

Beratung und Support
Technische Plattform
Support-Netz-Portal



paedML® – stabil und zuverlässig vernetzen

Anleitung

Tablets in der paedML Linux – Schwerpunkt Windows

Stand 04.12.2015

paedML® Linux

Version: 6.0

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111
70190 Stuttgart

Autoren

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

Endredaktion

Doreen Edel

Bildnachweis Titelbilder:

Thinkstock

Weitere Informationen

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

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2015

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen, sind nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1.	Abgrenzungen.....	5
1.1	Laptops, Convertibles, ... mit Windows	5
1.2	Windows-Tablets.....	5
1.3	Alternativen zu Windows.....	6
2.	Offene Punkte zum Tablet-Einsatz in der Schule.....	7
3.	Integrationsmöglichkeiten	10
3.1	Integration mobiler Endgeräte in das Gäste-Netz.....	11
3.2	Integration in das pädagogische Netz	11
3.2.1	Teil-Integration mobiler Endgeräte in das pädagogische Netz.....	12
3.2.2	Voll-Integration mobiler Endgeräte in das pädagogische Netz.....	13
4.	(Teil-) Integration von Windows-Tablets.....	14
4.1	Client-Registrierung in der paedML	15
4.2	Betrieb von Geräten MIT opsi-client-agent	15
4.2.1	Aufspielen des opsi-client-agents	15
4.2.2	Verwaltung des Rechners über opsi	17
4.3	Optional: Betrieb von Geräten OHNE opsi-client-agent	18
4.4	Deaktivieren der Windows-Firewall.....	19
5.	Voll-Integration am Beispiel eines Surface 3 Pro	21
5.1	Manuelle Client-Registrierung in der paedML	21
5.2	Gerät vorbereiten	21
5.3	Manueller Netzwerkboot	23
5.4	Überprüfen von opsi-Einstellungen bei UEFI-Geräten.....	24
5.5	Treiber bereitstellen	24
5.6	Clients ausrollen und damit arbeiten.....	27
5.6.1	Besonderheiten bei der Partitionierung	27
5.6.2	Netzwerk-Konfiguration.....	28
6.	Alternativen zu Windows	29
6.1	Einbinden von Android-Geräten.....	30
6.1.1	Grenzen der Integration in die paedML	30
6.1.2	Einstellungen für den Internet-Zugriff.....	31
6.1.3	Zugriff auf das pädagogische Netz	32
6.2	iOS	34
6.2.1	Grenzen der Integration in die paedML	34
6.2.2	Einstellungen für den Internet-Zugriff.....	34
6.2.3	Zugriff auf das pädagogische Netz	37

Vorwort

Die Entwicklung in der IT schreitet stetig voran. Die *paedML* ist ein System, das seit der ersten Veröffentlichung im Jahre 2001 im Kontext kabelgebundener Netzwerke entwickelt wurde. Das Endgerät dieser Zeit ist der Desktop-PC, der mit Tastatur, Maus und Monitor ausgestattet die PC-Räume der Schulen bestimmt hat. In der Zwischenzeit hat sich einiges getan. Sowohl WLAN als auch mobile Endgeräte wie Laptops, Tablets und teilweise auch Mobiltelefone gehören zum Alltag der Schulen.

Mit dem folgenden Dokument sollen Konzepte für die Integration von Tablets in die *paedML Linux* aufgezeigt werden.

Dieses Dokument war zunächst Bestandteil des WLAN-Konzeptes der *paedML Linux*. Es hat sich aber gezeigt, dass die beiden Themen (WLAN und mobile Endgeräte) gesondert betrachtet werden sollten. Aus der Historie dieser Anleitung bedingt, werden konzeptionelle Überlegungen in beiden Dokumentationen ausgeführt.

Die Anleitung zur Einrichtung von WLAN in der [paedML Linux](#)¹ beschreibt den Betrieb von Access-Points – sowohl im Pädagogischen Netz, als auch im Gästernetz. Es wird dringend empfohlen, diese Anleitung unter den Gesichtspunkten einer funktionierenden WLAN-Ausleuchtung zu berücksichtigen!

Im vorliegenden Dokument liegt der Fokus auf schuleigenen Geräten im pädagogischen Netz.



Es wird ausdrücklich empfohlen, dass Sie sich vor der Beschaffung von Geräten über Teststellungen durch Ihren Hardwarehändler vergewissern, dass die Geräte mit der *paedML Linux* betrieben werden können!



Wir freuen uns immer über eine Rückmeldung zu unseren Produkten.

Wenn Sie konkrete Verbesserungsvorschläge zu dieser Anleitung oder zu technischen Rahmenbedingungen – insbesondere im Zusammenhang mit der Integration mobiler Endgeräte – haben, nehmen Sie bitte Kontakt mit unserer Hotline auf.



Wir bitten Sie um Verständnis, dass unsere Mitarbeiter keinen Support für die Integration und Verwaltung von Endgeräten bieten können.

Dies gilt insbesondere die Verwaltung und Bedienung von nicht durch die *paedML Linux* unterstützten Betriebssystemen.

¹ Vgl. <http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/howtos/wlan-in-der-paedmlr-linux-60.html>

1. Abgrenzungen

Ein Dokument mit Abgrenzungen zu beginnen, mag dem geneigten Leser merkwürdig erscheinen, dennoch ist es unabdingbar zu beschreiben, was Gegenstand dieser Anleitung ist und was nicht.

1.1 Laptops, Convertibles, ... mit Windows

Diese Anleitung behandelt keine Endgeräte, die über eine Netzwerkkarte **und** über einen WLAN-Netzadapter in die paedML eingebunden werden. Hierzu gehören beispielsweise Laptops, Convertibles² (also Geräte, die als Tablet oder als Laptop benutzt werden können) oder ähnliche Endgeräte – mit und ohne Dockingstation.

Geräte mit zwei Netzwerkkarten können – wie im Administratorhandbuch beschrieben – ohne Probleme in die paedML aufgenommen und mit Software versorgt werden.

1.2 Windows-Tablets

Viele *Windows*-Tablets können voll in die *paedML* integriert und mit Betriebssystem, bzw. Software versorgt werden.

Manche dieser Geräte können jedoch nur mit einem erhöhten Aufwand über opsi verwaltet werden.

Bei *Windows*-Tablets gilt es generell folgende Punkte zu beachten:

- Da Tablets in der Regel nicht über eine Netzwerkkarte für Kabelnetze verfügen, werden sie häufig über einen USB-Netzwerkadapter mit einem Kabelnetz verbunden. Dies ist immer dann sinnvoll, wenn größere Datenmengen an ein oder mehrere Geräte gesendet werden sollen, also zum Beispiel bei der Installation des Betriebssystems.
Die Personalisierung (Computernamen im Netzwerk) der Clients wird über die MAC-Adresse des Netzadapters realisiert. Bei der Vollintegration³ in die *paedML* sollte daher darauf geachtet werden, dass die Geräte **IMMER DEN GLEICHEN USB-NETZWERKADAPTER** erhalten, wenn die Installation über opsi erfolgt. Als dienlich erweist sich eine Durchnummerierung der Geräte und Adapter mit einem Label-Drucker.
- Im Gegensatz zu Desktop-PCs booten viele Tablets nicht zuverlässig über PXE – also über das Kabel-Netzwerk, über das die Installation von Windows (und weiterer Software) auf den Geräten ausgeführt wird.
- Die Erfahrungen haben gezeigt, dass eine Aktualisierung der BIOS- (bzw. UEFI-)Versionen notwendig sein kann, um beispielsweise PXE-Funktionen auf den Geräten nachzurüsten. Es wird daher dringend empfohlen, die Firmware jedes Gerätes zu aktualisieren, bevor die Installation durchgeführt wird.

² https://de.wikipedia.org/wiki/Convertible_%28Computer%29

³ Voll- und Teil-integration vgl. Kapitel 3, ab Seite 9.

- Manche Geräte lassen sich über bestimmte Tastenkombinationen (z.B. gleichzeitiges Drücken der Lautstärke-Taste nach unten beim Einschaltprozess (Surface2)) dazu bewegen, über PXE zu starten. Diese Tastenkombination muss aber jedes Mal ausgeführt werden, wenn das Gerät neu über das Netzwerk starten soll - bei einer Neuinstallation mit opsi also mindestens zwei Mal (beim ersten Start wird partitioniert, beim zweiten Start installiert).

Wenn Sie sich nun vorstellen, dies bei einem Klassensatz von dreißig Geräten durchzuführen, dann werden opsi-Automatismen ad absurdum geführt.

- Geräte, die weder über PXE-Boot, noch über eine Kabelverbindung verfügen, können – nach Aufnahme in die *paedML*-Domäne – mit opsi-Clientpaketen versorgt werden. Imaging mit der *paedML* ist bei diesen Geräten nicht möglich. Software kann jedoch – vorausgesetzt das WLAN ist leistungstark – über opsi ausgespielt werden.

Diese Geräte müssen über ein anderes Verfahren gesichert und verwaltet werden, zum Beispiel über die Windows-System-Wiederherstellung oder über Imaging-Software, mit der ein Abbild der Ausgangsinstallation gemacht wird.

1.3 Alternativen zu Windows

Alternative Betriebssysteme wie *Android* oder *iOS* haben sich im Consumer-Segment eine große Anhängerschaft erarbeitet. Passionierte Anwender von *Android*- oder *Apple*-Produkten wünschen sich eine Integration dieser Geräte in die *paedML*. Leider ist dies nicht ohne weiteres umsetzbar. Gründe dafür sind:

- Die Geräte von *Google* (*Android*) und *Apple* benötigen im Auslieferungszustand ein Benutzerkonto, mit dem das Gerät betrieben werden kann. Ohne dieses Benutzerkonto können die Geräte in der Regel nicht bedient werden. Ein Ausspielen von Programmen ist daher nicht möglich.
- Die Geräte können nicht ohne Aufwand in der *paedML*-Domäne betrieben werden. Dies bedeutet, dass eine Anmeldung mit einem *paedML*-Konto nicht erfolgen kann.
- Um diese Restriktion zu umgehen, kann mit einem sogenannten Mobile Device Management (MDM) gearbeitet werden. Zuverlässige MDM-Lösungen können teuer sein.

Derzeit gibt es lediglich die Möglichkeit *Windows*-Tablets vollwertig in die *paedML* zu integrieren, später in dieser Anleitung soll jedoch aufgezeigt werden, wie Sie dennoch mit einem *Android* oder *iOS*-Gerät im *paedML*-Netzwerk arbeiten können.

2. Offene Punkte zum Tablet-Einsatz in der Schule

Den Vorzügen des unkomplizierten Tablet-Einsatzes im Privaten stehen Anforderungen im schulischen Kontext gegenüber. In diesem Abschnitt sollen ein paar Fragestellungen skizziert werden, zu denen keine allgemeingültigen Antworten gegeben werden. Stattdessen sollen die skizzierten Themen zum Nachdenken anregen:

1. Hardware und Beschaffung

1.1. Heterogenität der Geräte

- Die Unterschiede zwischen einem Galaxy Tab 3 und einem Surface 3 sind immens – Hardware muss auf den Einsatz hin überprüft werden. Was soll mein Tablet leisten können? (Siehe: 4. Pädagogische Anforderungen)
- Das Betriebssystem Android läuft beispielsweise auf den unterschiedlichsten Geräten. Vom 80 Euro 7-Zoll Tablet bis zum 12-Zoll Highend-Gadget jenseits der 500 Euro, gibt es unter Android aber auch die Software, die Sie einsetzen wollen und wie kommt diese auf Ihre Endgeräte?

Zusätzlich erschwerend kommt die Tatsache hinzu, dass die Produktlebenszeit der Geräte sehr kurz ist. Wenn heute ein Klassensatz mit Geräten beschafft wird, so stellt sich die Frage, ob diese Geräte in zwei Jahren immer noch verfügbar sind. Im Gegensatz zu Desktop-PCs lassen sich defekte Bauteile nicht einfach ersetzen. Stattdessen müssen die Geräte in der Regel vollständig ausgetauscht werden.

1.2. **Kosten** von leistungsfähigen Tablets (verglichen mit Computerarbeitsplätzen).

1.3. **Defekte Hardware lässt sich häufig nicht (einfach) tauschen**

- Ein defekter Akku kommt nicht selten einem „wirtschaftlichen Totalschaden“ gleich, da sich viele Geräte nicht öffnen lassen und der Akku fest verbaut ist. Das Gleiche gilt für ein defektes Display. Firmen, die sich auf den Austausch von defekter Hardware spezialisiert haben, können Reparaturen an Tablets durchführen, nicht selten sind die Preise hierfür aber in Dimensionen, in denen auch über eine Neuanschaffung nachgedacht werden kann. Dies gilt insbesondere für ältere Geräte, die intensiv genutzt wurden.
- Das Rundum-Sorglos-Paket mit Versicherung gegen jegliche Geräteschaden könnte im schulischen Umfeld Sinn ergeben und sollte überdacht werden.
- Ebenso sollte in Erwägung gezogen werden einen Wartungsvertrag mit dem Lieferanten abzuschließen.

1.4. **Augen auf beim Hardwarekauf**

- Vor der Beschaffung von Geräten sollte auf jeden Fall über eine Teststellung sichergestellt werden, dass die Geräte auch den Anforderungen entsprechen. Sind alle Funktionen verfügbar, die Sie später im Unterricht nutzen wollen? Lassen sich die Geräte reibungslos in Ihr Schulnetz integrieren?
- Vermeiden Sie den Kauf von Hardware, die später nicht – oder nur sehr aufwändig – in Ihrem Schulnetz betrieben werden kann.

2. Infrastruktur

2.1. Ein **leistungsfähiges WLAN muss vorhanden sein** – dies erfordert in der Regel eine strukturierte Verkabelung des Schulgebäudes – **hohe Investitionskosten!**

2.2. **Logistische Rahmenbedingungen**

- **Ladestationen**, die auch von den Besitzern regelmäßig genutzt werden müssen
 - **Verfügbarkeit von Steckdosen**, bei Dauernutzung in den Klassenräumen in ausreichender Anzahl
 - **Softwareverteilung über Switches** (nicht WLAN)
 - **Peripheriegeräte** (externe Netzwerkkarte, Dockingstationen, Eingabestift) **müssen mit dem Endgerät aufbewahrt** werden. Wenn ein Tablet über ein Netzkabel an das Schulnetz angeschlossen werden soll (zum Beispiel für das Ausspielen von Software), dann ist es zwingend notwendig, dass das Gerät *immer mit dem gleichen Netzwerkkabel* betrieben wird⁴. Die MAC-Adresse⁵ des Netzwerkkabels ist wichtig für das Erkennen von Geräten durch die paedML.
- 2.3. **Mobile Device Management** – Das Management von (Nicht-Windows-)Geräten bedingt den Einsatz von spezieller Software, über die diese Geräte verwaltet werden.

3. Handhabung der Geräte

- 3.1. Tablets haben eine andere **Usability** (Bedienbarkeit) als „klassische“ Computer.
- Es fehlen in der Regel Eingabegeräte wie Maus und Tastatur, die die Bedienung der Tablets erleichtern und die Geräte auch für den „produktiven Einsatz“ nutzbar machen. Dafür kommt der Anwender auch ohne eine Mausbedienung aus. Gesten und das Wischen über einen berührungsempfindlichen Monitor ersetzen Maus und Tastatur.
 - Arbeiten verändert sich dadurch. Kinder und Jugendliche wachsen mit anderen Bedienkonzepten auf als Erwachsene, die seit Jahren an Computer gewöhnt sind. Ist dies nun ein Vor- oder Nachteil?
 - Ist es zum Beispiel sinnvoll mit einem Tablet die Erstellung von Serienbriefen zu erlernen?
- 3.2. **Mobilität** ist nicht immer ein Vorteil (Stichworte: Schaden durch Herunterfallen, Diebstahl).
- 3.3. **Individuelle Geräte versus Domänenbenutzer**
- Android- und iOS-Tablets sind nicht dafür konzipiert worden, dass Sie im Unterricht von verschiedenen Schülern (nacheinander) bedient werden. Stichworte hierzu:
 - Daten werden häufig bei Cloud-Anbietern abgelegt. Wo stehen die Server und wie sind die Datenschutzbestimmungen in diesem Land?
 - Protokollierung der Nutzung durch eine händisch zu führende Benutzerliste.
 - Wer hat wann welches Gerät bekommen?
 - Wurde das Gerät in einwandfreiem Zustand zurückgegeben?
 - Es wurden 20 Tablets ausgeteilt, nur 19 sind zurückgekommen, wo ist das Gerät abgeblieben?
 - Wer ist verantwortlich bei Missbrauch und Beschädigungen?
 - Datenspeicherung von Benutzerdaten (Wie verbinde ich mich mit meinem Home-Laufwerk?)

⁴ Der Einsatz einer Etikettier-Maschine ist hierbei sinnvoll. Beschriften Sie sowohl das Tablet als auch den zugehörigen Netzadapter mit einer eindeutigen Kennung.

⁵ Vgl. <https://de.wikipedia.org/wiki/MAC-Adresse>

3.4. Besonderheiten bei Nicht-Windows-Geräten:

- Es bedarf Konzepte für das Austeilen und Einsammeln von Dateien durch den Lehrer.
- Es bedarf Konzepte für das Abbilden von Tauschlaufwerken für kollaborative Projekte.

3.5. **Einrichtung lokaler Benutzerkonten**

- Wenn (Windows-)Geräte auch außerhalb einer Domäne betrieben werden sollen (beispielsweise zu Hause), benötigen Schüler ein lokales Benutzerkonto, um auf das Gerät zugreifen zu können.

4. **Pädagogische Anforderungen**

- 4.1. Wie sollen die Geräte genutzt werden?
- 4.2. Mit welcher Software soll gearbeitet werden?
- 4.3. Die Bedienung der Geräte bzw. der eingesetzten Software muss erlernt werden – nicht nur von den Schülern sondern gerade auch von den Unterrichtenden!
- 4.4. Wie kann verhindert werden, dass die Technologie ablenkt (Anpassung des Unterrichts an den Geräteeinsatz durch Übungsaufgaben, ...).
- 4.5. **Austeilen von Unterrichtsmaterialien** – Insbesondere beim intensiven Einsatz von Filmen im Unterricht, kann es Sinn ergeben das Unterrichtsmaterial lokal auf den Endgeräten abzulegen, um die Bandbreite des WLANs nicht übermäßig auszulasten.

3. Integrationsmöglichkeiten

Dieses Kapitel ist eine gekürzte Version des gleichnamigen Abschnitts aus der WLAN-Dokumentation, die Sie unter <http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/howtos/wlan-in-der-paedmlr-linux-60.html> einsehen können.

Die *paedML Linux* wird mit zwei vorkonfigurierten Netzwerken ausgeliefert, in die Rechner aufgenommen werden können.

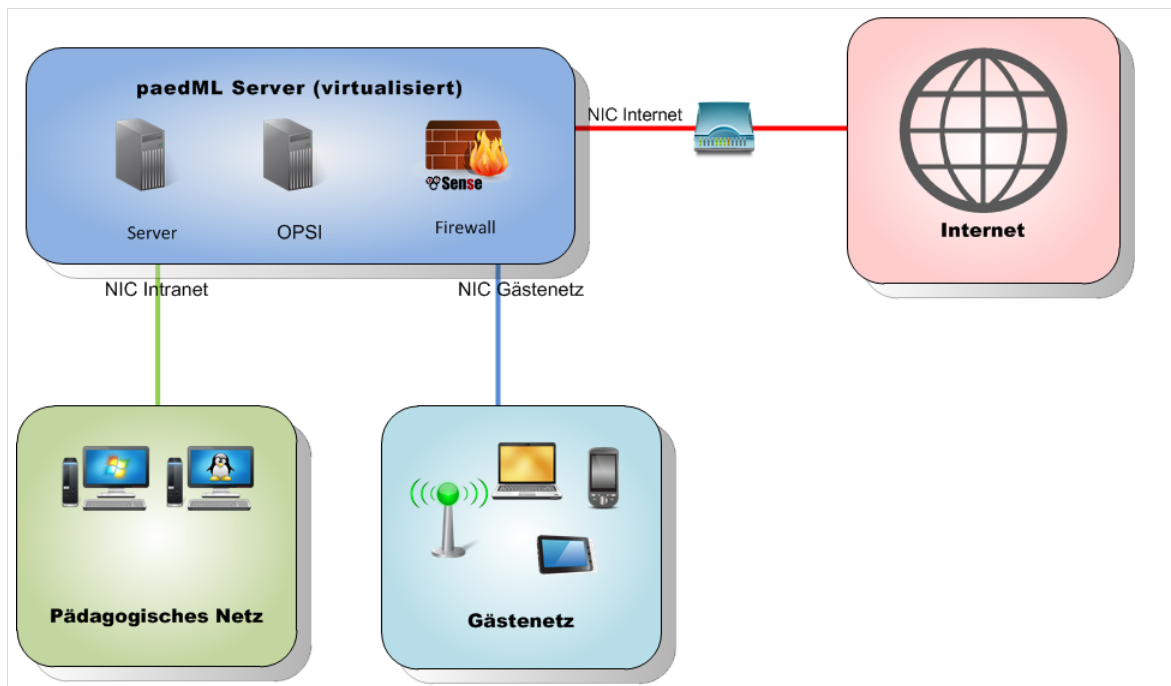


Abb. 1: Schematischer Aufbau der paedML Linux-Netze

Über das *Gästenetz* kann nur eine Internetverbindung via HTTP aufgebaut werden. Der Internetzugriff wird (über eine Anmeldung am Schulproxy, der auf dem Server läuft⁶) protokolliert und – mit demselben Filter, der im pädagogischen Netz aktiv ist – gefiltert.

Das *Pädagogische Netz* ist das Netz, in dem unterrichtet wird. Hier finden Sie die schulischen Ressourcen wie Home-Verzeichnisse oder Tauschlaufwerke.

Für die Integration mobiler Geräte sind drei Szenarien denkbar, die im Folgenden beschrieben werden.

⁶ Jeder Benutzer des Schulnetzes muss sich mit den Zugangsdaten am Schulnetz anmelden. Die Anmeldung an einem Rechner in der Domäne ermöglicht es ohne weitere Authentifikation im Internet zu surfen. Benutzer von Rechnern im Gästernetz müssen sich zunächst mit Ihren Schulzugangsdaten am Proxy-Server authentifizieren, bevor Sie einen Internetzugriff bekommen.

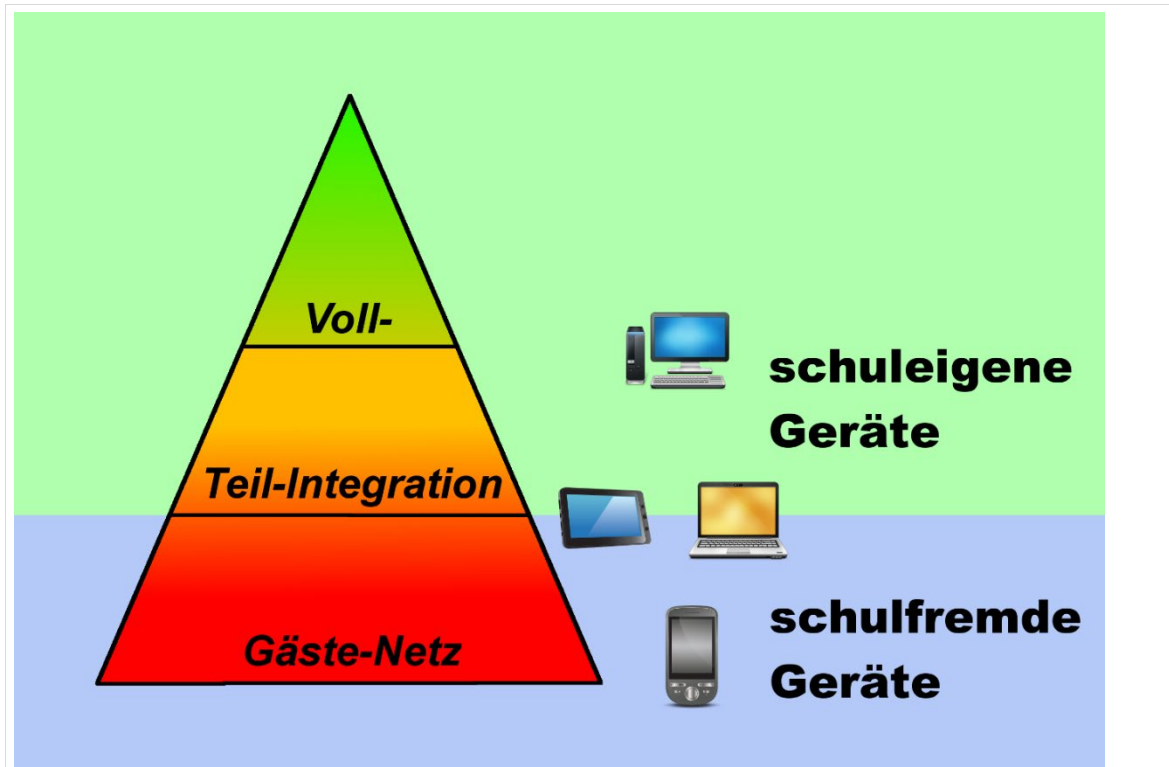


Abb. 2: Integration mobiler Endgeräte in die paedML Linux

3.1 Integration mobiler Endgeräte in das Gäste-Netz

Schulfremde Geräte sollten ausschließlich in das Gästernetz aufgenommen werden, um Risiken (Haftungsfragen und Sicherheitsaspekte) zu minimieren.

Um Geräte in das Gästernetz einzubinden, benötigen Sie Access-Points, die über das Netzwerk „Gäste“ an die *pfSense*-Firewall angeschlossen werden.

Die Einbindung von schuleigenen Geräten in das Gästernetz ergibt keinen Sinn, da dort zentrale pädagogische Funktionen und Netzwerkressourcen nicht zur Verfügung stehen. Dies gilt auch für schuleigene Tablets!

Benutzer des Gästernetzes haben die Möglichkeit – nach einer Authentifizierung am Proxy des Schulservers – auf das Internet zuzugreifen. Im Auslieferungszustand der *paedML Linux* können Benutzer im Gästernetz nur im Internet surfen. Alle anderen Protokolle sind deaktiviert.

Ein Zugriff auf das Schulnetz und die darin befindlichen Daten ist nur über eine *openVPN*-Verbindung möglich.

3.2 Integration in das pädagogische Netz

Schuleigene Geräte werden am sinnvollsten in das pädagogische Netz eingebunden, um auf schulische Ressourcen zugreifen zu können.

Die folgende Tabelle gibt einen Überblick darüber, was derzeit in der *paedML Linux* möglich ist.

Betriebssystem	Windows Gerät	Windows Gerät	Andere
Funktion	(Kabelnetz)	(drahtlos)	
Verteilung Betriebssystem	✓	✗	✗
Verteilung Software	✓	✓	✗
Verteilung von Sicherheitseinstellungen ⁷	✓	✓	✗
Zugriff auf das pädagogische Netz ⁸	✓	✓	✓
Unterrichtssteuerung ⁹	✓	✓	✗

Tabelle 1: Übersicht über Funktionen der paedML Linux

3.2.1 Teil-Integration mobiler Endgeräte in das pädagogische Netz

Bei der Teil-Integration handelt es sich um die **Einbindung schuleigener Geräte in das pädagogische Netzwerk, wobei hier nicht alle Funktionen der paedML verfügbar sind.**

Es sind verschiedene Szenarien denkbar:

- Integration von Nicht-*Windows*-Geräten – Imaging und Softwareverteilung über Fremdsoftware („Mobile Device Management“) bzw. manuell je Gerät. Ein Beispiel hierfür wäre der Einsatz von iPads.
- Integration von *Windows*-Tablets, die nicht über *opsi* installiert werden.
 - kein Imaging via *opsi*
 - Softwareverteilung nach dem Ausspielen von *opsi*-Client möglich. Das bedeutet, dass Sie erst *opsi* installieren müssen und anschließend Software auf die Geräte verteilt werden kann.
 - Wiederherstellung der Geräte über die Recovery-Prozeduren des Herstellers, beziehungsweise über Software von Drittanbietern.

Folgende Einschränkungen sind im Falle einer nicht vollständigen Integration möglich (abhängig von der Konfiguration der Geräte müssen nicht alle Einschränkungen zutreffen):

- Der Zugriff auf Schul-Laufwerke muss bei Nicht-*Windows*-Geräten gesondert eingerichtet werden (s.u.).

⁷ Dies geschieht über *Windows*-Gruppenrichtlinien

⁸ Home-Verzeichnis, Tausch-Verzeichnisse, lokaler Mailserver

⁹ Wer ist an welchem Gerät angemeldet? Bildschirmübertragung, Tastatur-/Monitorsperre, Klassenarbeitsmodus, Materialverteilung,...

- Benutzer von *Windows*-Geräten können sich nach dem Einspielen der *opsi*-Pakete für den Domänenbeitritt an der Domäne anmelden und auf Schul-Laufwerke zugreifen.
- Ohne *opsi-client-agent*-Installation ist keine Verwaltung von Programmen bzw. OS-Installationen über Mechanismen der *paedML* möglich.
- Keine *italc*-Integration – Rechner können nicht mit *paedML*-Bordmitteln überwacht und über das Computerraummodul gesteuert werden.
- Für nicht in die Domäne integrierte Geräte ist kein Klassenarbeitsmodus verfügbar¹⁰.

3.2.2 Voll-Integration mobiler Endgeräte in das pädagogische Netz

Schuleigene (Windows-)Geräte, die mit *opsi* verwaltet werden, können alle Funktionen der *paedML Linux* nutzen.

¹⁰ Dies gilt insbesondere bei nicht unterstützten Betriebssystemen!

4. (Teil-) Integration von Windows-Tablets

Im Gegensatz zu einer Standard-Rechnerinstallation mit *opsi* wird im hier beschriebenen Verfahren ein Rechner NICHT über die *paedML*-Werkzeuge (*opsi*) installiert. Stattdessen wird das auf dem jeweiligen Tablet installierte Betriebssystem genutzt und das Gerät wird lediglich in die *paedML*-Domäne integriert.

Es gibt zwei Möglichkeiten der Teilintegration von Windows-Tablets:

1. Betrieb von Geräten MIT *opsi-client-agent*

Bei dieser Variante wird ein Gerät in die *paedML*-Domäne aufgenommen und zusätzlich ein *opsi-client* auf die Geräte eingespielt, über den Sie Software via *opsi*-Konsole ausrollen können.

2. Betrieb von Geräten OHNE *opsi-client-agent*

Bei dieser Variante wird ein Gerät in die *paedML*-Domäne aufgenommen. Die Geräte werden nicht über *opsi* mit Software versorgt. Die Systemwiederherstellung geschieht über Windows-Bordmittel.

Voraussetzungen für die Teilintegration

- Einsatz der *paedML Linux* ab Version 6.0
- Endgeräte mit domänenfähigem Windows-Betriebssystem¹¹.
- Geräte wurden mit installierter und lizenzierter Software gekauft, die an das Gerät gebunden ist.
- Geräte lassen sich nicht „out of the box“ über das Netzwerk booten¹².



Alle Geräte, die über PXE gebootet und mit *opsi* verwaltet werden können, sollten über die *paedML*-Bordmittel gesteuert werden (Vollintegration), da ein hoher Administrationsaufwand entstehen kann, wenn viele Geräte über eine Teilintegration an die *paedML* angebunden werden.



1. Rechner, die nicht mit *opsi* installiert wurden, können nicht mit *opsi-local-image*-Paketen gesichert und wiederhergestellt werden.
2. In der *opsi-Konsole* sind keine Informationen darüber verfügbar, welche Software auf dem Client installiert wurde, **bevor** das Gerät mit *opsi* verwaltet wurde. Nur Programme, die über *opsi* verteilt werden sind in der *opsi*-Maske als installiert sichtbar.

¹¹ Die *paedML Linux* unterstützt derzeit Windows 7 Professional oder Windows 10 Professional (jeweils die x64-Version). Die Teilintegration kann auch mit x86-Versionen durchgeführt werden.

¹² Es ist notwendig, dass die Geräte für die Installation des Betriebssystems über das Netzwerk booten. Einige Geräte mit UEFI (Unified Extensible Firmware Interface) unterstützen dies jedoch nicht automatisiert und müssen jedes Mal händisch in den Netzwerkboot-Modus versetzt werden.

4.1 Client-Registrierung in der paedML

Alle beschriebenen Arbeitsschritte werden als lokaler Administrator ausgeführt.

Zunächst müssen Sie den Rechner (wie im Administratorhandbuch Kapitel „*Verwaltung von Geräten*“ beschrieben) in die *paedML* aufnehmen. Wählen Sie als „*Typ*“ den Eintrag „*Windows-System*“, damit das Gerät in opsi übernommen wird.

Dies geschieht in der Schulkonsole über den Menüpunkt „*Schuladministration | Rechner (Schulen)*“. Sämtliche UEFI-Geräte müssen manuell über die Schulkonsole in die *paedML* aufgenommen werden. Eine Aufnahme über den (PXE-)Netzwerkboot ist nicht möglich.

Geräte mit zwei Netzwerkkarten (physikalische NIC und WLAN-Modul) werden (wie im Administratorhandbuch Kapitel 4.4 „Geräte mit mehreren Netzwerkkarten“ beschrieben) entsprechend in das System aufgenommen.



Der Name des Computers bei der Geräteaufnahme in die *paedML* und der Name des Computers in der Systemsteuerung (vgl. den folgenden Abschnitt) müssen identisch sein!

4.2 Betrieb von Geräten MIT opsi-client-agent

4.2.1 Aufspielen des opsi-client-agents



Der *opsi-client-agent* muss immer (neu) installiert werden, wenn ein Rechner in eine neue Domäne aufgenommen wird. Dies gilt auch für Systeme, auf denen das Programm bereits installiert wurde.

Auf dem *opsi-Server* finden Sie in der Netzwerkfreigabe `\\backup\opsi-depot\opsi-client-agent` das Skript „*service_setup.cmd*“, das auf dem Rechner, der mit *opsi* bekannt gemacht werden soll, ausgeführt werden muss.

Melden Sie sich an dem *Windows-Rechner* an, öffnen Sie über den *Windows-Explorer* die Freigabe \\BACKUP\opsi_depot\opsi-client-agent.

Melden Sie sich als *Domänenadministrator* an (Benutzername: *paedml-linux\administrator* und zugehöriges Kennwort) und führen Sie das Skript „*service_setup.cmd*“ aus.

Abb. 3: Eingabe des Pfades zum opsi-client-agent

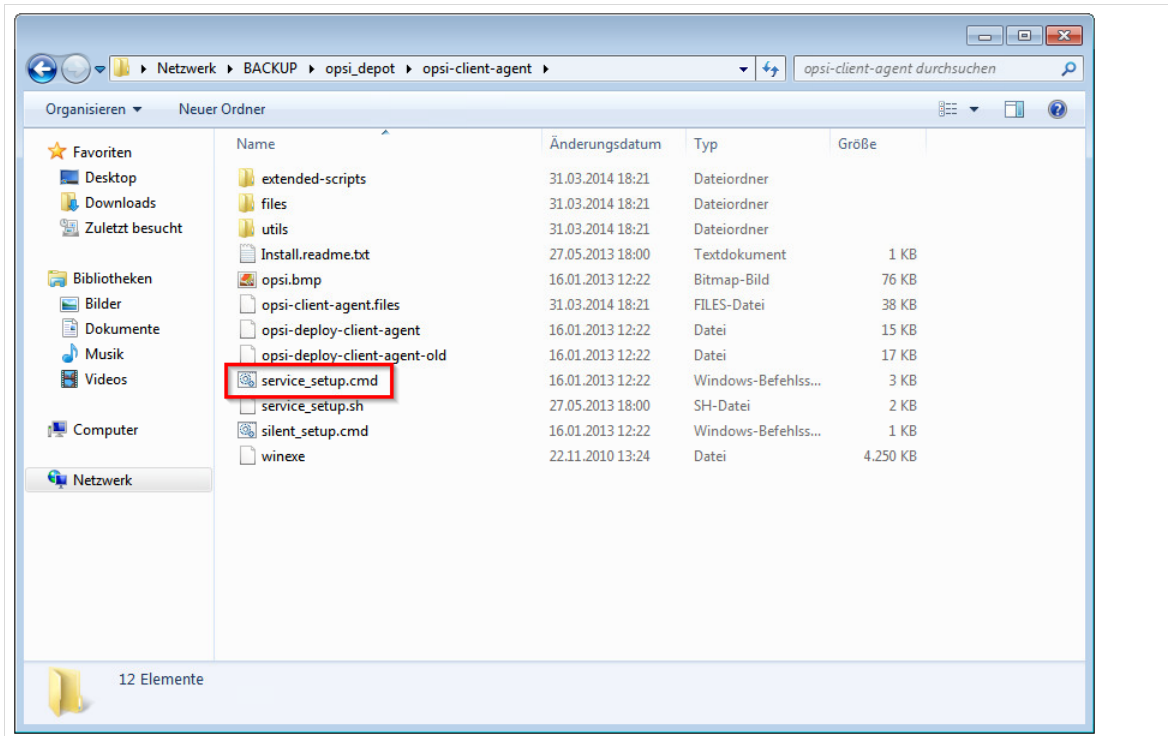


Abb. 4: Zugriff auf die Netzwerkfreigabe

Nach einem Doppelklick auf das Skript öffnet sich eine *Windows-Konsole*, in der Sie zur Bestätigung der Installation von „opsi-client-agent“ auf dem lokalen Rechner aufgefordert werden.

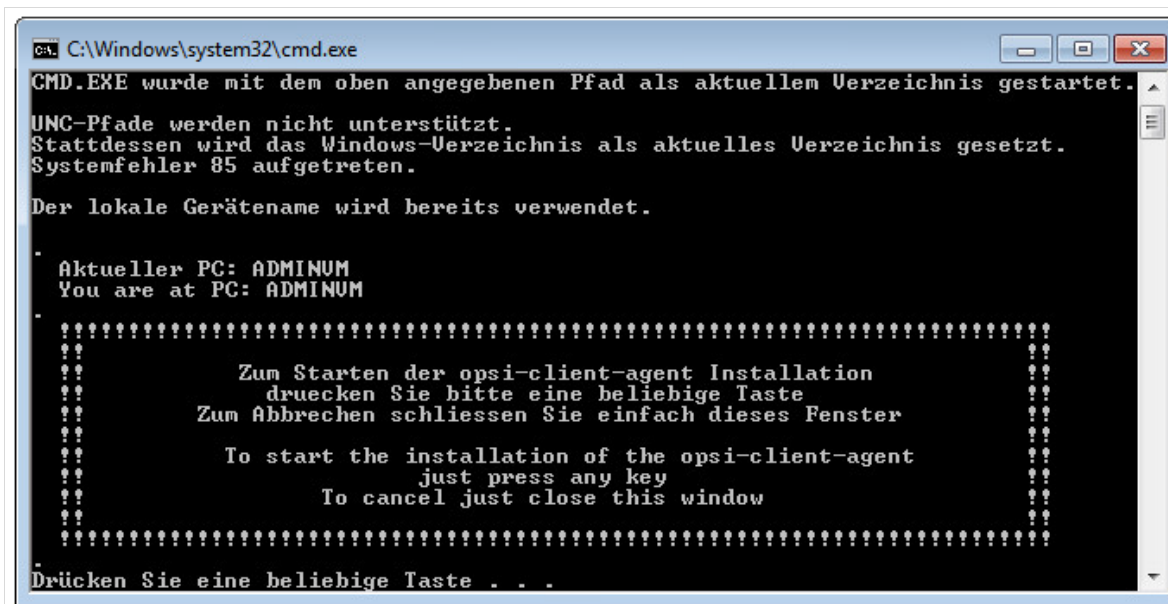


Abb. 5: Windows-Konsole vor Installation

Wenn Sie die Installation bestätigt haben, wird das Programm installiert.



Abb. 6: Installation des opsi-client-agent

Um die Installation vollständig auszuführen, benötigt das Paket erneut die Eingabe der Zugangsdaten des Domänen-Benutzers *Administrator* (ACHTUNG: großes A).

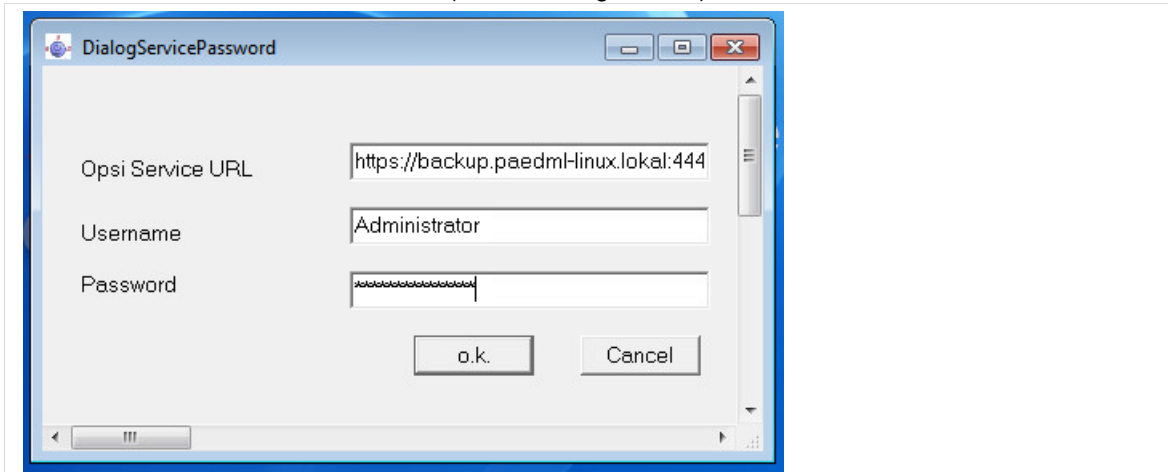


Abb. 7: Erneute Eingabe der Zugangsdaten des Domänenadministrators

4.2.2 Verwaltung des Rechners über opsi

Nachdem die Arbeitsschritte dieses Kapitels ausgeführt sind, können Sie den Rechner über opsi mit zusätzlicher Software versorgen. Sofern das Paket „*italc*“ auf den Rechnern installiert wird, ist eine Steuerung über die Schulkonsole (Rechner präsentieren, beobachten und sperren) möglich.

In der Übersicht der installierten Produkte (Reiter „*Netboot-Produkte*“ und „*Produktkonfiguration*“ sind jeweils nur die mittels opsi installierten Programme sichtbar!

Die Installation des opsi-Produktes „windomain“ ist zwingend notwendig, um den Rechner in die Domäne zu integrieren.

4.3 Optional: Betrieb von Geräten OHNE opsi-client-agent

Wenn Sie Geräte ohne opsi im Schulnetz betreiben wollen, muss der Domänenbeitritt unter Windows durchgeführt werden, damit sich Domänennutzer an dem Gerät anmelden können.

Nachdem der Client in der paedML registriert wurde, muss das Gerät in die Domäne „*paedml-linux.lokal*“ aufgenommen werden. Alle beschriebenen Arbeitsschritte werden als **lokaler Administrator** ausgeführt.

1. Schritt: Netzwerkeinstellungen überprüfen

Überprüfen Sie zunächst an der Eingabeaufforderung, ob sich das Gerät im IP-Adressbereich der paedML Linux befindet (Befehl: `ipconfig`):

```
C:\>ipconfig/all

Windows-IP-Konfiguration

    Hostname . . . . . : lehrerzimmer
    Primäres DNS-Suffix . . . . . :
    Knotentyp . . . . . : Hybrid
    IP-Routing aktiviert . . . . . : Nein
    WINS-Proxy aktiviert . . . . . : Nein

Ethernet-Adapter LAN-Verbindung:
    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : Intel(R) PRO/1000
    Physikalische Adresse . . . . . : 00-AA-11-BB-22-CC
    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . : Ja
    Verbindungslokale IPv6-Adresse . : fefe::fefe:fefe:fefe:fefe
    IPv4-Adresse . . . . . : 10.1.0.123
    Subnetzmaske . . . . . : 255.255.255.0

(...)
```

Stellen Sie sicher, dass der opsi-Server erreichbar ist (der Befehl `ping 10.1.0.2` muss eine Antwort vom opsi-Server erhalten!

Wenn die Netzwerkeinstellungen korrekt sind, geht es weiter mit dem 3. Schritt.

2. Schritt (optional): Netzwerkeinstellungen anpassen

Wenn der Computer nicht im paedML-Adressraum ist, müssen Sie die Netzwerkeinstellungen so anpassen, dass der Rechner eine IP-Adresse im Netz *10.1.0.0/24* erhält. Testen Sie die Einstellungen, wie in Schritt 1 beschrieben.

3. Schritt: Rechnernamen überprüfen und gegebenenfalls ändern

Öffnen Sie die *Systemsteuerung* und dort den Menüpunkt „System“. Im Abschnitt „*Einstellungen für Computernamen, Domäne und Arbeitsgruppe*“ finden Sie den Eintrag „*Einstellungen ändern*“ (1).

Wenn Sie diesen Punkt ausgewählt haben, öffnet sich ein neues Fenster „Systemeigenschaften“.

Klicken Sie auf „Ändern“ (2), um das nächste Dialogfenster „Ändern des Computernamens bzw. der Domäne“ aufzurufen.

Hier überprüfen Sie, ob der Computernamen mit dem Namen des Rechners bei der Client-Registrierung (Kapitel 4.1) übereinstimmt. Tragen Sie den Namen der Domäne „*paedml-linux.lokal*“ in das hierfür vorgesehene Feld ein (3).

Sie werden für den Domänenbeitritt nach einem Benutzer und einem Kennwort gefragt. Es handelt sich hierbei um den *Administrator der Domäne*. Der Domänenbeitritt kann auch mit dem Benutzerprofil *domadmin* durchgeführt werden.

Bestätigen Sie die Eingaben jeweils mit „OK“ und führen Sie im Anschluss einen Neustart durch, damit die Änderungen übernommen werden.



Sollte der Computer Mitglied einer anderen Domäne gewesen sein, müssen Sie zunächst – analog dem hier vorgestellten Verfahren einer beliebigen Arbeitsgruppe beitreten.

Anschließend müssen Sie den Rechner neu starten, bevor Sie ihn schließlich in die Domäne „*paedml-linux.lokal*“ aufnehmen können.

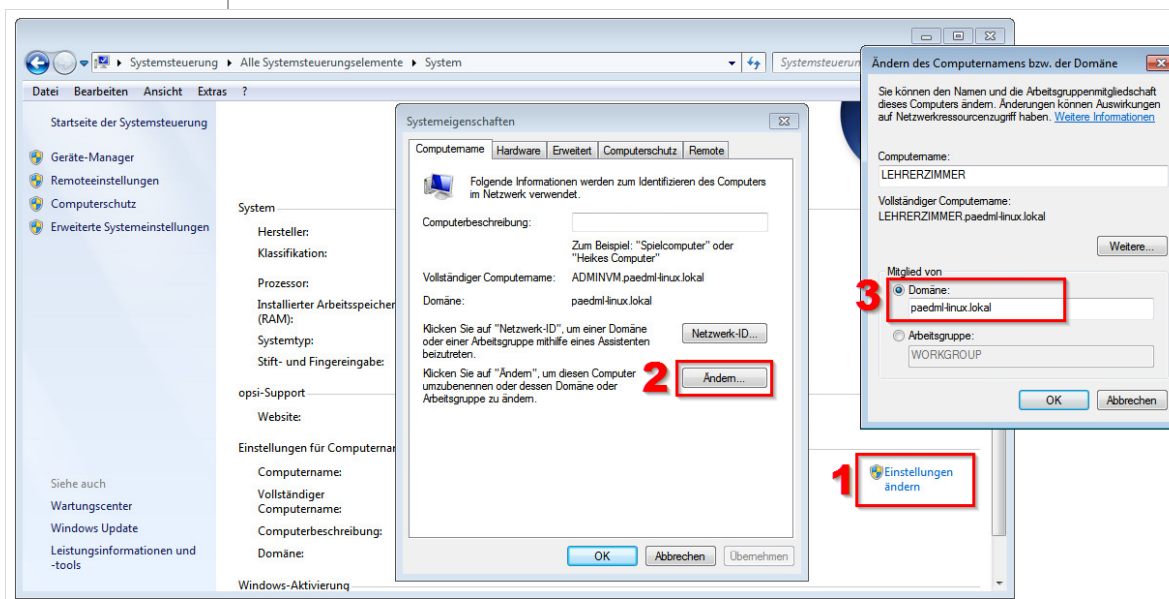


Abb. 8: Ändern von Computernamen und Domäne

Nun ist der Rechner in der paedML-Domäne aber nicht per opsi administrierbar.

4.4 Deaktivieren der Windows-Firewall

Damit die Rechner, die über eine Teilintegration in die paedML integriert wurden, mit pädagogischen Funktionen – wie der Bildschirmanzeige – betrieben werden können, müssen Sie auf den Geräten die Windows-Firewall deaktivieren.

Hierfür sind zwei Verfahren denkbar:

1. Manuelles Deaktivieren der Windows-Firewall je Client.

Beim Einsatz weniger Clients ist dieses Verfahren zu bevorzugen, da einfacher.

2. Deaktivieren der Firewall über ein opsi-Paket

Es besteht die Möglichkeit, dass über ein opsi-Paket („*windows-firewall-aus*“) zentral über die opsi-Konsole die Windows-Firewall deaktiviert wird. Dies funktioniert natürlich nur bei Rechnern, auf denen der opsi-client-agent installiert ist.

2.1 Installation des opsi-Paketes „*windows-firewall-aus*“ auf dem Server

Im ersten Schritt müssen Sie das opsi-Paket auf dem opsi-Server installieren. Loggen Sie sich hierfür als Benutzer „*root*“ auf der Konsole des opsi-Servers ein und führen Sie die folgenden Befehle aus (der Umbruch in der ersten Befehlszeile ist darstellungsbedingt):

```
#ucr set --force opsi/product-  
download/repository_uib/includeProductIds=windows-firewall-aus  
#opsi-product-updater -i -vv  
#ucr unset --force opsi/product-download/repository_uib/includeProductIds
```

2.2. Ausführen des opsi-Paketes auf den Arbeitsplatzrechnern

Wenn Sie das Paket auf dem opsi-Server installiert haben, können Sie im Anschluss das Programm opsi-configd starten und das Paket auf den zu konfigurierenden Clients ausführen.

5. Voll-Integration am Beispiel eines Surface 3 Pro



Im Rahmen einer mobilen paedML-Umgebung wurden Surface-Tablets beschafft. Bitte beachten Sie, dass es sich um Surface 3 **Pro** Geräte handelt. Die Anbindung dieser Geräte an die paedML Linux wurde hier dokumentiert.

Generell können auch andere Windows-Tablets voll in die paedML Linux integriert werden, wobei folgende Aspekte beachtet werden müssen:

- 64-bit UEFI-Unterstützung
- PXE-Boot-Fähigkeit

Testen Sie die Geräte vorher in der paedML, bevor sie angeschafft werden!

Im Gegensatz zu Standard-PCs oder Laptops sind bei Tablets einige Besonderheiten zu beachten, um eine Installation mit *paedML*-Bordmitteln vorzunehmen. Im Folgenden wird – am Beispiel eines Surface 3-Pro Tablets – aufgezeigt, wie Sie ein Windows-Tablet mit opsi ausspielen können.



Es ist ratsam die Geräte, die Sie mit opsi ausspielen, vorher komplett zu sichern, um später eine Möglichkeit zu haben, den Auslieferungszustand wiederherzustellen.

5.1 Manuelle Client-Registrierung in der paedML

Zunächst müssen Sie den Rechner (wie im Administratorhandbuch Kapitel „*Verwaltung von Geräten*“ beschrieben) in die *paedML* aufnehmen. Dies geschieht in der Schulkonsole über den Menüpunkt „*Schuladministration | Rechner (Schulen)*“. Setzen Sie unbedingt den Haken bei „*UEFI (nur für Windows-Systeme)*“.

UEFI-Geräte (also auch das Surface 3-Pro) müssen manuell über die Schulkonsole in die paedML aufgenommen werden. Eine Aufnahme über den (PXE-)Netzwerkboot ist nicht möglich.

Geräte mit zwei Netzwerkkarten (physikalische NIC und WLAN-Modul) werden (wie im Administratorhandbuch Kapitel 4.4 „*Geräte mit mehreren Netzwerkkarten*“ beschrieben) entsprechend in das System aufgenommen.

5.2 Gerät vorbereiten



Überprüfen Sie auf jeden Fall, ob die Firmware der Geräte auf dem aktuellen Stand ist und aktualisieren Sie diese zunächst.

Bei der Arbeit mit verschiedenen Tablets ist aufgefallen, dass einige Funktionen (zum Beispiel das Einstellen der Boot-Reihenfolge) erst nach Aktualisierung der Firmware verfügbar waren.

Mit der Einführung von UEFI, soll der bisher verbreitete BIOS-Standard abgelöst werden¹³. Hierbei wurde die „Secure-Boot-Technologie“ eingeführt.

Damit [mittels Secure-Boot] soll verhindert werden, dass [ein] unsigned und damit eventuell gefährlicher Code gestartet wird. Was sich so schön nach „Sicherheit“ anhört, sorgt für erhebliche Probleme: Die Signierung vergibt nur Microsoft. Viele freie Betriebssysteme, LiveCDs und selbst Windows 7 haben keine Signierung, können folglich auf Systemen mit aktiviertem Secure Boot nicht starten.

Quelle: <http://www.wintotal.de/uefi-der-bios-nachfolger-grundlagen-und-hilfestellung/>

Um die Geräte zukünftig über das Netzwerk starten¹⁴ und mit opsi verwalten zu können, muss im ersten Schritt „Secure-Boot“ deaktiviert werden.

Schalten Sie hierfür das Surface 3 Pro ein und drücken Sie gleichzeitig mit (besser vor) der Betätigung des Anschalt-Knopfes die Lautstärke-Wippe nach oben.

Sie gelangen im Anschluss in das Konfigurationsmenü des Surface-UEFI.

Dort müssen Sie die folgenden Einstellungen vornehmen:

- Stellen Sie den Wert „Secure Boot Control“ auf „Disabled“.
- Ändern Sie die Bootreihenfolge unter „Configure Alternate System Boot Order“ auf „Network → USB → SSD“.

Diese Einstellungen müssen für das Ausspielen von Windows oder anderen „Netboot-Produkten“ via opsi aktiv sein. Später müssen Sie die Bootreihenfolge wieder auf „SSD only“ zurückstellen, sofern das Gerät mit Kabel an das Netzwerk angeschlossen wird.

Werden die Geräte ausschließlich über WLAN genutzt, kann das Netzwerk weiterhin als erstes „Boot-Device“ aktiv bleiben.

- Beenden Sie den Dialog mit „Exit Setup“ und übernehmen Sie die Änderungen.

¹³ Vgl. https://de.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

¹⁴ Alle Aufgaben, die über opsi-Netboot-Produkte ausgeführt werden (z.B. Betriebssystem ausspielen, Backup erstellen/wiederherstellen,...) müssen über eine Kabel-Verbindung durchgeführt werden. Das Verteilen von Software kann prinzipiell über WLAN erfolgen, wobei bei einer großen Anzahl von Geräten, sowie bei großen Datenmengen nicht nur viel Zeit in Anspruch genommen wird, sondern auch Fehler auftreten können. Es wird daher empfohlen Software über eine Kabelverbindung der Tablets zu verteilen.

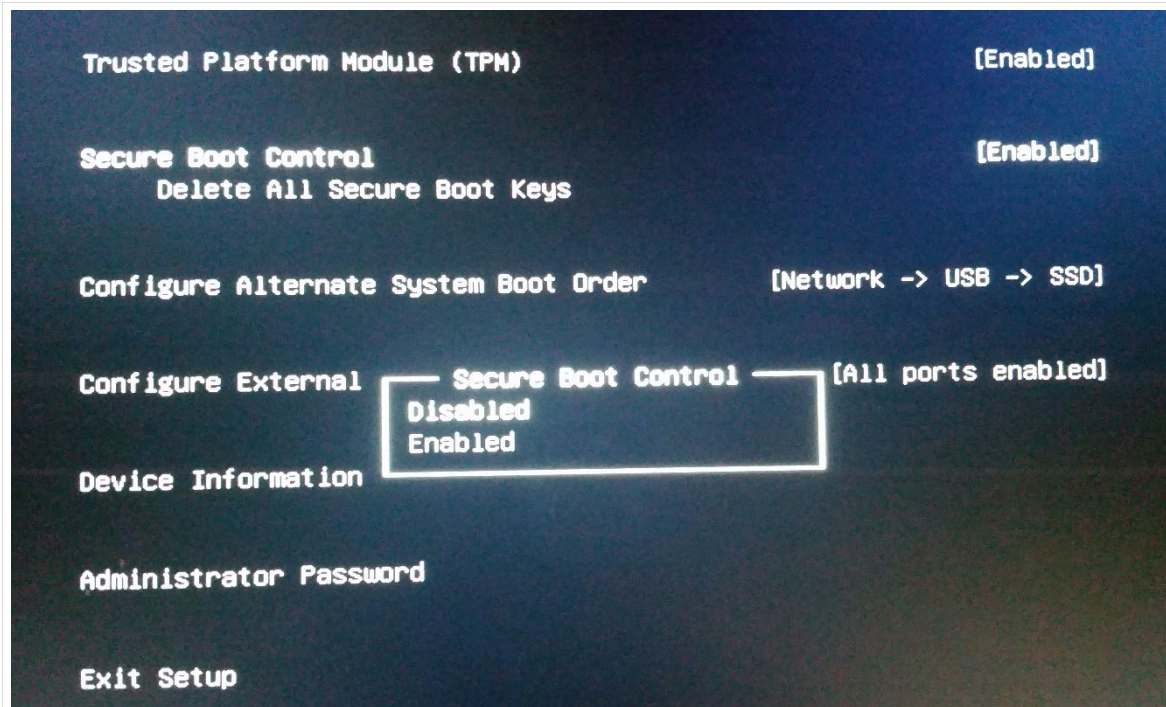


Abb. 9: UEFI-Konfiguration



Nach der Umstellung der Secure-Boot-Option wird der Bildschirm bei allen folgenden Systemstarts rot und in der Mitte steht „Surface“. Dies signalisiert, dass Secure-Boot deaktiviert wurde.

Sollte nach dem Neustart „ELILO Boot“ auf dem Bildschirm erscheinen, betätigen Sie die **Return**-Taste, um den Bootvorgang fortzusetzen.

5.3 Manueller Netzwerkboot



Wenn für den Netzwerkboot in opsi keine Aktionen gesetzt sind, dann kann opsi die UEFI-Clients nicht starten, sobald diese, mit Netzkabel an das Schulnetz angeschlossen, gestartet werden.

Das System gerät in eine Endlosschleife beim Versuch über das Netzwerk zu starten (Fehlermeldung: „no config file found on TFTP server in linux/pxelinux.cfg/ forcing interactive mode due to config file error(s)“).

Dieses Problem sollte nicht auftreten, wenn die Kabelverbindung getrennt und das Gerät über WLAN betrieben wird.

Aus diesem Grund darf der automatische Netzwerkboot bei Geräten, die mit einem Netzkabel betrieben werden, nur solange aktiv gesetzt sein, wie opsi-Netboot-Produkte installiert werden (Ausspielen von Betriebssystem, Erstellen von Backups, Erstellen und Verteilen von Capture-Images, ...).

Die Bootreihenfolge sollte anschließend auf „SSD only“ gestellt werden, damit das hier beschriebene Problem nicht auftritt. (Alternativ können Sie das Gerät vom Schulnetz trennen. Sobald eine Kabelverbindung mit dem Schulnetz hergestellt wird, wird das Gerät versuchen eine opsi-Netboot-Aktion auszuführen und – sofern keine Aktion gesetzt ist – nicht starten.

Es gibt einen Workaround, um Geräte, die über Kabel verbunden sind temporär über das Netz zu starten: **Um ein Surface 3 Pro Tablet manuell über das Netzwerk zu starten, muss gleichzeitig zu (besser vor) der Betätigung des Anschalt-Knopfes die Lautstärke-Wippe nach unten gedrückt werden.**

Anschließend startet das System über das Netz und arbeitet vorhandene opsi-Aufträge ab.

5.4 Überprüfen von opsi-Einstellungen bei UEFI-Geräten

Damit *opsi* auf UEFI-Geräte zugreifen kann, müssen die im folgenden Abschnitt beschriebenen Einstellungen im Reiter „Host-Parameter“ der opsi-Konsole gesetzt sein. Diese Einstellungen werden automatisch gesetzt, sobald ein Gerät bei der Aufnahme über die Schulkonsole den Haken „UEFI (nur für Windows-Systeme)“ gesetzt bekommt.

Sofern es beim PXE-Boot der Geräte zu Fehlern kommt, sollten diese Einstellungen überprüft werden. Wählen Sie in der Liste der Geräte auf der linken Seite der opsi-Konsole den zu konfigurierenden Client aus.

Wechseln Sie in den Reiter "Host-Parameter" und wählen Sie den Eintrag "clientconfig". In der Zeile „clientconfig.dhcpd.filename“ müssen Sie anschließend den Wert „pxelinux.cfg/elilo.efi“ eintragen.

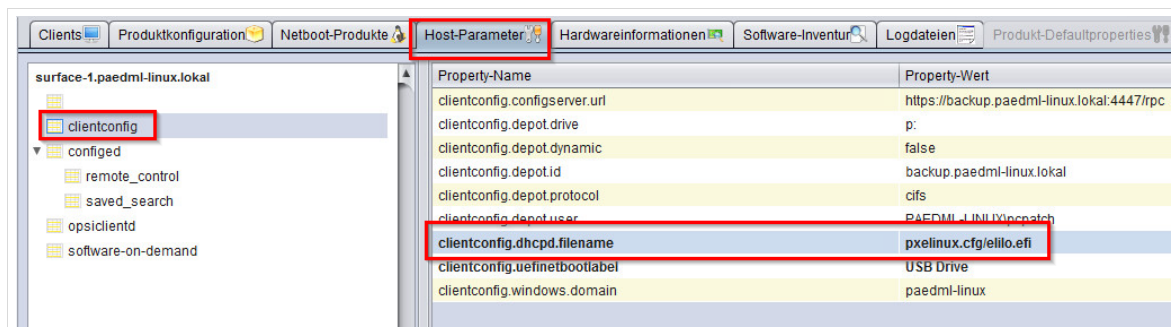


Abb. 10: UEFI-Anpassungen unter opsi

5.5 Treiber bereitstellen

Die Bereitstellung von Treibern wird im Administrator-Handbuch beschrieben. Hier sei zur Wiederholung ein kurzer Blick auf die Abläufe geworfen:

1. In opsi können bei der Installation von Windows Hardwaretreiber an das System übergeben werden.

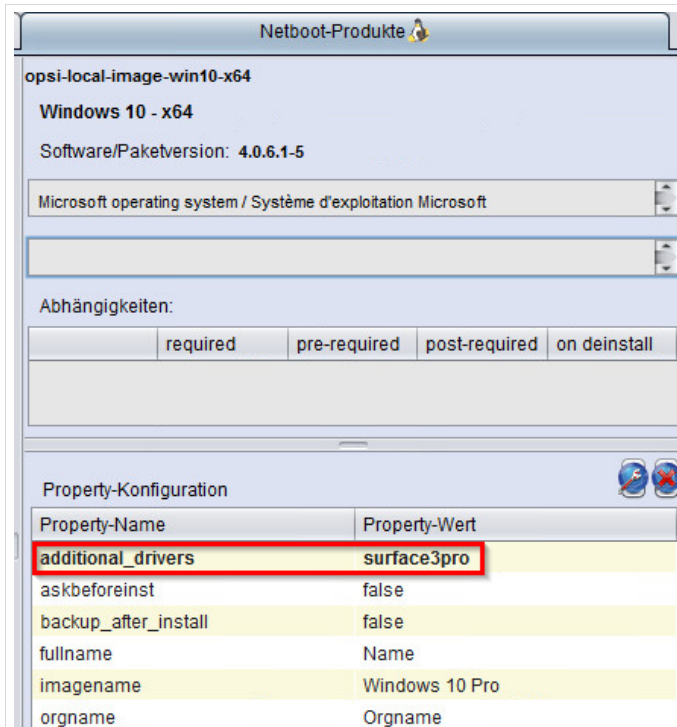


Abb. 11: Einbinden zusätzlicher Treiber in das System

2. Treiber müssen für jede Windows-Version, die auf der Hardwareklasse installiert werden soll, auf den opsi-Server hochgeladen werden. Im Reiter „Hardwareinformationen“ der opsi-Konsole gibt es eine Schaltfläche „Upload von Treibern“ (Plus-Symbol), mit dem der Ladevorgang initiiert wird.

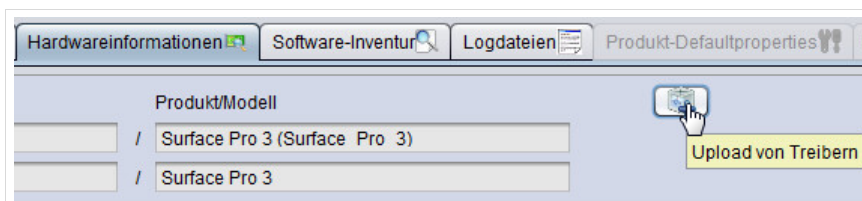


Abb. 12: Treiber auf den opsi-Server laden (1)

3. Es öffnet sich ein Fenster, in dem verschiedene Einstellungen vorgenommen werden können.
 - „für Windows-Produkt“: Wählen Sie hier das Betriebssystem, das mit Treibern versorgt werden soll.
 - „Treiber“: Hier wird der Pfad eingetragen, in dem die Hardwaretreiber für die Geräteklasse liegen. Die „Methode der Treiberintegration“ bestimmt, wie die Treiber bei der Installation an das Betriebssystem übergeben werden. Empfohlen wird der Wert „Additional“.
 - Über das Plus-Symbol (unten rechts) wird der Treiberupload gestartet.

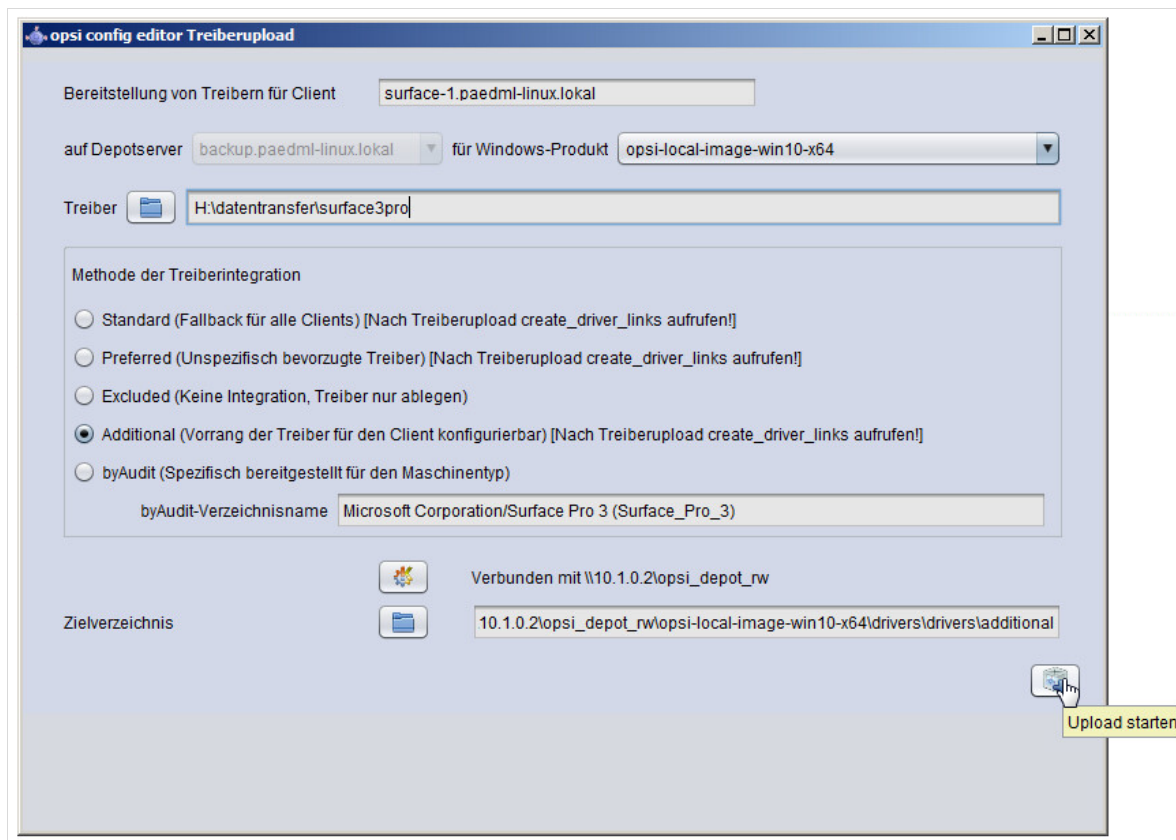


Abb. 13: Treiber auf den opsi-Server laden (2)

4. Sobald der Treiberupload abgeschlossen ist, müssen Sie auf die opsi-Server-Konsole wechseln.
 - Melden Sie sich als Benutzer „root“ mit dem zugehörigen Kennwort an.
 - Wechseln Sie in das Verzeichnis mit den Installationsdateien (z.B. opsi-local-image-win10-x64) und führen Sie den Befehl `./create_driver_links.py` aus. Beispielfür ein Windows 10 (64-Bit) wären die folgenden Befehle einzugeben:

```
#cd /var/lib/opsi/depot/opsi-local-image-win10-x64
#./create_driver_links.py
```

Nun sind die Treiber in das System eingespielt und können bei der Installation des Betriebssystems eingebunden werden¹⁵.

Bei der Konfiguration des opsi-Produktes, das die Installation des Betriebssystems durchführt, wird im Feld „*additional_drivers*“ der Verzeichnisname übergeben, in dem sich die Treiber befinden.

Der Verzeichnisname ist abhängig vom opsi-Produkt, das installiert wird. Im vorherigen Screenshot wird auf dem opsi-Server ein Verzeichnis erzeugt:

/var/lib/opsi/depot/opsi-local-image-win10-x64/drivers/drivers/additional/surface3pro.

¹⁵ Beim Surface 3 Pro kann über diesen Mechanismus auch eine Firmware bereitgestellt werden.

Der Wert für „*additional_drivers*“ wäre demnach „*surface3pro*“ (vgl. erster Screenshot von Kapitel 5.5).

5.6 Clients ausrollen und damit arbeiten

Im nächsten Schritt können Sie das Gerät mit Betriebssystem, Treibern und Software versorgen.

5.6.1 Besonderheiten bei der Partitionierung

Im Gegensatz zu herkömmlichen Desktop-Rechnern (in denen heute meist mehrere Hundert Gigabyte Festplatten-Platz vorhanden sind), verfügen viele Tablets über eine geringere Festplattenkapazität. Es ist daher im Vorfeld der Anschaffung solcher Geräte zu überlegen, ob die Festplattenkapazität ausreicht, um die Geräte sinnvoll zu betreiben. In dieser Beispielkonfiguration wurde ein Surface 3 Pro mit einer 64 Gigabyte Festplatte eingerichtet. Die Beschaffung von Geräten mit weniger als 64 Gigabyte ergibt vermutlich keinen Sinn, wenn Sie – wie empfohlen – eine Partition für die Sicherung von opsi-Images einrichten wollen.

Die Softwareinstallation, die ausgiebig im Administratorhandbuch beschrieben ist, geschieht über das opsi-Netboot-Produkt „*opsi-local-image-prepare*“. Bei der Einrichtung der Geräte wird über dieses opsi-Produkt eine Partitionierung der Festplatte durchgeführt. Hierbei sind ein paar Dinge zu beachten. Im Folgenden werden die Parameter exemplarisch an einer 64 Gigabyte-Platte erörtert. Die Werte können (bzw. müssen) bei anderen Ausstattungen angepasst werden.

- Der Parameter „*system_partition_size*“ bestimmt die Größe der Systempartition (c:\-Laufwerk). Hier sollte der Wert nicht zu groß bemessen werden, damit genügend Platz für eine Backup-Partition vorhanden ist. Im Gegenzug darf die Partition aber auch nicht zu klein werden, um ein sinnvolles Arbeiten mit Windows zu ermöglichen. Im folgenden Beispiel wurde eine Partitionsgröße von 30 Gigabyte gewählt.
- Die „*data_partition_size*“, also die Größe einer zweiten Datenpartition (d:\-Laufwerk) wurde auf 0 Gigabyte gesetzt.
- Der Wert „*winpe_partition_size*“ (Standard 4 G(igabyte)) bestimmt die Größe der Hilfspartition, auf der die Windows-Installationsdaten sowie Hardwaretreiber abgelegt werden. Dieser Wert wurde bei der Installation der Surfaces (um Speicherplatz zu sparen) auf 2 Gigabyte verringert und muss erhöht werden, sobald ein großes Datenvolumen von Treiberdateien bereitgestellt wird. Wenn der Rechner beim Hochladen der Installationsdateien vom opsi-Server auf den zu installierenden Rechner Probleme hat und den Ladevorgang abbricht, sollte der Wert der „*winpe_partition_size*“ sukzessive um 200 MB erhöht werden, bis die Installation durchläuft.
- Abhängig von den soeben vorgenommenen Einstellungen muss im letzten Schritt gegebenenfalls der Wert „*minimal_backup_partition_size*“ angepasst werden. Dieser Wert bestimmt die Größe der Backup-Partition in Relation zur Gesamtgröße der Systemplatte. Der Standard-Wert von 55% kann bei einer mit 32 Gigabyte allokierten Festplatte selbstverständlich nicht erreicht werden. Daher wurde dieser Wert (großzügig) auf 20% herunter gesetzt.

Property-Konfiguration	
Property-Name	Property-Wert
askbeforeinst	false
data_partition_size	0G
delay_for_reboot	0
minimal_backup_partition_size	20%
start_os_installation	opsi-local-image-win10-x64
system_partition_size	30G
winpe_partition_size	2G

Abb. 14: Anpassungen von opsi-local-image-prepare an eine kleine Festplatte

Wenn die Einstellungen vorgenommen wurden, sollten Sie das Gerät mit opsi installieren können. Achten Sie darauf, dass das Gerät nach dem Abarbeiten der Netboot-Produkte lokal oder über WLAN gestartet werden muss.

Sobald größere Programminstallationen vorgenommen werden (z.B. Office-Programme), sollte die Verbindung über das Kabelnetz wieder hergestellt werden, nachdem das Gerät angefangen hat.

5.6.2 Netzwerk-Konfiguration

1. Die Installation der Endgeräte sollte über einen (USB-)Netzwerkadapter erfolgen, der dauerhaft fest dem Gerät zugewiesen ist¹⁶. Auch sollten größere Datenmengen (Updates, Programminstallationen) aus Gründen der Performance über ein Netzkabel auf die Geräte verteilt werden. Es wird empfohlen sowohl das Tablet, als auch den Adapter mit einer eindeutigen Kennung zu versehen (z.B. mit Hilfe eines Label-Druckers).
2. Im Administratorhandbuch wird beschrieben, wie weitere MAC-Adressen (WLAN-Karten) an einen paedML-Client zugewiesen werden können.
3. Nach der erfolgten Installation bekommen die Geräte beim Systemstart über die Domäne eine IP-Adresse zugewiesen.
4. Je Gerät muss einmalig als lokaler Administrator eine Verbindung zum WLAN hergestellt werden, bei der der Netzwerkschlüssel im Gerät hinterlegt wird.

Nun ist die Konfiguration der Surface 3 Pro Tablets abgeschlossen und Sie können die Geräte in Ihrem Schulnetz einsetzen.

¹⁶ Anhand der MAC-Adresse des Netzadapters identifiziert die paedML das Endgerät und weist ihm den Computernamen zu. Wenn ein Adapter bei mehreren Geräten verwendet wird, führt dies dazu, dass die Geräte alle gleich heißen. Dies führt zu Problemen mit der Windows-Domäne.

6. Alternativen zu Windows

Die *paedML Linux* ist für den Betrieb von *Windows*-Endgeräten ausgelegt. Hierfür wurden Mechanismen wie Softwareverteilung, Unterrichtssteuerung und die Benutzerverwaltung, inklusive Zugriff auf persönliche Ressourcen, entwickelt.

Windows ist das am weitesten verbreitete Client-Betriebssystem¹⁷, das sowohl im privaten, geschäftlichen, als auch im schulischen Umfeld eine hohe Akzeptanz erfährt. Im Unterricht werden vornehmlich Programme aus der *Windows*-Welt behandelt und geschult.

Daneben gibt es eine Vielzahl von anderen Betriebssystemen, die nicht nur privat genutzt werden, sondern auch im schulischen Umfeld Befürworter finden.

In diesem Kapitel wollen wir einen Blick auf die bekanntesten *Windows*-Alternativen werfen. Dabei werden **ausschließlich Einsatzszenarien** von mobilen Endgeräten **im pädagogischen Netz** beschrieben. Die Einrichtung des Gästernetzes, sowie die Einbindung mobiler Clients ist in der HowTo-Anleitung „*WLAN in der paedML Linux*“¹⁸ beschrieben.

Die in diesem Kapitel vorgestellten Szenarien sind **Beschreibungen, wie einzelne Geräte auf Netzwerkressourcen der paedML zugreifen können**. Auf grundlegende paedML-Funktionen muss verzichtet werden.

Eine Integration von Nicht-*Windows*-Geräten bedeutet einen administrativen Mehr-Aufwand. Insbesondere zentrale Verwaltungsaufgaben (Softwareverteilung, Benutzerverwaltung, Verteilen von (Gruppen-)Richtlinien) sind nur mit dem Einsatz eines gesonderten Mobile-Device-Management-Systems sinnvoll.



Wenn Sie weitere Vorschläge für die zentrale Konfiguration von Nicht-*Windows*-Geräten haben und Ideen haben, wie wir diese in die *paedML* einbinden können, freuen wir uns über Ihre Rückmeldung.



Die im Folgenden vorgestellten Wege, um iPads oder Android-Geräte in das pädagogische Netz einzubinden, setzen voraus, dass das jeweilige Gerät einem eindeutigen Benutzer zugeteilt wird.

Da dies bei der Benutzung durch verschiedene Anwender (z.B. ein Tablet wird in der Kunst-Sammlung verwendet und von mehreren Schülern bedient) nicht zielführend ist, könnten Sie sich mit einem zusätzlichen Benutzerkonto helfen, das in der *paedML* angelegt wird. Mit diesem Benutzer (zum Beispiel „Tablet1“) könnten Daten auf dem Schulserver gespeichert werden.

¹⁷ Vgl. <http://www.webmasterpro.de/portal/webanalyse-systeme.html>

¹⁸ <http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/howtos/wlan-in-der-paedmlr-linux-60.html>

Über Projekte (Arbeitsgruppen), die Sie in der Schulkonsole anlegen, können Anwender auf ein Tauschverzeichnis zugreifen. Darauf können Daten zwischengespeichert werden.

Der Einsatz eines solchen – mehr oder weniger anonymen – Kontos bedeutet leider auch, dass die Lehrkräfte darüber Buch führen müssen, an welche Schüler diese Geräte zu welchem Zeitpunkt ausgeliehen werden!

Alternativ zu diesem Verfahren wird im Folgenden beschrieben, wie Sie Netzfreigaben für Homeverzeichnisse, Klassentausch- und Projekttauschverzeichnisse einbinden können.

Geräte, die in das pädagogische Netz aufgenommen wurden, erhalten mit den folgenden Parametern Zugriff auf das Internet und die Ressourcen des Netzwerkes:

Parameter	wird benötigt für	Wert
Proxy	Zugriff auf das Internet	Adresse: 10.1.0.1 Port: 3128
Zugangsdaten von paedML Benutzer	Zugriff auf das Internet – zusätzliche Authentifizierung am Proxy-Server, die entweder in den Netzwerkeinstellungen des jeweiligen Betriebssystems zentral oder für einzelne Applikationen bei der Benutzung eingetragen werden muss	Benutzername und Kennwort eines paedML-Benutzers
Zugangsdaten von paedML Benutzer ¹⁹	Zugriff auf Dateien im Home-Verzeichnis Zugriff auf Klassen-Tauschverzeichnisse Zugriff auf Projekt-Tauschverzeichnisse	Benutzername und Kennwort eines paedML-Benutzers

Tabelle 2: Benötigte Werte für den Zugriff auf Netzwerkressourcen der paedML

6.1 Einbinden von Android-Geräten²⁰

6.1.1 Grenzen der Integration in die paedML

Eine vollständige Integration von Endgeräten mit *Android*-Betriebssystem ist derzeit in **keiner** *paedML*-Version vorgesehen.

¹⁹ Für den Zugriff wird ein Programm benötigt, das auf Samba-Freigaben zugreifen kann.

²⁰ Die hier beschriebenen Verfahren wurden mit Android 4.4.2 ausgearbeitet und getestet.

Ein großer Nachteil bei Android-Systemen ist die Tatsache, dass im Auslieferungszustand *Android* kein Mehrbenutzer-Betriebssystem ist, das sich mit Bordmitteln in eine Domäne integrieren lässt und von verschiedenen Anwendern genutzt werden kann. Die Geräte sind dafür ausgelegt, dass sie mit einem Benutzer-Konto betrieben werden, dessen Hoheit beim Hersteller (Google) liegt.

Android-Geräte stellen die heterogenste Gruppe von Endgeräten dar. Hierdurch entstehen weitere noch offene Fragen bzw. Probleme:

- Die Geräte-Hersteller passen in der Regel das Benutzerinterface an – trotz gleicher *Android*-Version können verschiedene Geräte unterschiedlich zu bedienen sein.
- Es sind verschiedene Versionsstände von *Android* im Umlauf. Größere Updates bedeuten in der Regel ein neues Erscheinungsbild und andere Funktionen.
- Geräte können häufig nicht ohne großen Aufwand repariert werden, zum Beispiel, wenn der fest verbaute Akku defekt ist.
- Bei den Geräten stellt sich die Frage nach einer nachhaltigen Anschaffung (Ersatzgeräte sind unter Umständen nach einer gewissen Zeit nicht mehr lieferbar, wenn die Produktpalette getauscht wurde).
- Proxy-Einstellungen können bei *Android* nur für einzelne Programme vorgenommen werden. Es gibt derzeit (Version 4.x 5.x) keine zentrale Stellschraube, um die Konfiguration eines Proxy-Servers für alle *Android*-Programme eines Gerätes vorzunehmen.
- Ein Zugriff auf den Play-Store aus dem paedML Netz ist nicht möglich.
- Der Zugriff auf Netzressourcen der *paedML* muss über Drittsoftware geschehen. Hierfür müssen Programme installiert werden, die auf Samba-Freigaben zugreifen können.
- Für ein zentrales Management der Endgeräte, über das Betriebssystem und Software verteilt werden kann, muss auf ein MDM²¹-Produkt zugegriffen werden. Die erhältlichen Anwendungen unterscheiden sich stark im Preis und Umfang.

6.1.2 Einstellungen für den Internet-Zugriff

1. Zunächst müssen Sie die Geräte – wie im Administratorhandbuch beschrieben – in das pädagogische Netz aufnehmen. Wählen Sie für *Android*-Geräte den Typ „Gerät mit IP-Adresse“.
2. Verbinden Sie sich anschließend mit einem Access-Point Ihres Schulnetzes. Achten Sie darauf, dass die Endgeräte die IP-Adresse über DHCP beziehen.
3. Um auf das Internet zuzugreifen, muss der *Proxyserver* der *paedML* eingetragen werden. Dieser läuft auf der *IP-Adresse 10.1.0.1* und dort auf *Port 3128*.
4. Unter *Android* gibt es keine Möglichkeit einen zentralen Proxy-Server einzutragen, der von allen Apps genutzt wird. Die Proxy-Einstellungen gelten jedoch für den Browser und ein Surfen im Internet sollte möglich sein.

²¹ „Mobile Device Management“

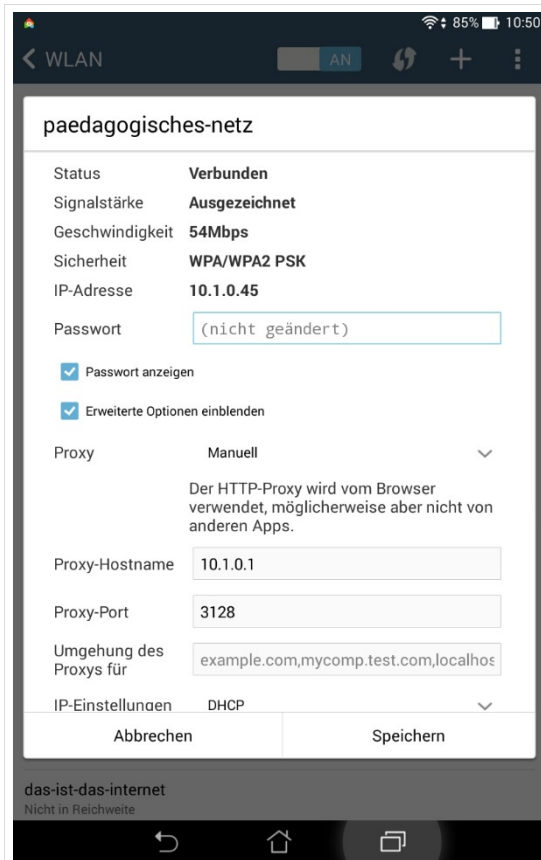


Abb. 15: Verbindung eines Android-Gerätes mit dem WLAN im pädagogischen Netz

6.1.3 Zugriff auf das pädagogische Netz

Nachdem das Gerät in das Schulnetz eingebunden wurde, können Sie mit einem Dateibrowser, der Samba unterstützt²², auf Daten, die auf dem Server liegen, zugreifen.

Um auf das Homeverzeichnis eines Benutzers zugreifen zu können, muss als Ziel für den Zugriff der Pfad `server/BENUTZERNAME` eingegeben werden. Auf Klassentausch-Verzeichnisse greifen Sie mit dem Pfad `/server/schule-KLASSE` und auf Projekt-Tauschverzeichnisse mit `server/schule-PROJEKTNAME` zu.

Als Zugangsdaten sind `BENUTZERNAME` und `PASSWORT` des jeweiligen Benutzers zu verwenden.

²² Es gibt einige *Android*-Dateibrowser, die den Zugriff auf Samba-Freigaben unterstützen. Geben Sie in der Suchmaske des *Play-Stores* einfach den Suchbegriff „Samba“ ein, um diese Programme angezeigt zu bekommen. In den Darstellungen in diesem Kapitel wurde der „*ES Datei Explorer*“ (Version 3.2.4.1) verwendet.



Abb. 16: Einrichtung des Zugriffs auf ein Homeverzeichnis

Wenn die Einrichtung erfolgreich war, können Sie von dem *Android*-Gerät auf das Homeverzeichnis des Benutzers zugreifen, für den der Netzwerkzugriff eingerichtet wurde.

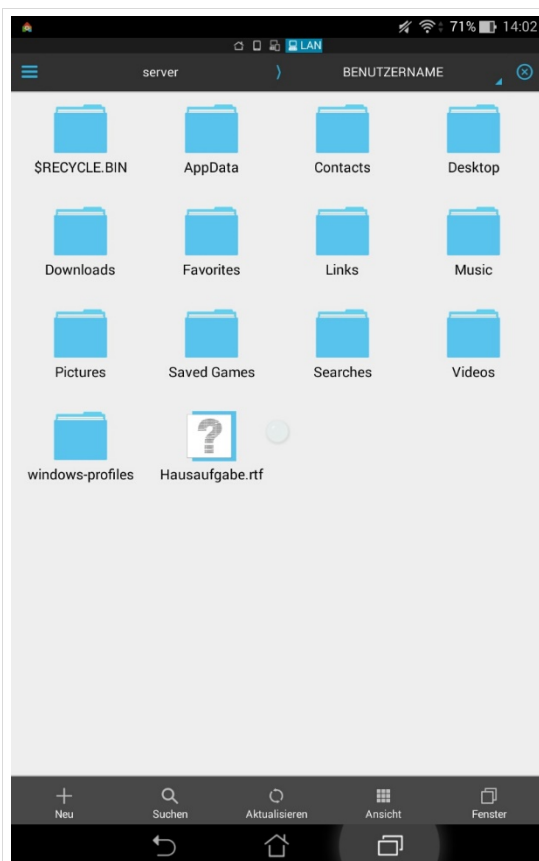


Abb. 17: Zugriff auf Homeverzeichnis eines Benutzers von einem Android-Gerät

6.2 iOS²³

6.2.1 Grenzen der Integration in die paedML

Im Consumer-Segment hat sich die Firma *Apple* eine treue Benutzergemeinde erarbeitet. Die Geräte werden für ihr intuitives Bedienkonzept und ihr Design gelobt. Der Einsatz von *iPads* in der Schule bietet sich vor allem deshalb an, weil die Geräte einfacher zu handhaben sind, als ein herkömmlicher PC.

Auch bei *iOS*-Geräten gilt, dass das Betriebssystem im Auslieferungszustand kein Mehrbenutzer-Betriebssystem ist, welches sich mit Bordmitteln in eine Domäne integrieren lässt. Auch hier scheidet die Nutzung von verschiedenen Anwendern, die sich an der Domäne anmelden und sofort auf ihre Ressourcen im Schulnetz zugreifen können, aus. Diese Geräte sind dafür ausgelegt, dass sie mit einem Benutzer-Konto betrieben werden, dessen Hoheit beim Hersteller (*Apple*) liegt. Mithilfe des „*Apple-Configurators*“²⁴ (Programm für die Verwaltung von iPads) lässt sich ein Gerät für den Gebrauch eines Benutzers konfigurieren, dieses Gerät kann anschließend jedoch nur von diesem Benutzer genutzt werden.

In der Standard-Installation bieten *iPads* keinen Dateibrowser, der auf Netzwerkressourcen zugreifen kann. Ein solches Programm muss über den *App-Store* bezogen und installiert werden.

Für die zentrale Verwaltung der Geräte wird – genau wie bei *Android*-Geräten – ein MDM-System benötigt. Hierfür gibt es verschiedene Anbieter, deren Produkte sich in Preis, Umfang und Bedienbarkeit unterscheiden. Für die Verwaltung mehrerer Geräte in einem angemessenen Rahmen sollte ein MDM-System unbedingt eingesetzt werden.

Bei der Integration eines *iPads* in die *paedML Linux* fiel auf, dass über den Standardbrowser *Safari* keine https-Verbindungen ins Internet aufgebaut werden konnten. Die Installation des *Chrome*-Browsers brachte hierbei Abhilfe, wobei das System die Proxy-Authentifizierung (siehe unten) nicht an Chrome weiter geleitet wurde und sich ein Benutzer vor dem Surfen am Proxy mit seinen *paedML* Benutzerdaten anmelden muss.

Im Gegensatz zu *Android* kann bei *iOS* der Proxy-Server an einer zentralen Stelle definiert werden. Dies wirkt sich auf alle Programme aus. Damit ist zum Beispiel ein Zugriff auf den *App-Store* möglich.

6.2.2 Einstellungen für den Internet-Zugriff

1. Zunächst müssen Sie die Geräte – wie im Administratorhandbuch beschrieben – in das pädagogische Netz aufnehmen. Wählen Sie für *iOS*-Geräte den Typ „Gerät mit IP-Adresse“.
2. Die Einstellungen des WLANs finden Sie über das Symbol „Einstellungen“ in den Verknüpfungen Ihres *iPads*.

²³ Die hier beschriebenen Verfahren wurden mit iOS 8 ausgearbeitet und getestet.

²⁴ <https://itunes.apple.com/de/app/apple-configurator/id434433123?mt=12>

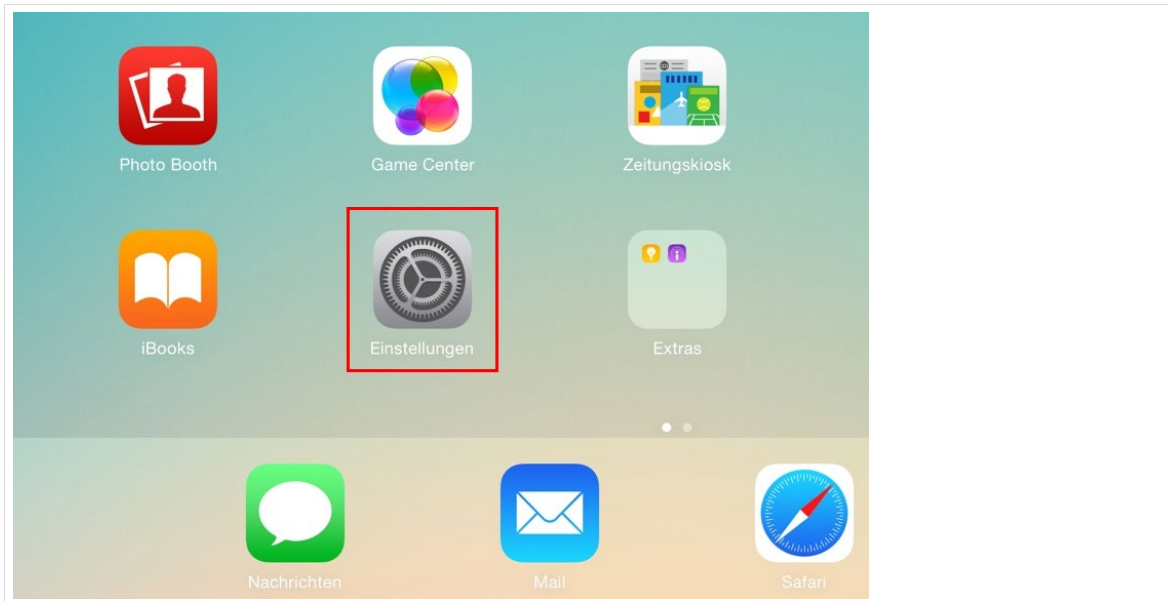


Abb. 18: Öffnen der Einstellungen des iPads

Navigieren Sie auf der linken Seite unter „Einstellungen“ zum Punkt „WLAN“ und wählen Sie das Netz, mit dem Sie sich verbinden wollen. Sie werden im nächsten Schritt dazu aufgefordert das Passwort für das WLAN einzugeben.

Nach erfolgreicher Anmeldung erscheint ein blauer Haken vor dem Netzwerk, mit dem die Verbindung besteht.

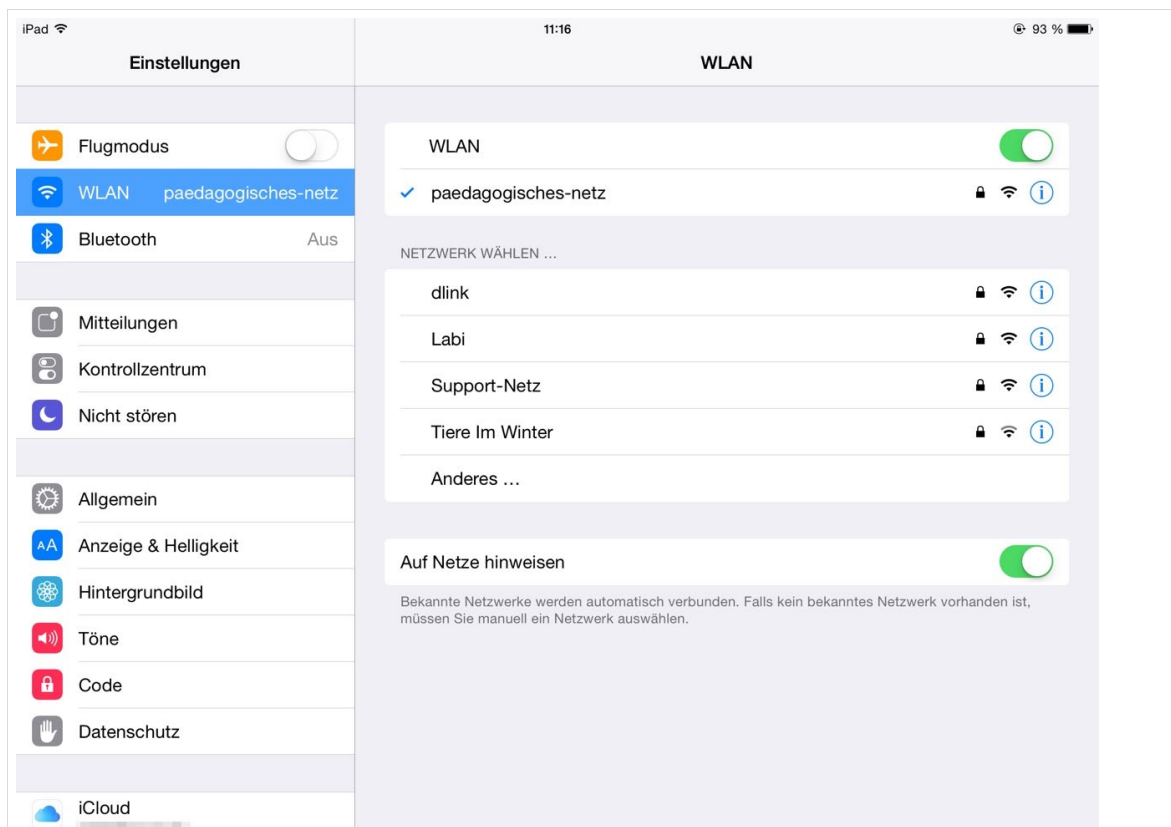


Abb. 19: Auswahl des WLANs

- Um auf das Internet zuzugreifen, muss der *Proxyserver* der *paedML* eingetragen werden. Dieser läuft auf der *IP-Adresse 10.1.0.1* und dort auf *Port 3128*.

Unter *iOS* wird der Proxy-Server zentral eingetragen und von allen Apps genutzt²⁵.

Klicken Sie auf die *WLAN-Verbindung*, um die Einträge vorzunehmen.

Über *DHCP* sollte das Gerät eine *IP-Adresse* erhalten haben.

Um auf das Internet zugreifen zu können, müssen Sie unter dem Abschnitt „*HTTP-PROXY*“ weitere Einstellungen vornehmen. Tragen Sie hier den *Proxyserver 10.1.0.1* und den *Port 3128* ein.

Für die Authentifizierung am Proxy werden außerdem der *Benutzername* und das *Passwort* eines *paedML Benutzers* benötigt.

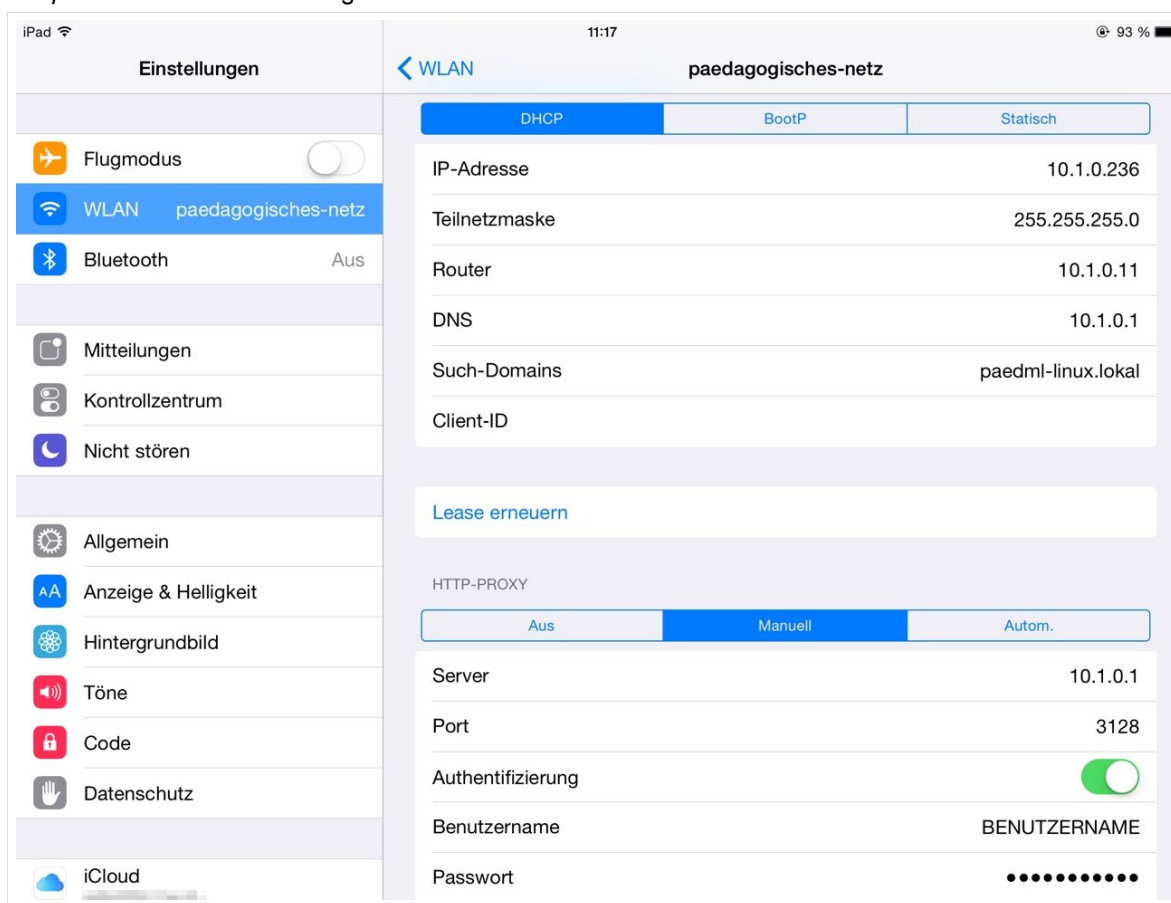


Abb. 20: Eintrag Proxy-Server

²⁵ Getestet mit iOS 8.

6.2.3 Zugriff auf das pädagogische Netz

Um auf das Home-Laufwerk eines Benutzers zugreifen zu können, müssen Sie sich aus dem *App Store* einen Dateibrowser laden, der auf Samba-Freigaben zugreifen kann. Zur Illustration des Zugriffs auf Serverdaten wurde die kostenlose Version des Programmes „*Remote File Manager*“ verwendet. Kostenlose Programmversionen können meist nur eine Netzwerkfreigabe speichern.

Um auf das Homeverzeichnis eines Benutzers zugreifen zu können, muss als Ziel für den Zugriff der Pfad *server/BENUTZERNAME* eingegeben werden. Auf Klassentausch-Verzeichnisse greifen Sie mit dem Pfad */server/schule-KLASSE* und auf Projekt-Tauschverzeichnisse mit *server/schule-PROJEKTNAME* zu.

Außerdem ist es notwendig die Login-Daten (*Benutzername* und *Kennwort*) des *paedML*-Benutzers einzutragen.

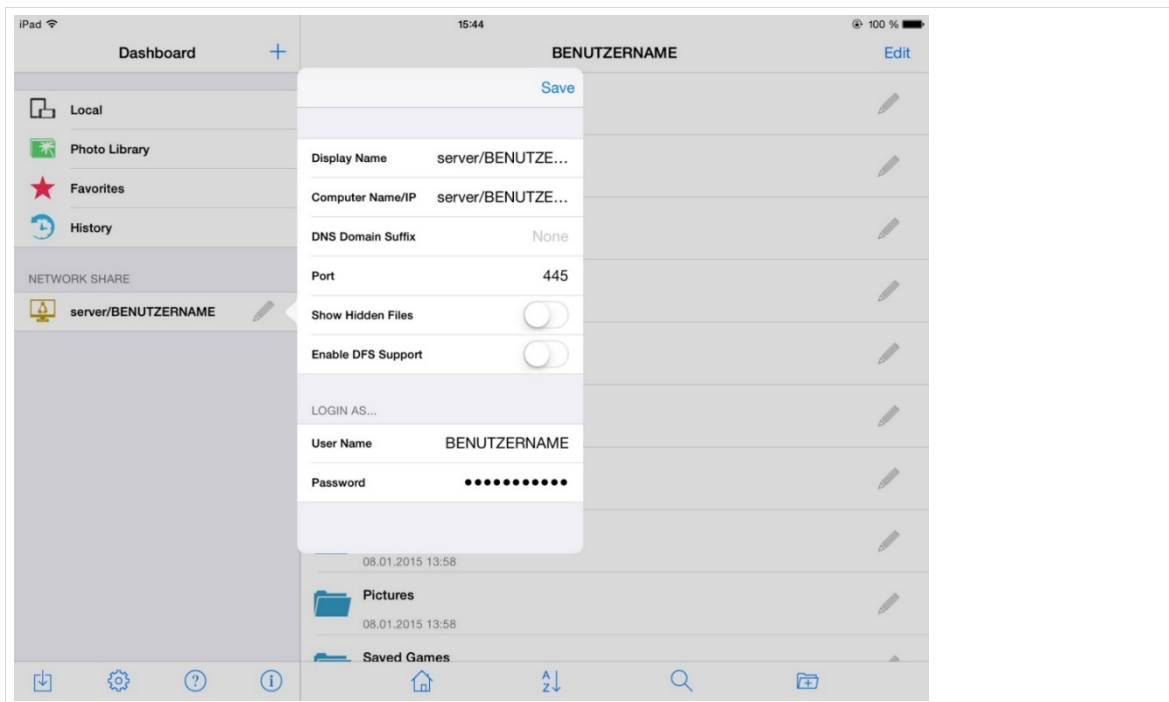


Abb. 21: Einstellungen des Dateibrowsers für den Samba-Zugriff

Wenn alle Daten eingetragen sind, können Sie anschließend auf das Homeverzeichnis des Benutzers zugreifen und dort Dateien bearbeiten.

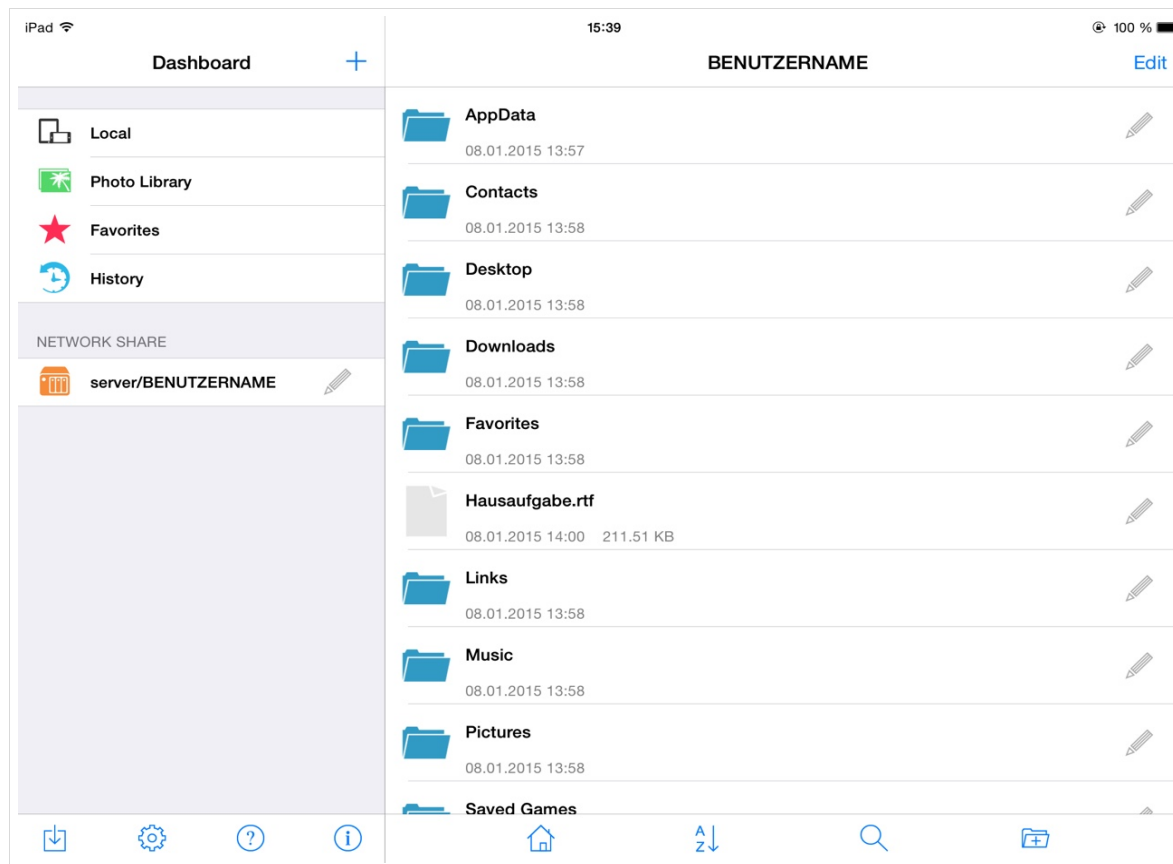


Abb. 22: Zugriff auf das Home-Verzeichnis eines Benutzers

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111
70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2015