Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Tablet-Integration (Schwerpunkt iOS)

Tablet-Integration in die paedML Linux und GS mit Schwerpunkt iOS

Stand 06.10.2021

paedML® Linux / GS

Version: 7.2

paedML L

LMZ Landesmedienzentrum Baden-Württemberg

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Nach Ideen von Roland Walter
Alexander Vötterle

Endredaktion

Kay Höllwarth

Bildnachweis

Symbole von “The Noun Project” (www.thenounproject.com)

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2021

Inhaltsverzeichnis

Vorwort

Im vorliegenden Dokument wird die Integration von Tablets in die *paedML Linux* beschrieben. Dieses Dokument richtet sich an Händler, Administratoren und technisch versierte Lehrkräfte, die Tablets in die *paedML Linux* einbinden wollen. Ziel ist dabei die von Windows-Geräten bekannten pädagogischen Funktionen der paedML Linux und paedML für Grundschulen auf Tablets zu übertragen.

Diese Anleitung bezieht sich auf die Version 7.2 der paedML Linux / GS. Allerdings sind ist diese Anleitung auch auf die Version 7.1 anwendbar, mit Ausnahme des Apple-School-Manager-Connectors (Kapitel 12.1) und des JAMF-School-Connectors (Kapitel 13). Für diese Connectoren ist die Version 7.2 Voraussetzung.

Die vorliegenden Konzepte sind selbstverständlich erprobt. Allerdings stehen längerfristig und groß angelegte Tests in schulischen Produktivsystemen derzeit noch aus.

Mittels MDM (Mobile Device Management) können Sie Tablets zentral verwalten. Eine grundlegende Einführung in technische Grundzüge der Tablet-Verwaltung und das Thema MDM finden Sie in unserem LMZ-Portal unter (https://www.lmz-bw.de/netzwerkloesung/fachwissen/tablets-in-der-schule/).

In einem Modellversuch hat das LMZ im Jahr 2018 den MDM-Support an Schulen evaluiert. Die darin gemachten Erfahrungen sind in den vorliegenden Text eingeflossen.

Während des Modellversuchs mussten wir erfahren, dass der großflächige Einsatz und die Verwaltung von Android-Geräten als schwierig erachtet werden kann. Gründe wie die Heterogenität des Android-Markts, unregelmäßige Betriebssystem-Updates und eine fehlende zentrale App-Lizenz-Verwaltung führen zu einem erhöhten Aufwand bei der Betreuung der Geräte. Dies wird sich vermutlich in den nächsten Jahren ändern, da sich Google mit der Weiterentwicklung der Verwaltung von mobilen Endgeräten neben dem Consumer-Markt auch den Business-Sektor als Zielgruppe erschließt.

Das im Folgenden beschriebene Konzept bezieht sich vornehmlich auf Apple-Geräte, im Folgenden iPads genannt, und beispielhaft auf die MDM-Lösung *Jamf School*. Die **grundlegende Vorgehensweise** kann auf weitere MDM-Lösungen **teilweise** übertragen werden.

Die Auswahl der genannten Hersteller ergibt sich aus Rückmeldungen und Anforderungen unserer paedML Linux und GS Kunden. **Eine Wertung oder gar Empfehlung stellt sie ausdrücklich nicht dar!**

Kapitel 12 und 13 setzen eine paedML Linux oder GS der Version 7.2 voraus. Alle anderen Kapitel setzen eine paedML Linux oder GS der Version 7.1 voraus.

1 Das Tablet-Konzept der paedML Linux und GS

Die paedML Linux und GS in ihrer jetzigen Ausprägung wurde ursprünglich für Windows-Geräte konzipiert. Tablets spielten im Schulbetrieb noch keine Rolle. Erste Konzepte zur Integration von Tablets bezogen sich daher auf Microsoft Surface Geräte. Diese können per opsi administriert und in die Domäne der paedML Linux und GS aufgenommen werden. Über die Schulkonsole können die Tablets gesteuert werden. Sie können somit zu einem vollintegrierten Bestandteil der paedML Linux und GS werden.

Windows-Geräte können vollumfänglich in das **Pädagogik-Netz** der paedML Linux und GS integriert werden (vgl. Handbücher der paedML Linux und GS).

In letzter Zeit setzen Schulen in Baden-Württemberg jedoch verstärkt auf Tablets, die nicht auf Windows 10-Basis funktionieren (im Folgenden Tablets genannt). Hier vor allem auf Tablets des Herstellers Apple (Ipads). Diese lassen sich nicht in der Domäne der paedML Linux und GS betreiben, da diese Betriebsart vom Hersteller Apple nicht vorgesehen ist. Auch andere Mechanismen der paedML Linux und GS, wie der Jugendschutzfilter, die Protokollierung von Internetzugriffen oder die Steuerung über die Schulkonsole greifen bei diesen Geräten nicht.

Im Folgenden beschreiben wir ein Konzept zur Integration von Tablets in die paedML Linux und GS. Ziel ist einerseits einen reibungsfreien technischen Betrieb zu ermöglichen. Auf der anderen Seite sollen die hohen Standards der paedML Linux und GS bezüglich der pädagogischen Sicherheit und des Datenschutzes erfüllt sein.

Zunächst sollte die Schule über ein **Mobile Device Management (MDM)** und einen Zugang zum **Apple School Manager**, kurz ASM, verfügen.

Wir empfehlen bei Verwendung von Tablets in der paedML Linux und GS die Erweiterung **Nextcloud** (kompatibel ab paedML Linux und GS 7.1+) zu installieren. Dies ermöglicht die sichere und **datenschutzkonforme Dateiablage** auf dem paedML Linux und GS Server bei der Arbeit mit Tablets.

Wir empfehlen als externen **Jugendschutzfilter** das entsprechende **BelWue-Produkt** zu konfigurieren. Eine Alternative stellt die Verwendung des per MDM konfigurierbaren **Jusprog-Webbrowsers** dar.

In der paedML Linux und GS wird ein weiteres **Netz MDM** angelegt. Mittels fest zugewiesener IP-Adressen und Weiterleitung von Informationen von der Firewall an den paedML Server wird die aus der paedML Linux und GS bekannte **Protokollierung von Internetzugriffen** ermöglicht.

Die **Synchronisation der paedML Linux und GS Benutzer in das MDM** ermöglicht eine schnelle Zuordnung von Benutzern zu ihren iPads ohne weiteren Verwaltungsaufwand. Dieses Vorgehen erscheint im Kontext sogenannter **1:1-Zuordnung**, seien sie dauerhaft oder temporär, sinnvoll.

Ein alternatives Vorgehen bei sogenannten **1:N-Zuordnungen**, etwa bei Tablet-Sätzen, die zeitweise an Klassen ausgeteilt werden, mithilfe des Apple School Managers, des Apple School Manager Connectors und der Techniken **„Temporary Shared Ipad“** und **„Shared Ipad“** wird ebenfalls beschrieben.

Die App **„Classroom“** des Herstellers Apple ermöglicht die **Steuerung des Unterrichtsgeschehens**. Dabei wird allerdings nur ein Teil des Umfangs der Schulkonsole abgebildet. Bei „Temporary Shared Ipads“ kann die Classroom App allerdings nicht verwendet werden.

Der Datenschutz muss bei der Verwendung von Ipads von vornherein mitbedacht werden. Dies betrifft sowohl das eingesetzte MDM und den Apple School Manager, als auch die eingesetzten Apps und die Integration der Tablets.

Die Verwednung von Präsentationstechnik und Druckern ist ebenfalls von vornherein mitzudenken und wird daher ebenfalls im Dokument augegriffen.

Geräte, die nicht von der Schule verwaltet werden, zum Beispiel schülereigene Geräte, die diese in der Schule benutzen dürfen (**Bring Your Own Device**) sollten in das **Gäste-Netz** integriert werden (siehe Kapitel 18).

2 Der Apple School Manager (ASM)

Voraussetzung für die Einführung eines Mobile Device Managements ist ein Zugang zum Apple School Manager (ASM).

Eine weiterführende Recherche starten Sie am besten bei:

https://www.apple.com/de/education/k12/it/

3 Das Mobile Device Management (MDM)

Bereits ab einer Stückzahl von 15 Tablets (ab einer „iPad-Klasse“) empfehlen wir Tablets zentral zu verwalten.

Hier gibt es eine Reihe von Anbietern. Unter anderem stellt Apple selbst den Apple Configurator bereit.

Drittanbieter wie *Relution* oder *Jamf School* stellen Software, sogenannte Mobile Device Managements, bereit, mit deren Hilfe Tablets verwaltet werden können. MDM-Systeme können auch in der Cloud, zum Beispiel im Rechenzentrum des Schulträgers, betrieben werden.

Die Auswahl der genannten Hersteller ergibt sich aus Rückmeldungen und Anforderungen unserer paedML Linux und GS Kunden. **Eine Wertung oder gar Empfehlung stellt sie ausdrücklich nicht dar!**

Anleitungen zur Installation und zum Betrieb von MDM würden den Rahmen dieses Dokuments bei weitem sprengen. Hier sei auf die Anleitungen der Hersteller verwiesen.

Im Kreismedienzentrum Rems-Murr-Kreis sind die folgenden Anleitungen für *Jamf School* entstanden.

Das Kreismedienzentrum Rems-Murr-Kreis kann nur Schulen aus dem Rems-Murr-Kreis unterstützen. Sehen Sie bitte daher von Supportanfragen ab und wenden Sie sich im Bedarfsfall an das für Ihren Kreis zuständige Kreismedienzentrum.

Link zu den Anleitungen: https://kreismedienzentrum-rmk.de/tablet-projekt/

4 Das Netz „MDM“

Die paedML Linux und GS verfügt über die Netze PAEDAGOGIK, INTERNET, DMZ und GAESTE. Für den Einsatz verwalteter Tablets wird ein weiteres Netz MDM angelegt. Dieses ermöglicht zum einen die Verwaltung der Tablets per MDM und genügt zum anderen möglichst hohen Sicherheitskriterien.

Zunächst wird im ESXi-Host bzw. im vSphere-Center ein virtueller Switch hinzugefügt. Anschließend wird eine neue Portgruppe MDM angelegt und konfiguriert.

Das in diesem Kapitel dokumentierte Vorgehen bezieht sich auf einen ESXi-Host in der weit verbreiteten Version 6.7.

Der Aufbau der zugehörigen Netzwerkinfrastruktur (Switch, Access-Points) ist nicht Bestandteil dieser Anleitung. Die Arbeiten müssen im Anschluss von einem erfahrenen und kompetenten Dienstleister durchgeführt werden.

Für die Arbeiten am ESXi-Host muss die Firewall und damit auch alle anderen virtuellen Maschinen der paedML Linux und GS heruntergefahren werden.

4.1 Einen virtuellen Switch hinzufügen

Melden Sie sich an Ihrem ESXi-Host mit dem Benutzer *root* an.

Fahren Sie die virtuellen Maschinen W10AdminVM; opsi-Server, Server und Firewall in dieser Reihenfolge herunter.

Klicken Sie auf den Reiter *Netzwerk* und wechseln Sie in den Reiter *Virtuelle Switches*. Klicken Sie auf *Virtuellen Standard-Switch hinzufügen*.

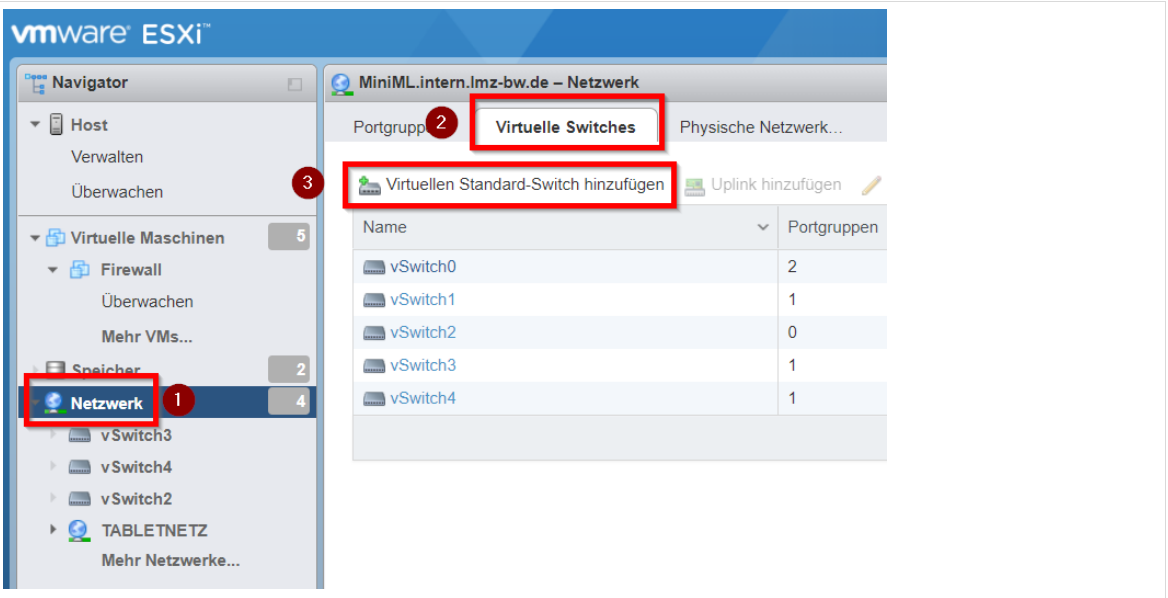

Abb. 1: Virtuellen Switch hinzufügen

Vergeben Sie einen Namen für den neuen virtuellen Switch, ordnen Sie einen freien physischen Adapter zu und klicken Sie auf *Hinzufügen*.

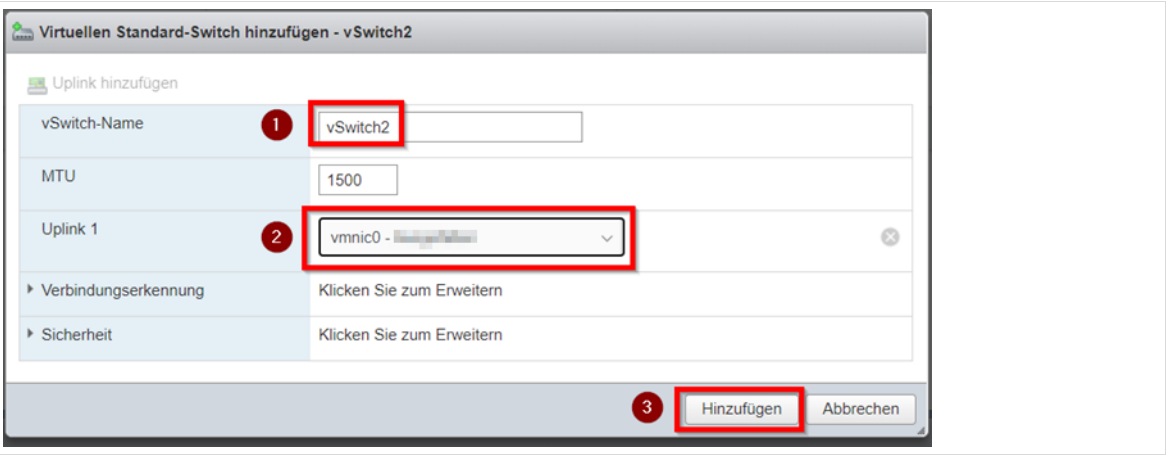

Abb. 2: Neuer Virtueller Switch

Der neu angelegte virtuelle Switch erscheint nun in der Übersicht.

Abb. 3: Neuer virtueller Switch erfolgreich hinzugefügt

4.2 Die Portgruppe MDM

Wechseln Sie in den Reiter *Portgruppen* und gehen Sie dort auf *Portgruppe hinzufügen*.

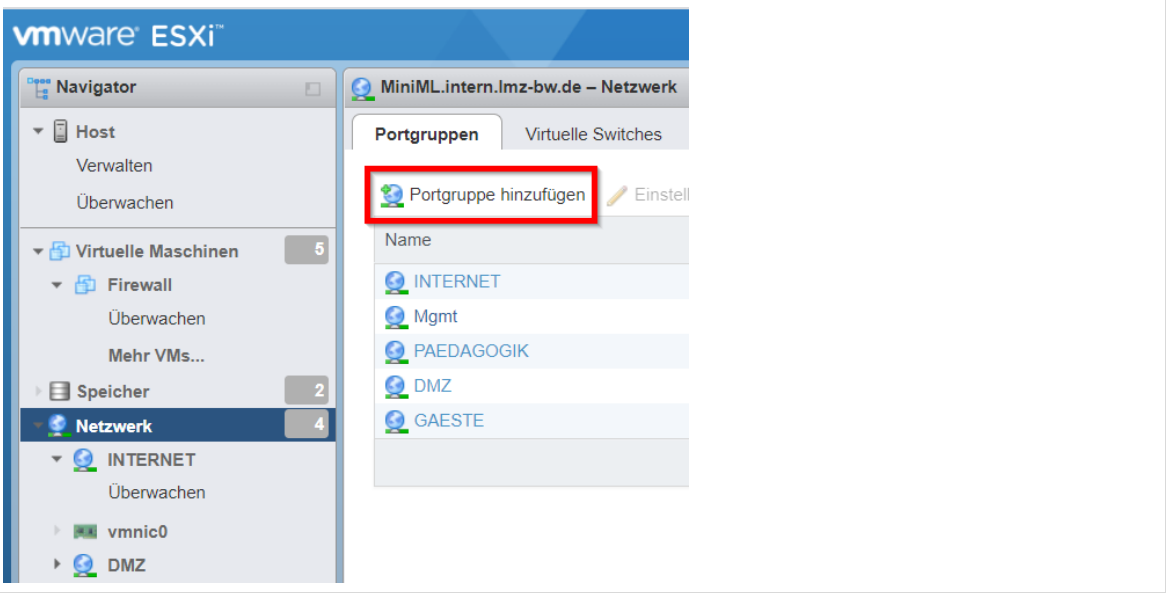

Abb. 4: Portgruppe hinzufügen

Vergeben Sie den Namen *MDM* und ordnen Sie den zuvor neu erstellten virtuellen Switch zu. Klicken Sie dann auf *Hinzufügen*.

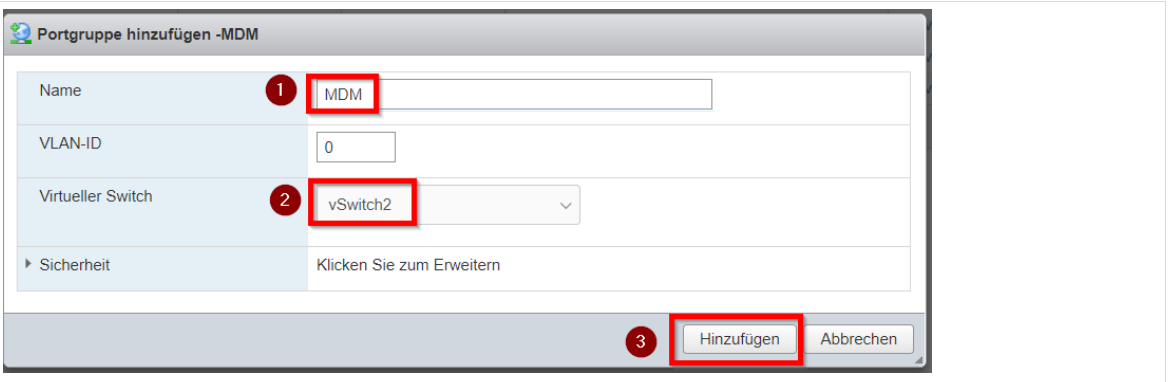

Abb. Portgruppe konfigurieren

Die neue Portgruppe erscheint in der Übersicht.

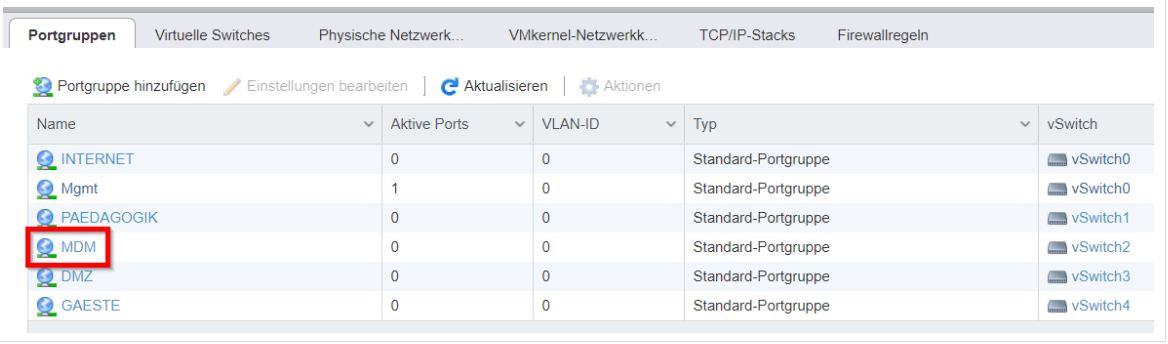

Abb. 5: Portgruppe Übersicht.

Klicken Sie im ESXi-Host auf *Virtuelle Maschinen* und auf *Firewall*. *Bearbeiten* Sie die virtuelle Maschine *Firewall*.

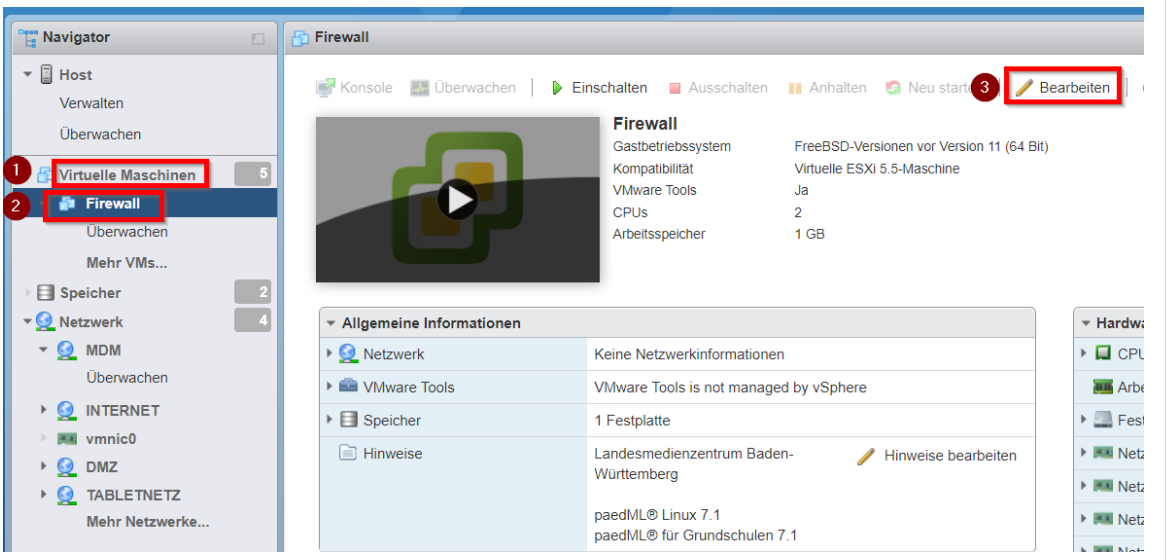

Abb. 6: Firewall bearbeiten.

Klicken Sie im nächsten Dialog auf *Netzwerkadapter hinzufügen*.

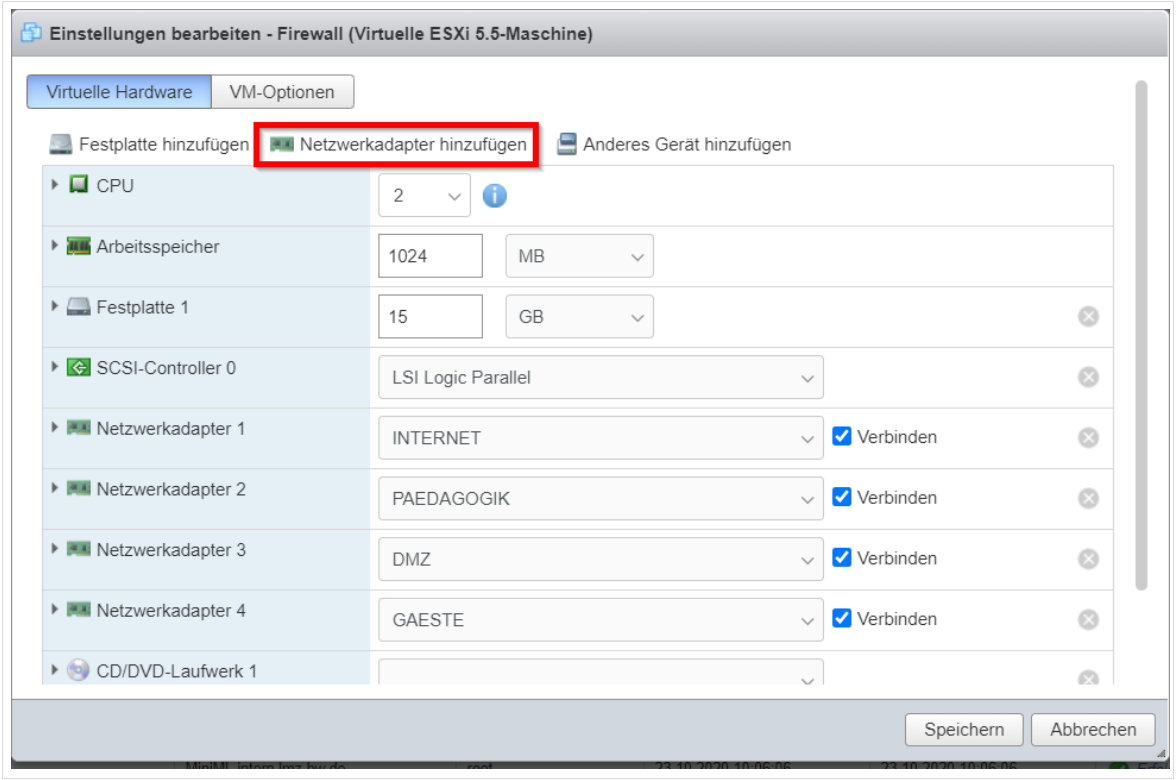

Abb. 7: Netzwerkadapter hinzufügen.

Ordnen Sie dem Netzwerkadapter die Portgruppe *MDM* zu und klicken Sie auf *Speichern*.

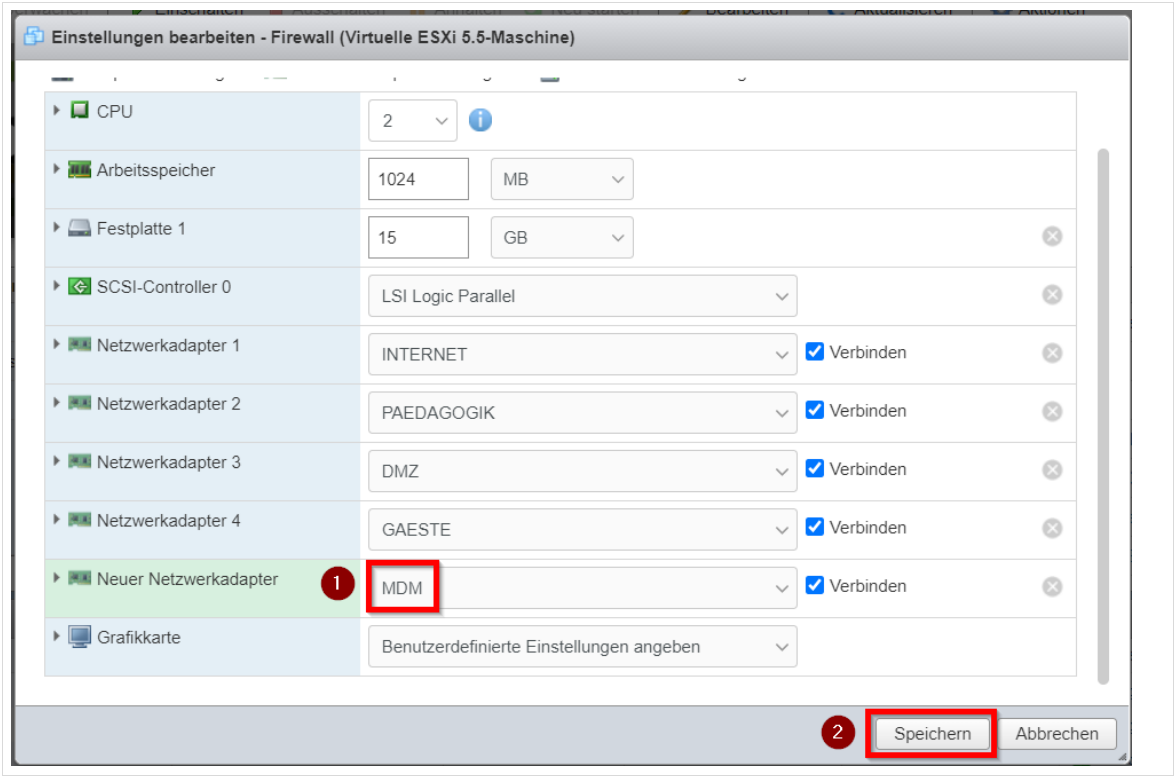

Abb. 8: Netzwerkadapter konfigurieren.

Die Arbeiten am ESXi-Host sind damit beendet. Fahren Sie die virtuellen Maschinen hoch und melden Sie sich an der *W10AdminVM* an.

5 Firewall-Regelwerk für MDM

Für das Netz MDM wird ein Satz von Firewall-Regeln erstellt, der die Verwaltung der Tablets ermöglicht und trotzdem einen hohen Sicherheitsstandard gewährleistet.

Melden Sie sich an der *Firewall* als Administrator an.

5.1 Anpassung an der Schnittstelle GAESTE

Für das Gästenetz wird in der Standardkonfiguration der paedML Linux und GS ein sehr großer Netzbereich reserviert, welcher auch den im Folgenden einzurichtenden Bereich des neuen MDM-Netzes abdeckt. Die Konfiguration für das Gäste-Netz muss daher angepasst werden.

Dies ist nur notwendig, wenn Sie das Gäste-Netz aktiviert haben oder planen, es zu aktiveren.

Klicken Sie unter dem Reiter *Schnittstellen* auf *GAESTE*.

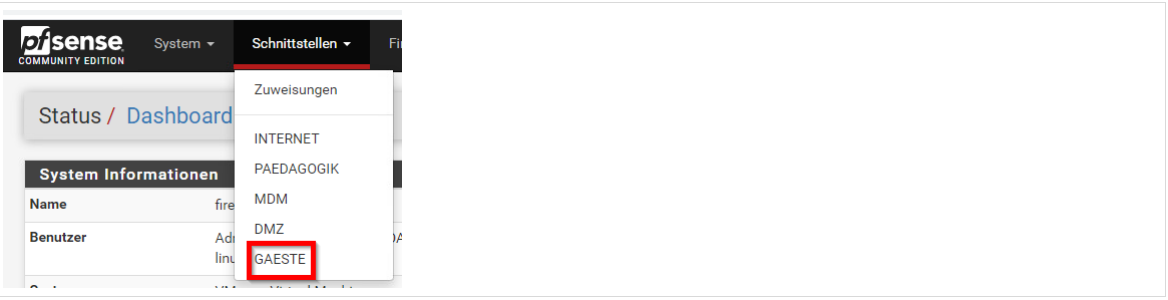

Abb. 9: Schnitstelle GAESTE

Tragen Sie *14* ein. Mit dieser Maßnahme verkleinern Sie das Gäste-Netz auf den IP-Bereich 172.16.0.1 – 172.19.255.254.

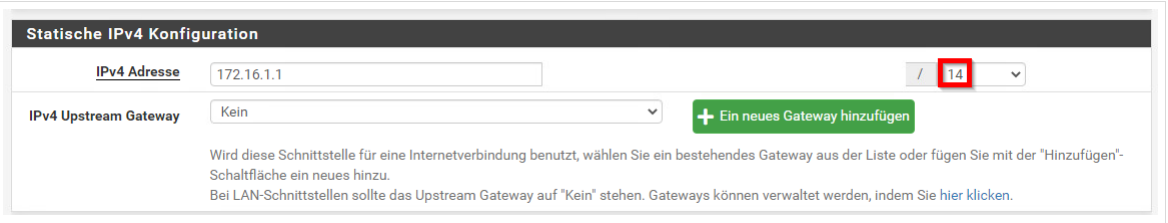

Abb. 10: Veränderung der Netzmaske

Speichern Sie die Änderungen und bestätigen Sie deren Anwendung.

Öffnen Sie unter dem Reiter *Dienste DHCP-Server*, klicken Sie dort auf GAESTE.

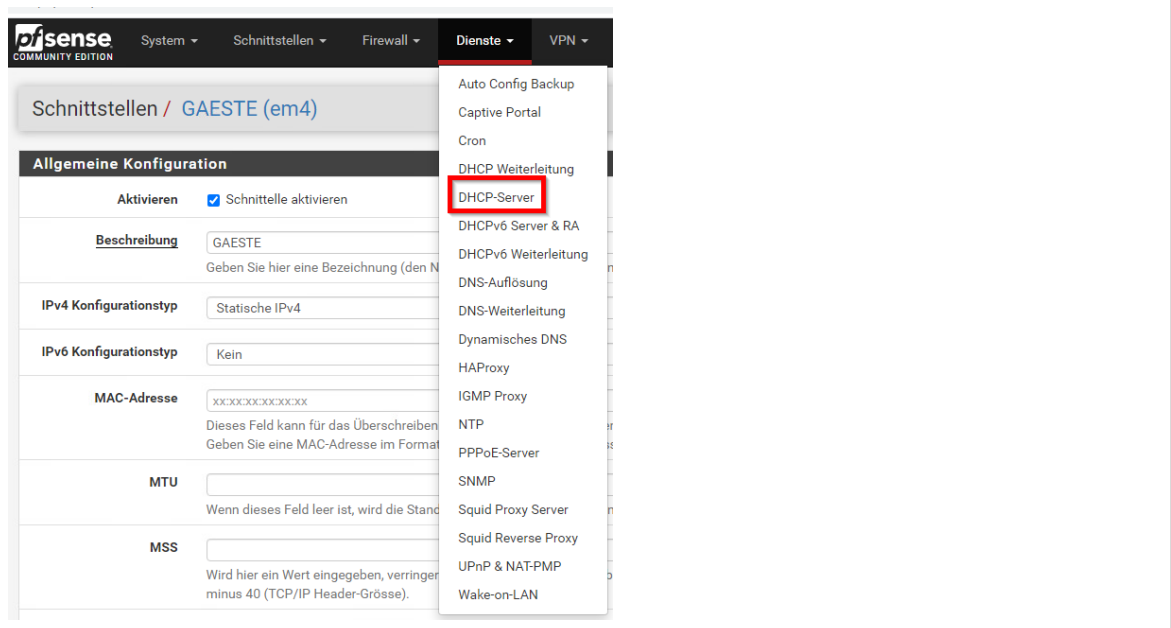

Abb. 11: DHCP-Server des Gäste-Netzes

Tragen Sie als *Bis*-Wert *172.19.255.254* ein. Dies ist nur eine Empfehlung und kann bei der Zuweisung fester IP-Adressen per DHCP variieren (siehe unten).

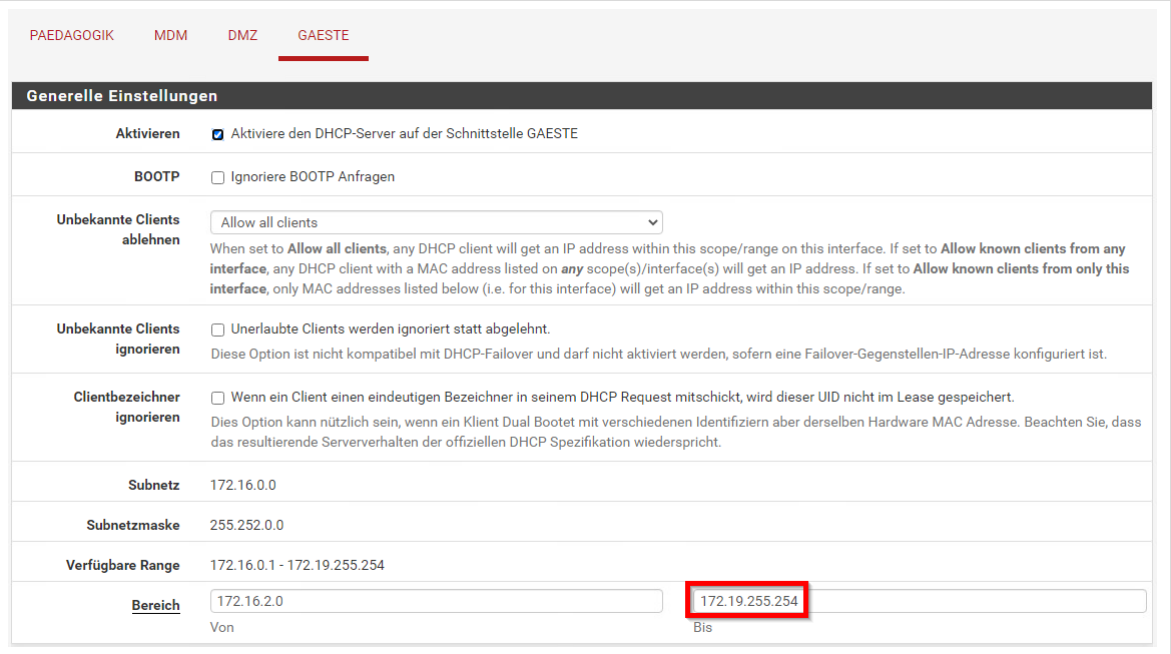

Abb. 12: Änderungen anwenden.

Speichern Sie die Änderungen.

In diesem Kapitel 5.1 „schneiden“ Sie einen Teil des sehr großen Gäste-Netzes ab. Prüfen Sie, ob Sie per DHCP feste IP-Adressen im abgeschnittenen Bereich zuweisen oder solche IP-Adressen direkt in der Hardware (Access-Points) eingetragen wurden!

5.2 Das Interface MDM hinzufügen

Zunächst muss in der Firewall eine neue Schnittstelle „*MDM*“ erstellt werden. Öffnen Sie dazu den Reiter *Schnittstellen* und klicken Sie anschließend auf *Zuweisungen*.

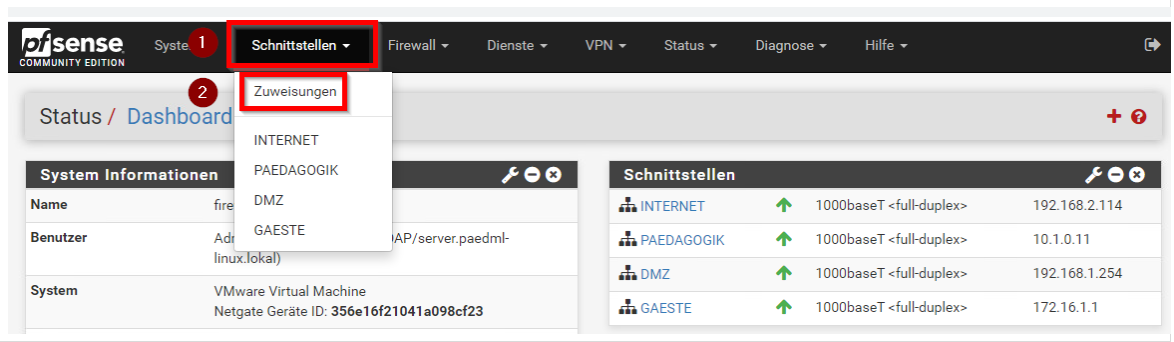

Abb. 13: Schnittstelle erstellen

Klicken Sie auf *Hinzufügen*.

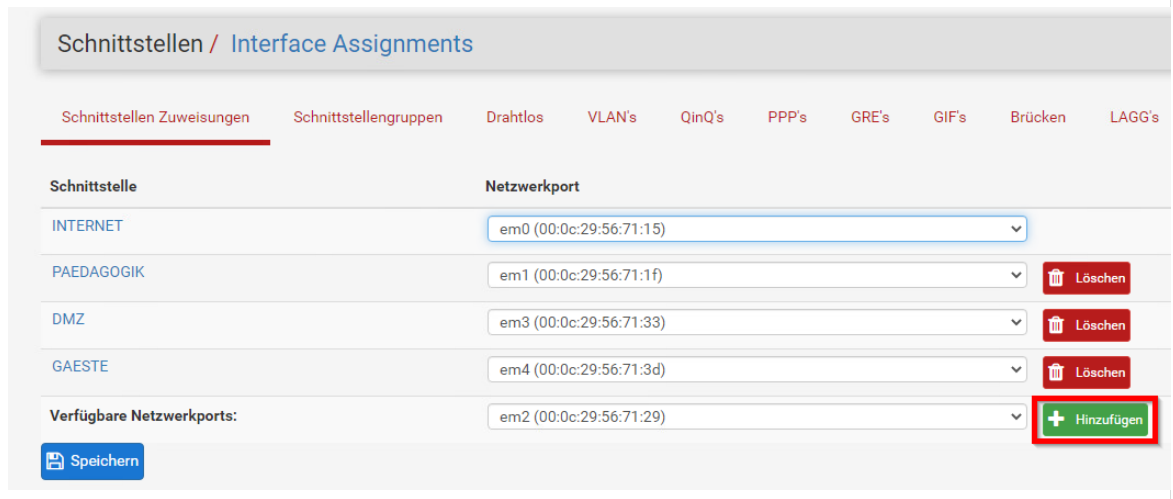

Abb. 14: Schnittstelle hinzufügen.

Die neue Schnittstelle erscheint in der Übersicht (hier *OPT1*). Klicken Sie auf die neue Schnittstelle. Setzen Sie den Haken bei *Schnittstelle aktivieren*, tragen Sie als *Beschreibung MDM* ein und setzen Sie *IPv4 Konfigurationstyp* auf *Statische IPv4*.

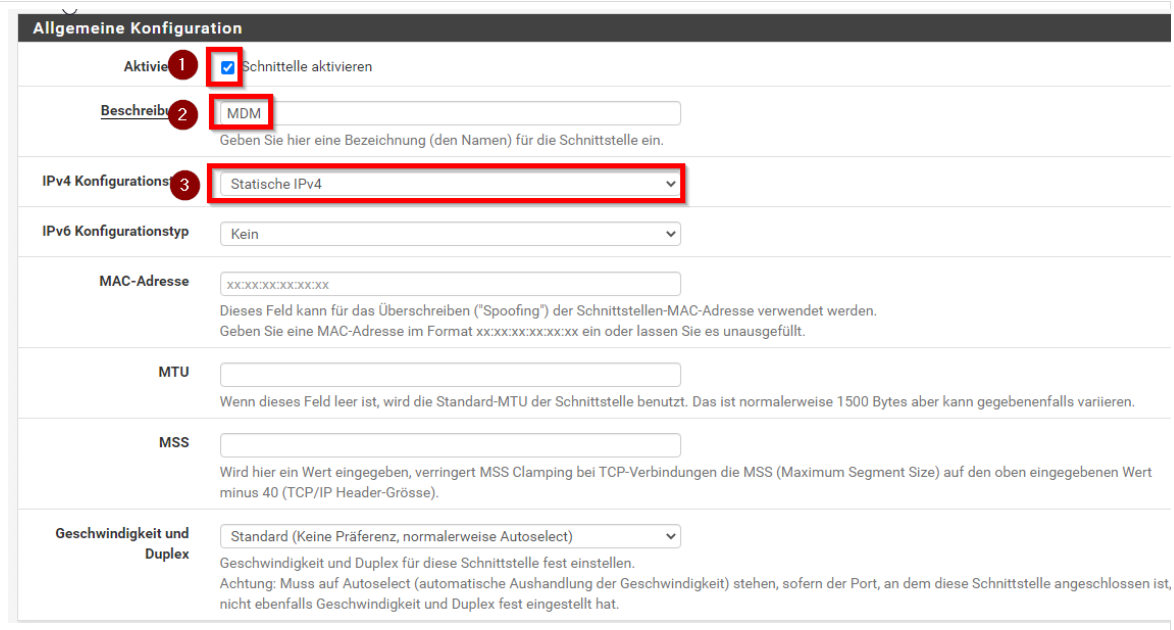

Abb. 15: Allgemeine Konfiguration

Tragen Sie als *IPv4-Adresse 172.20.1.1* und als Netz-Maske *14* ein.

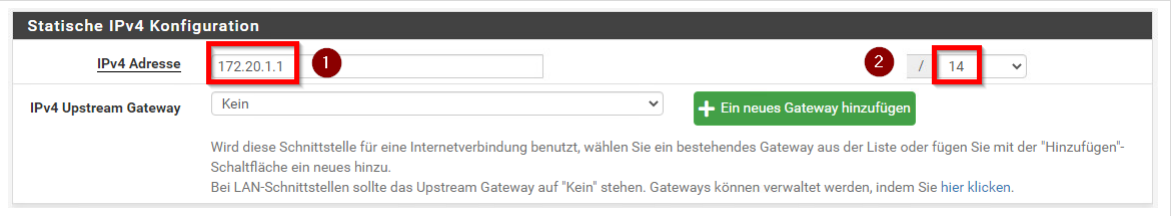

Abb. 16: Statische IPv4-Konfiguration.

Speichern Sie die Einstellungen.

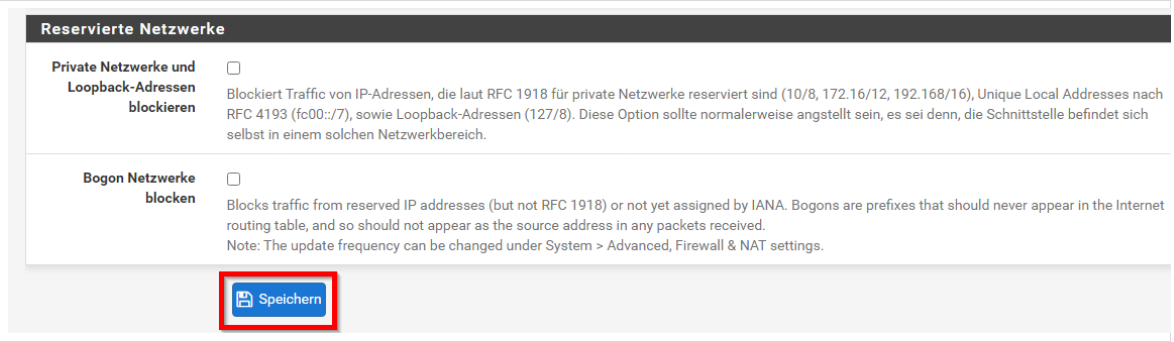

Abb. 17: Speichern.

Und wenden Sie die Änderungen an.

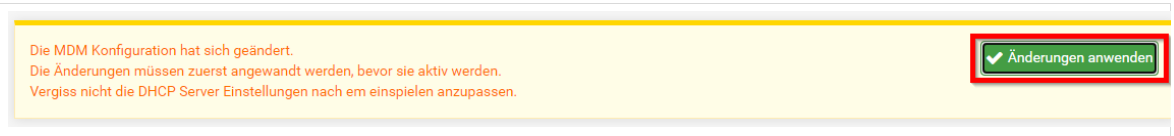

Abb. 18: Änderungen anwenden.

Die Schnittstelle *MDM* erscheint jetzt in der Übersicht der Firewall.

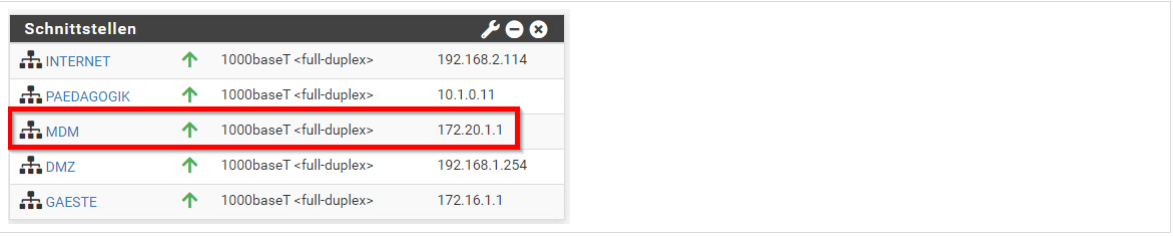

Abb. 19: Änderungen anwenden.

5.3 Regelwerk für MDM

5.3.1 Den Alias MDMPorts erstellen

In Testszenarien und an Testschulen hat sich herausgestellt, dass ein problemloses Verwalten von Tablets per MDM nur mit einigen geöffneten Ports möglich ist. Im Folgenden wird ein Port-Alias *MDMPorts* mit den benötigten Ports erstellt. Es ist nicht auszuschließen, dass sich die Anforderungen in Zukunft verändern und damit eine Anpassung des Alias nötig werden wird.

Klicken Sie auf *Firewall | Aliase*.

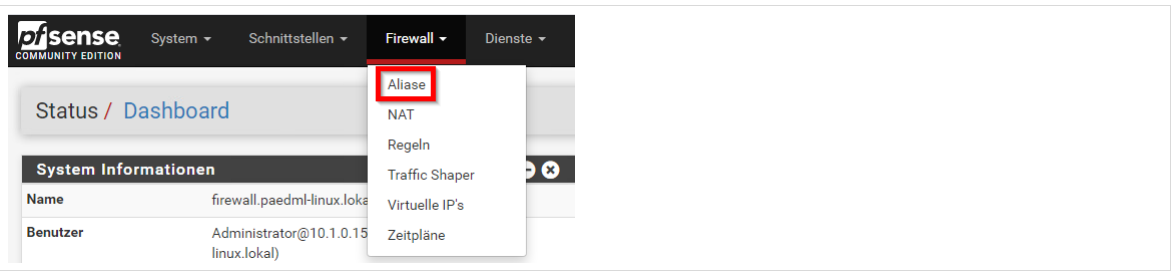

Abb. 20: Firewall | Aliase

Klicken Sie auf *Ports* und *Hinzufügen*.

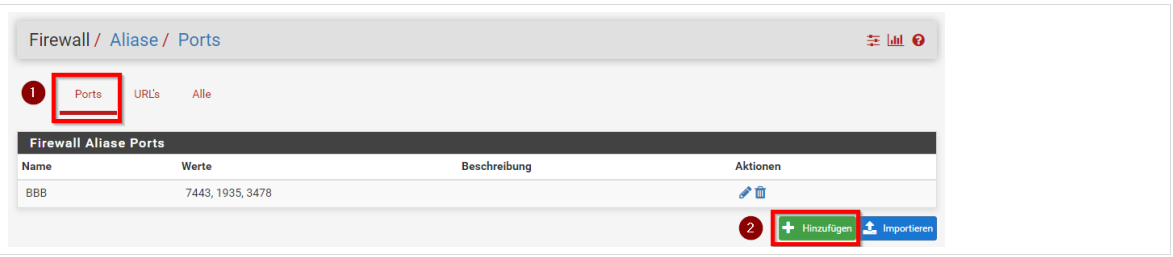

Abb. 21: Ports hinzufügen.

Als Namen tragen Sie *MDMPorts* ein. Fügen Sie insgesamt vier Ports hinzu und tragen sie Ports *80, 443, 5223 und 5228* ein. Die Auswahl der Ports bezieht sich auf die Verwendung von iPads und dem MDM *Jamf School*.

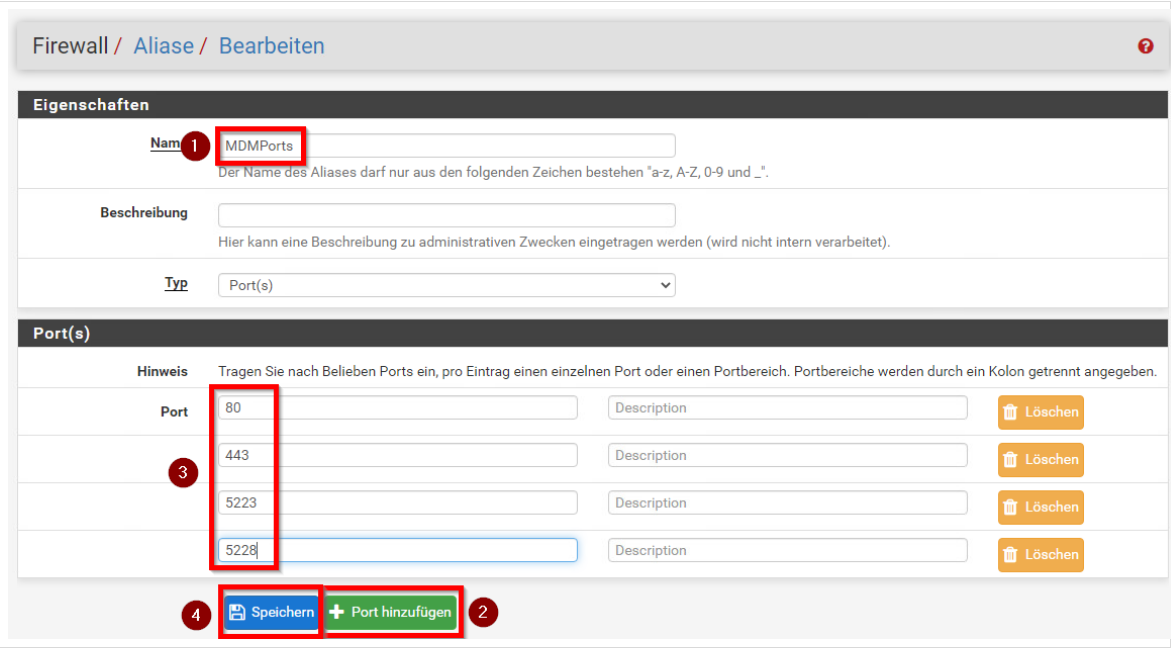

Abb. 22: MDMPorts konfigurieren.

Wenden Sie die Änderungen an.

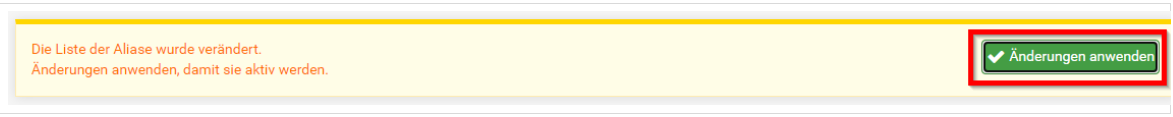

Abb. 23: Änderungen anwenden.

Der neu erstellte Alias erscheint nun in der Übersicht.

Abb. 24: Übersicht Port-Aliase

5.3.2 Regelwerk für die Schnittstelle MDM

5.3.2.1 Erlaube MDMPorts

Navigieren Sie zu *Firewall | Regeln | MDM*. Klicken Sie auf *Hinzufügen*.

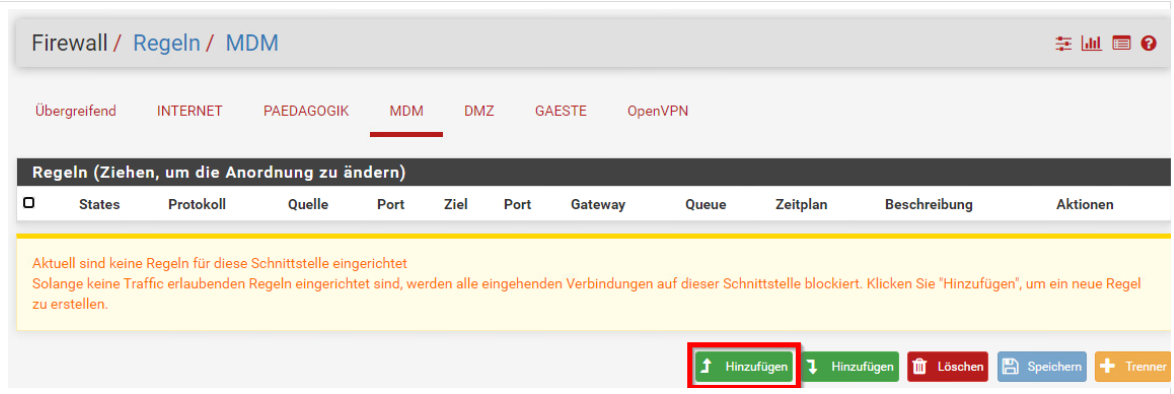

Abb. 25: Regel Hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: *Erlauben*
- Protokoll: *TCP*
- Quelle: *MDM net*
- Ziel: *alle*
- Bereich der Zielports: Von *(anderer) MDMPorts* bis *(anderer) MDMPorts*
- Beschreibung: *Erlaube MDMPorts*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

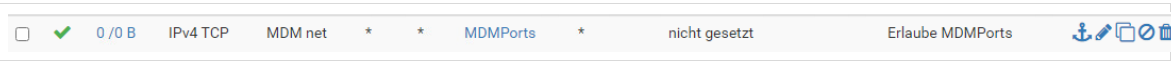

Abb. 26: Regel: Erlaube MDMPorts

5.3.2.2 Verbiete Zugriff auf GAESTE-Netz

Klicken Sie auf *Hinzufügen.*

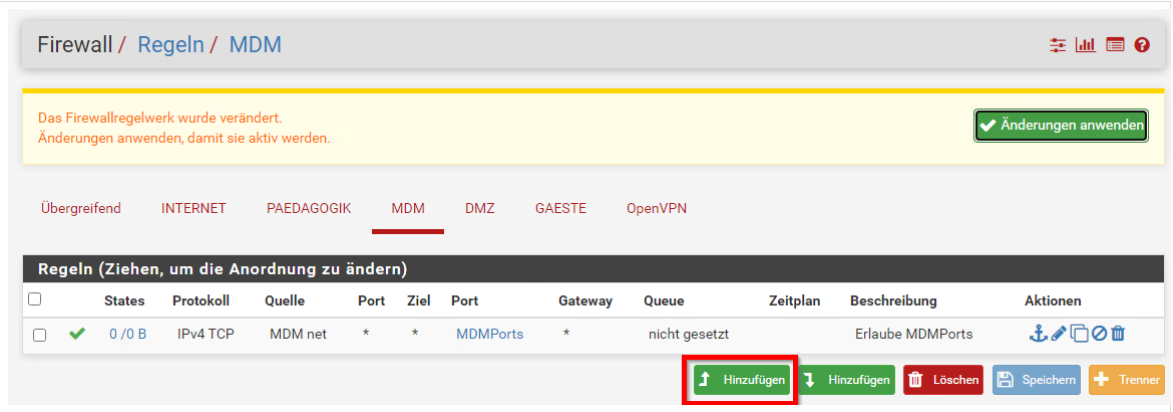

Abb. 27: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: *Blockieren*
- Protokoll: *alle*
- Quelle: *MDM net*

- Ziel: *GAESTE net*
- Beschreibung: *Verbiete Zugriff auf Gäste-Netz*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

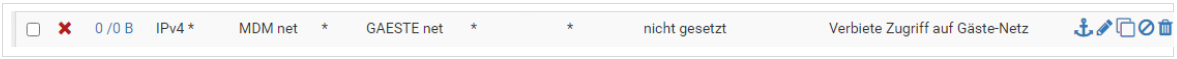

Abb. 28: Regel: Erlaube MDMPorts

5.3.2.3 Erlaube Samba-Zugriffe auf den paedML-Server

Klicken Sie auf *Hinzufügen.*

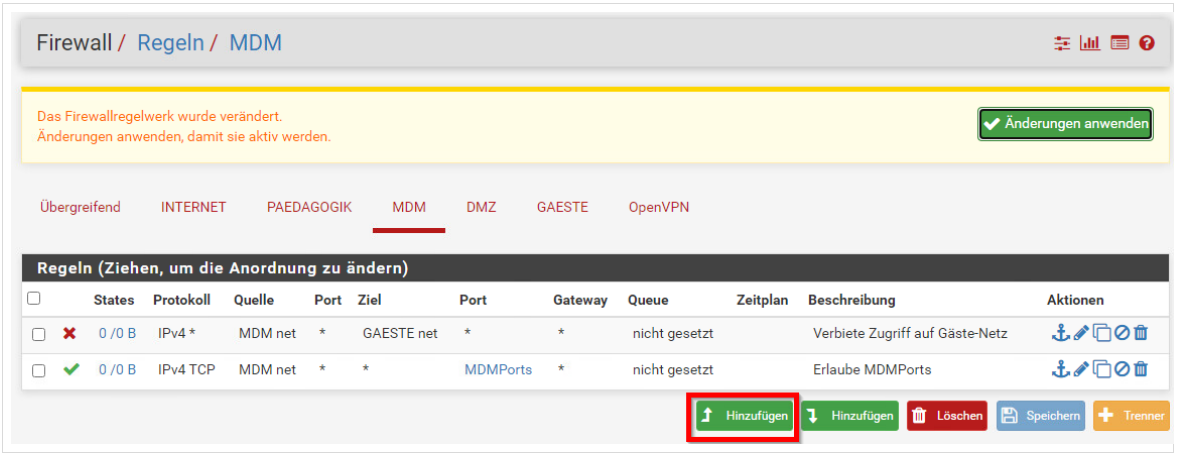

Abb. 29: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: Erlauben
- Protokoll: *TCP*
- Quelle: *MDM net*
- Ziel: Einzelner *Host oder Alias 10.1.0.1*
- Bereich der Zielports: Von *MS DS 445* bis *MS DS 445*
- Beschreibung: *Erlaube Samba-Zugriffe auf Server*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

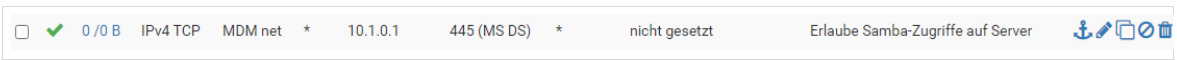

Abb. 30: Regel: Erlaube Samba-Zugriff auf Server

5.3.2.4 Erlaube DNS-Zugriffe

Klicken Sie auf *Hinzufügen.*

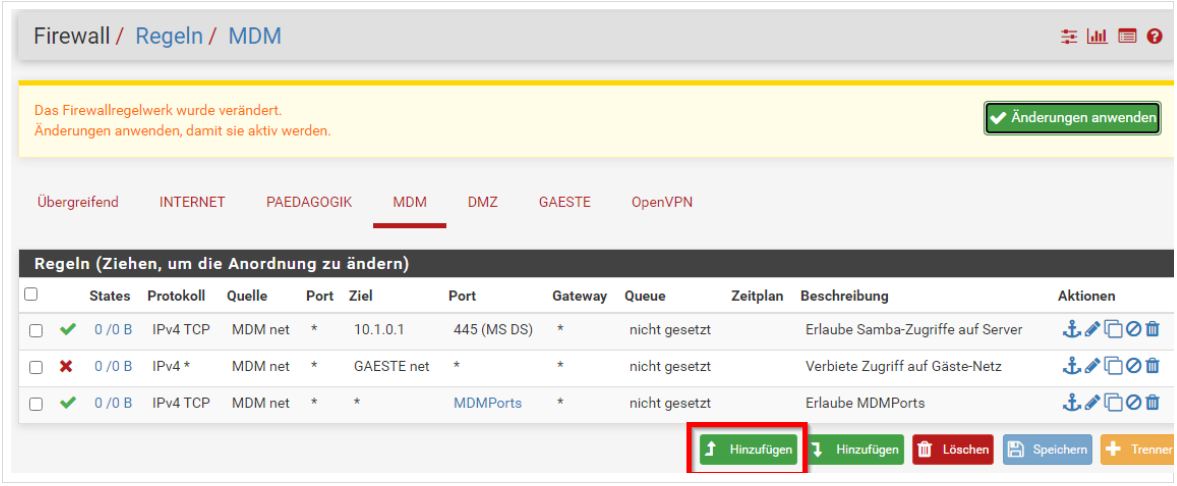

Abb. 31: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: *Erlauben*
- Protokoll: *UDP*
- Quelle: *MDM net*
- Ziel: MDM address
- Bereich der Zielports: Von *DNS 53* bis *DNS 53*
- Beschreibung: *Erlaube DNS-Zugriff*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

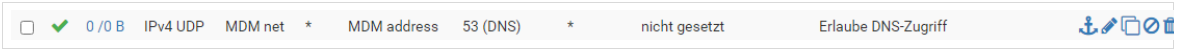

Abb. 32: Regel: Erlaube DNS-Zugriff

5.3.2.5 Erlaube ICMP-Anfragen

Klicken Sie auf *Hinzufügen.*

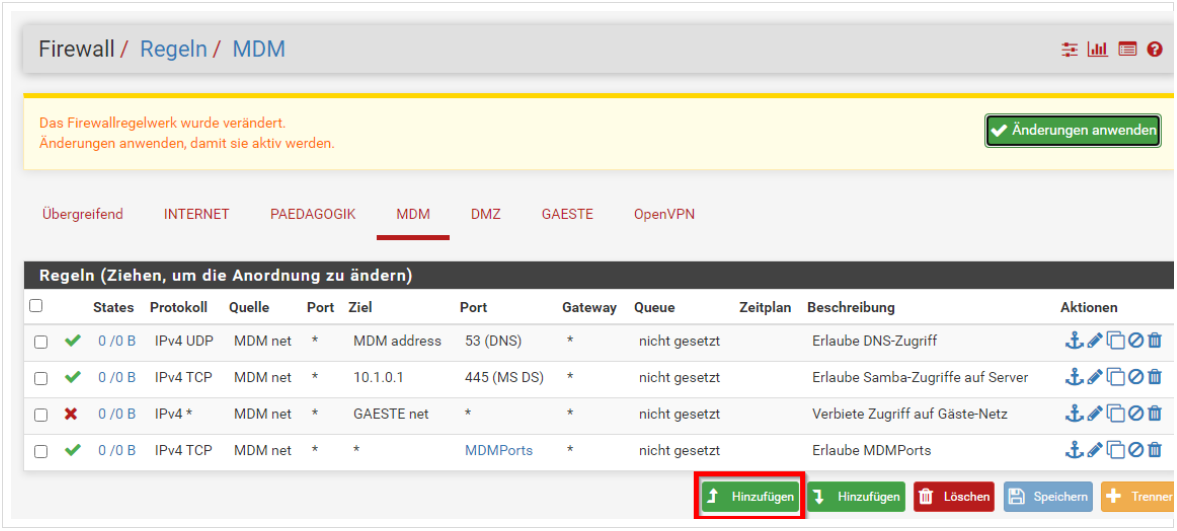

Abb. 33: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: *Erlauben*
- Protokoll: *ICMP*
- *ICMP-Untertypen: alle*
- Quelle: *MDM net*
- Ziel: *alle*
- Beschreibung: *Erlaube ICMP*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

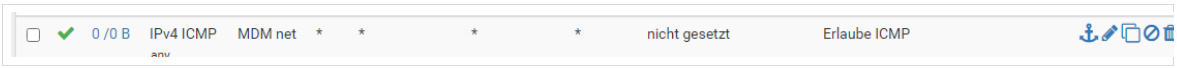

Abb. 34: Regel: Erlaube ICMP

5.3.2.6 Optional: Erlaube Video-Konferenz-Tools (BBB und Jitsi-Meet)

Video-Konferenztools wie Big Blue Button oder Jitsi-Meet benötigen geöffnete Ports in der Firewall. Im Folgenden wird das Anlegen entsprechender Firewall-Regeln für BBB und Jitsi-Meet beschrieben. Die Arbeiten müssen nur ausgeführt werden, wenn die Videokonferenz-Tools eingesetzt werden. Sie sind für den Einsatz des MDM-Netzes nicht erforderlich.

Big Blue Button

Klicken Sie auf *Hinzufügen.*

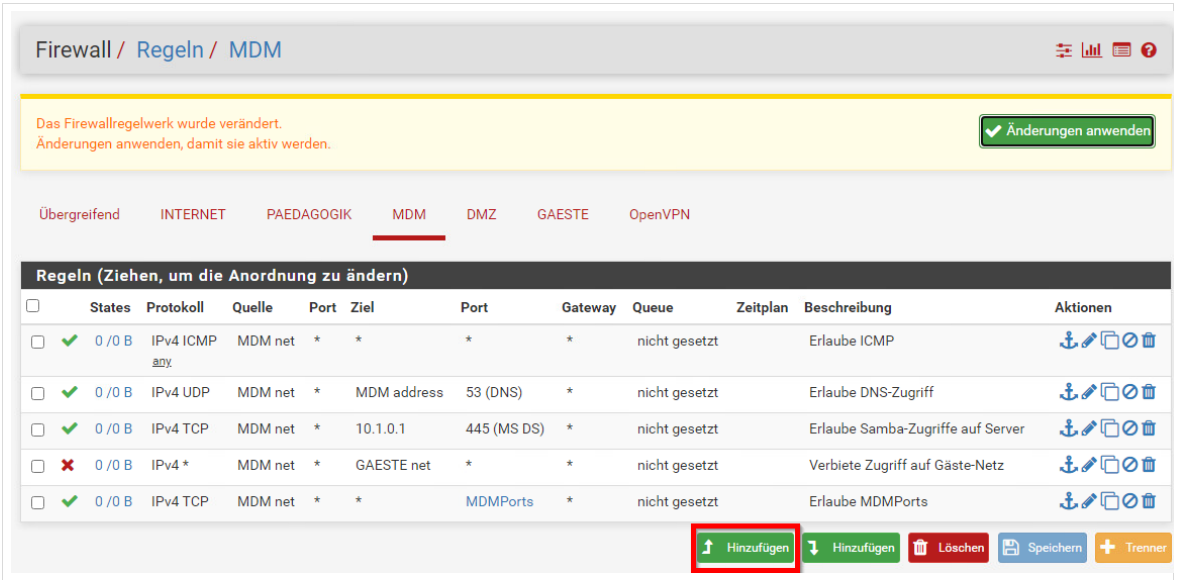

Abb. 35: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: Erlauben
- Protokoll: *UDP*
- Quelle: *MDM net*
- Ziel: *alle*

- Bereich der Zielports: Von 3478 bis *3478*
- Beschreibung: *Erlaube UDP 3478 für Big Blue Button*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

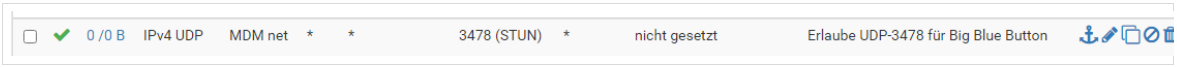

Abb. 36: Regel: Erlaube UDP 3478 für Big Blue Button

Klicken Sie auf *Hinzufügen.*

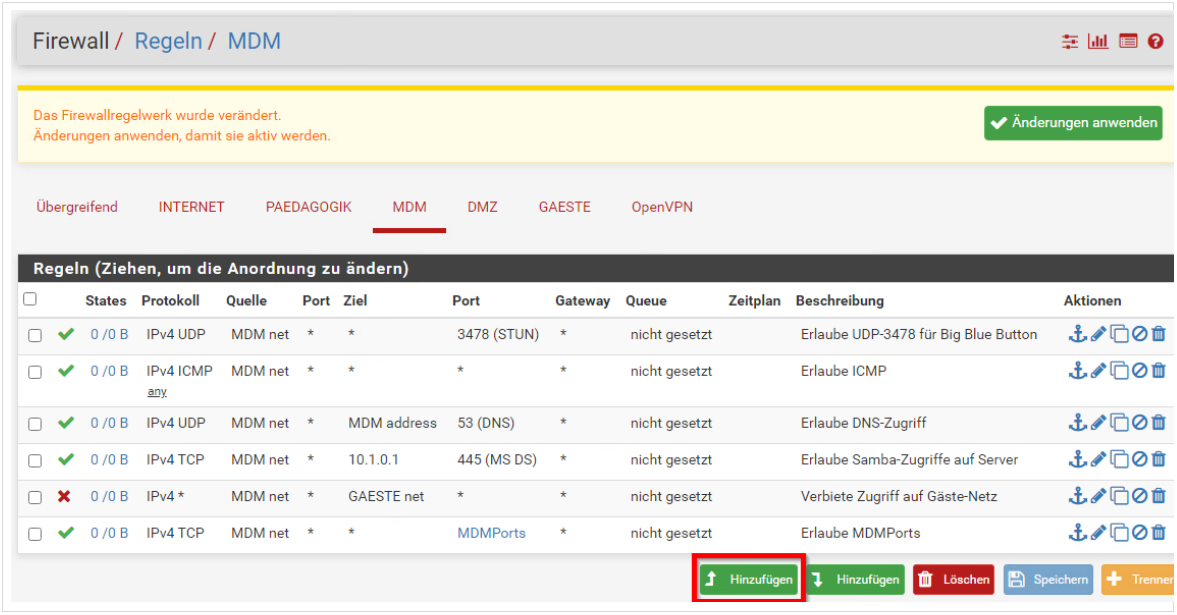

Abb. 37: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: Erlauben
- Protokoll: *TCP*
- Quelle: *MDM net*
- Ziel: *alle*
- Bereich der Zielports: Von *1935* bis *1935*
- Beschreibung: *Erlaube TCP 1935 für Big Blue Button*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

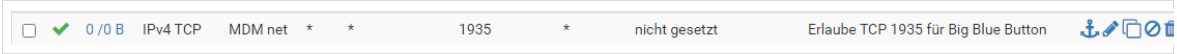

Abb. 38: Regel: Erlaube TCP 1935 für Big Blue Button

Klicken Sie auf *Hinzufügen.*

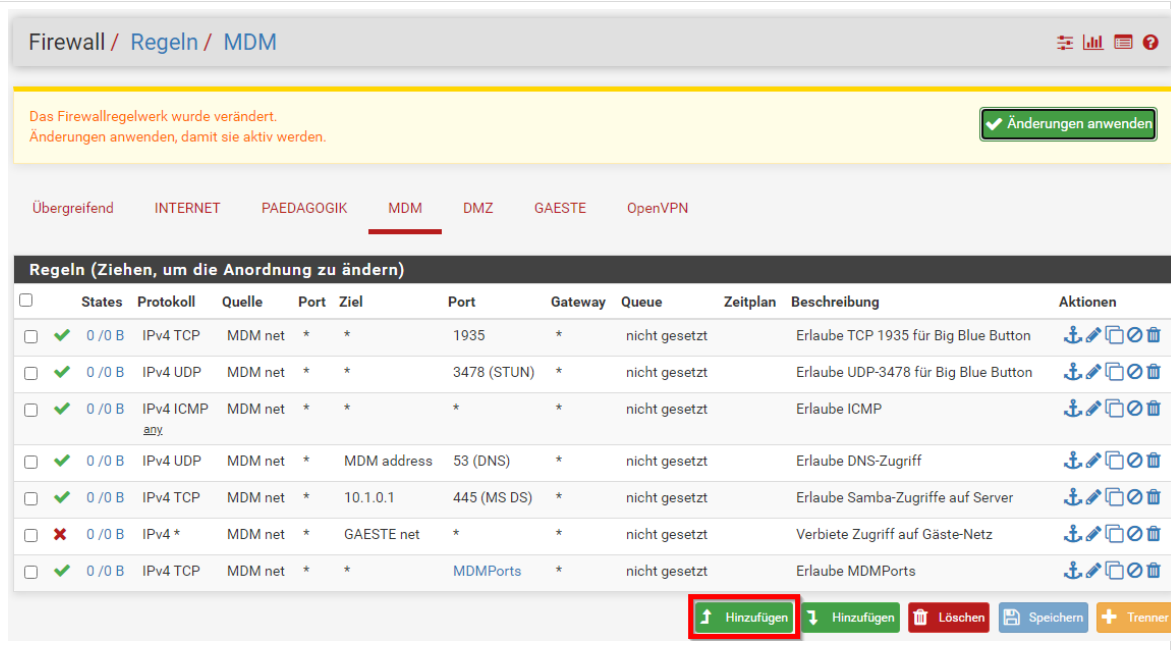

Abb. 39: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: Erlauben
- Protokoll: *TCP*
- Quelle: *MDM net*
- Ziel: *alle*
- Bereich der Zielports: Von 7443 bis *7443*
- Beschreibung: *Erlaube TCP 7443 für Big Blue Button*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

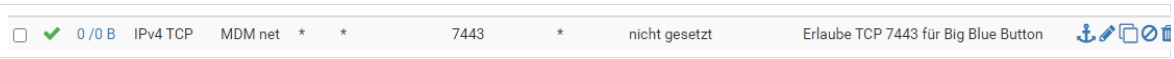

Abb. 40: Regel: Erlaube TCP 7443 für Big Blue Button

Jitsi-Meet

Klicken Sie auf *Hinzufügen.*

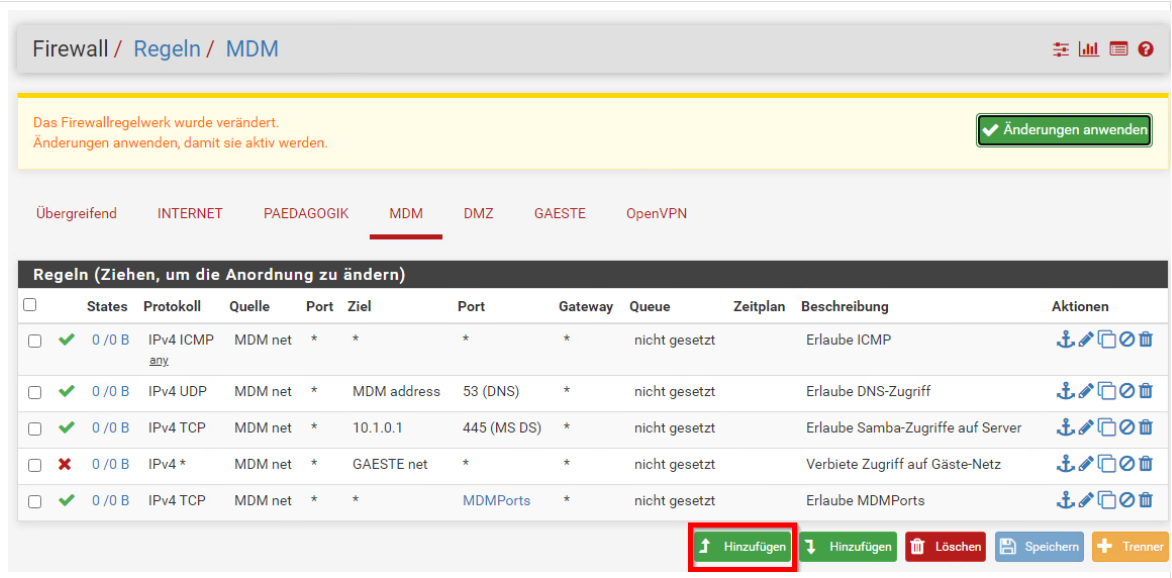

Abb. 41: Regel hinzufügen.

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: Erlauben
- Protokoll: *UDP*
- Quelle: *MDM net*
- Ziel: *alle*
- Bereich der Zielports: Von 10000 bis *10000*
- Beschreibung: *Erlaube UDP 10000 für Jitsi-Meet*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel.

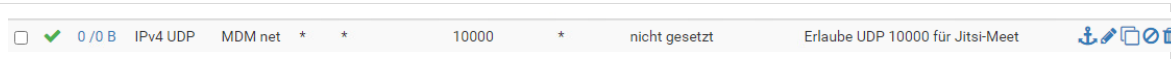

Abb. 42: Regel: Erlaube UDP 10000 für Jitsi-Meet

5.3.2.7 Änderungen anwenden

Das Regelwerk für das Netz MDM ist fertiggestellt. Die Änderungen können angewendet werden.

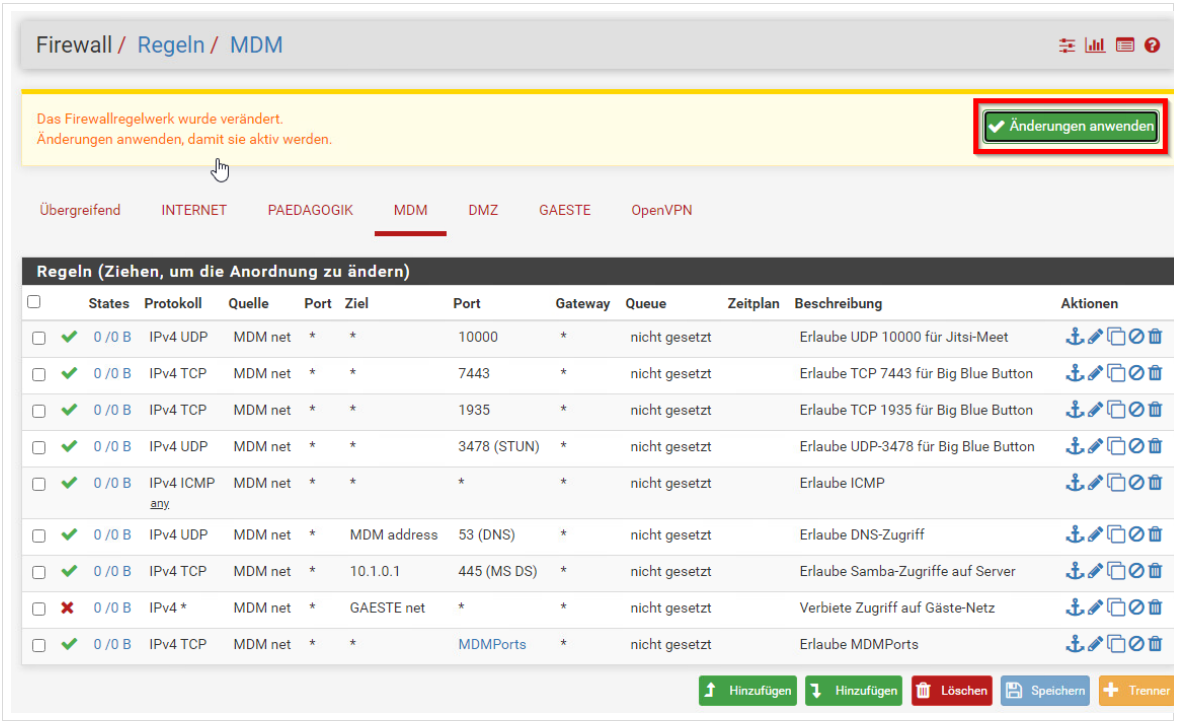

Abb. 43: Änderungen anwenden

5.3.2.8 Übersicht Regelwerk MDM

Die oberen fünf Regeln sind optionale Regeln.

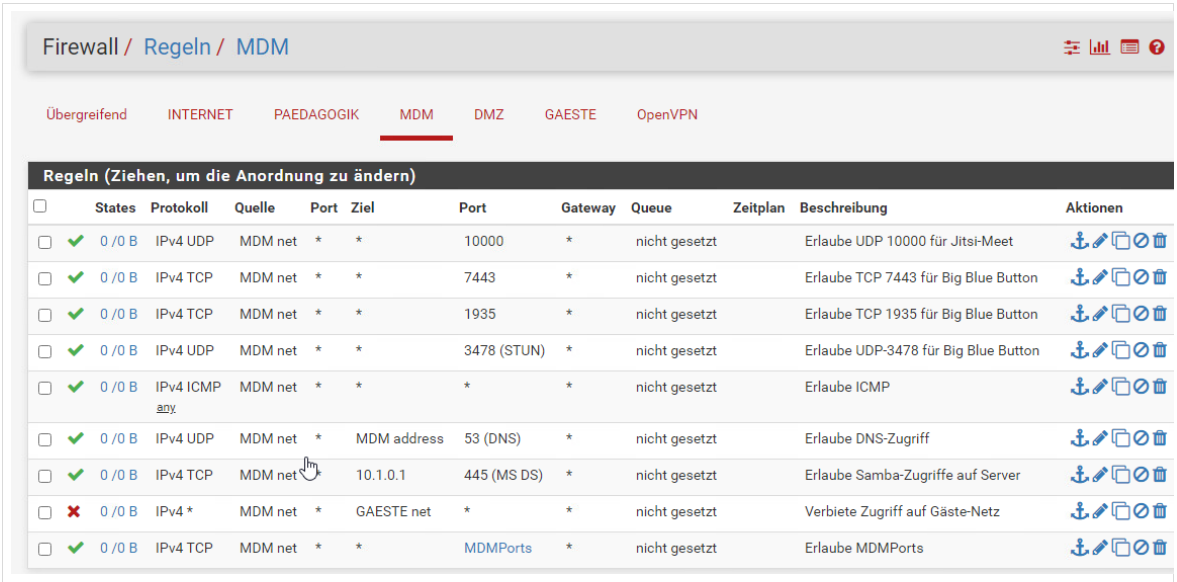

Abb. 44: Übersicht Regelwerk MDM

5.4 Anpassungen an den DMZ-Regeln

5.4.1 Blockiere Zugriffe auf MDM

Im Netz *DMZ* befindet sich in der paedML Linux und GS die Maschine *Nextcloud*. Das Netz wird im Rahmen der Erweiterung der paedML um die Nextcloud erstellt. Wie Sie die virtuelle Maschine Nextcloud importieren, konfigurieren und nutzen, finden Sie im Downloadbereich der paedML Linux: https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/

Navigieren Sie zu *Firewall | Regeln | DMZ*. Kopieren Sie de Regel *„Verbiete Zugriff auf PAEDAGOGIK"*.

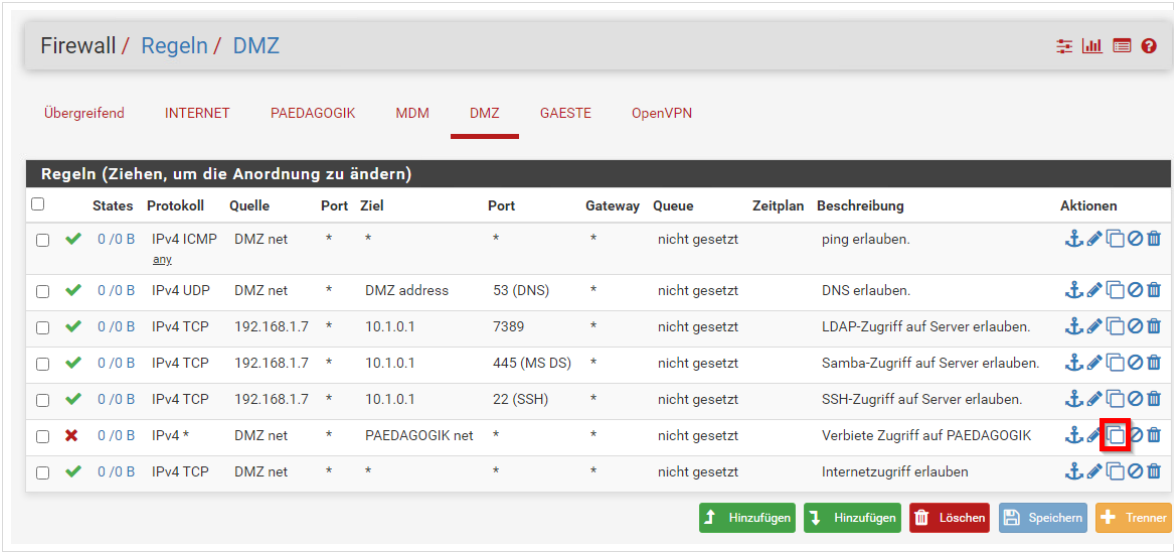

Abb. 45: Regel kopieren

Konfigurieren Sie die folgenden Einstellungen:

- Aktion: *Blockieren*
- Protokoll: *Alle*
- Quelle: *DMZ net*
- Ziel: *MDM net*
- Beschreibung: *Verbiete Zugriff auf MDM*

Bestätigen Sie die Einstellungen mit *Speichern*. Überprüfen Sie die Regel. Wenden Sie die Änderungen an.

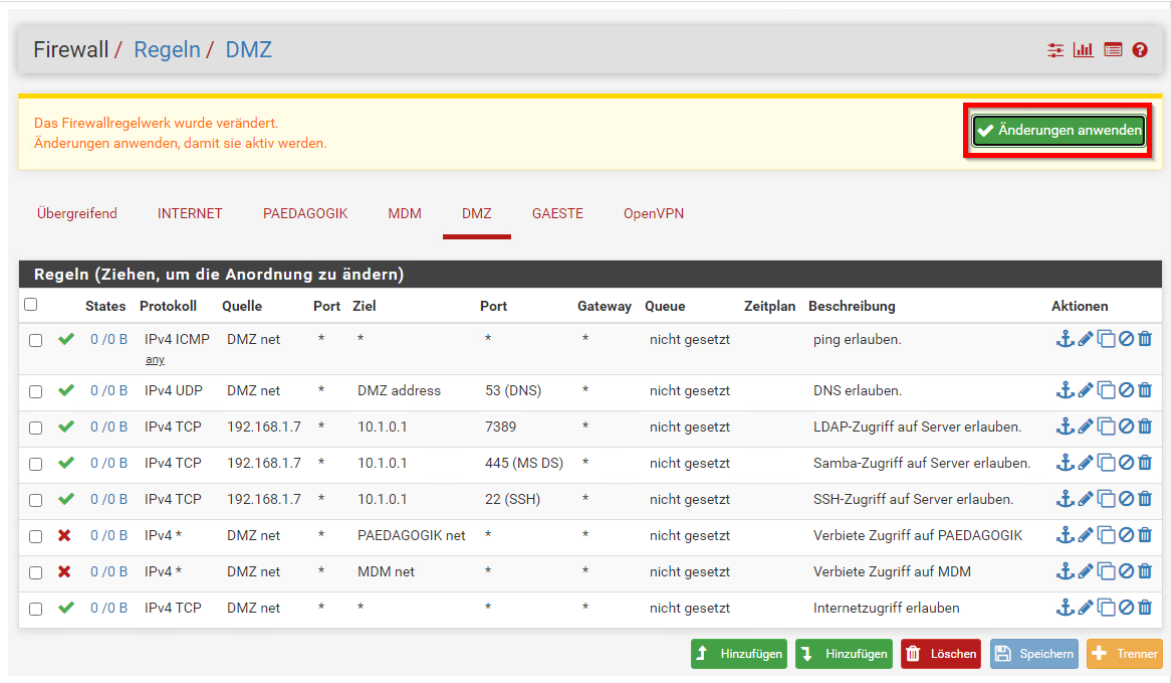

Abb. 46: Regel: Änderungen anwenden

5.5 Hinweise zum GAESTE-Netz

Bei der Verwendung von Tablets im Gäste-Netz sollte eine Anpassung des Regelwerkes im Allgemeinen nicht notwendig sein.

Abb. 47: Regelsatz Gäste-Netz

Die ausgegrauten Regeln beziehen sich auf die Verwendung der Radius-Authentifizierung bzw. von Captive Portal.

Lesen Sie dazu unsere Anleitungen „Radius-Server konfigurieren“ und „Captive Portal“ unter „How-Tos“:

https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#howtos

6 Protokollierung des Internetzugriffs

6.1 Der MDM-DHCP (Feste IP-Adressen verteilen)

Damit die Protokollierung von Internetzugriffen möglich wird, müssen den Geräten (über deren MAC-Adresse) jeweils feste IP-Adressen per DHCP zugeteilt werden. Diese Adressen erscheinen dann in der in Kapitel 6.3 beschriebenen Logdatei auf dem Server. Das MDM-Netz wird so konfiguriert, dass IP-Adressen von 172.20.0.1 bis 172.22.254.255 vergeben werden können. Anpassungen können hier jederzeit erfolgen.

Zunächst muss in der Firewall der *DHCP* aktiviert und der *Range* konfiguriert werden. Anschließend können den Geräten feste IP-Adressen zugewiesen werden. Außerdem müssen private MAC-Adressen in der WLAN-Verbindung des iPads über das MDM deaktiviert werden.

6.1.1 Aktvierung und Konfiguration des MDM-DHCP

Navigieren Sie *Dienste | DHCP-Server | MDM*. Aktivieren sie den *DHCP-Server für die Schnittstelle MDM*. Definieren Sie den *Range* der automatisch verteilten IP-Adressen. Der erste Teil des Verfügbaren Ranges sollte für die später fest vergebenen IP-Adressen reserviert bleiben.

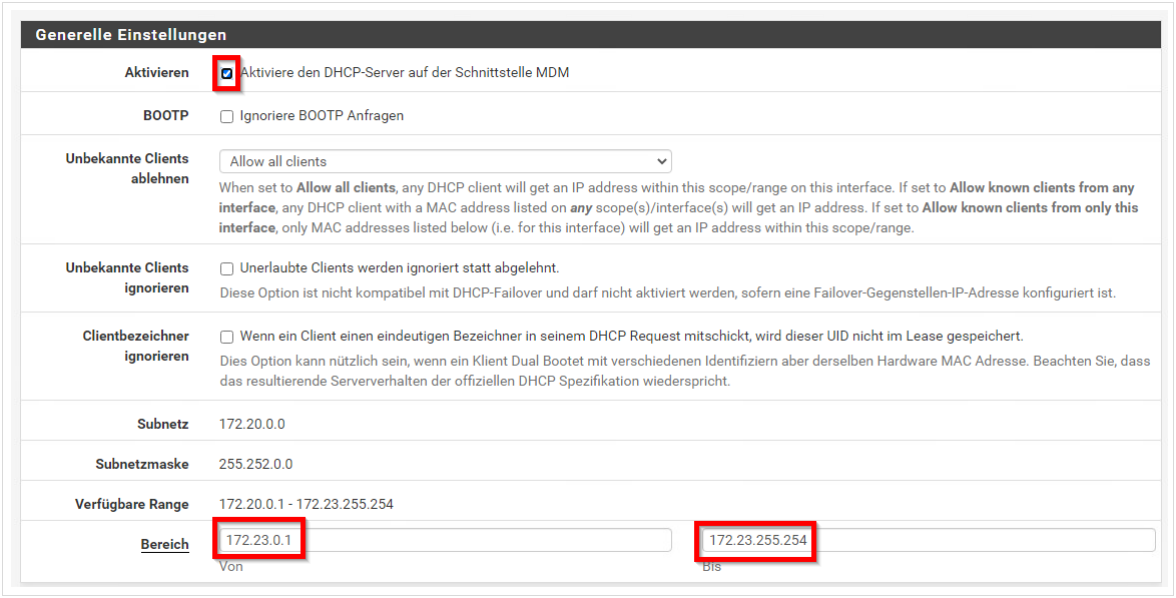

Abb. 48: DHCP konfigurieren.

Empfehlung: *Bereich Von 172.23.0.1 Bis 172.23.255.254*

Scrollen Sie nach unten bis *Speichern.*

6.1.2 Feste IP-Adressen vergeben

Scrollen Sie die Einstellungen des DHCP-Servers der Schnittstelle MDM nach unten, bis Sie zum Menü *DHCP statische Zuordnung für diese Schnittstelle* gelangen. Klicken Sie auf *Hinzufügen.*

Abb. 49: Statische Zuordnung hinzufügen.

Tragen Sie die MAC-Adresse des Geräts ein. Der Hinweis Semikola zu verwenden ist irreführend, Sie müssen Doppelpunkte verwenden.

Tragen Sie die IP-Adresse ein (hier *172.20.0.11*), die das Gerät per DHCP erhalten soll, vergeben Sie einen Hostnamen (hier *Ipad-2*) und setzen Sie den Haken bei *statischer ARP-Tabellen-Eintrag*.

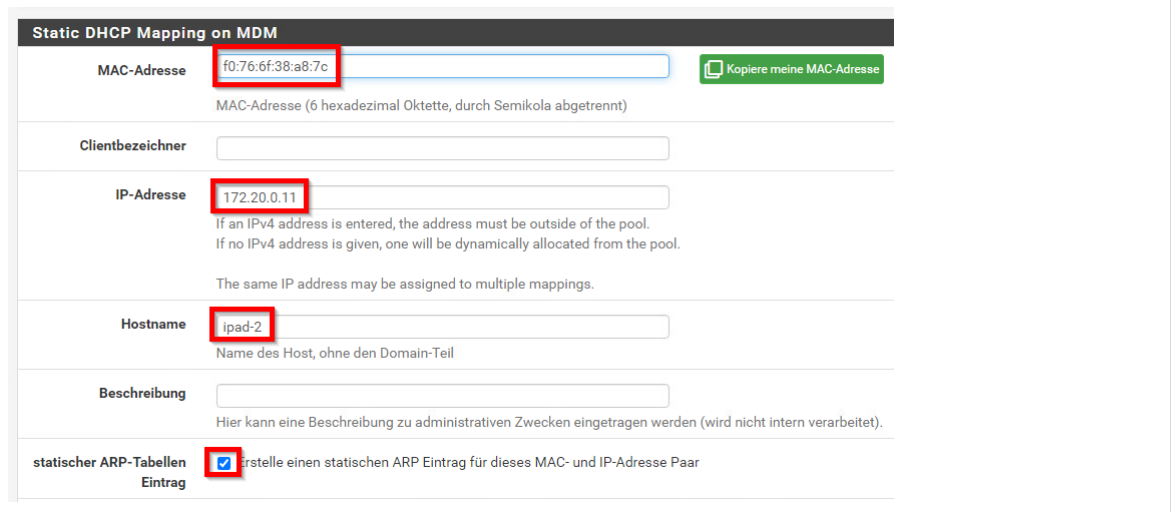

Abb. 50: Statische Zuordnung hinzufügen: Einstellungen

Scrollen Sie nach unten und klicken Sie auf *Speichern*.

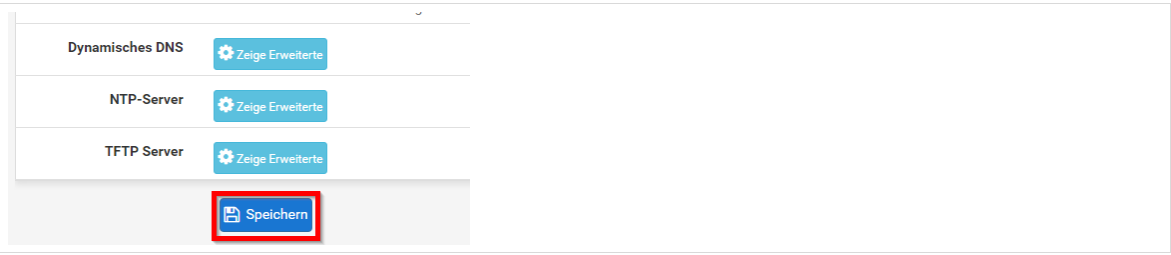

Abb. 51: Statische Zuordnung hinzufügen: Speichern

Sie sehen nun den Eintrag im Bereich *DHCP statische Zuordnung für diese Schnittstelle*.

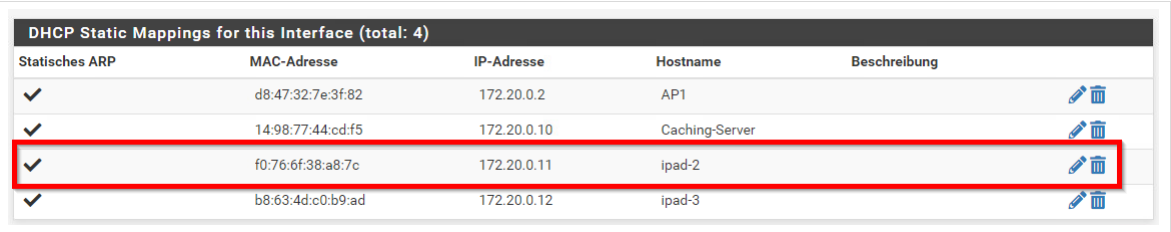

Abb. 52: Statische Zuordnung hinzufügen: Übersicht

Sie können nun weitere Geräte eintragen.

Es erscheint ratsam, an Access-Points feste IP-Adressen zu vergeben. So werden diese in der pfSense gelistet und können besser zugeordnet werden.

6.1.3 Deaktivierung von privaten MAC-Adressen

Mithilfe des MDM müssen nun private MAC-Adressen der WLAN-Verbindung ausgeschaltet werden. In Jamf-School muss dazu ein Profil erstellt werden, in dem die WLAN-Verbindung konfiguriert wird. Dort muss der Haken bei MAC-Adressen-Randomisierung gesetzt werden.

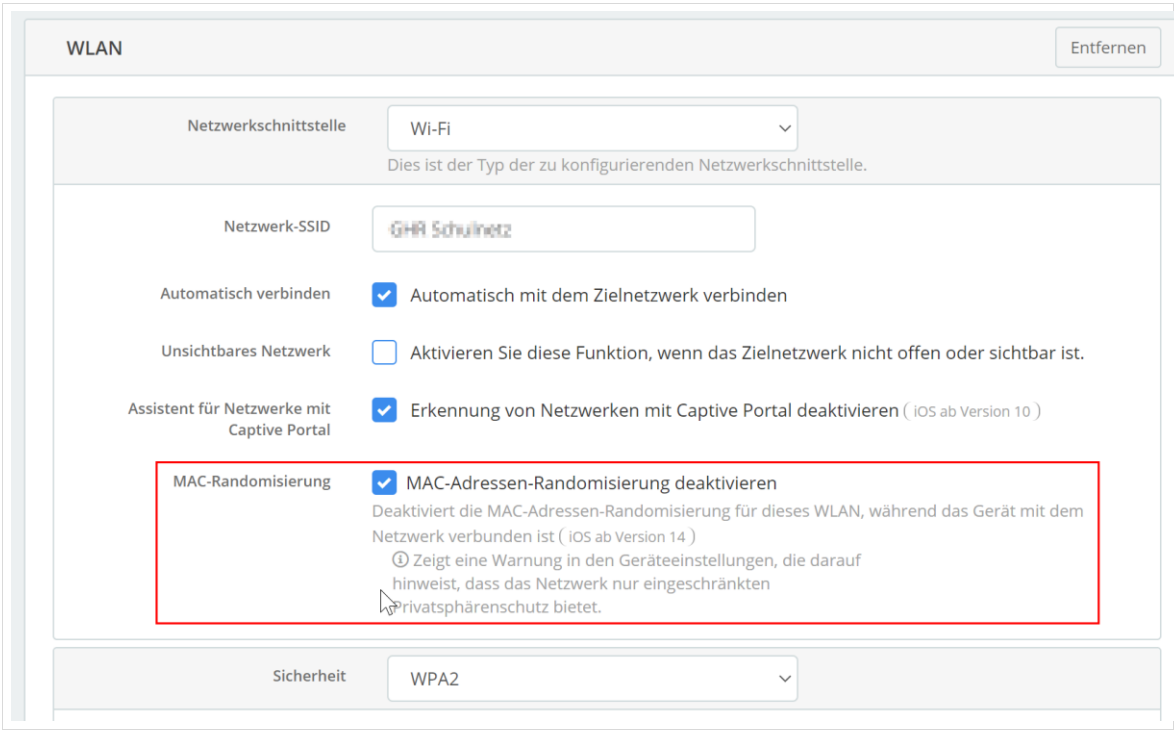

Abb. 53: MAC-Adressen Randomisierung deaktivieren

Speichern Sie die Einstellungen.

6.2 Einrichtung der Protokollierung von Internetzugriffen

6.2.1 Einrichtung des Loggings auf der Firewall

Die Zugriffe werden auf der Firewall mitgeloggt und an den paedML Linux und GS Server gesendet. Dort können die Zugriffe dann in der zugehörigen Protokoll-Datei ausgelesen werden.

Melden Sie sich an der Firewall an und gehen Sie im Menü Dienste zu DNS-Weiterleitung.

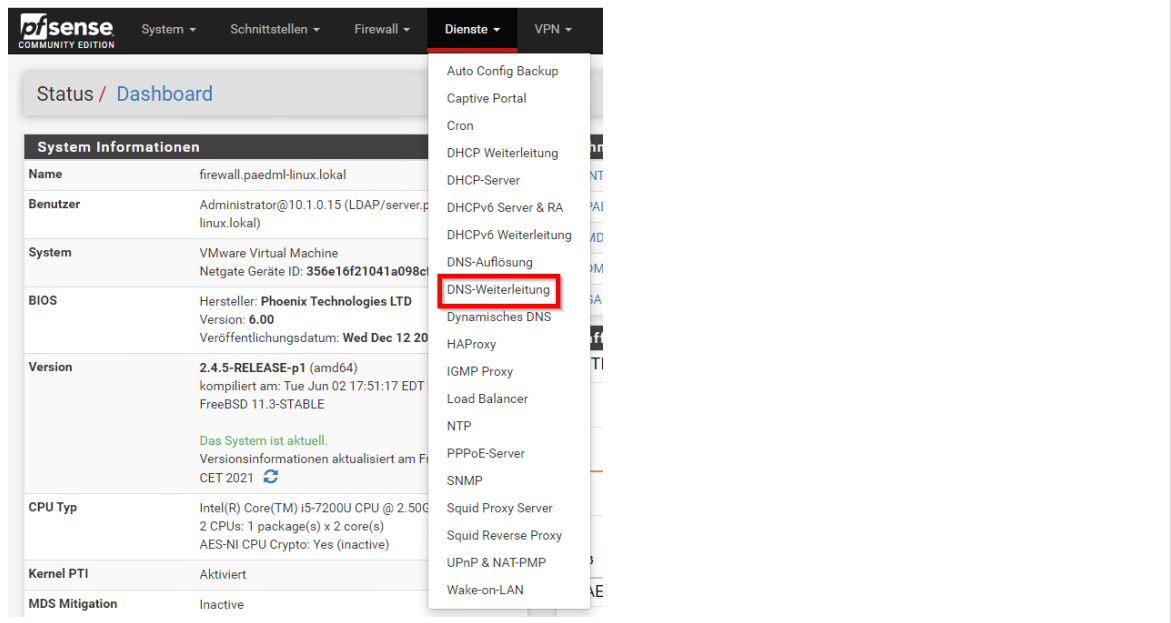

Abb. 54: DNS-Weiteleitung

Scrollen Sie nach unten, tragen Sie im Bereich *Benutzerdefinierte Optionen log-queries=extra* und speichern sie.

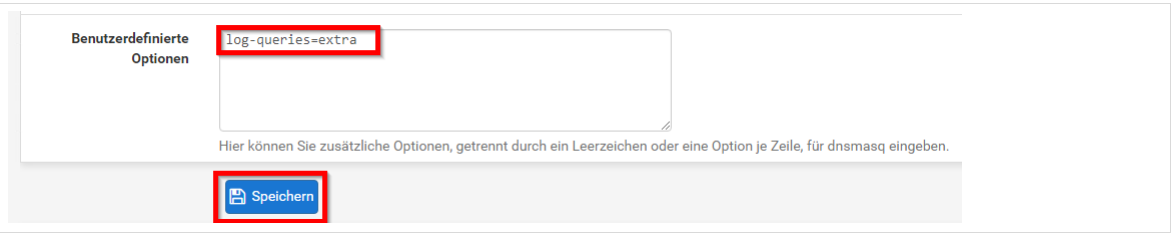

Abb. 55: log-queries=extra

Gehen Sie anschließend im Menü *Status* zur *Systemprotokollierung* und klicken Sie auf *Einstellungen*.

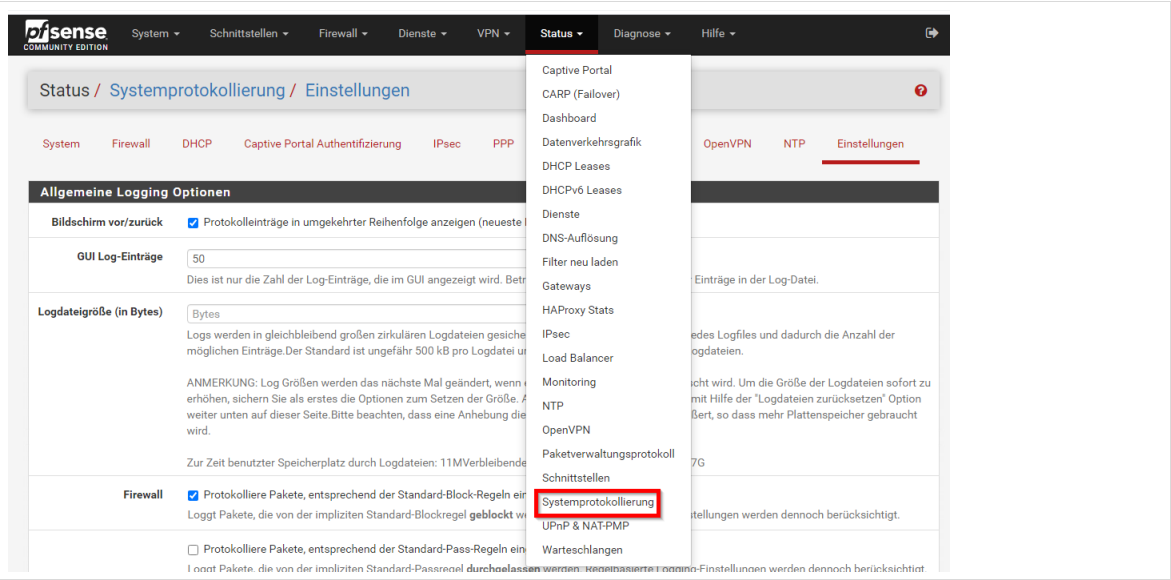

Abb. 56: Systemprotokollierung

In den Einstellungen scrollen Sie nach unten und setzen den Haken bei *DNS-Ereignisse*. Speichern Sie die Einstellungen.

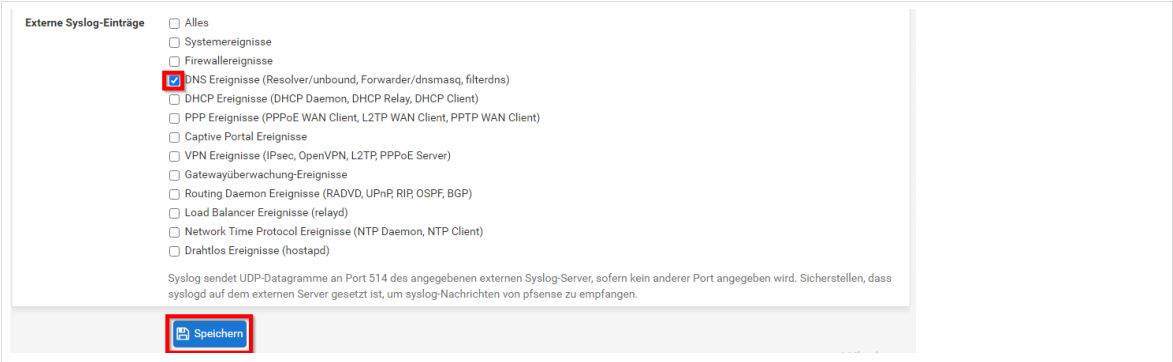

Abb. 57: DNS-Ereignisse

6.2.2 Die UCR-Variable udp

Öffnen Sie als Administrator die *System- und Domäneneinstellungen* des Servers und klicken Sie auf den Bereich *Univention Configuration Registry*.

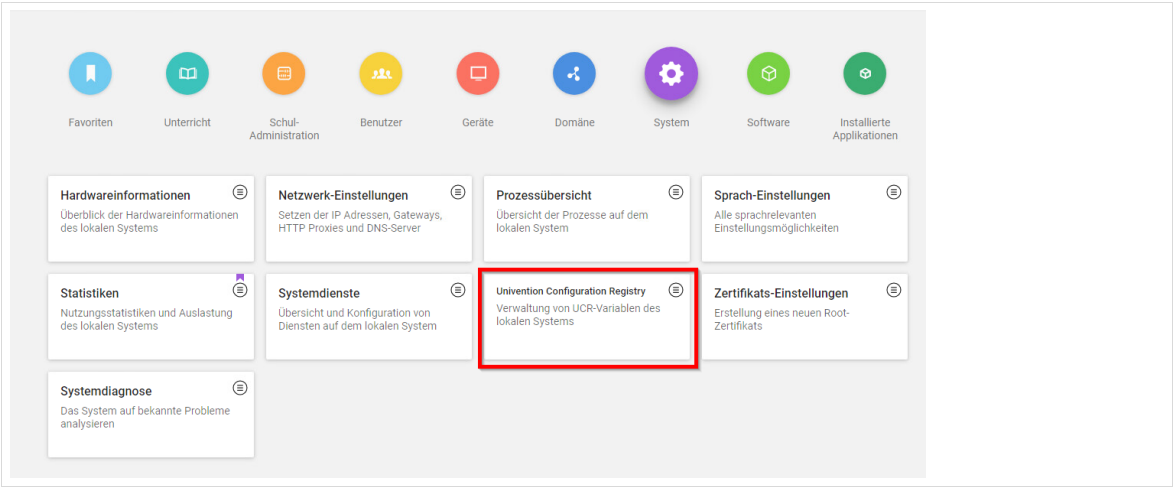

Abb. 58: System- und Domäneneinstellungen

Suchen Sie nach „syslog/input/udp“, klicken Sie die UCR-Variable syslog/input/udp an und setzen Sie den Wert 514. Speichern Sie die Einstellungen.

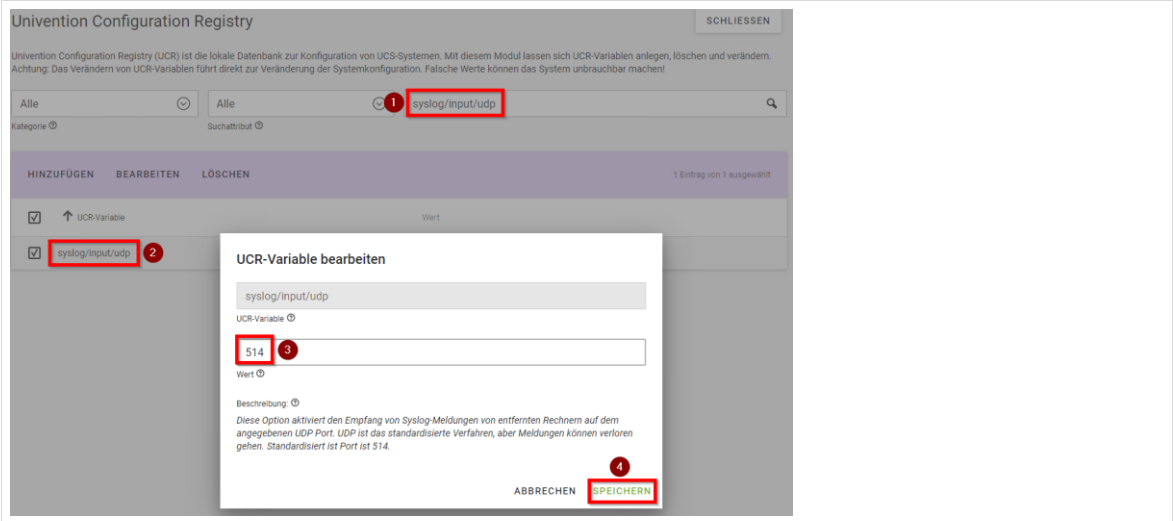

Abb. 59: System- und Domäneneinstellungen

Starten Sie den Server neu.

6.3 Logs der Internetzugriffe auf dem Server

Auf dem Server werden die Internetzugriffe unter */var/log/firewall.paedml-linux.lokal/dnsmasque.log* gespeichert. Diese Datei kann nun im Bedarfsfall ausgelesen werden. Die log-Dateien werden, wie in der paed ML Linux üblich, nach 30 Tagen gelöscht.

Im Folgenden Beispiel wurde per putty als root eine Verbindung zum Server aufgebaut und mit dem Befehl *tailf /var/log/firewall.paedml-linux.lokal/dnsmasque.log* die Datei in Echtzeit ausgelesen. Hier ist deutlich zu erkennen, dass am 9.3. um 16:19 von einem Gerät des MDM-Netzes mit der festen IP-Adresse 172.20.0.12 auf www.lmz-bw.de erfolgte.

```
Mar  9 16:19:30 firewall.paedml-linux.lokal dnsmasq[45721]: 1098 172.20.0.12/582
98 query[type=65] www.lmz-bw.de from 172.20.0.12
```

Abb. 60: Auslesen von /var/log/syslog mit

6.4 Protokollierung Gerätezuordung

Es kann nun aus der Logdatei ein Internetzugriff zu einer bestimmten Zeit einem bestimmten Gerät zugeordnet werden. Zusätzlich muss nun dokumentiert werden, welcher Nutzer an einem bestimmten Gerät zu welchem Zeitpunkt war. Das folgende Beispiel zeigt, wie eine solche Tabelle aussehen könnte.

Datum _____

Betreuende Lehrkraft _____

Gerätename	Schüler	Klasse	Uhrzeit
iPad1	Max Muster	7 A	10.15 – 11.30
iPad2	Berta Rave	7 A	10.15 – 10.30
iPad3	Rudolf Üpel	7 A	10.15 – 10.30
…	…	…	…

Beispiel für Benutzerprotokollierung

Achten Sie auf Löschfristen und vernichten Sie die Nutzungsprotokolle regelmäßig. Befragen Sie hierzu bitte Ihren Datenschutzbeauftragten.

7 Jugendschutzfilter

Der Zweck eines Jugendschutzfilters liegt darin, den Zugriff auf jugendgefährdende Inhalte einzuschränken. In der paedML Linux kommt hierfür ein Proxy-Server zum Einsatz. Dieser wird im MDM-Netz umgangen. Nur so kann ein reibungsfreier Internetzugriff und eine Verwaltung per MDM ermöglicht werden. Im Moment gibt es verschiedene Testprojekte mit alternativen DNS-Jugendschutzfiltern. Die Ergebnisse dieser Projekte werden in dieses Dokument einfließen, sobald sie vorliegen.

7.1 DNS-Server

Schulen können die Adresse eines externen DNS-Jugendschutzfilters in der Firewall eintragen. Navigieren Sie dazu zu *System | Allgemeine Einstellungen* und dort zu *DNS-Server Einstellungen. Tragen Sie dort die Adresse des Jugendschutzfilters ein.*

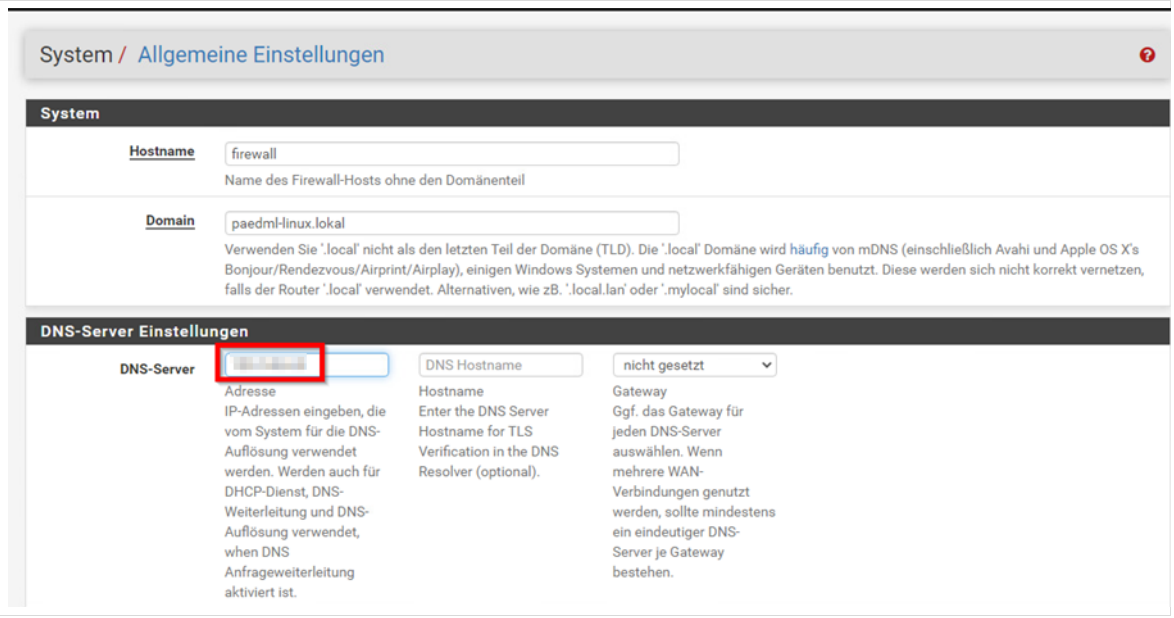

Abb. 61: DNS eintragen

Scrollen Sie nach unten und *Speichern* Sie die Eintragung.

7.2 Alternativen

Alternativ können Sie weitere Systeme als Jugendschutzfilter einsetzen. Sofern Sie Dienstleistungen von Dritten nutzen, sollten Sie sicherstellen, dass die Angebote datenschutzrechtlich unbedenklich sind und ggf. einen Vertrag zur Auftragsdatenverarbeitung abschließen.

Der eingetragene Verein JusProg hat in Zusammenarbeit mit dem LMZ BW einen per MDM konfigurierbaren Webbrowser veröffentlicht. Das LMZ stellt Konfigurationsdateien für einen altersgemäßen Jugendschutz für diesen Webbrowser zur Verfügung.

7.2.1 Installation des JusProg-Webbrowsers im MDM

Die iOS-App JusProg-Webbroser muss über den Apple School Manager (ASM) und das Volume Purchase Program (VPP) auf Ihr MDM übertragen werden. Der Vorgang entspricht einem „Kauf“ **ohne dass nach aktuellem Stand tatsächlich Kosten anfallen**. „Kaufen“ Sie auseichend Lizenzen. Bedenken Sie auch bereits geplante Anschaffungen.

Für weitere Informationen über den Hersteller gehen Sie zu https://www.jugendschutzprogramm.de/.

7.2.2 Konfiguration des JusProg Webbrowsers

Die App JusProg Webbrowser wurde in Kooperation mit dem LMZ weiterentwickelt. Sie wurde getestet. Größere „Feldversuche“ an Schulen stehen allerdings noch aus.

Wir liefern drei Konfigurationsdateien *LMZGS.jusprog* für Grundschulen, *LMZSEK.jusprog* für die Sekundarstufen 1 und 2 und *CUSTOM.jusprog* für die Umsetzung eigener Anpassungen.

7.2.2.1 Grundschul-Konfiguration

Öffnen Sie die Datei LMZGS.jusprog mit dem Texteditor. Kopieren Sie die den kompletten Inhalt in die Zwischenablage.

Melden Sie sich bei Ihrem MDM an. Navigieren Sie zu *Apps*. In Jamf School klicken Sie bei der App Jusprog-Webbrowser auf das Bearbeiten-Symbol.

Abb. 62: JusProg-Webbrowser konfigurieren.

Im Bereich *Optionen* setzen Sie den Haken bei *Verwaltete Konfiguration übernehmen*. Evtl. müssen die *Erweiterten Optionen* zunächst angezeigt werden.

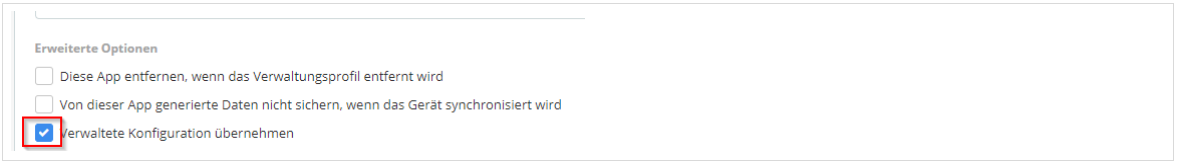

Abb. 63: JusProg-Webbrowser Optionen.

Nun kopieren Sie den kompletten Inhalt der Datei *„LMZGS.jusprog“* in das Feld *„Verwaltete Konfiguration“* und benennen die Konfiguration mit *LMZGS*. Klicken Sie anschließend auf *„Als Standardeinstellung für neue Bereiche festlegen“*.

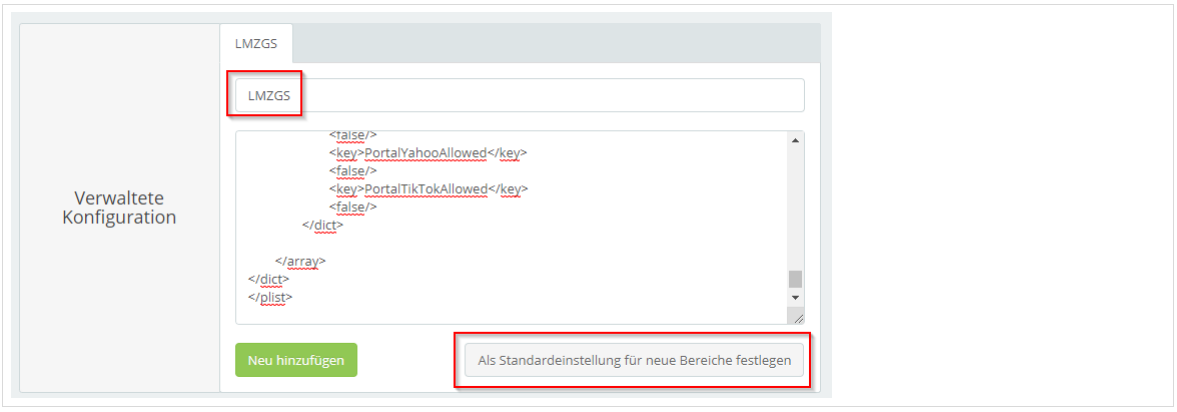

Abb. 64: JusProg-Webbrowser: Konfigurationsdatei hinzufügen

Vergessen Sie nicht zu speichern.

7.2.2.2 Sekundarstufen-Konfiguration

Öffnen Sie die Datei LMZSEk.jusprog mit dem Texteditor. Kopieren Sie die den kompletten Inhalt in die Zwischenablage.

Melden Sie sich bei Ihrem MDM an. Navigieren Sie zu Apps. In Jamf School klicken Sie bei der App Jusprog-Webbrowser auf das Bearbeiten-Symbol.

Abb. 65: JusProg-Webbrowser konfigurieren.

Im Bereich *Optionen* setzen Sie den Haken bei *Verwaltete Konfiguration übernehmen*. Evtl. müssen die *Erweiterten Optionen* zunächst angezeigt werden.

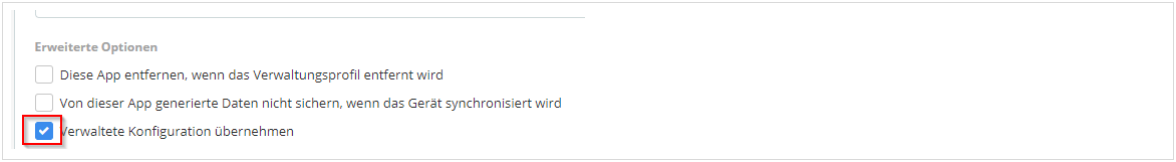

Abb. 66: JusProg-Webbrowser Optionen.

Nun kopieren Sie den kompletten Inhalt der Datei „*LMZSEK.jusprog*“ in das Feld „*Verwaltete Konfiguration*“ und benennen die Konfiguration mit *LMZGS*. Klicken Sie anschließend auf „*Als Standardeinstellung für neue Bereiche festlegen*“.

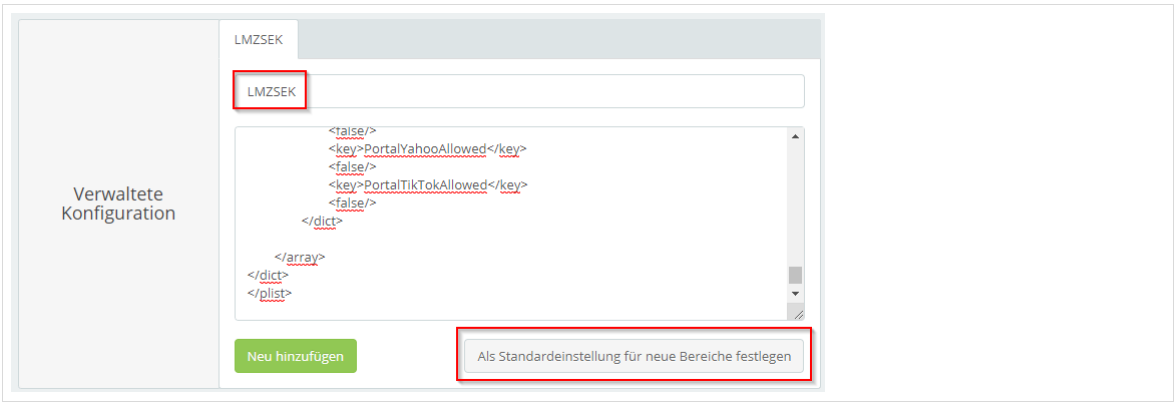

Abb. 67: JusProg-Webbrowser: Konfigurationsdatei hinzufügen

Vergessen Sie nicht zu speichern.

7.2.2.3 Angepasste Konfiguration

Öffnen Sie die Datei LMZCUSTOM.jusprog mit Notepad++ oder einem ähnlichen Programm.

Die folgende Tabelle gibt einen Überblick über die umfassenden Konfigurationsmöglichkeiten. Eine umfassende Anleitung kann nicht geliefert werden. Das Setzen der Werte in der Datei LMZCUSTOM.jusprog setzt Erfahrung im Umgang mit der Konfiguration von Apps per MDM voraus. Die gemachten Einstellungen sollten zunächst an einem Gerät getestet werden.

Denken Sie daran, nach jeder Änderung im Key „Version“ den Wert um eine Einheit zu erhöhen, bevor Sie die Datei an das iOS-Gerät übergeben.

Key	Standardwert	Anpassung
Elternkonto		
Version	14	Muss bei jeder Änderung erhöht werden. Nur so wird die geänderte jusprog-Datei als neu vom iPad erkannt.
Name	Administrator	Name des Elternkontos

Password	geheim123	Passwort des Elternkontos
Homepage Quickstarter OpenAtLaunch	https://www.lmz-bw.de/	Homepage der Schule
Kinderkonto		
Name	Kind1	Name des Kinderkontos
Password	123	Passwort des Kinderkontos, kann auch leer bleiben. Dies empfiehlt sich bei aktivem Autologin (siehe unten).
AutoLogin	<true/> bei GS <false/> bei SuS	True kann nur für ein Konto gesetzt werden. Dieses wird nach Start des Geräts automatisch angemeldet - bei mehreren Konten das Konto mit dem höchsten Sicherheitsstandard!
AgeCategory	<integer>3</integer>	Festlegung der Altersstufe: 0:<6 Jahre, 1:<12 Jahre, 2:<16 Jahre, 3:<18 Jahre, 4:>=18 Jahre
HomepageQuickstarter OpenAtLaunch	https://www.fragfinn.de/	Homepage der Schule
SearchEngineFragFinn SearchEngineBlindeKuh SearchEngineHellesKoepfchen SearchEngineEcosia SearchEngineGoogle SearchEngineBing SearchEngineYahoo	<true/> oder <false/> bei GS und SuS entsprechend der Alterstufe	Individuelle Festlegung erlaubter Suchmaschinen für jedes Konto
CheckCustomFilters	<true/> bzw. <false/>	True bei Verwendung eigener Filter (siehe unten)
CustomFilters		Hier werden Seiten erlaubt (Allow), bzw. gesperrt (Block)
Favorites	Title: LMZ URL: https://www.lmz-bw.de/	Hier können eigene Favoriten angezeigt werden.

PortalFacebookAllowed PortalInstagramAllowed PortalYoutubeAllowed PortalTwitterAllowed PortalGoogleAllowed PortalBingAllowed PortalYahooAllowed PortalTikTokAllowed	<true/> oder <false/> bei GS und SuS entsprechend der Alterstufe	Festlegung erlaubter Portale für jedes Konto individuell

Navigieren Sie zu Apps. In Jamf School klicken Sie bei der App Jusprog-Webbrowser auf das Bearbeiten-Symbol.

Abb. 68: JusProg-Webbrowser konfigurieren.

Im Bereich *Optionen* setzen Sie den Haken bei *Verwaltete Konfiguration übernehmen*. Evtl. müssen die *Erweiterten Optionen* zunächst angezeigt werden.

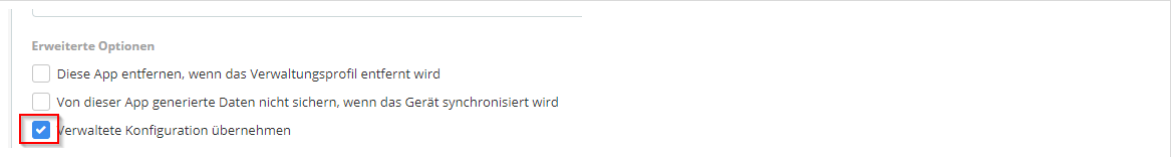

Abb. 69: JusProg-Webbrowser Optionen.

Nun kopieren Sie den kompletten Inhalt der Datei „*LMZCUSTOM.jusprog*“ in das Feld „*Verwaltete Konfiguration*“ und benennen die Konfiguration mit *LMZCUSTOM*. Klicken Sie anschließend auf „*Als Standardeinstellung für neue Bereiche festlegen*“.

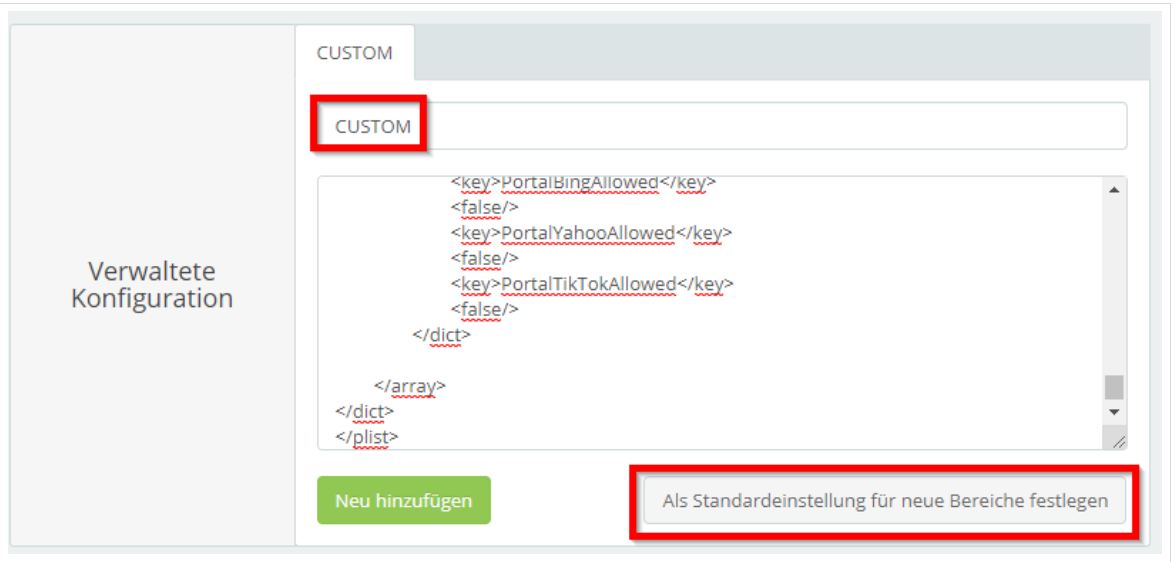

Abb. 70: JusProg-Webbrowser: Konfigurationsdatei hinzufügen

Vergessen Sie nicht zu speichern.

7.2.3 Installation des Jusprog-Webbrowsers

Nun müssen Sie die App JusProg-Webbrowser per MDM auf die iOS-Geräte übertragen. Da es hier viele verschiedene Wege gibt dies zu tun, verzichten wir auf eine nähere Beschreibung.

7.2.4 Anpassungen am iOS-Gerät

Die App JusProg-Webbrowser wurde altersentsprechend konfiguriert und auf die iOS-Geräte übertragen.

Damit die Schülerinnen und Schüler sicher surfen, müssen nun alle anderen Browser von den iOS-Geräten entfernt werden. Standardmäßig ist auf einem iOS-Gerät nur der Browser Safai installiert.

Um diesen zu deaktivieren, navigieren Sie in Jamf School zu *„Profile“ und* wählen dort ein Profil aus. Gehen Sie zu *Einschränkungen*. Im Bereich *Anwendungen* entfernen Sie den Haken bei Verwenden von Safari erlauben.

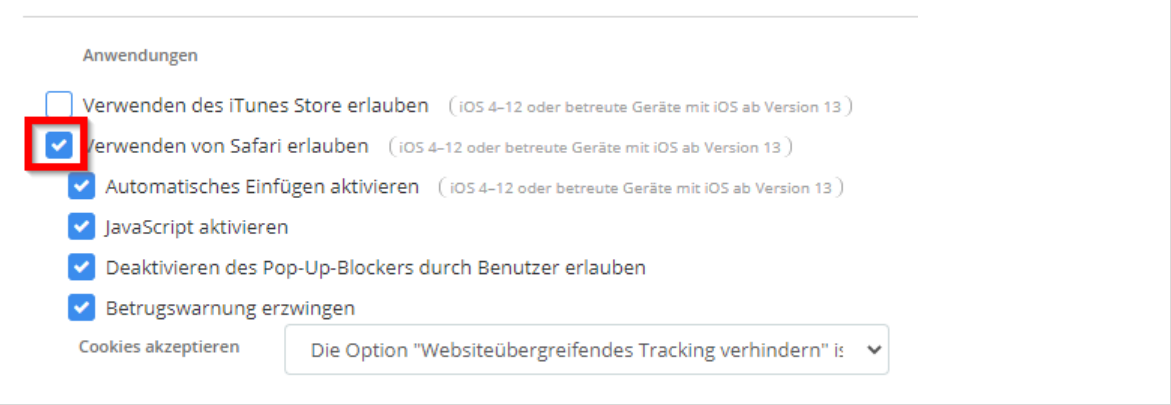

Abb. 71: Safari deaktivieren

Durch *Speichern* übertragen Sie das angepasste Profil auf das iOS-Gerät.

Die Schülerinnen und Schüler müssen über den neuen Browser JusProg informiert werden!

Wurden dem iOS-Gerät weitere Browser zugewiesen müssen diese ebenfalls über das MDM entfernt werden.

8 Dateiablage mit der paedML Nextcloud

Von der Nutzung von Cloud-Services der Hersteller ist aus datenschutzrechtlichen Gründen häufig abzuraten. Wenn Sie dennoch ein externes Angebot nutzen wollen, sollten Sie auf jeden Fall sicherstellen, dass die Anforderungen an den Datenschutz erfüllt werden (vgl. Dokumente unter https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/mobile). Aktuell (Stand März 2019) speichert Apple Daten weltweit in der iCloud. Da die Daten außerhalb europäischer Server abgespeichert werden können, ist die Nutzung der iCloud daher nicht datenschutzkonform.

Der Verbleib der Daten auf den Tablets ist jedoch kontraproduktiv, da diese bei einem Zurücksetzen des Tablets verloren gehen oder zum Zwecke der Benotung von Schülerabreiten durch eine Lehrkraft eingesehen werden sollten. Um Daten dauerhaft zu erhalten ist es notwendig alternative Speicherorte zu finden.

Nicht jede App unterstützt die Ablage von Daten in externe Laufwerke. Einige Apps ermöglichen nur die Speicherung fertiger Dateien. Roh-Dateien (z.B. von Film- oder Musik-Projekten) können häufig nicht extern gespeichert werden.

In der Praxis hat sich in diesen Fällen die Sicherung von Projektergebnissen per Airdrop auf ein dezidiertes geschütztes Lehrergerät (Ipad mit ausreichend Speicher, MAC) bewährt.

8.1 Nextcloud in der paedML Linux und GS

Die paedML Linux und GS ab Version 7.1 kann um eine Nextcloud erweitert werden. Wir empfehlen die Nutzung dieser virtuellen Maschine zu Dateiablage mit Tablets.

Unsere Nextcloud-Installationsanleitung und Nextcloud-Administratorhandbuch finden Sie unter https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#versions .

Das Nextcloud-Handbuch für Lehrkräfte ist unter https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#manuals zu finden.

8.2 Arbeiten mit der Nextcloud am Ipad

Soll die Nextcloud am Ipad genutzt werden, empfiehlt es sich auf die Nextcloud-iOS-App auf die Ipads zu installieren.

Bei der ersten Nutzung der App erfolgt die Anmeldung an der Nextcloud. Dazu müssen die paedML Linux und GS Zugangsdaten verwendet werden.

Die App erfordert bei der ersten Öffnung allerdings die exakte URL Ihrer Nextcloud ohne vorangestelltes https://. Hier muss überlegt werden, wie die URL an die SuS kommuniziert wird. In der Praxis haben sich Plakate in der großer Schriftgröße bewährt.

Die App ist – Stand heute – nicht in der Lage die URL als QR-Code einzulesen. Der in der App enthaltene Knopf QR-Code bezieht sich ausschließlich auf innerhalb der

Nextcloud-Konten-Einstellungen benutzerbezogen erzeugte QR-Codes. In der Schule scheint dieses Vorgehen im Moment aus unserer Sicht nicht praktikabel.

9 WLAN im MDM-Netz

Spätestens jetzt wird sich die Frage stellen, wie die im MDM-Netz aufgenommenen Ipads über WLAN im Schulhaus betrieben werden sollen.

Wir empfehlen die Aufnahme über WPA2-Keys, die per MDM an die Ipads verteilt werden. Es sollte unbedingt vermieden werden diese zu kommunizieren.

Die Access-Points sollten in das MDM-Netz aufgenommen werden.

Eine best-practice-Methode zur Aufhame und Widerherstellung von Ipads ist die Einrichtung eines frei zugänglichen nur für diesen Zweck eingesetzten WLAN-Start-Netzes. Dieses darf nur für den Ausroll- bzw. Wiederherstellungsprozess aktiviert werden.

9.1 Aufnahme der Access-Points in das MDM-Netz

Scrollen Sie die Einstellungen des DHCP-Servers der Schnittstelle MDM nach unten, bis Sie zum Menü *DHCP statische Zuordnung für diese Schnittstelle* gelangen. Klicken Sie auf *Hinzufügen*.

Abb. 72: Statische Zuordnung hinzufügen.

Tragen Sie die MAC-Adresse des Access-Points ein. Der Hinweis Semikola zu verwenden ist irreführend, Sie müssen Doppelpunkte verwenden.

Tragen Sie die IP-Adresse ein (hier *172.20.0.2*), die der Access-Point per DHCP erhalten soll, vergeben Sie einen Hostnamen (hier *AP1*) und setzen Sie den Haken bei *statischer ARP-Tabellen-Eintrag*.

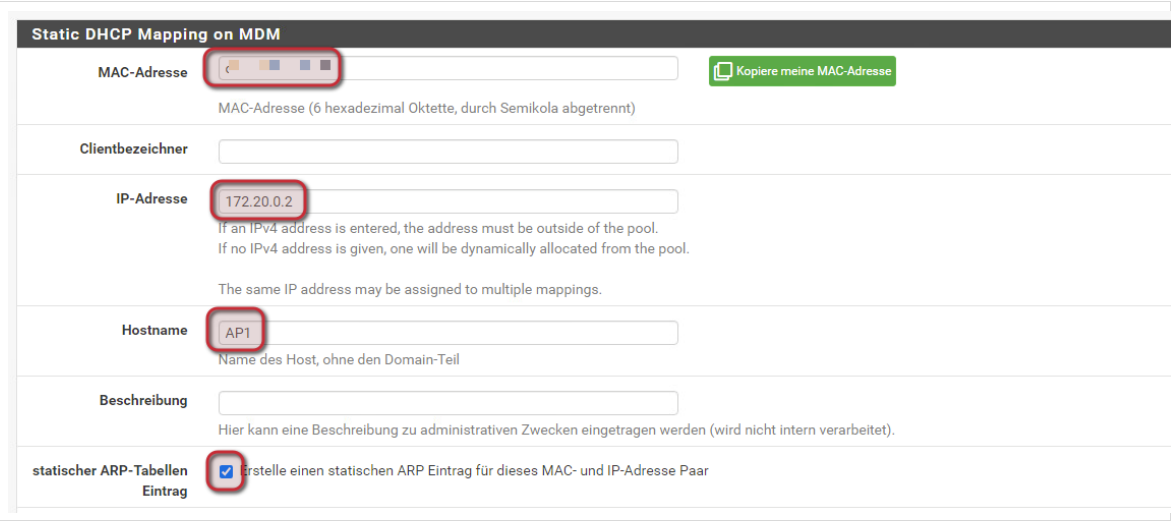

Abb. 73: Statische Zuordnung hinzufügen: Einstellungen 1

Scrollen Sie nach unten und klicken Sie auf *Speichern.*

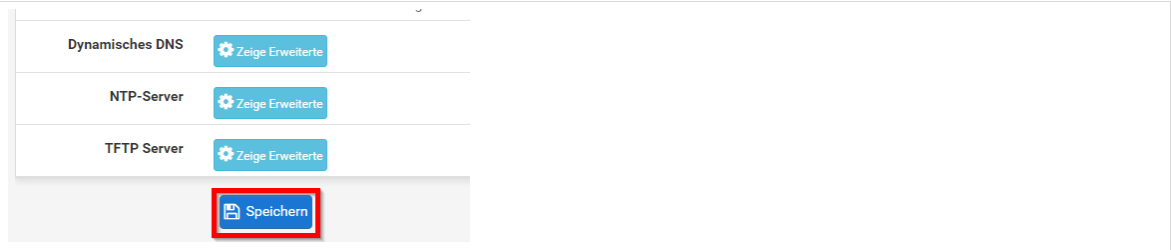

Abb. 74: Statische Zuordnung hinzufügen: Speichern

Sie sehen nun den Eintrag im Bereich *DHCP statische Zuordnung für diese Schnittstelle.*

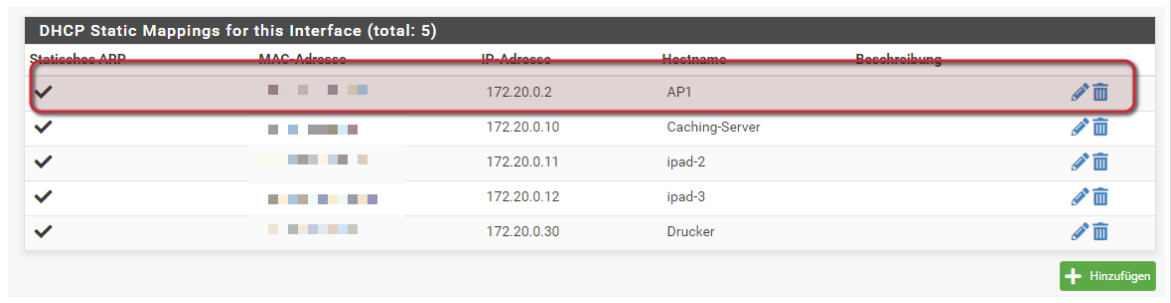

Abb. 75: Statische Zuordnung hinzufügen: Übersicht

Sie können nun weitere Access-Points eintragen.

9.2 WPA2-Keys an iPads verteilen

In Jamf School navigieren Sie zu Profile und wählen dort ein produktives Profil aus. Im Bereich WLAN tragen sie die SSID (hier PaedML), als Sicherheit WPA/ WPA2 und das Passwort ein.

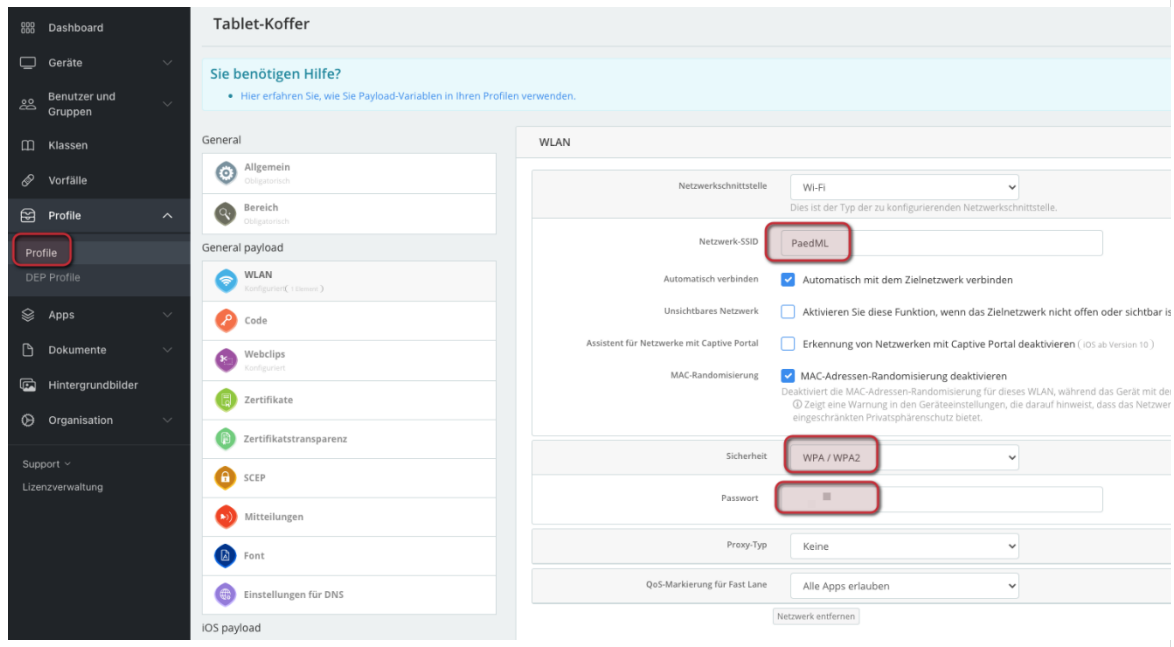

Abb. 76: WLAN: SSID konfigurieren

10 Einsatzszenarien von iPads in der paedML – Eine Übersicht

Die folgenden Kapitel beschreiben verschiedene technische Umsetzungen der Tablet-Integration. Welche Technik für welches Szenario geeignet ist, soll mit der folgenden Übersicht deutlicher werden. Eine Konzeption stellt die Übersicht nicht dar. Diese sollte bereits im Vorfeld – idealerweise anhand des MEP-Prozesses – erfolgt sein.

Auch der Verwaltungsaufwand bei der Administration der Geräte sollte bedacht werden. Hier erscheint die Umsetzung mithilfe der „*Temporary Shared Ipad*"-Technik einen erfreulich geringen Mehraufwand zu versprechen.

Entscheiden Sie im Vorfeld in Zusammenarbeit mit Ihrem Schulträger, Dienstleister und ggf. dem Medienzentrenverbund welche der in Kapitel 10-12 beschriebenen Techniken unter welchen Bedingungen an Ihrer Schule datenschutzkonform eingesetzt werden können.

Übersicht

Szenario	**1:N** **Kurzfristiges Arbeiten an** Ipads zur Internetrecherche, zur Verwendung von Lernapps/ Visualisierung (z. B. GeoGebra)	**1:N** **Mittelfristiges Arbeiten an** Ipads im Rahmen von Projekten oder in sogenannten Tablet-Klassen über mehrere Unterrichtsstunden hinweg.	**1:1** **Langfristige Zuordnung** von Ipads und SuS. Tablet-Klassen über ein Schuljahr oder über die ganze Schulzeit.
Technische Umsetzung	**Kapitel 11** „Temporary Shared Ipad"	**Kapitel 12** „Shared Ipad"	**Kapitel 13**
Speicherung	Ausschließlich in der paedML Nextcloud (o.ä.)	Ausschließlich in der paedML Nextcloud (o.ä.)	Ipad oder paedML Nextcloud (o.ä.)
Grenzen	Benutzerdaten auf dem Ipad werden nach jedem Abmeldevorgang gelöscht. Die Classroom-App kann nicht verwendet werden.	Synchronisation von paedML-Benutzernamen und Klassen in den ASM notwendig.	Synchronisation von paedML-Benutzernamen und Klassen in das MDM notwendig.

11 „Temporary Shared Ipad“

In vielen Schulen ist heute eine 1:N-Zuordnung üblich. Das heißt, Tablets werden von verschiedenen SuS benutzt. In diesem Fall muss unbedingt verhindert werden, dass Daten nach einem Wechsel auf dem Tablet verbleiben oder es muss gewährleistet werden, dass die Tablets vor dem Wechsel bereinigt werden.

Eine einfache Möglichkeit Ipads 1:N-fähig (mehrbenutzerfähig) zu machen, ist die von Apple bereitgestellte Technik „Temporary Shared Ipad“.

Die Technik hat gegenüber den in Kapitel 12 und 13 eingesetzten Techniken den Vorteil, dass keine Benutzerdaten in externe Systeme synchronisiert werden und dass sie nur wenig Verwaltungsaufwand bedeutet.

Bei der Nutzung von „Temporary Shared Ipads“ ist unbedingt zu beachten, dass auf dem Ipad gespeicherte Daten beim Abmeldevorgang gelöscht werden. Die SuS müssen daher Dateien auf der paedML Nextcloud speichern.

Die Apple Classroom App kann – Stand heute – nicht eingesetzt werden.

11.1 Ausrollen von Temporary Shared Ipads

Damit eine Nutzung von Ipads als *„Temporary Shared Ipads“* möglich ist, müssen diese als *„Shared Ipads“* eingerichtet werden.

In Jamf School wählen Sie dazu unter *Profile | DEP Profile | iOS Einstellungen | Geteiltes Ipad aktiveren*.

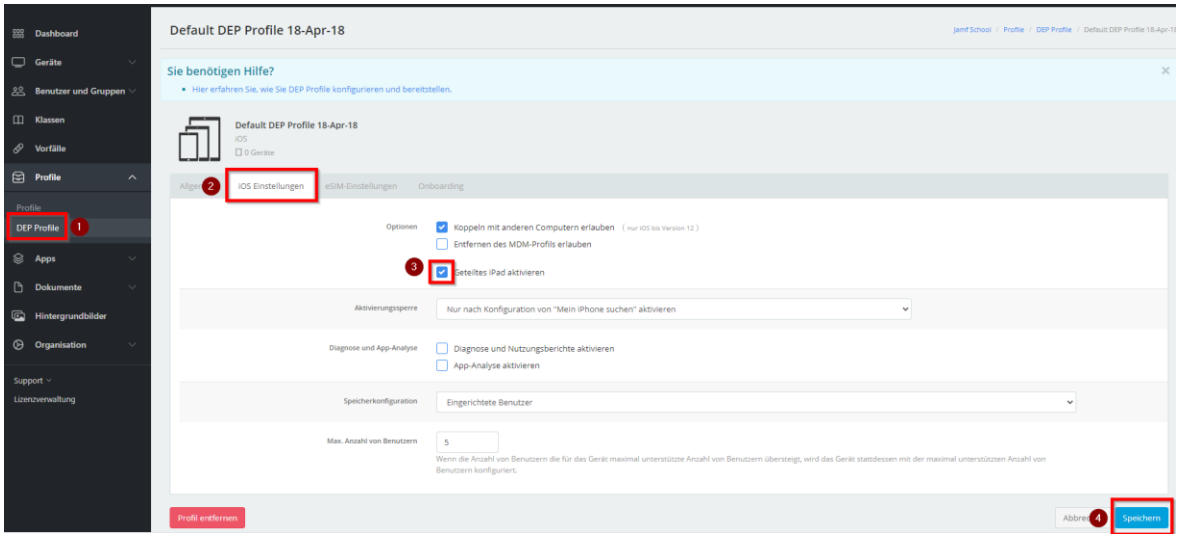

Abb. 77: ASM-Jamf School-Synchronisation ausführen

Im Anschluss müssen Sie das Ipad per MDM zurücksetzen.

Navigieren Sie in den Bereichen *Klassen* und wählen Sie dort eine Klasse aus, der sie das geteilte Ipad zuordnen möchten.

Die Klasse muss dabei nicht tatsächlich in der Schule vorhanden sein, sondern kann eine technische Klasse („Tablet-Koffer“) sein. Insbesondere benötigt die Klasse keine Benutzer.

Klicken Sie auf „*Geteilte Ipad-Geräte hinzufügen*“.

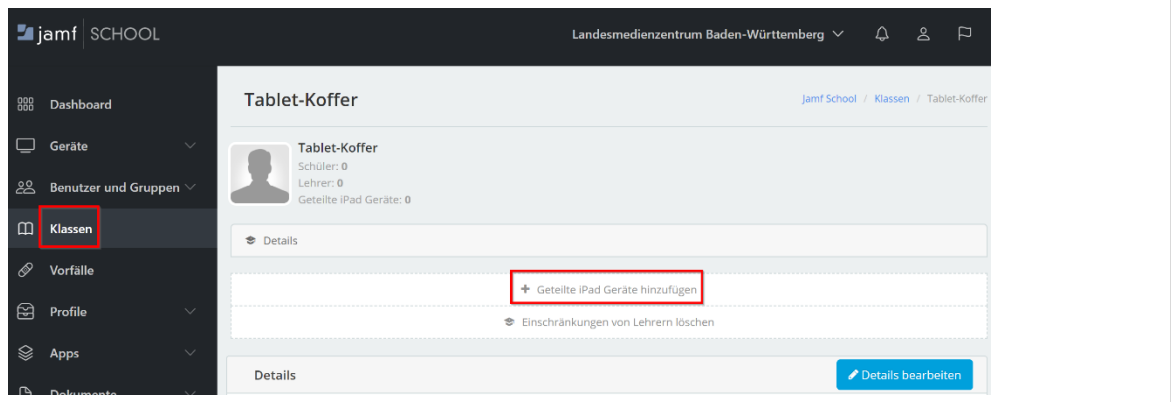

Abb. 78: Geteiltes Ipad Klasse zuordnen

Anschließend öffnen Sie die Einstellungen der Klasse, indem Sie die Klasse erneut wählen und „Details bearbeiten“ anklicken.

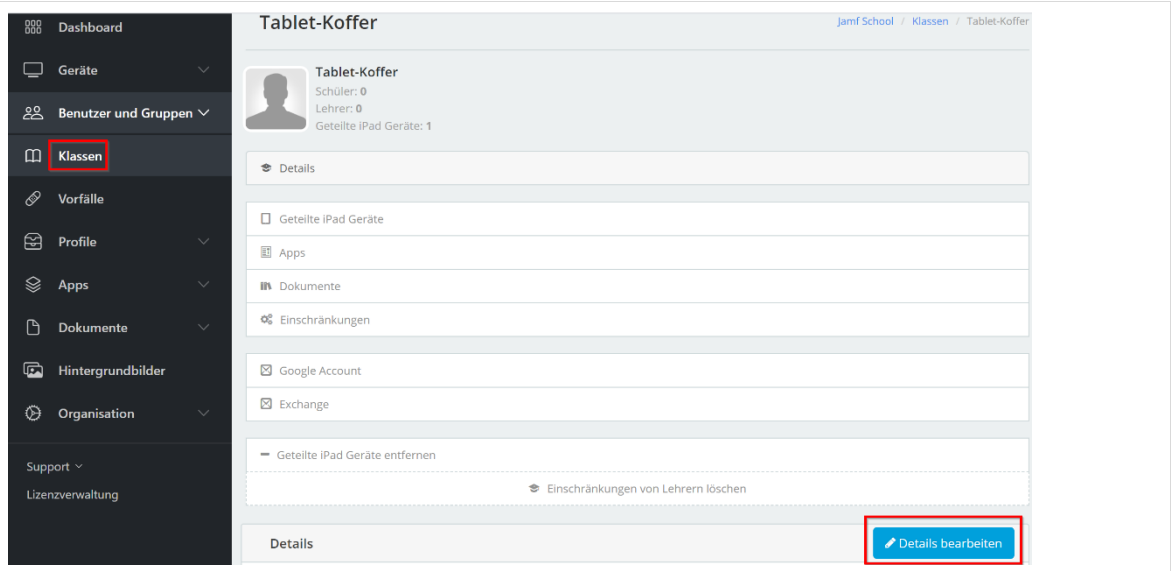

Abb. 79: Details bearbeiten aktivieren

In den Details setzen Sie den Haken bei „*Temporäre Sitzung auf geteiltem Ipad erlauben*“ (Ipad OS 13.4+)

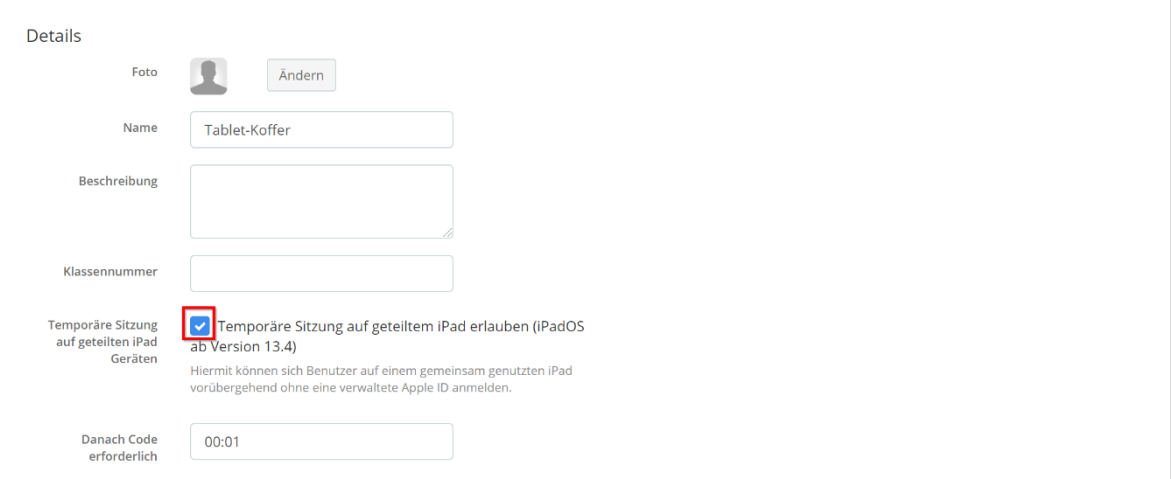

Abb. 80: Temporäre Sitzung aktivieren.

11.2 Anmelden und Arbeiten am Temporary Shared Ipad

Nach dem Starten erscheint im rechten unteren Bereich des Ipads die Möglichkeit sich als *Gast* anzumelden.

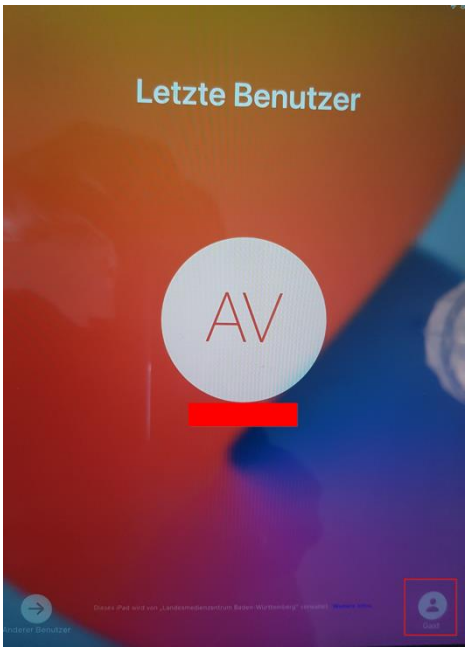

Abb. 81: Als Gast am Ipad anmelden

Nach dem Arbeiten meldet sich der Gast am Ipad ab. Dadurch werden alle Daten, die auf dem Ipad gespeichert wurden, gelöscht.

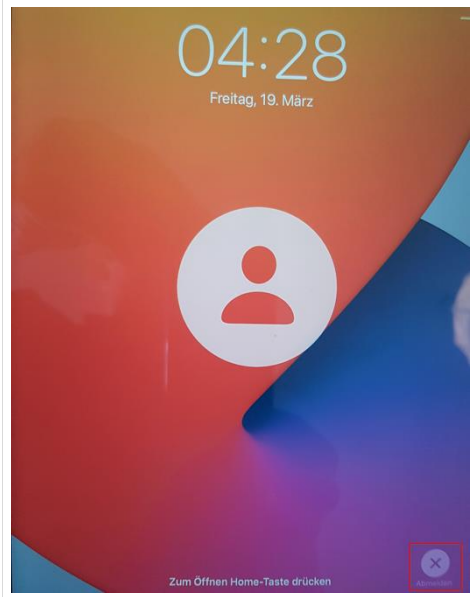

Abb. 82: Abmelden

12 „Shared Ipad" mit dem Apple School Manager

Die von Apple bereitgestellte Technologie "*Shared iPad*" macht es möglich, dass mehrere Nutzer ein gemeinsames Ipad verwenden, ohne dass Daten der anderen Benutzer eingesehen werden können. Voraussetzung für die Verwendung von „Shared Ipads" ist das Anlegen von AppleIDs und Klassen im Apple School Manager (ASM).

Die Technik ist datenschutzrechtlich umstritten. Insbesondere muss verhindert werden, dass Nutzerdaten wie Vor- und Nachname in den Apple School Manager synchronisiert werden. Der Einsatz der Technik sollte maßvoll geschehen, das heißt nur dann, wenn in der Schule auch tatsächlich auf geteilte Ipads umfänglich gesetzt wird.

Die paedML Linux und GS bietet über die Einbindung des Univention App Centers mir der App „Apple School Manager Connector" eine Möglichkeit, Benutzer und deren Rolle (Lehrer oder Schüler) anonymisiert (Benutzernamen) und die jeweiligen Klassen in den Apple School Manager zu synchronisieren. Auf Grundlage des synchronisierten Benutzernamens und der im Apple School Manager hinterlegten Domäne wird automatisch eine AppleID erzeugt.

Im Apple School Manager werden Anmeldeinformationen für jede AppleID, das heißt für jeden Schüler*in und jeden Lehrer*in, auf Basis des Benutzernamens erstellt. Zum Beispiel würde für den paedML-Benutzer *li.mu* der Schule mit der Domäne deine-schule.de die verwaltetet Apple-ID *li.mu-@appleid.deine-schule.de* erstellt.

Diese AppleIDs und Klassen werden nun in das MDM synchronisiert. Ipads können über das MDM als „Shared Ipads" definiert werden.

Mit der erstellen AppleID und der erstellten Anmeldeinformationen ist eine Anmeldung an „Shared Ipads" möglich.

12.1 Der Univention Apple School Manager Connector

Im Folgenden wird die Installation und Konfiguration des Apple School Manager Connectors beschrieben.

12.1.1 Installation des Apple School Manager Connectors

Öffnen Sie die System- und Domäneneinstellungen ihres paedML Linux und GS Servers und öffnen Sie unter Software das App-Center.

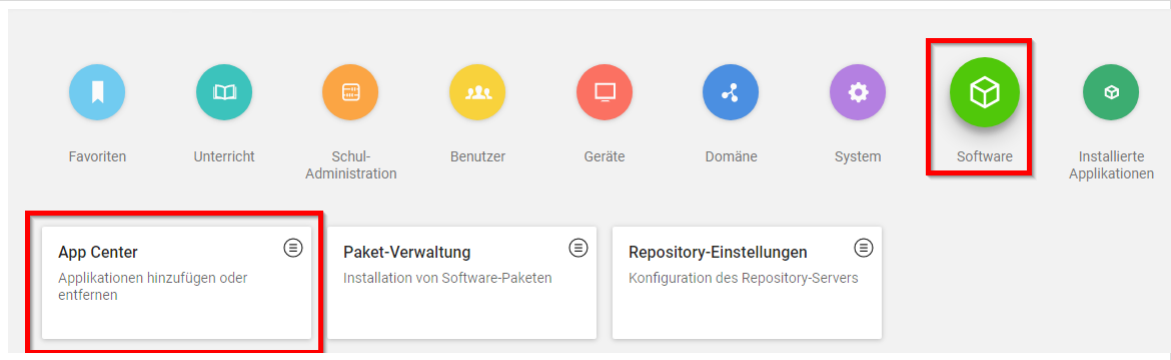

Abb. 83: App Center

Suchen Sie die Apple School Manager Connector und installieren Sie diesen.

12.1.2 Auslesen der Anmelde-Informationen aus dem ASM

Melden Sie sich mit einem administrativen Zugang am Apple School Manager an. Klicken Sie auf Einstellungen und auf Datenquelle SFTP. Gehen Sie auf Bearbeiten der SFTP-Verbindung.

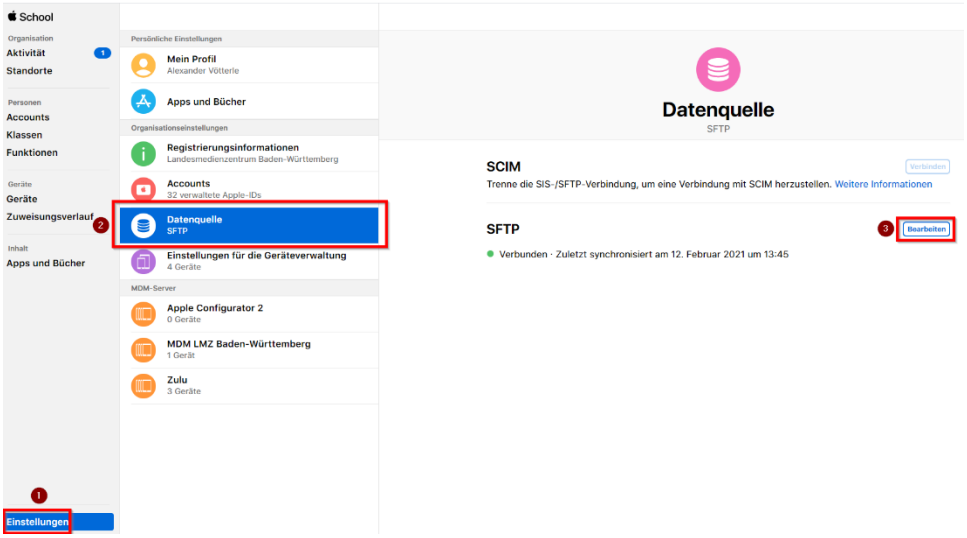

Abb. 84: Apple School Manager

Kopieren Sie den Benutzernamen und das Passwort. Diese Informationen benötigen Sie später bei der Einrichtung des Apple School Manager Connectors.

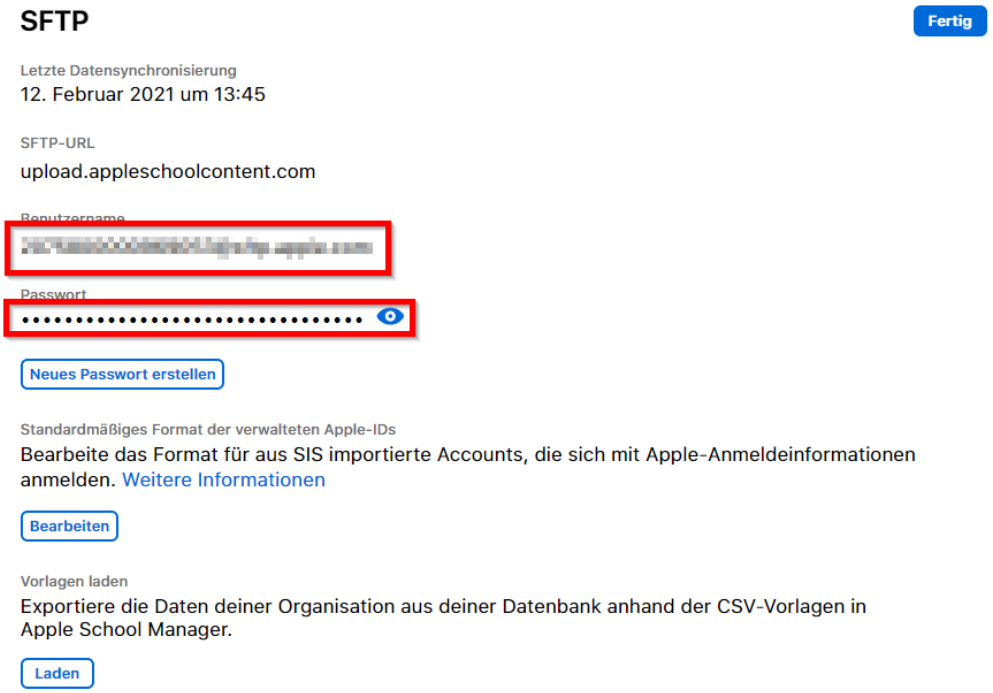

Abb. 85: Apple School Manager SFTP-Verbindung

12.1.3 Konfiguration des Apple School Manager Connectors

Öffnen Sie die System- und Domäneneinstellungen ihres paedML Linux und GS Servers. Klicken Sie im Bereich *Installierte Applikationen* auf den *Apple School Manager Connector*. Scrollen Sie nach unten zu *Installationen in der Domäne verwalten,* setzen Sie den Haken bei *server.paedml-linux.lokal* und klicken Sie auf *App-Einstellungen.*

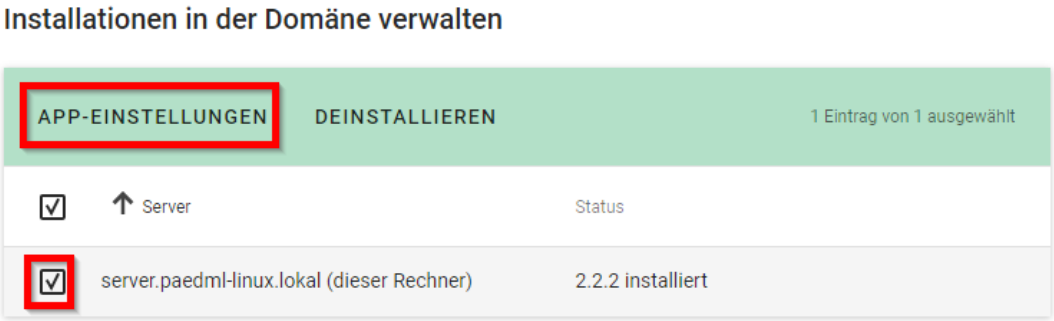

Abb. 86: Apple School Manager Konfiguration

Kopieren Sie den zuvor aus dem ASM gesicherten Benutzernamen und das zugehörige Passwort in die entsprechenden Felder. Setzen Sie den Haken für die Synchronisation nach der Speicherung der App-Einstellungen und wenden Sie die Änderungen an.

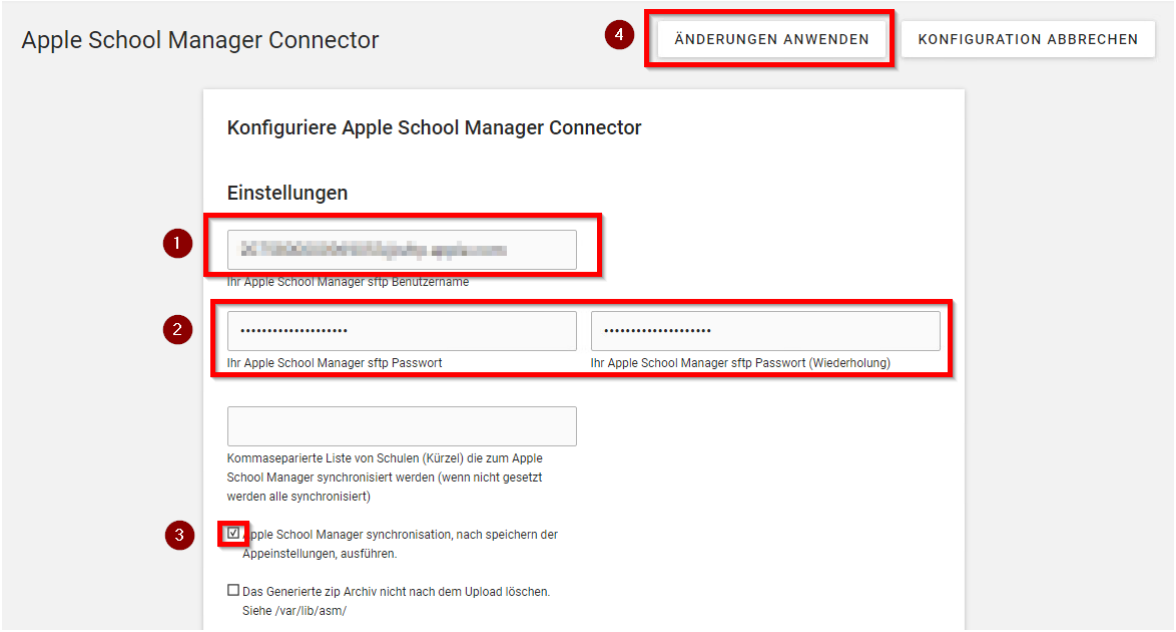

Abb. 87: Konfiguration des Apple School Manager Connectors

Optional können Sie eine tägliche automatisierte Synchronisation einrichten und eine Uhrzeit für diese definieren.

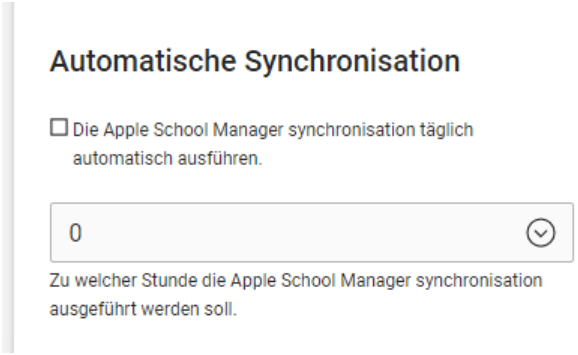

Abb. 88: ASM Connector: Automatische Synchronisation

12.2 Benutzerverwaltung im Apple School Manager

Im ASM werden nun auf Grundlage der anonymisierten paedML-Benutzer verwaltete AppleIDs angelegt. Zum Beispiel würde für den paedML-Benutzer *li.mu* der Schule mit der Domäne deine-schule.de die verwaltetet Apple-ID *li.mu-@appleid.deine-schule.de* erstellt.

Mit diesen erfolgt später die Anmeldung am Ipad. Zusätzlich müssen im ASM Passwörter vergeben werden. Die Verwaltung der Passwörter unterscheidet sich bei Lehrern und Schülern erheblich.

12.2.1 Lehrer-Zugänge

Melden Sie sich am ASM an. Sie sehen unter Accounts nun die synchronisierten paeedML-Benutzer. Wählen Sie den Lehrer-Account aus, für den Sie eine Anmeldeinformation (Passwort) erstellen möchten.

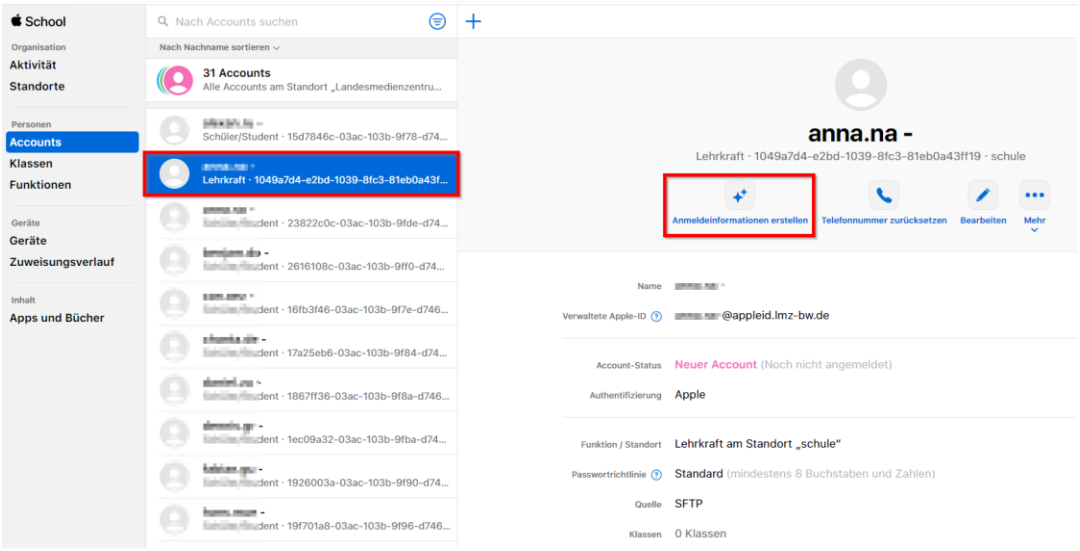

Abb. 89: ASM: Anmeldeinformation erstellen

Erstellen Sie nun die pdf mit den Anmeldeinformationen, klicken Sie auf *„laden“* oder kommunizieren Sie das Passwort auf anderem Wege.

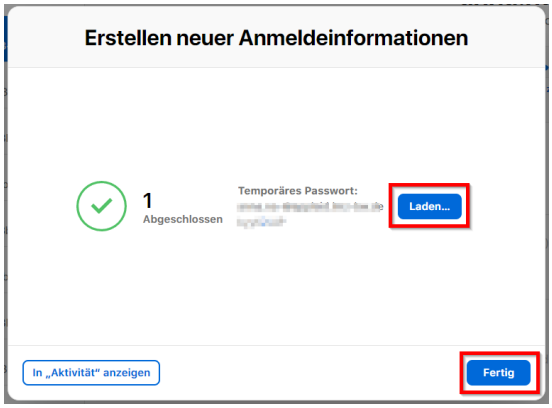

Abb. 90: ASM: Anmeldeinformation erstellen 2

Das Passwort ist ein temporäres Passwort, das die Benutzerin oder der Benutzer beim ersten Anmelden an einem Shared Ipad benötigt.

Der Lehrer oder die Lehrerin erstellt dann selbst eine sichere Anmeldung, die unter anderem eine Zwei-Faktoren-Authentifizierung enthält (siehe Kapitel 11.5).

12.2.2 Schüler-Zugänge

Melden Sie sich am ASM an. Sie sehen unter Accounts nun die synchronisierten paedML-Benutzer. Wählen Sie den Schüler-Account aus, für den Sie eine Anmeldeinformation (Passwort) erstellen möchten.

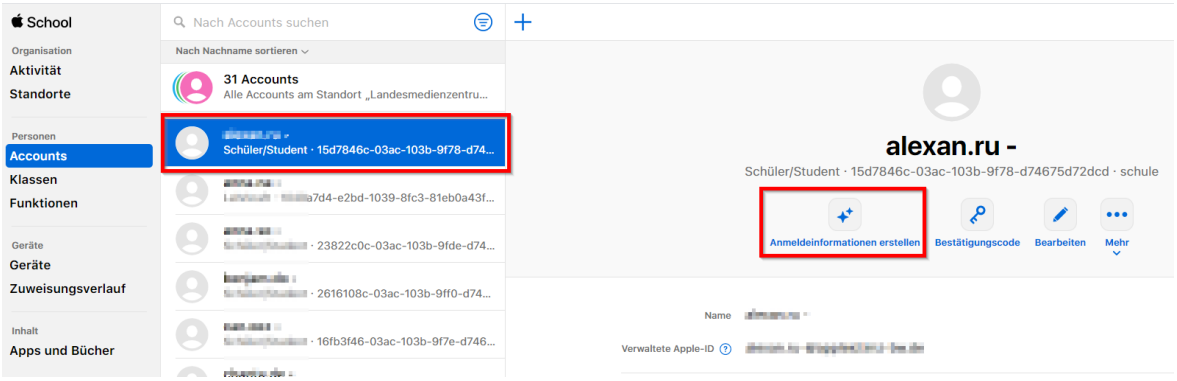

Abb. 91: ASM: Anmeldeinformation erstellen

Erstellen Sie nun ein vierstelliges Zahlen-Startpasswort, klicken Sie auf *„laden“* oder kommunizieren Sie das Passwort auf anderem Wege.

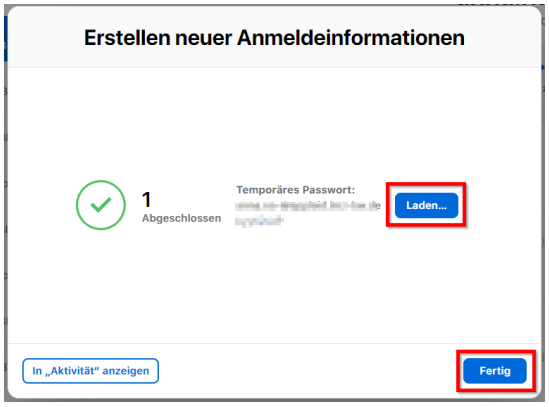

Abb. 92: ASM: Anmeldeinformation erstellen 2

Das Passwort ist ein temporäres Passwort, das die Benutzerin oder der Benutzer beim ersten Anmelden an einem Shared Ipad benötigt.

Der Schüler oder die Schülerin erstellt dann selbst ein vierstelliges Zahlen-Passwort.

12.3 Synchronisierung in das MDM

Die im ASM angelegten Benutzer müssen nun in das MDM synchronisiert werden. Die Anleitung bezieht sich wieder auf Jamf School. Ein abermaliger Hinweis auf die exemplarische Bedeutung des MDMs Jamf School für diese Dokumentation würde die Leser an dieser Stelle sicherlich langweilen.

Melden Sie sich bei Jamf School an und navigieren Sie zu *Einstellungen*. Klicken Sie im *Bereich Apple School Manager* auf Ihren ASM-Account.

Setzen Sie die Haken bei

- Synchronisierung verwalteter Apple IDs (…) aktivieren
- Synchronisierung von Klassen aktivieren
- Fehlende Klassen werden erstellt

- Fehlende Benutzer werden erstellt
- Versuchen, Benutzer (…) anhand des Benutzernamens abzugleichen
- Klassennamen verwenden

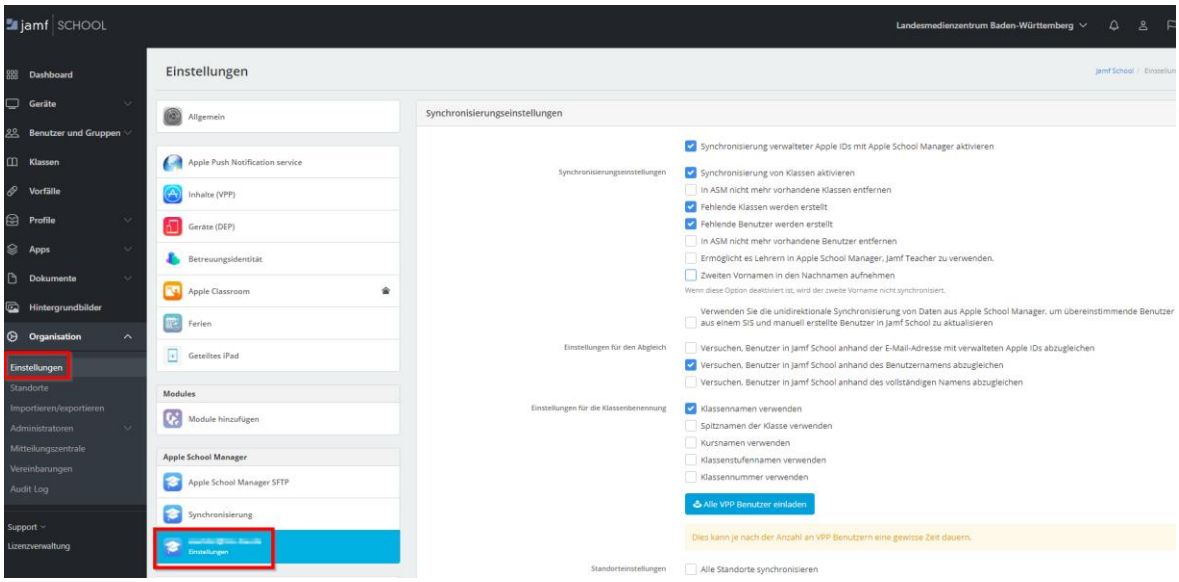

Abb. 93: ASM-Jamf School-Synchronisation einrichten

Führen Sie die Standortzuordnung durch. Die Standorte können Sie aus dem ASM und Jamf School auslesen. Speichern Sie die Einstellungen.

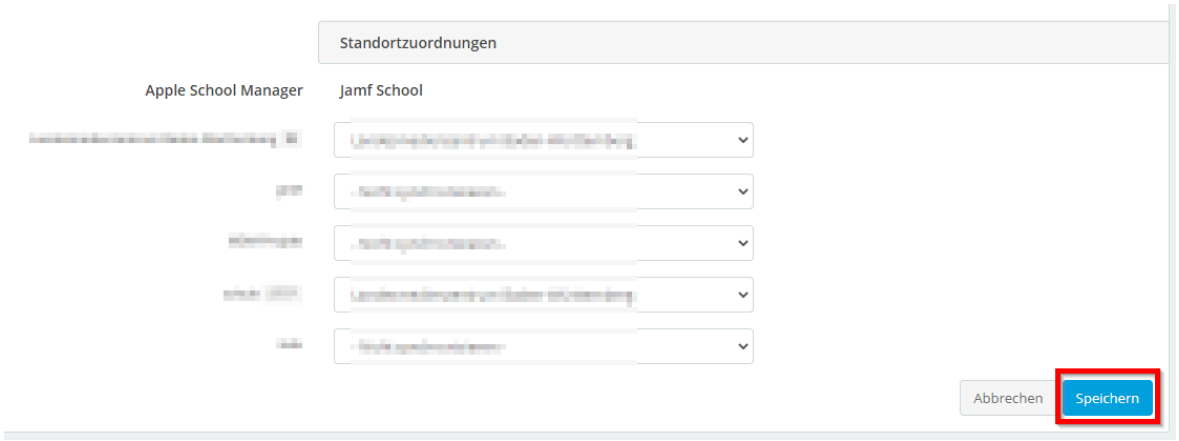

Abb. 94: ASM-Jamf School-Synchronisation einrichten und speichern

Klicken Sie unter *Klassen* auf *Mit ASM synchronisieren*.

Abb. 95: ASM-Jamf School-Synchronisation ausführen

Die Benutzer und Klassen sollten nun in jamf School vorliegen.

12.4 Ausrollen von Shared Ipads mithilfe des MDMs

Damit eine Anmeldung an Ipads mit den paedML-Benutzer-basierten AppleIDs möglich ist, müssen diese als Shared Ipad eingerichtet werden.

In Jamf School wählen Sie dazu unter *Profile | DEP Profile | iOS Einstellungen | Geteiltes Ipad aktiveren*.

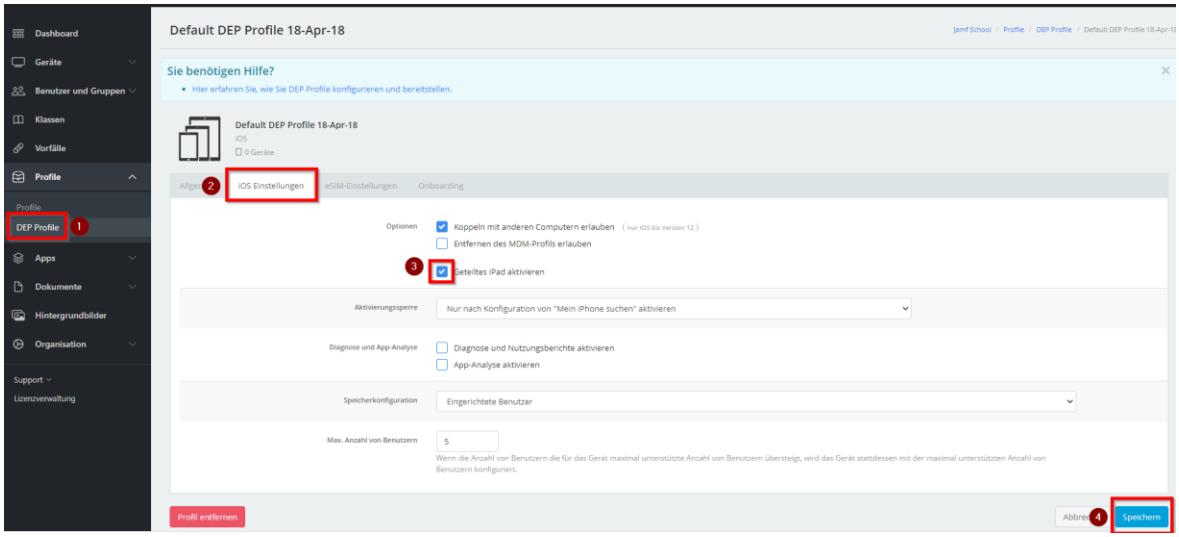

Abb. 96: ASM-Jamf School-Synchronisation ausführen

Im Anschluss müssen Sie das Ipad per MDM zurücksetzen.

12.5 Anmelden und Arbeiten am Shared Ipad

12.5.1 Anmelden als Lehrer/in

Die Anmeldung erfolgt am *Shared Ipad* mit der verwalteten AppleID und dem temporären Passwort. Nach erfolgreicher Anmeldung muss als zweiter Faktor eine Handynummer hinterlegt werden.

Anschließend muss ein eigenes Passwort erstellt werden.

12.5.2 Anmelden als Schüler/ in

Die Anmeldung erfolgt am *Shared Ipad* mit der verwalteten AppleID und dem temporären Passwort.

Anschließend muss ein eigenes Passwort erstellt werden.

12.5.3 Arbeiten mit dem Shared Ipad

Von Cloudprodukten von Apple empfehlen wir dringend Abstand zu nehmen. Dateien sollten daher in einer datenschutzkonformen Cloud gespeichert werden.

Wir empfehlen die Verwendung der paedML Linux Nextclouderweiterung (siehe Kapitel 8).

13 MDM: LDAP-Authentifizierung und Benutzer-Synchronisation

Es ist generell möglich, dass Nutzerdaten aus dem LDAP-Verzeichnis der paedML in andere Systeme übernommen werden. Im Folgenden wird am Beispiel des von vielen Schulen in unserem Kundenkreis eingesetzten MDM *„Jamf School“* die Synchronisation der paedML-Benutzer und Einrichtung einer LDAP-Authentifizierung beschrieben.

Eine konkrete Empfehlung wird nicht ausgesprochen. **Nicht zuletzt muss vom Betreiber der Instanz (Schule bzw. Schulträger) geprüft werden, ob Datenschutzbestimmung eingehalten werden.** Vergleiche hierzu https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen.

Das beschriebene Vorgehen erscheint im Zusammenhang mit der 1:1-Zuordnung von Ipads und vor allem bei on-premise-Installationen des MDM sinnvoll.

In kleineren Umgebungen erscheint auch der Einsatz technischer Nutzer der Art „ipad-1“ sinnvoll.

13.1 Installation des Jamf School Connectors

Der Jamf School Connector ist eine Univention-App, mit deren Hilfe ein systeminterner Nutzer angelegt wird, mit dessen Hilfe später die Synchronisation und Authentifizierung erfolgt.

Öffnen Sie die System- und Domäneneinstellungen ihres paedML Linux und GS Servers und öffnen Sie unter Software das *App-Center*.

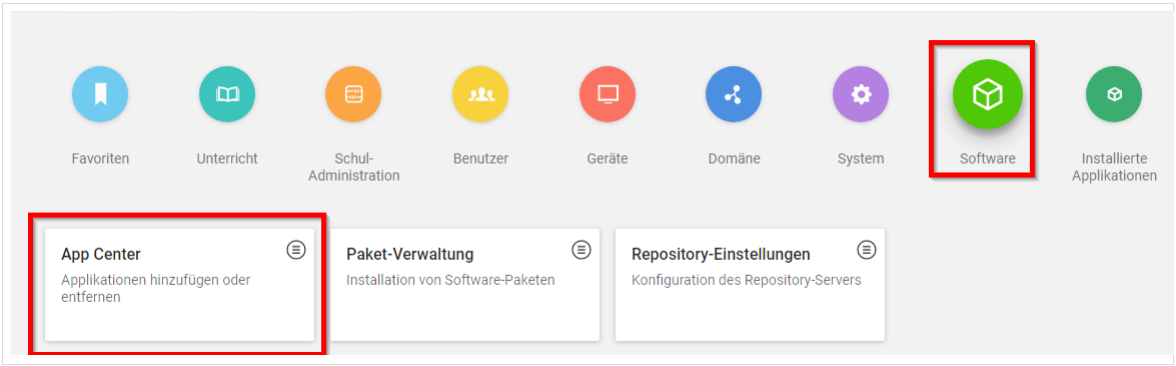

Abb. 97: App Center

Suchen Sie die App *Jamf School Connector* und installieren Sie diese.

13.2 Firewall-Einstellungen

Für eine LDAP-Authentifizierung gegen den paedML Linux und GS Server muss die Firewall angepasst werden.

13.2.1 Ports und IP-Adressen laut Jamf School

Damit der Zugriff von *Jamf School* auf das LDAP des paedML-Servers möglich ist, muss eine NAT-Regel in der Firewall erstellt werden. Dazu stellt *Jamf School* eine Doku zu den notwendigen Ports und IP-Adressen zur Verfügung:

https://docs.jamf.com/jamf-school/deploy-guide-docs/Firewall_Ports,_IP_Addresses,_and_URLs_Used_by_Jamf_School.html

Die IP-Adressen können sich ändern. In diesem Fall kann die Synchronisierung fehlschlagen. Bei Problemen mit der Synchronisation und Authentifzierung sollte daher zunächst geprüft werden, ob die IP-Adressen noch aktuell sind.

13.2.2 Alias-Erstellung

Melden Sie sich an der Firewall an. Legen Sie einen Alias *„JamfSchool"* für (**aktuell**) folgende IP-Adressen an:

```
94.130.139.182, 94.130.139.190, 94.130.139.187, 94.130.243.182,
94.130.139.188, 212.178.82.42, 94.130.10.180, 18.194.106.10, 18.194.230.93,
3.124.51.124
```

Vergessen Sie nicht die Änderungen nach dem Speichern des Alias anzuwenden.

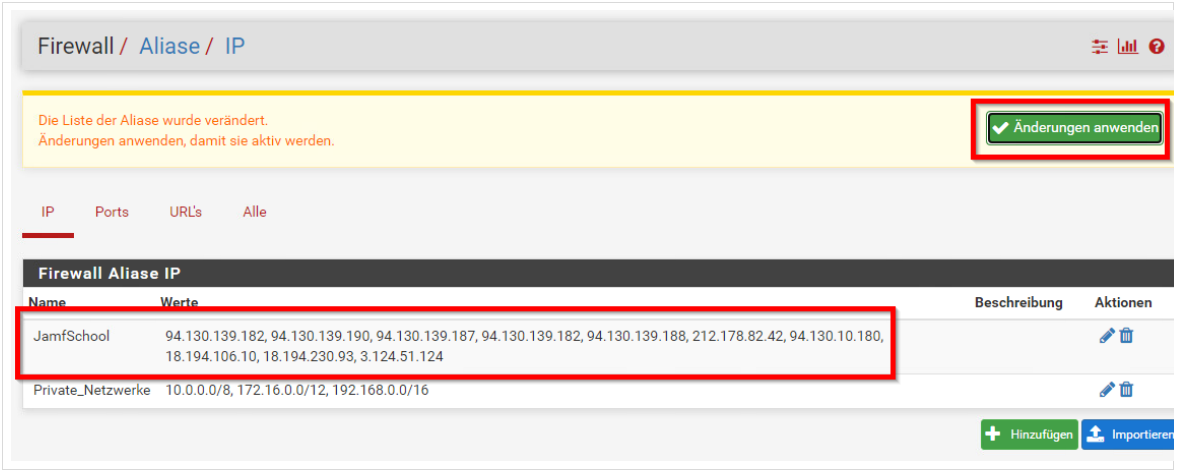

Abb. 98: Firewall Alias JamfSchool erstellen

13.2.3 NAT-Einstellung

Gehen Sie zu *Firewall | NAT | Port Weiterleitung*. Klicken Sie auf *Hinzufügen*.

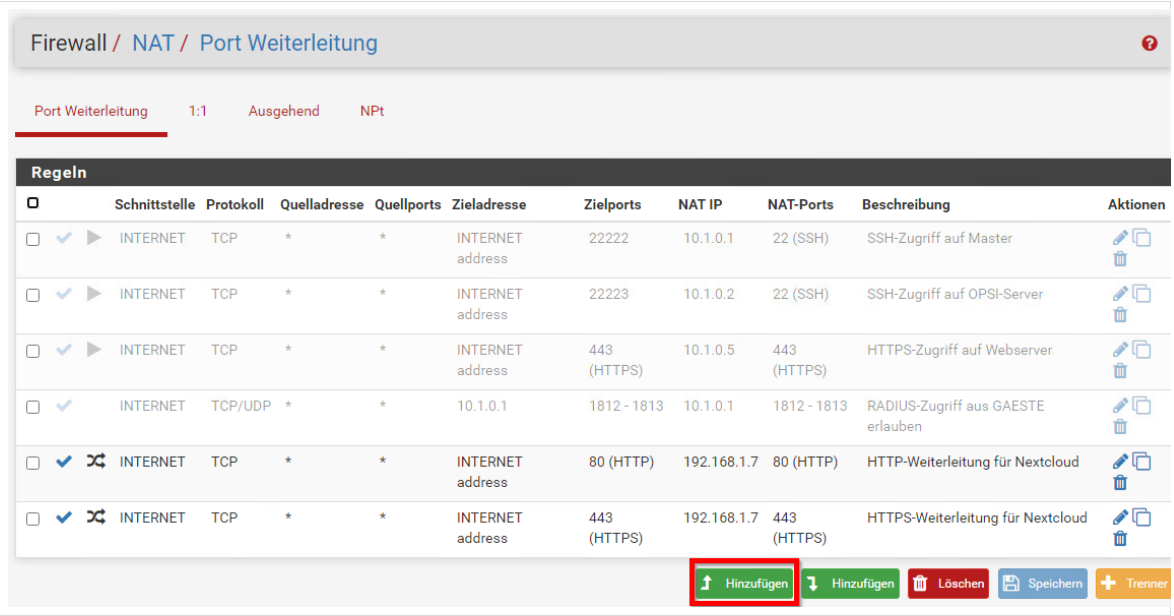

Abb. 99: Firewall NAT-Regel für LDAP(s) erstellen 1

Wählen Sie:

- Schnittstelle: INTERNET
- Protokoll: TCP/UDP
- Quelle: Einzelner Host oder Alias JamfSchool
- Ziel: Internet address
- Zielportbereich: *Von LDAP(s) bis LDAP(s)*
- Umleitungsziel-IP: *10.1.0.1*
- Umleitungszielport: *LDAP(s)*
- Beschreibung: LDAP-Weiterleitung von Jamf School zum Server auf LDAP(s)
- Und *speichern* Sie die Einstellungen.
- Klicken Sie auf *Änderungen anwenden*.

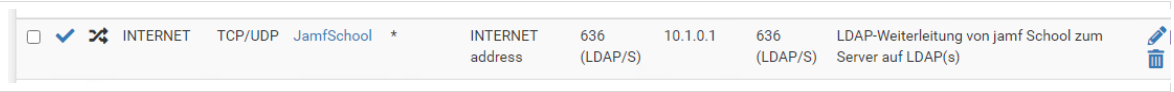

Abb. 100: Firewall NAT-Regel für LDAP(s) erstellen 2

13.3 Synchronisierung von Nutzern

Melden Sie sich bei *„Jamf School“* an.

Navigieren Sie zu *Organisation | Einstellungen | Synchronisierung*.

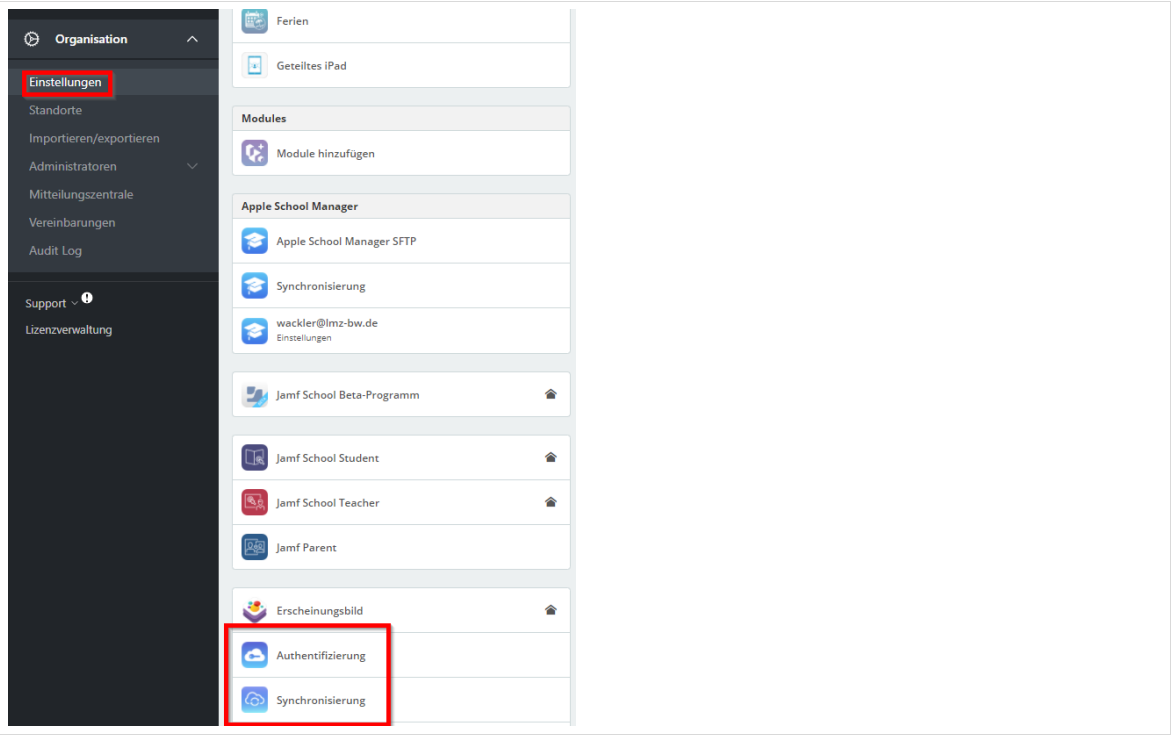

Abb. 101: Jamf School Synchronisierung 1

Tragen Sie dort die folgenden Werte ein. Unter LDAP-Server tragen Sie die externe IP-Adresse Ihres Schul-Servers ein.

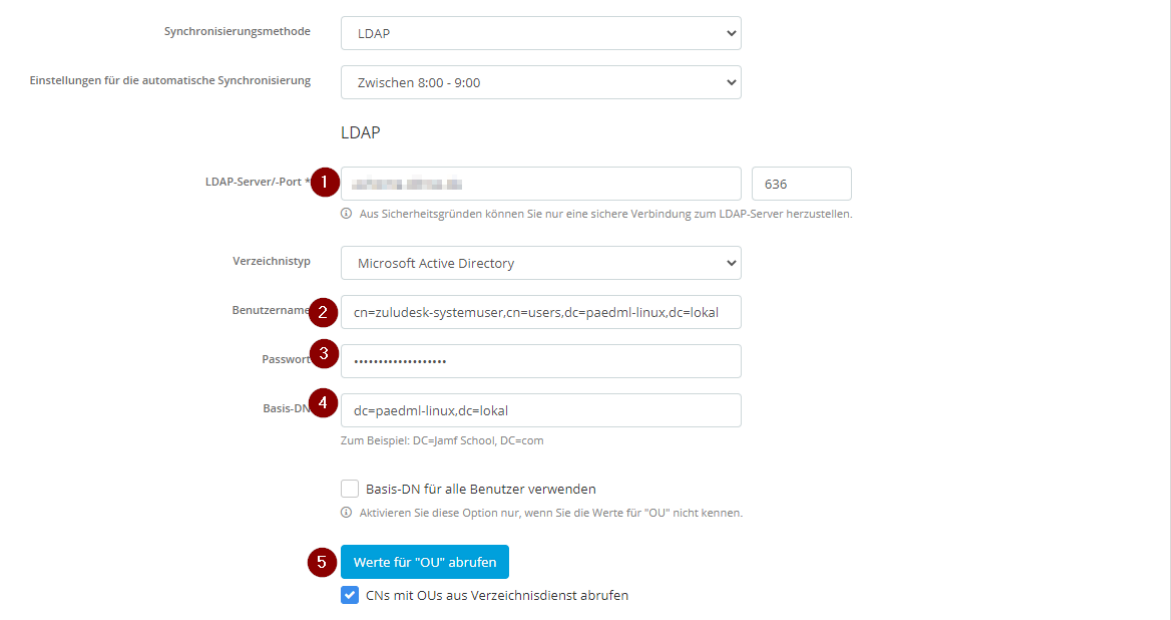

Abb. 102: Jamf School Synchronisierung 2

Tragen Sie 1. die externe Adresse ihres paedML Servers, 2. den Benutzernamen *cn=zuludesk-systemuser,cn=users,dc=paedml-linux,dc=lokal* und 3. das zugehörige Passwort ein. Das Passwort erhalten Sie aus der Datei */etc/zuludesk.secret* auf dem Server. Tragen Sie als *Base-DN dc=paedml-linux,dc=lokal* ein und klicken Sie auf *Werte für „OU" abrufen*.

Klicken Sie anschließend auf *Verbindung testen*.

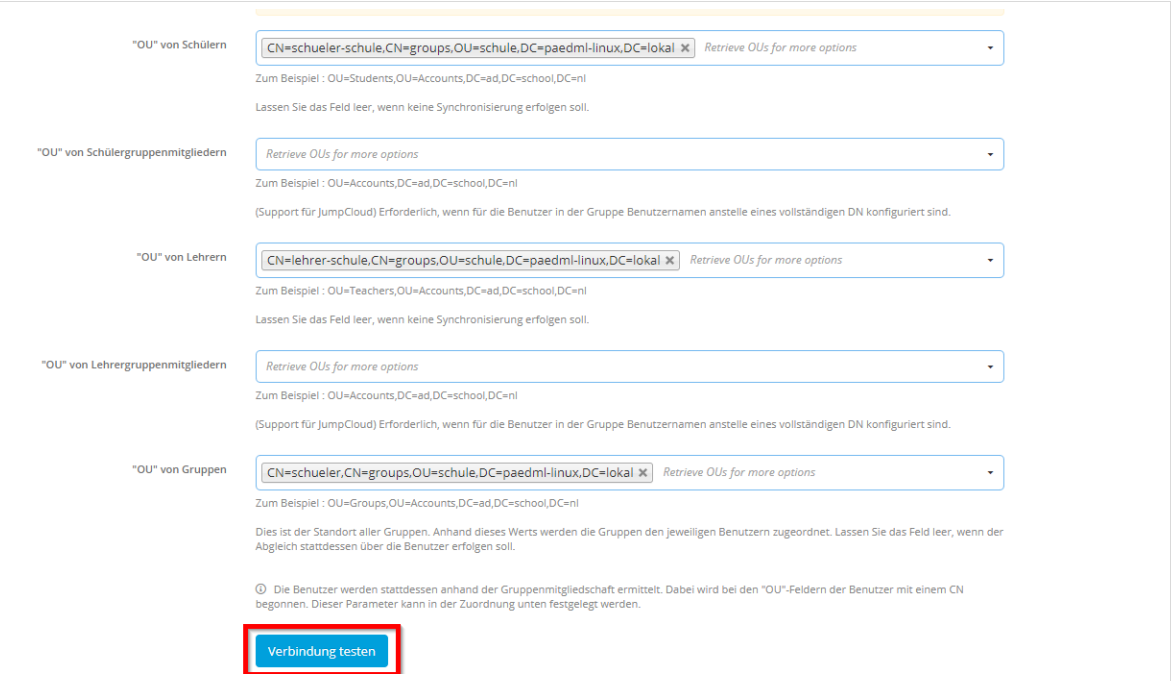

Abb. 103: Jamf School Synchronisierung 3

Die Verbindung muss erfolgreich sein.

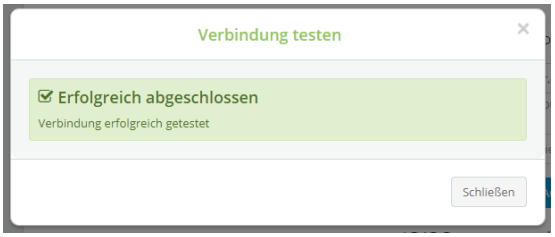

Abb. 104: Jamf School Synchronisierung Testergebnis

Kontrollieren Sie die folgenden Einstellungen. Der Eintrag beim Benutzernamen weicht vom Standardwert ab. Er muss *„cn“* lauten.

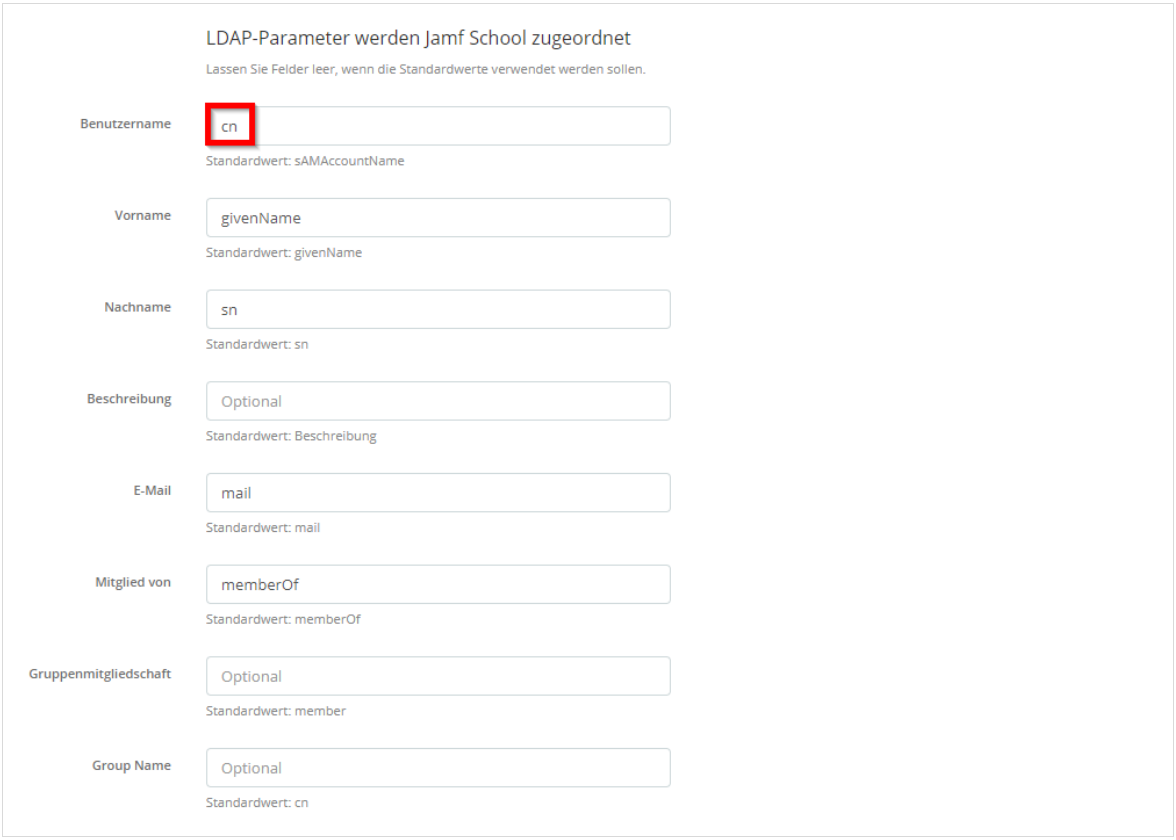

Abb. 105: Jamf School Synchronisierung 4

Speichern Sie die Einstellungen

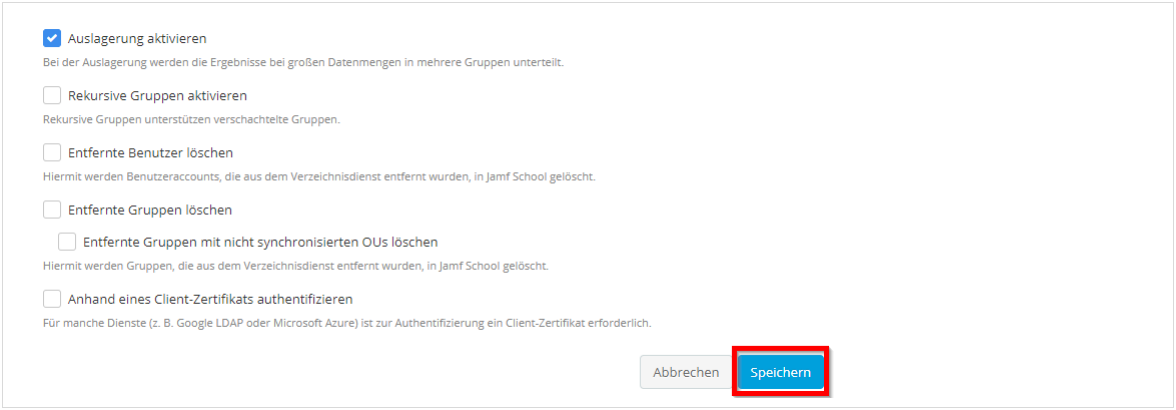

Abb. 106: Jamf School Synchronisierung: Speichern

Gehen Sie zum Dashboard und klicken Sie dort auf *Jetzt synchronisieren*.

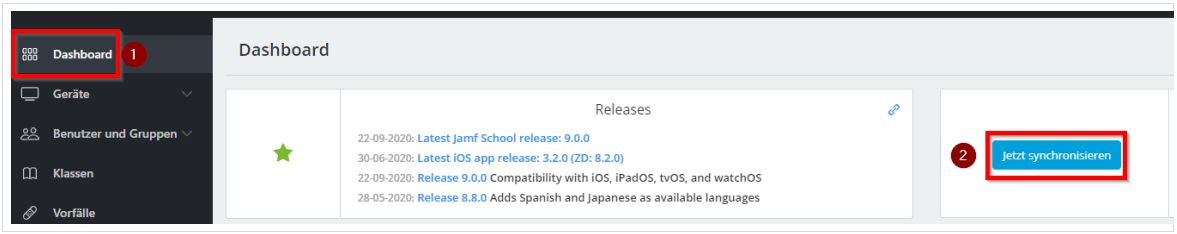

Abb. 107: Jamf School Synchronisierung durchführen

Kontrollieren Sie anhand der Benutzerzahl, ob die Synchronisierung erfolgreich war.

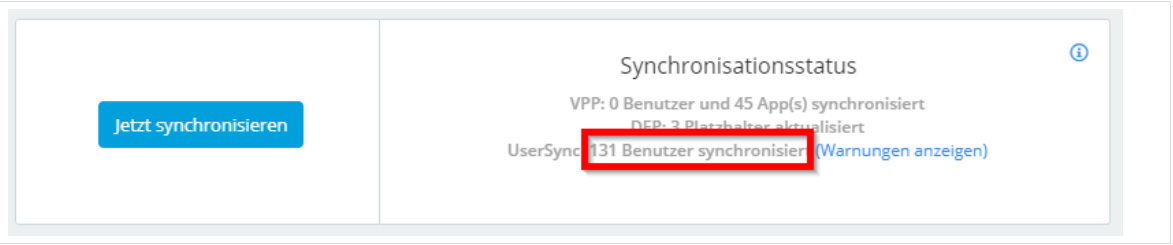

Abb. 108: Jamf School Synchronisierung durchgeführt

13.4 Benutzerauthentifizierung gegen das paedMLL-LDAP

Unter *Organisation | Einstellungen | Authentifizierung* ist einzustellen:

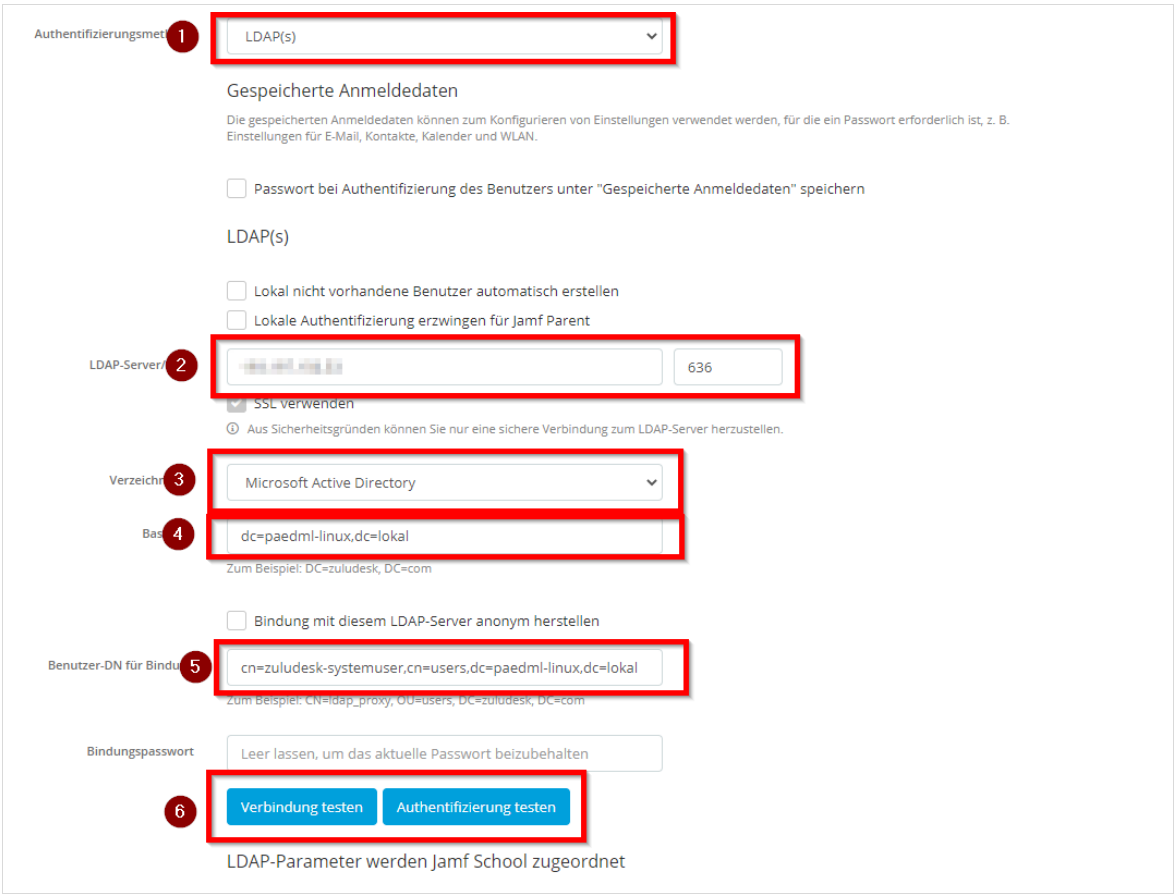

Abb. 109: Jamf School Authentifizierung 1

Klicken Sie auf Verbindung testen. Der Test muss erfolgreich abgeschlossen werden.

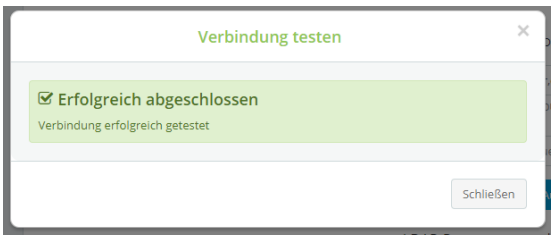

Abb. 110: Jamf School Authentifizierung: Testergebnis Verbindung

Anschließend klicken Sie auf Authentifizierung testen. Melden Sie sich mit den Zugangsdaten eines paedML-Benutzers an. Im Beispiel wurde der Benutzer *netzwerkberater* verwendet.

Abb. 111: Jamf School Authentifizierung:Test

Auch dieser Test muss erfolgreich sein.

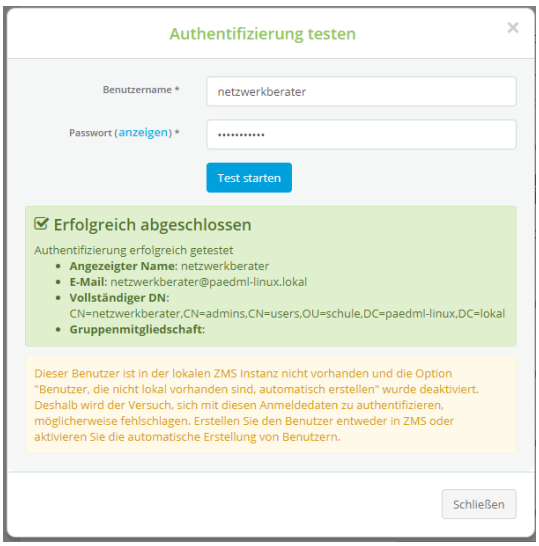

Abb. 112: Jamf School Authentifizierung: Testergebnis

14 Die Classroom-App – Steuerung von Schülergeräten

In diesem Kapitel soll aufgezeigt werden, wie mit den oben synchronisierten Benutzern in *Jamf School* und der App *Classroom* von Apple eine Steuerung des Unterrichts bei Tablets auf einem Niveau (ähnlich wie wir das aus der Schulkonsole der paedML Linux und GS kennen) erreicht werden kann. In Verbindung mit der oben beschriebenen Protokollierung und dem eingerichteten Jugendschutzfilter ist so eine Nutzung von Tablets möglich, die den hohen (pädagogischen und technischen) Ansprüchen der paedML genügt.

Dazu werden zunächst in *Jamf School* Klassen angelegt, die dann später in der App *Classroom* bei der Steuerung des Unterrichts verwendet werden können.

Die Classroom-App kann im Zusammenhang mit Gastzugängen am Ipad nicht genutzt werden, da in diesem Fall dem Ipad kein Benutzer zugeordnet oder am Ipad keiner angemeldet ist.

14.1 Anlegen von Klassen in Jamf School

Gehen Sie in den Bereich *Klassen* und klicken Sie dort auf *Klasse hinzufügen*.

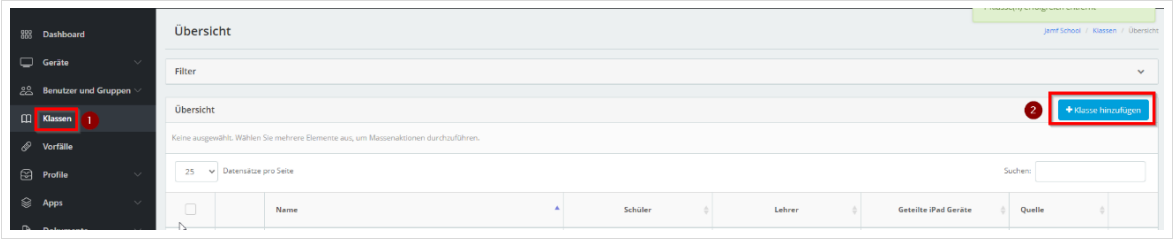

Abb. 113: Jamf School Klasse hinzufügen

Vergeben Sie einen Namen und tragen Sie optional eine Beschreibung ein.

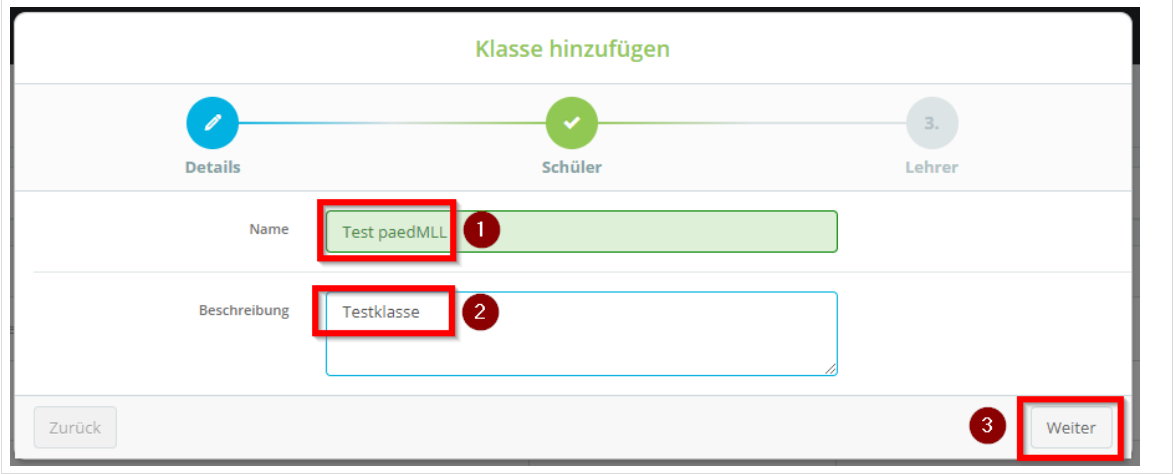

Abb. 114: Jamf School Klasse benennen

Sie können nun eine Klasse hinzufügen, indem Sie den Klassennamen aus der paedML Linux und GS mit vorangestelltem schule- eingeben. Hier schule-1a. Klicken Sie auf alle hinzufügen.

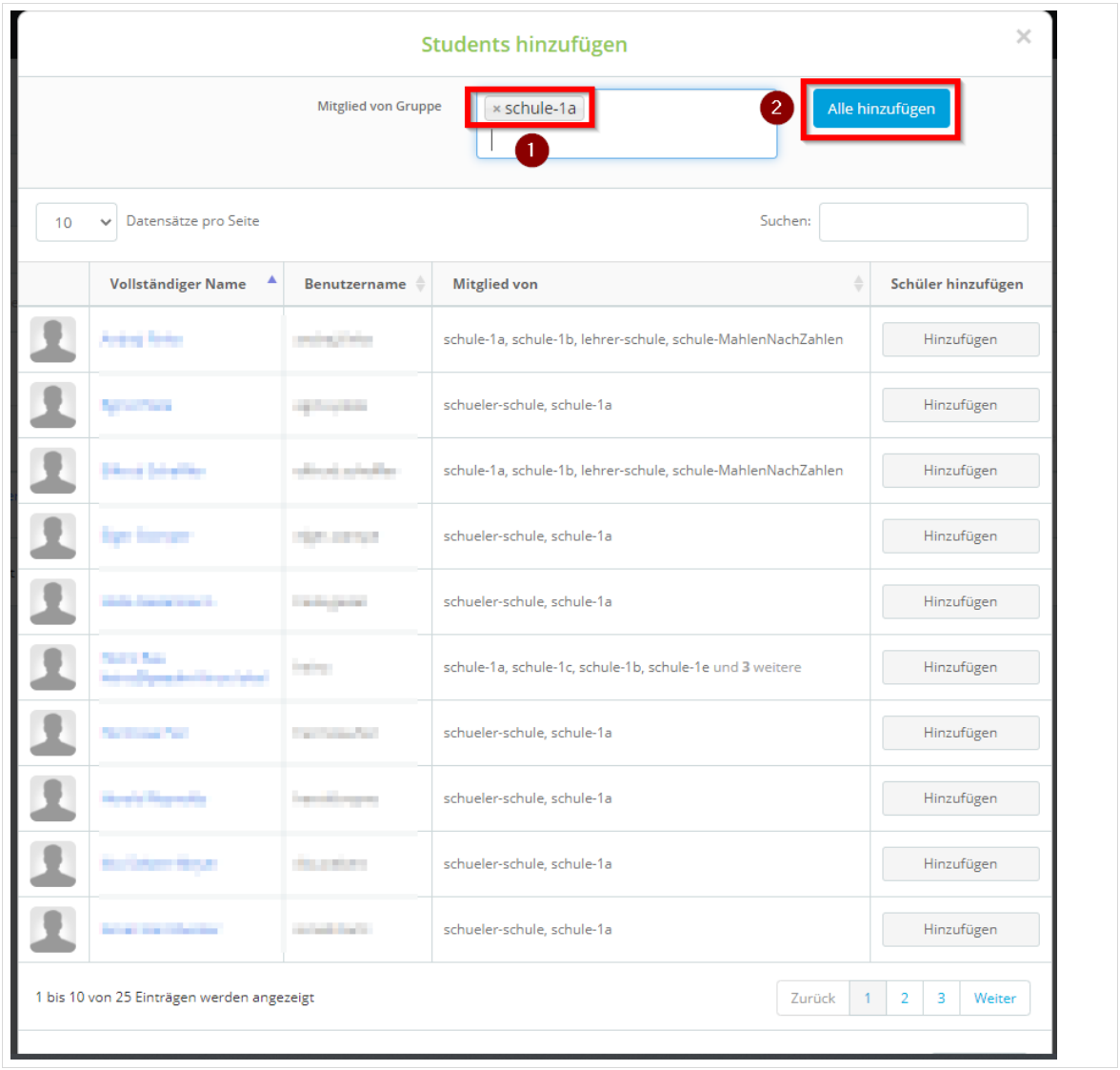

Abb. 115: Jamf School Benutzer zu Klasse hinzufügen

Kontrollieren Sie die folgende Liste auf eingetragene Lehrer und entfernen Sie diese. Hintergrund ist, dass Lehrer, die sich der Klasse in der paedML Linux und GS über die Schulkonsole zugeordnet haben, in der Gruppe der Klasse enthalten sind.

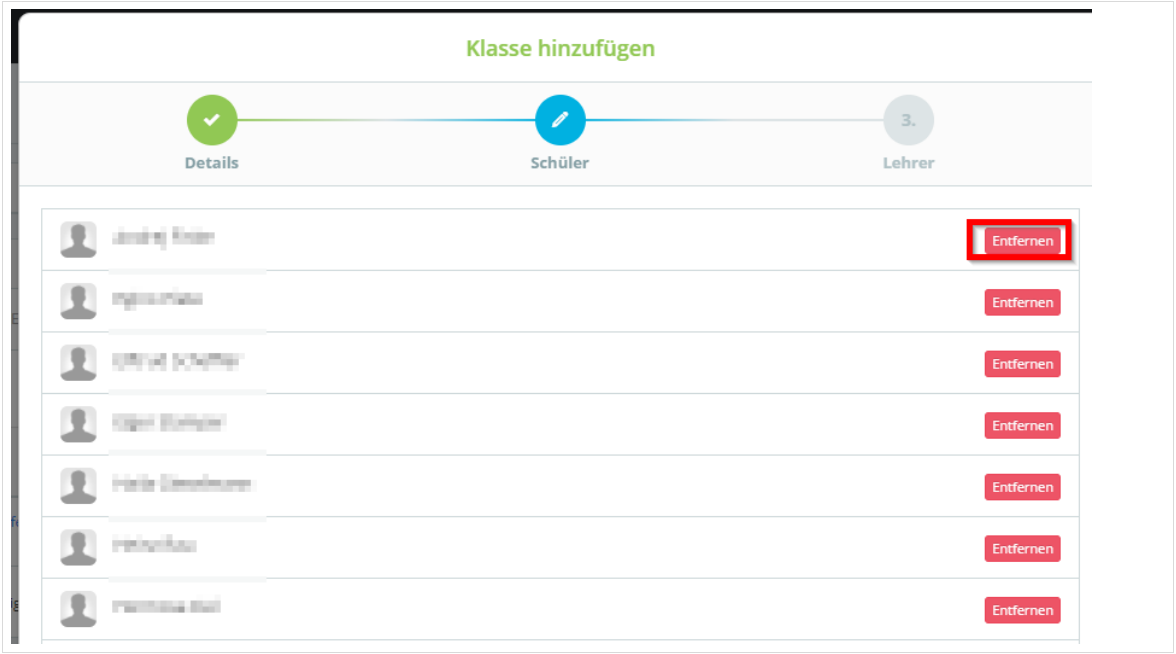

Abb. 116: Jamf School Lehrer entfernen

Fügen Sie nun einen Lehrer der Klasse hinzu und klicken Sie auf *Fertig stellen*.

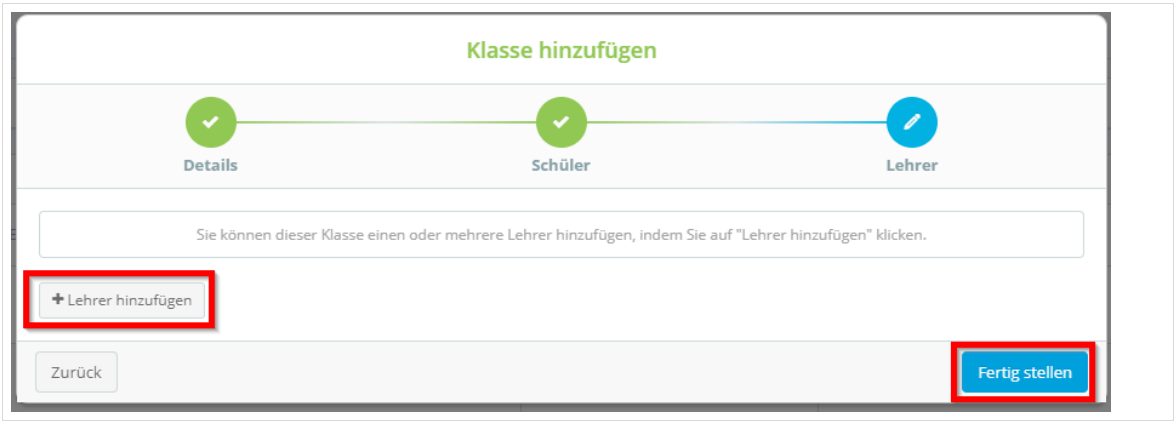

Abb. 117: Jamf School Lehrer hinzufügen

14.2 Apple Classroom-App konfigurieren und verteilen

Gehen Sie in *Jamf School* zu *Einstellungen | Apple Classroom*. Kontrollieren Sie, ob die Haken bei *Apple Classroom ausgehend von Klassen und Benutzern in Jamf School automatisch erstellen* und bei *Ändern der Berechtigung zum Beobachten des Bildschirms erlauben* gesetzt sind.

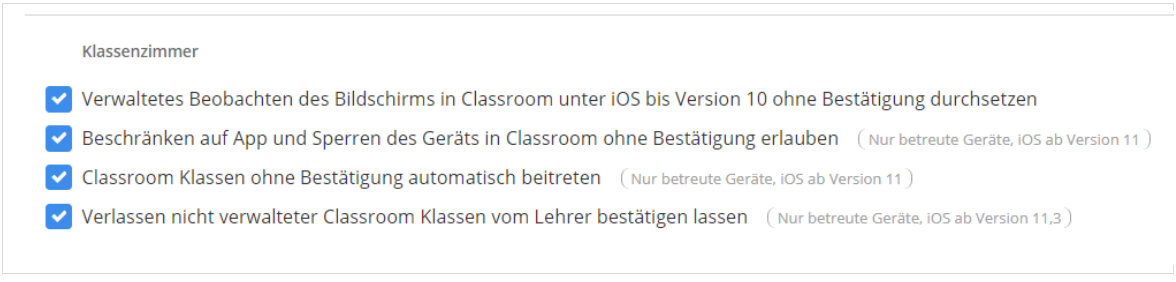

Abb. 118: Jamf School: Einschränkungen für Classroom-App

Das Profil der Schüler*innen-Tablets, die mithilfe der Classroom-App gesteuert werden sollen, muss angepasst werden. Navigieren Sie zu *Profile* und dort

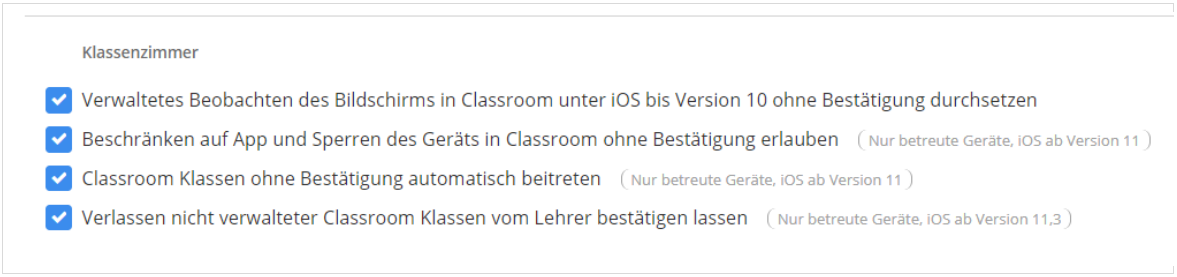

Abb. 119: Jamf School: Einschränkungen für Classroom-App

Verteilen Sie die App per Jamf School an die Tablets.

14.3 Arbeiten mit der Apple Classroom App

Öffnet der Lehrer einer Klasse an dem ihm zugeordneten Tablet die App Classroom erscheinen die den Schüler*innen der Klasse zugeordneten Tablets (fest im 1:1 Scenario oder temporär bei 1:n).

Im Folgenden sind zwei Ipads (Lehrer-iPad und ein Schüler-iPad) tatsächlich in einem Raum. Das im Raum befindliche Schüler-iPad wird mit seinem aktuellen Bildschirm angezeigt. Dies gibt der Lehrerkraft bereits eine erste Übersicht, welche Inhalte die Schüler*innen auf ihrem iPad betrachten.

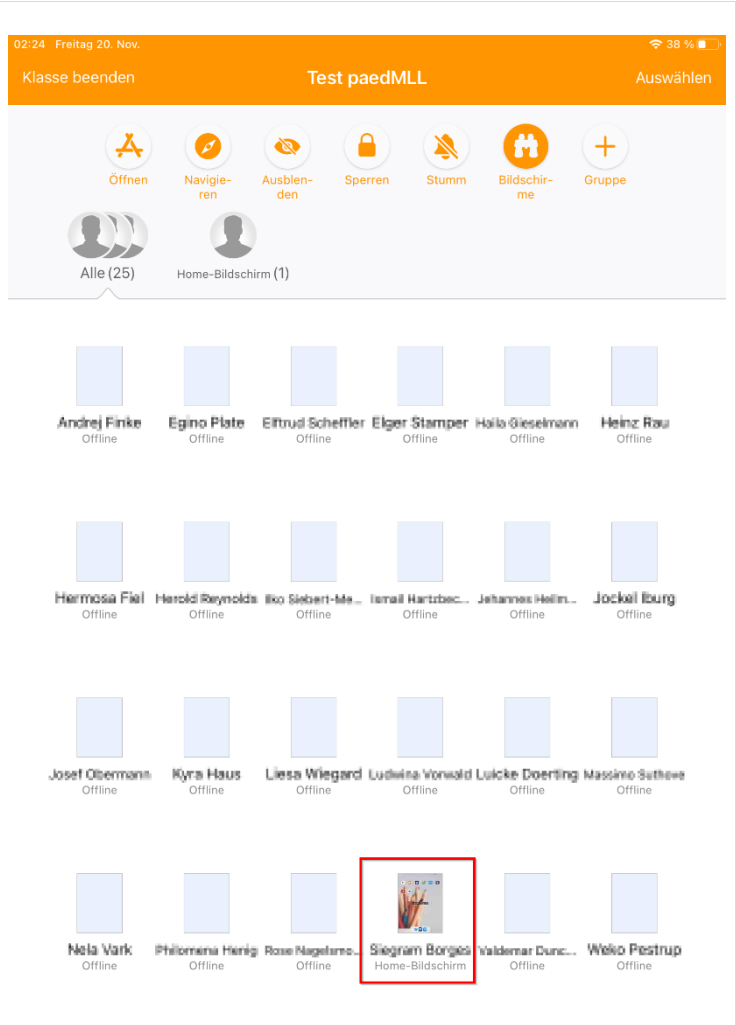

Abb. 120: Classroom App

Durch Berühren des Bildschirms öffnen sich weitere Möglichkeiten zur Steuerung des Schüler-Geräts.

1. Eine bestimmte App kann auf dem Schüler-iPad geöffnet werden.
2. In Safari kann zu einer bestimmten Seite navigiert werden.
3. Das Schüler-iPad kann gesperrt werden.
4. Der Bildschirm des Schüler-Ipads kann auf dem Lehrer-iPad gezeigt werden.

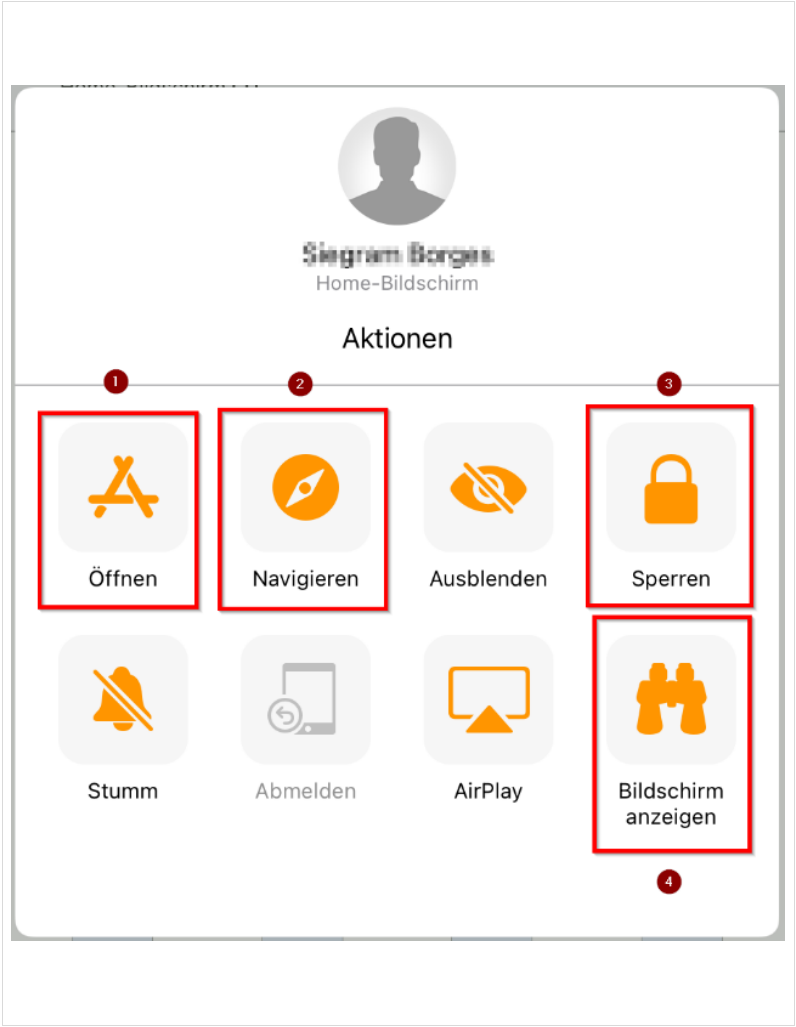

Abb. 121: Classroom App

Eine Anleitung zur *Classroom App* finden Sie unter https://support.apple.com/de-de/HT206151.

15 Konfiguration von Ipads im MDM-Netz

Windows-Clients in der paedML Linux und GS werden durch Gruppenrichtlinien und über opsi-Pakete so konfiguriert, dass möglichst wenig Telemetrie betrieben werden kann. Missbrauch durch SuS wird weitgehend unterbunden, indem Einstellungsmöglichkeiten reduziert werden. Umfangreiche technische Maßnahmen zum Schutz der Kinder und Jugendlichen sind vorhanden.

Ziel dieser Maßnahmen ist, SuS ein möglichst sicheres Arbeiten an den Clients zu ermöglichen.

Diese Zielsetzung möchten wir auf Ipads übertragen. Wir empfehlen daher über das MDM ein an die Verwendung im schulischen Kontext angepasstes Konfigurationsprofil zu erstellen und an die Ipads im MDM-Netz zu verteilen.

Die folgende Tabelle gibt eine Übersicht sinnvoller Einstellungen am Beispiel des MDM Jamf School.

Aus Gründen der Übersichtlichkeit werden nur Konfigurations-Items aufgeführt, bei der empfohlene Wert vom voreingestellten Wert differiert.

Die Übersicht erhebt keinerlei Anspruch auf Vollständigkeit. Sie soll lediglich Hinweise für sinnvolle Einstellungen im Zusammenhang mit Datenschutz, Missbrauchsvermeidung und dem Schutz von Kindern und Jugendlichen geben.

Konfigurations-Item	Empfohlener Wert	Ziel
FaceTime erlauben	Deaktiviert	Datenschutz
Automatisches Synchronisieren beim Roaming erlauben	Deaktiviert	Datenschutz
Installation von Apps erlauben	Deaktiviert	Vermeidung von Missbrauch
Entfernen von Apps erlauben	Deaktiviert	Vermeidung von Missbrauch
In-App-Käufe erlauben	Deaktiviert	Datenschutz, allgemeine Schutzfunktion
Siri erlauben	Deaktiviert	Datenschutz, Vermeidung von Missbrauch
Einschränkungen/Bildschirmzeit erlauben	Deaktiviert	Vermeidung von Missbrauch
Verwenden des iTunes Store erlauben	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion
iMessage erlauben	Deaktiviert	Vermeidung von Missbrauch
Podcasts erlauben	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion

„Meine Freunde suchen“ in der Suche-App erlauben	Deaktiviert	Vermeidung von Missbrauch
Game Center erlauben	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion
Book Store erlauben	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion
Apple Music erlauben	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion
Apple News erlauben	Deaktiviert	Allgemeine Schutzfunktion
iCloud ▪ Sichern in iCloud erlauben ▪ iCloud Dokumente… ▪ iCloud Schlüsselbund… ▪ iCloud Fotomediathek… ▪ Synchronisieren verwalteter Apps… ▪ Fotostream erlauben ▪ Gemeinsamer Fotostream…	Deaktiviert	Datenschutz
Touch ID das Entsperren des Geräts erlauben	Deaktiviert	Vermeidung von Missbrauch
Senden von Diagnosedaten an Apple erlauben	Deaktiviert	Datenschutz
Ändern des Codes erlauben	Deaktiviert	Vermeidung von Missbrauch
Abfrage von Passwörtern auf Geräten in der Nähe …	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion
Passwortfreigabe über Airdrop erlauben	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion
Interessensbezogene Werbung von Apple erlauben	Deaktiviert	Allgemeine Schutzfunktion
Koppeln mit Apple Watch erlauben	Deaktiviert	Vermeidung von Missbrauch
WLAN durchgehend aktiviert lassen	Aktiviert	Vermeidung von Missbrauch
Ändern der Accounteinstellungen…	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion, Datenschutz

Verwenden der Einstellung „Alle Inhalte (...) löschen“ erlauben	Deaktiviert	Vermeidung von Missbrauch
Ändern der Einstellung für „Freunde suchen“ erlauben	Deaktiviert	Vermeidung von Missbrauch
Ändern des Gerätenamens erlauben	Deaktiviert	Vermeidung von Missbrauch
App-Installation über den App Store erlauben	Deaktiviert	Vermeidung von Missbrauch, allgemeine Schutzfunktion, Datenschutz
Ändern persönlicher Hotspots erlauben	Deaktiviert	Vermeidung von Missbrauch
Ändern des Hintergrundbildes erlauben	Deaktiviert	Vermeidung von Missbrauch
Ändern von Mitteilungseinstellungen erlauben	Deaktiviert	Vermeidung von Missbrauch
Hinzufügen einer Mobilfunkverbindung (…) erlauben	Deaktiviert	Vermeidung von Missbrauch
Ändern von Einstellungen für Mobilfunkverbindungen erlauben (auch für Apps)	Deaktiviert	Vermeidung von Missbrauch

16 Drucken

Soll von den Geräten aus gedruckt werden, müssen verschiedene Bedingungen erfüllt sein:

- Der Drucker muss im selben Netz sein, wie die Tablets, von denen aus gedruckt werden soll.
- Die App muss das Drucken unterstützen.
- *iOS*: Der Drucker muss *AirPrint* unterstützen (https://support.apple.com/de-de/HT201311).

Wir empfehlen die Aufnahme von Druckern in das MDM-Netz gemäß Kapitel 6.

17 Präsentation

Um Inhalte von Tablets aus zu präsentieren, können Sie die Bildschirmausgabe auf einen Beamer spiegeln. Dies kann über einen Hardware-Adapter geschehen, der das Signal aus dem Anschluss des Ipads für HDMI- oder VGA-Anschlüsse übersetzt. Vorteil ist, dass Sie unabhängig von der WLAN-Qualität sind und das Gerät auch mal schnell an einen externen Monitor anschließen können. Ein wesentlicher Nachteil ist die Verwendung eines Kabels, das die Vorteile des mobilen Geräts während der Präsentation einschränkt.

Die kabellose Präsentation dürfte daher mehr Zuspruch erhalten. Hierfür müssen die Geräte kompatibel sein, da es leider keinen einheitlichen Standard für die kabellose Präsentation gibt. Apple hat hierfür einen eigenen Standard entwickelt.

Die Geräte zur kabellosen Präsentation müssen im gleichen WLAN sein, wie die Ipads, von denen aus präsentiert werden soll. Wie empfehlen die Aufnahme der Geräte in das MDM-Netz gemäß Kapitel 6.

In unserer allgemeinen Anleitung zu Tablets in allen paedMLs (vgl. https://www.lmz-bw.de/netzwerkloesung/fachwissen/tablets-in-der-schule/) werden Technologien zur Präsentation beschrieben.

18 Bring Your Own Device

Geräte, die von Schüler*innen selbst verwaltet werden, sollten im Gästenetz arbeiten. Insbesondere sei hier auf die Möglichkeiten der Radius-Authentifizierung und der Nutzung von Captive Portal in der paedML GS und Linux hingewiesen (siehe https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#howtos).

19 Caching Server

Bei der Verwaltung von Ipads per MDM werden große Datenmengen von Apple-Servern auf die Ipads übertragen. Zum einen sollte hier überlegt werden, wann etwa Tablets neu aufgesetzt, also per MDM auf Werkseinstellungen zurückgesetzt werden. Auch sollte das Ausspielen von Apps auf den Schulalltag abgestimmt werden.

Viele Schulen setzen zudem Apple-PCs, im Folgenden Mac genannt, als sogenannte Caching Server ein. Diese speichern Inhalte bei der ersten Übertragung auf ein Ipad. Fragen nun weitere Ipads dieselben Inhalte an, so werden diese nicht mehr aus dem Internet heruntergeladen, sondern aus dem Speicher des Caching-Servers. Dies gilt für iOS-Updates, für Apps, aber auch für Profile bei geteilten Ipads. Allerdings werden nicht alle Inhalte durch den Caching-Server gespeichert.

Im Folgenden wird die Einrichtung und der Betrieb eines aktuellen Mac Mini (MacOS Big Sur 11.2.2) als Caching-Server im Netz MDM beschrieben.

19.1 Aufnahme des Mac in der pfSense

Der Caching-Server muss im selben Netz betrieben werden, wie die Ipads, die über den Caching-Server mit Inhalten bespielt werden sollen.

Die Anleitung beschreibt daher im Folgenden den Betrieb des Caching-Servers im MDM-Netz.

Wir empfehlen, den Caching Server gemäß Kapitel 6.1.2 in der pfSense aufzunehmen. Damit bekommt der Caching Server eine feste IP-Adresse im Netz MDM zugewiesen. Im Beispiel wird die IP-Adresse *172.20.0.10* vergeben.

Überprüfen Sie den Erfolg der Aufnahme ins MDM-Netz, indem Sie auf dem Mac in den Systemeinstellungen unter Verbindungen überprüfen, ob die IP-Adresse zugewiesen wird.

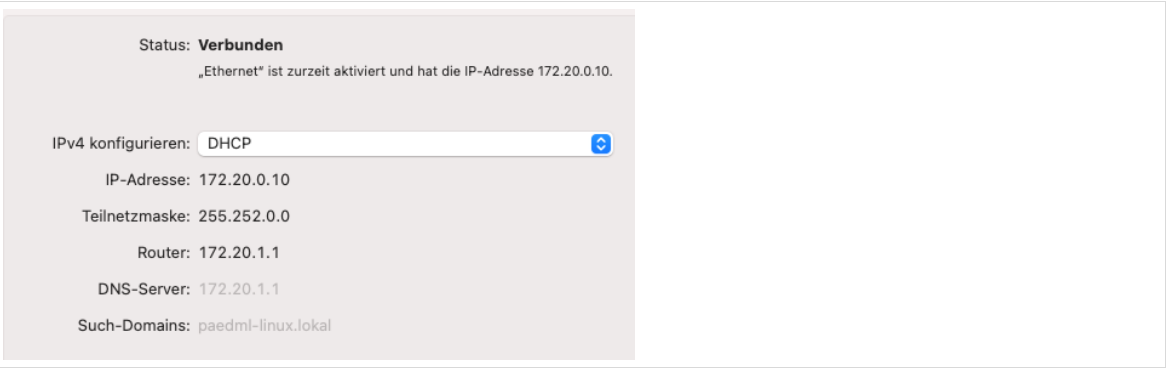

Abb. 122: Kontrolle MDM-Netz

19.2 Aktivierung des Caching Servers.

Öffnen Sie auf dem Mac die *Systemeinstellungen*. Gehen Sie zu *Freigaben* und klicken Sie dort auf *Inhaltscaching*. Das Teilen der Internetleitung über USB-Kabel ist dann sinnvoll, wenn die Ipads über USB-Kabel synchronisiert werden können. Dies ist bei einigen Aufbewahrungssystem möglich.

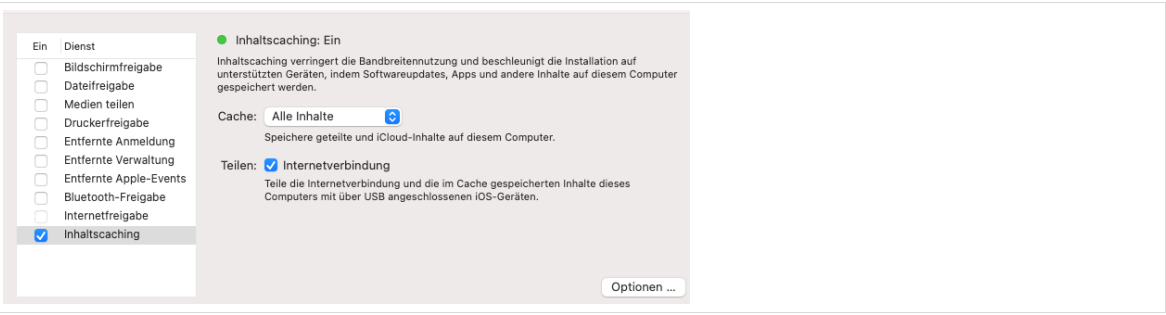

Abb. 123: Inhaltscaching

Überprüfen Sie, ob das Caching funktioniert, indem Sie während des ersten Ausrollens von zum Beispiel einem iOS-Update auf Optionen klicken und dort die Größe des Caching-Speichers beobachten. Im Beispiel wurde die Größe des Cache auf 20 GB begrenzt

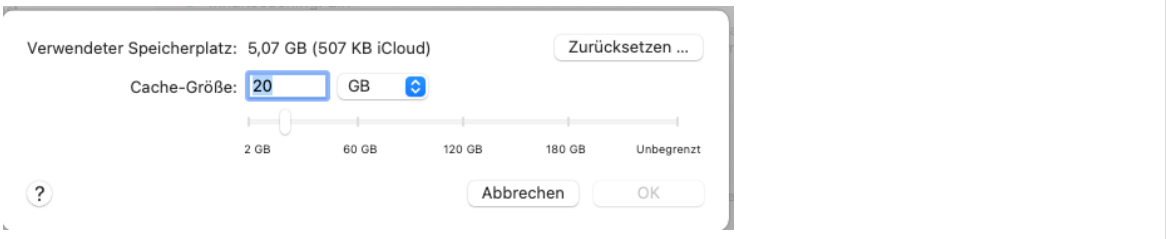

Abb. 124: Caching-Speicher

19.3 Aktivierung von Tethered Caching im MDM

In Jamf School muss für einzelne Gerätegruppen Tethered Caching aktiviert werden. Navigieren Sie dazu in jamf School in den Bereich *Organisation* und dort zu *Einstellungen | Tethered Caching*.

Wählen Sie die Gerätegruppen aus, für die der Caching Server arbeiten soll und markieren Sie die Haken für das Betriebssystem bzw. für Apps.

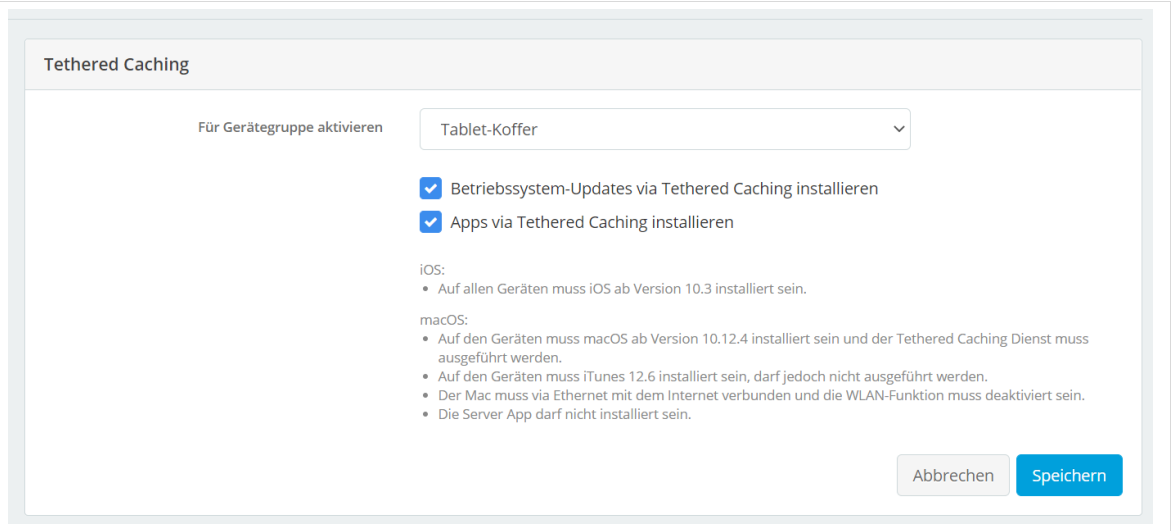

Abb. 125: Tethered Caching in Jamf School

20 Anhang

20.1 Dateiablage auf dem paedML Server

Öffnen Sie die App „Dateien“, den Dateimanager von iOS.

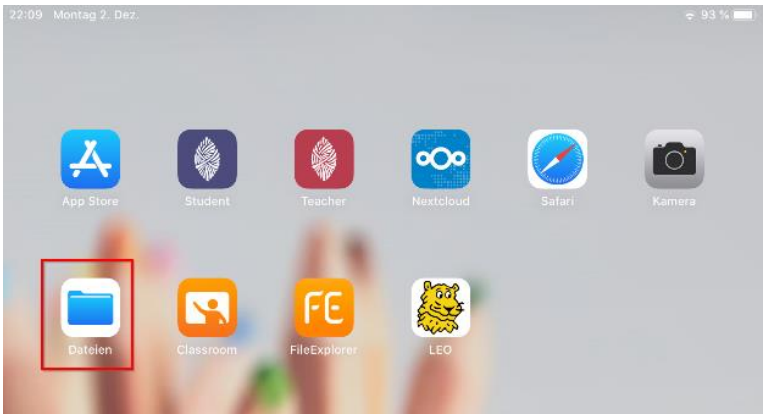

Abb. 126: Dateimanager öffnen

Tippen Sie auf das Symbol mit den drei Punkten und wählen Sie im nächsten Dialogfenster „*Mit Server verbinden*“.

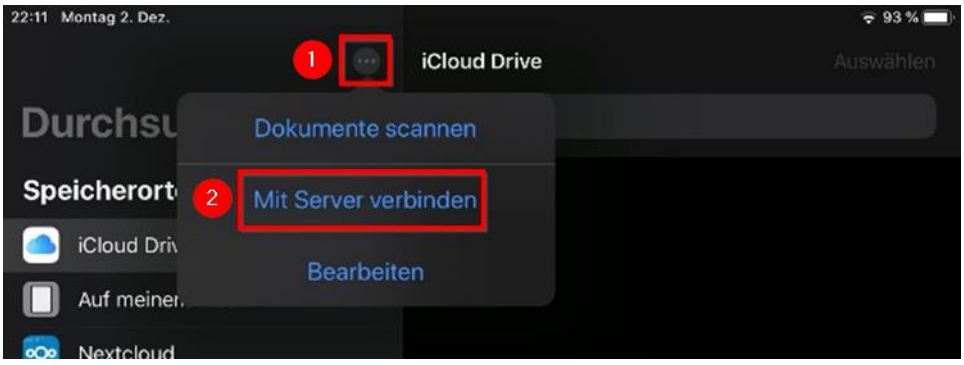

Abb. 127: Dateimanager: Mit Server verbinden

Im nächsten Dialogfenster geben Sie bei „Server“ *10.1.0.1/Benutzernamen* der paedML ein.

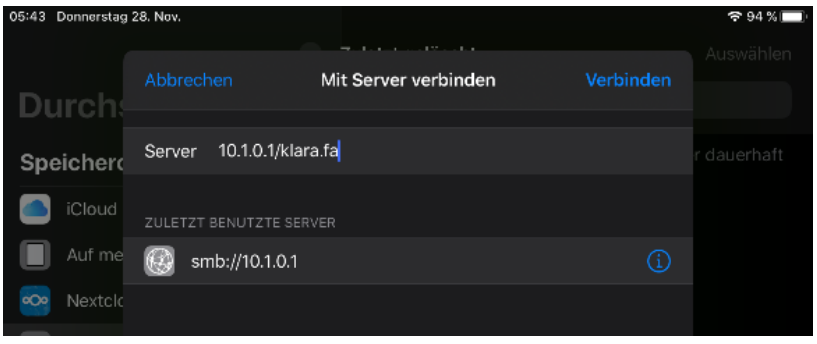

Abb. 128: Dateimanager: Verbindungsnamen eingeben

Markieren Sie „*Registrierter Benutzer*“ und hinterlegen Sie dort die Zugangsdaten aus der paedML.

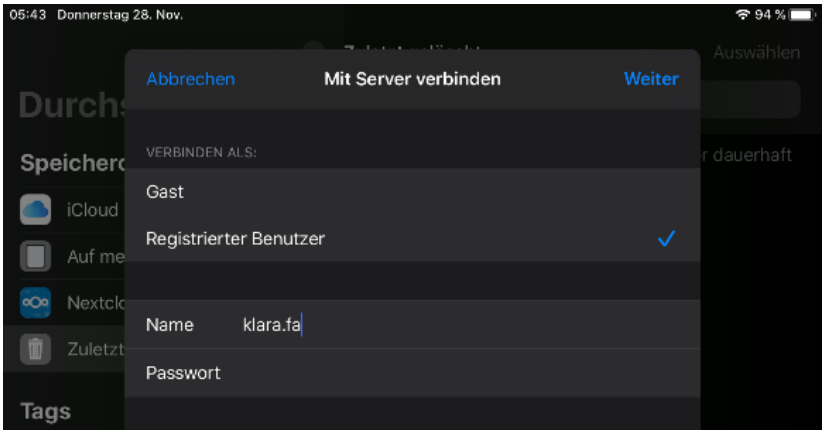

Abb. 129: Dateimanager: Benutzerdaten aus der paedML eingeben

Nun werden Ihnen die unter dem Benutzernamen der paedML gespeicherten Ordner angezeigt.

Abb. 130: Dateimanager: Ordner des paedML Benutzers

Soll eine Datei in diesem Bereich gespeichert werden geschieht dies in der Regel innerhalb der verwendeten App. Im Folgenden wird das Vorgehen exemplarisch anhand der iOS-internen App *Kamera* beschrieben.

Öffnen Sie dazu die Kamera-App und dort das Foto, das auf dem Server gespeichert werden soll. Wählen Sie das „Teilen-Symbol“.

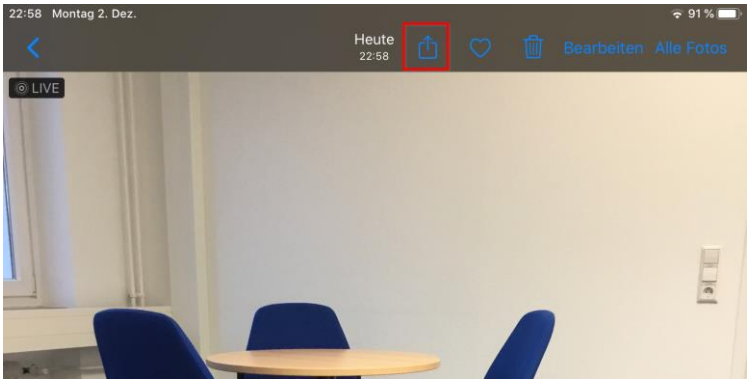

Abb. 131: Kamera-App: Bilddatei speichern

Navigieren Sie zu *in Dateien sichern*.

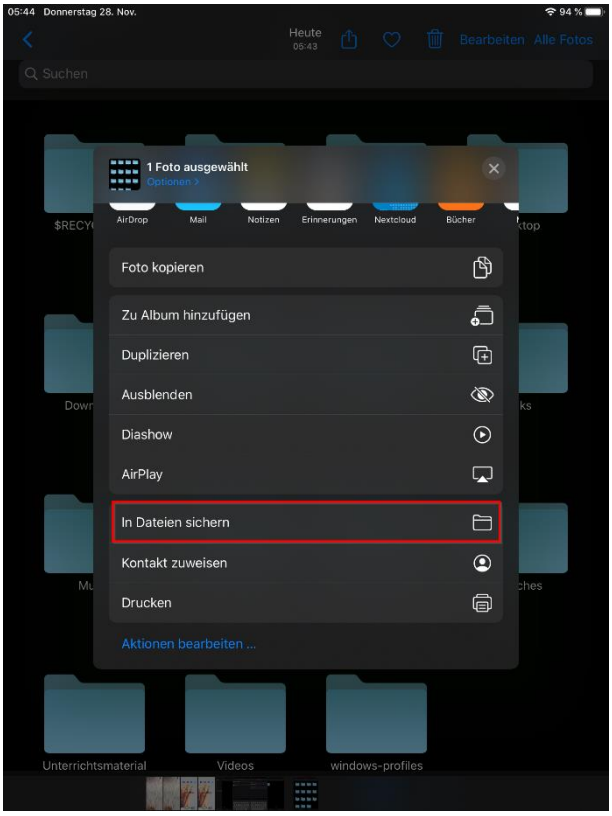

Abb. 132: Kamera-App: Bilddatei speichern

Wählen Sie dort die Server-Verbindung und einen geeigneten Speicherort.

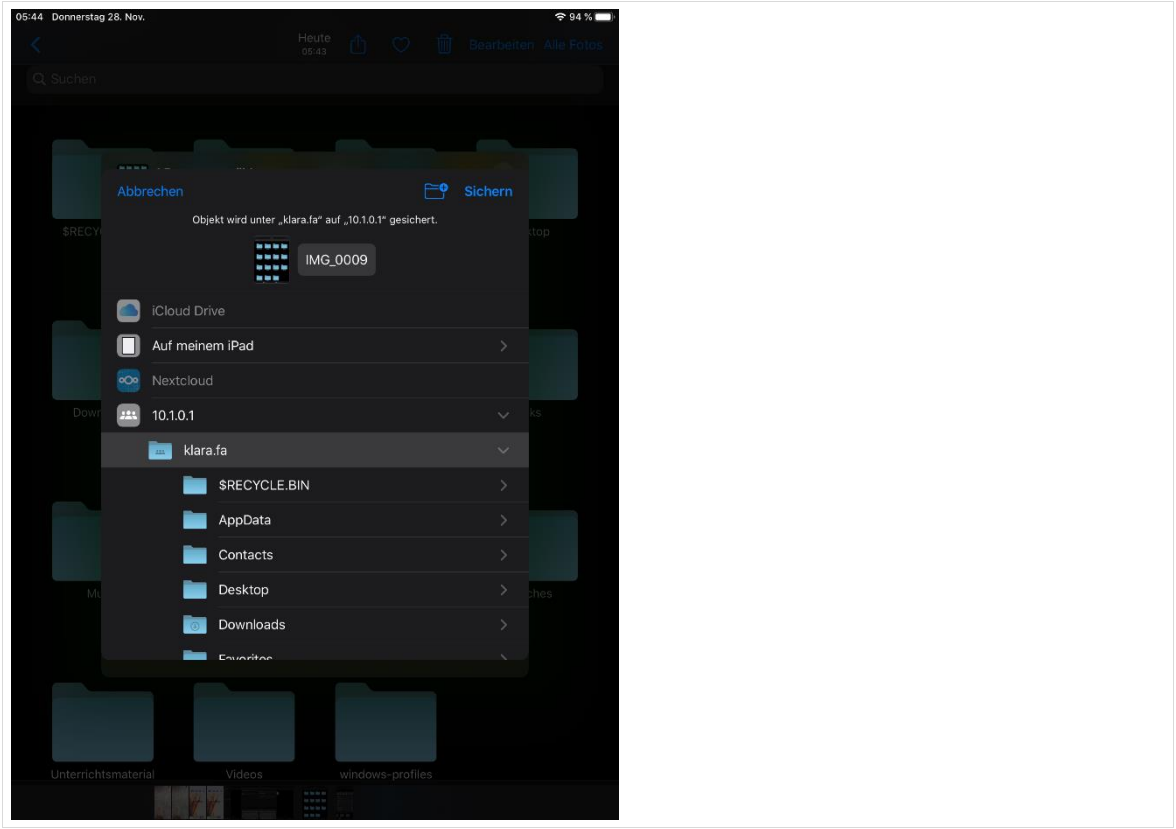

Abb. 133: Kamera-App: Bilddatei speichern

Verbindung zur Freigabe trennen

Nach dem Unterricht sollte die Freigabe zu den individuellen Home-Laufwerken getrennt werden. Klicken Sie dazu im Dateimanager auf das „Auswerfen“-Symbol. Nun können andere Benutzer nicht mehr auf die Freigabe zugreifen.

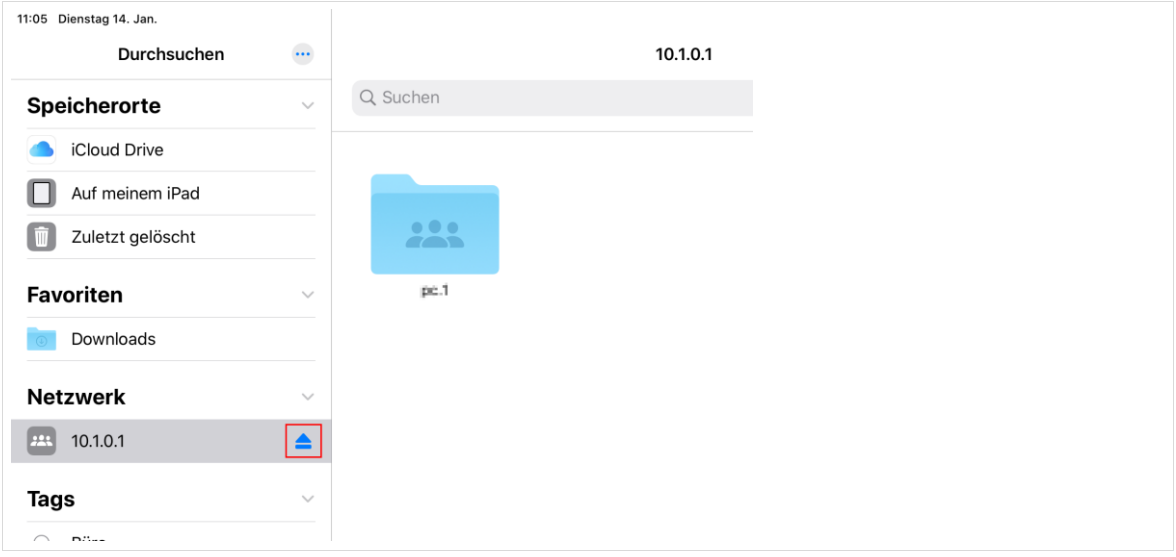

Abb. 134: Verbindung trennen

Die Freigabe bleibt solange bestehen, bis das Gerät zurückgesetzt wird oder die Verbindung zu dieser Freigabe getrennt wird. Andere Benutzer können dadurch auf Ihr Homeverzeichnis zugreifen und Ihre Daten einsehen.

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart

paedML L

LMZ Landesmedienzentrum Baden-Württemberg