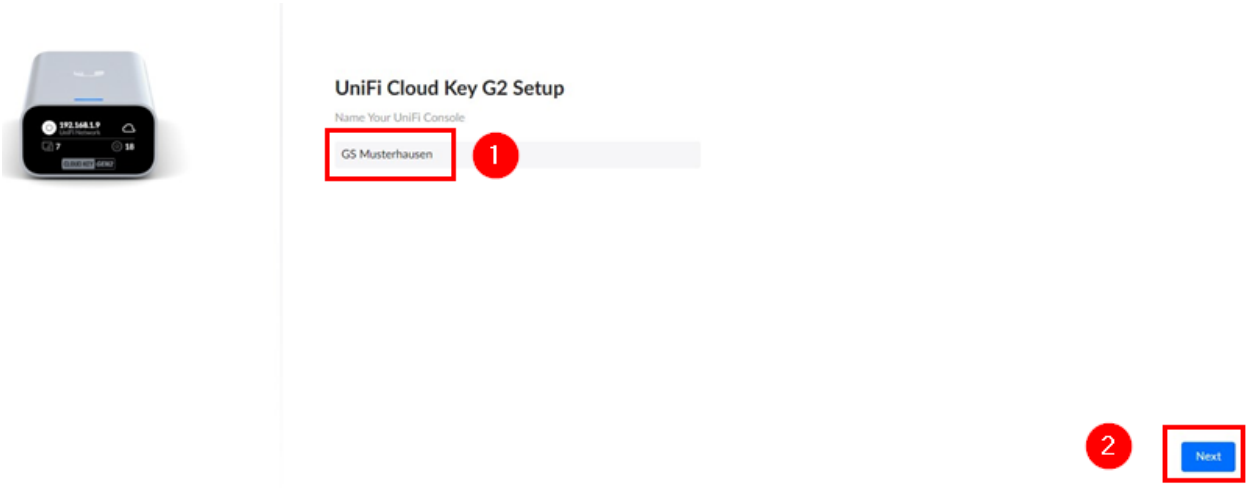
Im Anschluss „Set Up the Console Offline“ wählen:



Die Offline-Einrichtung erneut bestätigen:

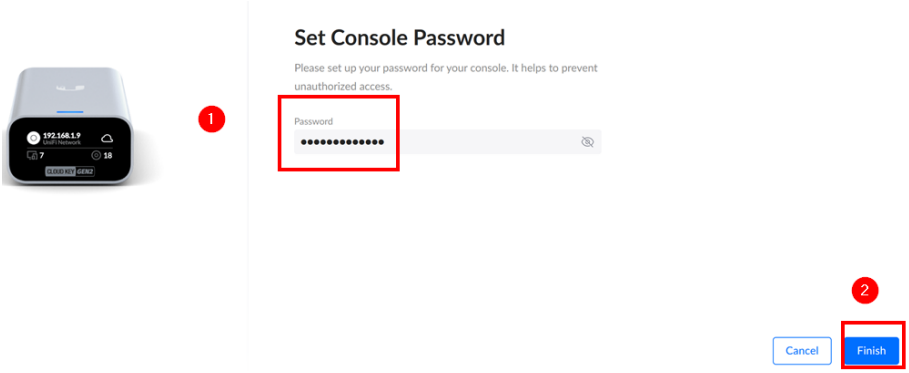


Im Anschluss als Controllernamen den Namen der Schule (z. B. „GS Musterhausen“) wählen (1) und mit „Next“ fortfahren (2):



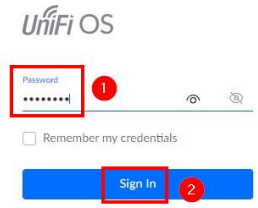
Hinweis: Die Anpassung des Controller-Namens ist wichtig, damit z. B. später bei der Zusendung von E-Mail-Benachrichtigungen am Betreff erkannt werden kann, an welcher Schule ein Fehler aufgetreten ist.

Das Controller-Passwort festlegen (1), mit „Finish“ (2) bestätigen und die Einrichtung des Controllers abwarten:

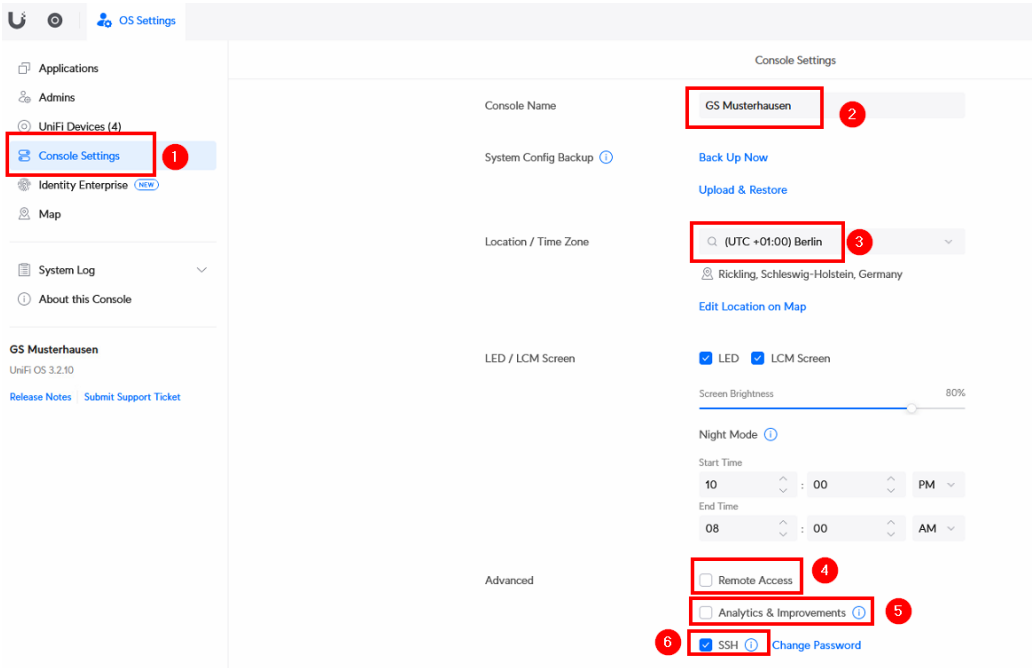


Hinweis: Das Passwort in der IT-Dokumentation der Schule eintragen. Der Benutzername wird weiter unten noch angepasst.

Mit dem neuen Passwort auf der Weboberfläche des Controllers einloggen:



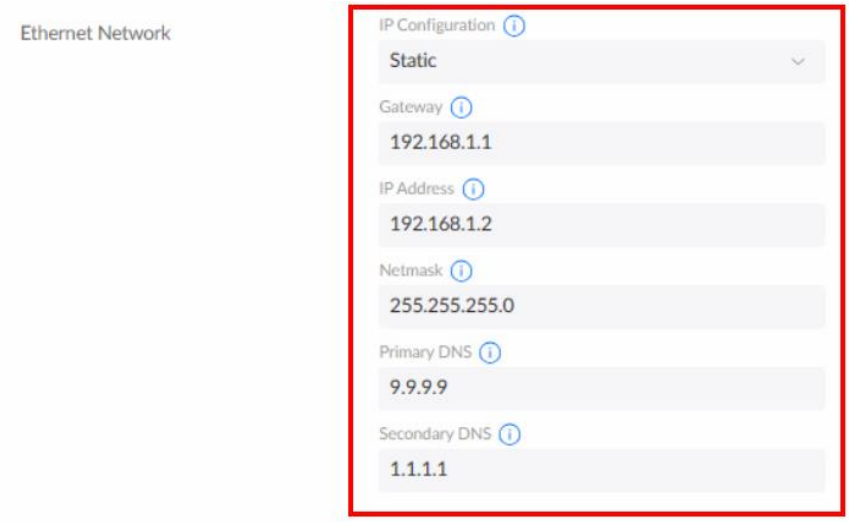
Unter dem Menüpunkt „Console Settings“ (1) den Namen des Controllers (2) auf die Schule anpassen (wenn noch nicht bei der Ersteinrichtung geschehen, siehe oben), ggf. die Zeitzone anpassen (3), den Remote-Zugriff deaktivieren (4), die Option „Analytics & Improvements“ deaktivieren (5) und den SSH-Zugriff aktivieren (6):



Im Anschluss an das Aktivieren des SSH-Zugriffs den Hinweis akzeptieren und ein Passwort für den Zugriff festlegen.

Hinweis: Das SSH-Passwort für den Zugriff auf den Controller in der IT-Dokumentation der Schule notieren. Für die Access Points und Switches wird später ein separates SSH-Kennwort erstellt.

Ebenfalls unter dem Menüpunkt „Console Settings“ die IP-Konfiguration auf „Static“ umstellen, als Gateway 192.168.1.1, als IP-Adresse 192.168.1.2, als Netzmaske 255.255.255.0, als primären DNS 9.9.9.9 und als sekundären DNS 1.1.1.1 eintragen sowie alle Änderungen mit „Apply Changes“ bestätigen:

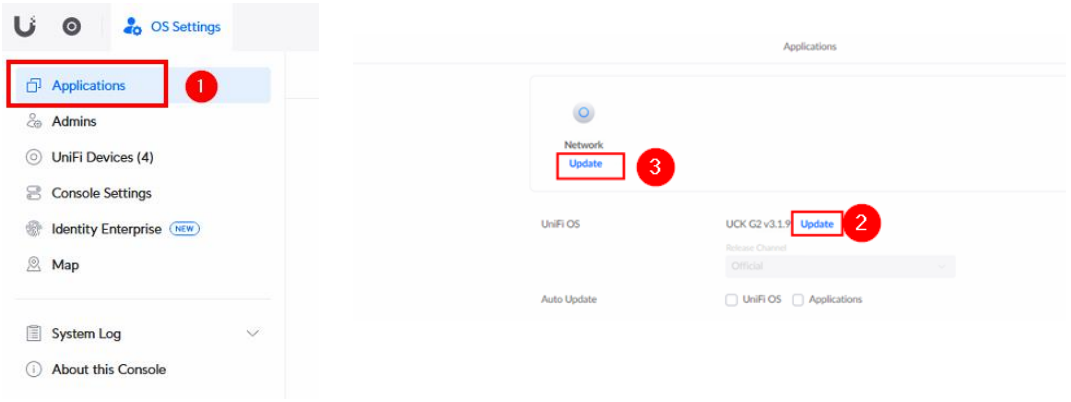


Hinweis: Sollte der Bereich der IP-Adresskonfiguration nicht unter dem Menüpunkt „Console Settings“ auftauchen, muss der nächste Schritt (Herstellung einer Internetverbindung) vorgezogen werden. Der Controller erhält dann eine neue IP-Adresse per DHCP. Unter dieser Adresse ruft man die Weboberfläche erneut auf und stellt dann auf die statische IP-Adresse wie oben angegeben um.

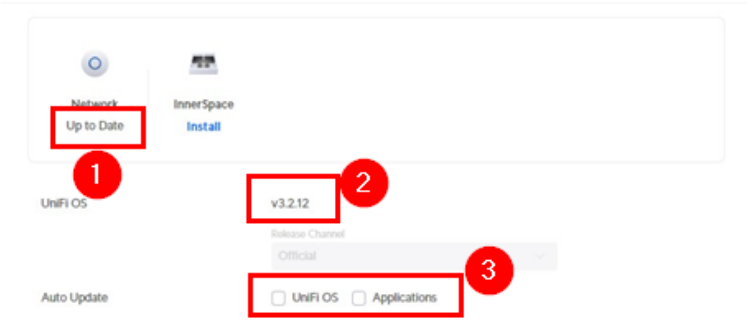
Nach der Änderung der IP-Adresse eine Internetverbindung für den Cloudkey herstellen. Dazu den Draytek-Router an den Switch anschließen (z. B. Port 1).

Im Anschluss über die neue IP-Adresse 192.168.1.2 die Weboberfläche des Controllers aufrufen und einloggen:

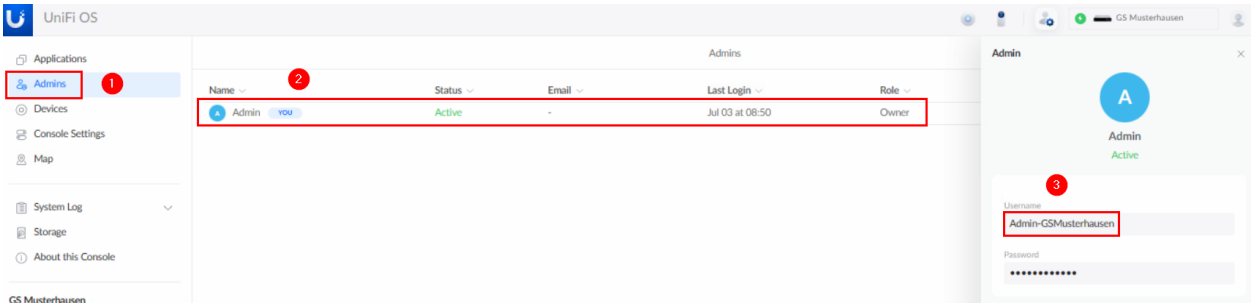
„Applications“ (1) wählen und nacheinander das Update für das UniFi OS (Cloudkey-Firmware) (2) und die Network-Software (3) durchführen:



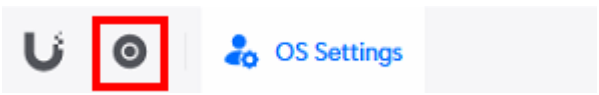
Nach Abschluss der Updates wird für die Network-Application der Status „Up to Date“ (1) angezeigt und für das UniFi-OS steht kein neues Update mehr zur Verfügung (2). Die automatischen Updates deaktivieren (3):



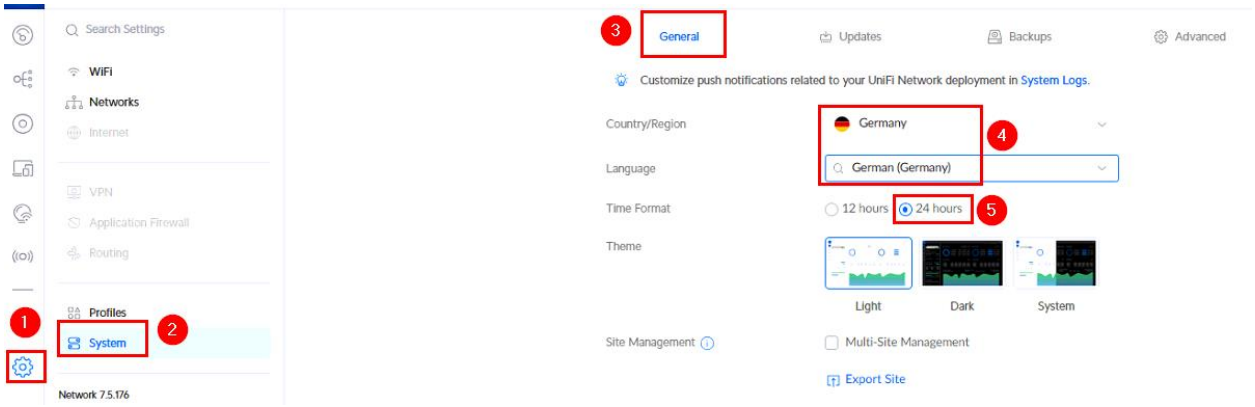
Unter „Admins“ die Benutzerverwaltung des Controllers öffnen (1), den vorhandenen Admin-Benutzer (mit der Rolle „Owner“) klicken (2) und den Benutzernamen individuell z. B. auf den Nachnamen des Administrators bzw. der Administratorin abändern (3) sowie mit „Apply Change“ bestätigen:



Oben links am Fensterrand auf die Weboberfläche der Netzwerkeinstellungen wechseln:

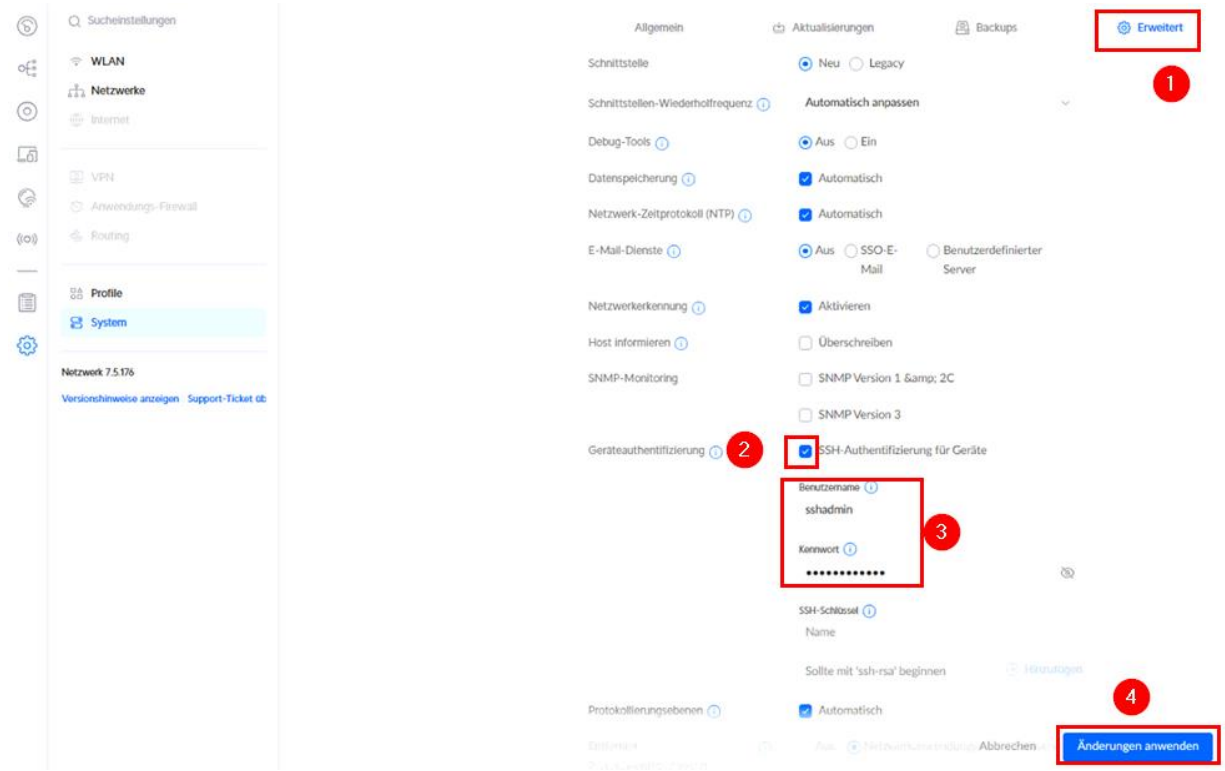


Dort die Einstellungen öffnen (1). Im Anschluss unter „System“ (2) im Bereich „General“ (3) die Region auf „Germany“ und die Sprache der Konfigurationsoberfläche auf „German (Germany)“ umstellen (4) sowie das Zeitformat anpassen (5):



Mit „Apply Changes“ bestätigen.

Beim Menüpunkt „System“ bleiben und unter „Erweitert“ (1) die „SSH-Authentifizierung für Geräte“ aktivieren (2), einen neuen Benutzernamen sowie ein neues Passwort für den Zugriff vom Controller auf die Geräte (Access Points und Switches) festlegen (3) und mit „Änderungen anwenden“ (4) bestätigen:



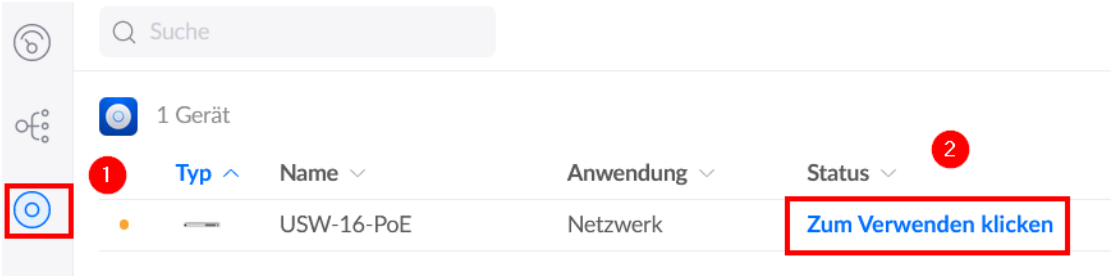
Hinweis: Das Gerätepasswort wird z. B. für die nachträgliche Einbindung eines Gerätes benötigt. Es sollte sich von dem Passwort des Controllers unterscheiden.

Benutzernamen und Passwort in der IT-Dokumentation der Schule eintragen.

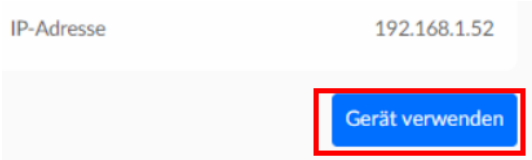
4 Switch(es) einbinden

Hinweis: Die IP-Adresse für den/die Switch(es) wird automatisch per DHCP durch den angeschlossenen Draytek-Router im Bereich 192.168.1.x vergeben.

In der Network-Application des Controllers den Menüpunkt „UniFi Geräte“ wählen (1) und im Anschluss den/die Switch(es) auswählen und „Zum Verwenden klicken“ wählen (2):



In den Gerätedetails auf der rechten Seite im Anschluss ggf. mit „Gerät verwenden“ bestätigen:



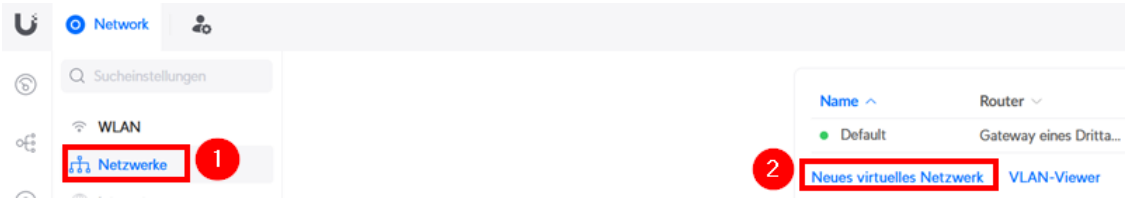
Hinweis: Das Einbinden des/der Geräte kann in einigen Fällen mehrere Minuten dauern und ist abgeschlossen, sobald die Statusanzeige von gelb („erste Schritte“ bzw. „Aktualisierung“) auf grün („Online“ bzw. „Aktuell“) wechselt:

Typ	Name	Anwendung	Status	IP-Adresse
	USW-16-PoE	Netzwerk	Online	192.168.1.50
	US-24-250W	Netzwerk	Aktualisierung	192.168.1.52

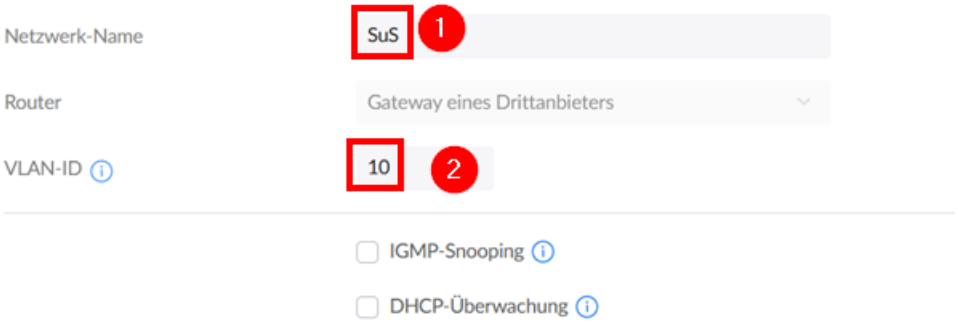
5 Einrichtung Netzwerke

Hinweis: Das vorhandenen Netzwerk „Default“ kann (ohne UniFi-Router) nicht angepasst werden. Es wird als zukünftiges Admin-Netzwerk (192.168.1.1/24) verwendet.

Zusätzlich werden drei virtuelle Netze für Lehrkräfte, Schülerinnen und Schüler sowie Gäste erstellt. Dazu in den Einstellungen den Menüpunkt „Netzwerke“ (1) und den Punkt „Neues virtuelles Netzwerk“ (2) wählen:

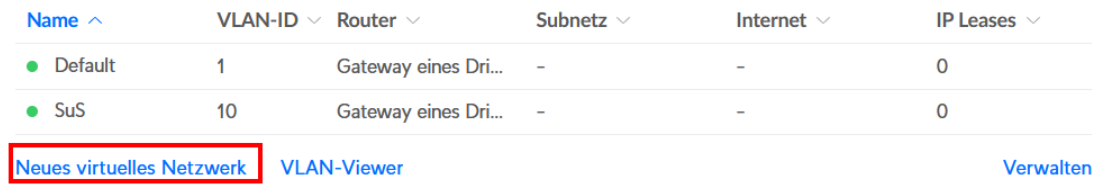


Das **Netz für schuleigene Endgeräte der Schülerinnen und Schüler** (SuS) mit dem Namen „SuS“ (1) und aktivierter VLAN-ID 10 (2) hinzufügen:

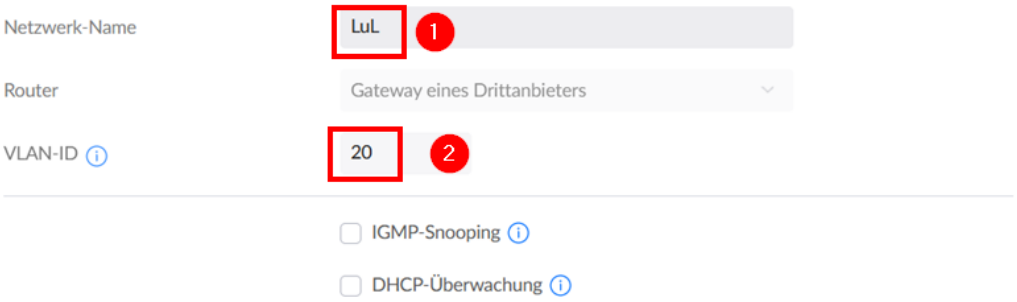


Mit „Hinzufügen“ bestätigen.

Im Menüpunkt „Netzwerke“ erneut „Neues virtuelles Netzwerk“ wählen:

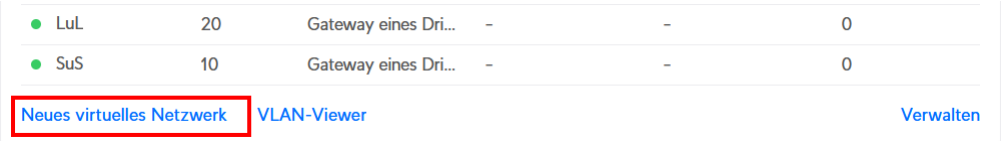


Das **Netz für schuleigene Endgeräte der Lehrerinnen und Lehrer** (LuL) mit dem Namen „LuL“ (1) und aktivierter VLAN-ID 20 (2) hinzufügen:

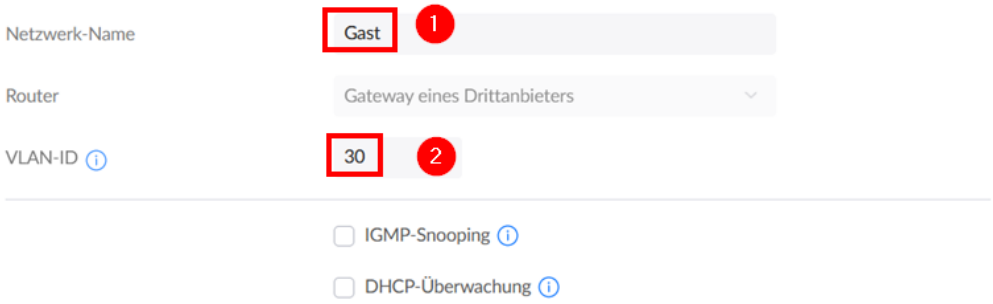


Mit „Hinzufügen“ bestätigen.

Im Menüpunkt „Netzwerke“ erneut „Neues virtuelles Netzwerk“ wählen:

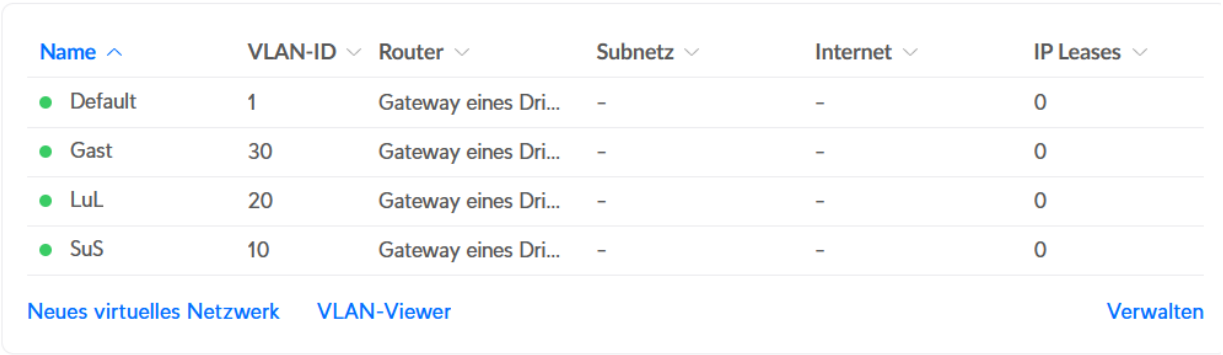


Das **Netz für private Endgeräte** mit dem Namen „Gast“ (1) und aktivierter VLAN-ID 30 (2) hinzufügen:



Mit „Hinzufügen“ bestätigen.

Folgende (virtuelle) Netzwerke sollten jetzt vorhanden sein:

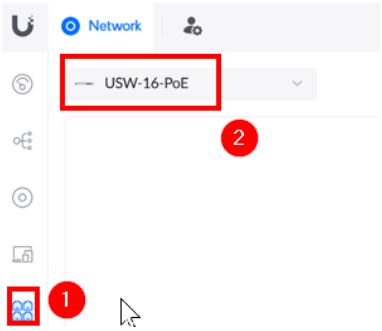


6 Einrichtung Switch(es)

Neben dem Router, dem Controller und dem Admin-Endgeräte auch weitere Geräte (NAS, ggf. Wartungsrechner oder Cachingserver) an den Switch anschließen. Die Ports sollen zum Netzwerk „Default“ gehören, was bereits voreingestellt ist. Beispielhafte Portbelegung:

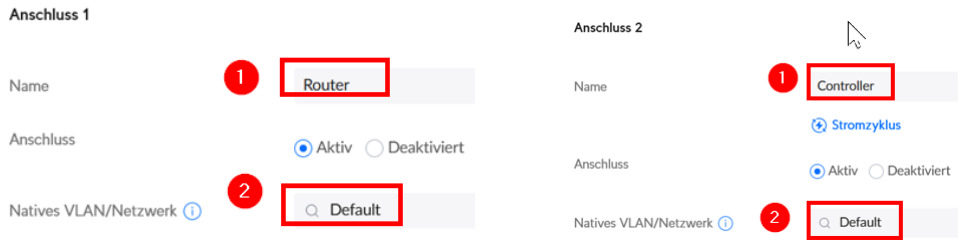
- Port 1 (Netz „Default“): Draytek-Router (über LAN-Port 1)
- Port 2 (Netz „Default“): UniFi-Controller
- Ports 3 + 4 (Netz „Default“): NAS (beide LAN-Ports verbinden)
- Port 5 (Netz „Default“): Admin-Endgerät, ggf. Wartungsrechner, Caching-Server

Im Menü „Ports“ wählen (1) und dort den betreffenden Switch auswählen (2):



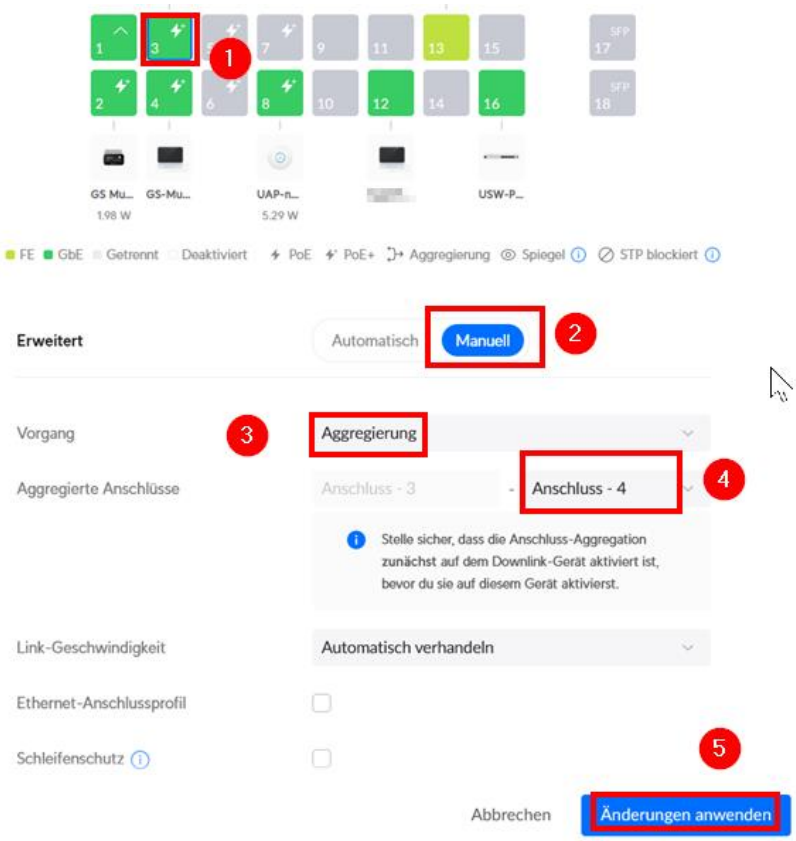
In der Portübersicht den Port für den Router (z. B. Port 1) auswählen:

Als Namen „Router“ eingeben (1), als Netzwerk „Default“ belassen (2) und mit „Änderungen anwenden“ bestätigen. Analog auch für den Port des Controllers (zum Beispiel Port 2) vorgehen:



In der Portliste den ersten der beiden Ports am Switch wählen, an denen das NAS angeschlossen ist (z. B. Port 3), als Namen „NAS“ eingeben (1), das Netzwerk „Default“ belassen (2) und mit „Änderungen anwenden“ bestätigen:

Im Anschluss den ersten der beiden Ports am Switch auswählen (1), an denen das NAS angeschlosen ist (z. B. Port 3), im Bereich „Erweitert“ auf „Manuell“ umstellen (2), die Option „Vorgang“ auf „Aggregierung“ (3) umstellen und „Aggregierte Anschlüsse“ auf den anderen Port des NAS (z. B. Port 4) einstellen (4) sowie mit „Änderungen anwenden“ bestätigen (5):



Hinweis: Durch die Aggregation der beiden NAS-Ports wird u. a. die Bandbreite beim gleichzeitigen Zugriff mehrerer Geräte auf die Datenablage erhöht. **Wichtig**: Auch auf der Datenablage muss die Port-Aggregation eingerichtet werden (siehe Anleitung Musterlösung Grundschule SH_NAS.pdf).

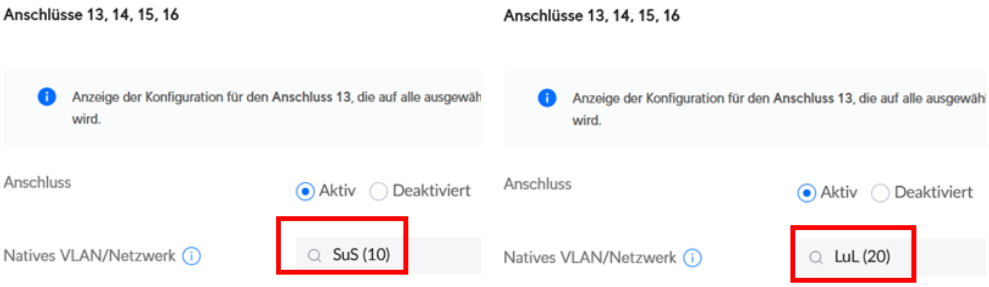
In der Portliste den passenden Port für den ggf. vorhandenen Wartungsrechner bzw. Caching-Server (z. B. Port 5) auswählen, als Namen „Wartungsrechner“ bzw. “Caching-Server“ eingeben (1), das Netzwerk „Default“ belassen (2) und mit „Änderungen anwenden“ bestätigen:

Anschließend einzeln die Ports für die WLAN Access Points auswählen (z. B. 6 - 12). Als Namen jeweils „WLAN Access Point“ wählen (1), das Netzwerk auf „Default“ eingestellt lassen (2) und mit „Änderungen anwenden“ bestätigen:

Hinweis: Werden weitere Switches eingerichtet, so werden diese miteinander über einen Port, der auf das Netzwerk „Default“ eingestellt wurde, verbunden. Alle weiteren Ports an den zusätzlichen Switches werden je nach Bedarf für die unterschiedlichen Netze eingerichtet (siehe oben).

Wenn Ports für schuleigene Endgeräte von Schülerinnen und Schülern (zum Beispiel im PC-Raum) bzw. Dienstgeräte für Lehrkräfte (zum Beispiel im Lehrerzimmer) benötigt werden:

- Ports auswählen (zum Beispiel die Ports 13-16), das Profil für schuleigene Endgeräte der Schülerinnen und Schüler („SuS“) bzw. Dienstgeräte der Lehrkräfte („LuL“) festlegen und mit „Änderungen anwenden“ bestätigen:



- Nachträglich auch die Namen der betreffenden Ports wie oben für den Router und Controller beschrieben auf „LuL“ bzw. „SuS“ „abändern.

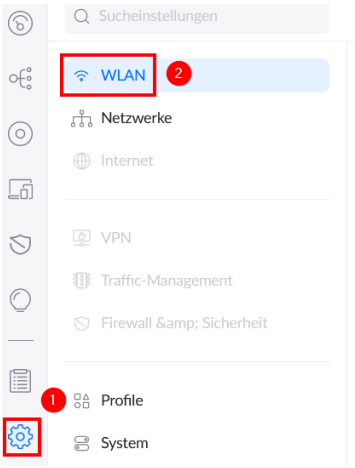
  Hinweis: Das Netz für private Endgeräte („Gast“) wird im Normalfall lediglich über die WLAN Access Points bereitgestellt.

7 WLAN einrichten

7.1 WLAN-Netze einrichten

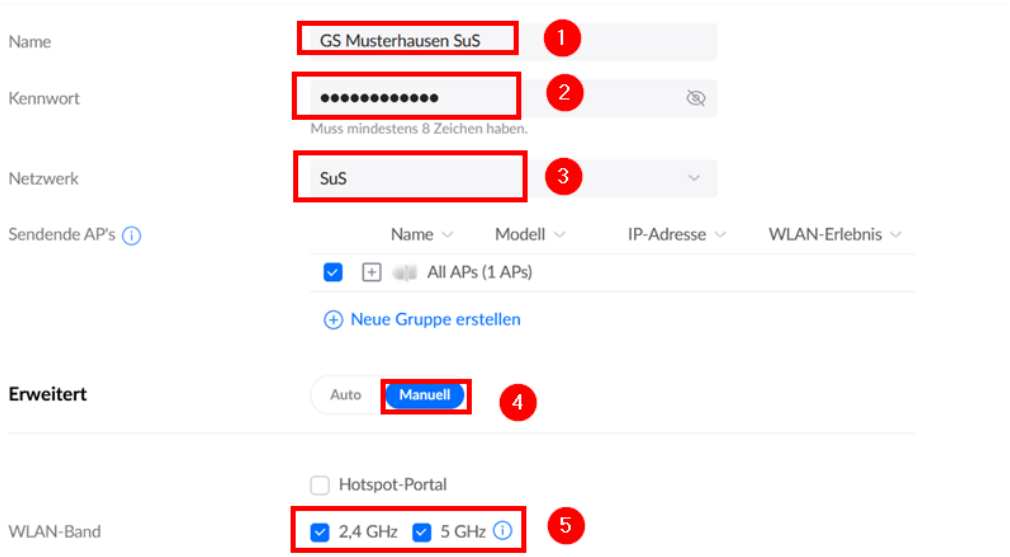
Zunächst die WLAN-Netze einrichten.

Dazu unter den Einstellungen (1) den Menüpunkt „WLAN“ (2) wählen:

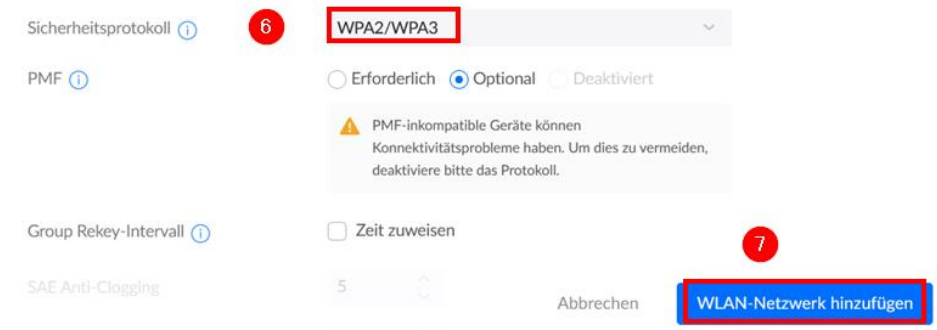


Hinweis: Die Namen für die WLAN-SSIDs können individuell festgelegt werden. Sie sollten nach Möglichkeit den Schulnamen bzw. das Schulkürzel enthalten sowie eine Kennzeichnung für die drei Netze (Schülerinnen und Schüler, Lehrkräfte und Gäste), zum Beispiel: „GS Musterhausen SuS“, „GS Musterhausen LuL“ und „GS Musterhausen Gast“.

Die SSID für schuleigene Endgeräte der Schülerinnen und Schüler einrichten. Dazu den Namen vergeben (zum Beispiel „GS Musterhausen SuS“) (1), ein sicheres und nicht leicht zu merkendes Passwort festlegen (2), mit dem oben angelegten Netzwerk für schuleigene Endgeräte der Schülerinnen und Schüler („SuS“) verbinden (3), im erweiterten Bereich (4) das 2.4-GHz- und 5 GHz-Netz aktivieren (5), als Sicherheitsprotokoll „WPA2/WPA3“ wählen (6) sowie mit „WLAN-Netzwerk hinzufügen“ bestätigen (7):



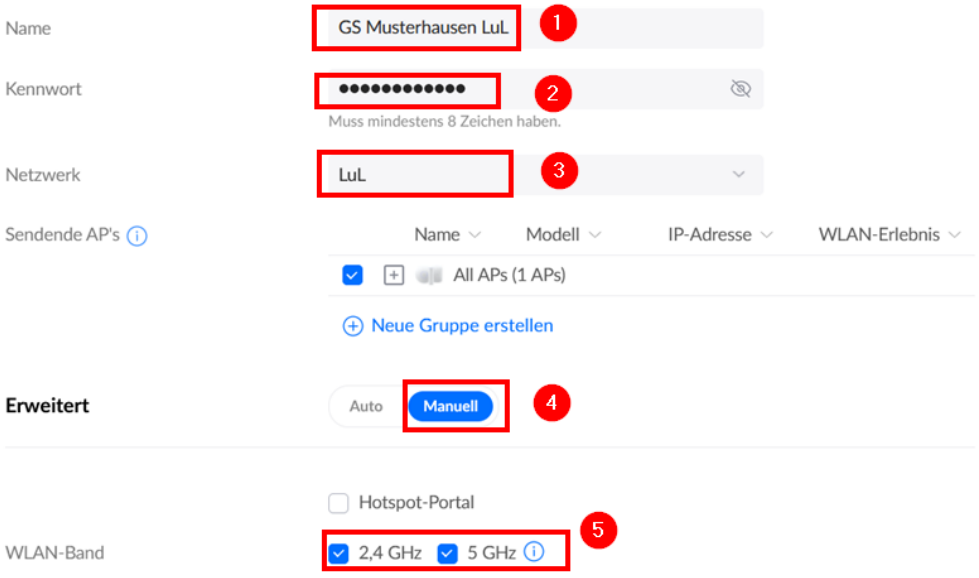
Hinweis: Das Passwort für das SuS-Netz in der IT-Dokumentation der Schule hinterlegen und nicht an Personen der Schule weitergeben. Das Passwort soll stattdessen fest auf den schuleigenen Endgeräten für Schülerinnen und Schüler gespeichert werden.



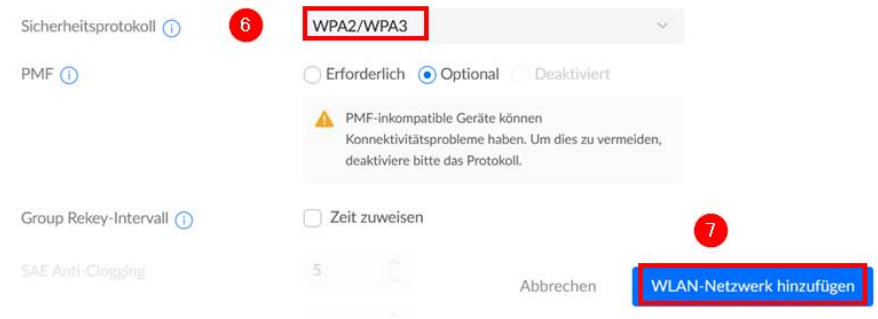
Hinweis: Ältere Access-Point-Modelle bzw. ältere Firmwareversionen unterstützen WPA3-Verbindungen nicht. Endgeräte, die das Protokoll nicht unterstützen, wechseln automatisch in den WPA2-Modus.

Unter dem angelegte WLAN-Netzwerk „Neues erstellen“ wählen:

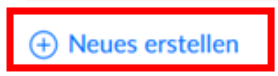
Die SSID für Dienstgeräte der Lehrkräfte einrichten. Dazu den Namen vergeben (zum Beispiel „GS Musterhausen LuL“) (1), ein sicheres und nicht leicht zu merkendes Passwort festlegen (2), mit dem oben angelegten Netzwerk für dienstliche Endgeräte der Lehrkräfte („LuL“) verbinden (3), im erweiterten Bereich (4) das 2.4-GHz- und 5 GHz-Netz aktivieren (5), als Sicherheitsprotokoll „WPA2/WPA3“ wählen (6) sowie mit „WLAN-Netzwerk hinzufügen“ bestätigen (7):



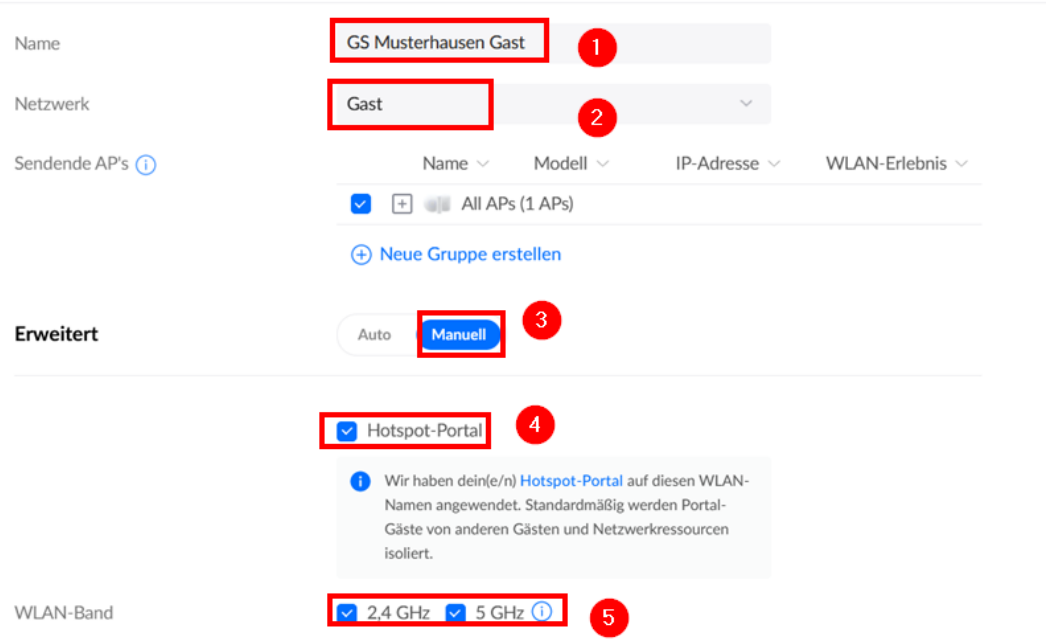
Hinweis: Das Passwort für das LuL-Netz in der IT-Dokumentation der Schule hinterlegen. Das Passwort soll durch die Schulleitung an Lehrkräfte nur für die Verwendung auf **dienstlichen** Lehrkräfte-Endgeräten weitergegeben werden. Private Endgeräte von Lehrkräften sollen über Langzeit-Gutscheine des Gast-WLANs verbunden werden.

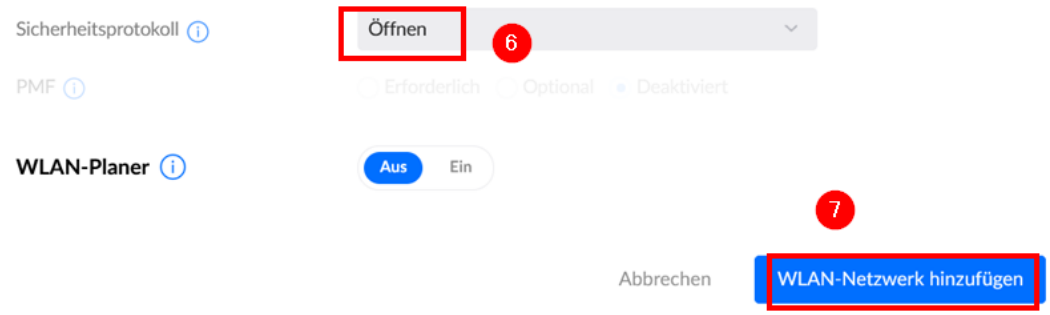


Weiteres Netzwerk mit „Neues erstellen“ anlegen:



Die SSID für private Endgeräte von Lehrkräften, Mitarbeitenden und Gästen einrichten. Dazu den Namen vergeben (zum Beispiel „GS Musterhausen Gast“) (1), mit dem oben angelegten Netzwerk für Gäste („Gast“) verbinden (2), im erweiterten Bereich (3) das Hotspot-Portal aktivieren (4), 2.4-GHz- und 5 GHz-Netz aktivieren (5) und als Sicherheitsprotokoll ein offenes Netz wählen (6)) sowie mit „WLAN-Netzwerk hinzufügen“ bestätigen (7):





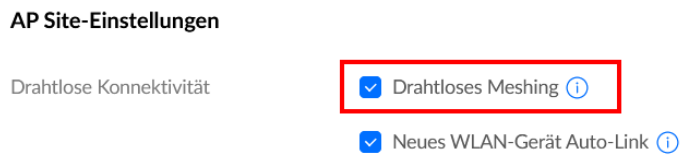
Folgende Drahtlos-Netzwerke sollten jetzt vorhanden sein:

Name	Netzwerk	AP-Gruppen	Clients (Peak)	Sicherheit	Erlebnis
GS Musterhaus...	Gast	All APs	0 (0)	Öffnen	–
GS Musterhaus...	LuL	All APs	0 (0)	WPA Personal	–
GS Musterhaus...	SuS	All APs	0 (0)	WPA Personal	–

Hinweis: Die gewählten SSID-Namen und Passwörter in der IT-Dokumentation der Schule vermerken.

7.2 WLAN-Access Points einbinden

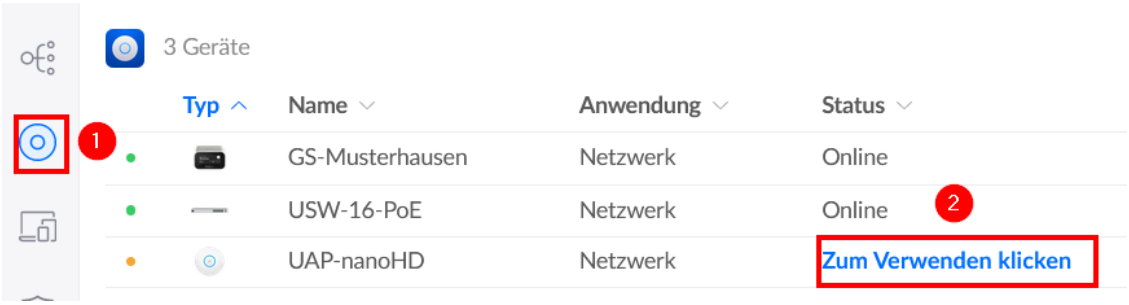
Hinweis: Bei Bedarf kann vor dem Anschließen der Access Points die Funktion „Wireless Meshing“ vorübergehend deaktiviert werden (siehe Menüpunkt „WLAN“ in den Netzwerkeinstellungen – dort ggf. „Vorkonfigurieren“ wählen), damit beim Einbinden der Access Points nur kabelbasierte Verbindungen zugelassen werden. Defekte Kabel zu Access Points können auf diesem Wege leichter identifiziert werden. Anschließend sollte jedoch die Funktion „Drahtloses Meshing“ als Fallback-Lösung wieder aktiviert werden.



WLAN Access Points an die oben konfigurierten Ports für das Netzwerk „Default“ (siehe oben) anschließen.

Hinweis: Die IP-Adressen für die Access Points werden automatisch per DHCP im Bereich 192.168.1.x vergeben.

Im Menüpunkt „UniFi-Geräte“ (1) die Access Points auswählen und „Zum Verwenden klicken“ wählen (2):



Im Anschluss auf der rechten Seite in den Gerätedetails mit „Gerät verwenden“ bestätigen:

Hinweis: Das Einbinden des/der Geräte kann in einigen Fällen mehrere Minuten dauern und ist abgeschlossen, sobald die Statusanzeige von gelb („Verwendung wird ausgeführt“ bzw. „Erste Schritte“) auf grün („Online“ bzw. „Aktuell“) wechselt:

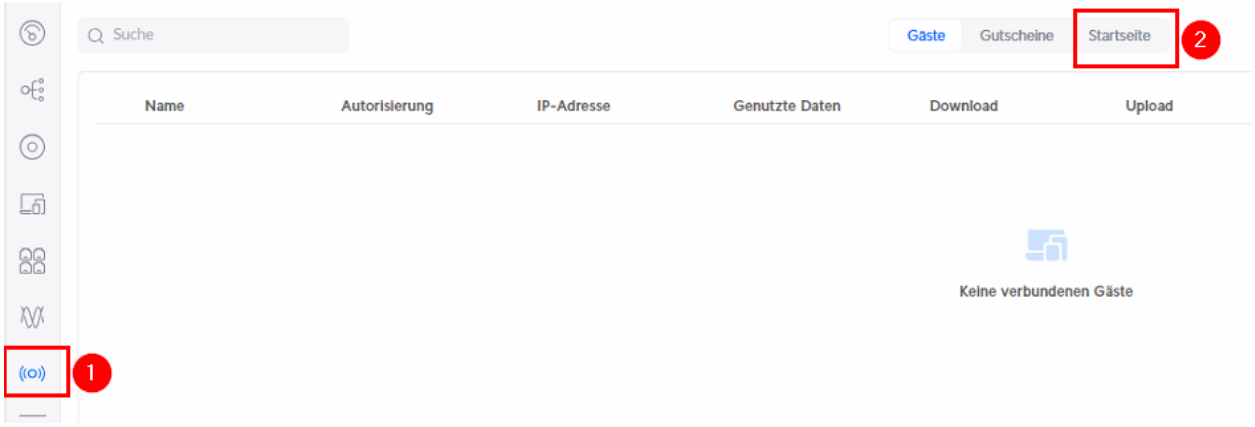
Hinweis: Die Access Points benötigen etwa 30 Sekunden, um die Einstellungen zu übernehmen.

Nach der Konfiguration des Beispiel-Switches sind die Ports wie in der Liste aufgeführt belegt:

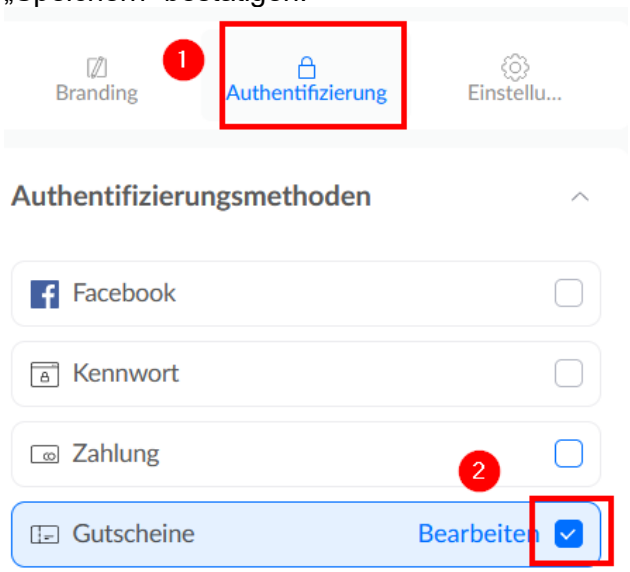
- Ports 1-5 (Netzwerk „Default“): Router, Controller, NAS, ggf. Wartungsrechner/Cachingserver, ggf. Drucker
- Ports 6-12 (Netzwerk „Default“): WLAN Access Points
- Ports 13-15 (Netzwerk „SuS“ bzw. „LuL“): ggf. per LAN angeschlossene schuleigene Endgeräte von Schülerinnen und Schülern bzw. dienstliche Geräte von Lehrkräften
- Port 16 (Netzwerk „Default“): ggf. Verbindung zu weiterem Switch

8 Gastportal einrichten

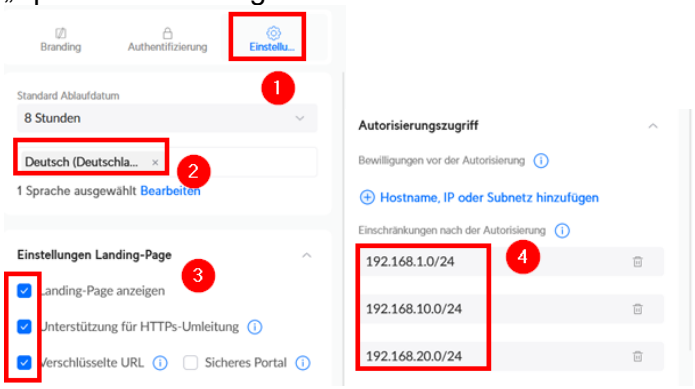
Im Hauptmenü „Hotspot-Manager“ wählen (1) und dort die Einstellungen für die „Startseite“ (2) öffnen:



Auf der rechten Seite unter „Authentifizierung“ (1) die Option „Gutscheine“ aktivieren (2) und mit „Speichern“ bestätigen:



Unter „Einstellungen“ (1) die voreingestellte Sprache durch „Deutsch“ ersetzen (2), nachfolgende Einstellungen für die Landing-Page (3) setzen sowie den Zugriff auf das Unterrichtsnetz (die Netze „SuS“ und „LuL“) und das Adminnetz verhindern (4) sowie mit „Speichern“ bestätigen:



Unter „Branding“ (1) den Titel auf den Namen der Schule und den Begrüßungstext auf „Herzlich willkommen im Gast-WLAN!“ bzw. auf einen individuellen Text in Absprache mit der Schulleitung anpassen (2), die Nutzungsbedingungen aktivieren (3) und den vorhandenen Text zu den Nutzungsbedingungen durch den Text aus der Box (siehe unten) austauschen (4):

Text für die Nutzungsbedingungen:

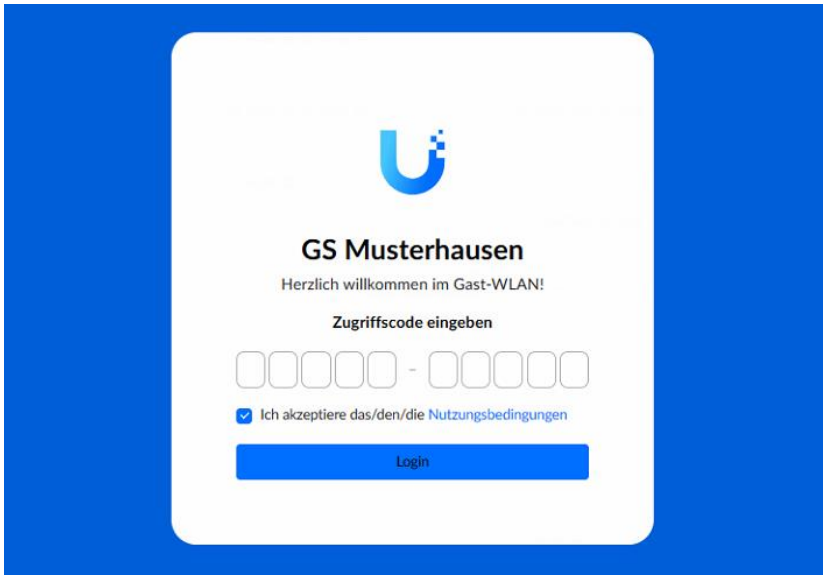
Mit der Nutzung des WLAN sind folgende Regelungen zu beachten. Diese gelten für alle mit dem WLAN verbundenen Geräte:

- Die Schule behält sich jederzeit das Recht vor, Zugangsdaten zu ändern oder zu deaktivieren.
- Das schulische WLAN darf nur für unterrichtsbezogene Zwecke genutzt werden.
- Die Nutzenden sind verpflichtet, die gesetzlichen Bestimmungen (z.B. Urheberrecht, Datenschutzrecht, Jugendschutzrecht) einzuhalten.
- Nutzungseinschränkungen durch das Vorhandensein von Jugendschutzfiltersoftware der Schule sind zu akzeptieren. Der Versuch, die technischen Filtersperren zu umgehen, kann zum Entzug der Nutzungserlaubnis führen.
- Die Schule übernimmt keine Haftung für die Datensicherheit der mit dem WLAN verbundenen privaten Geräte. Die Verantwortung hierfür liegt ausschließlich bei den Nutzenden.
- Missbrauch der Netzwerkstruktur wird nachgegangen und ggf. zur Anzeige gebracht.

Ebenfalls im Bereich „Branding“ die Schaltfächen-Textfarbe auf „Schwarz“ (#000000) ändern (5) und im Bereich „Erfolg Landing-Page“ den Text auf „Erfolgreich eingeloggt!“ abändern (6):

Am Ende mit „Speichern“ alle Einstellungen bestätigen.

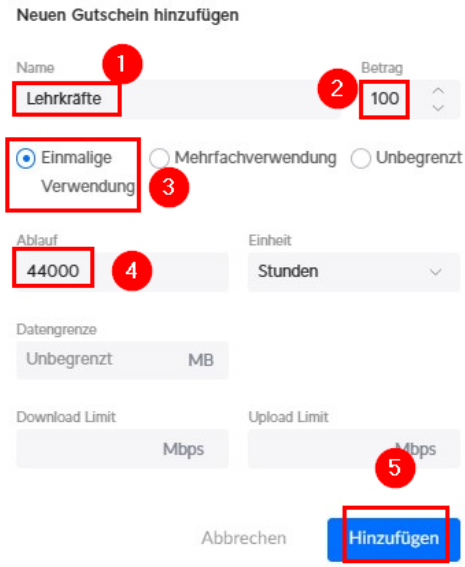
Das fertig eingerichtete Gast-Portal soll so aussehen:



8.1 WLAN-Gutscheine erstellen

Im Netzwerk-Menü den Punkt „Hotspot Manager“ (1) wählen und unter „Gutscheine“ (2) die Option „Gutschein hinzufügen“ (3) wählen:

Für private Endgeräte von Lehrkräften und Mitarbeitenden (1) 100 Gutscheincodes (2) erstellen, die jeweils nur von einem Gerät (3) benutzt werden können und etwa 5 Jahre (44.000 Stunden) gültig sind (4). Am Ende mit „Hinzufügen“ (5) bestätigen:



Für private Endgeräte von Gästen (1) 100 weitere Gutscheincodes erstellen (2), die jeweils von einem Gerät (2) benutzt werden können und 24 Stunden gültig sind (3). Am Ende mit „Hinzufügen“ (4) bestätigen:

Die Gutschein-Codes im Anschluss in einer PDF-Datei speichern bzw. ausdrucken.

Hinweis: Zum Aufruf der Druckfunktion sollte Microsoft Edge oder ein anderer chromiumbasierter Browser verwendet werden, da es sonst zu Problemen bei der Erstellung des PDF-Dokumentes kommen kann.

Dazu oben rechts „Alles drucken“ wählen:

Drucker bzw. PDF-Drucker („Microsoft Print to PDF“ oder „Als PDF speichern“) wählen (1) und mit „Drucken“ bestätigen(2):

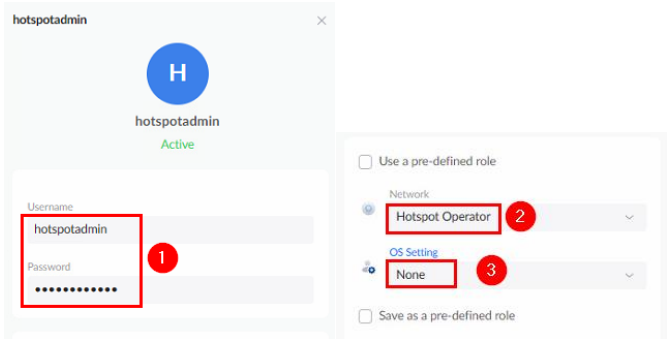
Hinweis: Sollten in der Druckvorschau nicht alle Gutscheine auf einer Seite erscheinen, muss der Druckvorgang ggf. mit einem anderen Browser durchgeführt werden.

Die erstellten Gutscheine der Schulleitung in Form einer PDF-Datei bzw. eines Ausdrucks zur Verfügung stellen.

Hinweis: Bei Bedarf kann für die Schule ein eigener Account zur Erstellung von WLAN-Gutscheinen eingerichtet werden.

- Dazu oben links am Fensterrand in die Einstellungen des Controllers wechseln:

- Dort im Menüpunkt „Admins“ über das Plus-Symbol einen neuen Benutzer-Account anlegen, einen individuellen Namen wählen sowie ein Passwort vergeben (1), die Rolle „Network Operator“ (2) für die Netzwerkapplikation und „None“ (3) für Controller-Einstellungen wählen:



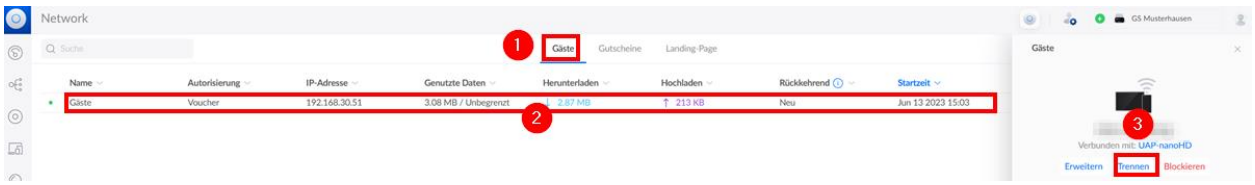
- Zugangsdaten in der IT-Dokumentation der Schule notieren.

Hinweis: Als Loginseite sollte der Schule hier die Adresse https://192.168.1.2/network mitgegeben werden, damit gleich nach dem Login die Netzwerk-Applikation angezeigt wird.

8.2 WLAN-Gutschein deaktivieren

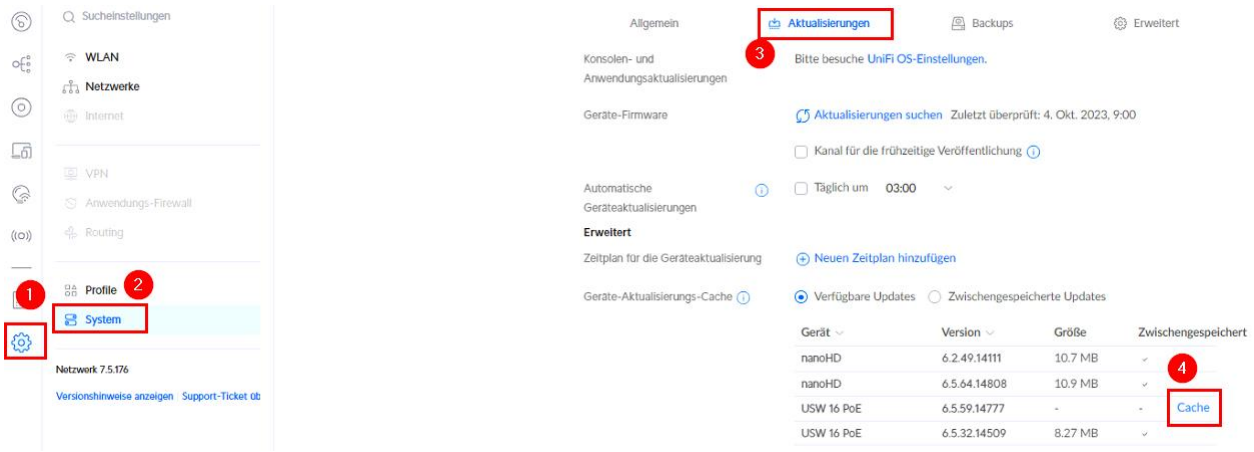
Soll einem Benutzer, der über einen Gutschein die Zugangsberechtigung zum WLAN bekommen hat, der Zugang zum WLAN vor Ablauf des Gutscheins gesperrt werden, so sind folgende Schritte notwendig:

Wie oben beschrieben die Weboberfläche des Hotspot-Managers aufrufen. In der Weboberfläche des Controllers den Menüpunkt „Gäste“ wählen (1), das zu sperrende Gerät auswählen (2) und „Trennen“ wählen (3):



9 Update aller Komponenten durchführen

Zunächst in den Einstellungen (1) unter „System“ (2) im Reiter „Aktualisierungen“ (3) die entsprechenden neuen Updates aller vorhandenen Komponenten in den Zwischenspeicher (Cache) kopieren (4):



Hinweis: Durch das Zwischenspeichern der Update-Dateien laden die einzelnen Geräte die Updates nun nicht mehr direkt aus dem Internet sondern nur noch netzintern über den Controller herunter.

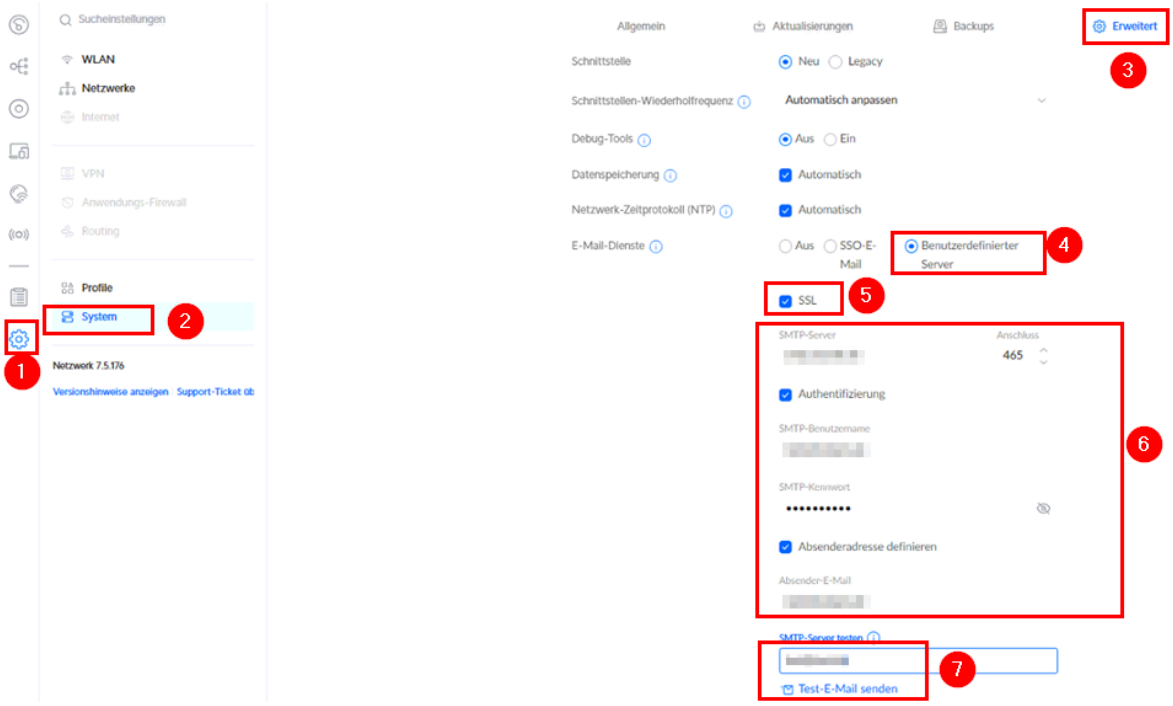
Im Anschluss Update/Upgrade aller Switches hintereinander durchführen. Dazu die jeweiligen Geräte unter dem Menüpunkt „Geräte“ (1) auswählen und „Zum Aktualisieren klicken“ (2) wählen:

Im Anschluss auch die Updates für alle Access Points durchführen.

10 E-Mail-Benachrichtigung aktivieren

Hinweis: Der mit der Wartung beauftragte Dienstleister bzw. Schulträger-Admin, soll mit Hilfe die Benachrichtigungsfunktion des Controllers über wichtige Ereignisse informiert werden. Dazu wird die E-Mail-Benachrichtigung aktiviert:

In den Einstellungen (1) „System“ (2) und den Reiter „Erweitert“ (3) wählen. E-Mail-Dienste auf „Benutzerdefinierter Server“ stellen (4), SSL aktivieren (5), die Konfigurationsdaten des E-Mailkontos eingeben (6) und eine Test-E-Mail versenden (7):



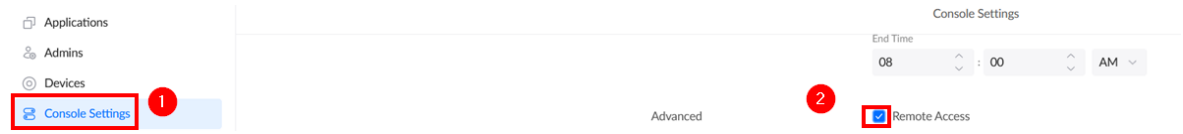
Mit „Änderungen anwenden“ speichern.

Hinweis: E-Mail-Benachrichtigungen werden nur an im Controller hinterlegte E-Mail-Adressen von UI.com-Accounts (https://account.ui.com) versendet. Dazu muss der Admin-Account zunächst mit einem UI.com-Account verknüpft werden.

Wichtig: Ein UniFi-Account zur Registrierung eines bzw. mehrerer Cloudkeys soll maximal die Geräte eines Schulträgers enthalten. Für einen weiteren Schulträger soll ein neuer UniFi-Account mit einer neuen E-Mail-Adresse angelegt werden. Dadurch soll sichergestellt werden, dass im Falle eines Dienstleisterwechsels, der UniFi-Account problemlos an den neuen Dienstleister übergeben werden kann. Im Security-Bereich des Accounts muss dann lediglich die E-Mail-Adresse angepasst werden.

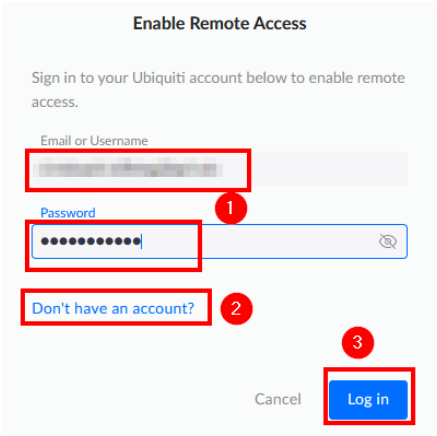
Zur Verbindung des Controllers mit dem UniFi-Account oben links am Fensterrand in die Einstellungen des Controllers wechseln:

Dort unter „Console Settings“ (1) den Remote Access kurzzeitig aktivieren (2):



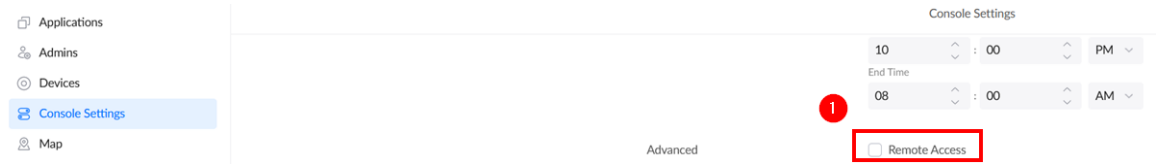
Im Anschluss mit den Zugangsdaten eines vorhandenen UI.Com-Account anmelden (1 + 3) bzw. einen neuen Account über „Don’t have an acoount?“ (2) anlegen.

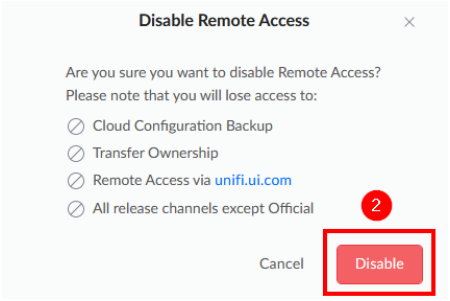
Wichtig: Der registrierte Online-Account wird automatisch in der Rolle „Administrator – Owner“ angelegt und kann im Controller nachträglich nicht mehr geändert werden. In den Account-Einstellungen unter https://account.ui.com kann jedoch später die E-Mail-Adresse des Zugangs bei Bedarf angepasst werden.



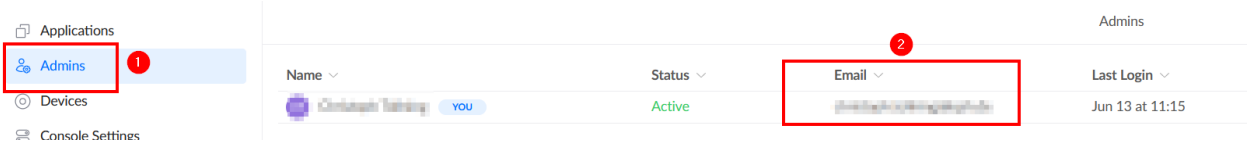
Zugangsdaten des Online-Accounts in der Netzwerkdokumentation der Schule notieren.

Im Anschluss den Remote-Zugriff wieder deaktivieren (1) und nachfolgenden Hinweis mit „Disable“ bestätigen (2):





Die im UI.Com-Account registrierte E-Mailadresse wurde dem vorhandenen lokalen Admin-Account zugeordnet (2). Dies lässt sich in der Benutzerverwaltung (1) überprüfen:

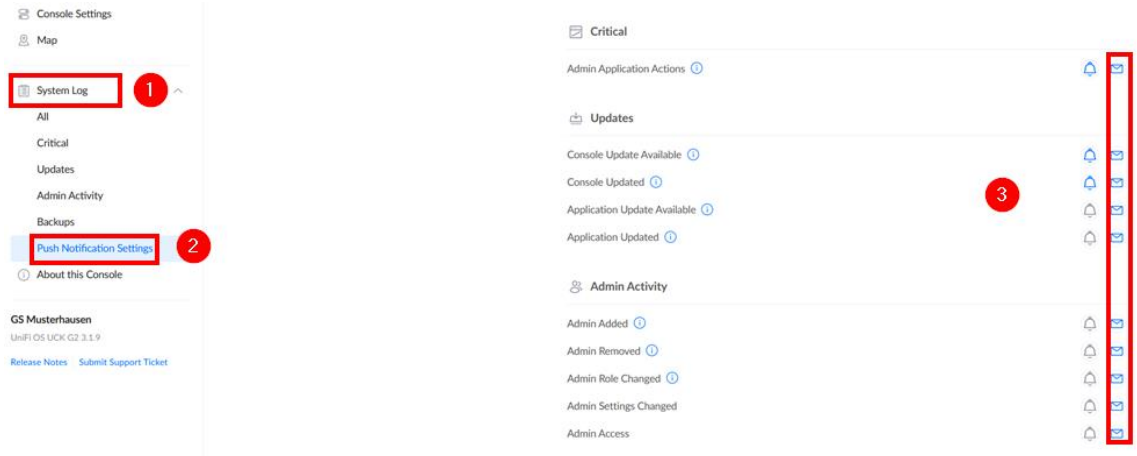


Hinweise:

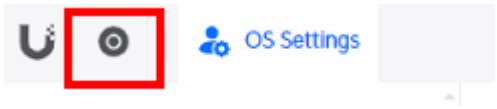
- Es wird nun der im Online-Account hinterlegte Name der Benutzerin bzw. des Benutzers angezeigt. Der Login in die Controller-Oberfläche ist sowohl über den oben vergebenen Namen des Administrators/der Administratorin und das vergebene Passwort als auch über die Zugangsdaten des Online-Accounts möglich.
- Bei Bedarf kann ein weiterer UI.com-Account registriert werden. Dazu muss zunächst der Remote-Access wieder aktiviert werden. Danach legt man mit „Add User“ einen neuen Benutzer mit dem Account-Typ „Ubiquiti-Account“ an, fügt diesem neuen Konto über „Add Local Credentials“ auch lokale Logindaten hinzu und verifiziert den hinzugefügten Account über die zugesandte Mail. Am Ende soll der Remote-Access wieder deaktiviert werden.

Im Anschluss die Benachrichtigungen konfigurieren:

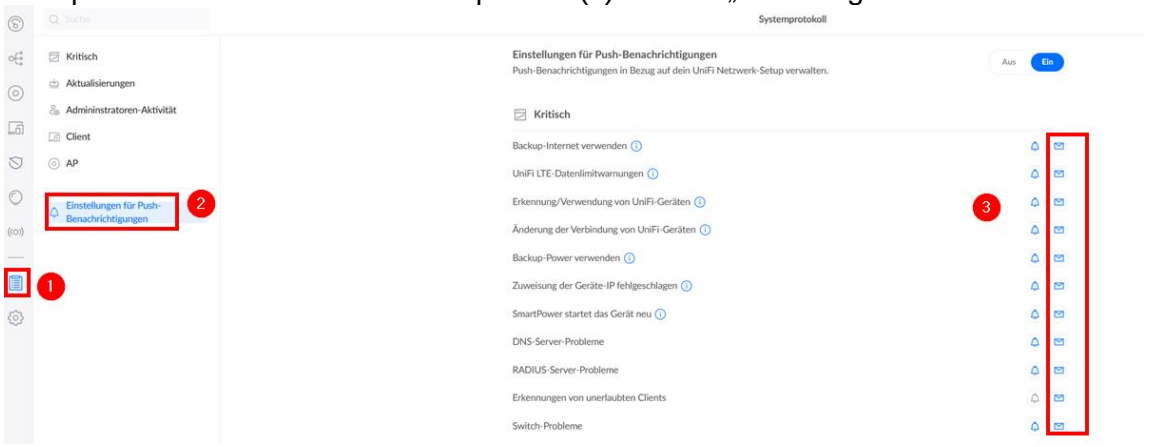
- Zunächst die Benachrichtigungen für UniFI OS einstellen. Dazu im Menü „System Log“ (1) – „Push Notification Settings“ (2) wählen und dort nach Bedarf die E-Mail-Benachrichtungen aktivieren (3):



- Im Anschluss die Netzwerk-Benachrichtigungen einstellen. Dazu oben links am Fensterrand auf die Weboberfläche der Netzwerkeinstellungen wechseln:



- Im Menü unter „Systemprotokoll“ (1) und „Einstellungen für Push-Benachrichtigungen“ (2) die Spalte für E-Mail nach Bedarf anpassen (3) und mit „Änderungen anwenden“:

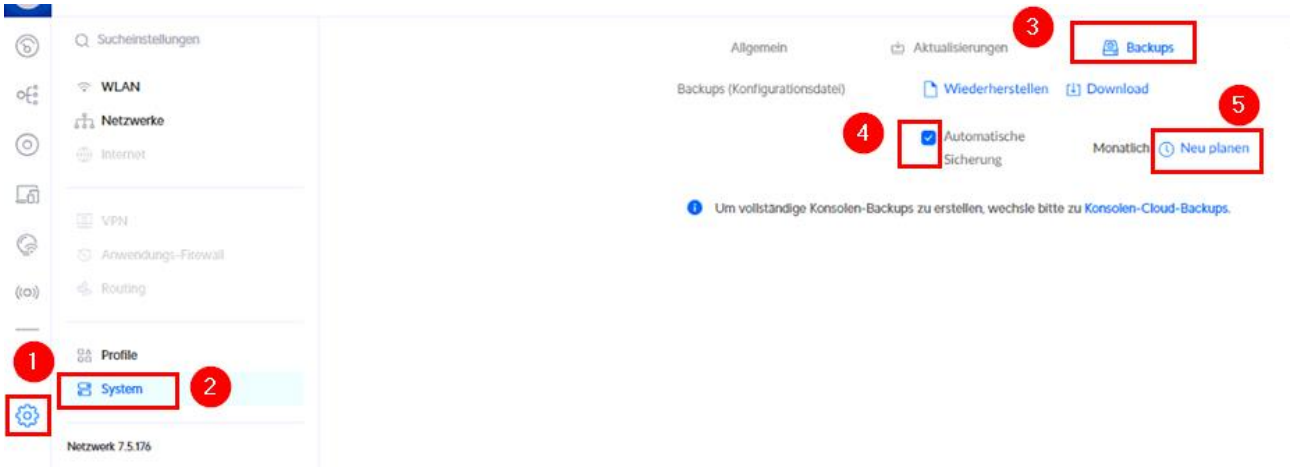


11 Controller-Konfiguration speichern und Automatisches Backup aktivieren

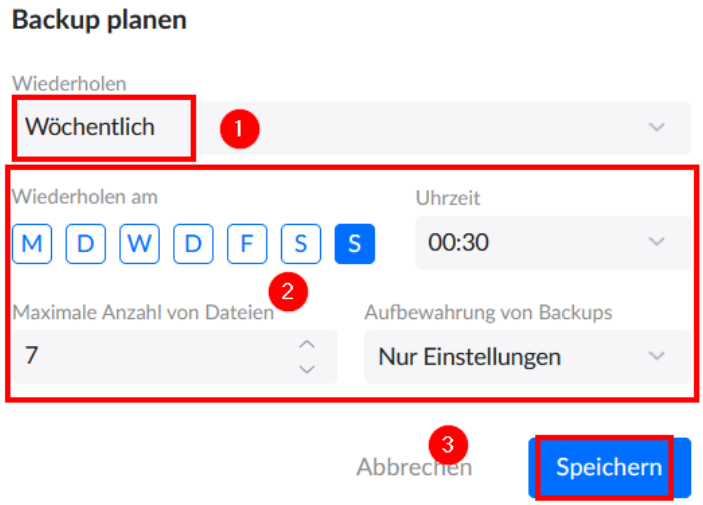
Micro-SD-Karte (mind. 8 GB) in den vorgesehenen Slot am Cloudkey einschieben.

Hinweis: Für den Fall eines Geräteausfalls soll die Backup-Datei nicht auf dem internen Speicher sondern auf der SD-Karte abgelegt werden.

In den Einstellungen (1) den Bereich „System“ (2) und den Reiter „Backups“ (3) wählen, die „Automatische Sicherung“ aktivieren (4) und „Neu planen“ wählen (5):



Die Wiederholung auf „wöchentlich“ umstellen (1), einen Wochentag auswählen (2) und mit „Speichern“ bestätigen (3):



Hinweis: Die Backup-Dateien werden automatisch auf der SD-Karte gespeichert.

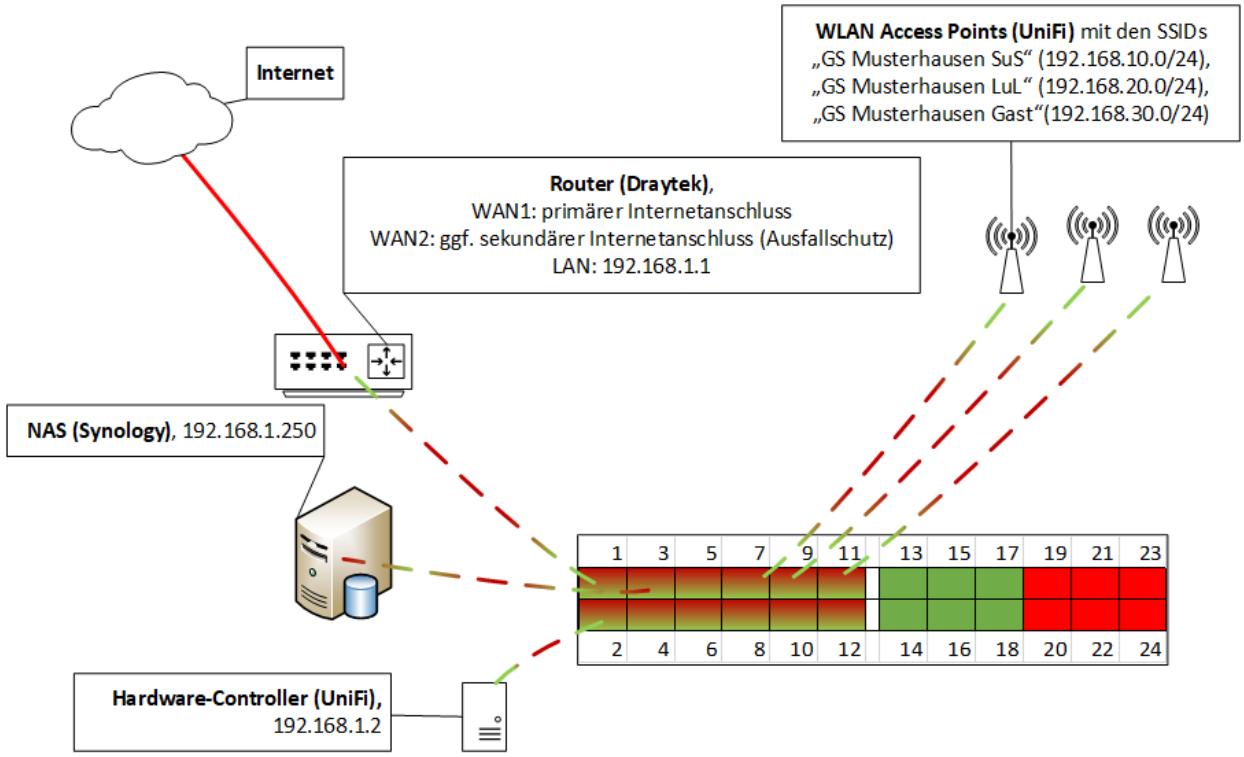
Mit „Änderungen anwenden“ bestätigen.

Unter dem Reiter „Backup“ die Konfiguration als Sicherungskopie herunterladen:

Die heruntergeladene UNF-Datei auf der Datenablage (Synology-NAS) in einem passwortgeschützten Ordner ablegen.

12 Netzwerkschema

Die eingerichteten Netze im Überblick:



Switch (UniFi), z.B. 192.168.1.50, beispielhafte Konfiguration:
Ports 1-12: Netz „Default“ (ohne VLAN-ID) für Router, Controller, NAS, WLAN-Accesspoints, Drucker, weitere Switches
Ports 13-18: Netz „SuS“ (VLAN-ID 10) für schuleigene Endgeräte der Schülerinnen und Schüler
Ports 19-24: Netz „LuL“ (VLAN-ID 20) für interaktive Displays, dienstliche Endgeräte der Lehrkräfte

Änderungshistorie

Änderung vom 15.03.2024:

- Die Einbindung von WLAN-Access Points funktioniert nur, wenn bereits WLAN-Netze angelegt wurden. Daher wurde die Reihenfolge im Kapitel WLAN einrichten geändert.

Änderung vom 14.03.2024:

- Ein UniFi-Account zur Registrierung eines bzw. mehrerer Cloudkeys soll zukünftig maximal die Geräte der Schule(n) eines Schulträgers enthalten. Für weitere zu betreuende Schulträger soll jeweils ein neuer UniFi-Account mit einer neuen E-Mail-Adresse angelegt werden. Dadurch soll sichergestellt werden, dass im Falle eines Dienstleisterwechsels, der UniFi-Account problemlos an den neuen Dienstleister übergeben werden kann (siehe Kapitel E-Mail-Benachrichtigung aktivieren).

Änderung vom 07.02.2024:

- Durch die Aktualisierung der UniFi Network Application haben sich einige Screenshots im Kapitel Controller einrichten geändert.

Änderung vom 29.11.2023:

- Durch die Aktualisierung der UniFi Network Application haben sich einige Screenshots im Kapitel Controller einrichten geändert. So gibt es im Systemmenü zur Einrichtung der UniFi-Komponenten nun z. B. einen eigenen Menüpunkt zum Einstellen der Switch-Ports.

Änderung vom 17.10.2023:

- Ergänzung eines Hinweises, wie ein aktuell auftretendes Problem mit dem Gastportal gelöst werden kann (siehe Kapitel Gastportal einrichten).

Änderungen vom 04.10.2023:

- Ein Screenshot zur Einrichtung eines VPN-Kontos im DrayTek-Router wurde ausgetauscht (siehe Kapitel VPN-Einrichtung).
- Alle Screenshots, die den Bereich der Systemeinstellungen des Controllers betreffen, wurden aufgrund einer neuen Version der UniFi Network Application ausgetauscht (siehe Kapitel Controller einrichten).

Änderungen vom 06.07.2023:

- Zur optionalen Einrichtung einer sekundären Internetschnittstelle wurde ein Kapitel ergänzt (siehe Kapitel Sekundäre Internetschnittstelle einrichten (optional)).

Änderungen vom 03.07.2023:

- Für die Admin-Accounts des Routers und des Controllers sollen individuelle Namen vergeben werden (siehe Kapitel Router einrichten und Controller einrichten).

- Bei Bedarf kann für die Schule ein eigener Account zur Erstellung von WLAN-Gutscheinen eingerichtet werden (siehe Kapitel WLAN-Gutscheine erstellen).

Änderungen vom 14.06.2023:

- Die Screenshots zur Einrichtung der UniFi-Komponenten wurden an die aktuelle Version der Network-Application angepasst (siehe Kapitel 3-11).
- Die Einrichtung der Netzwerke hat sich durch die Aktualisierung der Network-Application leicht verändert (siehe Kapitel Einrichtung Netzwerke).
- Die primäre DNS-Adresse des Cloudkeys wurde von 192.168.1.1 auf 9.9.9.9 geändert, um Probleme beim Empfangen von Update-Informationen zu verhindern (siehe Kapitel Controller einrichten).
- Die Einrichtung des Gästeportals hat sich durch die Aktualisierung der Network-Application verändert. Sie wird in einem gesonderten Kapitel beschrieben, welches nun auch die Unterkapitel zum Einrichten und Deaktivieren von WLAN-Gutscheinen umfasst (siehe Kapitel Gastportal einrichten).

Änderungen vom 23.05.2023:

- Es wurden nur kleinere Änderungen durchgeführt: z. B. das Anpassen einiger Screenshots an die aktuelle Firmware-Version des UniFi-Controllers.

Änderungen vom 04.05.2023:

- Die Einrichtungs-Hinweise für das Router-Modell DrayTek Vigor 2865 wurden aus der Anleitung entfernt, da nur noch das Modell DrayTek Vigor 2927 genutzt werden soll (siehe Kapitel Router einrichten).
- Der Screenshot für das Einstellen der Zeitzone hat sich leicht verändert (siehe Kapitel Zeitzone einstellen).

Änderung vom 11.01.2023:

- Aufgrund der neuen Cloudkey-Firmware 3.0.x wurden einige Screenshots für die Controller-Einrichtung angepasst (siehe Kapitel Controller einrichten).

Änderungen vom 22.09.2022:

- Die Konfiguration der Switch-Ports hat sich durch das Update der Controller-Software leicht verändert (siehe Kapitel Einrichtung Switch).
- Die Synology-Datenablage soll mit beiden LAN-Anschlüssen am Switch angebunden werden und die zugehörigen Ports aggregiert werden, um u. a. eine höhere Bandbreite beim Zugriff mehrerer Geräte auf die Datenablage zu ermöglichen (siehe Kapitel Einrichtung Switch).

Änderung vom 17.08.2022:

- Hinweis zur Funktion „Wireless Meshing“ aufgenommen (siehe Kapitel WLAN Access Points einrichten).

Änderung vom 03.06.2022

- Die Einrichtung aller UniFi-Komponenten wurde auf das neue Layout der UniFi-Netzwerk-Software (Version 7.1.66) angepasst (siehe Kapitel 3 - 12).

Änderung vom 16.05.2022

- Die Screenshots für das Kapitel der Router-Einrichtung wurden auf die deutsche Sprachversion angepasst.

Änderungen vom 29.04.2022

- Die bisherige Anleitung wurde in zwei Dokumente für Schulen mit und ohne Landes-Breitbandanschluss aufgeteilt.
- Um auch netzintern auf die öffentliche Webadresse der Datenablage (z. B. https//gs-musterhausen.synology.me) zugreifen zu können, muss ein interner DNS-Eintrag angelegt werden (siehe Kapitel Internen DNS-Eintrag anlegen).

Änderung vom 17.11.2021

- Um einen externen Zugriff auf Netzwerk-Ordner der Datenablage zur ermöglichen, wird eine Port-Weiterleitung für das Protokoll WebDAV eingerichtet (siehe Kapitel 2.8).

Änderungen vom 06.08.2021

- Der Management-Zugriff auf den Router soll ausschließlich über HTTPS plus Portangabe funktionieren. Dazu wurde der HTTP-Zugriff deaktiviert (siehe Kapitel 2.7).
- Der Controller-Name soll auf den Namen der jeweiligen Schule geändert werden, damit bei der Zusendung von E-Mail-Benachrichtigungen am Betreff erkannt werden kann, an welcher Schule ein Fehler aufgetreten ist (siehe Kapitel 6).
- Die Switch-Ports sollen passend zu den angeschlossenen Geräten bezeichnet werden (siehe Kapitel 9).
- Für die Drahtlos-Netzwerke soll das Verschlüsselungsprotokoll WPA3 aktiviert werden (siehe Kapitel 10).
- Die Einstellungen für die E-Mail-Benachrichtigung sollen manuell angepasst werden (siehe Kapitel 13).