

Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Anleitung

Administrationshandbuch

Stand 20.03.2024

paedML® Linux / GS

Version: 7.2

Impressum

Herausgeber

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

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ
Roland Walter, Michael Salm, Kay Höllwarth

Endredaktion

Alexander Vötterle

Bildnachweis

Symbole von "The Noun Project" (www.thenounproject.com)

Weitere Informationen

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

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2024

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

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1	Übersicht über die paedML Linux	12
1.1	Virtuelle Maschinen und Netze	12
1.1.1	Virtualisierung.....	13
1.1.2	Firewall pfSense.....	14
1.1.3	paedML Server.....	15
1.1.4	paedML opsi-Server.....	15
1.1.5	W10-AdminVM.....	16
1.1.6	Clients und Netzwerkgeräte	16
1.1.7	Gäste-Netz für schulfremde Geräte.....	16
1.1.8	Optional: MDM-Netz	17
1.1.9	Optional: Nextcloud und DMZ-Netz.....	17
1.2	Benutzerrollen der paedML Linux	17
1.3	Wichtige Administrationstools	18
1.3.1	Startseite.....	18
1.3.2	Schulkonsole	20
1.3.2.1	Der Aufbau der Schulkonsole	20
1.3.2.2	Navigation in der Schulkonsole	21
1.3.2.3	Schulkonsolenmodule	22
1.3.2.4	Favoriten	26
1.3.2.5	Benachrichtigungen.....	26
1.3.3	Univention Configuration Registry.....	27
1.3.4	opsi-configed editor	29
1.3.5	Startseite Nextcloud.....	29
1.4	Nützliche Werkzeuge.....	29
1.4.1	PuTTY – der Alternative Weg zur Serverkonsole	30
1.4.2	WinSCP und Explorer – Datenaustausch mit dem Server.....	31
1.4.3	Editoren.....	33
1.5	Allgemeine Hinweise	34
2	Unterrichtsorganisation und -steuerung	35
3	Benutzerverwaltung.....	36
3.1	Benutzerimport und Schuljahreswechsel.....	36
3.2	Anwender manuell hinzufügen	36
3.3	Benutzerdatensätze löschen	39
3.3.1	Daten gelöschter Benutzer	39
3.4	Änderung von Passwörtern	40
3.4.1	Änderung von Lehrer- und Schüler-Passwörtern	40
3.4.2	Änderung von Passwörtern administrativer paedML-Benutzer	41
3.4.3	Optional: Änderung der Passwörter für SQL-Server	42
3.5	Passwort des lokalen Windows-Administrators ändern.....	43
3.6	Passwort-Policy	45
3.6.1	Systemgenerierte Passwörter	45
3.6.2	Von Benutzern angelegte Passwörter	45
3.7	Anlegen von Arbeitsgruppen	45
4	Verwaltung von Geräten	46
4.1	Vorbemerkungen.....	46

4.1.1	Rechnertypen.....	47
4.1.2	Hinweise zum Rechnertyp „Windows-System“	48
4.2	Aufnahme von Geräten in das paedML Netz.....	48
4.2.1	Vorbereiten der Clients	50
4.2.2	Rechneraufnahme über die Schulkonsole.....	50
4.2.3	Aufnahme über Rechnerliste	53
4.2.4	Clients mit UEFI-Firmware.....	55
4.3	Geräte mit mehreren Netzwerkkarten (z.B. WLAN und Kabelnetzwerk).....	56
4.4	Integration von weiteren Geräten.....	59
4.5	Ändern und Löschen von Geräten.....	60
4.5.1	Neuer Name bestehender Geräte.....	60
4.5.2	Löschen bestehender Geräte.....	60
5	Verwaltung der Computerräume	62
5.1	Anlegen von Computerraum und Zuweisung von Geräten.....	62
5.2	Lehrercomputer definieren.....	64
5.3	Entfernen von Rechnern aus Computerräumen.....	65
5.4	Entfernen von Computerräumen.....	65
6	Einrichtung der Arbeitsplatzrechner	67
6.1	opsi-Lizenzierung.....	68
6.2	Unterstützte Betriebssysteme	68
6.3	Einführung in opsi	69
6.4	Start des opsi configurations editors	71
6.5	Die Benutzeroberfläche.....	72
6.6	Bereitstellen der Windows-Installationsdateien.....	80
6.7	Installation der Arbeitsplatzrechner	80
6.8	Treiberintegration.....	86
6.8.1	Identifizieren von Treibern.....	87
6.8.2	Einspielen von Treibern in das opsi-Depot	89
6.8.3	Integration der Treiber in die Installation	90
6.9	Hinweise zur Arbeit mit „product-properties“	91
6.10	opsi-Standard-Einstellungen („Produkt-Defaultproperties“).	92
6.11	Troubleshooting – Probleme beim Booten	95
6.11.1	Konfigurieren von Bootparametern	95
6.11.2	Anzeige der opsi-Konsolenausgabe im Fehlerfall.....	96
6.11.3	Log-Dateien zu Boot-Problemen	97
6.11.4	Besonderheiten beim UEFI-Boot	98
6.12	Windows 10 Funktionsupgrades (Build-Upgrades)	99
6.13	Windows 10 Qualitätsupdates (Hotfixes)	100
6.14	Einspielen von Software.....	101
6.15	Empfohlene opsi-Localboot-Produkte	103
6.16	Windows 10 Gruppenrichtlinien.....	108
6.17	Neuinstallation von Rechnern.....	111
6.18	Erstellen von opsi-Paketen.....	112
6.19	Einbindung von opsi-Paketen	112
6.20	Bearbeitung ganzer PC-Räume.....	115
6.21	PDF-Reports erstellen.....	117
6.22	Erneuerung des opsi-Lizenzschlüssel	120
7	Übernahme alter Rechner in die Domäne	121

7.1.1	Rechneraufnahme in die paedML	121
7.1.2	Einspielen von opsi-client-agent	121
7.1.3	Rechneraufnahme in die Domäne	123
8	Arbeiten mit lokalen Images von Rechnern	126
8.1	opsi-local-image-prepare	126
8.1.1	opsi-local-image-backup	126
8.2	opsi-local-image-restore	129
8.3	opsi-local-image-delimage	131
9	Capture-Images	133
9.1	Ablauf	134
9.2	Erstellen von Capture-Images	135
9.3	Einspielen eines Capture-Images	138
10	Gruppenrichtlinien für Windows-Clients	140
10.1	Gruppenrichtlinien in der paedML Linux	140
10.1.1	Aufruf der Gruppenrichtlinienverwaltung	140
10.1.2	Aufbau der Gruppenrichtlinienverwaltung	141
10.1.3	Übersicht über die Gruppenrichtlinien der paedML Linux	142
10.2	Änderung der Gruppenrichtlinien	142
10.2.1	Aktivieren und Deaktivieren von Gruppenrichtlinien	143
10.2.2	Optionale Gruppenrichtlinie Wechselmedienzugriff	144
10.2.3	Optionale Gruppenrichtlinie Lehrer	144
10.2.4	Optionale Gruppenrichtlinie Utilman	145
10.2.5	Bearbeiten von Gruppenrichtlinien	145
10.3	Desktop-Verknüpfungen mit Gruppenrichtlinien erstellen	149
10.4	Festlegen eines eigenen Hintergrundbildes	153
10.5	Zugriff auf Wechselmedien	154
11	Einrichtung von Druckern	155
11.1	Aufnahme des Druckers in die Domäne	156
11.2	Anlegen einer Druckerfreigabe	157
11.3	Bereitstellen von Druckertreibern für Windows	160
11.3.1	Treiber hochladen	161
11.3.2	Treiber an Drucker zuweisen	162
11.3.3	Standardeinstellungen setzen	164
11.4	Verteilung von Druckertreibern an Clients über opsi	164
11.5	Druckerzuordnung an Räume	166
12	Aktivierung von Windows / MS-Office	169
12.1	MAK-Proxy und VAMT-Service	169
12.1.1	Suche nach Microsoft-Produkten	169
12.1.2	Eingabe der Lizenzschlüssel	172
12.1.3	Aktivierung der Lizenzen	173
12.1.4	Sicherung der Lizenzinformationen	177
12.1.4.1	Sicherung über ein lokales Image auf den Rechnern	177
12.1.4.2	Sicherung der Lizenzinformationen von VAMT	177
12.1.5	Reaktivierung von Lizenzen nach Neuaufsetzen	177
12.2	KMS-Server	179
12.2.1	Aktivierung des KMS auf der W10AdminVM	179

12.2.2	Veröffentlichung des KMS	180
12.2.3	KMS-Aktivierung über das Volume Activation Management Tool (VAMT).....	183
13	Updates für die paedML Linux	183
13.1	paedML Linux Server	183
13.2	pfSense-Firewall.....	184
13.3	Updates/Hotfixes für Windows und opsi-Pakete	184
13.4	Übersicht über Updatezeiten	185
14	Steuerung der Internetzugriffe.....	186
14.1	Definition von Internetregeln	186
14.2	Internetregeln zuweisen.....	188
14.3	Unbeschränkten Internetzugriff für Lehrer	189
14.4	Verwendung eines externen Jugendschutzfilters (DNS-Filter).....	190
14.5	Protokollierung von Internetzugriffen.....	191
15	Nagios	194
15.1	Funktionsweise	194
15.2	Die Nagiosübersichtsseiten	195
15.3	Übersicht über die überwachten Dienste	197
16	Horde Groupware.....	200
16.1	Aufruf von Horde.....	200
16.2	Posteingang	201
16.3	Versand von E-Mails.....	202
16.4	Adressbuch	203
16.5	Änderung von Anhangsgrößen (Attachments).....	204
17	Verzeichnisstruktur Nutzerdaten.....	205
17.1	Anwendersicht auf Home-Verzeichnisse (H:\)	206
17.2	Administratorsicht auf /home	207
17.3	Tauschverzeichnisse für Gruppen (T:\)	208
17.4	Programmverzeichnis (K:\)	209
17.5	Für alle beschreibbares Share	210
18	Datensicherung und Datenwiederherstellung	213
19	Fernzugriff zur Wartung	213
19.1	Zugriff auf Teamviewer.....	213
19.2	Einrichtung von Teamviewer als Systemdienst	214
20	Unterrichtszeiten	217
21	Known Issues	219
21.1	Lehrertauschverzeichnis.....	219
21.2	Probleme bei der Domänenanmeldung	219
21.3	Internetzugriff für Apps.....	219
21.4	Materialverteilung – Dateigröße	220
Anhang A Nomenklatur		221
Anhang B Vervollständigen der opsi-Pakete für die Windows-Installation		223

Einführung

Vielen Dank, dass Sie sich für die *paedML Linux* entschieden haben. Die Arbeit mit Computern bietet täglich vielfältige Herausforderungen, denen Sie sich als IT-Verantwortlicher Ihrer Schule stellen müssen. Wir hoffen, dass wir mit unserem Produkt dazu beitragen, dass Sie die an Sie gestellten Aufgaben meistern und Spaß an der Arbeit als Netzwerkberater haben.

Die *paedML Linux* ist seit der Version 6.0 eine Neuentwicklung, die im Vergleich zu ihren Vorgängerversionen mit einem komplett neuen Server- und Clientmanagement ausgestattet wurde. *Univention Corporate Server („UCS“ mit der Applikation UCS@school)* bilden nun die technologische Plattform für die Schul-IT-Komplettlösung. Damit ist die *paedML* hervorragend geeignet, um IT-Infrastrukturen im Schulumfeld bereitzustellen und zu verwalten. Für Lehrkräfte wurde die Anwenderoberfläche neugestaltet und mit einer intuitiven „*Schulkonsole*“ ausgestattet. Hinzugekommen sind neue Steuerungsfunktionen, die den Lehrkräften noch mehr Sicherheit beim Unterrichten geben (zum Beispiel „Schülercomputer steuern“, „Klassenarbeiten schreiben“, „Internet verwalten“ oder „Drucker moderieren“). Die neue Version ermöglicht deutlich mehr Mobilität beim Lernen, denn Schülerinnen und Schüler können auch mit ihren privaten Geräten im „Gäste-Netz“ der Schule arbeiten (*Bring Your Own Device*). Schuleigene Geräte sind im pädagogischen Schulnetz integriert.

Neben den Verbesserungen für den aktiven Unterrichtablauf bringt die *paedML Linux* auch für Netzwerkbetreuer deutliche Arbeitserleichterungen mit sich: Viele Installationsroutinen wurden automatisiert. Das beginnt mit einem vereinfachten und weniger fehleranfälligen Installationsverfahren der *paedML*-Server mittels Virtualisierung. Außerdem erfolgen Betriebssysteminstallation und Softwareverteilung weitgehend automatisch mit der Open Source Software *Open Server Integration* – kurz: *opsi*. Die Restaurierung wurde ebenso deutlich verbessert, sodass jetzt einzelne oder die gesamten Schüler-Computer in einem Klassenraum innerhalb kürzester Zeit mittels zentraler Steuerung wiederhergestellt werden können.

Mit der *paedML Linux* haben Sie sich für eine moderne IT-Lösung entschieden, die mit einem professionellen technischen Unterbau ausgestattet ist. Verlässlichkeit und Stabilität kennzeichnen die neue Version, denn Hardwareunterstützung und die Handhabung wurden deutlich verbessert. Technologisch gesehen ist die *paedML Linux* stärker modular aufgebaut, wodurch die weitere Produktentwicklung in Zukunft flexibler gestaltet werden kann. Wir sind an der Rückmeldung unserer Kunden interessiert und wenn Sie Anregungen oder Wünsche für die Weiterentwicklung der *paedML* haben, bitten wir Sie um Rückmeldung, z. B. über unseren User-Helpdesk.

Die Mitarbeiter der Hotline stehen Ihnen mit Rat und Tat zur Seite, um Sie in der Administration Ihres schulischen Netzwerks zu unterstützen. Die Erfahrung hat gezeigt, dass es ratsam ist lieber einmal zu viel, als einmal zu wenig in der Hotline anzurufen. Wenn Sie Fragen zu Ihrer *paedML Linux* haben, dann kontaktieren Sie bitte Ihre Supportmitarbeiter.

Linux-Hotline

0711 – 25 35 83 88

linux-hotline@lmz-bw.de

Geschäftszeiten:

montags - donnerstags 8.00 - 16.00 Uhr

freitags 8.00 - 14.30 Uhr

Grundschul-Hotline

0711 - 25 35 83 91

gs-hotline@lmz-bw.de

montags - donnerstags 8.00 - 16.00 Uhr

freitags 8.00 - 14.30 Uhr

Dokumentationen zur *paedML Linux*

Es gibt drei Handbücher für die *paedML Linux*, die sich an verschiedene Zielgruppen richten:

- Das hier vorliegende „**Administrationshandbuch**“ richtet sich an den Netzwerkberater als Systembetreuer der Schule und an den Dienstleister. Hier werden administrative Aufgaben beschrieben, die im Schulalltag getätigt werden können. Darüber hinaus werden hier auch administrative Aufgaben bei der Einrichtung des Schulnetzes beschrieben, die primäre Aufgaben des Dienstleisters sind, der das Schulnetz einrichtet.
- Die „**Installationsanleitung**“, welche die Einrichtung von *VMware*, das Aufsetzen der *paedML* Infrastruktur und den technischen Aufbau des *paedML*-Netzwerks behandelt, richtet sich ausschließlich an Dienstleister.
- Das „**Handbuch für Lehrkräfte**“, welches die pädagogischen Funktionen Ihrer *paedML Linux* näher beschreibt, erläutert relevante Module für den Unterricht.

Neben diesen drei Handbüchern gibt es weitere Dokumente, die Sie bei der Planung und dem Aufbau eines *paedML Linux* Netzwerkes unterstützen.

- Der „**Konzeptionsleitfaden**“ bietet eine kurze Einführung in die *paedML Linux*. Dieses Dokument enthält Hinweise zur Planung der Installation des schulischen Netzwerkes.
- Hinweise für die Ausschreibung des schulischen Netzes und bei der Übergabe des Netzwerks von Ihrem Dienstleister an die Schule finden Sie in unserem „**Ausschreibungsleitfaden**“.
- In einem weiteren Dokument haben wir die „**Hardwareanforderungen**“ der *paedML Linux* zusammengefasst.

Um inhaltliche Doppelungen zu vermeiden, verweisen wir mit Link an gegebener Stelle auf andere Handbücher.

Alle hier genannten Handreichungen zur *paedML Linux* finden Sie unter <https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/>.

Überprüfen Sie diese Seite bitte regelmäßig nach Aktualisierungen!



Anmerkung zum vorliegenden Administrationshandbuch:

Das vorliegende Handbuch richtet sich an die Systemrollen „*Dienstleister*“ und „*Netzwerkberater*“. Leider sind die Aufgaben der beiden Rollen nicht immer klar voneinander zu trennen, da sowohl der Dienstleister als auch der Netzwerkberater administrative Aufgaben übernehmen.

In diesem Handbuch finden Sie daher mehr Informationen, als Ihnen als Netzwerkberater recht sein dürfte! Aber vielleicht nicht genug, um den „Geek“ (Streber) unter den Netzwerkberatern zufrieden zu stellen?

Als Anbieter der *paedML Linux* stellen wir fest, dass die Bandbreite schulischer Anforderungen in den letzten Jahren immer größer geworden ist. Das hängt zum Beispiel mit den veränderten Lern- und Schulformen und dem Wunsch nach mehr Mobilität und Kollaboration beim Lernen zusammen. Parallel dazu wurden verbesserte Technologien für schulische IT-Lösungen entwickelt, die wir u.a. auch in der *paedML* integriert haben, um den Wünschen der Schulen gerecht zu werden. Technisch gesehen ist die *paedML* deutlich innovativer, flexibler und komfortabler

geworden. Andererseits hat die Komplexität zugenommen, weil das Spektrum an Möglichkeiten größer geworden ist.

Wir hoffen, dass uns mit unseren Handreichungen der Spagat zwischen diesen unterschiedlichen Anforderungen gelingt.

Wir möchten Sie ausdrücklich darauf hinweisen, dass es nicht Aufgabe des Netzwerkberaters sein sollte, das schulische Netzwerk allein zu betreuen. Hilfe des Dienstleisters sollte bei Bedarf in Anspruch genommen werden. Wir möchten Sie dennoch dazu ermutigen, bei Bedarf jederzeit unsere Hotline-Kollegen, als Ansprechpartner für die Administration der *paedML Linux* bzw. der *paedML für Grundschulen* zu kontaktieren.

Wenn Sie konkrete Anmerkungen zu unseren Dokumentationen haben, dann freuen wir uns auf Ihre Rückmeldung unter

linux-hotline@lmz-bw.de bzw. gs-hotline@lmz-bw.de

Typografische Konventionen

Zur besseren Lesbarkeit werden bestimmte Elemente typografisch vom Rest des Textes abgehoben.

- Hervorhebungen in diesem Dokument sind *kursiv*.
- **Besondere Hervorhebungen** sind **fett** ausgezeichnet.
- Ausgaben oder Abfragen von Programmen sind „*kursiv und erhalten Anführungszeichen*“. Ebenso werden Menüs oder Knöpfe, in Programmen und Bedienoberflächen mit Anführungszeichen hervorgehoben.
- Vom Benutzer auszuführende Tastatureingaben an der *Linux*-Konsole oder an der *Windows* Eingabeaufforderung (zum Beispiel Systembefehle) sowie Auszüge aus Systemdateien, werden durch die Darstellung in Courier New vom Rest des Textes abgesetzt. Das Gleiche gilt für Zugangsdaten wie Benutzernamen oder Passwörter.
- Tastenbeschriftungen werden durch Rahmen hervorgehoben.
- Verschachtelte Menüstrukturen werden durch einen senkrechten Strich (|) als Trennzeichen (in der *Linux* Welt auch „*Pipe*“¹ genannt) voneinander getrennt. So finden Sie zum Beispiel den Zugriff für das Helpdesk-Modul (vgl. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**, Seite **Fehler! Textmarke nicht definiert.**) unter „*Schulkonsole: Unterricht | Helpdesk kontaktieren*“.

Unter einigen Kapitelüberschriften finden Sie einen Hinweis, wie Sie den in dem Kapitel beschriebenen Baustein der *paedML Linux* aufrufen können. In der Regel werden konfigurative Änderungen, die in diesem Handbuch beschrieben sind, vom Netzwerkberater ausgeführt. Manche Menüs sind jedoch nur für den Administrator zugänglich. Diese Ausnahmen werden durch Nennung des vom Benutzer „*netzwerkberater*“ abweichenden Benutzernamens gekennzeichnet.

¹ http://de.wikipedia.org/wiki/Pipe_%28Informatik%29

Beispiele:

Aufruf über Schulkonsole (netzwerkberater): Schul-Administration | Benutzer (Schulen)

Adresse: <https://server.paedml-linux.lokal/nagios>



Der Aufruf aller internen Webseiten der *paedML Linux* muss über den FQDN (voll qualifizierten Domain-Namen) der jeweiligen Seite geschehen.

Es genügt also nicht bspw. <https://server/horde> einzugeben, um die Startseite des Webmailers aufzurufen.

Nutzen Sie stattdessen <https://server.paedml-linux.lokal/horde>.

Hinweise und Tipps werden durch besondere Symbole grafisch vom Text abgehoben:



Durch Hinweis-Felder werden Sie auf Sachverhalte hingewiesen, die Sie beachten sollten, um bestimmte Probleme zu vermeiden, die den Betrieb der *paedML Linux* beeinträchtigen könnten.



Das Tipp-Feld gibt Hinweise, die nicht zwingend notwendig, aber hilfreich sind.



Dieses Feld kennzeichnet Inhalte, die nicht von der Hotline unterstützt werden.

Es handelt sich um Funktionen und Programme, die nicht Bestandteil der Entwicklung der *paedML Linux* sind. Diese Programme sind in der Regel zu komplex und zu umfangreich, um in Ihrer Tiefe durch die Hotline unterstützt werden zu können.

Andererseits bewirken Änderungen in den beschriebenen Funktionen, Abweichungen von Standardeinstellungen der *paedML Linux*².

Aufgrund der besseren Lesbarkeit wird in diesem Handbuch die männliche Form verwendet. Die weibliche Form ist selbstverständlich immer miteingeschlossen.

² In der Entwicklung unserer Produkte setzen wir Standards, die durch die Hotline unterstützt werden (können). Wir bitten Sie um Verständnis, dass es unseren Mitarbeitern nicht möglich ist, auf alle Bedürfnisse in Detail einzugehen. Wir können Ihnen bei manchen Anfragen lediglich Hinweise geben, wie Sie Änderungen am System vornehmen oder wo Sie weitere Dokumentationen zu dem Thema finden können.

1 Übersicht über die paedML Linux

Die *paedML Linux* bietet viele Neuerungen im Vergleich zu Ihren Vorgängerversionen. Wir wollen Ihnen hier zunächst einen Überblick über die Infrastruktur Ihres Netzwerkes geben (Kapitel 1.1, Seite 12), dann werfen wir einen kurzen Blick auf Benutzerrollen, die in der *paedML Linux* zum Einsatz kommen (Kapitel 1.2, Seite 17). Das darauffolgende Unterkapitel (Kapitel 1.3, Seite 18) beschreibt die Werkzeuge, die Ihnen für die Konfiguration der *paedML Linux* zur Verfügung stehen. Im Anschluss an dieses Kapitel erhalten Sie eine Übersicht über nützliche Werkzeuge, die den Systemadministrator bei der Arbeit unterstützen (Kapitel 1.4, Seite 29), sowie ein paar allgemeine Tipps.

1.1 Virtuelle Maschinen und Netze

In der folgenden Grafik sehen Sie ein *paedML Linux* Netzwerk. Beachten Sie im Zusammenhang mit der Adressierung der Geräte bitte auch die Tabelle auf Seite 47. In diesem Unterkapitel werden wir uns einen Überblick über die Rechner verschaffen, die im Netzwerk der *paedML Linux* zum Einsatz kommen.



Wenn eine Erweiterung des Schulnetzwerks um weitere IP-Adressen gewünscht ist, dann sind folgende Schritte zu tun:

- Die Erweiterung der Netze wird mit VLANs realisiert.
- Die VLANs sind serverseitig schon eingerichtet.
- Die VLANs sind auf der Switchebene noch einzurichten.

Detaillierte Informationen zur Netzerweiterung der *paedML Linux* / GS entnehmen Sie dem HowTo „Netzerweiterung in der *paedML Linux*“ unter <https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads#howtos>.

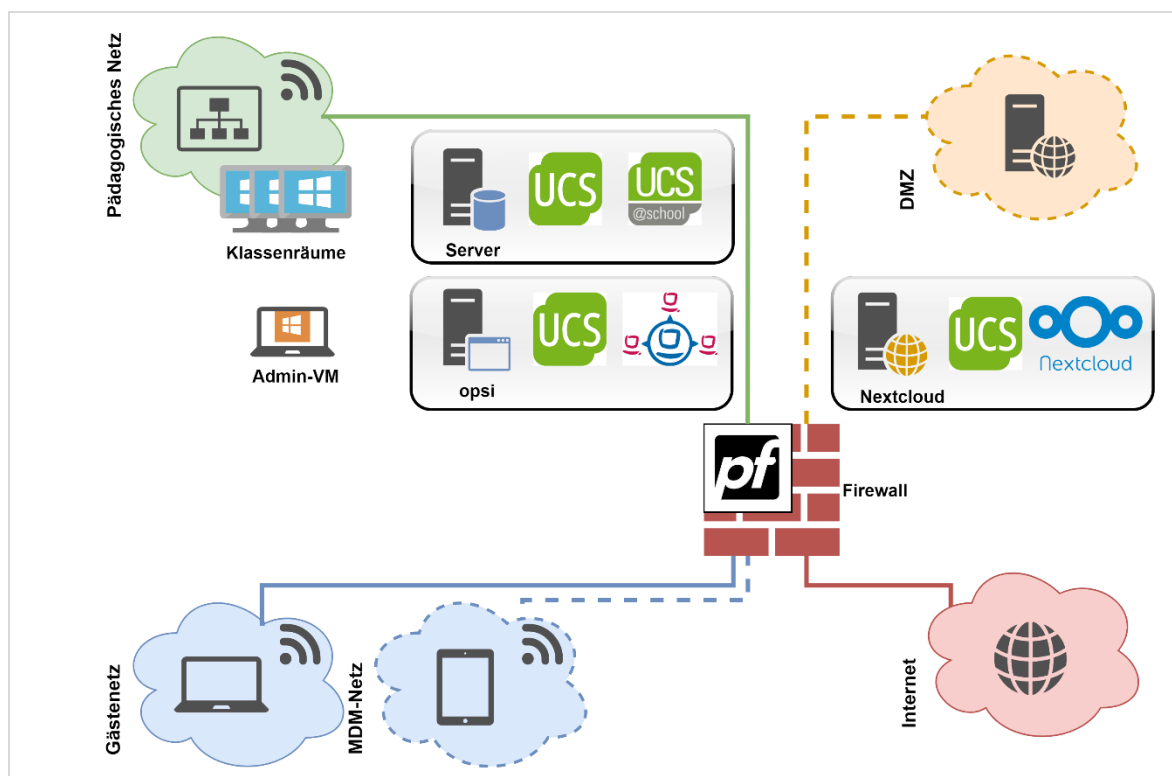


Abb. 1: Übersicht über die *paedML Linux*

1.1.1 Virtualisierung

Die Server der *paedML Linux* werden virtualisiert ausgeliefert. Virtualisierung hat den großen Vorteil der Hardware-Unabhängigkeit. Sie benötigen also keine Treiber für Hardwarekomponenten, wenn Sie in einer virtualisierten Umgebung installieren.

Wir empfehlen für die Virtualisierung ausdrücklich einen aktuellen VMware ESX(i) Hypervisor³. Auf solchen Systemen wird die *paedML Linux* auch in Zukunft weiterentwickelt und getestet. Die *paedML* läuft zwar auch auf einem anderen Hypervisor, die Hotline leistet allerdings nur für Systeme Unterstützung, die mit *VMware* installiert werden.

Die nächste Abbildung zeigt eine schematische Darstellung des Netzwerks der *paedML Linux*. Der Übersichtlichkeit wegen wurde auf Netzwerkkomponenten wie Switches etc. verzichtet.

In der Virtualisierungsschicht (gelb) befinden sich die *paedML Server*, deren virtuelle Netzwerkkarten über virtuelle Switches („v-Switches“) auf physikalische Netzwerkkarten auf der Hardwareebene (grau) des Virtualisierungsservers verweisen. Zwischen der Hardwareebene und den virtuellen Maschinen liegt der Hypervisor (blau), der auch „Virtualisierungsschicht“ genannt wird.

³ Bitte entnehmen Sie die Version den Releasenotes der jeweiligen *paedML Linux* Version.

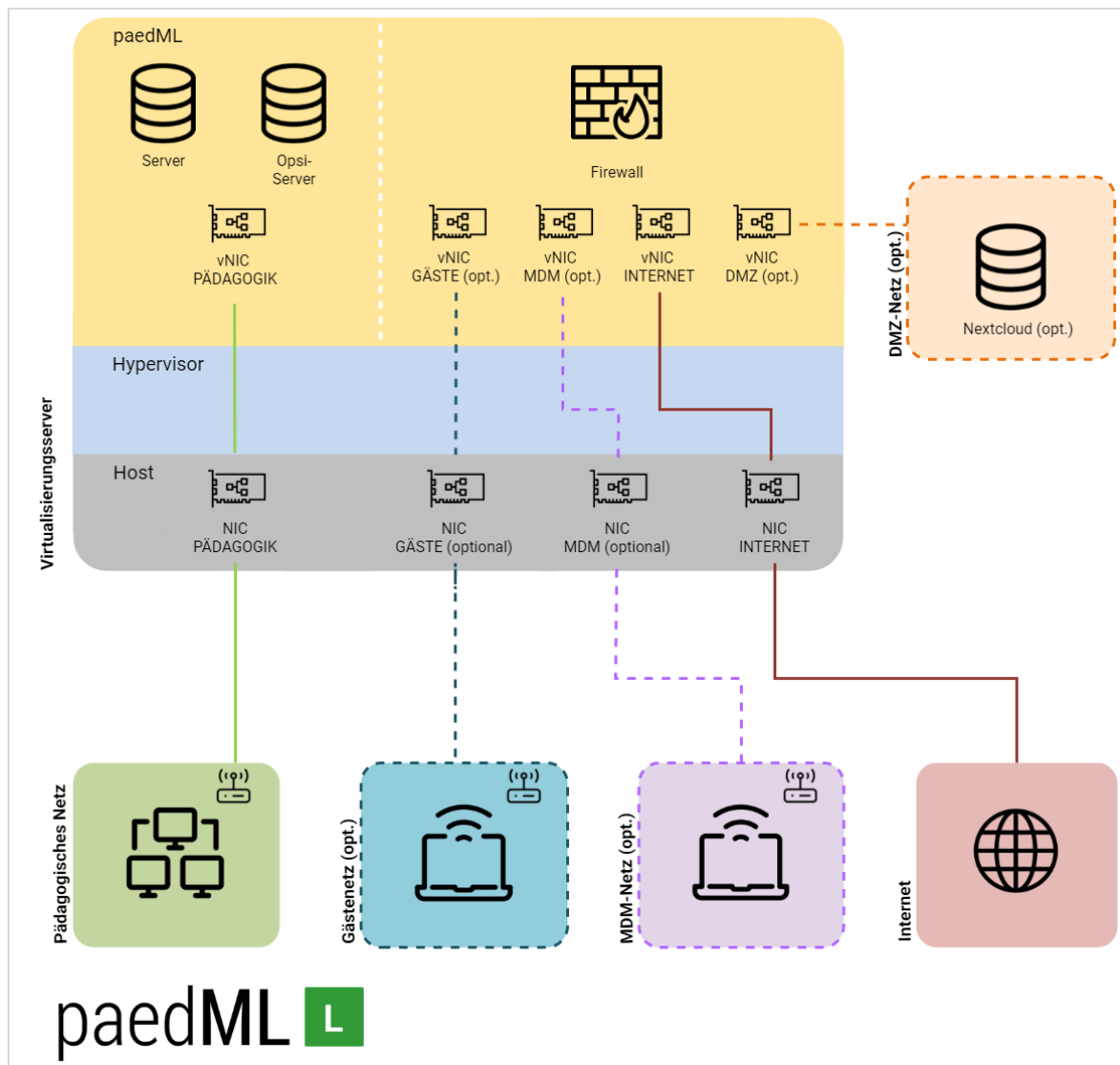


Abb. 2: Schematische Darstellung der Virtualisierung

1.1.2 Firewall pfSense

DNS-Name: firewall.paedml-linux.lokal – **IP-Adresse:** 10.1.0.11

Die Firewall steht als Gateway zwischen dem internen pädagogischen Netzwerk und dem Internet. Sie schützt vor Angriffen von außen und regelt, welche Dienste aus dem schulischen Netzwerk Verbindungen nach außen aufbauen dürfen. Auf dem System ist die auf *FreeBSD* basierende Distribution *pfSense* installiert. Nach der initialen Einrichtung während der Installation des Schulnetzwerkes muss diese Maschine in der Regel nicht weiter konfiguriert werden.

Auf der Firewall läuft ein Zeitserver, über den die Server im Schulnetz mit der aktuellen Uhrzeit versorgt werden. Die Rechner im Schulnetz synchronisieren wiederum Ihre Zeit mit den *paedML*-Servern.

Sie haben die Möglichkeit über ein zusätzliches Netzwerk an der Firewall ein WLAN für schulfremde Geräte in Ihrer Schule einzurichten. Dieses WLAN wird als Gäste-Netz bezeichnet.

Die Firewall wird durch Ihren Dienstleister eingerichtet. Ein Zugriff auf die Konfigurationsoberfläche sollte nicht notwendig werden.

Einige Anpassungen sind im Anhang dieses Dokumentes beschrieben. Wenn Sie weitergehende Änderungswünsche bezüglich der Firewall-Konfiguration haben, wenden Sie sich bitte an ihren Dienstleister oder an die Hotline.

1.1.3 paedML Server

DNS-Name: server.paedml-linux.lokal – **IP-Adresse:** 10.1.0.1

Die *paedML* wird mit zwei virtualisierten Servern ausgeliefert. Der eine ist der Master-Server (Server), der andere der opsi-Server. Auf den beiden *paedML* Servern werden verschiedene Dienste, die für den Betrieb der *paedML Linux* notwendig sind, ausgeführt. Hierfür werden manche Dienste auf einer Maschine zur Verfügung gestellt, andere Dienste werden von beiden Systemen ausgeführt.

Die *paedML* Server sind DNS-Server für das interne Netzwerk. Sie brauchen sich beim Betrieb der *paedML* keine IP-Adressen von Maschinen zu merken. Via Namensauflösung sind alle Geräte im schulischen Netzwerk erreichbar.

Auf dem Server laufen – neben den Standard-*Linux* Systemdiensten – weitere Dienste wie z.B.:

- *Samba 4* – als Domänencontroller mit Active Directory Funktionen
- *Nagios* – ein Werkzeug zur Überwachung verschiedener Parameter Ihrer Hardware und Ihres Netzwerkes
- *Horde* – die Groupware in der *paedML Linux*

Sie können auf diese Funktionen über die Startseite des Servers (siehe auch Kapitel 1.3.1, Seite 18) zugreifen.



Die *paedML Linux* wird mit zwei virtualisierten Servern ausgeliefert. Wir bitten Sie darum, diese beiden Server **IMMER** gleichzeitig zu betreiben, damit die im Hintergrund laufenden Dienste gewährleistet sind.

1.1.4 paedML opsi-Server⁴

DNS-Name: backup.paedml-linux.lokal – **IP-Adresse:** 10.1.0.2

Auf dem *opsi*- oder *Backup-Server* ist *opsi* (zur Verwaltung von *Windows*rechnern) installiert. Hier laufen die *opsi*-Dienste, durch die die *Windows*-Clients installiert und mit Software versorgt werden. Der Name *Backup-Server* ist historisch aus der Systemrolle im *Univention-Corporate-Server*-Kontext übernommen. In der *paedML Linux* bekommt dieses System als zentrale Aufgabe die Clientverwaltung mit *opsi*. Daher wird das System auch als *opsi-Server* bezeichnet.

⁴ Aus Gründen, die dem Unterbau auf *Univention Corporate Server* geschuldet sind, lautet die Bezeichnung an manchen Stellen auch „*backup-Server*“.

Im „opsi-Depot“ werden Pakete von *Windows*programmen, Installationsimages des Betriebssystems und Systemwerkzeuge abgelegt, die benötigt werden, um einen *Windows*rechner auszuspielen, mit Software zu versorgen und/oder zu warten.

Sie können auf die *opsi*-Konfiguration über die Startseite des Servers (siehe auch Kapitel 1.3.1, Seite 18) zugreifen.



Sowohl Ihr Server als auch Ihr *opsi*-Server können über die in dieser Anleitung beschriebenen Werkzeuge (wie zum Beispiel die Schulkonsole) konfiguriert werden. Die Standardkonfiguration des *opsi*-Servers sollte nicht durch Sie oder Ihren Dienstleister verändert werden.

1.1.5 W10-AdminVM

DNS-Name: AdminVM.paedml-linux.lokal – IP-Adresse: 10.1.0.13

Es gibt einige Services für den Betrieb der paedML-Linux, die auf einer Windows-Maschine laufen müssen. Dafür ist die virtuelle Maschine W10-AdminVM vorgesehen.

Vorteile des Einsatzes eines auf Windows 10 basierenden Administratorrechners bietet u.a. der in Windows 10 integrierte SSH-Zugriff oder die umfassenderen Möglichkeiten von DISM. Auf der W10-AdminVM sind überdies hilfreiche Tools (z. B. LDAP-Admin) zur Administration vorinstalliert.

Außerdem werden die Verwaltung von Windows- und Office-Lizenzen und die Druckverwaltung verbessert.

Das vorinstallierte Windows-10-System der AdminVM muss lizenziert werden.

1.1.6 Clients und Netzwerkgeräte

DNS-Name: Computername – IP-Adresse: wird bei Rechneraufnahme vergeben

Die Geräte der *paedML Linux* bekommen bei der Aufnahme in die *paedML* eine feste Systemrolle zugewiesen, von der abhängt, wie ein Client verwaltet wird.



Als Client-Betriebssysteme wird die deutsche Version von *10 Education* (64-Bit) Build 20H2 und 21H2 (Voraussetzung: *opsi* 4.2) unterstützt. Andere Versionen sollten **nicht** auf dem OPSI-Server eingespielt werden.

1.1.7 Gäste-Netz für schulfremde Geräte

Das Schulnetz wird durch ein zusätzliches Netzwerk, das *Gäste-Netz*, erweitert.

Wir raten Ihnen aus Sicherheitsgründen dringend dazu, schulfremde Geräte NICHT in das Schulnetz aufzunehmen, sondern über das Gäste-Netz an die IT-Infrastruktur anzubinden.

Besonderheiten:

- Eigenes, vom Schulnetz getrenntes Netz. Adressbereich 172.16.0.0/12 (IP-Adressen von 172.16.0.1 – 172.31.255.254)
- IP-Adressierung per DHCP oder feste IP-Vergabe möglich.
- Keine Anmeldung an schulischen Ressourcen, wie Home- oder Tauschverzeichnissen.

- Proxy-Authentifizierung für Internetaufrufe. Anmeldung mit Domänenkonto (Benutzername und Passwort wie im Schulnetz).
- In den Standardeinstellungen ist nur ein Zugang zu den Protokollen http und https, also nur das Surfen im Internet offen.
- Webfilterung wie im pädagogischen Schulnetz.

In der Anleitung „WLAN in der *paedML Linux*“ finden Sie weitere Informationen zur Einrichtung des Gäste-Netzes: <https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#howtos> .

1.1.8 Optional: MDM-Netz

Viele Schulen setzen mittlerweile 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.

In der *paedML Linux* und GS wird deshalb ein weiteres Netz „MDM“ verwendet. 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.

Das Dokument „*Tablet-Integration in die paedML Linux und GS mit Schwerpunkt iOS*“ finden Sie im Downloadbereich der *paedML Linux* unter <https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#manuals> .



Bestandskunden müssen das MDM-Netz durch einen Dienstleister auf dem ESXi-Host nachinstallieren lassen. Bei Neukunden ist das MDM-Netz nach der Installation bereits vorkonfiguriert.

1.1.9 Optional: Nextcloud und DMZ-Netz

Die Nextcloud wird als vorinstalliert App auf einer Virtuellen Maschine (VM) ausgeliefert. Diese wird auf dem bestehenden ESXi-Host der Schule importiert. Das Betriebssystem dieser VM ist das bereits vom Server und opsi-Server der *paedML Linux* und GS bekannte linuxbasierte UCS der Firma Univention.

Die Nextcloud-VM wird in einem eigenen Netzsegment, der DMZ, installiert. Dieses ist nötig, um die Sicherheit des Schulnetzwerkes bei Zugriffen von außerhalb auf die Nextcloud zu schützen.

Die Nextcloud-Installationsanleitung ist unter <https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#manuals> zu finden.

1.2 Benutzerrollen der *paedML Linux*

Um die einzelnen Bereiche wie Unterricht, Pflege der Nutzerdaten und Administration voneinander zu trennen, gibt es in der *paedML Linux* verschiedene Benutzerrollen mit unterschiedlichen Berechtigungen. Die verschiedenen Rollen bestimmen auch darüber, welche Module die Anwender in der *Schulkonsole*

angezeigt bekommen. Die Benutzerrollen werden in *nicht administrative* und *administrative* Benutzer unterschieden.

1. Nicht administrative Benutzerrollen:

- 1.1. Mitglieder der Gruppe *Schüler* erhalten in der Standardeinstellung nur Zugriff auf Ihr eigenes Kennwort. Sie können sich mit ihren Benutzerkonten an Windows-Clients anmelden und die für sie freigegebenen Dateifreigaben und Drucker verwenden.
- 1.2. *Lehrer* haben gegenüber Schülern zusätzliche Funktionen in der *Schulkonsole*, mit denen Sie z.B. auf *Schulkonsolenmodule* zugreifen können, die das Zurücksetzen von Schülerpasswörtern oder das Auswählen von Internetfiltern ermöglichen. Für die Steuerung des Unterrichts sind pädagogische Funktionen ebenso enthalten.

2. Administrative Benutzerrollen:

- 2.1. Um administrative Aufgaben im Netz auszuführen, wurde der Benutzer *netzwerkberater* als *paedML*-eigener Benutzer eingeführt.
- 2.2. Der Benutzer *domadmin* ist **ausschließlich** für die Rechneraufnahme über die *Schulkonsole* oder den Domänenbeitritt bei der Clientaufnahme erstellt worden. **Mit diesem Konto sollten Sie sich nicht im Schulnetz anmelden.**
- 2.3. Vollen Zugriff auf die Administrationsfunktionen der *Schulkonsole* erhält der *Administrator*. Er kann neben den *paedML*-Funktionen auch Einstellungen auf der Betriebssystemebene des Servers vornehmen. Dieses Konto sollte **NUR** bei der Einrichtung des Servers oder dann, wenn es die hier beschriebenen Änderungen erfordern, benutzt werden. Das Benutzerprofil *Administrator* sollte nur dann zum Einsatz kommen, wenn Sie genau wissen, was sie ändern. **Mit diesem Konto sollten Sie sich nicht an einem Client im Schulnetz anmelden.** Eine Dokumentation Ihrer Änderungen hilft bei der späteren Fehlersuche durch die Hotline oder den Dienstleister!
Der Benutzer *Administrator* kann zudem Änderungen an der Firewall vornehmen und ist administrativer Benutzer des Clientmanagements *opsi*.



Systeminterne Informationen oder Störungen werden per E-Mail an das Konto *netzwerkberater* gesendet. Dieses Konto ist mit einer internen Mailadresse angelegt und muss nicht konfiguriert werden.

1.3 Wichtige Administrationstools

1.3.1 Startseite

Adresse: <https://server.paedml-linux.local>

Sie erreichen den Server der *paedML Linux* über die folgende URL: <https://server.paedml-linux.local>



Wir empfehlen Ihnen ausdrücklich, administrative Aufgaben über diese Adresse auszuführen. Dort finden Sie eine Übersicht mit allen wichtigen Links zur *paedML Linux*, z.B. über die in der *paedML* verfügbaren Dienste und über externe Angebote, wie z.B. www.lmz-bw.de.

Wie bereits oben beschrieben, müssen Sie in der Regel **nichts** am *Backup-Server* ändern. Im Folgenden werden daher nur die Administratortools des Servers beschrieben.

Die Startseite des Servers enthält verschiedene Kacheln, die in „Applikationen“ und „Verwaltung“ untergliedert sind.

Unter „Applikationen“ sind folgende Schaltflächen zu finden:

1. „*Schulkonsole*“ – Über diesen Link gelangen Sie zur Schulkonsole. Der Inhalt der Schulkonsole richtet sich nach der Benutzerrolle (vgl. Kapitel 1.2). Dieser Link führt jeden autorisierten Benutzer (Administratoren und Lehrer) in das Computerraummodul, in dem die Unterrichtsfunktionen genutzt werden können.
2. „*Sesam Mediathek*“ – Hier finden Sie vielfältige Unterrichtsmedien und -materialien – vom Film über die Mediensammlung bis hin zum ausgearbeiteten Unterrichtsmodul.
3. „*Horde Webmail*“ – Dieser Link führt Sie zu Horde (vgl. Kapitel 16, Seite 200).
4. „*LMZ-Portal*“ – Verknüpfung zur Startseite des LMZ
5. „*Impressum*“ – Verknüpfung zum Impressum der *paedML Linux*
6. „*Passwort ändern*“ – *Eigenes Passwort ändern*

„Verwaltung“ enthält Verknüpfungen zu:

7. „*System- und Domäneneinstellungen*“ – Über diesen Link gelangen Sie zur Schulkonsole (s. Kapitel 1.3.2, Seite 20). Der Inhalt der Schulkonsole richtet sich nach der Benutzerrolle (vgl. Kapitel 1.2).
8. „*Lokales Nagios*“ – Überwachung von Netzwerk, Host und Services (vgl. Kapitel 15 ab Seite 194)
9. „*Admin Diary*“ – Überblick über administrativer Änderungen in der Domäne
10. „*OPSI-Server*“ – Dieser Link bringt Sie auf die Startseite des Backup-Servers. An diesem System muss in der Regel nichts konfiguriert werden.



Abb. 3: Die Startseite der paedML – Anlaufstelle für die meisten steuernden Aufgaben

1.3.2 Schulkonsole

Aufruf über Startseite: <https://server.paedml-linux.lokal> | Schaltfläche „Schulkonsole“

1.3.2.1 Der Aufbau der Schulkonsole

Der Aufbau der *Schulkonsole* ist für alle Benutzer gleich. Er enthält folgende Elemente:

Nr.	Beschreibung
1	Zurück zur Übersicht
2	Oben sehen Sie in Reitern sortiert bereits zuvor geöffnete Module, zu denen Sie mit einem Klick wechseln können.
3	Hier kann nach Funktionen und Modulen gesucht werden.
4	Anzeige von Mitteilungen, z.B. bei verfügbaren Updates
5	„Mehr Optionen“ für den jeweils angemeldeten Benutzer: <ul style="list-style-type: none"> Benutzereinstellungen: Passwort ändern Zertifikate: Wurzelzertifikat und Zertifikat-Sperrliste herunterladen Sprache ändern: Deutsch, Englisch Hilfe: Verschiedene Verknüpfungen zu Hilfe-Seiten Zurück zur Startseite und Abmelden des Benutzers
6	Hier finden Sie die dem Benutzer zur Verfügung stehenden Menüpunkte. Wenn Sie eine Kategorie anklicken, werden die darin enthaltenen Module angezeigt.
7	Im Hauptfenster der Schulkonsole werden die zur Auswahl stehenden Module oder der Inhalt des jeweils aktiven Moduls angezeigt.

Tabelle 1: Aufbau der Schulkonsole

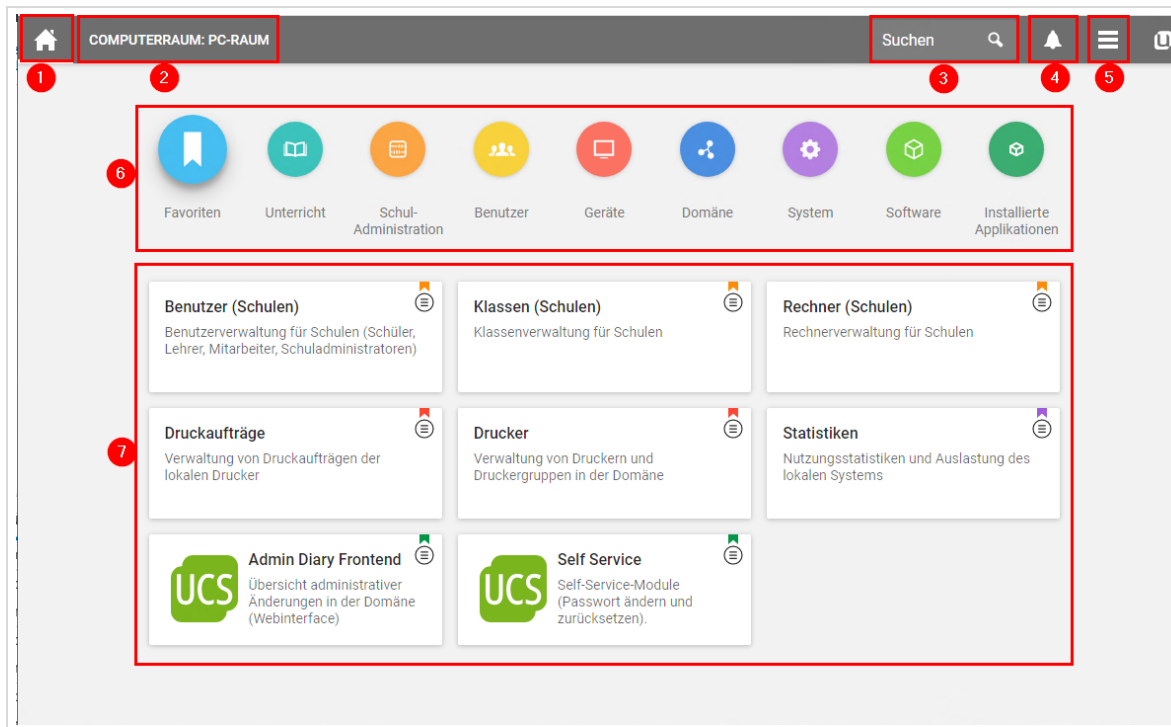


Abb. 4: Schulkonsolenansicht für den Admin

1.3.2.2 Navigation in der Schulkonsole

Nr. Beschreibung

- 1 Hier gelangen Sie zurück zur Übersicht über alle Module.
- 2 Mit einem Rechtsklick auf den Reiter oder mit einem Klick auf das „x“, kann das Modul geschlossen werden. Dies hat die gleiche Funktion wie 3.
- 3 Über dieses Symbol wird das Modul geschlossen. Es hat die gleiche Funktion, wie 2.
- 4 Bereits geöffnete Module werden als Reiter angezeigt. Reiter, die aktuell angezeigt werden sind farbig. Inaktive Reiter erscheinen grau. Sie können zu einem anderen Reiter wechseln, indem Sie darauf klicken.
- 5 In der Modulsuche können Sie gezielt nach Modulen suchen.
- 6 Die verschiedenen Funktionen des Moduls werden in diesem Bereich angezeigt.

Tabelle 2: Navigation in der Schulkonsole

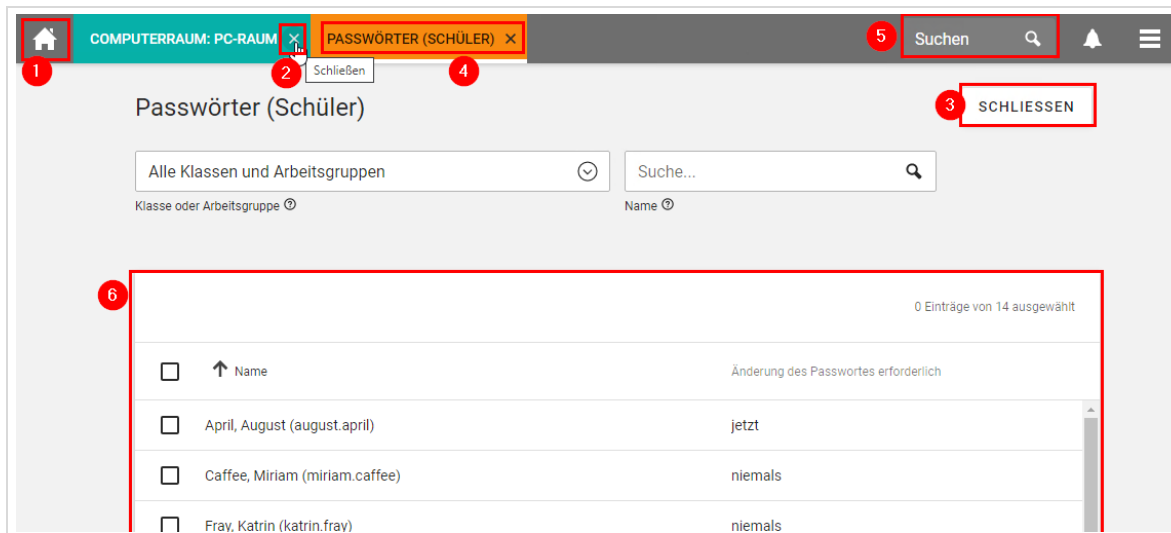


Abb. 5: Navigation in der Schulkonsole

1.3.2.3 Schulkonsolenmodule

Die *Schulkonsole* lädt dynamisch Module – abhängig von der Benutzergruppe, der ein Anwender angehört:

11. *Administrative Benutzer* – Administratoren können in der *Schulkonsole* fast alle Anpassungen des Schulnetzwerkes vornehmen. Hier werden zum Beispiel neue Räume, Drucker, Rechner angelegt oder Benutzer verwaltet. Die *Schulkonsole* ist aber auch ein effektives Instrument zur Konfiguration Ihrer Server. **Diese Funktionen sollten nur mit Vorsicht (oder nur nach Rücksprache mit der Hotline) genutzt werden!**
Wir empfehlen Ihnen ausdrücklich, administrative Aufgaben mit dem Benutzer „netzwerkberater“ durchzuführen.
12. *Lehrer* können über die *Schulkonsole* Ihren Unterricht steuern.
13. *Schüler* können sich an der *Schulkonsole* zwar anmelden, erhalten jedoch keinen Zugriff auf Module. Schüler können über die *Schulkonsole* das eigene Passwort ändern. Dies ist auch mit Windows-Bordmitteln möglich (**Strg** + **Alt** + **Entf**).

Nach Anmeldung an der *Schulkonsole* sehen Sie die für den jeweiligen Benutzer verfügbaren Menüs.



Die folgende Übersicht beschreibt kurz alle im System verfügbaren Menüs und deren einzelne Module.

Sofern wir in unseren Anleitungen nicht explizit auf ein Modul verweisen, bitten wir Sie dringend, keine eigenständigen Veränderungen an einem solchen Modul vorzunehmen.

Die Anforderungen an Schulnetzwerke sind vielfältig. Sie sollten die Möglichkeit haben, Ihr System an die schulischen Bedürfnisse anzupassen. Wir raten Ihnen jedoch dringend davon ab, im Live-System zu experimentieren.

Nehmen Sie nur in Ausnahmefällen Änderungen an nicht dokumentierten Modulen vor, wenn Sie wirklich wissen, was Sie machen! Dokumentieren Sie alle Änderungen sorgfältig!

Nehmen Sie im Zweifelsfall immer Kontakt mit der Hotline auf!

Melden Sie im Fehlerfall die Änderungen am System an die Hotline, damit die Fehlersuche einfacher wird!



Die Einstellungsmöglichkeiten des Benutzers *Administrator* reichen tief in das System hinein. Ein unbedachter Klick kann unter Umständen ungewollte Auswirkungen haben. Für die Aufgaben als Netzwerkberater sollte die Anmeldung mit dem Benutzerprofil *netzwerkberater* ausreichend sein.

1. Im Menü „*Favoriten*“ können Sie häufig genutzte Module ablegen, um schnell darauf zugreifen zu können. Dieses Menü ist dynamisch und kann von jedem Benutzer individuell gestaltet werden (vgl. Kapitel 1.3.2.4, Seite 26).
2. Der Menüpunkt „*Unterricht*“ beinhaltet die pädagogischen Funktionen der *paedML Linux*. Eine Beschreibung der einzelnen Module finden Sie im Lehrerhandbuch.

Unterricht

Klassenlisten	Generieren von Listen für Klassen und Arbeitsgruppen im CSV-Format
Computerraum	Zugriff auf Schülerrechner via iTalc, Internet-Einstellungen, Rechner sperren, ...
Materialien verteilen	Unterrichtsmaterial verteilen und einsammeln
Klassenarbeiten	Klassearbeit einrichten und starten
Drucker moderieren	Moderation von Druckaufträgen

3. Der Menüpunkt „*Schuladministration*“ deckt die organisatorischen Aufgaben des Netzbetriebes ab.

Schul-Administration

Benutzer (Schulen)	Benutzer verwalten und anlegen
Klassen (Schulen)	Klassen verwalten und anlegen
Rechner (Schulen)	Geräte verwalten und anlegen
Passwörter (Schüler)	Schülerpasswörter ändern
Passwörter (Lehrer)	Lehrerpasswörter ändern
Passwörter (Mitarbeiter)	Mitarbeiterpasswörter ändern
Computerräume verwalten	Computerräume anlegen und Rechner zuweisen
Klassen zuordnen	Klassen den Lehrern zuordnen
Lehrer zuordnen	Lehrer den Klassen zuordnen

Arbeitsgruppen verwalten	Arbeitsgruppen anlegen und verwalten
Internetregeln zuweisen	Internetregeln für Klassen oder Arbeitsgruppen zuweisen
Internetregeln definieren	Internetregeln bearbeiten
Unterrichtszeiten	Unterrichtszeiten definieren
Benutzerimport	Automatischer Benutzerimport über eine csv-Datei
UCS@school-Konfigurationsassistent	Bleibt ungenutzt, da der Konfigurationsassistent bereits bei der erstmaligen Einrichtung durchlaufen wurde.

4. Das Schulkonsolenmodul „Benutzer“ beinhaltet verschiedene Menüs, um die Benutzerattribute in der Schuldomäne *paedml-linux.lokal* zu konfigurieren.

Benutzer

Benutzer	Verwaltung aller Domänennutzer, also auch der Admins und der System-Accounts.
Dateisystem Quota	Setzen, Entfernen und Bearbeiten von Quota-Einstellungen von lokalen Systemen
Gruppen	Verwaltung von Benutzer- und Rechnergruppen der Domäne
Kontakte	Verwaltung von Kontakten

5. Das Schulkonsolenmodul „Geräte“ beinhaltet verschiedene Menüs, um die Geräteattribute der Schuldomäne *paedml-linux.lokal* zu konfigurieren.

Geräte

Druckaufträge	Verwalten von Druckaufträgen
Drucker	Verwaltung von Druckern
Nagios	Nagios-Konfiguration
Rechner	Verwaltung von Rechnern der Domäne

6. Das Schulkonsolenmodul „Domäne“ beinhaltet verschiedene Menüs, um die Domänenattribute der Schuldomäne *paedml-linux.lokal* zu konfigurieren.

Domäne

Admin Diary	Übersicht über alle wichtigen Vorgänge in der Domäne
DHCP	DHCP-Einstellungen der Domäne

DNS	DNS-Einstellungen der Domäne
Domänenbeitritt	Domänenbeitritt des lokalen Systems
E-Mail	Verwaltung von Mail-Domänen und Mailinglisten
Freigaben	Verwaltung von Verzeichnisfreigaben
LDAP-Verzeichnis	Durchsuchen und Verwalten des LDAP-Verzeichnisses
Netzwerke	Konfiguration von Netzwerkeinstellungen
Portaleinstellungen	Anpassung von Portaleinträgen (Startseite)
Richtlinien	Verwaltung von domänenweiten Richtlinien
SAML identity provider	Konfiguration des Service Providers für die Single Sign On Funktion

7. Unter „System“ finden Sie Menüs, die für den jeweiligen Server (Master-Server oder opsi-Server) aktiv sind.

System

Hardwareinformationen	Übersicht über Hardwareinformationen des lokalen Systems (Server)
Netzwerk-Einstellungen	Setzen der IP-Adressen, Gateways, http-Proxies und DNS-Server
Prozessübersicht	Prozessübersicht des lokalen Systems (Server)
Sprach-Einstellungen	Konfiguration aller sprachrelevanten Einstellungen
Statistiken	Nutzungsstatistiken zur Auslastung der Maschine (CPU/Swap/Speicher)
Systemdienste	Übersicht und Konfiguration lokaler Systemdienste
Univention Configuration Registry	Verwaltung von UCR-Variablen des lokalen Systems (Server)
Zertifikats-Einstellungen	Erstellung eines neuen Root-Zertifikats
Systemdiagnose	Das System auf bekannte Probleme analysieren

8. Unter „Software“ finden Sie Menüs, für Softwareaktualisierungen und zur Paketverwaltung.

Software

App Center	Applikationen hinzufügen oder entfernen
Paket-Verwaltung	Installation von Software-Paketen

9. Das letzte Schulkonsolenmodul „*Installierte Applikationen*“ schließlich gibt eine Übersicht über die verschiedenen Softwarepakete, die für den Betrieb der *paedML Linux* auf dem Server installiert sind. Nehmen Sie hier nur Änderungen vor, wenn Sie wissen, welche Auswirkungen die Installation haben kann.

1.3.2.4 Favoriten

Jeder Benutzer hat die Möglichkeit, häufig benutzte Menüpunkte als *Favoriten* in einem eigenen Menü abzulegen.

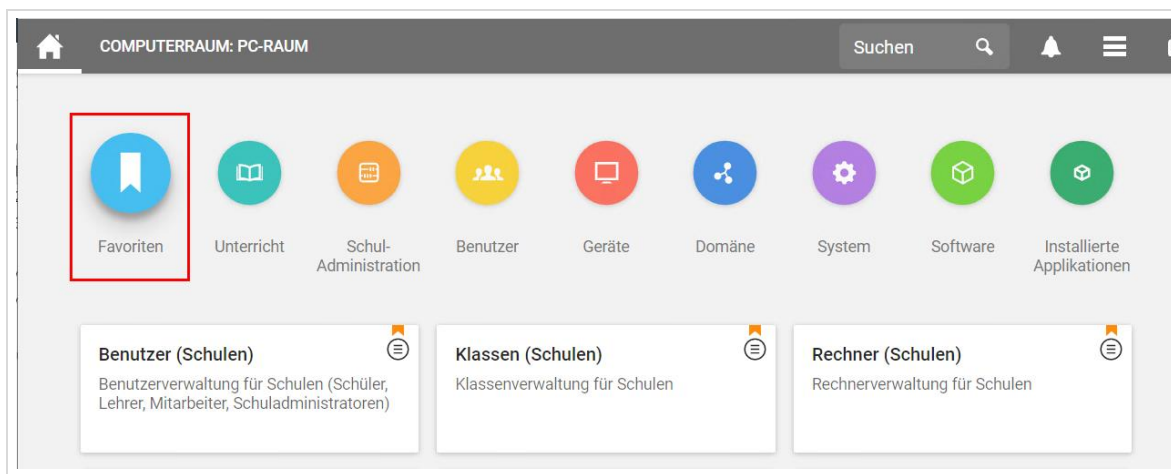


Abb. 6: Favoriten

Um einen Menüpunkt zu den Favoriten hinzuzufügen, klicken Sie mit der linken Maustaste einmal auf das Menüsymbol des jeweiligen Moduls. Ein *neues Menüsymbol* erscheint. Es öffnet sich ein Dialog, mit dem Sie die Möglichkeit erhalten, den Menüpunkt zu den Favoriten hinzuzufügen oder aus den Favoriten zu entfernen.

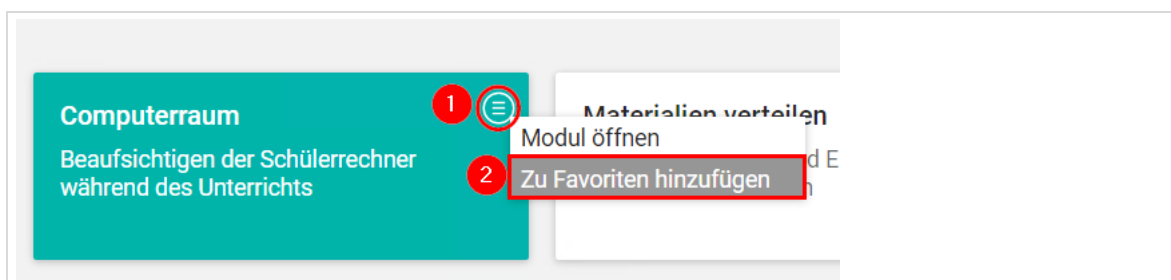


Abb. 7: Favoriten können Sie selbst verwalten

1.3.2.5 Benachrichtigungen

Benachrichtigungen werden am unteren Bildschirmrand angezeigt, zum Beispiel, wenn ein Computer angelegt wurde.

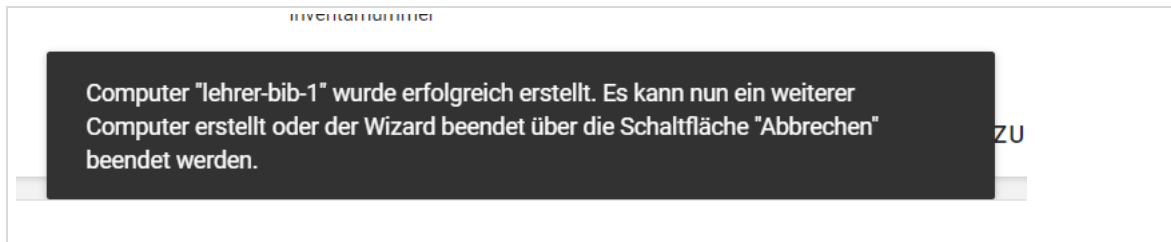


Abb. 8: Benachrichtigung: Ein Computer wurde erstellt...

1.3.3 Univention Configuration Registry

Aufruf über Schulkonsole (Administrator): System | Univention Configuration Registry

Einige Parameter der *paedML Linux* werden über die „Univention Configuration Registry“ (kurz „UCR“) konfiguriert.



Falsche Einträge in der *UCR* können zu unerwünschten Effekten führen. Dieses Modul ist mächtig und relativ komplex, weniger in der Bedienung, jedoch im Funktionsumfang und in den Auswirkungen von Änderungen.

Wir möchten Sie ausdrücklich darauf hinweisen, dass Sie Änderungen an der UCR nur dann vornehmen dürfen, wenn Sie sich im Klaren darüber sind, was diese Änderungen im System bewirken.

BESSER IST ES, IN DIESEM MODUL NICHTS ZU ÄNDERN!

Dokumentieren Sie jede Änderung und teilen Sie Änderungen im Fehlerfall der Hotline mit!

In diesem Handbuch werden an ein einigen Stellen Parameter der *UCR* und deren Optionen beschrieben. Das Verfahren zum Ändern dieser Parameter wird nur hier beschrieben.

Sie öffnen das Schulkonsolenmodul „Univention Configuration Registry“ in der *Schulkonsole* über dem Menüpunkt „System | Univention Configuration Registry“.

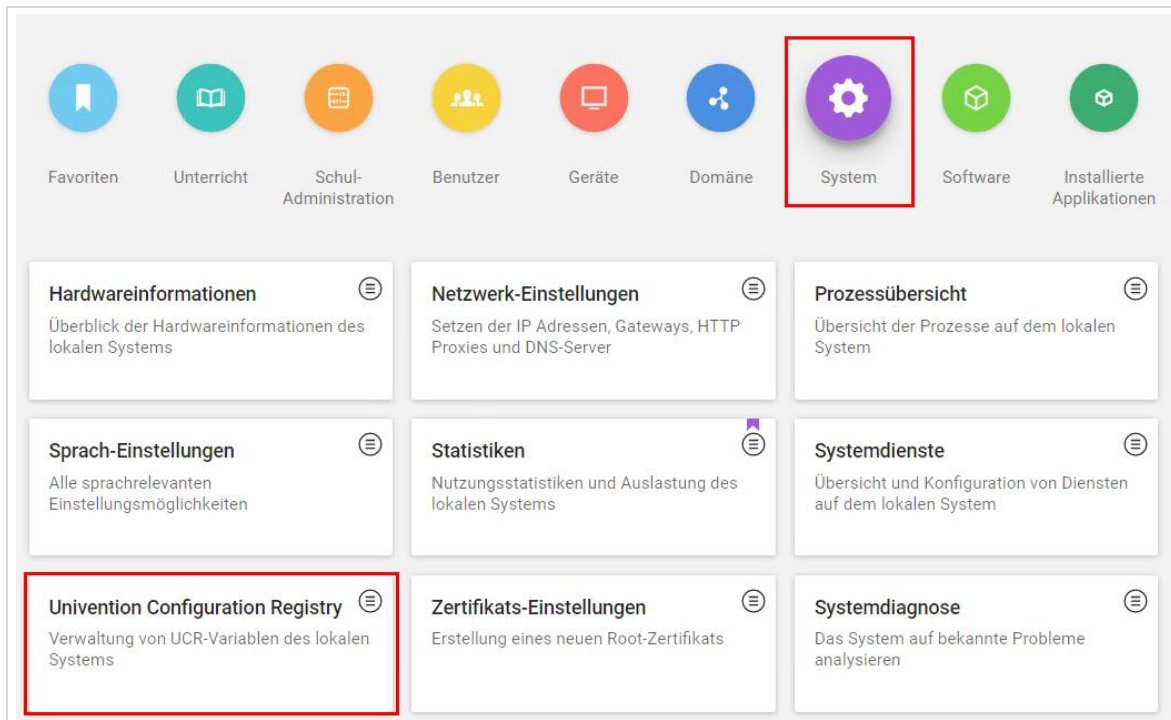


Abb. 9: Aufruf des UCR-Moduls

Es öffnet sich ein neuer Reiter, in dem ALLE UCR-Variablen angezeigt werden. Um eine bestimmte Variable zu finden, können Sie ein „Schlüsselwort“ in das gleichnamige Feld eintragen. Die Suche kann über die Angabe einer „Kategorie“ oder der Auswahl eines Wertes im Feld „Suchattribut“ verfeinert werden. Mit Klick auf „Suchen“ startet Ihre Suche.

Die Suchergebnisse werden im Hauptfenster angezeigt. Um eine UCR-Variable zu ändern, markieren Sie die Checkbox („Haken“) vor der Variablen. Anschließend werden oberhalb der Variablen (neben dem „Hinzufügen“-Knopf) zwei weitere Knöpfe „Bearbeiten“ und „Löschen“ angezeigt. Mit Klick auf „Bearbeiten“ öffnet sich ein neuer Dialog.

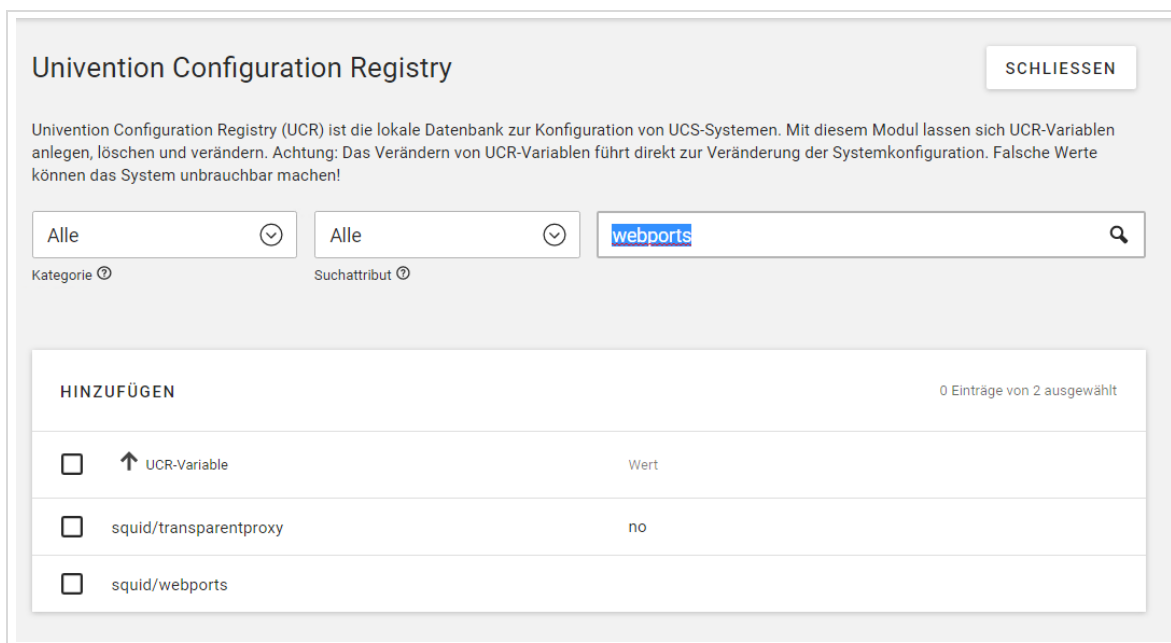


Abb. 10: Auswahl der UCR-Variable „squid/webports“ für die Bearbeitung

Im Dialogfenster „UCR-Variable bearbeiten“ können Sie Änderungen der Variablen vornehmen. Viele Variable haben im Beschreibungstext eine Erläuterung zu den Parametern. Übernehmen Sie die Änderungen mit „Speichern“.



UCR-Variable bearbeiten

squid/webports

UCR-Variable ⓘ

80 21

Wert ⓘ

Beschreibung: ⓘ

Ist die Variable nicht gesetzt, leitet Squid nur Anfragen von Clients weiter, die an die Ports 80 (HTTP), 443 (HTTPS) oder 21 (FTP) gerichtet werden. Mit dieser Variable kann die Liste der erlaubten Ports geändert werden, mehrere Angaben sind dabei durch Leerzeichen zu trennen. Beispiel: '80 443 21 8080'.

ABBRECHEN SPEICHERN

Abb. 11: Änderung einer UCR-Variable.

1.3.4 opsi-configed editor

Aufruf über lokal installierten opsi-configed.

Der opsi configed Editor ist ein Java Programm, mit dem sich Windows-Clients grafisch verwalten lassen. Das Programmpaket opsi, das für die Softwareverteilung benötigt wird, ist in Kapitel 0 ab Seite 67 beschrieben.

1.3.5 Startseite Nextcloud

Wenn Sie die Nextcloud in der paedML Linux / GS einsetzen, können Sie über die Nextcloudoberfläche verschiedene Einstellungen vornehmen.

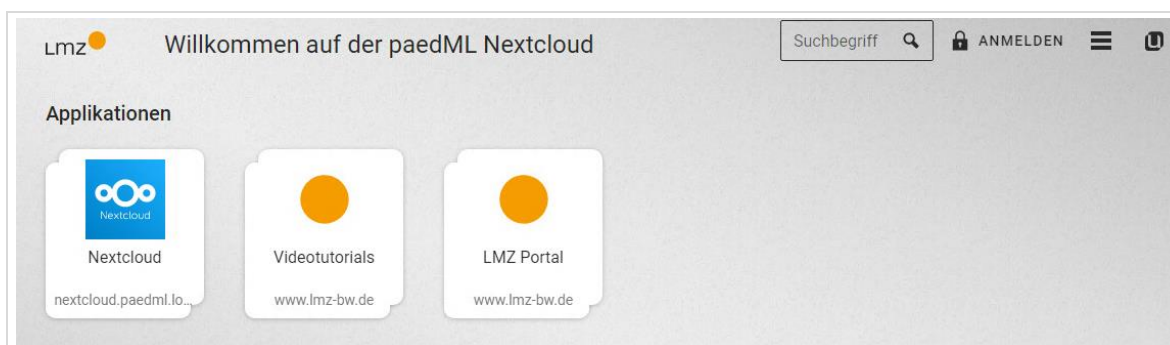


Abb. 12: Nextcloud Startseite

1.4 Nützliche Werkzeuge

Die Liste der Werkzeuge für die Arbeit mit Computern ist groß und die Vorlieben der Benutzer sind verschieden. Häufig erfüllen verschiedene Programme denselben Zweck. Wir möchten Ihnen hier ein paar Programme vorstellen, die Ihnen die Arbeit im schulischen Netzwerk erleichtern.

1.4.1 PuTTY – der Alternative Weg zur Serverkonsole

Der ssh-Client *PuTTY* stellt Verbindungen zu (*Linux*-) Servern her, auf denen der Dienst das Protokoll *ssh*⁵ verfügbar macht. Dadurch können Sie von einem *Windows*-Rechner aus über das Netzwerk auf die Kommandozeile Ihres Servers zugreifen und dort Befehle ausführen. *PuTTY* ist eine Alternative zur Arbeit an der Serverkonsole. Administrative Aufgaben können von einem *Windows*-Rechner aus erledigt werden.

Einen Downloadlink finden Sie unter

<http://www.chiark.greenend.org.uk/~sgtatham/PuTTY/download.html> .

System	Adresse	Port
Server von intern	server.paedml-linux.lokal	22
opsi-Server von intern	backup.paedml-linux.lokal	22

Tabelle 3: Adressen für den Zugriff auf die paedML Server

Die Anmeldung am jeweiligen Zielserver geschieht mit Benutzername und Passwort des Servers. Empfohlener Benutzer ist der *Administrator*.

Nach erfolgreichem Login haben Sie mit *PuTTY* eine vollwertige Serverkonsole, mit der Sie Befehle an den Server senden können. Die Abmeldung erfolgt über den Befehl `exit` oder durch Schließen der *PuTTY*-Konsole.

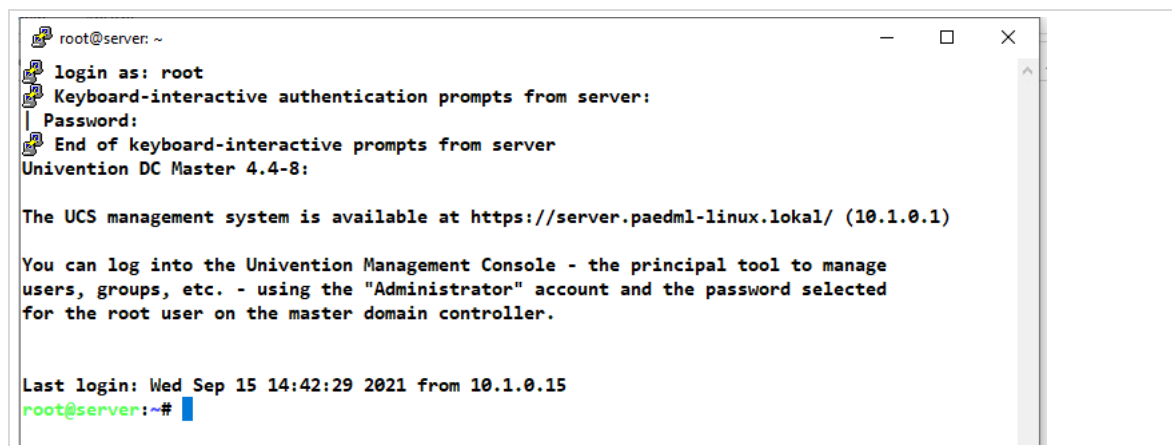


Abb. 13: Eine PuTTY-Konsole nach erfolgter Anmeldung.

⁵ http://de.wikipedia.org/wiki/Secure_Shell

1.4.2 WinSCP und Explorer – Datenaustausch mit dem Server



WinSCP ermöglicht Ihnen den Zugriff auf die Verzeichnisstruktur des Servers und kann beispielsweise für das Übertragen von *opsi*-Paketen verwendet werden.

Wenn Sie Daten (beispielsweise für den Benutzerimport) nur im Home-Verzeichnis des Administrators ablegen wollen, können Sie auch den *Windows-Explorer* nutzen.

WinSCP

WinSCP ist eines von vielen Programmen, das Ihnen den Datenaustausch zwischen *Windows*-Systemen und dem *Linux*-Server ermöglicht. Dadurch können Sie zum Beispiel Benutzerlisten auf den Server übertragen. Die Software steht als *opsi*-Paket zur Verfügung und kann einfach auf Clients, die mit *opsi* verwaltet werden, installiert werden.

Sie können WinSCP aber auch direkt vom Hersteller herunterladen und installieren (<http://winscp.net/eng/docs/lang:de>).

Wenn Sie WinSCP auf Ihrem Arbeitsplatz installiert haben und die Anwendung aufrufen, öffnet sich ein Anmeldefenster. Hier geben Sie die Zugangsdaten für den Rechner an, mit dem Sie sich verbinden wollen. Sie können auf den Server intern, (also innerhalb des Schulnetzes), oder auch von außerhalb des Schulnetzes zugreifen. Der Zugriff von außen kann beispielsweise durch den Dienstleister geschehen. Hierfür müssen in der Firewall im Menüpunkt „Firewall / NAT“ und dort im Reiter „Port Forward“ die vordefinierten Zugriffsregeln aktiviert werden. Die Regeln sind im Auslieferungszustand deaktiviert.

Der Zugriff auf das jeweilige System geschieht über den „Rechnernamen“ (bzw. die IP-Adresse bei Zugriff von außen), die jeweilige „Portnummer“, den „Benutzernamen“ und das zugehörige „Kennwort“.

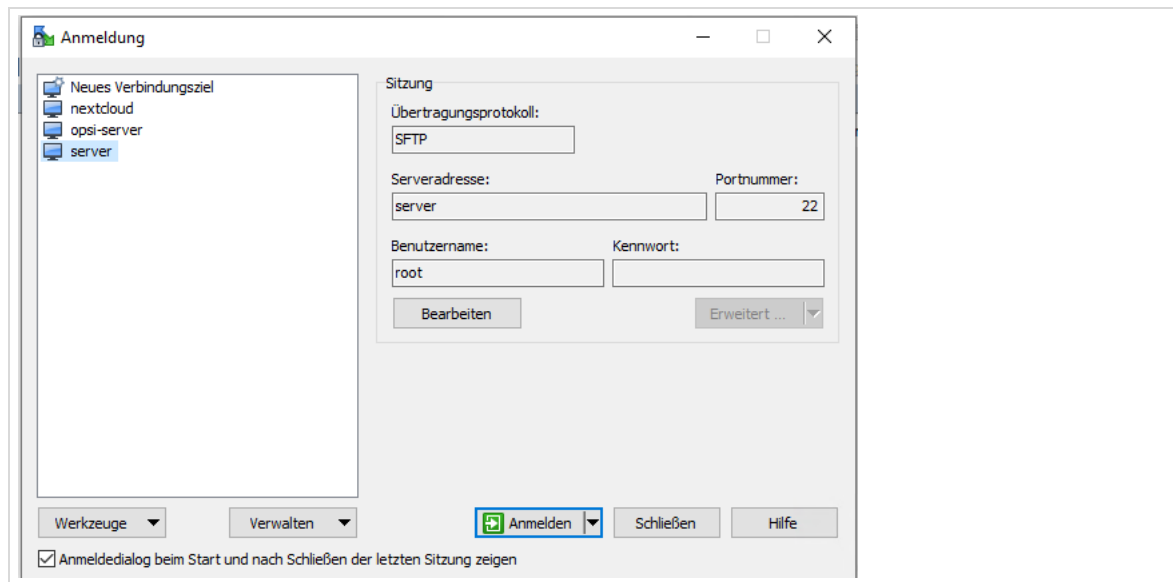


Abb. 14: Anmeldedaten beim Aufruf von WinSCP

Es öffnet sich ein neues Fenster. Auf der linken Seite ist zunächst der lokale Rechner, auf dem das Programm aufgerufen wurde. Auf der rechten Seite befindet sich der Rechner, auf den Sie zugreifen wollen.

Sie können nun Daten zwischen den beiden Systemen austauschen. Markieren Sie hierfür die entsprechenden Dateien und verschieben Sie diese per „Drag and Drop“ oder nutzen Sie die Schaltflächen im oberen Viertel des Programmes.

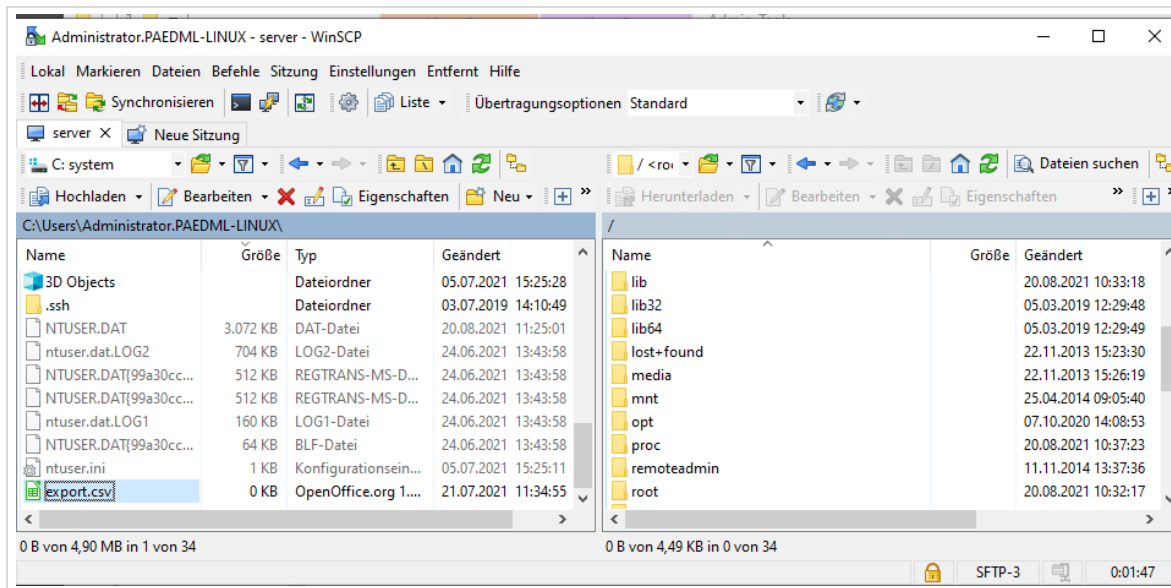


Abb. 15: WinSCP in Aktion

Windows-Explorer

Während mit WinSCP Zugriff auf alle Verzeichnisse der Server möglich ist, ist der Zugriff durch den Windows-Explorer begrenzt. Hier können unter Windows angemeldete Benutzer nur auf Windows-Freigaben zugreifen, die auf Server erreichbar sind. Hinweise zur Verzeichnisstruktur finden Sie in Kapitel 17, ab Seite 205.

Für bestimmte administrative Aufgaben ist ein eingeschränkter Zugriff ausreichend. Als Beispiel sei die Übertragung von Benutzer- und Rechnerlisten für den Import an der Konsole genannt.

Im folgenden Beispiel sehen Sie den Zugriff von Windows auf das Homeverzeichnis `H:\` des Administrators. Melden Sie sich hierfür als Administrator der Domäne mit „Administrator@paedml-linux“ und dem zugehörigen Kennwort an der W10-AdminVM an.

In der Taskleiste liegt die Verknüpfung zum Dateimanager (1) über den Sie zu einer Übersicht der lokalen Laufwerke des Rechners, sowie der für den jeweiligen Benutzer verfügbaren Netzwerkfreigaben gelangen.

Öffnen Sie nun die Netzwerkfreigabe „Administrator (\server) (H:)“ (2), um in das Homeverzeichnis des Administrators zu gelangen.

Sie können anschließend eine auf dem Desktop abgelegte Benutzerliste in das Verzeichnis übertragen (3).

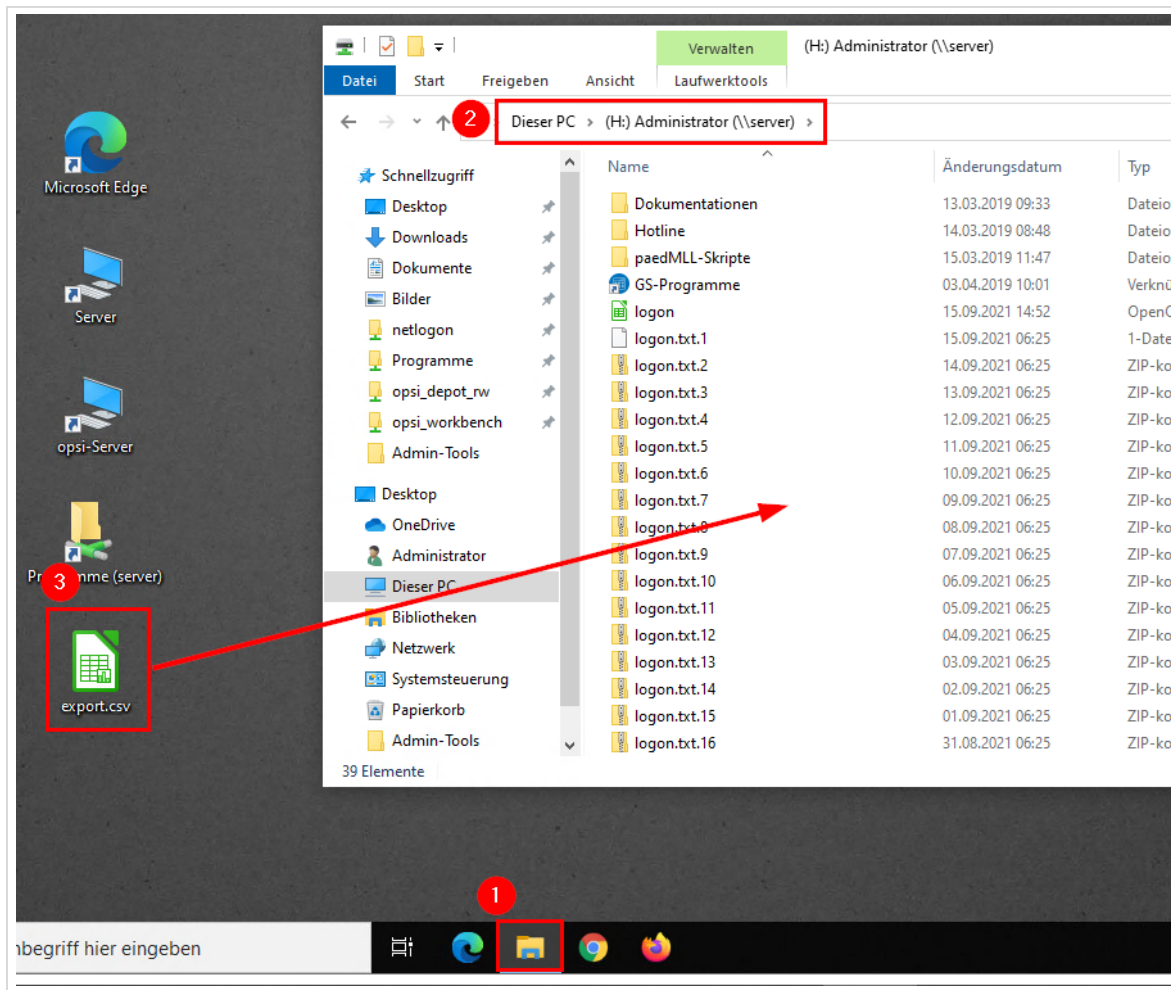


Abb. 16: Anmeldung im Home-Laufwerk des Administrators.



Alle Domänen-Benutzer (und damit auch der Administrator) können über die Eingabe von „H:“ in der Adressleiste des *Windows-Explorers* jederzeit auf das eigene Home-Laufwerk zugreifen.

Kopieren Sie Dateien auf „opsi_depot_rw“ (auf dem opsi-Server) bitte nur per WinSCP!

1.4.3 Editoren

Häufig gehen Anpassungen am System mit Änderungen an (Konfigurations-) Dateien einher. Der beständige Wechsel der Systembenutzer ist ein Beispiel dafür. Neue Schüler, neue Lehrer kommen, alte müssen gelöscht werden. Um Dateien zu ändern, werden Bearbeitungsprogramme, sogenannte Editoren, eingesetzt. Mit diesen Programmen können Sie Dateien öffnen, modifizieren und die neue Datei speichern.

Die Wahl eines Editors ist abhängig vom Geschmack des Anwenders. Es gibt Programme, die direkt auf dem Server ausgeführt werden können (*vi*, *mcedit*, *nano*,...) und Programme, die unter *Windows* laufen. Erstere sind schlank, an der Serverkonsole verfügbar, aber zum Teil wenig intuitiv. Letztere bieten einen höheren Komfort (Mausbedienung, Plugins,..) und eine einfachere Bedienbarkeit. Welchen Editor Sie benutzen, bleibt letztlich Ihnen überlassen. Unter *Windows* empfehlen wir *Notepad++*.

Notepad++

Ein unter *Windows* weit verbreiteter Editor ist das Programm *Notepad++*. Wir empfehlen Ihnen die Installation des Editors. Dieser relativ einfach zu bedienende Editor hat den Vorteil, dass er Kodierungen konvertieren kann.



Wir empfehlen Ihnen *notepad++* für das Bearbeiten von Dateien zu verwenden. Dieser Editor ist auf der W10AdminVM installiert.

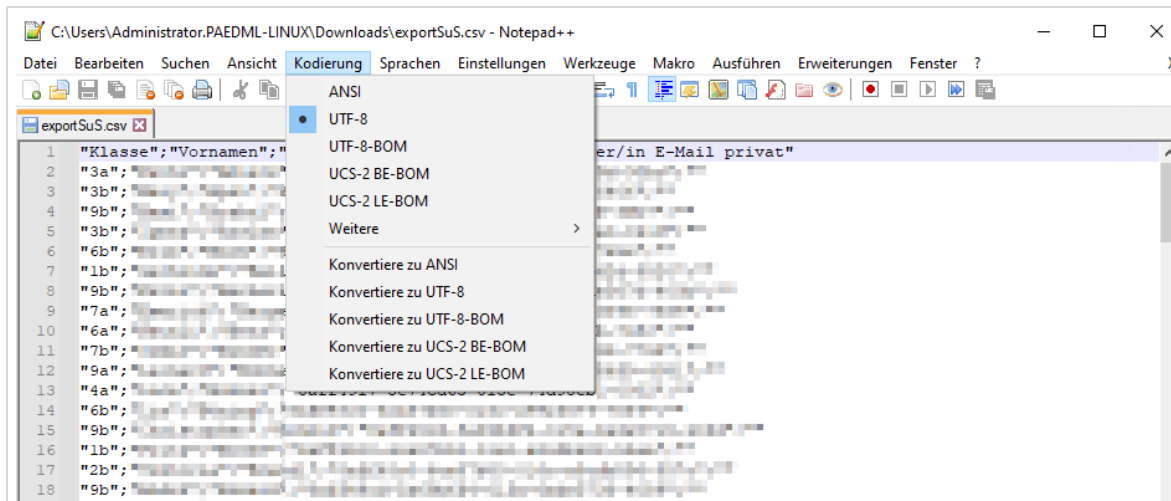


Abb. 17: Eine Benutzerliste im Editor Notepad++

1.5 Allgemeine Hinweise

1. Legen Sie immer Sicherungskopien von Dateien an bevor Sie darin Änderungen vornehmen.
2. Erstellen Sie regelmäßig Sicherungen Ihres Systems. Die Mitarbeiter der Hotline werden gegebenenfalls nur in Ihr System eingreifen, wenn Sie uns versichern können, dass Sie ein funktionierendes Backup vorliegen haben.
3. Bevor es hierbei zu Kapazitätsproblemen kommt, sollten nicht benötigte Daten gelöscht werden. Der Schuljahreswechsel bietet sich für ein „Großreinemachen“ an.
4. Ein wichtiger Bestandteil für den Umgang mit PCs in der Schule ist eine Nutzungsordnung⁶, die alle Schüler – beziehungsweise deren Erziehungsberechtigte – unterschreiben müssen.
5. Im Zusammenhang mit Sicherheitsüberlegungen muss auch das Sperren von USB-Sticks in den Blick genommen werden.

⁶ Ein Beispiel einer Nutzungsordnung finden Sie unter https://lehrerfortbildung-bw.de/st_recht/form/netz/

2 Unterrichtsorganisation und -steuerung

Unter dem Hauptmenü *Schulkonsole / Unterricht* stehen Ihnen als Netzwerkberater die gleichen Werkzeuge für die Gestaltung des Unterrichts zur Verfügung, auf die alle Lehrkräfte nach Anmeldung an der Schulkonsole zugreifen können. Da die Unterrichtsorganisation ausführlich im Lehrerhandbuch der *paedML Linux / GS* beschrieben wird, möchten wir Sie auf dieses Handbuch verweisen.

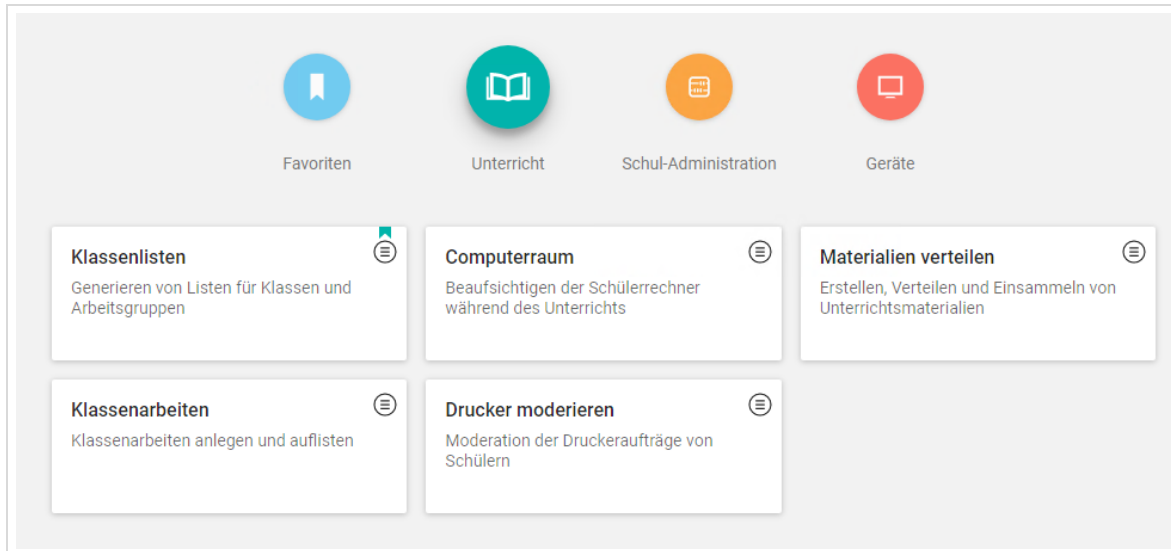


Abb. 18: Unterrichten mit der Schulkonsole

3 Benutzerverwaltung

Die paedML Linux 7.2 bringt eine neue Benutzerverwaltung mit und schafft gleichzeitig den vorigen Benutzerimport ab.

Wichtig: Der **neue Benutzerimport** übernimmt viele Aufgaben der **Benutzerverwaltung**. Es wird in Zukunft nicht notwendig sein, Schülerinnen und Schüler zu löschen, neu anzulegen oder zu versetzen, all dies ist automatisiert, sobald Sie den Export aus der Schulverwaltung einpflegen. Auch bei **Veränderungen im laufenden Schuljahr** werden Änderungen wie An- und Abmeldungen, Klassenwechsel oder Korrekturen über einen **erneuten Import** aus der Schulverwaltungssoftware **realisiert**.

Benutzerkonten, welche über andere Quellen importiert wurden, werden jedoch nicht verändert und damit auch nicht aktualisiert. Diese Quellen sind der alte Benutzerimport und der händische Benutzerimport über die Schulkonsole „Benutzer (Schulen)“. Bestehende Benutzerkonten, welche vom Benutzerimport verwaltet werden sollen, **müssen** bei der Umstellung **gelöscht werden**.

3.1 Benutzerimport und Schuljahreswechsel



Sämtliche Beschreibungen zum Benutzerimport und zum Schuljahreswechsel sind im Dokument „Hinweise zum Schuljahreswechsel Version 7.2“ zu finden, welches Sie unter <https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#howtos> abrufen können.

Bitte lesen Sie dieses Dokument aufmerksam durch, bevor Sie mit dem neuen Benutzerimport beginnen.

3.2 Anwender manuell hinzufügen



Wir empfehlen ausdrücklich, den Import von Benutzern über CSV-Dateien durchzuführen. Im Einzelfall kann es sinnvoll sein, Benutzer über das hier beschriebene Verfahren manuell einzupflegen.

Ebenfalls im Schulkonsolenmenü **Schul-Administration | Benutzer (Schulen)** finden Sie den Knopf „Hinzufügen“, über den Benutzer angelegt werden können.

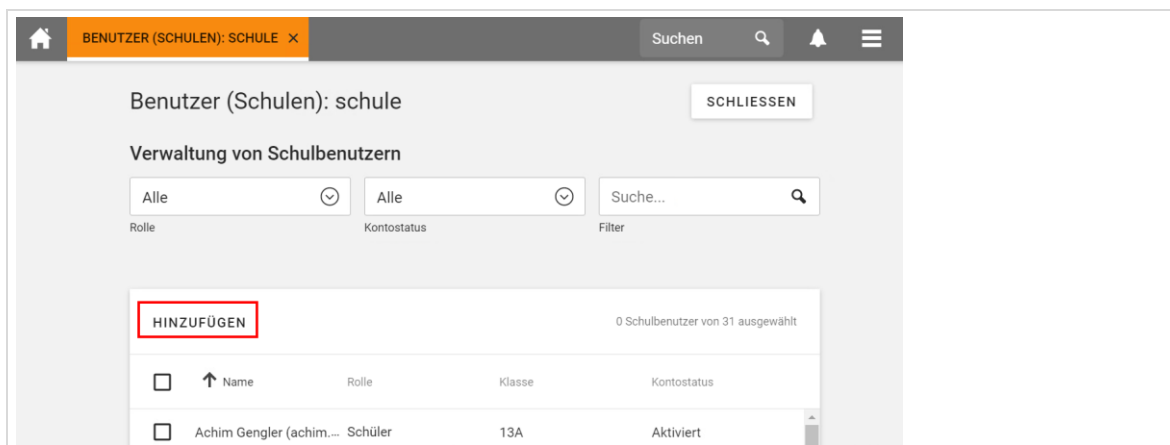


Abb. 19: Hinzufügen einzelner Benutzer.

In der ersten Maske werden Sie gefragt, was für einen Benutzer Sie anlegen wollen. Wählen Sie einen Benutzertyp („Schüler“ oder „Lehrer“) und klicken Sie auf „Weiter“.

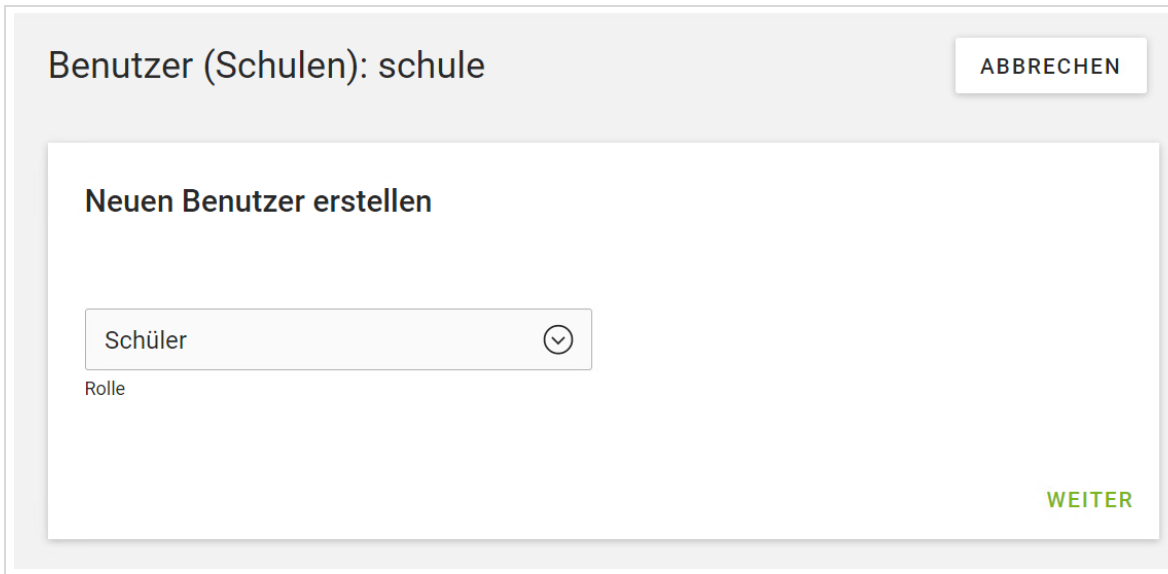


Abb. 20: Erster Schritt: Festlegen eines Benutzertyps.

Für das Anlegen von Benutzern benötigen Sie „Vor- und Nachnamen“ und einen „Benutzernamen“⁷. Optional können Sie den Benutzern noch eine „E-Mail“-Adresse und das „Geburtsdatum“ zuweisen.

Die Masken für das Anlegen von Lehrern und Schülern unterscheiden sich im Feld „Klasse“. Dieses ist bei Schülern vorhanden und muss mit einem Wert befüllt werden. Bitte verwenden Sie keine Leerzeichen!

Lehrer können sich – wie im „Handbuch für Lehrkräfte“ beschrieben – über die Schulkonsole einer Klasse zuordnen. Dies ergibt aus administrativer Sicht Sinn, da die Zuordnung sich regelmäßig ändern kann. Außerdem können Lehrer auch in Vertretungsstunden die „Kontrolle“ über Klassen übernehmen, beispielsweise um Unterrichtsmaterial an die Klasse verteilen zu können.



Das Feld „Mailadresse“ kann leer bleiben, sofern Sie den Benutzern keine Mailadresse vergeben wollen. In diesem Fall wird für den Benutzer kein Konto mit dem Benutzernamen im Mailsystem angelegt.

Das Feld „Mailadresse“ darf keine Umlaute, kein ß oder andere Sonderzeichen enthalten!



Wenn Sie kein Kennwort eingeben, dann wird ein Zufallskennwort vergeben.

Da es keine Möglichkeit gibt, dieses Kennwort auszulesen, empfehlen wir hier ein Kennwort zu setzen und dem Benutzer mitzuteilen.

⁷ Das Standardformat von Benutzernamen der *paedML Linux* ist *vorname.nachname*.



Achten Sie unbedingt darauf, dass der Benutzername höchstens 15 Zeichen enthalten darf!

schule: Schüler erstellen
 Geben Sie Detailinformationen zum Anlegen eines neuen Benutzers an.

Thomas

Vorname *

Häßler

Nachname *

☐ Deaktiviert *

thomas.hae

Benutzername *

5b

Klasse *

thomas.hae@paedml-linux.lokal

E-Mail

.....

Passwort

.....

Passwort (Wiederholung)

NEUE KLASSE ERSTELLEN

ZURÜCK

SPEICHERN

Abb. 21: Anlegen eines Schülers.

schule: Lehrer erstellen
 Geben Sie Detailinformationen zum Anlegen eines neuen Benutzers an.

Sepp

Vorname *

Herberger

Nachname *

☐ Deaktiviert *

sepp.her

Benutzername *

sepp.her@paedml-linux.lokal

E-Mail

.....

Passwort

.....

Passwort (Wiederholung)

SPEICHERN

Abb. 22: Anlegen eines Lehrers mit lokalem Mailkonto

Ein neu angelegtes Benutzerkonto wird mit einer Meldung im oberen Bereich des Browserfensters quittiert:

Benutzer "sepp.her" wurde erfolgreich erstellt. Es kann nun ein weiterer Benutzer erstellt oder der Wizard über die Schaltfläche "Abbrechen" beendet werden.

Abb. 23: Ein Benutzer wurde erfolgreich angelegt

3.3 Benutzerdatensätze löschen

Aufruf über Schulkonsole (netzwerkberater): Schul-Administration | Benutzer (Schulen)

Das Löschen angelegter Benutzer geschieht im Menü „Schul-Administration | Benutzer (Schulen)“.



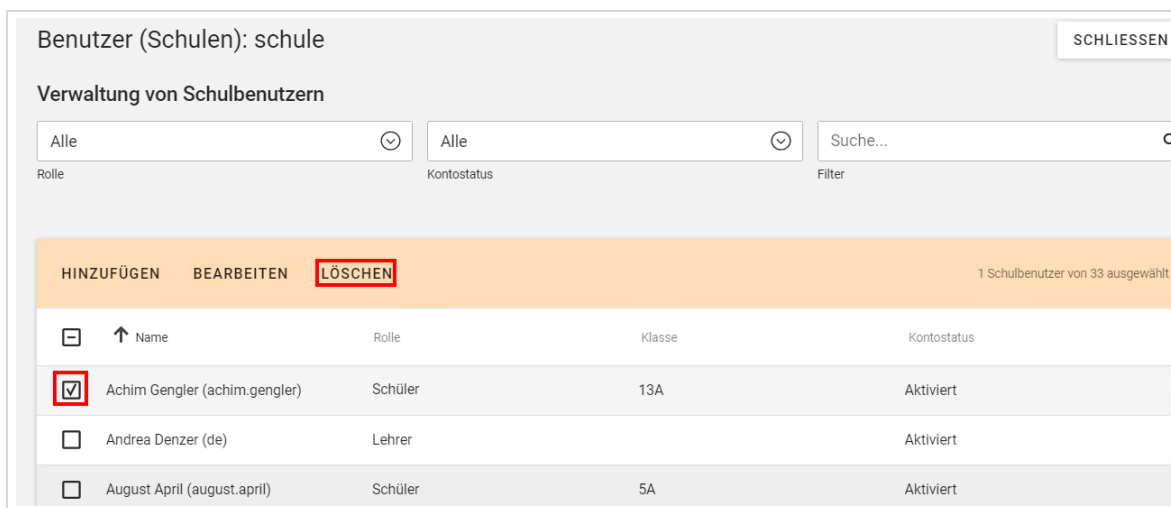
Der in dieser Maske vorhandene Benutzer „netzwerkberater“ darf unter keinen Umständen gelöscht werden.

Sollte dies doch versehentlich geschehen, müssen Sie an der Server-Konsole den Befehl

```
#lmz-settings-users
```

ausführen.

Markieren Sie alle Anwender, die Sie aus dem System löschen wollen und klicken Sie auf „Löschen“.



Benutzer (Schulen): schule SCHLIESSEN

Verwaltung von Schulbenutzern

Alle ⌵ Alle ⌵ Suche... 🔍

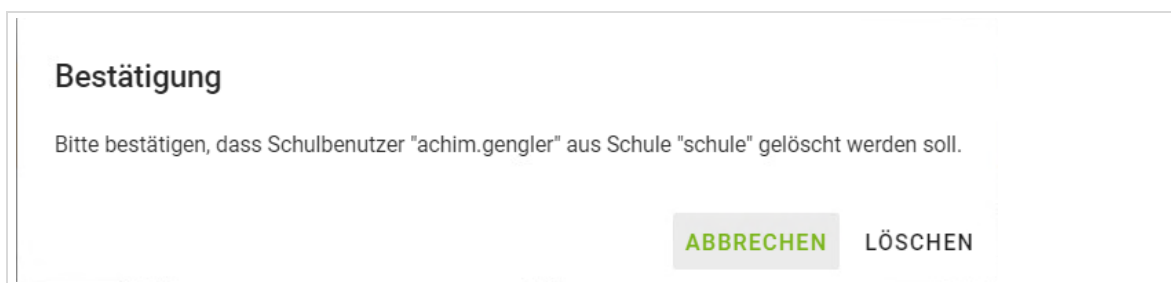
Rolle Kontostatus Filter

HINZUFÜGEN BEARBEITEN **LÖSCHEN** 1 Schulbenutzer von 33 ausgewählt

<input type="checkbox"/>	↑ Name	Rolle	Klasse	Kontostatus
<input checked="" type="checkbox"/>	Achim Gengler (achim.gengler)	Schüler	13A	Aktiviert
<input type="checkbox"/>	Andrea Denzer (de)	Lehrer		Aktiviert
<input type="checkbox"/>	August April (august.april)	Schüler	5A	Aktiviert

Abb. 24: Auswahl der zu löschenden Benutzer.

Eine letzte Bestätigung ist erforderlich, bevor die Daten gelöscht werden. Drücken Sie im nächsten Fenster nochmals auf „Löschen“, wenn die Schulbenutzer endgültig entfernt werden sollen



Bestätigung

Bitte bestätigen, dass Schulbenutzer "achim.gengler" aus Schule "schule" gelöscht werden soll.

ABBRECHEN LÖSCHEN

Abb. 25: Bestätigung des Löschvorganges.

3.3.1 Daten gelöschter Benutzer

Wenn ein Benutzer aus dem System gelöscht wird, wird der LDAP-Datensatz des Benutzers entfernt. Dadurch ist **mit sofortiger Wirkung** keine Anmeldung am System möglich.

Die Daten des gelöschten Benutzers aus dessen Home-Verzeichnis werden nach `/home/backup/BENUTZERNAME` gesichert. Dort kann ein administrativer Benutzer auf die Daten zugreifen, falls zum Beispiel der Benutzer versehentlich gelöscht wurde.

Alte Benutzerverzeichnisse aus `/home/backup` müssen manuell gelöscht werden.

Daten, die ein Benutzer auf ein Tauschverzeichnis kopiert hat, werden nicht verschoben.

3.4 Änderung von Passwörtern

3.4.1 Änderung von Lehrer- und Schüler-Passwörtern

Aufruf über Schulkonsole (**netzwerkberater**): **Schul-Administration | Passwörter (Schüler)**

Aufruf über Schulkonsole (**netzwerkberater**): Schul-Administration | Passwörter (Lehrer)



Die Änderung von Passwörtern für Schüler und für Lehrer erfolgt nach dem gleichen Schema. Hier wird nur die Änderung von Schülerpasswörtern beschrieben.

Organisatorisch ist es vermutlich am einfachsten, wenn beim ersten IT-Unterricht durch den Lehrer ein Kennwort für alle Schüler der zu unterrichtenden Klasse gesetzt wird, das diese bei Ihrer ersten Anmeldung ändern müssen. Dieses Verfahren ist im Lehrerhandbuch beschrieben.

Für den Fall, dass Sie als „netzwerkberater“ Kennwörter (bspw. der Kollegen) ändern müssen, ist das Verfahren hier nochmals beschrieben.

Um Kennwörter zu ändern, navigieren Sie in der Schulkonsole in das Menü „Schul-Administration | Passwörter (Schüler)“.

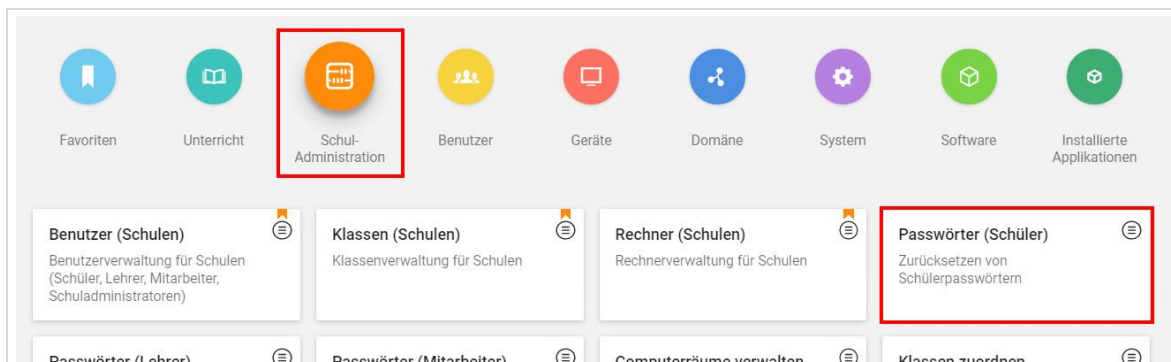
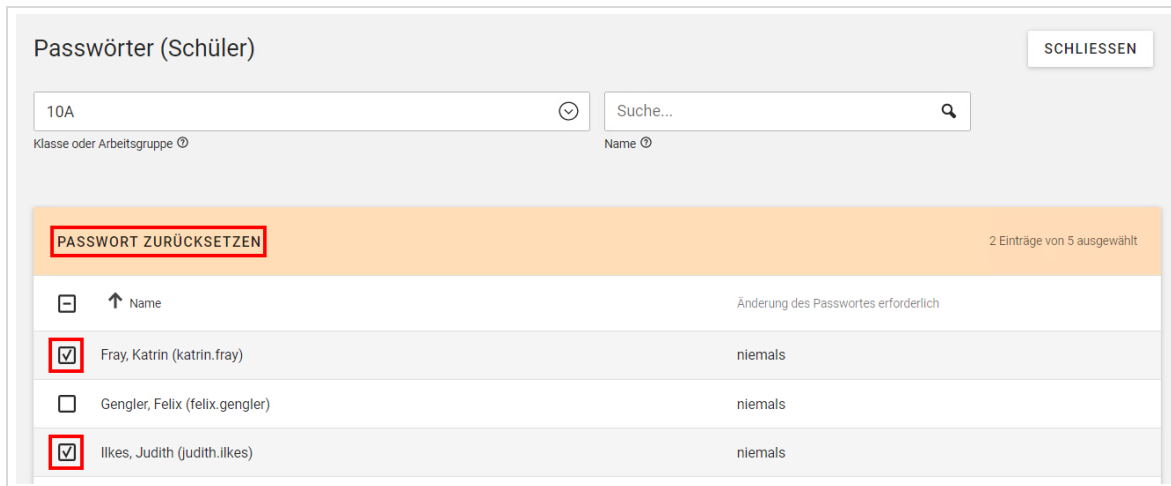


Abb. 26: Aufruf der Passwortänderung

Sie erhalten eine Übersicht über alle Schüler. Sie können über das Dropdownmenü „Klasse oder Arbeitsgruppe“ die Liste auf eine bestimmte Klasse verkleinern. Über das Suchfeld „Name“ und anschließenden Druck auf „Suchen“ können Sie einen Schüler direkt suchen. Sie können einzelne oder mehrere Schüler auswählen, deren Kennwort geändert werden soll. Markieren Sie hierfür die Checkboxes vor dem Namen der entsprechenden Schüler.

Drücken Sie auf „Passwort zurücksetzen“, um die Schülerkennwörter zu ändern.

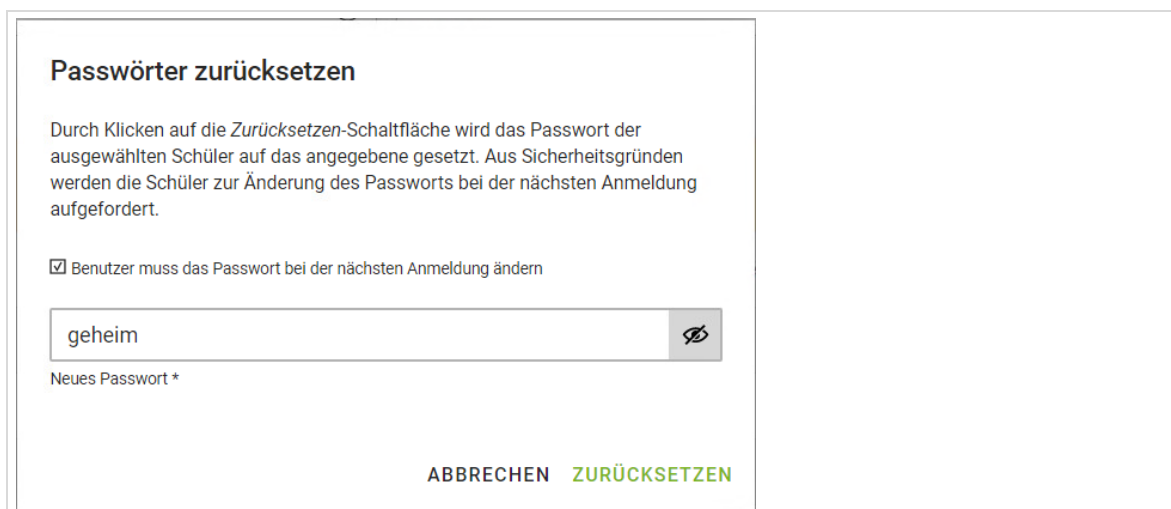


<input type="checkbox"/>	Name	Änderung des Passwortes erforderlich
<input checked="" type="checkbox"/>	Fray, Katrin (katrin.fray)	niemals
<input type="checkbox"/>	Gengler, Felix (felix.gengler)	niemals
<input checked="" type="checkbox"/>	Ilkes, Judith (judith.ilkes)	niemals

Abb. 27: Anzeige von Schülern für die Passwortänderung

In der folgenden Maske können Sie ein neues Kennwort eingeben. Dieses wird Ihnen zur Kontrolle im Klartext angezeigt. Sie können markieren, ob der Benutzer sein Passwort bei der nächsten Anmeldung ändern muss (empfohlen). Ein Klick auf „Zurücksetzen“ ändert das Passwort.


Teilen Sie das neue Kennwort dem Benutzer mit.



Passwörter zurücksetzen

Durch Klicken auf die *Zurücksetzen*-Schaltfläche wird das Passwort der ausgewählten Schüler auf das angegebene gesetzt. Aus Sicherheitsgründen werden die Schüler zur Änderung des Passworts bei der nächsten Anmeldung aufgefordert.

☒ Benutzer muss das Passwort bei der nächsten Anmeldung ändern

geheim 

Neues Passwort *

ABBRECHEN ZURÜCKSETZEN

Abb. 28: Eingabe eines neuen Passworts

3.4.2 Änderung von Passwörtern administrativer paedML-Benutzer

Alle Passwörter von administrativen Benutzern werden bei der Installation des Systems mit dem Ausführen des Skriptes `lmz-initial-setup` auf denselben Wert gesetzt. Wird dieser Befehl nach der Ersteinrichtung erneut ausgeführt, werden im Hintergrund noch weitere Prozesse angestoßen. So wird beispielsweise das Server-Zertifikat neu generiert. Nach Möglichkeit sollten dieser Befehl also nicht ausgeführt werden. Stattdessen wird empfohlen die Kennwörter der administrativen Benutzer – wie im Folgenden beschrieben – zu ändern.

Die Kennwörter der Administratoren-Konten können wie folgt geändert werden:

Benutzer	Passwortänderung via
root	Passwortänderung an der Server-Konsole mit dem Befehl. Hierüber werden die Passwörter für den Benutzer „root“ am Server und am Backupserver geändert: <code>#lmz-initial-setup --root</code>
Administrator	Änderung (nur des Passwortes) über das Schulkonsolenmenü „Domäne Benutzer“. ⁸
domadmin	Passwortänderung an der Server-Konsole mit dem Befehl <code>#lmz-initial-setup --domadmin</code>
netzwerkberater	Änderung (nur des Passwortes) über das Schulkonsolenmenü „Domäne Benutzer“. ⁹

Tabelle 4: Optionen für die Passwortänderung von administrativen Benutzern.

3.4.3 Optional: Änderung der Passwörter für SQL-Server



Dieser Abschnitt ist nur relevant, wenn Sie die Windows-Aktivierung über VAMT durchführen und das Passwort des **lokalen Administrators** auf der AdminVM (bzw. der Maschine, auf der VAMT installiert ist) geändert wurde.

Näheres zu VAMT finden Sie in Kapitel 12.1 ab Seite 169.

Um das lokale Administratorkennwort auf dem SQL-Server zu hinterlegen, öffnen Sie die Computerverwaltung und navigieren dort auf „*Dienste / SQL Server (INSTANCE1)*“. Ein Doppelklick öffnet die Eigenschaften des SQL-Servers. Dort navigieren Sie in den Reiter „Anmelden“ und hier können Sie das neue Kennwort eintragen.

⁸ Alternativ kann das Kennwort auch über `Strg` + `Alt` + `Entf` an einem Windows-Rechner geändert werden. Hierfür muss der entsprechende Benutzer natürlich an der Domäne angemeldet sein.

⁹ Alternativ kann das Kennwort auch über `Strg` + `Alt` + `Entf` an einem Windows-Rechner geändert werden. Hierfür muss der entsprechende Benutzer natürlich an der Domäne angemeldet sein.

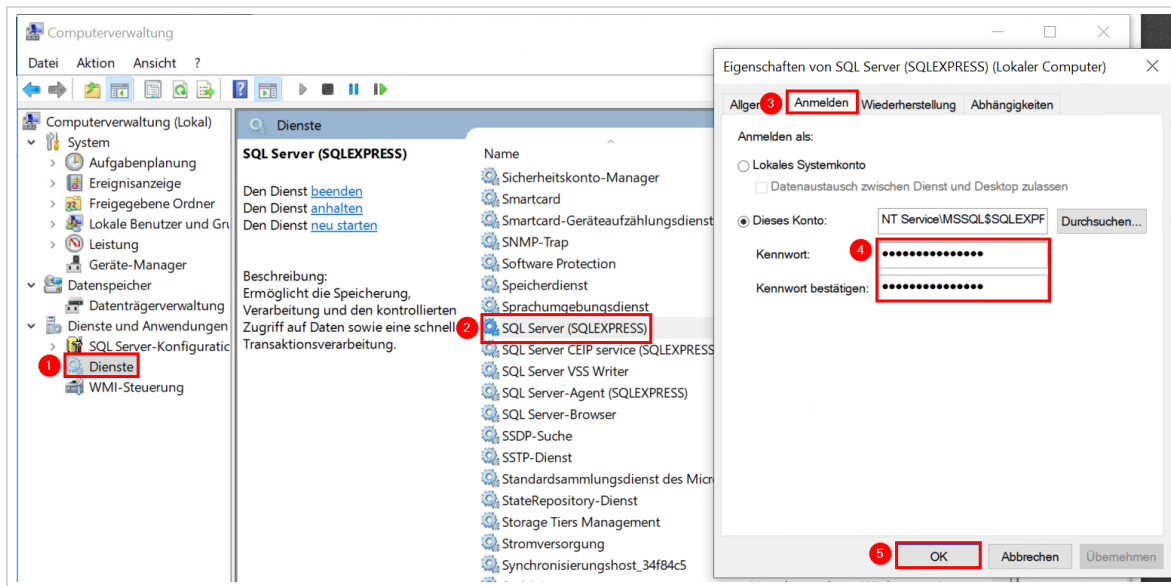


Abb. 29: Änderung des Administrator-Kennwortes für den SQL-Server

3.5 Passwort des lokalen Windows-Administrators ändern



Rechner, die mit opsi installiert werden, bekommen unter Windows das lokale Administrator-Passwort paedmlinux.

Da dies ein potentielles Sicherheitsrisiko darstellt, wurde eine Möglichkeit umgesetzt, wie das lokale Administrator-Kennwort geändert werden kann.

Es wird dringend empfohlen dieses Kennwort zu ändern.

Die Änderung des lokalen Administrator-Kennwortes geschieht über die Gruppenrichtlinie „*paedMLL_Computer*“, welche Sie über die Gruppenrichtlinien-Verwaltung „*gpmc.msc*“ (group policy management console) ändern können.

Sie können auf das Programm zugreifen, in dem Sie in der Admin-VM auf „*Start | Ausführen*“ drücken.

Im sich anschließend öffnenden Fenster geben Sie „*gpmc.msc*“ ein.

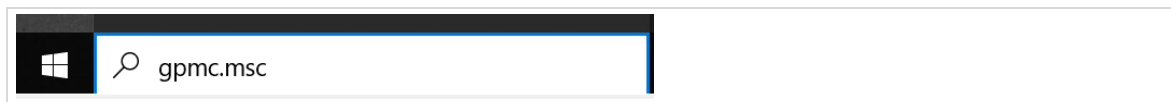


Abb. 30: Ausführen der Gruppenrichtlinien-Verwaltung

Navigieren Sie im Fenster der Gruppenrichtlinien-Verwaltung auf der linken Seite zu dem Gruppenrichtlinienobjekt „*Gruppenrichtlinienverwaltung | Gesamtstruktur: paedml-linux.lokal | Domänen | paedml-linux.lokal | schule | Musterloesung_Computer*“.

Klicken Sie über diesen Eintrag mit der rechten Maustaste und wählen Sie „*Bearbeiten*“.

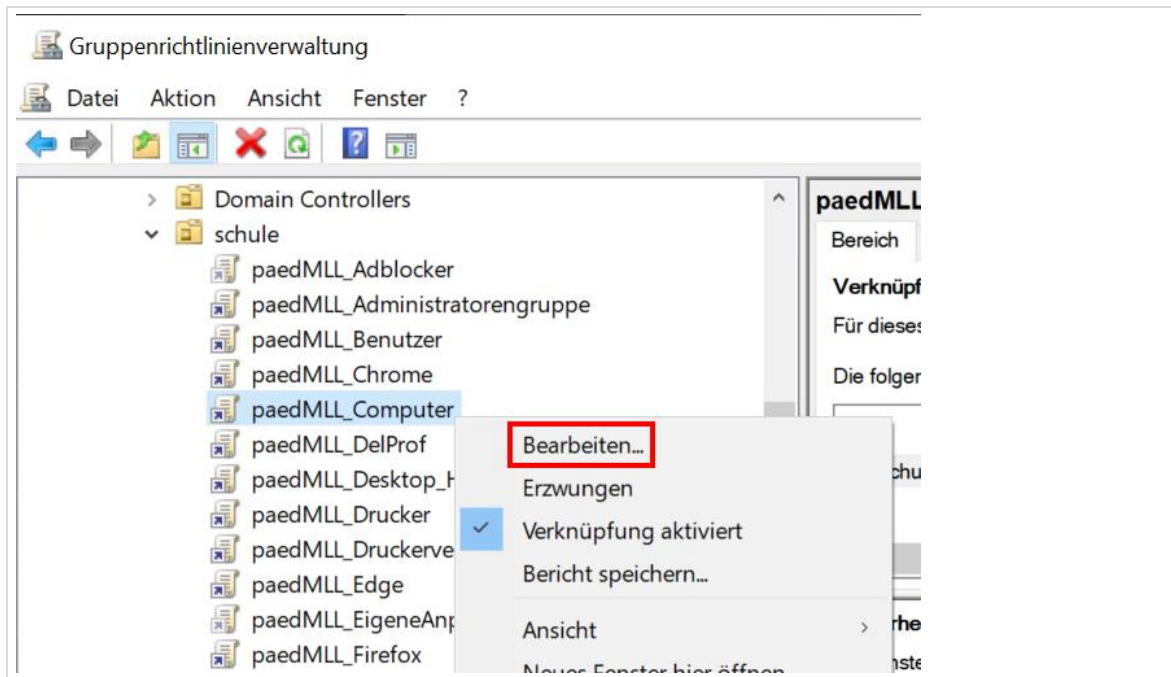


Abb. 31: Bearbeiten von „paedMML_Computer“

Im sich öffnenden „Gruppenrichtlinienverwaltungs-Editor“ wählen Sie den Eintrag „Musterloesung_Computer ... | Computerkonfiguration | Richtlinien | Windows-Einstellungen | Skripts (Start/Herunterfahren)“ (1).

Mit einem Doppelklick auf „Starten“ (2) öffnet sich das Fenster „Eigenschaften von Starten“.

Wählen Sie im Reiter „Skripts“ den Eintrag „\\server\netlogon\ScriptsML\StartUp\setPWLocalAdmin.cmd“ und klicken Sie auf „Bearbeiten“ (3).

Im letzten Arbeitsschritt vergeben Sie im Feld „Skriptparameter“ Ihr neues Kennwort für die Anmeldung des lokalen Administrators (4). Beim Rechnerneustart werden die Gruppenrichtlinien abgearbeitet und das neue Kennwort gesetzt.

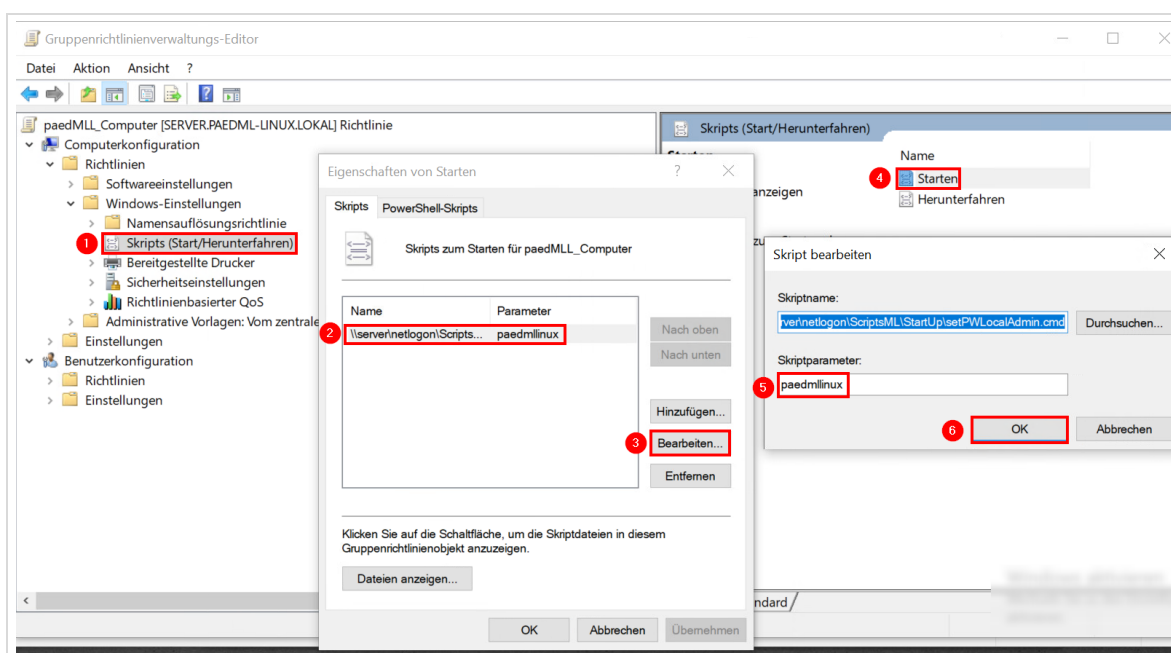


Abb. 32: Setzen des lokalen Administrator-Kennworts



Ändern Sie bitte keine anderen Einstellungen an der Gruppenrichtlinie.

Eigene Einstellungen dürfen nur über die extra hierfür bereitgestellten Gruppenrichtlinie „*paedMLL_EigeneAnpassungen*“ vorgenommen werden!

3.6 Passwort-Policy

3.6.1 Systemgenerierte Passwörter

Die Kennwörter, die die *paedML Linux* beim Benutzerimport anlegt, sind komplex. Sie bestehen aus **mindestens acht Zeichen** mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Passwörter können nicht ausgelesen werden!

3.6.2 Von Benutzern angelegte Passwörter



Das System akzeptiert neue Kennwörter nur, wenn diese sich von den vorherigen Kennwörtern eines Benutzers unterscheiden. Hierbei werden die letzten drei Passwörter berücksichtigt, das heißt nach drei Passwortwechseln darf wieder ein altes Passwort verwendet werden.

Wenn ein Benutzer beispielsweise beim Login unter Windows nach der Änderungsaufforderung dasselbe Passwort verwendet, welches er bereits verwendet hatte, wird er bei jeder Anmeldung an der Schulkonsole erneut aufgefordert das Kennwort zu ändern. Erst durch das Setzen eines neuen Kennworts verschwindet die Änderungsaufforderung.

Die einzige Beschränkung bei benutzergenerierten Kennwörtern ist die Zeichenlänge von **mindestens acht Zeichen bzw. vier Zeichen in der paedML für Grundschulen**.

3.7 Anlegen von Arbeitsgruppen

Aufruf über Schulkonsole (netzwerkberater): Schul-Administration | Arbeitsgruppen verwalten

Über Arbeitsgruppen können Sie Projektarbeiten innerhalb sowie außerhalb des regulären Klassenverbandes abbilden. So könnten Sie der Schulband, die sich aus verschiedenen Klassen zusammensetzt, in einem gleichnamigen Projekt Noten austeilten. Es ist aber auch möglich Projekte in Klassen anzulegen, um Arbeitsgruppen mit Material zu versorgen.

Für jedes Projekt wird ein Ordner nach dem Austeilen in den Home-Laufwerken der Schüler angelegt. Sollten diese Ordner nicht mehr benötigt werden, müssen sie von Hand gelöscht werden. Achten Sie bitte darauf, dass Sie bei der Bezeichnung von Arbeitsgruppen und Klassen keine Leerzeichen verwenden.

Eine genaue Beschreibung für den Umgang mit Arbeitsgruppen finden Sie im Lehrerhandbuch.

4 Verwaltung von Geräten



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* ab Seite 220, vor allem die Hinweise zu Rechner- und Gerätenamen.

4.1 Vorbemerkungen

Die Domäne der *paedML Linux* arbeitet mit Namensauflösung (DNS). Alle Geräte im Netzwerk können über Ihren Netzwerknamen adressiert werden. Die Kenntnis von IP-Adressen ist für den Betrieb der *paedML Linux* daher nicht zwingend notwendig.

Beispiele zur Illustration:

Die Eingabe von <https://server.paedml-linux.lokal> in der Adressleiste Ihres Browsers führt Sie auf die Startseite des Servers.

Netzwerkbefehle wie bspw. `#ping` können ebenfalls auf einen DNS-Namen oder auf eine IP-Adresse ausgeführt werden. Um einen Rechner im Netzwerk zu pingen, kann dieser per Namen oder per IP-Adresse erreicht werden. Der DNS-Name eines Rechners (zum Beispiel `r119-pc09`) ist vermutlich einfacher zu merken als die IP-Adresse `10.1.0.153`.

Bei der Aufnahme von neuen Geräten wird durch die Angabe von `10.1.0.0` (Netzadresse) die nächste freie IP-Adresse aus dem Adresspool der *paedML* vergeben. Sie brauchen sich also eigentlich keine Gedanken über IP-Adressen zu machen.

Allerdings ist ein strukturiertes Netzwerk mit fest vergebenen IP-Adressen durchaus sinnvoll, wenn Sie bspw. im IT-Unterricht mit IP-Adressen arbeiten wollen und hierfür wissen möchten, wie die Rechner in einem Raum zu erreichen sind. Sie können IP-Adressen bei der Rechneraufnahme auch selbst vergeben. Bitte wählen Sie hierfür jeweils eine Adresse zwischen `10.1.0.32` und `10.1.0.229`. Sollte die von Ihnen gewählte Adresse bereits vergeben sein, dann erhalten Sie eine Fehlermeldung.

Wir empfehlen Ihnen ausdrücklich, bei der manuellen Vergabe von IP-Adressen Ihr Netzwerk im Vorfeld der Installation zu planen und die IP-Adressierung entsprechend umzusetzen. Hinweise hierzu finden Sie im oben erwähnten Konzeptionsleitfaden¹⁰.

¹⁰ <https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedmlr-linux/#manuals>

Die folgende Tabelle gibt Ihnen eine Übersicht über den IP-Adressraum der *paedML Linux*.

IP-Adressen	Was befindet sich im Adressraum?	Anzahl der verfügbaren IP-Adressen
10.1.0.0/24	Pädagogisches Netzwerk	254
10.1.0.1 - 10.1.0.20	Reservierte IP-Adressen	20
10.1.0.1	Server	
10.1.0.2	opsi-Server	
10.1.0.10	Router (optionales Gateway für das Routen in andere interne Netzwerke ¹¹)	
10.1.0.11	Firewall	
10.1.0.13	AdminVM (alt)	
10.1.0.15	W10AdminVM	
10.1.0.21 - 10.1.0.229	Arbeitsplatzrechner und Geräte im pädagogischen Netzwerk	209
10.1.0.230 - 10.1.0.254	DHCP-Pool für nicht registrierte Geräte, zum Beispiel bei der Rechneraufnahme	25
Weitere Netzsegmente der <i>paedML Linux</i>		
10.1.1.0/24	separates Lehrernetz	254
172.16.0.0/12	Adressbereich für Gäste-Netz (WLAN) – Anschluss über Firewall	1.048.576
10.1.2.0/24	Kleines pädagogisches Netz	254
10.2.0.0/16	Großes pädagogisches Netz	65534
172.20.0.0/14	Adressbereich für MDM-Netz – Anschluss über Firewall	262142

Tabelle 5: IP-Adressen der *paedML Linux*.

4.1.1 Rechnertypen

Bei der Aufnahme eines neuen Rechners in die *paedML Linux* bekommt der Rechner einen Namen, eine IP-Adresse (optional: eine Inventarnummer) und eine Systemrolle, bzw. einen Systemtypen zugewiesen.

Bevor ein Gerät in die Domäne aufgenommen wird, sollte geklärt werden, um was für einen „Typ“ Gerät es sich handelt. Diese Zuordnung bestimmt, wie das Gerät von der *paedML* verwaltet wird. Bei der Aufnahme von Geräten in das Schulnetz stehen verschiedene Gerätetypen zur Auswahl:

¹¹ Wird benötigt, falls die Schule über VLAN mehrere Netzwerke abbilden will.

Rechner-Typ Schulkonsole	Typ in CSV-Datei	Erklärung
Windows-System	windows	Client mit Windows
Gerät mit IP-Adresse	ipmanagedclient	Drucker, Printserver, WLAN-Access-Points

Tabelle 6: Gerätetypen der paedML Linux

Bitte beachten Sie die folgenden Hinweise:

- Der Typ „Windows-System“ wird für alle Clients verwendet, die Mitglied der *paedML* Domäne sind und mit *Microsoft Windows*-Betriebssystem betrieben werden. Dies ist unabhängig davon, ob die Rechner über Netzwerk gebootet und von opsi mit Software versorgt werden oder nicht.
- Bei Auswahl des Typs „Gerät mit IP-Adresse“ wird kein Computerkonto in der *Samba*-Domäne angelegt.
- Im Computerraummodul werden nur Clients des Typs „Windows-System“ angezeigt.

4.1.2 Hinweise zum Rechnertyp „Windows-System“

Windows-Rechner werden über den auf dem Backup-Server laufenden Dienst opsi verwaltet und von dort aus mit Betriebssystem, Software und Updates versorgt. Die Konfiguration läuft über den opsi-config-editor (siehe auch Kapitel 0 ab Seite 67).



Bitte beachten Sie, dass unterschiedliche Windows 10 Versionen unterschiedlich lange unterstützt werden. Wählen Sie eine Version, die möglichst lange unterstützt wird.¹²

Als Client-Betriebssysteme wird deshalb die deutsche Version von *Windows 10 Education* (64-Bit) **Build 20H2 und 21H2 (Voraussetzung: opsi 4.2)** empfohlen. Andere Versionen sollten **nicht** auf dem OPSI-Server eingespielt werden.

4.2 Aufnahme von Geräten in das paedML Netz



Achten Sie bei der Aufnahme der Rechner darauf, welche Firmware-Variante in den Rechnern verbaut ist. Das bisherige Firmware-System BIOS wird durch den Nachfolger UEFI¹³ abgelöst, der in neuer Computerhardware verbaut ist.

opsi verwaltet Rechner mit den verschiedenen Firmware-Varianten unterschiedlich. Daher muss bei der Clientintegration darauf geachtet werden, um welches System es sich handelt.

¹² Details finden Sie unter: https://en.wikipedia.org/wiki/Windows_10#Updates_and_support

¹³ http://de.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

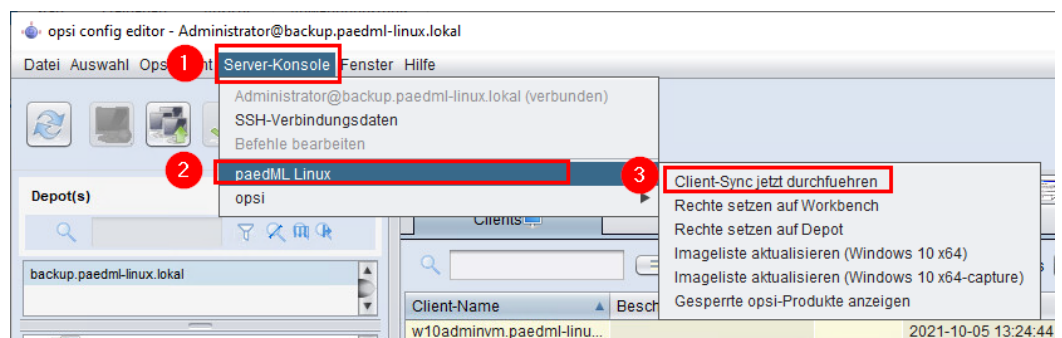
Im Folgenden wird an den entsprechenden Stellen darauf hingewiesen, dass Sie darauf achten müssen, ob ein PC mit BIOS oder mit UEFI und mit oder ohne Secure Boot¹⁴ läuft.

Ein falsch angelegtes System kann nur durch Löschen und Neuaufnahme korrigiert werden.

Zulässige Zeichen für den Hostnamen sind Buchstaben ohne Umlaute, Ziffern sowie das Minuszeichen. Wir empfehlen dringend, den Hostnamen in Kleinbuchstaben zu schreiben. Die Bezeichnungen in der Schulkonsole und in opsi müssen identisch sein. Außerdem darf die Länge von Gerätenamen 14 Zeichen nicht überschreiten. Weitere Angaben zur Nomenklatur entnehmen Sie bitte Anhang A ab Seite 221.



Bitte beachten Sie, dass die Synchronisation der Clients zwischen Server und opsi-Server aus Performancegründen alle 15 Minuten stattfindet. Soll die Synchronisation manuell angestoßen werden (z.B. nachdem ein oder mehrere Clients in der Schulkonsole aufgenommen wurden), führen Sie bitte folgenden Befehl über den opsi-config-editor aus:



Um einen neuen Client in die *paedML Linux* aufzunehmen, können Sie zwei Wege beschreiten:

1. Rechneraufnahme über die *Schulkonsole* (empfohlen)
2. Rechneraufnahme über eine Rechnerliste an der Konsole des Servers

Diese beiden Aufnahmeverfahren setzen voraus, dass Sie alle MAC-Adressen¹⁵ der Netzwerkkarten kennen. Die Rechneraufnahme kann in diesen Fällen bequem von einem Schreibtischstuhl aus erledigt werden.

¹⁴ Vgl. https://de.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface#Secure_Boot

¹⁵ MAC-Adressen sind die eindeutigen IDs der Netzwerkkarten (vgl. <http://de.wikipedia.org/wiki/MAC-Adresse>)

4.2.1 Vorbereiten der Clients

Um einen schuleigenen Rechner in Ihr Schulnetz aufzunehmen, schließen Sie diesen an das Netzwerk Pädagogik an (vgl. Grafik auf Seite 12).

Starten Sie den Rechner und stellen Sie im BIOS bzw. UEFI die Bootreihenfolge so ein, dass der Rechner zuerst über das Netzwerk (PXE-Boot), dann von der die Festplatte startet. Diese Einstellung sollte dauerhaft vorgenommen werden, damit spätere Änderungen¹⁶ beim Hochfahren der Rechner angewandt werden können.

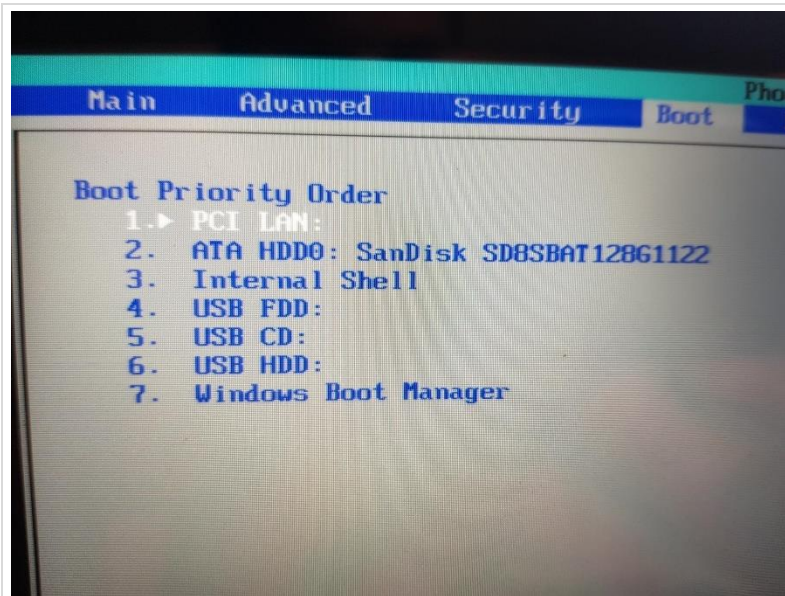


Abb. 33: Bootreihenfolge im Bios Menü einstellen

Speichern Sie die Einstellung.

4.2.2 Rechneraufnahme über die Schulkonsole

Aufruf über Schulkonsole (netzwerkberater): Schul-Administration | Rechner (Schulen)

Eine Möglichkeit, Rechner in das Netzwerk zu integrieren, bietet die Schulkonsole. Bitte beachten Sie, dass Sie für diesen Weg alle MAC-Adressen der aufzunehmenden Rechner kennen müssen.

Melden Sie sich als Netzwerkberater an der Schulkonsole an und öffnen Sie das Menü „Schul-Administration“. Hier wählen Sie den Menüpunkt „Rechner (Schulen)“.

¹⁶ Zum Beispiel Neuinstallation, Imagerestaurierung,... Diese Prozesse werden teilweise von *opsi* beim Systemstart initiiert.

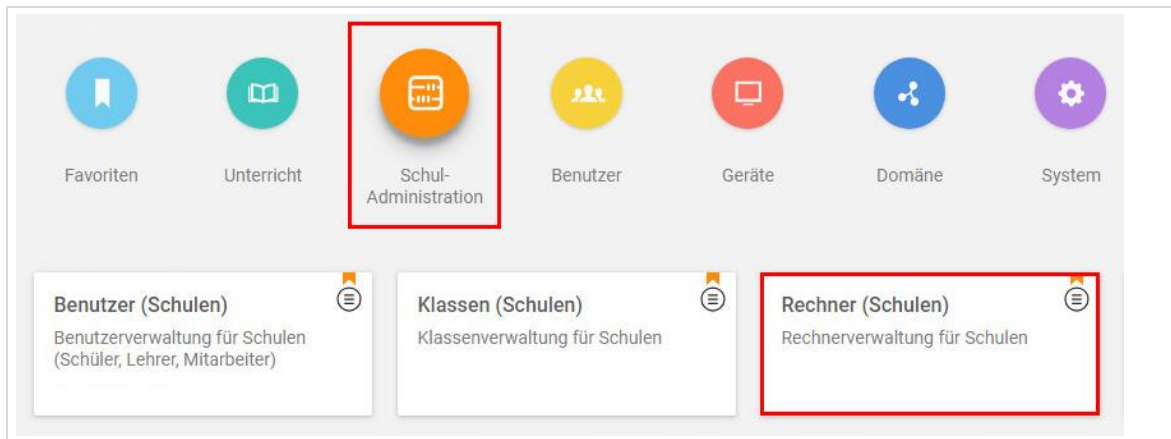


Abb. 34: Neuanlegen von Rechnern über Menüpunkt Rechner Schulen

Es öffnet sich eine neue Maske mit der Übersicht über alle im System angelegten Geräte. Klicken Sie oben links auf den Knopf „Hinzufügen“, um ein neues Rechnerobjekt zu erstellen.

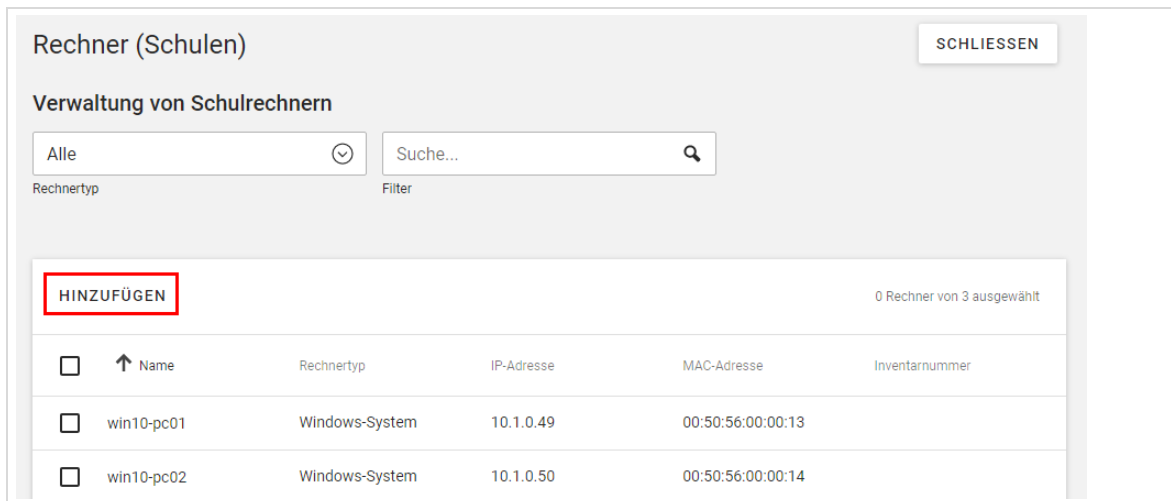


Abb. 35: Rechnerobjekt hinzufügen

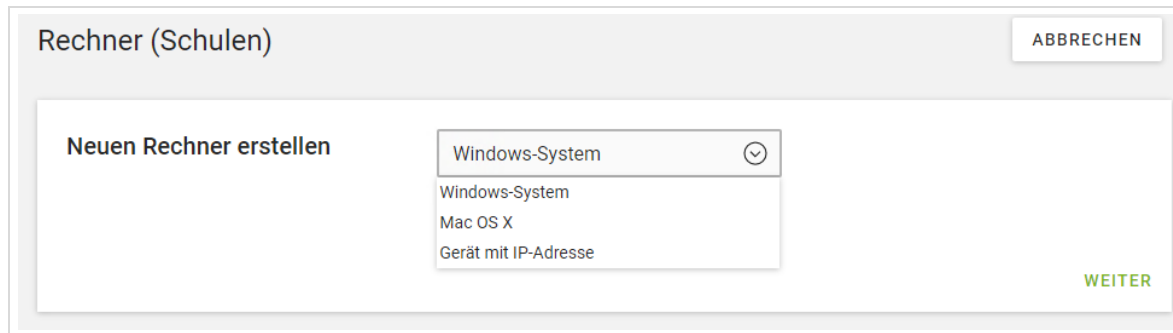
In der nächsten Maske können Sie bestimmen, welches Betriebssystem der Rechner später bekommen soll. Das Dropdown-Menü „Typ“ gibt Ihnen hierfür verschiedene Auswahlmöglichkeiten.

Wählen Sie „Windows-System“, wenn es sich um einen Windows-Rechner handeln soll.

Der Rechnertyp „Mac OS X“ wird derzeit in der paedML Linux nicht verwendet.


Der Eintrag Gerät mit IP-Adresse ist für Netzwerkgeräte, z.B. Printserver bzw. WLAN-Accesspoints vorgesehen. Hierbei wird für das Gerät eine DHCP-Adresse reserviert und ein DNS-Eintrag erstellt. Es wird kein Computerkonto angelegt.

Bestätigen Sie Ihre Auswahl mit „Weiter“.



Rechner (Schulen) ABBRECHEN

Neuen Rechner erstellen

Windows-System 

Windows-System
Mac OS X
Gerät mit IP-Adresse

WEITER

Abb. 36: Welcher Client soll in das Schulnetzwerk integriert werden?

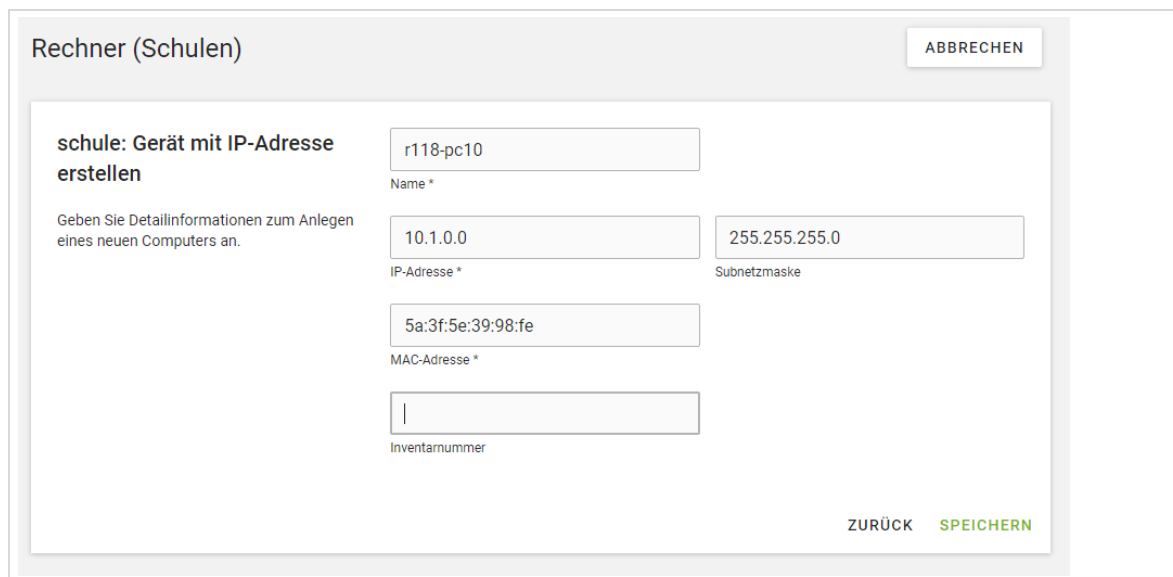
Die folgende Maske hilft Ihnen dabei, den Rechner für die Domäne zu konfigurieren. Geben Sie hierfür den „Namen¹⁷“ und die „IP-Adresse“ des Rechners ein. Die Eingabe der Netz-Adresse „10.1.0.0“ vergibt die nächste freie IP-Adresse im Adresspool. Wenn Sie eine eigene Adresse vergeben wollen, dann wählen Sie bitte eine Adresse zwischen 10.1.0.21 und 10.1.0.229.

Der Wert der „Subnetzmaske“ ist vorgeschrieben und darf **nicht** geändert werden.

Die „MAC-Adresse“ des aufzunehmenden Rechners muss in das entsprechende Feld eingetragen werden. Bitte beachten Sie für die Einrichtung eines Computers mit mehreren Netzwerkkarten den Hinweis am Ende dieses Unterkapitels.

Falls Ihre Hardware inventarisiert ist, können Sie die „Inventarnummer“ angeben.

Speichern Sie die Werte mit „Weiter“, um Änderungen zu übernehmen. Falls das System Fehler entdeckt (doppelte Namen, MAC- oder IP-Adressen, nicht zulässige Sonderzeichen) bekommen Sie eine Meldung mit der Aufforderung, den Datensatz zu korrigieren.



Rechner (Schulen) ABBRECHEN

schule: Gerät mit IP-Adresse erstellen

Geben Sie Detailinformationen zum Anlegen eines neuen Computers an.

Name *

IP-Adresse *

Subnetzmaske

MAC-Adresse *

Inventarnummer

ZURÜCK SPEICHERN

Abb. 37: Rechneraufnahme

¹⁷ Bitte achten Sie unbedingt darauf, Namen für Objekte in der Schule eindeutig zu vergeben.

Das System quittiert die Neuaufnahme mit einem Hinweis, der nur kurz eingeblendet wird.

Wenn Sie wollen, können Sie anschließend weitere Rechner aufnehmen oder das Untermenü verlassen.

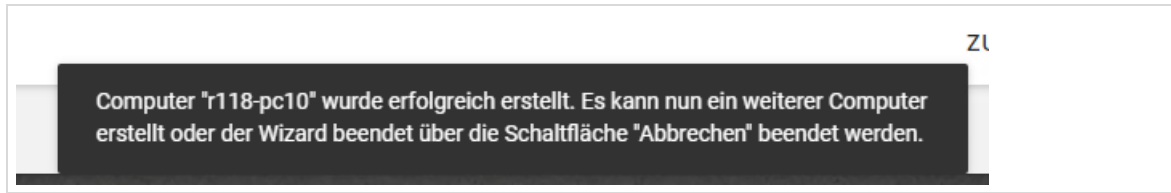


Abb. 38: Computer wurde erfolgreich erstellt Bild aktualisieren



Wenn Sie Geräte mit UEFI-Firmware einsetzen, beachten Sie bitte Kapitel 4.2.4 auf Seite 55.

4.2.3 Aufnahme über Rechnerliste

Das erste Verfahren ist sinnvoll, wenn Sie die gleichzeitige Aufnahme mehrerer Clients durchführen. Diese Aufnahme kann über eine Text-Datei erfolgen.

Die Text-Datei für skriptbasierten Client-Import benötigt die folgenden Felder:

	Feld	Beschreibung	Beispiel
1	Rechner-Typ	Siehe Tabelle 6: Gerätetypen der <i>paedML Linux</i>	windows
2	Hostname ¹⁸	Name des Clients Bitte achten Sie auf Kleinschreibung.	pcraum2-pc12
3	MAC-Adresse	Wird für DHCP benötigt	00:0c:29:12:34:56
4	LDAP-OU	die LDAP-Schul-OU „schule“	schule ¹⁹
5	IP-Adresse / Netzmaske ²⁰	IP-Adresse und Netzmaske des Clients	10.1.0.0/24
6	Inventarnummer	optionale Inventarnummer	5146 Zimmer 114
7	Zone	In der <i>paedML</i> nicht belegt	

Tabelle 7: Felder der CSV-Datei für den skriptbasierten Client-Import

¹⁸ Bitte beachten Sie hierzu die Hinweise zur Nomenklatur in Anhang A

¹⁹ Dieser Wert muss „schule“ heißen, da alle Objekte der *paedML Linux* im LDAP-Container „schule“ gespeichert werden!

²⁰ Die Angabe der Netzmaske ist obligatorisch, wenn Sie die Netzerweiterung umgesetzt haben. Weitere Informationen diesbezüglich siehe <https://docs.software-univention.de/ucsschool-handbuch-4.4.html#school:schoolcreate:computers>

Hinweise:

Die ersten fünf Felder sind **Pflichtfelder**, um einen Rechner einzurichten. Jedes Rechnerobjekt muss in eine eigene Zeile geschrieben werden.

- Verwenden Sie als Trennzeichen zwischen den Feldern einen *Tabulator*.
- Das Feld 6 ist optional, Feld 7 ist derzeit nicht belegt. Fügen Sie entsprechend *Tabulatoren* ein.
- Der Hostname muss in der ganzen Schule eindeutig sein.
- Zulässige Zeichen sind Buchstaben ohne Umlaute, Ziffern sowie das Minuszeichen.
- Rechner mit mehreren MAC-Adressen können beim Import nur eine Adresse zugewiesen bekommen. Die Einrichtung mehrerer MAC-Adressen wird ab Seite 53 beschrieben.
- Die *LDAP-OU* ist in der *paedML Linux* immer „schule“.
- Wird als IP-Adresse ein Subnetz angegeben (z.B. *10.1.0.0*), wird dem Client automatisch die nächste freie IP-Adresse aus diesem IP-Subnetz zugewiesen. Sie können hier aber auch eine feste IP-Adresse aus dem Adressbereich *10.1.0.32 - 10.1.0.229* vergeben.
- Die Netzmaske (im Feld „IP-Adresse“ einzugeben) kann sowohl als *Prefix (/24)* als auch in *Oktettschreibweise (255.255.255.0)* angegeben werden. **Die Angabe der Netzmaske ist obligatorisch, wenn Sie die Netzerweiterung umgesetzt haben.** Wird sie weggelassen, wird die Netzmaske *255.255.255.0* angenommen.

Die folgenden Felder (Feld sechs und sieben) sind optional, das bedeutet, dass der Import auch ohne diese Felder durchgeführt werden kann. Beachten Sie jedoch, dass die Reihenfolge eingehalten werden muss, falls Sie eines dieser Felder benutzen.

- Die *Inventar-Nummer* kann Buchstaben und Zahlen enthalten.
- Es folgen **zwei leere Felder, wenn Sie keine Inventarnummer angeben** (Trennzeichen = Tabulator).

Beispiel einer Importdatei:

```
windows pc01 d2:13:96:26:47:91 schule 10.1.0.0/24 → →
windows pc02 52:13:96:26:48:09 schule 10.1.0.0/24 → →
```

Exportieren Sie die Rechner-Liste in eine Text-Datei. Nennen Sie die Datei „*rechner.txt*“.



Achten Sie beim Import von Listen (Benutzerlisten/Gerätelisten) auf die richtige Zeichencodierung²¹ (Character Encoding) der Dateien.

Unterstützt wird nur der Zeichensatz ANSI. Bei anderen Zeichensätzen kann es zu Problemen beim Import von Daten kommen.

Die eben exportierte Datei „*rechner.txt*“ muss nun in das Home-Verzeichnis des Benutzers „*Administrator*“ kopiert werden, z.B. mit Hilfe von *WinSCP* oder dem *Windows-Explorer* (Vgl. Kapitel 1.4.2, Seite 31).

²¹ <http://de.wikipedia.org/wiki/Zeichenkodierung>



Das Kopieren der Datei auf den Server sollte von einem Rechner erfolgen, der im pädagogischen Netzwerk angeschlossen ist und per DHCP eine IP-Adresse bekommen hat. Außerdem sollten *WinSCP* (optional) und *PuTTY* auf dem Rechner installiert sein.

Öffnen Sie anschließend *PuTTY* (vgl. Kapitel 1.4.1 auf Seite 30) und loggen Sie sich mit den Zugangsdaten des Benutzers „*root*“ auf dem Server ein. Sie können sich auch direkt an einer Serverkonsole anmelden.

Navigieren Sie in das Verzeichnis, in das die Datei importiert wurde (`#cd /home/Administrator`). Führen Sie folgenden Befehl aus (ergänzen Sie dabei „*IMPORTDATEI.txt*“ durch den Namen Ihrer Datei):

```
#/usr/share/ucs-school-import/scripts/import_computer IMPORTDATEI.txt >>
/var/log/client_import.log 2>&1
```

Der Umbruch des Befehls ist darstellungsbedingt. Schreiben Sie den Befehl in eine Zeile!

Die importierten Rechnerobjekte werden nun so konfiguriert, dass jedes Mal, wenn sich ein Rechner an der Domäne anmeldet, dieser die angegebene IP-Adresse zugeordnet bekommt und der angegebene Hostname über das *Domain Name System* (DNS) aufgelöst werden kann. Der Befehl generiert keine Rückmeldung an der Server-Konsole. Ob der Import erfolgreich war, können Sie mithilfe der Log-Datei „*/var/log/client_import.log*“ oder in der Schulkonsole (Schul-Administration | Rechner (Schulen)) überprüfen.

```
Processing line 1: windows      pc01      d2:13:96:26:47:91      schule 10.1.0.0$
generate computer pc01 (school schule)
Network 10.1.0.0/24 exists in school schule!
creating object cn=pc01,cn=computers,ou=schule,dc=paedml-linux,dc=lokal
```

Abb. 39: Ausschnitt aus „*client-import.log*“

HINZUFÜGEN					0 Rechner von 9 ausgewählt
<input type="checkbox"/>	↑ Name	Rechnertyp	IP-Adresse	MAC-Adresse	Inventarnummer
<input type="checkbox"/>	pc01	Windows-System	10.1.0.57	d2:13:96:26:47:91	
<input type="checkbox"/>	pc02	Windows-System	10.1.0.58	52:13:96:26:48:09	

Abb. 40: Neu angelegte Rechner in der Schulkonsole (Schul-Administration | Rechner (Schulen))



Wenn Sie Geräte mit UEFI-Firmware einsetzen, beachten Sie bitte das folgende Kapitel.

4.2.4 Clients mit UEFI-Firmware

UEFI-Geräte werden nach der Rechneraufnahme als solche im *opsi-configd* definiert. Eine ausführliche Anleitung zu *opsi* und dem *opsi-configd* finden Sie ab Seite 67.

Öffnen Sie dazu den opsi-configed, wählen Sie den UEFI-Client aus (1), setzen Sie den Haken bei „Uefi Boot“ und speichern Sie die Konfiguration mit einem Klick auf den roten Haken ab (3). Setzen Sie diesen Haken NUR bei Geräten des Typs „Windows-System“!

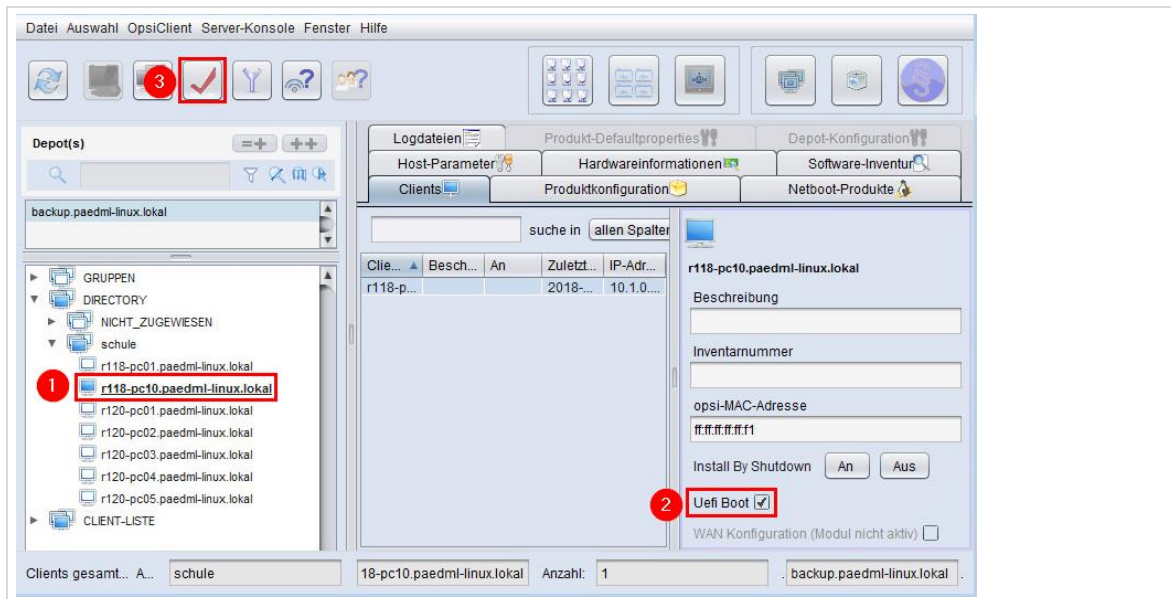


Abb. 41: UEFI-Boot aktivieren

4.3 Geräte mit mehreren Netzwerkkarten (z.B. WLAN und Kabelnetzwerk)

Aufruf über Schulkonsole (als Administrator): Geräte | Rechner

Die Aufnahme von Clients über eine Import-Datei ist in Kapitel 4.2.3 auf Seite 53 beschrieben. In diesem Abschnitt wird beschrieben, wie an Rechner weitere Netzwerkkarten zugewiesen werden, die bisher nur mit einer Netzwerkkarte im System geführt werden. Dies ist z.B. bei Laptops der Fall, die mit Kabelnetzwerk und WLAN betrieben werden sollen. Die Zuweisung einer weiteren Netzwerkkarte erfolgt über die Eintragung einer weiteren MAC-Adresse.

Hierfür müssen Sie nach dem Anlegen des Rechners in die *Schulkonsole* wechseln und das Rechnerobjekt bearbeiten. Sie können jedem Gerät weitere MAC-Adressen zuweisen.



Pro Rechner darf es nur eine IP-Adresse geben.

Es können in einem Rechnerobjekt mehrere Netzwerkkarten hinterlegt werden. So kann beispielsweise ein Laptop mit Kabelverbindung und mit WLAN-Karte im Netz betrieben werden. Der Rechner bekommt vom Server immer die gleiche IP –Adresse bei der Anmeldung am Netzwerk.



Die hier beschriebenen Einstellungen haben den Vorteil, dass die Rechner immer mit derselben IP-Adresse (Kabel oder WLAN) an das Netzwerk angeschlossen sind.

Wichtig: Die Beschränkung auf eine IP-Adresse ist notwendig, da sowohl das Computerraum-Modul der Schulkonsole sowie opsi nur mit einer IP-Adresse pro Client umgehen können!

Hinweis: Der gleichzeitige Anschluss beider Netzwerkkarten sollte vermieden werden, da nur eine Karte die richtige IP-Adresse bekommt.

Im Menüpunkt „Geräte / Rechner“ finden Sie eine Liste aller Clients des Schulnetzes. Wählen Sie sich das Gerät, dem Sie eine zweite Netzwerkkarte zuweisen wollen und öffnen Sie dieses mit einem Mausklick.

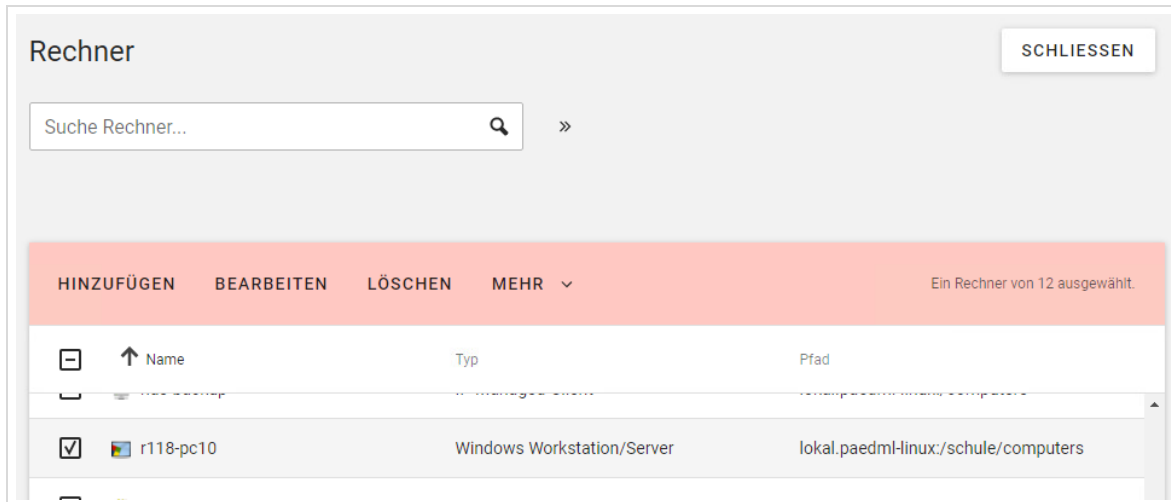


Abb. 42: Auswahl des zu bearbeitenden Gerätes

Scrollen Sie in dem sich öffnenden Fenster bis zu den „Netzwerk-Einstellungen“. Drücken Sie auf das **+** Symbol und tragen Sie in das entsprechende Feld unter der vorhandenen „MAC-Adresse“ die MAC-Adresse der zweiten Netzwerkkarte ein.



Abb. 43: Eintragen einer weiteren MAC-Adresse

Scrollen Sie noch weiter nach unten bis zu dem Feld „DHCP“. Dort befinden sich drei Dropdownmenüs, die wie folgt befüllt werden müssen:

Feld	Wert
DHCP-Dienst	schule
IP-Adresse	Dieselbe Adresse, die der Rechner schon für die andere Netzwerk-Karte zugewiesen bekommen hat.
MAC-Adresse	Die oben eingegebene MAC-Adresse der zweiten Netzwerkkarte

Tabelle 8: Einträge im Feld DHCP

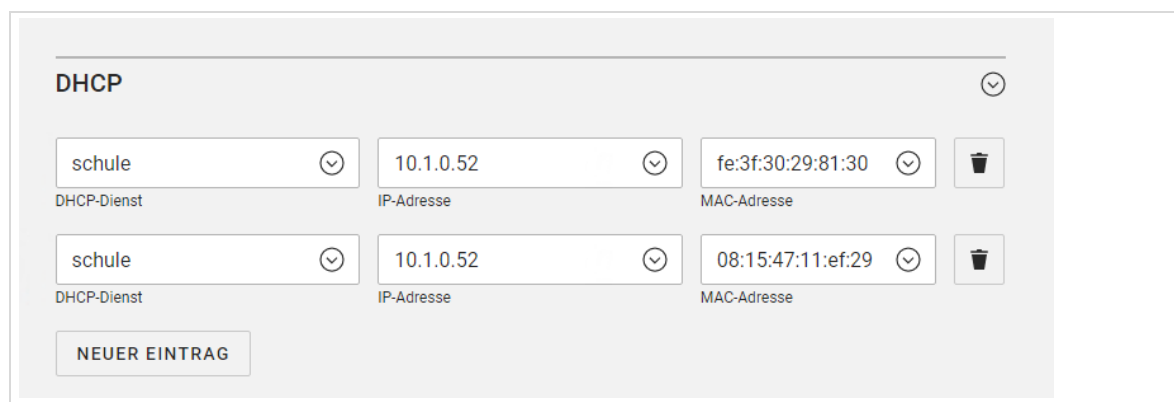


Abb. 44: Einstellungen für den DHCP-Server

Übernehmen Sie die Änderungen mit „SPEICHERN“.

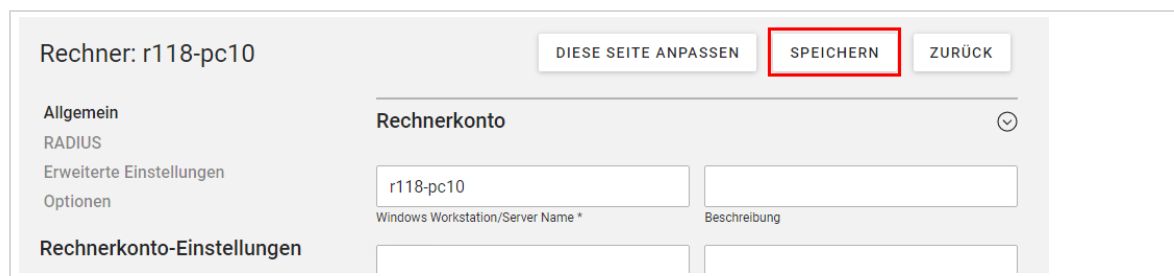


Abb. 45: Änderungen speichern



Mögliche Probleme mit Tablets:

Da Tablets in der Regel nicht über Netzwerkkarten verfügen, gibt es häufig die Möglichkeit mit USB-Ethernet-Adaptern eine Kabelverbindung zum Netzwerk herzustellen. Über diese Kabelverbindung kann ein Gerät beispielsweise mit neuer Software versorgt werden. Jeder dieser USB-Ethernet-Adapter hat eine eigene MAC-Adresse.

ACHTUNG! Da diese USB-Geräte mobil sind, könnte der USB-Ethernet-Adapter zu einem anderen Tablet wandern und die Client-Registrierung, welche an die MAC-Adresse gebunden ist, würde fälschlicherweise mitwandern. Folgende Fehler könnten hierbei auftreten:

- Geräte erhalten evtl. die falsche IP-Adresse – zunächst nicht schlimm
- Im Computerraum werden die Geräte im falschen Raum angezeigt, bzw. es wird das falsche Tablet als online angezeigt – störend.
- Beim Rollout wird das falsche Gerät ausgerollt, bzw. nichts ausgerollt – problematisch.

Im Falle eines Rollouts muss der Administrator sicherstellen, dass das richtige Gerät mit dem richtigen Adapter ausgerollt wird.

Daher empfehlen wir pro Tablet einen eigenen Adapter zu beschaffen. Alle Adapter sollten mit der MAC-Adresse beschriftet und (per Markierung) einem Gerät zugewiesen werden. Jedes Tablet sollte ausschließlich mit dem ihm zugewiesenen Adapter betrieben werden.

4.4 Integration von weiteren Geräten

Die bisher beschriebenen Verfahren gelten für Rechner, die von der *paedML* verwaltet werden sollen. Diese Rechner werden in der Regel über *opsi* installiert und bekommen Softwarepakete über *opsi* verteilt. Es gibt jedoch Geräte, die nicht in diese Kategorie fallen.

Hierzu zählen zum Beispiel:

- Netzwerkgeräte (wie Router, Switches, Accesspoints) mit eigener IP-Adresse
- Drucker mit Netzwerkanschluss
- Computer, die in das Netzwerk aufgenommen, aber nicht via *opsi* verwaltet werden sollen²².

Diese Geräte werden wie oben beschrieben in das Netzwerk eingebunden, es wird jedoch bei der Auswahl des Computertyps der Wert „Gerät mit IP-Adresse“ ausgewählt. Bei Verwendung dieses Typs wird nur eine DHCP-Reservierung angelegt und kein Computerkonto in der Domäne.



Für Geräte, die nicht der Schule gehören, empfehlen wir ausdrücklich eine Anbindung über das *Gäste-Netz*.

²² Zum Beispiel Rechner, die mit OEM-Lizenzen beschafft wurden oder Maschinen, die von Kollegen betreut werden, die nicht als Netzwerkberater agieren. Wir möchten in diesem Zusammenhang darauf hinweisen, dass private Rechner jedweder Art nichts im Schulnetz zu suchen haben. Deren Einbindung sollte über das Gäste-Netz geschehen.

4.5 Ändern und Löschen von Geräten

4.5.1 Neuer Name bestehender Geräte



Da das Umbenennen von Geräten über die Schulkonsole nicht möglich ist, müssen Sie Geräte löschen und neu anlegen, wenn deren Name geändert werden soll.

Dieser Löschvorgang wird im folgenden Abschnitt beschrieben.

Anschließend müssen alle neu angelegten Rechner erneut mit opsi eingerichtet werden (Betriebssystem und Software).

4.5.2 Löschen bestehender Geräte

Aufruf über Schulkonsole (als Administrator): Geräte | Rechner

Die Verwaltung der Rechner geschieht über das Schulkonsolenmodul „Geräte | Rechner“, das Sie als *Administrator* aufrufen müssen.

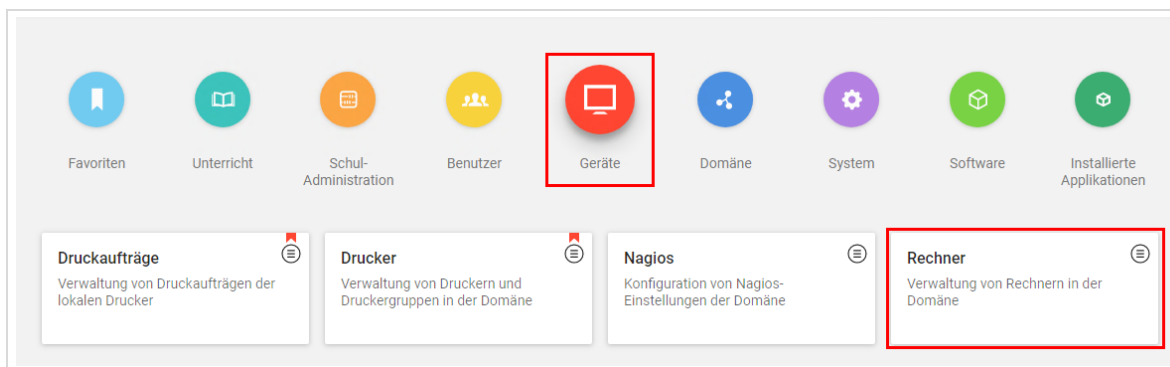


Abb. 46: Aufruf der Rechnerverwaltung

Nach Aufruf des „Rechner“-Moduls bekommen Sie eine Liste aller im System angelegten Geräte angezeigt. Hier werden nicht nur Rechner, sondern alle Geräte, also auch Drucker und andere „Geräte mit IP-Adresse“ angezeigt.

Um einen Eintrag zu löschen, markieren Sie die Checkbox vor dem Gerät. Oberhalb der Liste werden jetzt Schaltflächen angezeigt. Klicken Sie auf die Schaltfläche „Löschen“, um den Eintrag aus dem System zu entfernen.



Bitte beachten Sie, dass in dieser Liste ALLE Geräte der *paedML Linux* angezeigt werden und ein unbedachtes Löschen (zum Beispiel das Entfernen des Servers) unangenehme Folgen haben kann.

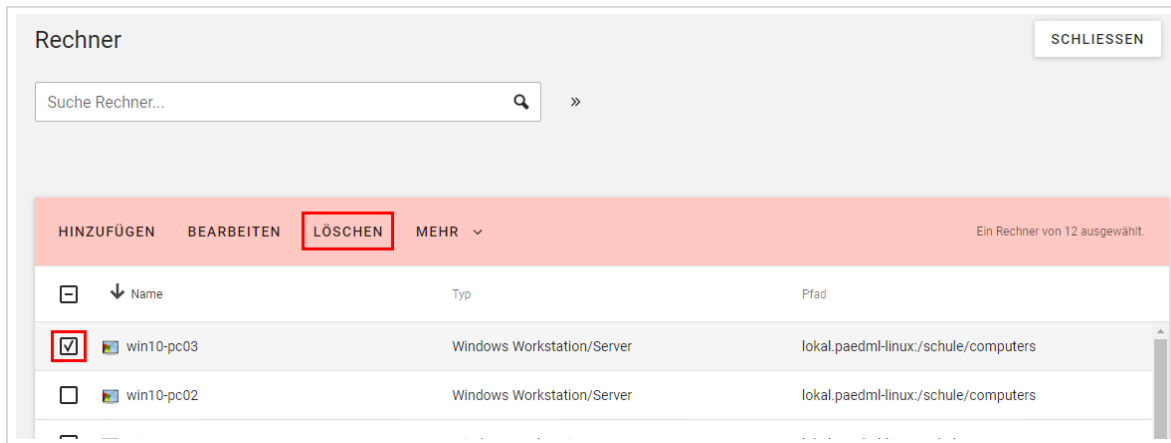


Abb. 47: Ein Rechner wurde zum Löschen markiert.

Bevor das Gerät aus dem System gelöscht werden kann, müssen Sie in einem Dialogfenster den Löschvorgang bestätigen. Achten Sie dabei darauf, dass der Haken bei „Zugehörige Objekte löschen“ gesetzt ist.

Starten Sie nun den opsi-configed. Klicken Sie auf den soeben entfernten Rechner mit der rechten Maustaste und klicken Sie dann auf „Lösche Clients“.

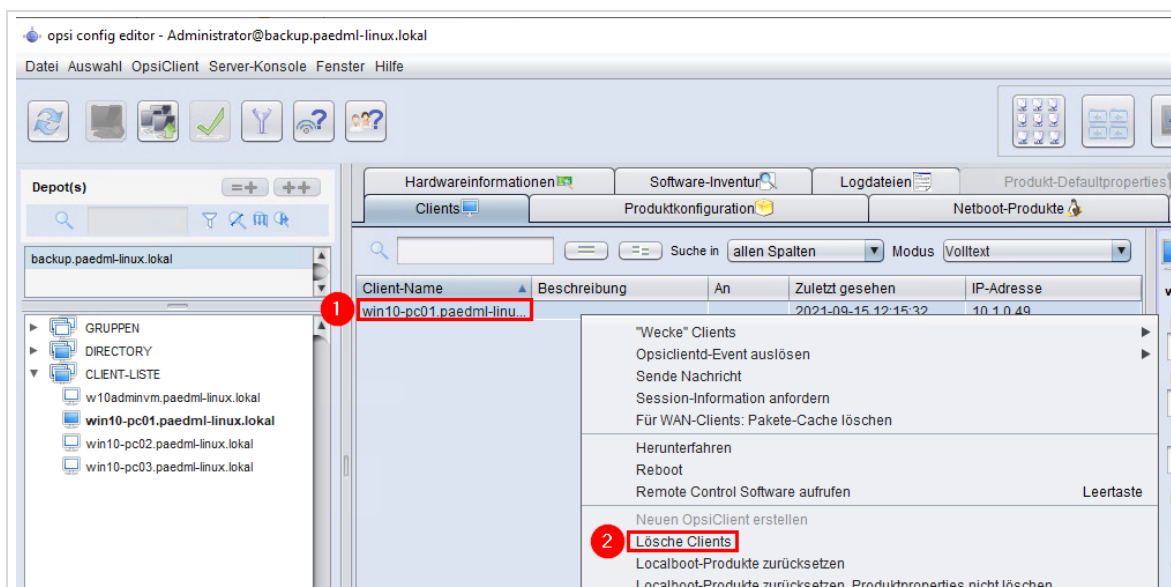


Abb. 48: Ein Rechner wurde zum Löschen markiert.

5 Verwaltung der Computerräume

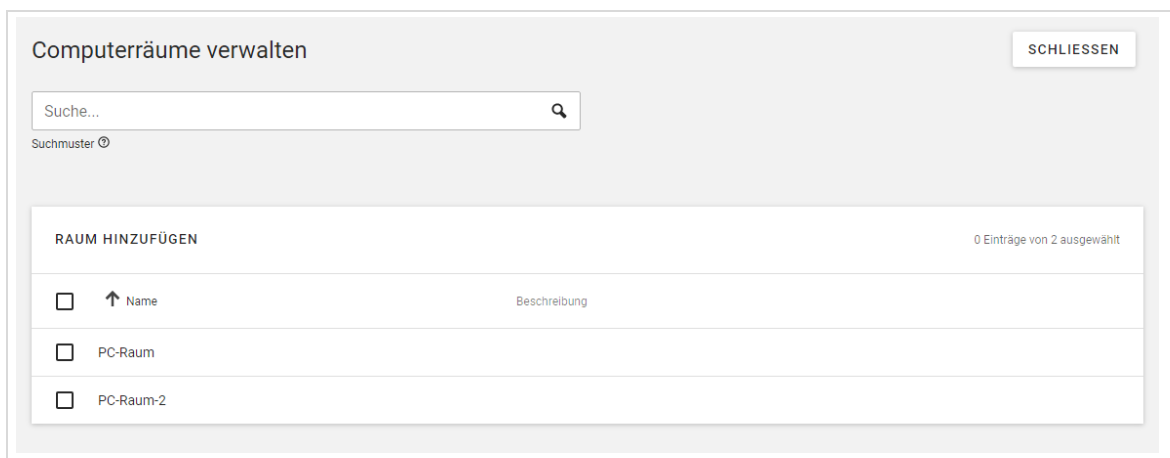
Aufruf über Schulkonsole (Administrator): Schul-Administration | Computerräume verwalten



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 221.

Um neue Computerräume hinzuzufügen, melden Sie sich als „netzwerkberater“ an der Schulkonsole an.

Im Menü „Schul-Administration | Computerräume verwalten“ werden die in Kapitel 4 angelegten Geräte der Schule einem Computerraum zugeordnet. Diese Computerräume können von den Lehrern während des Unterrichts verwaltet werden, etwa indem der Internetzugang freigegeben wird.



RAUM HINZUFÜGEN		0 Einträge von 2 ausgewählt
<input type="checkbox"/>	↑ Name	Beschreibung
<input type="checkbox"/>	PC-Raum	
<input type="checkbox"/>	PC-Raum-2	

Abb. 49: Übersicht über die Computerräume

5.1 Anlegen von Computerraum und Zuweisung von Geräten



Es gibt keine Überprüfung, ob ein Computer bereits einem Raum zugeordnet wurde, daher können Rechner verschiedenen Räumen zugewiesen werden. Dies sollte nach Möglichkeit vermieden werden!

Andernfalls erscheinen die Rechner in verschiedenen Computerräumen und Lehrende könnten sich bei der Bedienung der Schulkonsole in die Quere kommen. Wenn beispielsweise beim Unterrichten in Raum A ein Client gesperrt wird, der in Raum B steht und beiden Räumen zugewiesen ist, würde der Client (ohne Wissen der Lehrkraft in Raum B) gesperrt werden.

Mit dem Knopf „Raum hinzufügen“ wird ein neuer Computerraum angelegt.

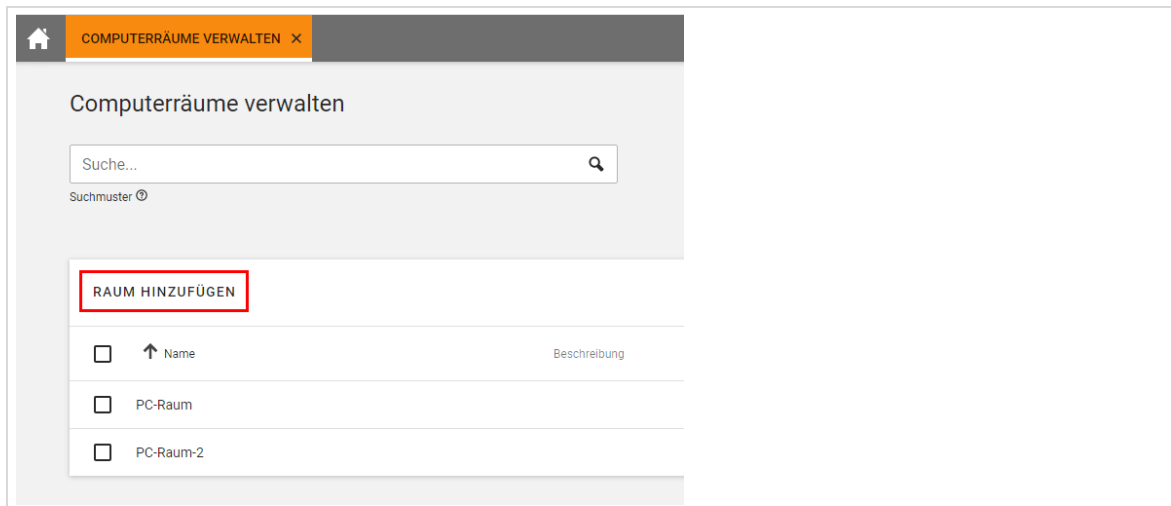


Abb. 50: Computerraum hinzufügen

Tippen Sie einen Namen (1) und eine optionale Beschreibung des Raumes (2) ein.

Belassen Sie das Computerraum Backend auf „Italc (Standard)“ (3).

Im Abschnitt „Computer“ werden alle dem Raum zugewiesenen Computer angezeigt. Wenn Sie auf „HINZUFÜGEN“ klicken (4), können Sie weitere Rechner hinzufügen.

Das sich öffnende Fenster „Objekte hinzufügen“ verfügt über eine Suchfunktion, über die Sie nach Computern suchen können. Wenn Sie nichts eingeben und auf das Lupensymbol klicken werden alle im System registrierten Geräte angezeigt. Geben Sie einen Teil eines bekannten Namens ein, dann wird danach gesucht.

Wählen Sie aus, welche Objekte in den Raum aufgenommen werden sollen (5) und klicken Sie anschließend auf „HINZUFÜGEN“ (6).

Wenn die Bearbeitung eines Computerraumes abgeschlossen ist, wird das Ergebnis gespeichert, damit die Änderungen aktiv werden (7).

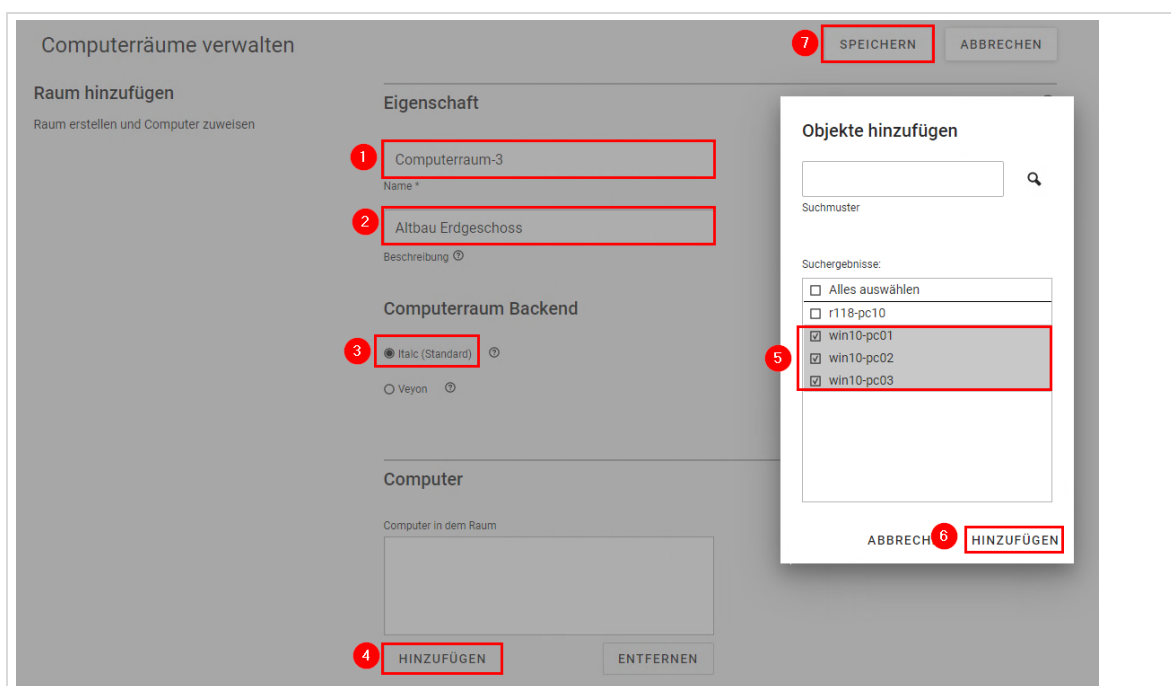


Abb. 51: Hinzufügen eines neuen Computerraumes

Die Erstellung des Computerraums ist nun abgeschlossen. Mit „Bearbeiten“ können Sie später auch noch Computer und Geräte hinzufügen.

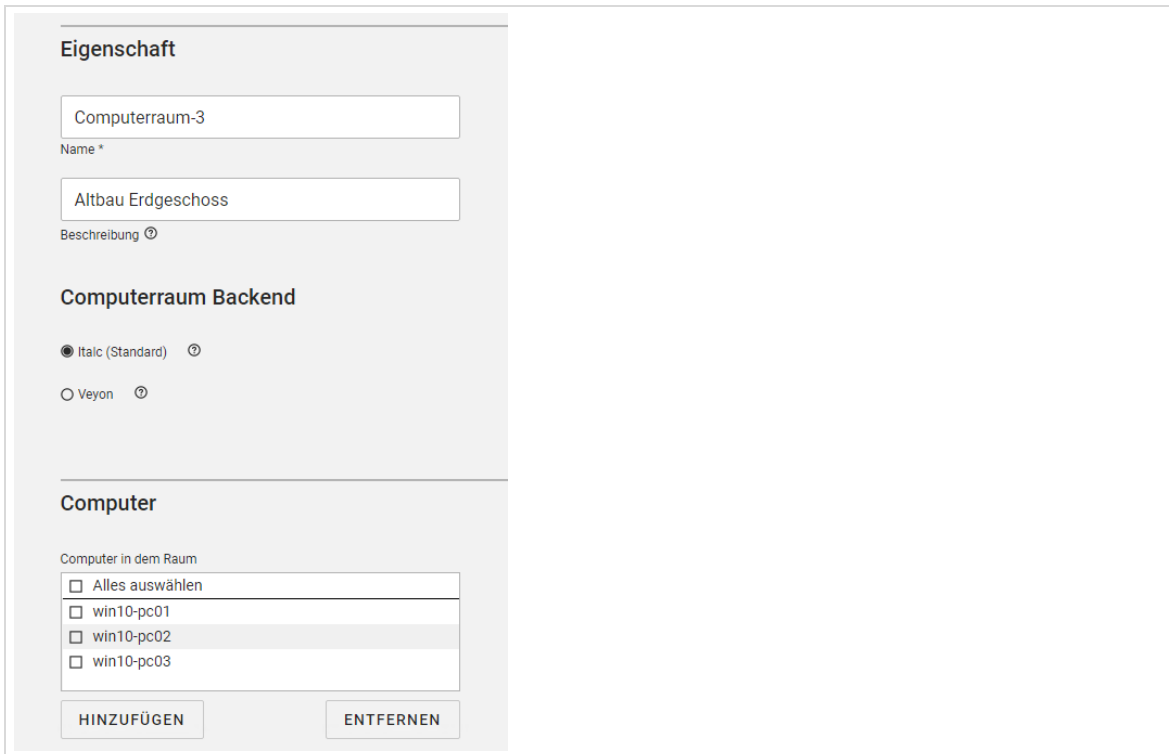


Abb. 52: Der neu angelegte Raum mit allen darin befindlichen Clients

5.2 Lehrercomputer definieren

Lehrercomputer werden von der Internetsperre ausgenommen. Sie können Lehrercomputer im Modul „Computerräume verwalten“ definieren, indem Sie einen Haken vor den Computer setzen und dann auf Speichern klicken.

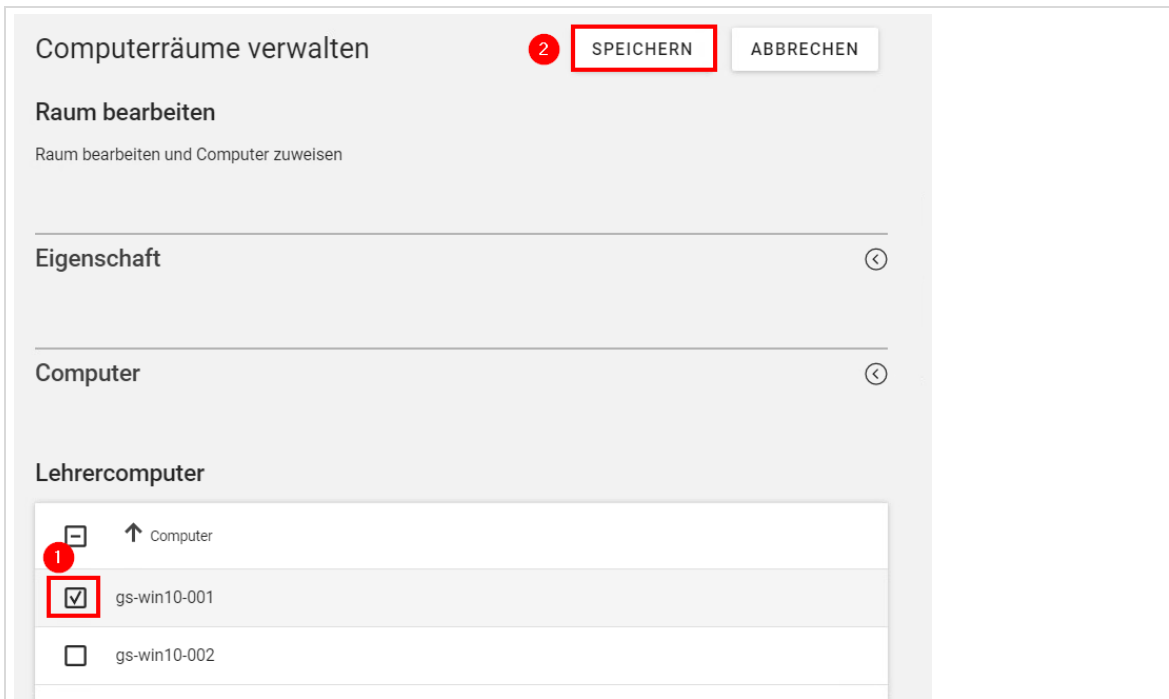
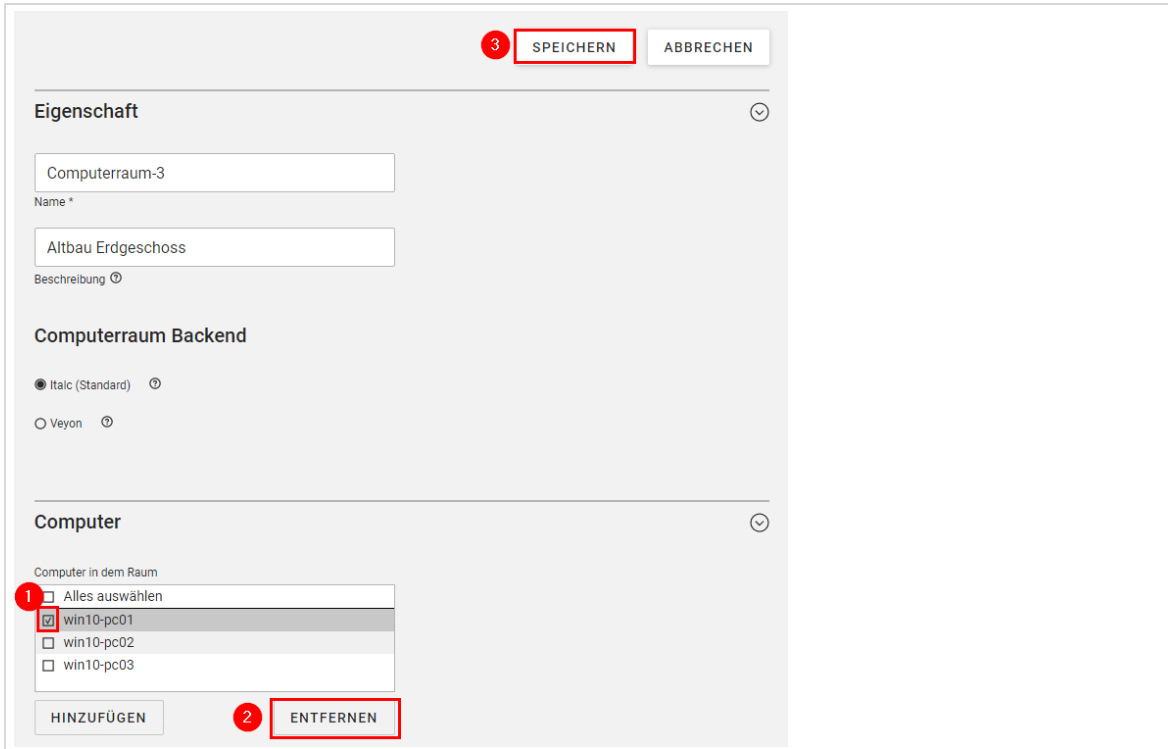


Abb. 53: Lehrercomputer definieren

5.3 Entfernen von Rechnern aus Computerräumen

Wenn Sie Rechner aus einem Raum löschen wollen, dann wählen Sie den jeweiligen Raum in der Übersicht der Computerräume aus. Anschließend aktivieren Sie die Checkbox vor dem Rechnernamen (Auswahl mehrerer Objekte möglich). Ein Klick auf „Entfernen“ löscht die ausgewählten Objekte aus dem Raum, das Gerät selbst wird dabei aber nicht gelöscht. Klicken Sie abschließend auf „Speichern“.



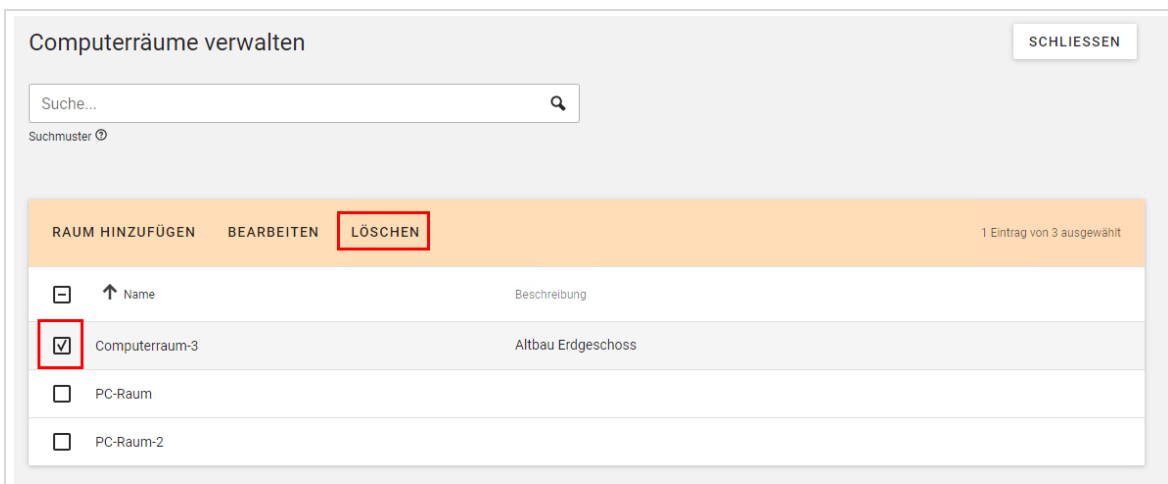
The screenshot shows the 'Computer' management interface. At the top, there are buttons for 'SPEICHERN' (highlighted with a red box and a red '3') and 'ABBRECHEN'. Below this is the 'Eigenschaft' section with fields for 'Name' (Computerraum-3) and 'Beschreibung' (Altbau Erdgeschoss). The 'Computerraum Backend' section shows radio buttons for 'Italc (Standard)' and 'Veyon'. The 'Computer' section shows a list of computers in the room. The 'win10-pc01' checkbox is selected (marked with a red '1'). The 'ENTFERNEN' button is highlighted with a red box and a red '2'. The 'SPEICHERN' button is highlighted with a red box and a red '3'.

Abb. 54: Computer aus Räumen entfernen

5.4 Entfernen von Computerräumen

Bereits angelegte Computerräume können nachträglich über die Computerraumverwaltung bearbeitet oder gelöscht werden. Aktivieren Sie in der Übersicht die Checkbox vor einem Raum und klicken Sie auf „Löschen“, um den Raum zu löschen. Es ist nicht möglich, mehrere Räume gleichzeitig zu löschen. Bevor der Löschvorgang ausgeführt wird, erscheint eine Abfrage, die bestätigt werden muss.

Die Geräte, die einem Raum zugeordnet sind, werden nicht gelöscht, wenn der Raum gelöscht wird.



The screenshot shows the 'Computerräume verwalten' interface. At the top right is a 'SCHLIESSEN' button. Below is a search bar labeled 'Suche...' and 'Suchmuster'. The main section has buttons for 'RAUM HINZUFÜGEN', 'BEARBEITEN', and 'LÖSCHEN' (highlighted with a red box). Below these buttons is a table with columns for 'Name' and 'Beschreibung'. The first row is 'Computerraum-3' with 'Altbau Erdgeschoss' as the description. The checkbox for 'Computerraum-3' is selected (marked with a red box). The second row is 'PC-Raum' and the third row is 'PC-Raum-2'. A status bar at the bottom right indicates '1 Eintrag von 3 ausgewählt'.

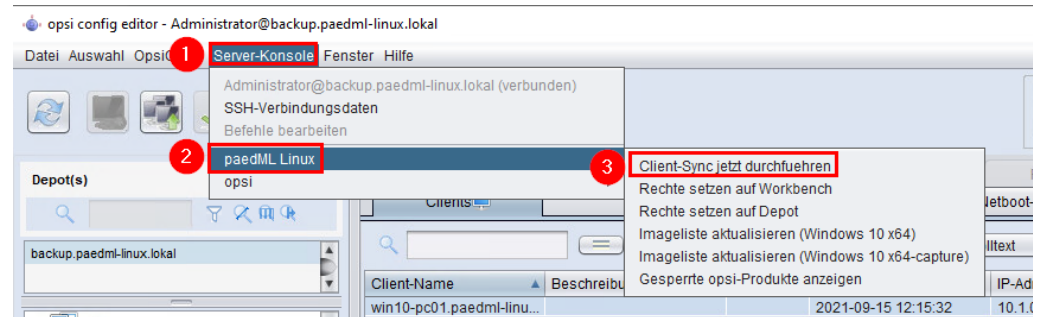
Abb. 55: Computerraum löschen

6 Einrichtung der Arbeitsplatzrechner

Der Aufruf erfolgt über die opsi-Anwendung (opsi configuration editor), die lokal auf Rechnern installiert werden kann. Im Auslieferungszustand ist der opsi-configed auf der W10AdminVM bereits installiert.



Bitte beachten Sie, dass die Synchronisation der Clients zwischen Server und opsi-Server aus Performancegründen viertelstündlich stattfindet. Soll die Synchronisation manuell angestoßen werden (z.B. nachdem ein oder mehrere Clients in der Schulkonsole aufgenommen wurden), führen Sie bitte einen „Client-Sync“ über den opsi-configed aus:



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 221.

6.1 opsi-Lizenzierung

opsi-Lizenzierung im Rahmen der paedML gültig ab 01.08.2022

Seit Sommer 2022 ist neben den opsi-Erweiterungen UEFI, Secureboot, Local Image/WinVHD und Directory Connector auch das mySQL-Backend für paedML Schulen lizenziert.

Jede paedML-Schule erhält vom Landesmedienzentrum Baden-Württemberg jährlich eine Freischaltung bis 500 Clients für Ihren opsi-Server.

Verwaltet eine Schule mehr als 500 Clients mit opsi, so sind für die zusätzlichen Clients opsi-Subscriptionskosten ab dem 501 Client in Höhe von 2 € pro Client / pro Jahr fällig, ab dem 1001 Client 1,5 € pro Client / pro Jahr.

Die Mengen sind in 50er Schritten erweiterbar.

Zusätzliche opsi-Erweiterungen, die nicht in der paedML enthalten sind, können als Subscription ab dem 1. Client zum Subscriptionspreis von 1,5 € pro Client / pro Jahr und ab dem 1001 Client 1 € pro Client / pro Jahr lizenziert werden. Mindestmenge sind hier 500 Clients.

Für ein konkretes Angebot wenden Sie sich bitte an paedml@uib.de.

Voraussetzung ist die Version UCS 4.4-9 errata1233 oder höher.

6.2 Unterstützte Betriebssysteme



Bitte beachten Sie, dass unterschiedliche Windows 10 Versionen unterschiedlich lange unterstützt werden. Wählen Sie eine Version, die möglichst lange unterstützt wird.²³ Dies sind die Versionen, die meist im Herbst herausgebracht werden.

Als Client-Betriebssysteme wird deshalb die deutsche Version von *Windows 10 Education* (64-Bit) **Build 20H2 und 21H2 (Voraussetzung: opsi 4.2)** empfohlen. Andere Versionen sollten **nicht** auf dem OPSI-Server eingespielt werden.

Windows 10 Education

Windows 10 Education entspricht im Wesentlichen der Enterprise Version, darf aber nur an Bildungseinrichtungen eingesetzt werden und ist deshalb kostengünstiger als die Enterprise-Edition.

Windows 10 Education bietet weitreichende Konfigurations- und Einstellmöglichkeiten, welche im Hinblick auf den Datenschutz und Administration an Schulen wichtig sein können und in Windows 10 Pro nicht möglich sind.

Dazu zählen u.a.:

²³ Details finden Sie unter: https://en.wikipedia.org/wiki/Windows_10#Updates_and_support

- Sperre des Microsoft Stores: Mit aktiviertem Microsoft Store ist es Benutzern möglich, Apps auch ohne Administratorrechte zu installieren.
- Übermittlung von Telemetriedaten an Microsoft deaktivieren
- Deaktivieren des Sprachassistenten „Cortana“ (*Standardeinstellung in der Education Edition*)
- Anpassen der Taskleiste und des Startmenüs mithilfe von Gruppenrichtlinien

6.3 Einführung in opsi

Das Clientmanagementsystem *opsi* („*open pc server integration*“) wird zur Verwaltung von *Windows*-Clients verwendet. Mit *opsi* können Sie das Betriebssystem ausrollen, Software verteilen und die Rechner des Schulnetzes mit Updates versorgen.



opsi ist ein umfangreiches Softwaremanagement-System, dessen gesamter Funktionsumfang in dieser Anleitung nicht abgebildet werden kann.

Wir beschreiben hier, die für den Betrieb der *paedML Linux* wesentlichen Features von *opsi*. Wenn Sie nähere Informationen zu *opsi* benötigen, dann nehmen Sie bitte Kontakt mit der Hotline auf.

Weitergehende Informationen zu *opsi* finden Sie auf der Webseite des Herstellers unter <http://uib.de/de/opsi-dokumentation/dokumentationen>.

opsi wird als „Gesamtpaket“ auf dem *paedML*-System „*opsi-Server*“ installiert. *opsi* besteht aus mehreren Komponenten, deren Zusammenspiel dafür sorgt, dass die Arbeitsplatzrechner mit Software versorgt werden:

1. Auf dem *opsi-Server* (Backup-Server) läuft eine *Datenbank*, in der gespeichert wird, welche Software auf einem Rechner installiert ist. In dieser Datenbank werden alle *opsi*-Aktionen protokolliert. Hier finden sich Einträge über erfolgte oder fehlgeschlagene Installationen. Pakete, die installiert werden sollen, werden mit einem entsprechenden Vermerk versehen.
2. Im sogenannten *opsi-Depot* (Verzeichnis `/var/lib/opsi/depot`) liegen alle Softwarekomponenten (*opsi-Produkte*), die installiert werden können (s. u.).
3. Ein listener-notifier-Mechanismus sorgt dafür, dass bei Bedarf die Software installiert wird.
 - 3.1. Auf dem Server läuft ein Webservice (*opsiconfd*), der die Informationen über neue Softwarepakete an die Clients übermittelt (notifier).
 - 3.2. Auf den Clients läuft ein Agent (*opsi-winst*), der beim Systemstart mit dem Betriebssystem gestartet wird und Befehle von *opsiconfd* entgegennimmt (listener).
 - 3.3. Wenn ein Paket zur Installation vorgemerkt ist, wird dieses auf den Client ausgespielt. Die Installation geschieht in der Regel beim Start der Maschine²⁴, kann über die *opsi*-Management-Konsole aber auch manuell gestartet werden.

²⁴ Hierbei wird – sofern der Rechner über PXE-Boot gestartet wird – eine Routine ausgeführt, über die Software vor dem Start des Betriebssystems verteilt wird.

- Die Konfiguration der *opsi*-Datenbank geschieht über das Programm „*opsi-configd*“. Dieses kann an der Konsole des Backup-Servers mit *opsi*-Befehlen bedient werden. Angenehmer in der Bedienung ist die grafische *opsi*-Management-Konsole. *opsi-configd* kann als Paket auf den Clients installiert oder über einen Webbrowser ausgeführt werden.

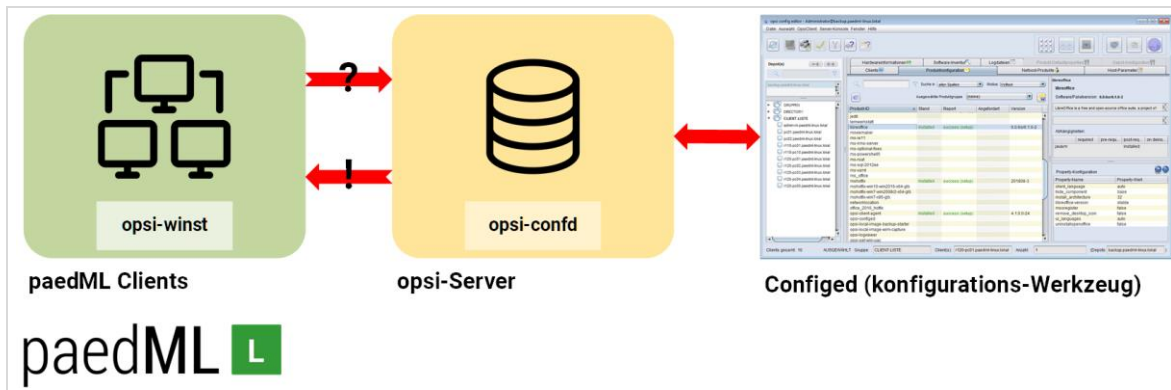


Abb. 56: schematische Darstellung von *opsi*

opsi-Produkte

In der Benutzeroberfläche von *opsi* werden alle installierbaren Softwarekomponenten als *opsi-Produkte* bezeichnet. *opsi-Produkte* werden unterteilt in *Netboot-Produkte* und *Localboot-Produkte*.

- Netboot-Produkte* sind Routinen, die beim Starten eines Rechners über PXE ausgeführt werden. Hierzu zählt die Installation von *Windows* sowie die Erstellung und Wiederherstellung von lokalen Rechnerabbildern.



Generell gilt, dass Rechner, die mit opsi verwaltet werden sollen, immer über das Netzwerk gebootet werden müssen.

Nur so bekommen die Rechner über das Netzwerk ein Signal gesendet, wenn opsi Netboot-Aktionen, wie die Installation von Betriebssystem, das Erstellen oder Wiederherstellen von Backups,... ausführen soll.

- Localboot-Produkte* sind vor allem Anwendungen, die auf den Rechnern installiert werden. Hierzu zählen Officepakete, Internetprogramme und andere Anwendungen. Daneben finden sich in diesem Bereich *Microsoft „Hotfixes“* für *Windows* und *Microsoft Office* sowie Skripte für Aktionen wie den Domänenbeitritt oder das Herunterfahren der Rechner. Diese sind unter dem Reiter Produktkonfiguration zu finden.

opsi verwaltet seine Pakete in einem sogenannten *opsi-Depot*. Der Speicherort auf dem *opsi*-Server ist */var/lib/opsi/depot*. Dieser Ort ist auch als *Windows*-Freigabe aufrufbar.

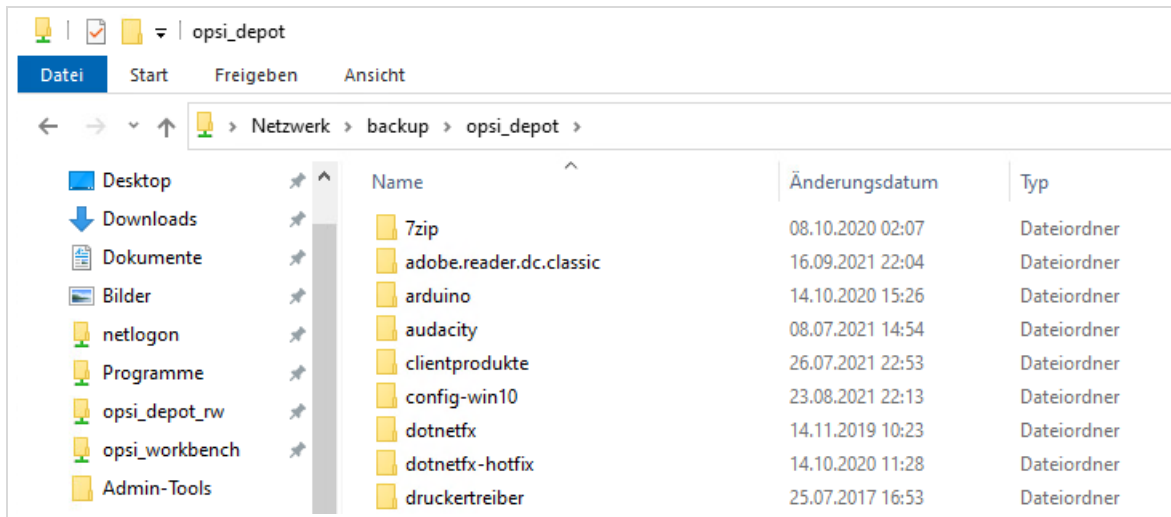


Abb. 57: Einblick in das opsi-Depot via Windows-Explorer

In dieses Verzeichnis werden alle auf Windowsrechnern zu installierenden Softwarepakete abgelegt. Das Einspielen von opsi-Paketen auf dem Backup-Server wird im Kapitel 6.19 auf Seite 112 beschrieben.

6.4 Start des opsi configurations editors

Das opsi-Paket *opsi-configed* kann auf jedem Rechner im Netzwerk installiert werden. Das Programm ist Bestandteil der Standardinstallation der virtuellen Maschine W10AdminVM.

Auf der W10AdminVM ist der opsi-configed Bestandteil des Ordners Admin-Tools

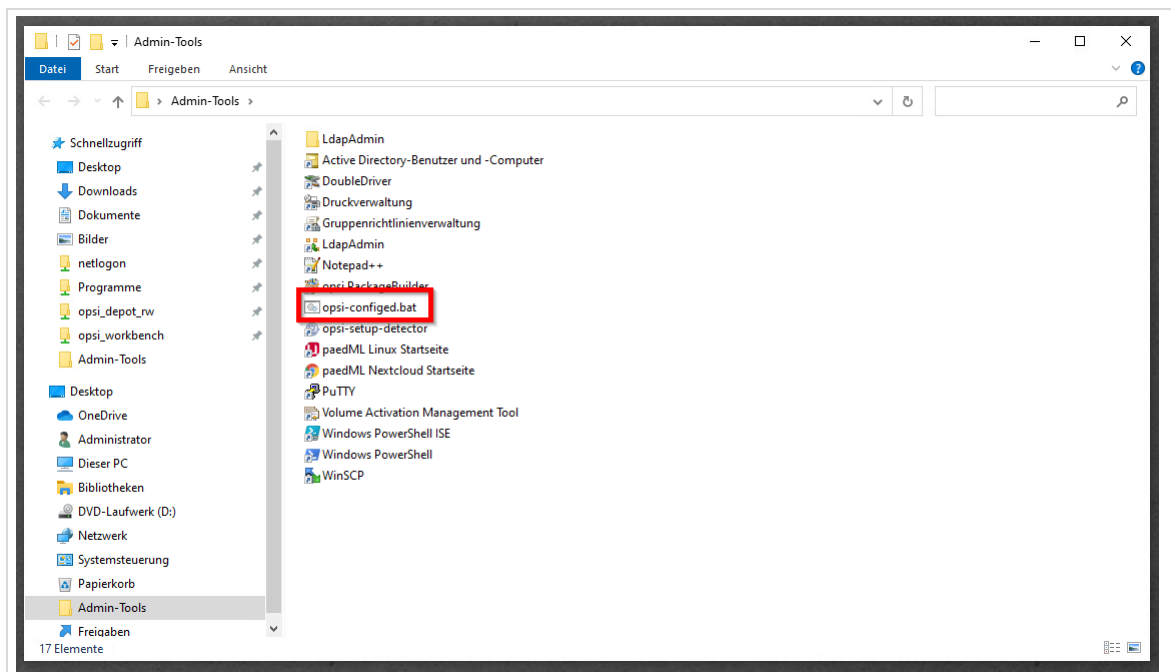


Abb. 58: Aufruf des lokalen opsi-Konfigurationsprogrammes opsi-configed

Wenn Sie das Programm ausführen, werden Sie nach Benutzernamen und Passwort gefragt. Geben Sie hier die Zugangsdaten für den Benutzer *Administrator* (mit großem A) ein.

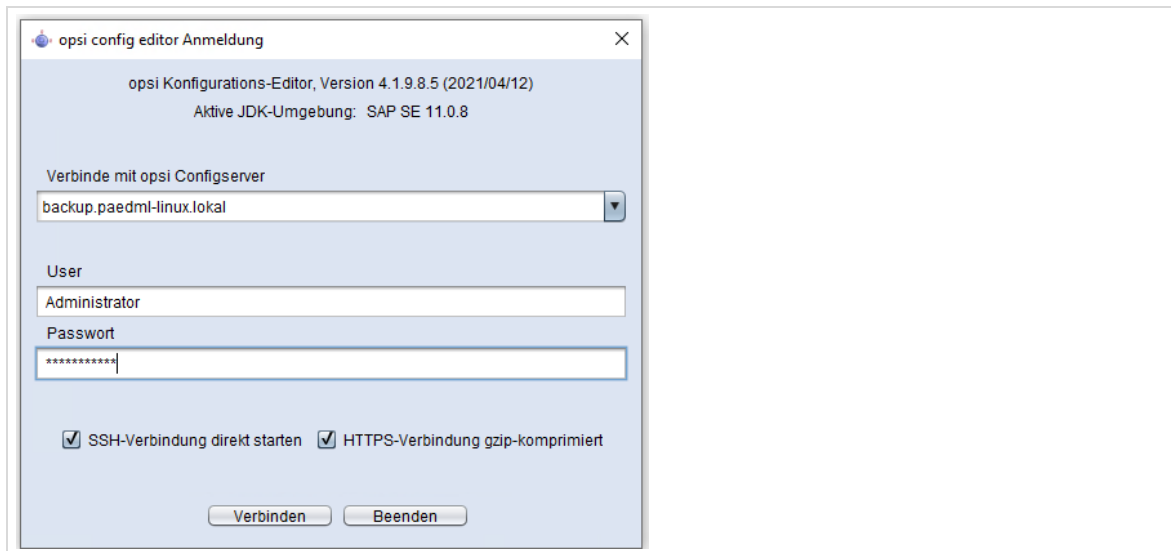


Abb. 59: Anmeldung an der opsi-Konsole als Domänen-Administrator

6.5 Die Benutzeroberfläche






Wir raten davon ab, nicht von uns dokumentierte Änderungen im *opsi-config editor*²⁵ vorzunehmen, da dies zu Problemen bei der Synchronisation mit dem *paedML* Server führen kann.

Sie sollten insbesondere keine Rechner über opsi anlegen oder angelegte Rechnerobjekte mit Hilfe von opsi ändern (zum Beispiel umbenennen von Clients).

Eine Ausnahme stellt das Löschen der Clients dar.

Wir wollen Ihnen hier einen Überblick über die im Schulalltag wichtigsten Funktionen von *opsi* geben, wobei für die Verwaltung der Schulrechner nur ein Teil der *opsi*-Bausteine Relevanz hat. Die hier benannten *opsi*-Elemente haben wir in der Vorstellung der *opsi*-Benutzeroberfläche mit Symbolen gekennzeichnet:

-  - Diese Funktion ist wichtig für die Arbeit im Schulnetz.
-  - Das Modul unterstützt Sie bei der Arbeit, muss aber nicht zwangsweise genutzt werden.
-  - Die Benutzung dieser Funktion führt mit hoher Wahrscheinlichkeit zu Problemen. Bitte nicht benutzen. Dieses Symbol kennzeichnet ferner Module, die nicht im Standardlieferungsumfang der *paedML Linux* enthalten sind (z.B. das Modul „Lizenzverwaltung“).

Die Benutzeroberfläche – der *opsi config editor* – teilt sich in sechs Bereiche auf (s. folgender Screenshot).

1. Die Menüleiste,

²⁵ In dieser Anleitung finden die Begriffe „opsi config editor“ und „opsi-Konsole“ für die Benennung der opsi-Benutzeroberfläche Anwendung.

2. sieben Knöpfe links oben,
3. sechs weitere Knöpfe rechts oben,
4. das Auswahlfenster, in dem Clients und Gruppen für die Konfiguration ausgewählt werden können,
5. das in verschiedene Reiter unterteilte Hauptfenster und
6. ein dynamischer Bereich, der, je nach selektiertem Modul im Hauptfenster mit Inhalt versorgt wird.

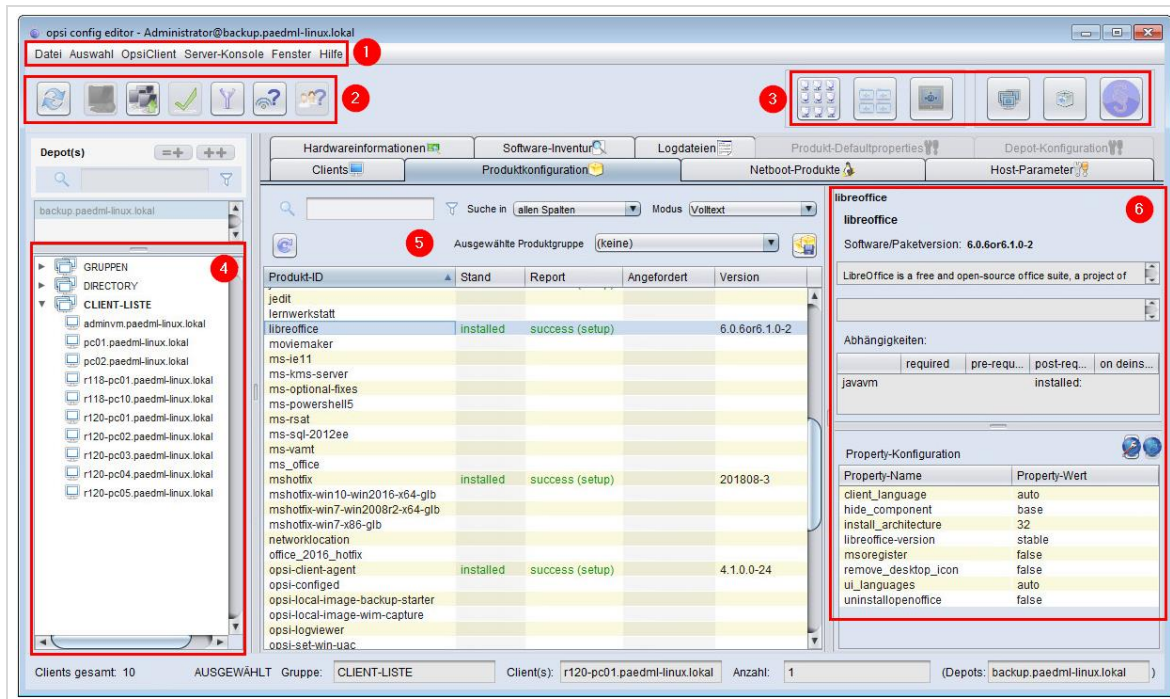


Abb. 60: Übersicht über den opsi config editor

Da in diesem Kapitel immer wieder auf die Übersicht der *opsi*-Konsole Bezug genommen wird, finden Sie die Übersicht über die *opsi*-Konsole nochmals im Anhang. Sie können sich die Grafik für die Arbeit mit diesem Kapitel ausdrucken. Dadurch finden Sie sich hoffentlich schneller zurecht, wenn beispielsweise von der Rechnerliste (4) oder dem Hauptfenster (5) die Rede ist.

1. Die Menüleiste

Hinter der Menüleiste verbergen sich verschiedene Einträge, die größtenteils auch in der Hauptmaske abgebildet werden.

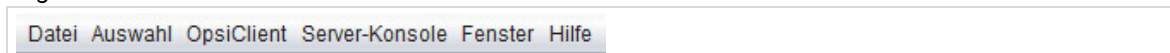


Abb. 61: Die Menüleiste von opsi

1.1. Unter „Datei“ befinden sich die folgenden Menüeinträge:

- 1.1.1. * „Speichern der Konfiguration“
- 1.1.2. * „Alle Daten neu laden“
- 1.1.3. * „International languages“ – hier können Sie die Sprache der Oberfläche auswählen.
- 1.1.4. * „Beenden“ – hierüber kann das Fenster geschlossen werden.

1.2. Unter „Auswahl“ finden Sie:

- 1.2.1. * „Freie Anfrage“ – öffnet ein neues Fenster, in dem Sie Rechner nach Eigenschaften suchen und auswählen können.
- 1.2.2. * „Gespeicherte Anfragen“ – „Freie Anfragen“ können gespeichert und wieder aufgerufen werden.

- 1.2.3. ★ „*Installation nicht aktuell für Produkt ...*“ – mit diesem Menüpunkt können Sie Rechner anzeigen lassen, bei denen ein ausgewähltes Programmpaket installiert ist, aber nicht in der aktuell verfügbaren Version vorliegt. Die Anzeige der betroffenen Rechner erfolgt im Reiter „*Clients*“ im Hauptfenster.
 - 1.2.4. ★ „*Installation nicht aktuell oder defekt für Produkt ...*“ – mit diesem Menüpunkt können Sie Rechner anzeigen lassen, bei denen ein ausgewähltes Programmpaket installiert ist, aber nicht in der aktuell verfügbaren Version vorliegt oder defekt ist. Die Anzeige der betroffenen Rechner erfolgt im Reiter „*Clients*“ im Hauptfenster.
 - 1.2.5. ★ „*Fehlgeschlagene Aktionen bei Produkt...*“ – mit diesem Menüpunkt können Sie Programmpakete anzeigen lassen, die nicht vollständig installiert wurden. Die Anzeige der betroffenen Rechner erfolgt im Reiter „*Clients*“ im Hauptfenster.
 - 1.2.6. ★ „*Fehlgeschlagene Aktionen*“ – zeigt an, welche Aktionen *opsi* nicht durchgeführt hat. Die Anzeige kann zeitlich eingegrenzt werden. Es werden hier, sowie beim vorigen Punkt nur Ergebnisse angezeigt, wenn Fehler in der Konfiguration der Rechner vorliegen. Die Anzeige der betroffenen Rechner erfolgt im Reiter „*Clients*“ im Hauptfenster.
 - 1.2.7. ★ „*Nur die ausgewählten Clients anzeigen*“ – blendet alle Rechner aus, die nicht der Auswahl entsprechen.
- 1.3. Im Menü „OpsiClient“ sind verschiedene Menüpunkte, die das Verhalten von Rechnern steuern.**

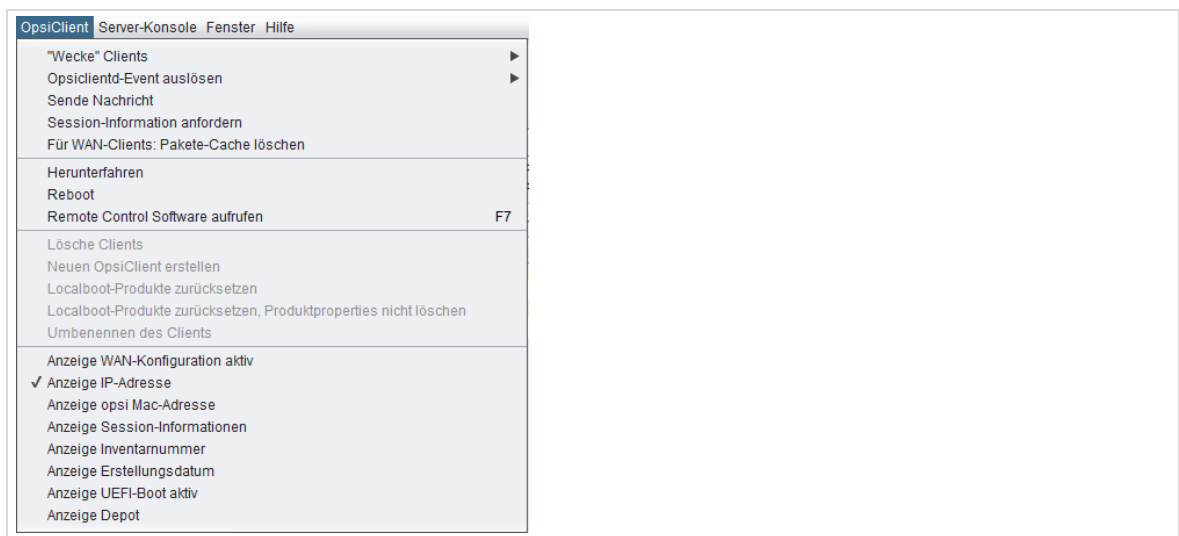


Abb. 62: Der Menüeintrag „OpsClient“

- 1.3.1. ★ „*Wecke Clients*“ – hier können Sie einen Zeitraum festlegen, der ausgewertet wird, wenn markierte Rechner zeitgleich (0 Sekunden) oder zeitversetzt geweckt werden sollen.
- 1.3.2. ★ „*Opsclientd-Event auslösen*“ – Hinter diesem Menüeintrag finden Sie einen Eintrag „*on_demand*“, mit dem Sie Änderungen sofort (bzw. beim nächsten Systemstart) an Rechner einspielen können.
- 1.3.3. ★ „*Sende Nachricht*“ – Hiermit können Sie Benutzern von selektierten Rechnern eine Nachricht auf den Monitor schicken. Dadurch können Anwender beispielsweise über das Einspielen von Software informiert werden.
- 1.3.4. ★ „*Session-Information anfordern*“ – Hiermit können Sie überprüfen, welche Benutzer an Clients angemeldet sind (Anzeige im Hauptfenster | Reiter „*Clients*“).
- 1.3.5. 🌐 „*Für WAN-Clients: Pakete-Cache löschen*“ – Ohne Funktion in der *paedML*

- 1.3.6. ✱ „Herunterfahren“ – Hier können Sie – nach Bestätigung eines Dialogfensters – ausgewählte Clients herunterfahren.
 - 1.3.7. ✱ „Reboot“ – Hier können Sie – nach Bestätigung eines Dialogfensters – ausgewählte Clients neu starten.
 - 1.3.8. ✱ „Remote Control Software aufrufen“ – hier können die ausgewählten Clients gepingt werden.
 - 1.3.9. ✱ „Lösche Clients“ – löscht einen Client. Dies ist zusätzlich notwendig, nachdem der Client aus der Schulkonsole entfernt wurde.
 - 1.3.10. 🌐 „Neuen OpsiClient erstellen“ – **Deaktiviert.**
 - 1.3.11. ✱ „Localboot-Produkte zurücksetzen“ – löscht alle Einträge, die für einen Client in der Produktkonfiguration (Localboot-, nicht Netboot-Produkte!) hinterlegt sind. Also die Informationen darüber, welche Software in welcher Version installiert ist. **Dieser Schritt ist notwendig, bevor ein Client neu installiert wird.**
 - 1.3.12. 🌐 „Umbenennen des Clients“ – **Nicht Benutzen!**
 - 1.3.13. ✱ „Anzeige ...“ – Der untere Bereich dieses Menüs ermöglicht es Ihnen die Anzeige der Rechnerinformationen im Reiter „Clients“ des Hauptfensters (5) anzupassen. Sie können mit diesem Abschnitt Spalten ein- oder ausblenden.
- 1.4. ✱ **Der Menüeintrag „Server-Konsole – paedML Linux“** – Hier ist es möglich, grafisch bestimmte paedML Linux spezifische Befehle auszuführen, ohne auf die opsi-Serverkonsole wechseln zu müssen.

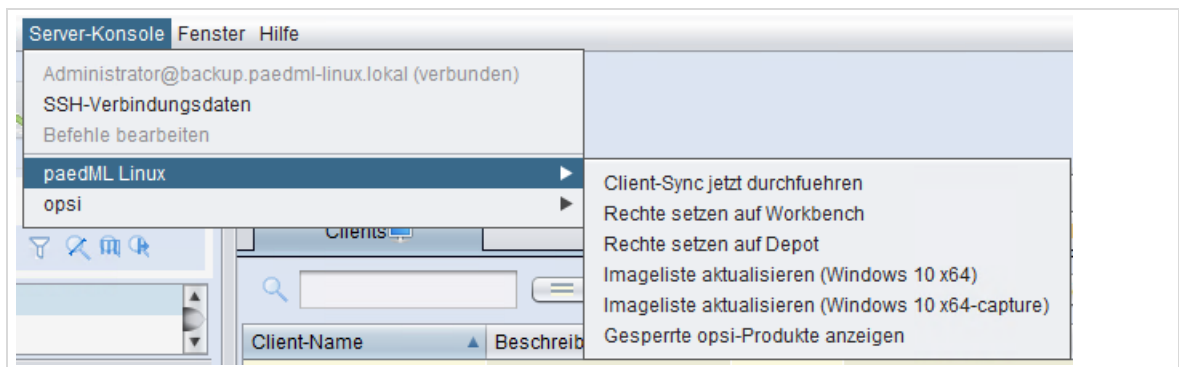


Abb. 63: Der Menüeintrag „Server-Konsole -paedML Linux“

- 1.4.1. Client-Sync jetzt durchführen: Synchronisiert Clients, die auf dem Server neu angelegt wurden mit dem opsi-Server.
 - 1.4.2. Rechte setzen auf Workbench:
 - 1.4.3. Rechte setzen auf Depot:
 - 1.4.4. Imageliste aktualisieren (Windows 10 x64)
 - 1.4.5. Imageliste aktualisieren (Windows 10 x64-capture)
 - 1.4.6. Gesperrte opsi-Produkte anzeigen
- 1.5. ✱ **Der Menüeintrag „Server-Konsole – opsi“** – Hier ist es möglich, grafisch bestimmte opsi-Befehle auszuführen, ohne auf die opsi-Serverkonsole wechseln zu müssen.

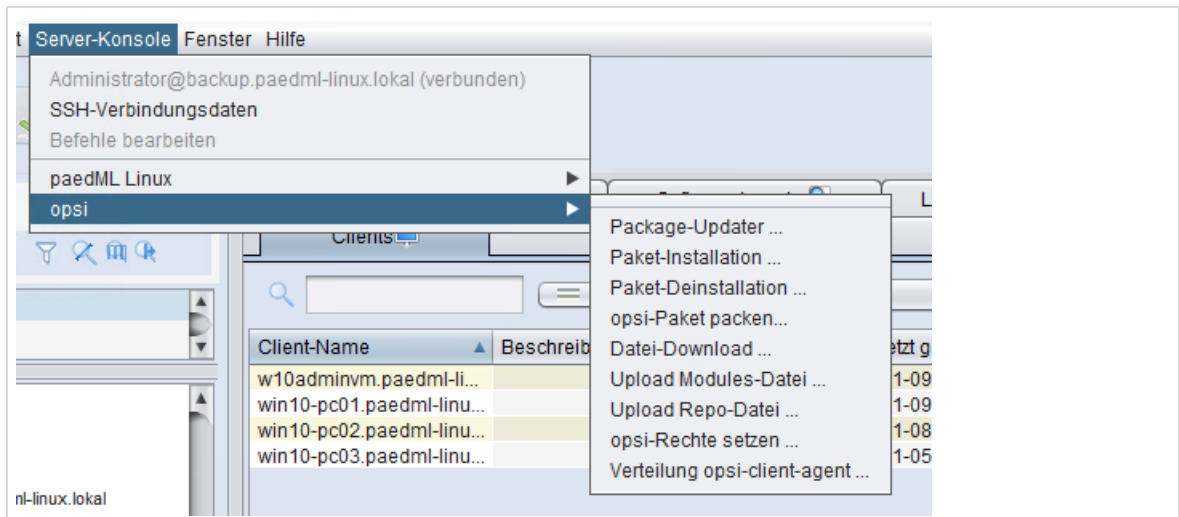


Abb. 64: Der Menüeintrag „Server-Konsole - opsi“


- 1.5.1. Package-Updater: Aktualisiert die opsi-Pakete auf dem opsi-Server
- 1.5.2. Paket-Installation: Installation eines neuen opsi-Pakets auf dem opsi-Server
- 1.5.3. Paket-Deinstallation: Deinstallation eines opsi-Pakets auf dem opsi-Serve
- 1.5.4. Opsi-Paket packen ...
- 1.5.5. Datei-Download: Dateien von anderen Quellen im Internet auf den opsi-Server herunterladen
- 1.5.6. Upload Modules-Datei: Diese Datei ist u.a. für die Lizenzierung des opsi-Servers notwendig.
- 1.5.7. Opsi-Rechte setzen: Setzt die opsi-Rechte neu, z.B. nach einer opsi-Paketinstallation
- 1.5.8. Verteilung opsi-client-agent ...
- 1.6. **★ Der Menüeintrag „Fenster“**
 - 1.6.1.  „Lizenzen“ – Ist in dieser Version noch ohne Funktion.
 - 1.6.2. **★** „Produkte (Spezialfunktionen)“ – Ohne Funktion in der paedML Linux.
- 1.7. **★ Der Menüeintrag „Hilfe“** verbirgt Verweise zu Unterstützungsangeboten rund um opsi. Hier können Sie außerdem Informationen rund um die opsi-Installation einsehen



Abb. 65: Der Menüeintrag „Hilfe“

- 1.7.1. **★** Für die Fehlersuche relevant und daher hier gesondert erwähnt ist der Menüeintrag „ConfigEditor Log-Stufe“. Hier können Sie festlegen, welche Meldungen in die Log-Dateien geschrieben werden sollen („Log-Level“).

2. Symbolleiste links oben

Unter der Menüleiste finden Sie verschiedene Symbole, die im Folgenden erklärt werden. Für alle Symbole des oberen Bereichs der opsi-Konfigurationsseite gibt es eine Beschreibung, die Sie angezeigt bekommen, wenn Sie mit dem Mauszeiger über dem jeweiligen Symbol verweilen.

Die *Symbole links oben* bieten einen Schnellzugriff auf Menüpunkte



Abb. 66: Detail opsi config editor








Symbol	Beschreibung
	<p>★ Daten von opsi neu laden</p>
	<p>☛ Neue Rechner in opsi hinzufügen</p> <p>Achtung! Diese Funktion darf nicht verwendet werden, wenn die Rechner mit der paedML Linux verwaltet werden. Das Symbol ist daher inaktiv.</p>
	<p>★ Auswahl definieren: Ein Klick auf das Symbol öffnet ein neues Fenster, das Sie dafür nutzen, Rechner mit bestimmten Eigenschaften anzeigen zu lassen. Sie können Computer aus dem Schulnetz nach „Host-Eigenschaften“ (zum Beispiel IP-Adresse, Name („ID“, ...) „opsi Produkt-Eigenschaften“ anzeigen lassen.</p> <p>Sie können aus einer großen Kriterienliste wählen, nach welchen Hardwareeigenschaften eine Auswahl von Rechnern angezeigt werden soll.</p>
	<p>★ Speichern der Konfiguration: Das fünfte Symbol der Liste ist ein grüner Haken, der rot wird, wenn Sie Änderungen an der Konfiguration von Rechnern vorgenommen haben, die noch nicht gespeichert wurden.</p> <p>Um Änderungen zu speichern, muss der rote Haken angeklickt werden.</p>
	<p>★ Filter: Der blaue Trichter ermöglicht es Ihnen, aus der Liste der Clients die nicht selektierten auszublenden und nur ausgewählte Clients zu zeigen.</p>
	<p>★ Das nächste Symbol können Sie nutzen, um zu überprüfen, welche Rechner mit opsi verbunden sind.</p>
	<p>★ Das letzte Symbol dieser Leiste bietet die Möglichkeit, im Hauptfenster (5) im Reiter „Clients“ eine „Abfrage der Session-Informationen von allen Clients“ anzeigen zu lassen. Um diese Informationen einsehen zu können, müssen Sie in der Menüleiste (1) im Menü „Opsi-Client“ den Punkt „Anzeige Session-Informationen“ aktivieren.</p>

Tabelle 9: Symbole der opsi-Konsole

3. Symbolleiste rechts oben

Einige der *Symbole rechts oben* helfen Ihnen bei der Navigation. Die Auswahl einzelner *opsi*-Komponenten (zum Beispiel das dritte Symbol „*Host-Parameter*“) ändern die Auswahlmöglichkeiten im Hauptfenster, die Sie mit hier beschriebenen Knöpfen wiederherstellen können.



Abb. 67: Detail opsi config editor

Symbol	Beschreibung
--------	--------------



★ Das erste Symbol auf der rechten Seite bringt Sie direkt in die Clientansicht („Clientkonfiguration“) des Hauptfensters (5).



☛ Über das nächste Symbol gelangen Sie zu den „Depoteigenschaften“. Hier dürfen keine Werte verändert werden!



☛ Das Monitorsymbol mit dem opsi-Logo führt zur „Server -Konfiguration“ und öffnet den besonderen Reiter „Host-Parameter“ im Hauptfenster (5). Mit diesem Knopf können Sie globale Parameter für die Clients einstellen. Hier bitte nichts ohne Rücksprache mit der Hotline ändern.



★ „Gruppenbezogene Aktionen“ können über das nächste Symbol ausgeführt werden.



☛ Produkte „Spezialfunktionen“: Bitte nicht verwenden



☛ Die Verwaltung von „Lizenzen“ verbirgt sich hinter dem letzten Symbol. Dieses Modul ist nicht aktiv. Mehr Informationen erhalten Sie über einen Klick auf den Knopf.

Tabelle 10: weitere Symbole der opsi-Konsole

4. Rechnerliste

★ Im weißen Fenster, der *Rechnerliste* auf der linken Seite, sehen Sie alle über die Schulkonsole aufgenommenen Rechner des Rechner Typs „*Windows-System*“.

Sie können einzelne Rechner („*CLIENT-LISTE*“) auswählen. Mit Hilfe der **Strg**-Taste können Sie mehrere Objekte einzeln markieren (**Strg** gedrückt halten und mit der Maus Clients hinzu- oder abwählen). Die **Shift**-Taste ermöglicht es Ihnen, größere Bereiche zwischen zwei Objekten hinzuzufügen oder abzuwählen.

Ausgewählte Rechner werden markiert und in der Hauptseite (Punkt 5) im Reiter „*Clients*“ angezeigt. Der Eintrag bei „*Depot-Server*“ zeigt den Namen des *paedML*-Servers, auf dem das opsi-Depot installiert ist.

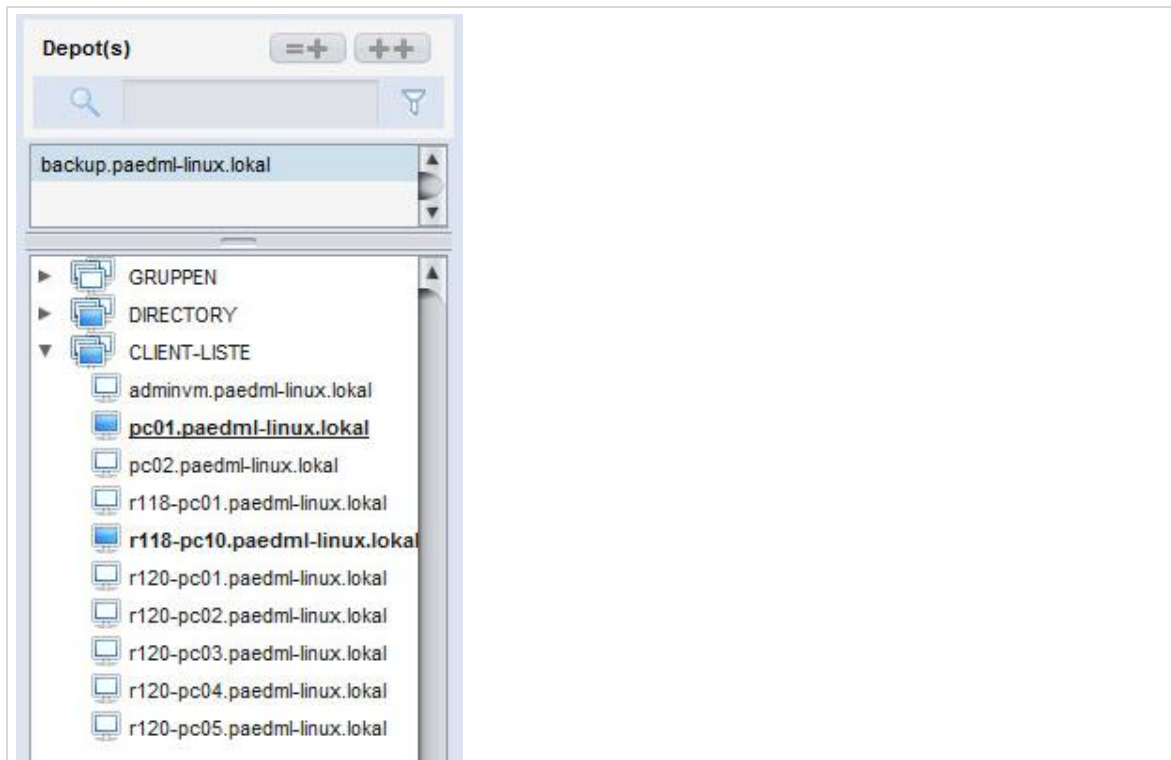


Abb. 68: opsi-config editor Detail – Auswahl einzelner Rechner

5. Hauptfenster

Das Hauptfenster ist in verschiedene Reiter unterteilt:

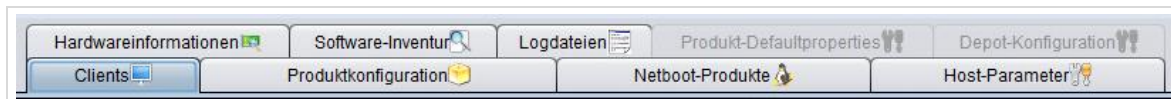


Abb. 69: Übersicht der Reiter im Hauptfenster

- 5.1. * „Clients“: Hier finden Sie alle unter Punkt 4 ausgewählten Rechner.
- 5.2. * „Produktkonfiguration“: Hier können Sie Software auf Rechner verteilen.
- 5.3. * „Netboot-Produkte“: Dies sind Routinen, die über PXE-Boot verteilt werden können.
- 5.4. * „Host-Parameter“: Hier finden Sie u.a. Parameter, die angepasst werden müssen, falls es Probleme beim Start von Rechnern gibt.
- 5.5. * „Hardwareinformationen“; Über das Netboot-Produkt *hwinvent* wird eine Liste der Hardwarekomponenten eines Clients erstellt. Diese Informationen werden zur Treiberintegration beim Windows-Rollout herangezogen.
- 5.6. * „Software-Inventur“: Hier wird von *opsi* die am Client installierte Software aufgelistet. Hierfür muss auf den Clients das Programmpaket *swaudit* mindestens einmal installiert worden sein.
- 5.7. ★ „Logdateien“: Hier finden Sie verschiedene *opsi*-Logdateien. Der Log-Level kann angepasst werden.
- 5.8. ★ „Produkt-Defaultproperties“: Hier können Standard-Werte eingestellt werden, die den Produkten bei der Installation zugewiesen werden.
- 5.9. ● „Depots“: Hier kann zwischen verschiedenen *opsi*-Depots gewechselt werden. Der Knopf ist zunächst inaktiv, wird aber durch den Knopf „Depoteigenschaften“ aktiviert. **Hier dürfen keine Werte verändert werden!**

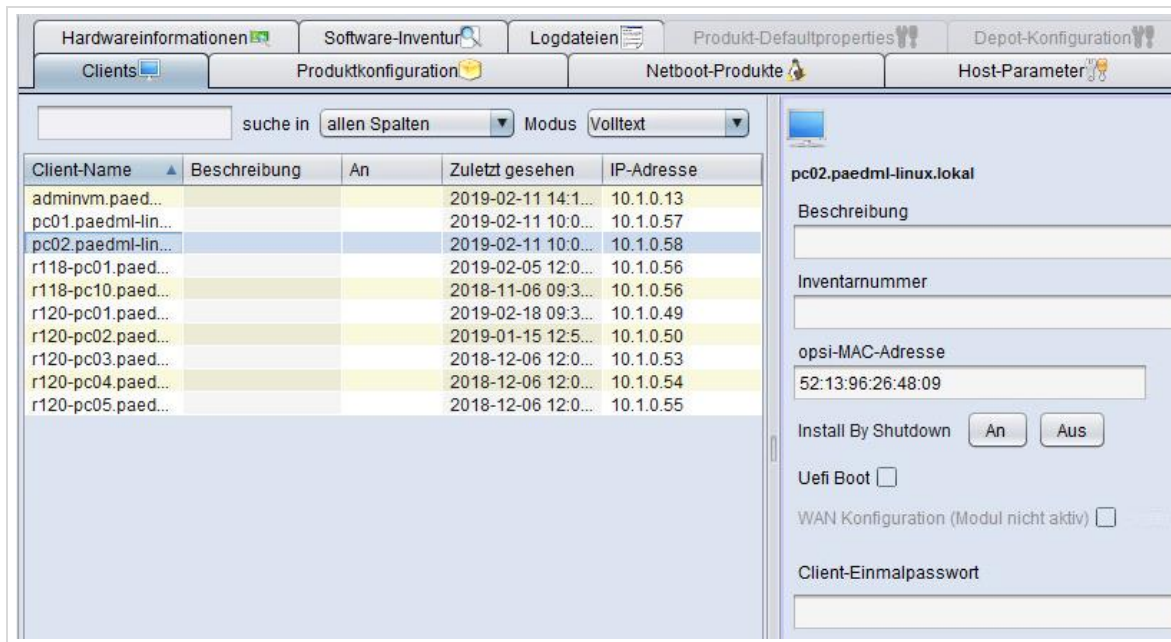


Abb. 70: opsi config editor Detail

Auf der rechten Seite finden Sie einen Bereich der – je nach Auswahl des opsi-Menüs – dynamisch befüllt wird. Hier können Parameter für die einzelnen opsi-Module eingesehen und bei Bedarf geändert werden.

6.6 Bereitstellen der Windows-Installationsdateien



Die folgende Beschreibung bezieht sich auf die Verwendung der W10AdminVM auf Windows 10 Basis. Es wird empfohlen bei der Umstellung auf Clients mit Windows 10 auch diese neue AdminVM zu installieren. Informationen zur W10AdminVM erhalten sie [hier](#).

Die opsi-Produkte „*opsi-local-image-win10-x64*“ und „*windows10-upgrade*“ sollten mit der Windows 10-Version 21H2 versorgt werden. Führen Sie dazu die Datei „*austausch-windows21h2.exe*“ im Ordner `\\backup\opsi_depot_rw\update72\Skripte` aus.

Bitte beachten Sie, dass der Download ca. 6 GB groß ist.

Die Datei enthält die deutschen Business-Editionen von Windows 10 21H2 in 64-Bit.

6.7 Installation der Arbeitsplatzrechner

Nachdem im vorigen Abschnitt die Installationsdateien für die Windowsinstallation bereitgestellt wurden, kann nun mit der Vorbereitung und dem Ausrollen der Arbeitsplatzrechner begonnen werden.

Bevor Clients jedoch mit *opsi* verwaltet werden können, müssen Sie am Server registriert werden (vgl. Kapitel 4.2 Seite 48 ff.). Bitte beachten Sie, dass Clients bei der Registrierung unbedingt mit dem Systemtyp „*Windows-System*“ versehen werden müssen, damit Sie mit *opsi* installiert werden können.

Bei der Rechneraufnahme in die *paedML* wird ein Rechner-Objekt in der *opsi*-Datenbank erstellt. Diese Rechner erscheinen in der Rechner-Liste (3) und können dort ausgewählt werden.

In der *opsi*-Konsole können Sie definieren, mit welcher Software ein Rechner versorgt werden soll. Hierüber können Sie beispielsweise das Betriebssystem einspielen (inklusive Anpassung der Partitionsgrößen), Softwarepakete installieren oder ein Programm anstoßen, das die Rechnerhardware inventarisiert (wichtig für die Integration von Treibern).

Die Installation der ausgewählten Pakete können Sie zu verschiedenen Zeitpunkten²⁶ starten:

1. sofort, sofern der Rechner gestartet ist,
2. sofort, sofern der Rechner ausgeschaltet ist und über PXE gebootet werden kann oder
3. beim nächsten Systemstart.



Die Einrichtung und Aufnahme von Rechnern in die *paedML* ist originäre Aufgabe des Dienstleisters.



Beachten Sie, dass bei einem mit *opsi* verwalteten Rechner (Windows-)Updates nicht manuell oder automatisch eingespielt werden dürfen.

Spielen Sie (Windows-)Aktualisierungen **NUR** über *opsi* ein. Das *opsi*-Paket „mshotfix“ beinhaltet diese Updates.

Große Feature-Updates können Sie über das *opsi*-Paket „*windows10-upgrade*“ einspielen.

Um Computer Ihres schulischen Netzes zu installieren, markieren Sie diese in der Rechnerliste (4).

Im Hauptfenster (5) wählen Sie den Reiter „*Netboot-Produkte*“.

Wir empfehlen, die Installation der Rechner immer mit dem *Netboot-Produkt* „*opsi-local-image-prepare*“ durchzuführen. Mit diesem *opsi*-Werkzeug wird die Festplatte in verschiedene Bereiche partitioniert.

opsi-local-image-prepare arbeitet mit einem statischen Partitionskonzept (vgl. die folgende Grafik):

- Auf der *System-Partition* liegt das Betriebssystem mit allen Programmdateien.
- Bei jeder Partitionierung wird eine *Hilfs-Partition* angelegt, die für die Ablage der Installationsdateien des Betriebssystems (Windows-PE) genutzt wird. *Linux*-Systeme könnten diese Partition später als *Swap-Partition* verwenden.
- Die optionale *Daten-Partition* kann eingerichtet werden, um Festplattenplatz für Projekte bereit zu stellen. So kann man zum Beispiel für Videoprojekte dauerhaft Daten auf der *Daten-Partition* ablegen und lokal damit arbeiten. Der Austausch großer Datenmengen mit dem Server kann so verhindert werden.

²⁶ Die Installation bei laufenden Systemen oder über PXE-Boot kann „on demand“ über die *opsi*-Konsole angestoßen werden, ansonsten wird Software beim nächsten Systemstart installiert.

- Ein zentraler Bestandteil der Installation mit „*opsi-local-image-prepare*“ ist das Erstellen einer *Backup-Partition*. In dieser *Backup-Partition* werden lokale Images der Rechner vorgehalten.



Achtung! Rechner mit UEFI dürfen keine Datenpartition erhalten. Die Partition wird zwar richtig angelegt, es ist aber nicht möglich unter Windows auf die Partition zuzugreifen.

Die optionale Datenpartition muss gesondert gesichert werden – natürlich nur, wenn Sie die Daten gesichert haben wollen.

Ein Problem bei Datenpartitionen ist, dass sie im Klassenarbeitsmodus NICHT deaktiviert werden. Dadurch können Schüler „virtuelle Spickzettel“ erstellen und damit arbeiten.

Außerdem wird die Datenpartition nicht von der paedML verwaltet. Alle dort abgelegten Daten bleiben unangetastet, bis sie händisch gelöscht werden oder das System mit Hilfe des Netboot-Produktes *opsi-local-image-prepare* neu installiert wird.

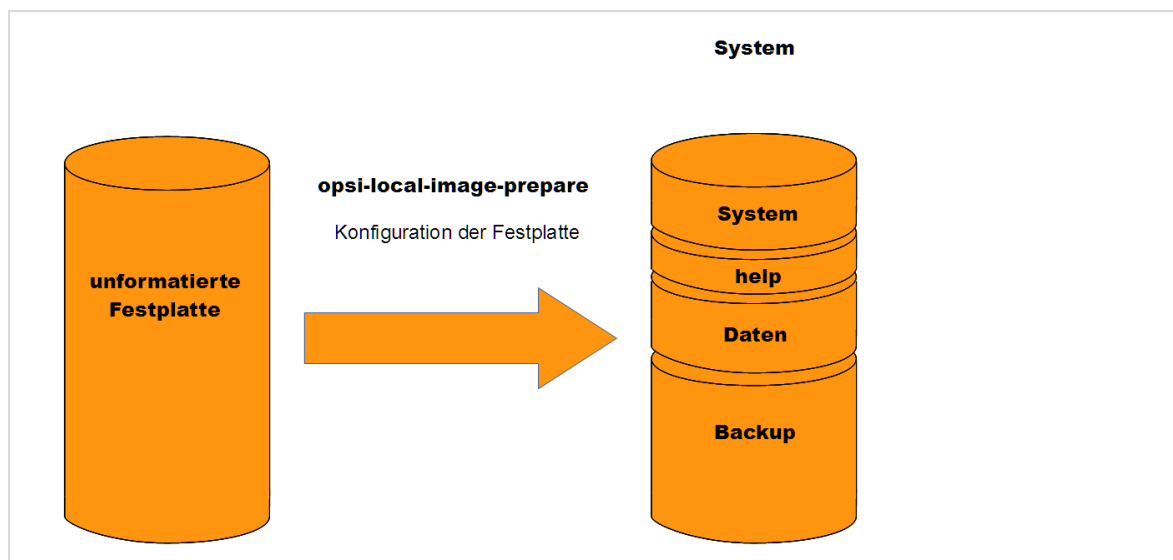


Abb. 71: Konfiguration der Festplatte mit *opsi-local-image-prepare*

Bei der Einrichtung eines Rechners können Sie verschiedene Anpassungen an *opsi-local-image-prepare* vornehmen. Wählen Sie das Produkt aus und klicken Sie in die Spalte „Angefordert“. Wählen Sie dort den Eintrag „Setup“.

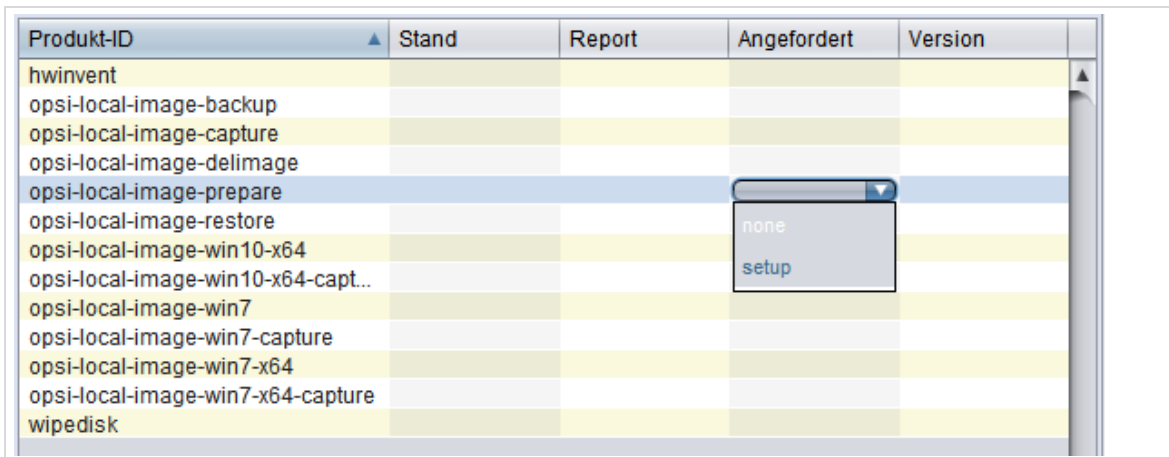


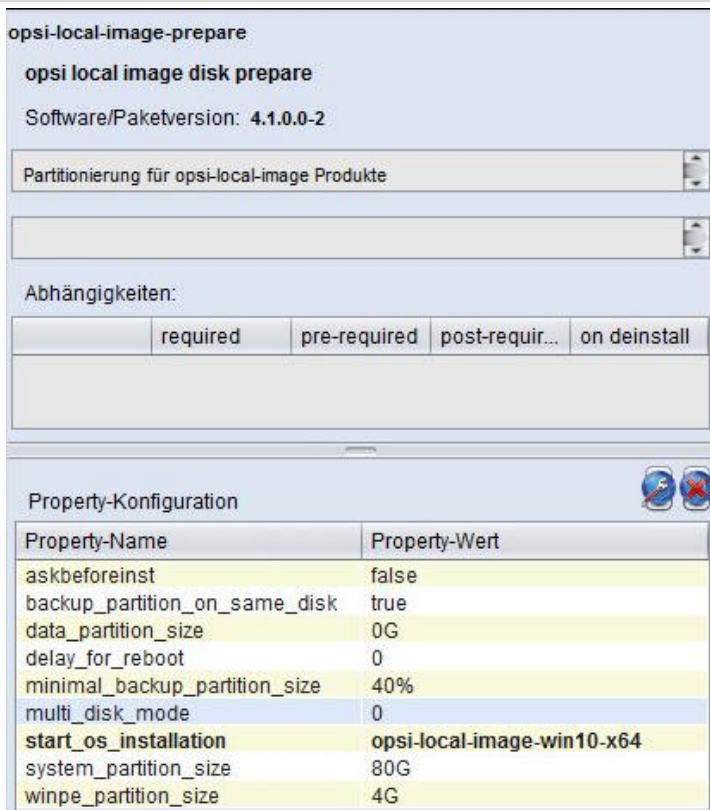
Abb. 72: Auswahl von opsi-local-image-prepare für die Windowsinstallation

Der dynamische Inhalt des opsi-config-editor (6) wird mit Informationen zum Netbootprodukt und mit Parametern (Bereich: „Konfiguration für Client“) gefüllt, die angepasst werden müssen. Die Einstellungen können wie folgt vorgenommen werden:

Property-Name	Property-Wert
architecture	Bitte auf 64 bit belassen.
askbeforeinst	Hier kann eine Bestätigung vor der Installation am Arbeitsplatzrechner eingebaut werden. Sofern der Wert auf „false“ belassen wird (empfohlen), läuft die Installation automatisch durch. Bei der Installation wird die Festplatte komplett formatiert!
backup_partition_on_same_disk	Wird der Wert auf „true“ eingestellt, wird die Backup-Partition auf der gleichen Festplatte erstellt, auf der das Betriebssystem installiert wurde. „False“ erstellt die Backup-Partition auf der zweiten Festplatte.
data_partition_size	(optional) – Wie groß soll eine Datenpartition angelegt werden. Der Property-Wert für data_partition_size ist im Standard auf 0G gestellt. Wobei G für Gigabyte steht. Wenn Sie Datenpartitionen anlegen wollen, müssen Sie diesen Wert entsprechend ändern.
delay_for_reboot	Hier kann eine Verzögerung in Sekunden angegeben werden, bevor das System neu startet.
minimal_backup_partition_size	Minimale Größe der Backup-Partition (relational zur Gesamtgröße der Festplatte) – Standardwert: 40%
multi_disk_mode	Hier wird angegeben auf welcher Festplatte das Betriebssystem installiert werden soll. „0“ steht für die erste Festplatte, „1“ für die Zweite. Wird „prefer_rotational“ ausgewählt werden gewöhnliche Festplatten für die Installation bevorzugt, bei „prefer_ssd“ Solid State Drives (SSD). Bitte beachten Sie, dass Sie bei BIOS-Geräten die Bootreihenfolge ändern müssen, bei UEFI-Geräten ist dies nicht nötig.

start_os_installation	Hier wird ausgewählt, welches Betriebssystem installiert werden soll.
system_partition_size	Wie groß soll die Systempartition angelegt werden? Der Property-Wert für system_partition_size ist im Standard auf 80G gesetzt. Wählen Sie hier einen anderen vordefinierten Wert oder geben Sie eine eigene Partitionsgröße ein, falls Sie Ihre Windows-Partition größer anlegen wollen.
winpe_partition_size	Ablage des Windows-PE-Images und der Treiber – Standard-Größe: 4GB

Tabelle 11: Parameter von „opsi-local-image-prepare“



opsi-local-image-prepare

opsi local image disk prepare

Software/Paketversion: 4.1.0.0-2

Partitionierung für opsi-local-image Produkte

Abhängigkeiten:

	required	pre-required	post-requir...	on deinstall

Property-Konfiguration

Property-Name	Property-Wert
askbeforeinst	false
backup_partition_on_same_disk	true
data_partition_size	0G
delay_for_reboot	0
minimal_backup_partition_size	40%
multi_disk_mode	0
start_os_installation	opsi-local-image-win10-x64
system_partition_size	80G
winpe_partition_size	4G

Abb. 73: Einstellungen für „opsi-local-image-prepare“

Das Feld „start_os_installation“ wird mit den auf dem Backup-Server installierten Windowsabbildern befüllt. Dieser Wert ist daher abhängig von der Einrichtung der Installationsdateien, die Sie im vorhergehenden Kapitel vorgenommen haben. Zu jeder installierten Windowsversion gibt es ein eigenes Netboot-Produkt „opsi-local-image-VERSION“, das Sie für die Installation auswählen können.

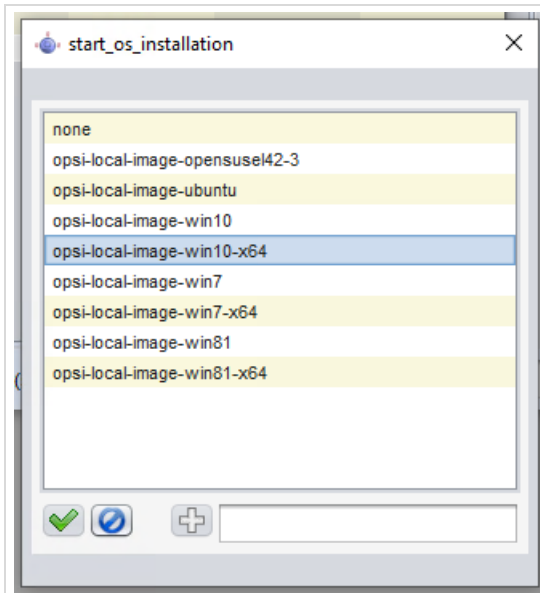


Abb. 74: Auswahl des zu installierenden Betriebssystems

Alle Änderungen müssen anschließend mit dem *roten Haken* unter (2) gespeichert werden.



Abb. 75: Der rote Haken zeigt an, dass Änderungen noch nicht übernommen wurden.

Wenn die Werte übernommen wurden, wird der Haken *grün*.

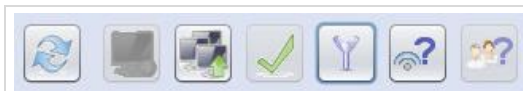


Abb. 76: Änderungen wurden übernommen.

Vor der Installation des Betriebssystems auf den Rechnern können Sie im Reiter „*Produktkonfiguration*“ (1) auswählen, welche Software Sie installieren wollen. Setzen Sie dafür das Produkt bzw. die Produkte auf „*setup*“ (2) und speichern Sie danach die Konfiguration mit einem Klick auf den roten Haken (3).

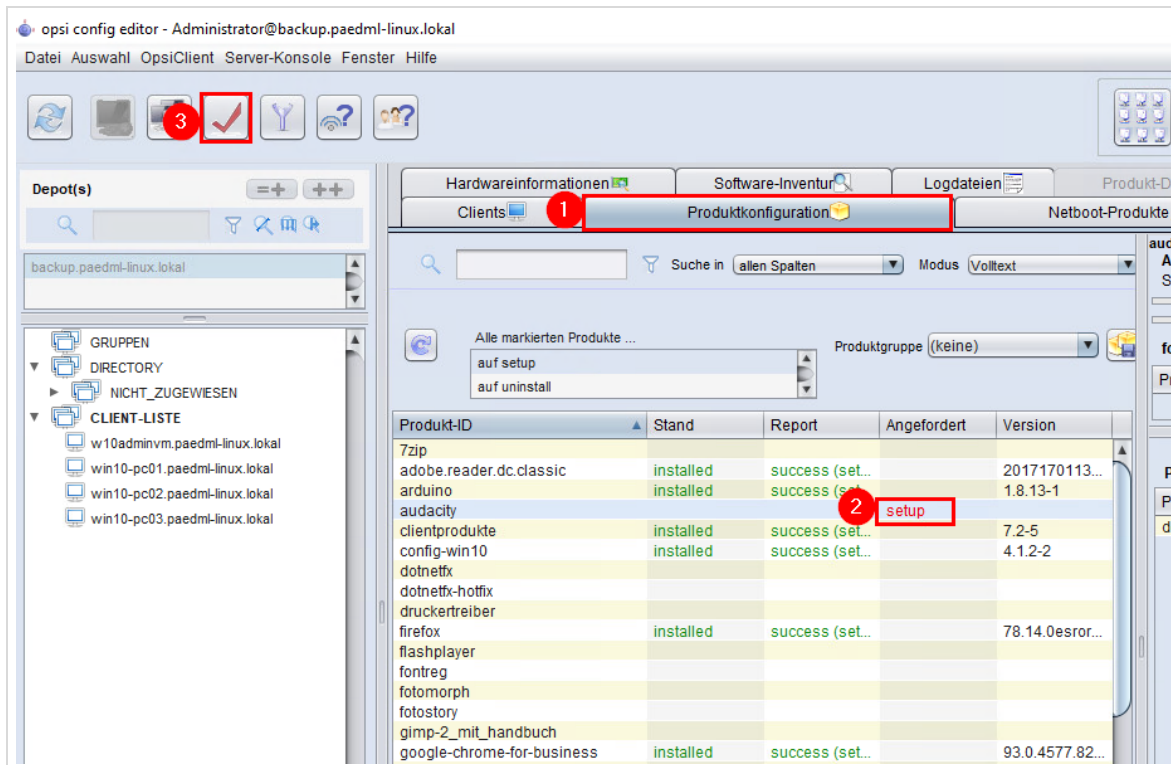


Abb. 77: Produkte auf „setup“ setzen

Beim nächsten Clientstart wird die Installation angestoßen, sofern der Client über PXE bootet. Das System wird ggf. automatisch neu gestartet, um die Installation durchzuführen.

Die Zuweisung spezieller Treiber geschieht über das Netboot-Produkt, welches im Feld „start_os_installation“ angegeben wird. Das Einspielen spezieller Geräte-Treiber ist Gegenstand des folgenden Abschnittes.

6.8 Treiberintegration

Ein häufig anzutreffendes Problem bei der Installation von Betriebssystemen sind fehlende Treiber.

Leider kann dieses Problem auch durch den Einsatz von opsi nicht gelöst werden, so dass die Suche nach fehlenden Treibern immer noch Aufgabe des Administrators bleiben wird! Was opsi aber bietet ist das zentrale Bereitstellen von Treibern²⁷, die bei der Installation automatisiert auf den Clients installiert werden.

Wenn kein Treiber für eine Komponente auf dem opsi-Server gefunden wurde, dann bricht die Installation entweder ab oder es wird ein Eintrag in den opsi-Logdateien erstellt, in dem auf den nicht vorhandenen Treiber hingewiesen wird.

²⁷ In Netboot-Produkten zu XP und Windows 7 sind einige gängige Hardwaretreiber enthalten.

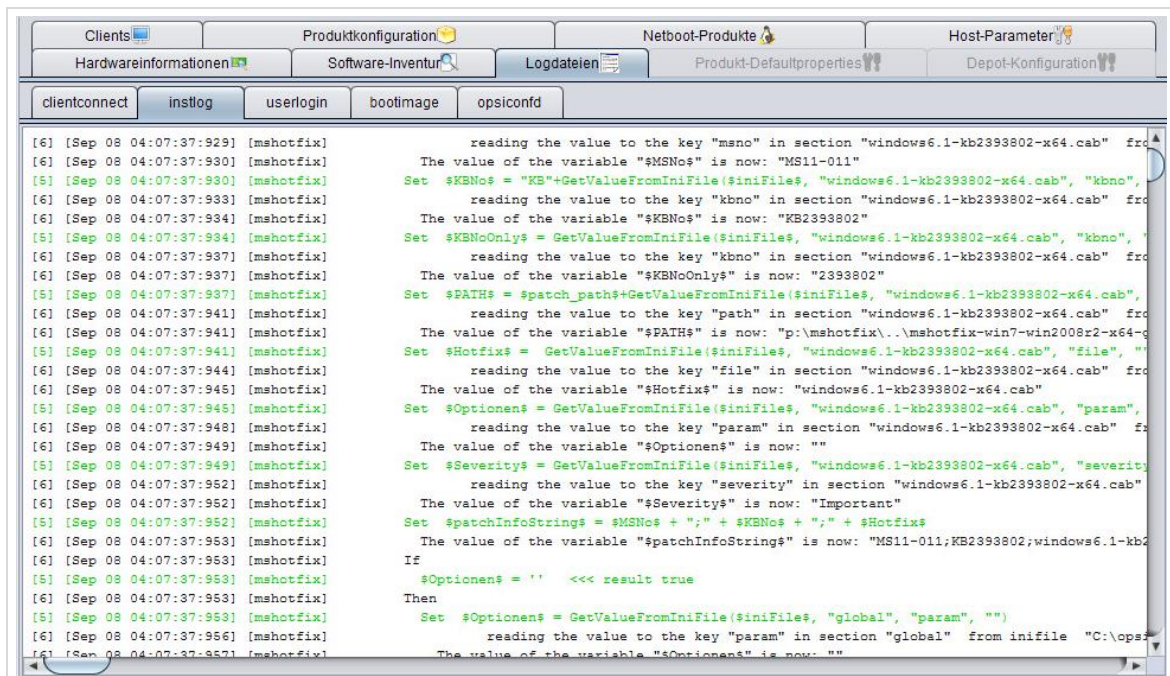
```
(...)
[6] [Feb 24 11:14:22] Searching driver for PCI_DEVICE '3rd Gen Core
processor Graphics Controller', id '8086:0166' (WindowsDrivers.py|94)

[3] [Feb 24 11:14:22] PCI_DEVICE vendor directory 'opsi-local-image-win10-
x64/drivers/pciids/8086' not found (WindowsDrivers.py|108)
(...)
```



Die Log-Dateien des Systems sollten auf Einträge, wie die im folgenden Screenshot gezeigten, untersucht werden. Damit kann sichergestellt werden, dass die Installation aller Treiber auf den Rechnern durchgelaufen ist.

Sie finden die entsprechenden Einträge im *opsi-Hauptfenster* (5) im Reiter „Logdateien“ und dort im Unterreiter „boot-Image“.



```
[6] [Sep 08 04:07:37:929] [mshotfix]      reading the value to the key "msno" in section "windows6.1-kb2393802-x64.cab" fro
[6] [Sep 08 04:07:37:930] [mshotfix]      The value of the variable "$MSNo$" is now: "MS11-011"
[5] [Sep 08 04:07:37:930] [mshotfix]      Set $KbNo$ = "KB"+GetValueFromIniFile($iniFile$, "windows6.1-kb2393802-x64.cab", "kbno",
[6] [Sep 08 04:07:37:933] [mshotfix]      reading the value to the key "kbno" in section "windows6.1-kb2393802-x64.cab" fro
[6] [Sep 08 04:07:37:934] [mshotfix]      The value of the variable "$KbNo$" is now: "KB2393802"
[5] [Sep 08 04:07:37:934] [mshotfix]      Set $KbNoOnly$ = GetValueFromIniFile($iniFile$, "windows6.1-kb2393802-x64.cab", "kbno",
[6] [Sep 08 04:07:37:937] [mshotfix]      reading the value to the key "kbno" in section "windows6.1-kb2393802-x64.cab" fro
[6] [Sep 08 04:07:37:937] [mshotfix]      The value of the variable "$KbNoOnly$" is now: "2393802"
[5] [Sep 08 04:07:37:937] [mshotfix]      Set $PATH$ = $patch_path$+GetValueFromIniFile($iniFile$, "windows6.1-kb2393802-x64.cab",
[6] [Sep 08 04:07:37:941] [mshotfix]      reading the value to the key "path" in section "windows6.1-kb2393802-x64.cab" fro
[6] [Sep 08 04:07:37:941] [mshotfix]      The value of the variable "$PATH$" is now: "p:\mshotfix-win7-win2008r2-x64-d
[5] [Sep 08 04:07:37:941] [mshotfix]      Set $Hotfix$ = GetValueFromIniFile($iniFile$, "windows6.1-kb2393802-x64.cab", "file",
[6] [Sep 08 04:07:37:944] [mshotfix]      reading the value to the key "file" in section "windows6.1-kb2393802-x64.cab" fro
[6] [Sep 08 04:07:37:945] [mshotfix]      The value of the variable "$Hotfix$" is now: "windows6.1-kb2393802-x64.cab"
[5] [Sep 08 04:07:37:945] [mshotfix]      Set $Optionen$ = GetValueFromIniFile($iniFile$, "windows6.1-kb2393802-x64.cab", "param",
[6] [Sep 08 04:07:37:948] [mshotfix]      reading the value to the key "param" in section "windows6.1-kb2393802-x64.cab" fr
[6] [Sep 08 04:07:37:949] [mshotfix]      The value of the variable "$Optionen$" is now: ""
[5] [Sep 08 04:07:37:949] [mshotfix]      Set $Severity$ = GetValueFromIniFile($iniFile$, "windows6.1-kb2393802-x64.cab", "severity
[6] [Sep 08 04:07:37:952] [mshotfix]      reading the value to the key "severity" in section "windows6.1-kb2393802-x64.cab"
[6] [Sep 08 04:07:37:952] [mshotfix]      The value of the variable "$Severity$" is now: "Important"
[5] [Sep 08 04:07:37:952] [mshotfix]      Set $patchInfoString$ = $MSNo$ + ";" + $KbNo$ + ";" + $Hotfix$
[6] [Sep 08 04:07:37:953] [mshotfix]      The value of the variable "$patchInfoString$" is now: "MS11-011;KB2393802;windows6.1-kb2
[6] [Sep 08 04:07:37:953] [mshotfix]      If
[5] [Sep 08 04:07:37:953] [mshotfix]      $Optionen$ = '' <<< result true
[6] [Sep 08 04:07:37:953] [mshotfix]      Then
[5] [Sep 08 04:07:37:953] [mshotfix]      Set $Optionen$ = GetValueFromIniFile($iniFile$, "global", "param", "")
[6] [Sep 08 04:07:37:956] [mshotfix]      reading the value to the key "param" in section "global" from ini file "C:\ops
[6] [Sep 08 04:07:37:957] [mshotfix]      The value of the variable "$Optionen$" is now: ""
```

Abb. 78: Ansichtsfenster der Logdateien

Wenn bei der Installation nicht automatisch die Treiber aller Komponenten eines Rechners gefunden werden können die Treiber gemeinsam mit der Windows-Installation per opsi verteilt werden. Zunächst müssen die fehlenden Treiber identifiziert werden.

6.8.1 Identifizieren von Treibern

Wenn Sie das Problem haben, dass die Arbeitsplatzrechner nicht automatisch mit allen Treibern versorgt werden, stellt sich die Frage, um welche Treiber es sich handelt, die nicht installiert werden können. opsi bietet hier die komfortable Möglichkeit, dies herauszufinden.

Das *opsi-Netbootprodukt hwinvent* liest die Hardwareinformationen der Arbeitsplatzrechner aus und stellt diese im Reiter „Hardwareinformationen“ im Hauptfenster (5) dar. Das Programm läuft automatisch bei jeder Installation, kann aber auch händisch gestartet werden. Wählen Sie das Produkt im Reiter „Netboot-Produkte“ aus und stellen Sie den Wert in der Spalte „Angefordert“ auf „setup“.

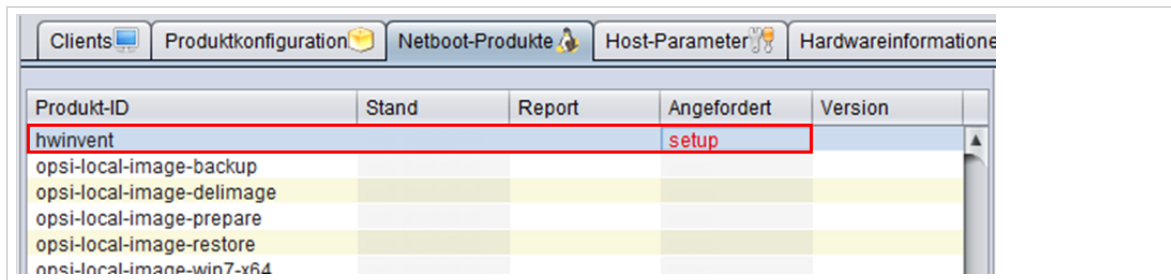


Abb. 79: Manuelle Initialisierung von hwinvent

Wenn *hwinvent* erfolgreich ausgeführt wurde, wird der Reiter „Hardwareinformationen“ befüllt. Anschließend können Sie beispielsweise das Computermodell in Erfahrung bringen und beim Hersteller nach Treibern suchen.

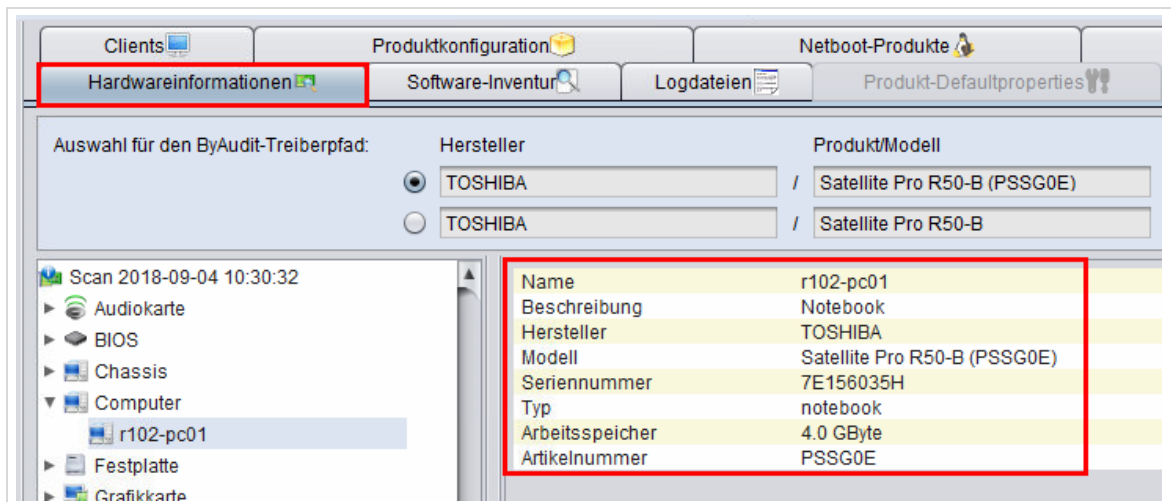


Abb. 80: Anzeige des Computermodells

Sie können sich aber auch gezielt Komponenten anzeigen lassen und nach Treibern suchen. Dies ist zum Beispiel sinnvoll, wenn Rechner nicht als Gesamtpaket gekauft, sondern zusammengestellt wurden.

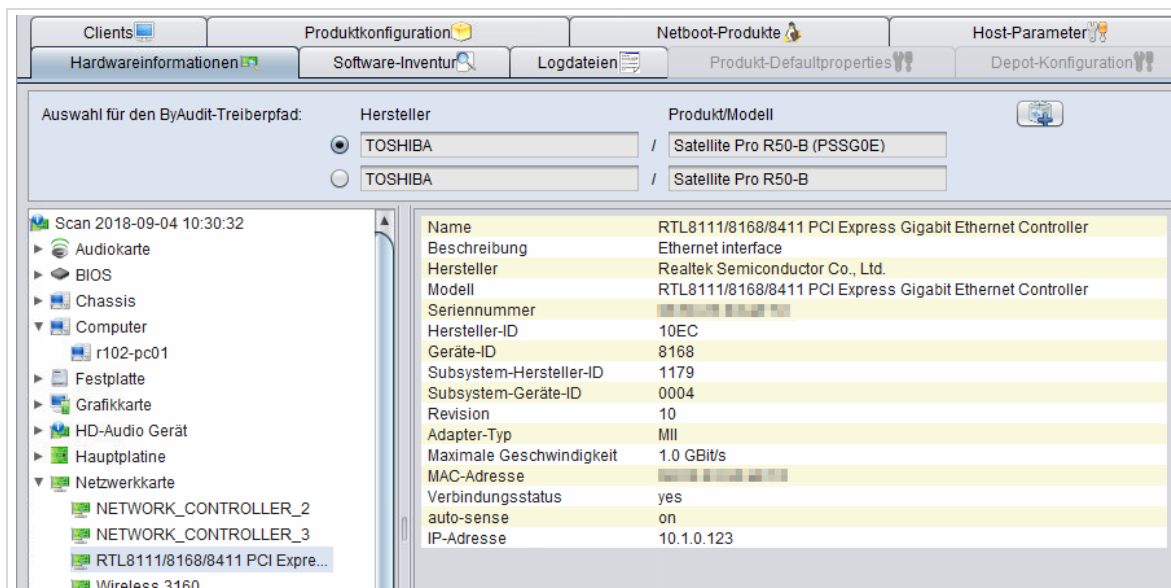


Abb. 81: Anzeige einzelner Hardwarekomponenten

6.8.2 Einspielen von Treibern in das opsi-Depot

Alle manuell einzuspielenden Treiber müssen auf den opsi-Server übertragen werden (vgl. Kapitel 1.4.2, S. 31 ff.).

Im Verzeichnis `/var/lib/opsi/depot/` liegen alle Daten für die Betriebssysteminstallation, die Sie auf dem Server angelegt haben.

Für jedes dieser Betriebssysteme müssen, die dem Betriebssystem entsprechenden Treiber zur Verfügung gestellt werden. Die Treiber werden in das Verzeichnis `/var/lib/opsi/depot/OS-NAME/drivers/drivers/` kopiert, wobei OS-NAME durch den von Ihnen für das jeweilige Betriebssystem erstellten Ordnernamen ersetzt werden muss.



Achten Sie darauf KEINE Umlaute, KEINE Sonderzeichen sowie KEINE Leerzeichen beim Anlegen der Treiberverzeichnisse zu verwenden.

Ein Beispiel:

Die Treiber für die Windows 10 Installation werden nach `/var/lib/opsi/depot/opsi-local-image-win10-x64/drivers/drivers` kopiert.

Konkrete Umsetzung am Beispiel einer Hardwaregruppe mit Fujitsu-Netbooks

Laden Sie die Dateien des Treibers mithilfe der gesammelten Hardware-Informationen herunter. Entpacken Sie die Treiberdateien. Benötigt werden die `*.inf`-Dateien. Ausführbare Archive (`*.exe` oder `*.msi`) sind nicht brauchbar, außer es handelt sich um selbst entpackende Archive, in denen die Treiber im `*.inf`-Format vorliegen. Der Einfachheit halber können die gesamten entpackten Inhalte von Archiven auf den opsi-Server übertragen werden. In der Praxis sollten Sie aber darauf achten, dass die richtigen Treiber in die richtigen Verzeichnisse gelangen.

Verbinden Sie sich mittels WinSCP mit Ihrem opsi-Server. Navigieren Sie im linken Quell-Bildschirm zu den Treiberdateien und im rechten Ziel-Bildschirm nach `/var/lib/opsi/depot/opsi-local-image-win10-x64/drivers/drivers`.

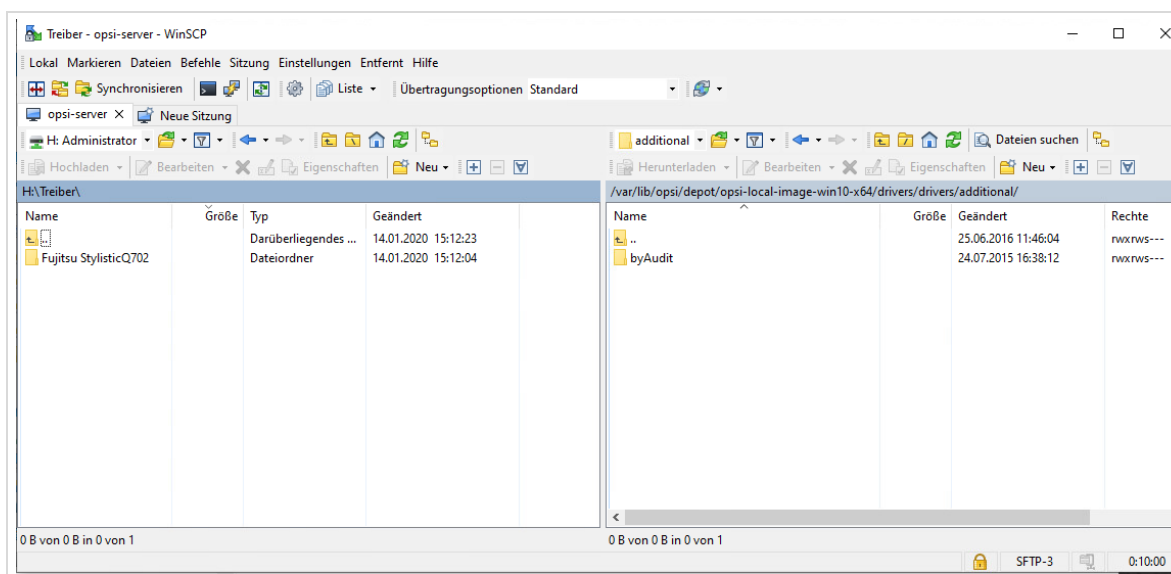


Abb. 82: Hochladen der Hardwaretreiber mit WinSCP

Nach Rechtsklick in den rechten Bildschirm können Sie ein neues Verzeichnis erstellen. Die Rechte können auf 0755 belassen werden. Sie werden im Anschluss durch „opsi-Rechte setzen“ neu gesetzt. Als Verzeichnisnamen wählen Sie einen aussagekräftigen, der Hardware und dem Treiber zuordenbaren Namen.

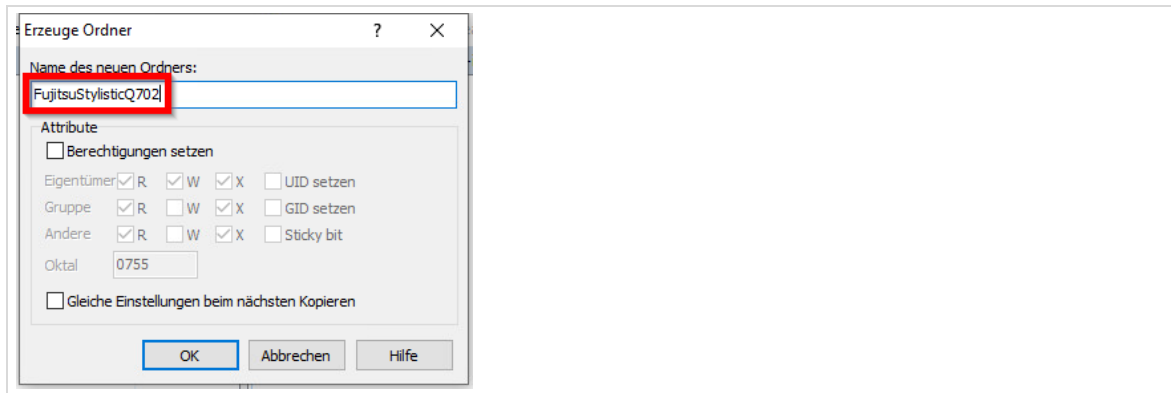


Abb. 83: Hochladen der Hardwaretreiber mit WinSCP



Achten Sie darauf KEINE Umlaute, KEINE Sonderzeichen sowie KEINE Leerzeichen beim Anlegen der Treiberverzeichnisse zu verwenden.



Damit *opsi* die neu auf den Server geladenen Dateien verarbeiten kann, muss der Befehl „opsi-Rechte setzen“ im configed ausgeführt werden (siehe oben).

Symlinks für Treiber setzen

Der letzte auf dem *opsi*-Server durchzuführende Schritt ist das Setzen von Symlinks für *opsi*. Dies geschieht aus dem jeweiligen Haupt-Verzeichnis des betroffenen Netboot-Produktes (*/var/lib/opsi/depot/opsi-local-image-BETRIEBSSYSTEM*) mit dem Befehl

```
# ./create_driver_links.py
```

```
root@backup: /var/lib/opsi/depot/opsi-local-image-win10-x64# ./create_driver_links.py
```

Abb. 84: Setzen von *opsi*-Symlinks.

Hiermit sind die Vorbereitungen auf dem Server abgeschlossen und die Treiberintegration in der *opsi*-Konsole kann vorgenommen werden.

6.8.3 Integration der Treiber in die Installation

Um den soeben im System hinterlegten Treiber bei der Installation einzubinden, markieren Sie im Auswahlfenster (4) der *opsi*-Konsole die zu installierenden Rechner.

Wählen Sie im Hauptfenster (5) den Reiter „Netboot-Produkte“ und dort das zu installierende Produkt. Tragen Sie im Feld „Property-Wert“ von „additional_drivers“ den Namen des von Ihnen erstellten

Verzeichnisses, in dem die Treiberdateien liegen, ein. Der Verzeichnis-Name ist dabei ohne den Verzeichnis-Pfad anzugeben (vgl. folgender Screenshot). Speichern Sie die Änderungen.



Der Wert des Verzeichnisnamens ist case-sensitive. Es ist also wichtig, dass Sie den genauen Namen (Groß-/Kleinschreibung beachten) eintragen!

Property-Name	Property-Wert
additional_drivers	
administrator_password	
architecture	64bit
askbeforeinst	false
backup_after_install	false
fullname	Name
imagename	Windows 10 Education
install_local_bootimage	false
installto	oli
orgname	Orgname
productkey	
setup_after_install	clientprodukte, windomain
system_keyboard_layout	0407:00000407
system_language	de-DE
system_timezone	W. Europe Standard Time
winpe_debug_cmd_exe	false
winpe_dir	auto
winpe_inputlocale	0407:00000407
winpe_uilanguage	de-DE
winpe_uilanguage_fallback	de-DE
winpenetworkmode	true

Abb. 85: Eintrag des Verzeichnisnamens der Treiberdateien

Im Beispiel lautet der Wert der Property `additional_drivers` „FujitsuStylisticQ702“.

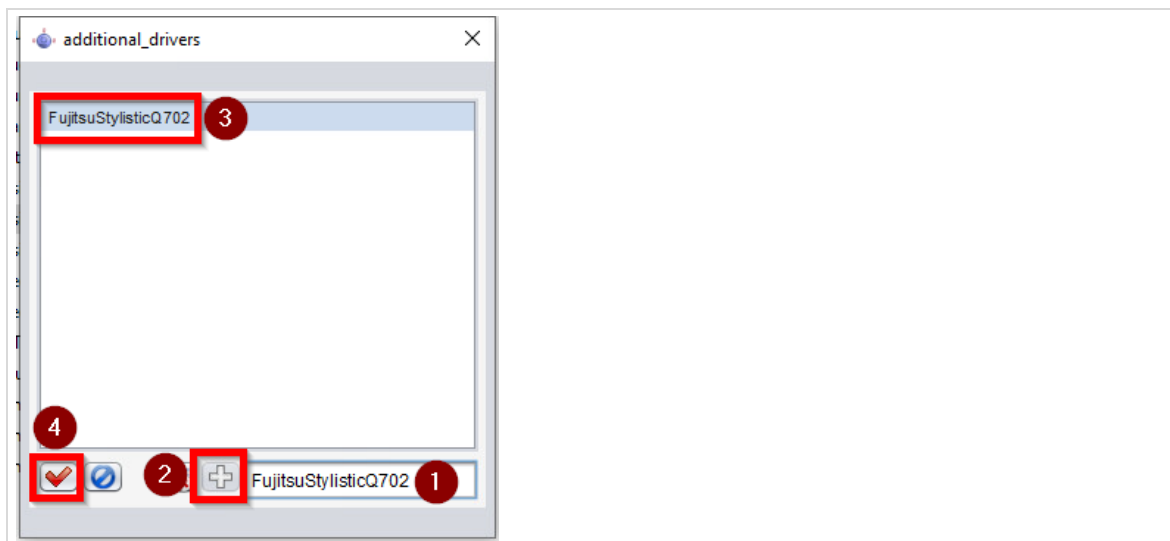


Abb. 86: Wert der Property `additional_drivers`

6.9 Hinweise zur Arbeit mit „product-properties“

Im dynamischen Bereich (6) der opsi-Konsole können Sie vordefinierte Werte für Produkteigenschaften („product-properties“) auswählen oder häufig auch eigene Werte eintragen, die dann in das jeweilige opsi-Produkt übernommen werden. Bei der Auswahl von „Property-Wert(en)“ muss darauf geachtet werden, dass die Werte eindeutig sind und KEINE leeren Felder übergeben werden.

Ein Beispiel hierfür wäre die Produkteigenschaft „additional_drivers“, über die Sie beim Ausrollen von Betriebssystemen an Rechner definieren können, welche zusätzlichen Gerätetreiber installiert werden

sollen. Wird dort aus Versehen der „leere“ Eintrag, der sich am Beginn der Liste befindet, mit ausgewählt, führt dies zu Problemen bei der Rechnerinstallation.



Der leere Eintrag versteckt sich gut. Im folgenden Screenshot ist nicht zu erkennen, dass über dem Eintrag „Fujitsu...“ ein leeres Feld steht, dass ebenfalls ausgewählt wurde.

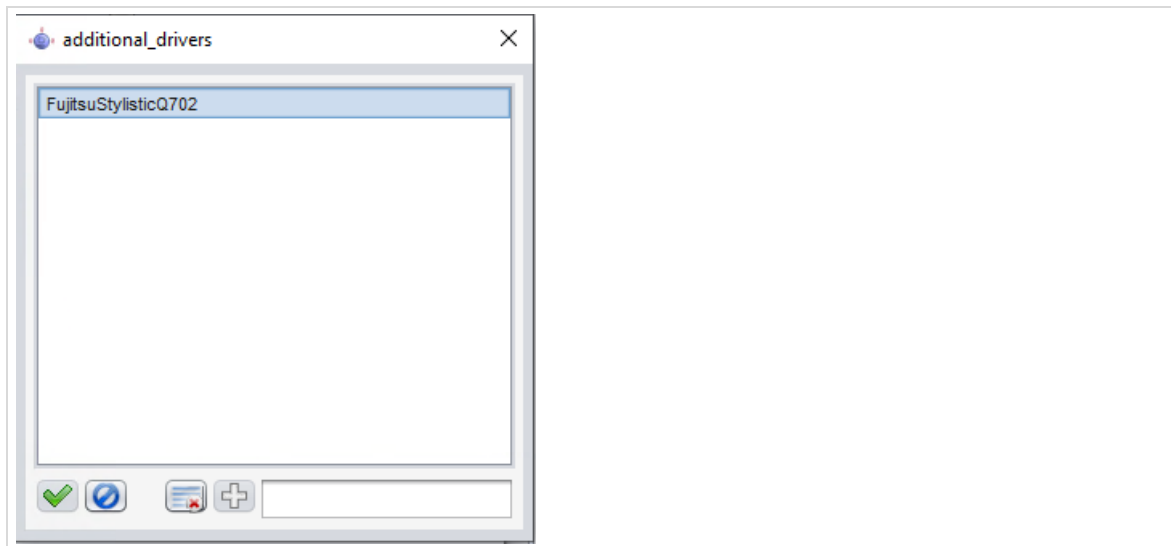


Abb. 87: Obacht in der opsi-Auswahl

Erst nach der Übernahme des „Property-Wertes“ ist zu erkennen, dass ein leeres Feld mit übernommen wurde: Die „Property-Werte“ werden durch Kommata getrennt. Ein Komma am Anfang mehrerer Werte lässt auf ein leeres Feld schließen.

Durch einen Doppelklick auf den „Property-Wert“ kann der Fehler behoben werden. Achten Sie in diesem Fall unbedingt darauf nur gültige Werte auszuwählen.

Property-Name	Property-Wert
additional_drivers	, FujitsuStylisticQ702
askbeforeinst	false
backup_after_install	false

Abb. 88: Hier hat sich ein leeres Feld eingeschlichen (erkennbar durch das Komma am Anfang)

6.10 opsi-Standard-Einstellungen („Produkt-Defaultproperties“)

Die meisten opsi-Produkte können bei der Installation angepasst werden. So gibt es für bestimmte Programme die Option bei der Installation einen Proxy einzurichten. Für das Netboot-Produkt „opsi-local-image-prepare“ kann eingestellt werden, wie groß Festplattenpartitionen angelegt werden sollen.

Bevor ein opsi-Produkt ausgespielt wird, können Sie die „Property-Konfiguration“, also die konfigurierbaren Werte, für die zur Installation vorgesehenen Programme ändern.



Die *Property*-Konfiguration gilt zunächst global. Dies bedeutet, dass alle Rechner mit den vordefinierten Werten installiert werden.

Produkt-Properties können aber auch für ausgewählte Clients gesetzt werden. Diese Werte können bei der Installation des jeweiligen Produktes angepasst werden. In diesem Fall wirken sich nachträgliche Änderungen an den Default-Properties NICHT auf diese Rechner aus.

Um die Standard-Einstellungen dauerhaft zu ändern, müssen diese im Reiter „*Produkt-Default-Properties*“ eingestellt werden. Der Reiter „*Produkt-Defaultproperties*“ im Hauptfenster (5) ist zunächst inaktiv und wird erst durch das Anklicken der Schaltfläche „*Depoteigenschaften*“ verfügbar.

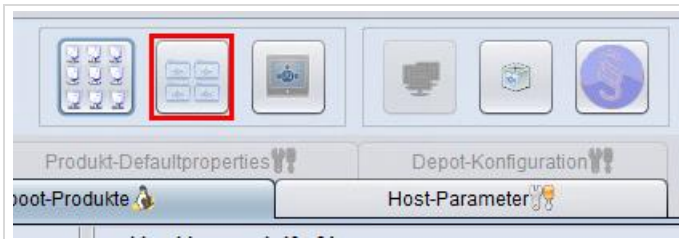


Abb. 89: Zugriff auf „*Produkt-Defaultproperties*“ über die „*Depoteigenschaften*“



Im Reiter „*Depot-Konfiguration*“, der ebenfalls nach dem Klick auf „*Depoteigenschaften*“ verfügbar ist, **darf NICHTS geändert werden.**

Um die Parameter eines *opsi*-Produktes dauerhaft zu verändern, wählen Sie das Produkt aus. Alle konfigurierbaren Werte (die sogenannten „*Produkt-Properties*“) finden Sie nach Auswahl des *opsi*-Produktes im dynamischen Bereich (6) der *opsi*-Konsole.

Im folgenden Beispiel wird die Systempartition von Windows angepasst. Geänderte Werte werden fett hervorgehoben.

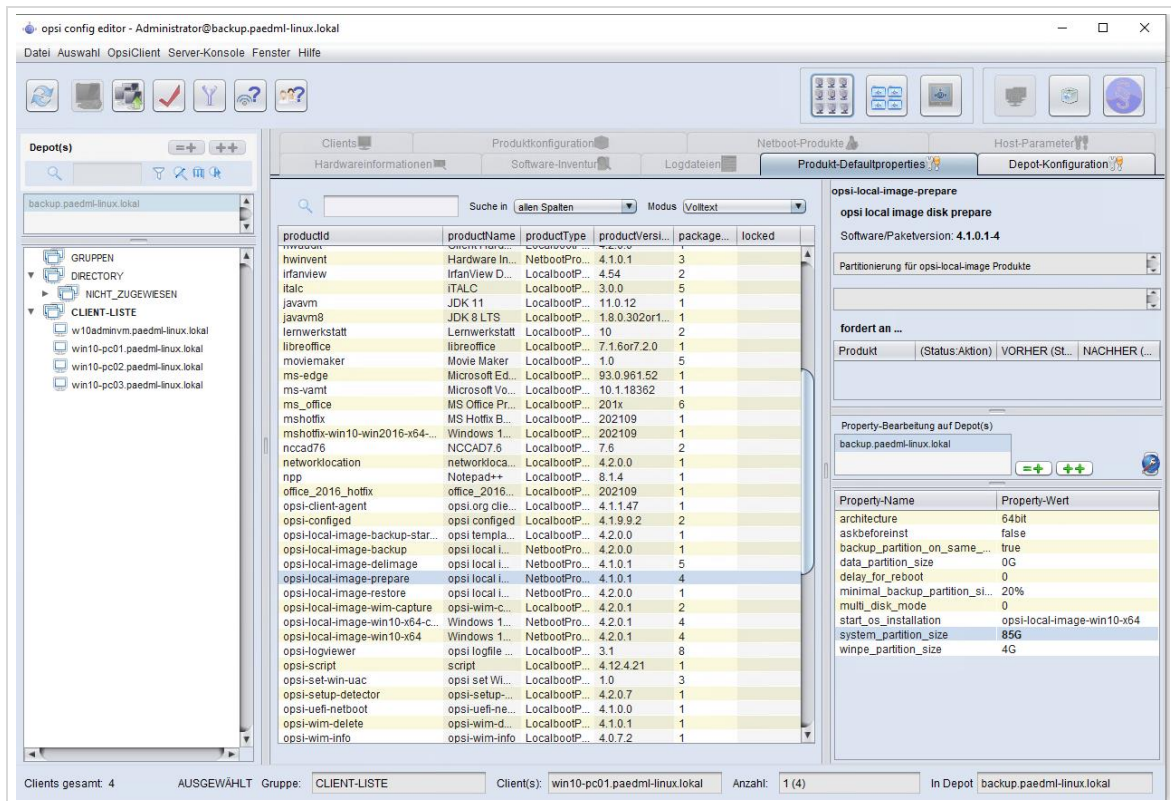


Abb. 90: Auswahl des opsi-Produktes

Die Produkteigenschaften können Sie ändern, indem Sie den zu ändernden Wert mit einem Doppelklick in der Spalte „Property-Wert“ öffnen. Sie können einen der vordefinierten Werte übernehmen oder einen neuen Index-Eintrag erstellen. Letzteres geschieht, in dem Sie den neuen Wert in das leere Feld eintragen und auf das *gelbe Plus-Zeichen* drücken. Der neue Wert wird in die Liste der auswählbaren Werte übernommen und kann ausgewählt werden.

Ein Klick auf den grünen Haken übernimmt den selektierten Eintrag als „Default-Produktproperty“. Künftig werden alle Installationen von opsi-Produkten – bis zu nächsten Änderung – mit dem neu definierten Wert ausgeführt.

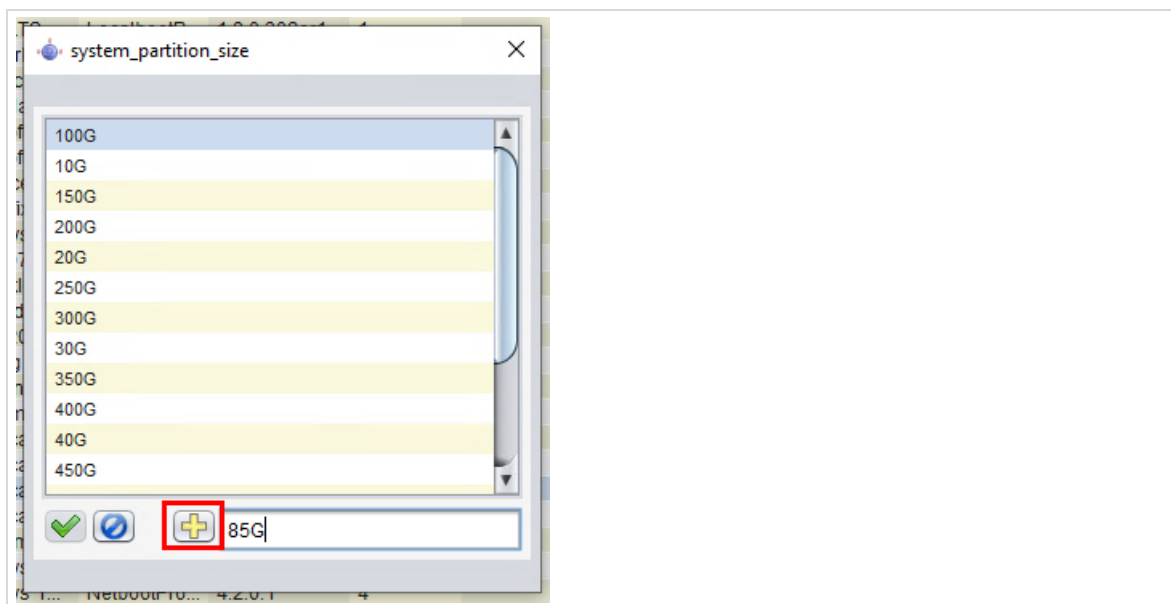


Abb. 91: Eintragen eines neuen Wertes für die Partitionsgröße

Wenn die Depot-Eigenschaften konfiguriert werden, sind alle anderen *opsi*-Reiter ausgegraut. Sie können die Reiterauswahl wieder rückgängig machen, indem Sie auf den Knopf „Client-Konfiguration“ klicken.



Abb. 92: Zugriff auf die *opsi*-Standardreiter via „Client-Konfiguration“

6.11 Troubleshooting – Probleme beim Booten

6.11.1 Konfigurieren von Bootparametern

opsi bootet beim Systemstart über das Netzwerk ein Mini-*Linux*, das Aufgaben, wie das Einspielen von *Netboot-Produkten* übernimmt. Dieses Mini-*Linux* bekommt in regelmäßigen Abständen Updates, so dass der „Kernel“, den *opsi* verwendet, stets relativ aktuell ist.

Aufgrund der Heterogenität von Hardware kann es dennoch zu Problemen beim Starten eines Rechnermodells geben. Hier können Sie versuchen, die Bootparameter der betroffenen Rechner anzupassen. Markieren Sie hierfür den (oder die) Rechner in der Übersicht (4). Wechseln Sie in den Reiter „Hostparameter“ und öffnen Sie den ersten Eintrag (ohne Bezeichnung).

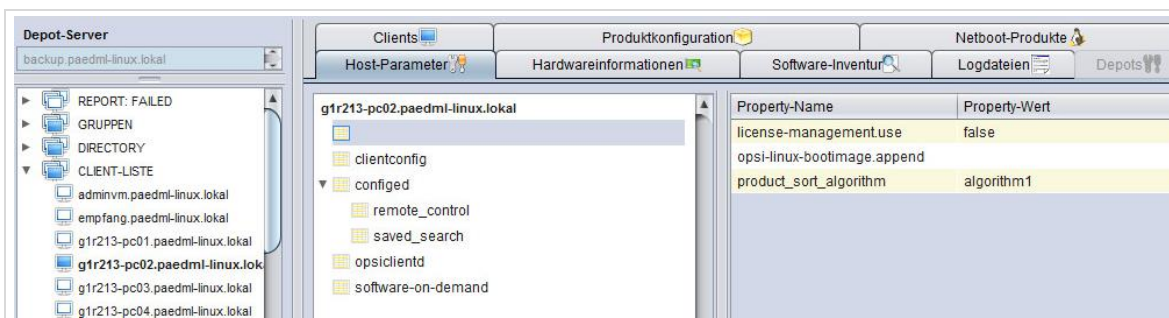


Abb. 93: Anpassen von Hostparametern für den Systemstart.

Im dynamisch gefüllten Bereich der *opsi*-Konsole (6) gibt es den Parameter „*opsi-linux-bootimage.append*“, an dem Anpassungen vorgenommen werden können. Um mehrere Werte auszuwählen, drücken Sie bitte die **Strg**-Taste und wählen Sie mit der linken Maustaste die Einträge, die in das Feld „Property-Wert“ übernommen werden sollen.

Speichern Sie die Werte, bevor Sie die Maske schließen.

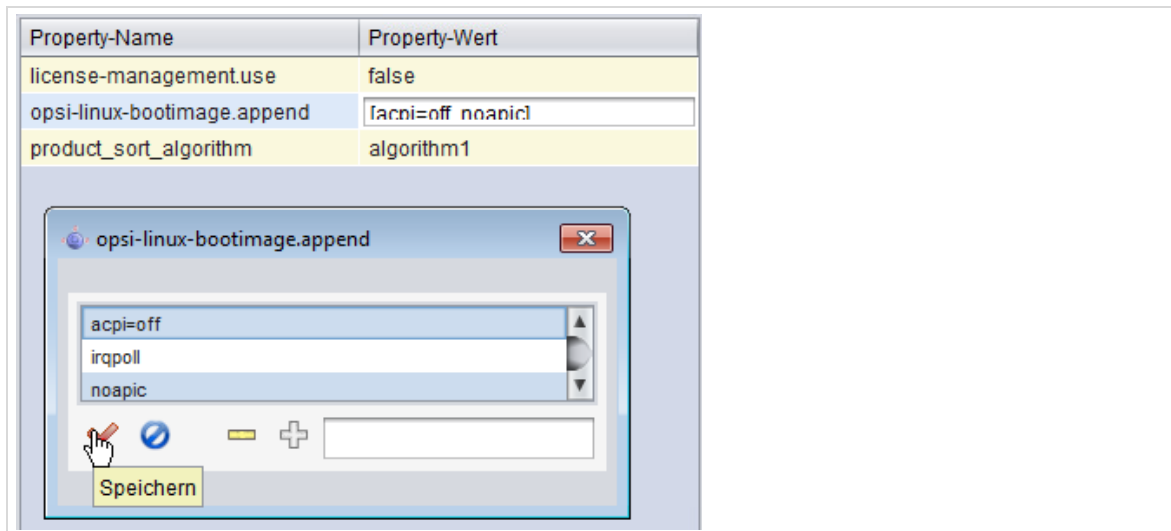


Abb. 94: Eintrag von Bootparametern in opsi

Zusätzlich zu den Anpassungen in *opsi* müssen Sie ggf. die Einstellungen des BIOS der betroffenen Rechner überprüfen und ändern.

Hierbei handelt es sich um Festplattenparameter des BIOS. Bezeichnungen und verfügbare Werte variieren je nach Hersteller:

- SATA: *deaktiviert, auto, IDE, Native, Legacy*
- AHCI: *aktiviert, deaktiviert*
- LBA: *aktiviert, deaktiviert, auto*
- 32-Bit-Zugriff: *aktiviert, deaktiviert*

Bei problematischer Hardware wird man es nicht vermeiden können, durch systematisches Probieren eine funktionierende Kombination aus PXE- und BIOS-Einstellungen zu finden.

6.11.2 Anzeige der opsi-Konsolenausgabe im Fehlerfall

Sollte sich Hardware partout nicht booten lassen, kann möglicherweise ein Blick in die Ausgabe des Bootvorganges von opsi weiterhelfen. Diese Ausgabe verbirgt sich in der Standardkonfiguration hinter einem Splash-Screen und kann erst nach Anpassungen sichtbar gemacht werden.

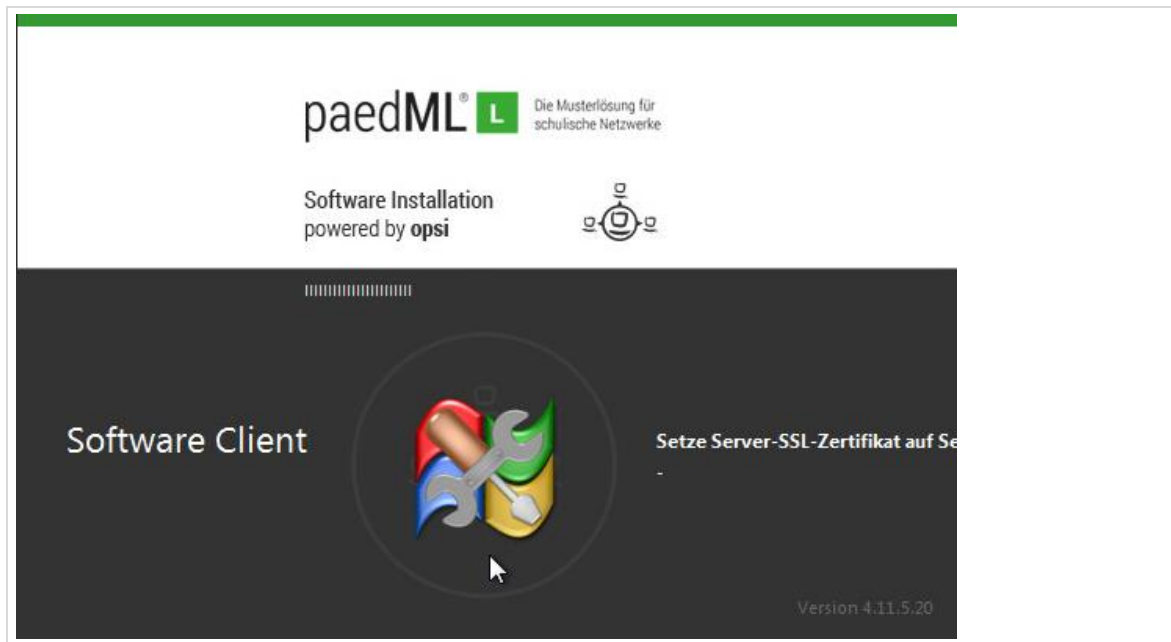


Abb. 95: Standard Splash-Screen

Um das opsi-Logo auszublenden, müssen Sie die Datei `/tftboot/linux/pxelinux.cfg/install` bearbeiten.

Entfernen Sie die letzten beiden Wörter „*quiet*“ und „*splash*“. Erstellen Sie vor dem Ändern eine Sicherungskopie der Originaldatei!

Originaldatei:

```
default opsi-install

label opsi-install
    kernel install
    append initrd=miniroot.bz2 video=vesa:ywrap,mtrr vga=791 quiet splash
```

geänderte Version:

```
default opsi-install

label opsi-install
    kernel install
    append initrd=miniroot.bz2 video=vesa:ywrap,mtrr vga=791
```

Wenn Sie anschließend einen Rechner starten, wird das opsi-Logo nicht mehr angezeigt. Stattdessen werden auf dem Bildschirm die Meldungen des Systemboots ausgegeben. Aus der Anzeige der Boot-Meldungen können Fehler ausgelesen werden.

6.11.3 Log-Dateien zu Boot-Problemen

Sollte das Problem auch über die Ausgabe des opsi-Bootimages nicht erkennbar sein, hilft häufig ein Blick in die Log-Datei des Rechners.

Beim Start von Clients schreibt opsi Logdateien, die – sofern der Rechner eine Netzwerk-Verbindung hat – auf dem Backup-Server unter `/var/log/opsi/bootimage` abgelegt werden. Hier wird für jeden Client eine Datei erstellt.

Sollte der Rechner beim Starten den Backup-Server nicht erreichen und keine Log-Datei übertragen können, so findet sich die Logdatei im Bootimage unter `/tmp/log/`. Um in einem solchen Fall an die Logdatei des Bootimages zu kommen, gibt es zwei Wege:

1. Wenn der Rechner eine Netzwerkverbindung hat, kann man per WinSCP die Datei `/tmp/log` vom Client holen.

2. Wenn das Netzwerk vom Client aus nicht erreichbar ist, können Sie die Datei per USB-Stick übertragen. Loggen Sie sich hierfür auf dem Client an der *Linux*-Konsole ein:

Benutzername: `root`, Kennwort: `linux123`

Verbinden Sie einen USB-Stick mit dem Rechner und warten Sie ein paar Sekunden. Mit dem Befehl `sfdisk -l` prüfen Sie, auf welchem Device der USB-Stick eingebunden wurde.

Anschließend muss der USB-Stick eingebunden (`#mount`), die Datei kopiert und der USB-Stick wieder ausgehängt werden.

Anschließend können Sie die Logdatei für die Analyse auslesen oder der Hotline senden.

Selbstverständlich kann die Log-Datei auch lokal ausgelesen werden.

Ein Beispiel für dieses Verfahren.

```
#sfdisk -l
Disk /dev/sda: 30401 cylinders, 255 heads, 63 sectors/track
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0
Device           Boot   Start End     #cyls #blocks   Id   System
/dev/sda1        *      0+    30401 30402   244197528 7     HPFS/NTFS
/dev/sda2         0        -      0      0           0     Empty
/dev/sda3         0        -      0      0           0     Empty
/dev/sda4         0        -      0      0           0     Empty

Disk /dev/sdb: 1017 cylinders, 33 heads, 61 sectors/track
Units = cylinders of 1030656 bytes, blocks of 1024 bytes, counting from 0
Device           Boot   Start End     #cyls #blocks   Id   System
/dev/sdb1        0+    1016 1017-   1023580  b     W95 FAT32
/dev/sdb2         0        -      0      0           0     Empty
/dev/sdb3         0        -      0      0           0     Empty
/dev/sdb4         0        -      0      0           0     Empty
# mount /dev/sdb1 /mnt
# cp /tmp/log /mnt
#umount /mnt
```

6.11.4 Besonderheiten beim UEFI-Boot

Wird ein Rechner mit UEFI-Boot verwendet, so muss das Häkchen bei UEFI-Boot gesetzt werden. Dazu klicken Sie den Reiter *Clients* an und wählen den auszurollenden UEFI-Client aus.

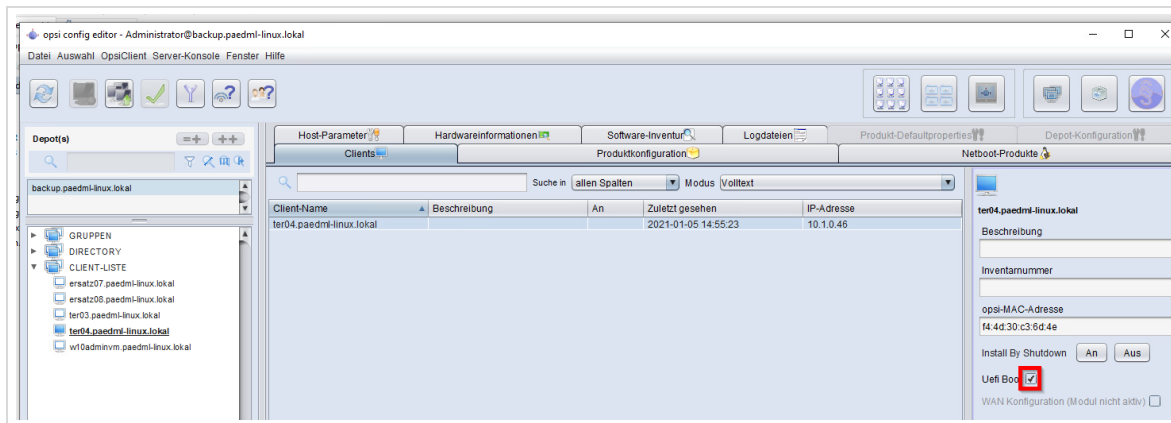


Abb. 96: UEFI-Häkchen gesetzt.

Opsi unterstützt mittlerweile auch den Secure-Boot.



Eine häufige Fehlerquelle beim Ausrollen von UEFI-Geräten sind falsche UEFI-Einstellungen.

In seltenen Fällen kommt es vor, dass sich Hardware mit opsi nicht ausrollen lässt.

An dieser Stelle sei nochmal daran erinnert, dass vor einer Anschaffung von Hardware eine Teststellung in einer aktuellen paedML Linux und GS erfolgen muss.

Bei UEFI-Geräten wird beim Starten für einen kurzen Moment ein Menü angezeigt, falls kein Netboot-Produkt angefordert wurde.

6.12 Windows 10 Funktionsupgrades (Build-Upgrades)

Funktionsupgrades (sog. Build-Upgrades) werden mit dem opsi-Produkt windows10-enablement eingespielt. Voraussetzung ist, dass das Produkt „mshotfix“ aktuell ist. Setzen Sie dafür auf allen Clients, die ein Funktionsupgrade erhalten sollen, das Produkt „mshotfix“ auf „setup“, wenn es nicht aktuell sein sollte (siehe Kapitel 6.13).

1. Wählen Sie dann alle Clients aus, die ein Funktionsupgrade erhalten sollen.
2. Wählen Sie das Produkt „windows10-enablement“ aus.
3. Klicken Sie auf den „Property-Wert“ der Property „update-to-version“.
4. Wählen Sie eine Windows 10 Version aus, auf die aktualisiert werden soll. Die aktuelle Version ist 22H2.
5. Bestätigen Sie Ihre Wahl mit dem grünen Haken.
6. Speichern Sie die Konfiguration mit einem Klick auf den roten Haken.
7. Schalten Sie nun den Client / die Clients ein. Die aktuelle Windows-Version wird gesetzt und der Client / die Clients neu gestartet.

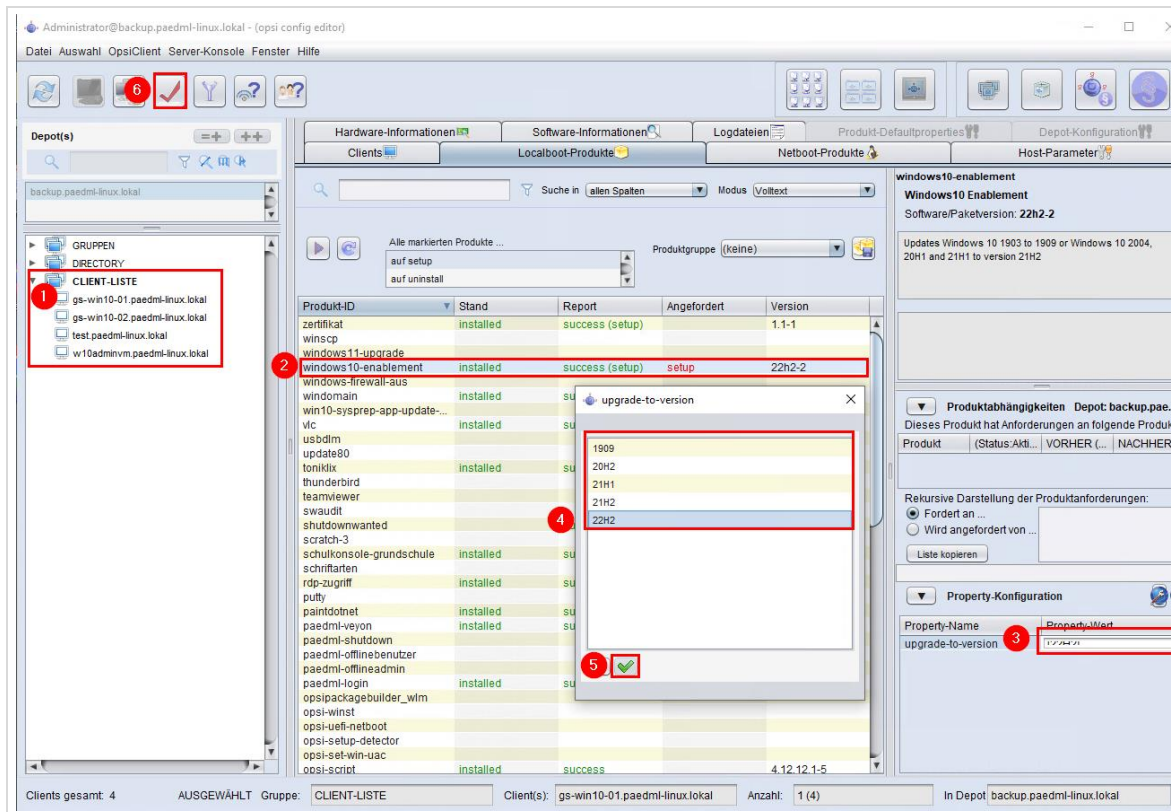


Abb. 97: Windows 10 Funktionsupgrade mit windows10-enablement

6.13 Windows 10 Qualitätsupdates (Hotfixes)

Zu den Qualitätsupdates zählen kritische Updates, sowie Sicherheits- und Treiberupdates. Sie werden über das opsi-Produkt „mshotfix“ im opsi config editor eingespielt. Um „mshotfix“ zu konfigurieren, starten Sie den opsi config editor, z.B. auf der AdminVM.

- ❶ Wählen Sie den Windows 10 Client aus. Es ist auch eine Mehrauswahl möglich, indem Sie die Shift-Taste gedrückt halten und die Clients auswählen.
- ❷ Wechseln Sie in den Reiter *Produktkonfiguration*.
- ❸ Setzen Sie das Produkt „mshotfix“ auf „setup“.
- ❹ Speichern Sie die Konfiguration mit einem Klick auf den Haken in der Symbolleiste.

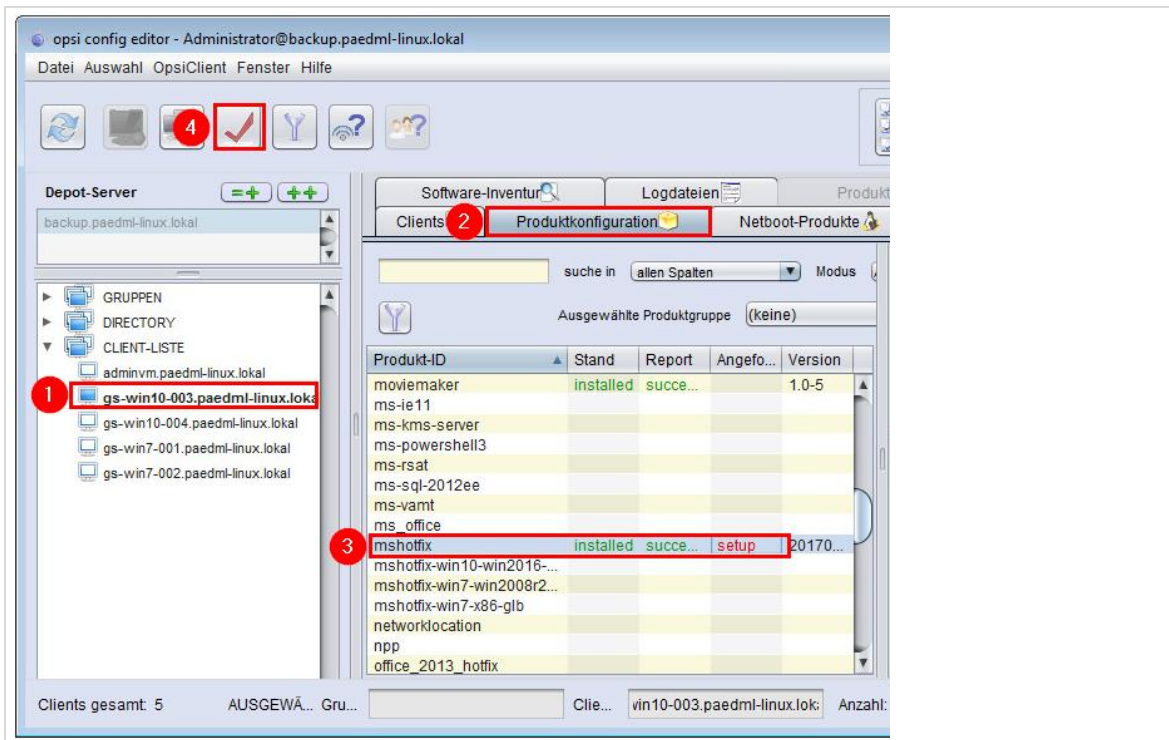


Abb. 98: opsi-Produkt mshotfix

6.14 Einspielen von Software



Wenn der zu installierende Rechner bereits über *opsi* verwaltet und das Betriebssystem erneut installiert wurde, sind in der Datenbank von *opsi* noch alte Informationen zu der bisher installierten Software eingetragen. Diese Werte müssen manuell gelöscht werden!

Um die Informationen zu löschen, müssen Sie den neu installierten Rechner in der *Clientliste* (4) markieren. Anschließend öffnen Sie in der *Menüleiste* (1) den Eintrag „*opsiClient* | *Localboot-Produkte zurücksetzen*“. Im anschließenden Dialogfenster müssen Sie die Änderungen mit „Ja“ übernehmen.

Die Werte in der „*Produktkonfiguration*“ des Rechners sind anschließend unwiederbringlich gelöscht.

Folgende OPSI-Produkte dürfen nicht erneut installiert werden, wenn die Versionsnummer rot angezeigt wird: „adminvm“, „clientprodukte“, „dotnetfx“, alle Produkte beginnend mit „ms-“, außer „ms-edge“.

Bei der Softwareverteilung kommen die Localboot-Produkte zum Einsatz. Um Software auszuspielen, öffnen Sie im Hauptfenster (5) den Reiter „Produktkonfiguration“.

Software, die Sie auf Clients einspielen wollen, muss im opsi-Depot vorgehalten werden. Wie Sie Software in das opsi-Depot hochladen können, ist in Kapitel 6.19 beschrieben.

Die Verteilung eines Localboot-Produkts kann auf einzelne Rechner oder auf Rechnergruppen geschehen, die in der Rechnerliste (4) markiert wurden.

Wählen Sie das Produkt aus und klicken Sie in die Spalte „Angefordert“. Wählen Sie dort den Eintrag „Setup“.

Der dynamische Inhalt der opsi-Konsole (6) wird nun mit Informationen zum ausgewählten Produkt und mit Parametern („Konfiguration für Client“) gefüllt, die angepasst werden können. Wenn Abhängigkeiten zu anderen Paketen bestehen, werden diese automatisch mitinstalliert.

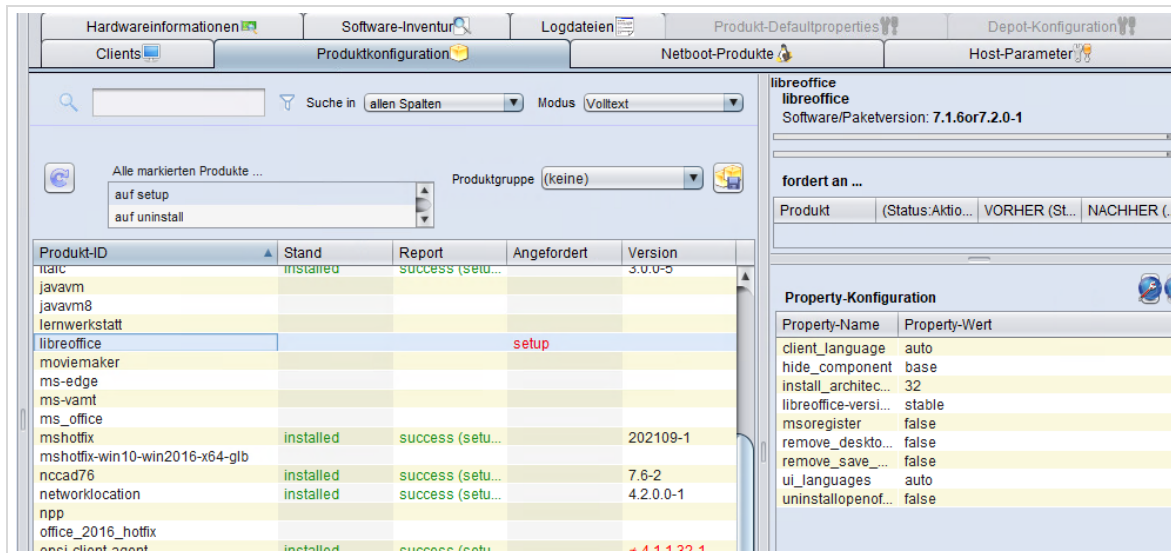


Abb. 99: Softwareinstallation am Beispiel von Audacity

Alle Änderungen müssen anschließend wieder mit dem roten Haken unter (2) gespeichert werden.

Sie können die Installation von Produktpaketen entweder gleich nach der Konfiguration von Netboot-Produkten vornehmen. Die Software wird im Anschluss an die Installation des Betriebssystems ausgespielt.

Oder Sie können nachträglich Programme auf installierten Rechnern einspielen.

Die Installation der ausgewählten Netboot-Produkte startet automatisch, wenn der Rechner das nächste Mal hochgefahren wird. opsi überprüft nach jedem Systemstart, ob es Aktualisierungen für den Rechner gibt.

Alternativ kann die Installation neuer Pakete manuell ausgelöst werden. Um die Installation auszulösen, wechseln Sie im Hauptfenster (5) in den Reiter Clients und klicken Sie mit der rechten Maustaste über die ausgewählten Clients. Sie haben nun verschiedene Optionen, um die Installation zu initiieren. So können Sie – sofern der Rechner das unterstützt – bei ausgeschaltetem System einen Systemstart anstoßen. Sie können bei eingeschalteten Rechnern auch ein Ereignis „on_demand“ auf den ausgewählten Clients auslösen (Rechtsklick auf das Produkt in der Produktkonfiguration).

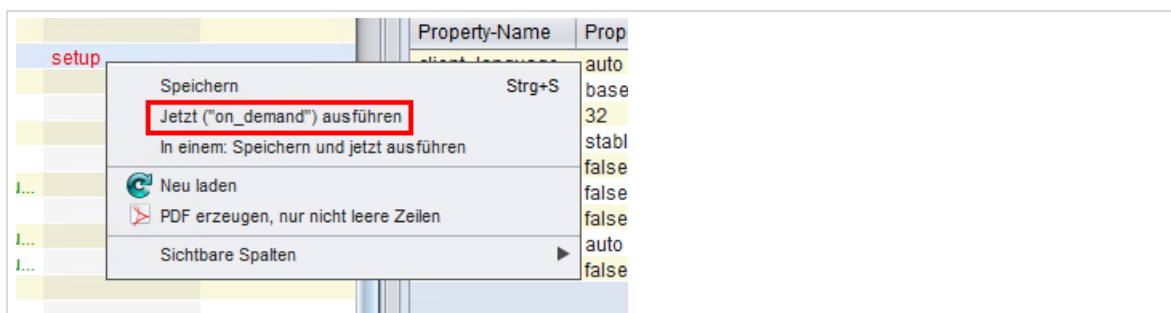


Abb. 100: Start der Softwareinstallation

Hinweis

Das sogenannte „user-profile-management“²⁸ kann beispielsweise dazu genutzt werden Benutzereinstellungen bei der Anmeldung des Benutzers vorzunehmen.

Solange der Prozess aktiv ist, erscheint folgende Meldung:



Abb. 101: Dialogfenster bei aktivem „user-profile-management“

6.15 Empfohlene opsi-Localboot-Produkte

Wenn ein Rechner mit Software versorgt wird, so gibt es einige Pakete, die installiert werden müssen, damit die Funktionen der paedML Linux im pädagogischen Netzwerk gewährleistet sind. Bitte wählen Sie diese nachfolgend genannten Pakete unbedingt aus! (Fast)²⁹ alle hier beschriebenen Localboot-Produkte und weitere Programme finden Sie im opsi-Paket „clientprodukte“, das bei der automatischen Rechnerinstallation aktiv ist oder manuell ausgespielt werden kann.

1. *Windomain* – Dieses Paket führt den Domänenbeitritt der Rechner durch und muss installiert werden. Bei jeder Wiederherstellung eines Images wird dieses Paket ausgeführt, um dem Rechner erneut in die Domäne aufzunehmen.
2. *paedml-login*: Das Paket kopiert Skripte für die Anmeldung auf den Client. Außerdem kann hier die paedML Variante (paedML für Grundschulen oder paedML Linux) angegeben werden.
3. *zertifikat* – Dieses Paket installiert das Stammzertifikat des Servers, das für die verschlüsselte Kommunikation zwischen Server und Clients (z.B. Schulkonsole, ...) benutzt wird.
4. *italc* – Dieses Paket ermöglicht den Zugriff auf Schülerrechner aus der Schulkonsole. Die Funktionsweise ist im Lehrerhandbuch beschrieben. Angemeldet als Lehrer, sollte Bildschirmübertragung mittels italc nicht möglich sein. Dies ist in der paedML Linux als Standard konfiguriert, sodass hier keine manuellen Arbeiten notwendig sind.
5. *google-chrome-for-business* – Wir empfehlen Chrome als Standardbrowser für die *paedML Linux*. Sie können auch andere Browser verwenden. Es treten aber unter Umständen Probleme auf, beispielsweise beim Umgang mit Server-Zertifikaten.

²⁸ Vgl. <http://download.uib.de/opsi4.0/doc/opsi-manual-de.pdf> Kapitel 20 „opsi Erweiterung User Profile Management“

²⁹ Das Paket windomain ist nicht im Paket „clientprodukte“ enthalten, da der Domänenbeitritt über einen anderen Automatismus angestoßen wird.

6. *config-win10* – Dieses Paket nimmt einige Einstellungen unter Windows 10 vor. Ausführliche Informationen zu diesem Paket finden Sie am Ende dieses Kapitels.
7. *usbdlm* – verhindert, dass sich USB-Laufwerke (z.B. Cardreader) von der *paedML* reservierte Laufwerksbuchstaben (z.B. H:\) übernehmen.
8. *shutdownwanted* – Über dieses Paket können Rechner nach der Durchführung von Installationen automatisiert heruntergefahren werden. Dieses Paket ist nötig, da opsi Rechner so lange neu startet, bis keine Aktionen mehr ausgeführt werden. Ein Rechner würde also ohne dieses Paket nach der Installation eingeschaltet bleiben.
9. Des Weiteren empfehlen wir Ihnen, alle in opsi verfügbaren *Hotfixes* auszuspielen. Bitte beachten Sie, dass die Installation von Hotfixes viel Zeit beanspruchen kann.

opsi-Paket „config-win10“

Melden Sie sich als Administrator im *opsi config editor* an. Wählen Sie dann einen oder mehrere zu konfigurierende Windows 10-Clients aus (❶). Klicken Sie dann im *opsi config editor* im Reiter „Produktkonfiguration“ (❷) auf das Produkt „config-win10“ (❸). Sollte es noch nicht installiert sein, können Sie dies nachholen, indem Sie das Produkt in der Spalte „Angefordert“ auf „setup“ setzen. In der Property-Konfiguration (❹) können Sie nun *Windows 10* anpassen. Zum Abschluss wird die Konfiguration mit einem Klick auf den Haken in der Symbolliste gespeichert (❺).

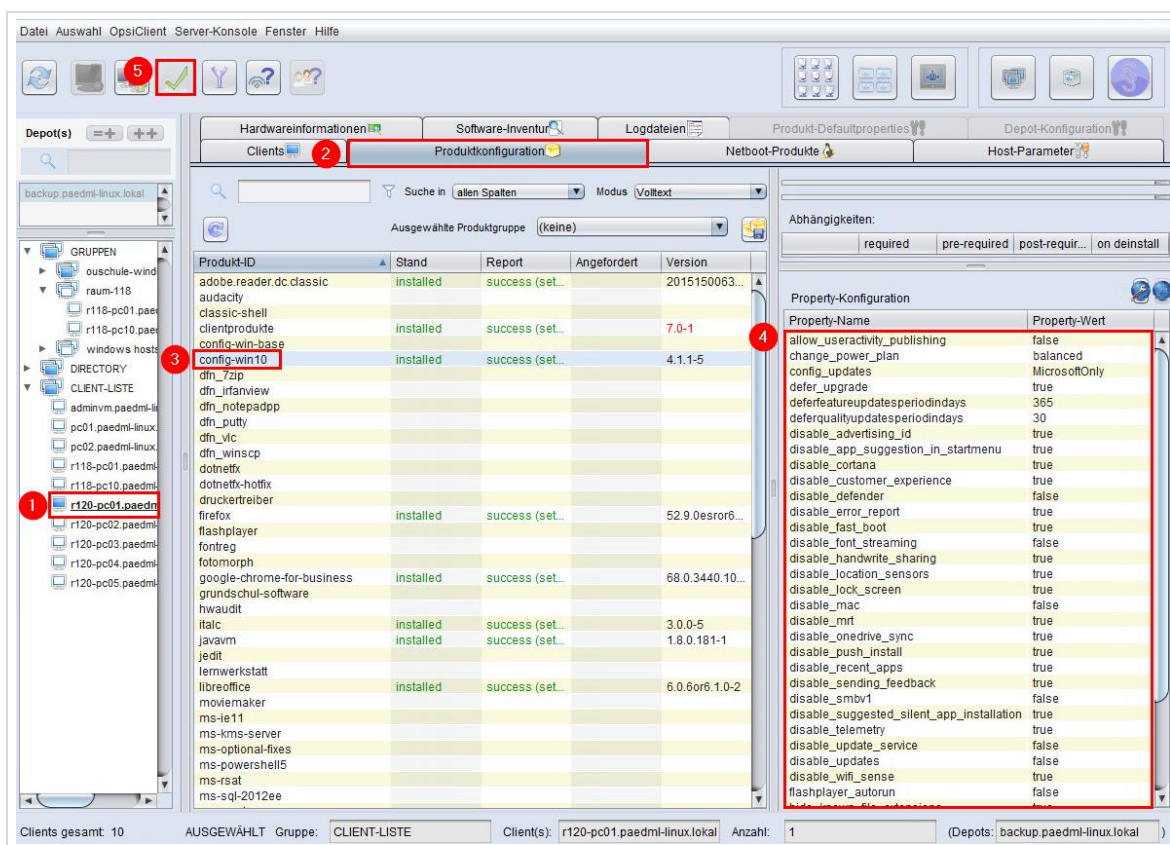


Abb. 102: Properties von „config-win10“

Die einzelnen „Properties“ werden in der nachfolgenden Tabelle erklärt und eine Empfehlung für den Einsatz in Schulen ausgesprochen. Beachten Sie bitte, dass nachfolgende Empfehlungen nicht für jeden Einsatzzweck gültig sein können. Dringend empfohlen ist der Einsatz von *Windows 10 Education*, da in anderen Editionen bestimmte Einstellungen nicht oder nur teilweise möglich sind.



Bei Änderungen, die nicht mit unseren Vorgaben übereinstimmen (z.B. eine Änderung der Property „location_sensors“ müssen die Gruppenrichtlinien entsprechend geändert werden.

Property-Name	Erklärung	Empfehlung
allow_useractivity_publishing	Bestimmt, ob Benutzeraktivitäten veröffentlicht werden dürfen.	Deaktivierung empfohlen
change_power_plan	<p>Auswahl des Energiesparplans:</p> <p>„balanced“: Automatischer Ausgleich zwischen Leistung und Stromverbrauch</p> <p>„high performance“: Leistung hat Vorrang</p> <p>„Energiesparmodus“: Stromverbrauch wird reduziert</p>	<p>Je nach Einsatzzweck, „high performance“ für die adminVM dringend empfohlen</p>
config_updates	<p>Windows 10 bietet verschiedene Möglichkeiten an, Updates aus dem Internet herunterzuladen:</p> <p>AllowPeerToPeer: Erlaubt Updates von Microsoft und von „Peer-to-Peer“ Clients im Internet. Dies können beliebige Clients im Internet sein, die das Update bereits geladen haben.</p> <p>Achtung: Ist diese Updatevariante aktiviert, können andere Windows 10 Nutzer im Internet Updates von Ihrem Client herunterladen. Dies kann Ihre Uploadbandbreite beanspruchen.</p> <p>LocalPeerToPeer: Erlaubt Updates von Microsoft und von lokalen „Peer-to-Peer“ Clients. Diese Option kann Ihre Internetbandbreite schonen, da das Update im Idealfall zumindest teilweise von Clients im lokalen Netzwerk geladen wird.</p> <p>Microsoft Only: Erlaubt Updates nur von offiziellen Microsoft Servern.</p>	<p>Kann auf „MicrosoftOnly“ belassen werden.</p>
defer_upgrade	<p>Stellt Qualitätsupdates 4 Wochen und Funktionsupdates 8 Monate zurück. Danach werden die Updates durch Microsoft automatisch installiert.</p> <p>Achtung: „defer_upgrade“ ist abhängig von „disable_updates“ und umgekehrt. Es darf nur eines der beiden Properties auf „true“ gesetzt sein.</p>	<p>Empfohlen wird, „defer_upgrade“ auf „true“ und „disable_upgrade“ auf „false“ zu setzen.</p>

deferfeatureupdatesperiodindays	Verschiebt die i. d. R. zwei Mal pro Jahr erscheinenden großen Microsoft Windows 10 Feature Updates um die angegebenen Tage.	365 empfohlen
deferqualityupdatesperiodindays	Verschiebt kleinere Microsoft Windows 10 Updates um die angegebenen Tage.	30 empfohlen
disable_advertising_id	Deaktiviert die „Advertising ID“, welche von Microsoft dazu verwendet wird, individualisierte Werbung zu platzieren.	Deaktivierung empfohlen
disable_app_suggestion_in_startmenu	App-Vorschläge im Startmenü deaktivieren	Deaktivierung empfohlen
disable_cortana	Deaktiviert den Sprachassistenten „Cortana“	Deaktivierung empfohlen
disable_customer_experience	Deaktiviert das Kundenzufriedenheitsprogramm von Microsoft	Deaktivierung empfohlen
disable_defender	Deaktiviert den „Windows-Defender“ (Schutz vor Viren und Schadsoftware). Wird ein Antivirus-Programm eines Fremdherstellers eingesetzt, sollte der Windows-Defender deaktiviert werden.	Der Defender sollte aktiviert sein.
disable_error_report	Deaktiviert die Windows-Fehlerberichterstattung.	
disable_fast_boot	Deaktiviert die Funktion „Fast Boot“, die ein schnelleres Booten des Clients ermöglichen soll. Diese Funktion sollte auf dem Wert „true“ belassen werden, da es sonst zu Problemen mit <i>opsi</i> kommen kann.	Deaktivierung empfohlen
disable_font_streaming	Deaktiviert das automatische Laden (Streaming) von nicht installierten Schriften aus dem Internet.	Kann aktiviert bleiben
disable_handwrite_sharing	Deaktiviert die Übermittlung von Daten an Microsoft, die die Handschriftenerkennung (z.B. bei Tablets) verbessern sollen.	Deaktivierung empfohlen
disable_location_sensors	Auf „true“ gestellt wird die Standort- und Sensorenerkennung abgeschaltet	Je nach Einsatzzweck und Endgerät
disable_lock_screen	Abschalten des „Lock Screens“: Der Lock-Bildschirm wird vor dem eigentlichen Login-Bildschirm angezeigt. Er enthält ein Bild, Uhrzeit und Datum.	Deaktivierung empfohlen

disable_mrt	Deaktiviert das Tool zur Schadsoftware-Entfernung	Deaktivierung empfohlen
disable_news_and_interest	Nachrichten in der Taskleiste deaktivieren	Je nach Einsatzzweck
disable_onedrive_sync	Deaktiviert die Microsoft Onedrive-Synchronisierung	Je nach Einsatzzweck
disable_push_install	Verhindert, dass Nutzer Apps aus dem Store auf den Rechner pushen können.	Deaktivierung empfohlen
disable_recent_apps	Verhindert, dass häufig genutzte Programme im Startmenü erscheinen. Weitere Startmenü Einstellungen werden mithilfe der Gruppenrichtlinie paedMLL_Benutzer konfiguriert.	Deaktivierung empfohlen
disable_sending_feedback	Deaktiviert das Senden von Diagnosedaten an Microsoft	Deaktivierung empfohlen
disable_smbv1	Deaktivierung des SMBV1-Protokolls	Deaktivierung nicht empfohlen
disable_suggested_silent_app_installation	Verhindert, dass bestimmte Apps (u. a. Spiele) im Hintergrund heruntergeladen und installiert werden.	Deaktivierung empfohlen
disable_telemetry	Verhindert das Senden von gesammelten Daten an Microsoft.	Deaktivierung empfohlen
disable_update_button	Deaktivierung des „Update-Buttons“ in den Einstellungen	Deaktivierung nicht empfohlen
disable_update_service	Deaktiviert den Windows Update Service. Achtung: Kann bei Verwendung von DISM zu Problemen führen.	Deaktivierung nicht empfohlen
disable_updates	Verhindert Windows 10 Updates (Funktions- und Qualitätsupdates). Sicherheitsupdates können eingespielt werden, indem Sie das Produkt „mshotfix“ für den entsprechenden Client im Reiter „Produktkonfiguration“ auf „setup“ setzen. Werden Updates abgeschaltet, können keine Windows-Updates, Defender-Signaturen-Updates und Treiber mehr von "Microsoft Windows Update" automatisch heruntergeladen werden.	Deaktivierung nicht empfohlen
disable_wifi_sense	Deaktivieren von „WiFi-Sense“. WiFi-Sense (WLAN-Optimierung) ermöglicht es, WLAN-	Deaktivierung empfohlen

	Zugangsdaten mit Outlook.com, Skype- oder Facebook-Kontakten zu teilen. ³⁰	
flashplayer_autorun	Automatischer Start des Adobe Flashplayers deaktivieren	Deaktivierung empfohlen
hide_known_file_extensions	Bei Aktivierung werden gängige und bekannte Dateierweiterungen, wie zum Beispiel .exe versteckt.	Deaktivierung empfohlen
local_wsus_available	Bitte nur aktivieren, wenn sie einen WSUS-Server betreiben.	Je nach Einsatzzweck
minimize_recommendations	Bei Aktivierung werden von Win 10 weniger Hinweise angezeigt.	Aktivierung empfohlen
no_new_app_install_notification	Bei Aktivierung werden Mitteilungen über neu installierte Apps nicht angezeigt.	Aktivierung nicht empfohlen
online_search	Deaktiviert die Web-Suche, wenn nach einer Datei oder einem Kommando gesucht wird.	Deaktivierung empfohlen
remove_edge_from_desktop	Entfernt ab Win 10 1803 die Edge Verknüpfung vom Desktop.	Keine Empfehlung
show_all_folder_in_navbar	Bei Aktivierung werden alle Ordner in der linken Navigationsspalte des Explorers angezeigt.	Keine Empfehlung
show_drive_letter_first	Zeigt den Laufwerksbuchstaben vor der Laufwerksbezeichnung an.	Keine Empfehlung
show_thispc_instead_of_quicklaunch	Bei Aktivierung öffnet der Explorer „DieserPC“ statt „Schnellzugriff“.	Aktivierung empfohlen
sync_settings	Synchronisiert die Windows-Einstellungen mit einer Account-ID, z.B. einem Microsoft-Konto.	Deaktivierung empfohlen

6.16 Windows 10 Gruppenrichtlinien

Über das opsi-Paket „*config-win-10*“ kann Windows 10 konfiguriert werden (siehe voriges Kapitel). Um weitere Einstellungen vornehmen zu können (z.B. das Festlegen der Standardprogramme) kommt in der paedML Linux eine speziell für Windows 10 angepasste Gruppenrichtlinie „*paedML_Win10*“ zum Einsatz.

³⁰ Vgl. <http://stadt-bremerhaven.de/windows10-wi-fi-sense/>, abgerufen am 24.03.2017

Wie Sie die Gruppenrichtlinien in ein bestehendes System einpflegen, ist in der Upgradeanleitung auf die paedML Linux 7.2 beschrieben:

<https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#updates>



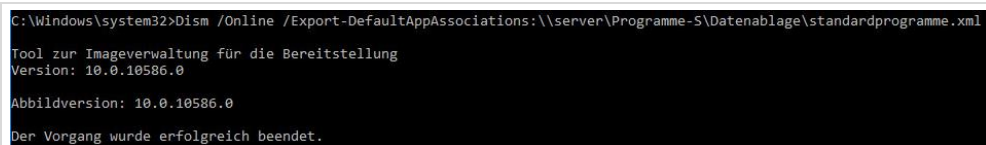
Achtung: Nehmen Sie bitte nur Änderungen an den Gruppenrichtlinien vor, wenn Sie sich über deren Auswirkungen bewusst sind.

Beispiel: Einstellen der Standardprogramme unter Windows 10

Nachfolgend ist beschrieben, wie Sie unter Windows 10 mithilfe eines Referenzrechners Standardprogramme festlegen können. Die Konfiguration wird als XML-Datei exportiert und über eine Gruppenrichtlinie an die anderen Clients verteilt, sodass an allen Clients die gleichen Standardprogramme eingestellt sind:

1. Melden Sie sich an einem Windows 10 Client als Administrator an.
2. Legen Sie die Standardprogramme fest: Start | Einstellungen | System | Standard Apps
3. Erstellen Sie eine XML-Datei mit folgendem Befehl in der Eingabeaufforderung von Windows. Ersetzen Sie „<path to xml file>“ durch den Speicherort, z.B. \\SERVER\Programme-S\Datenablage

```
Dism /Online /Export-DefaultAppAssociations:<path to xml
file>\standardprogramme.xml>
```



```
C:\Windows\system32>Dism /Online /Export-DefaultAppAssociations:\\server\Programme-S\Datenablage\standardprogramme.xml
Tool zur Imageverwaltung für die Bereitstellung
Version: 10.0.10586.0
Abbildversion: 10.0.10586.0
Der Vorgang wurde erfolgreich beendet.
```

Abb. 103: XML-Datei mit Standardzuordnungen wurde erfolgreich erstellt

Nun kann die XML-Datei über eine Gruppenrichtlinie an alle Clients verteilt werden. Öffnen Sie in der Admin-VM den Gruppenrichtlinienditor, bearbeiten eine Computergruppenrichtlinie (z.B.: „paedMLL_EigeneAnpassungen“) und navigieren Sie zu:

Computerkonfiguration | Richtlinien | Administrative Vorlagen | Windows-Komponenten | Datei-Explorer

4. Klicken Sie doppelt auf „Konfigurationsdatei für Standardzuordnungen festlegen“.

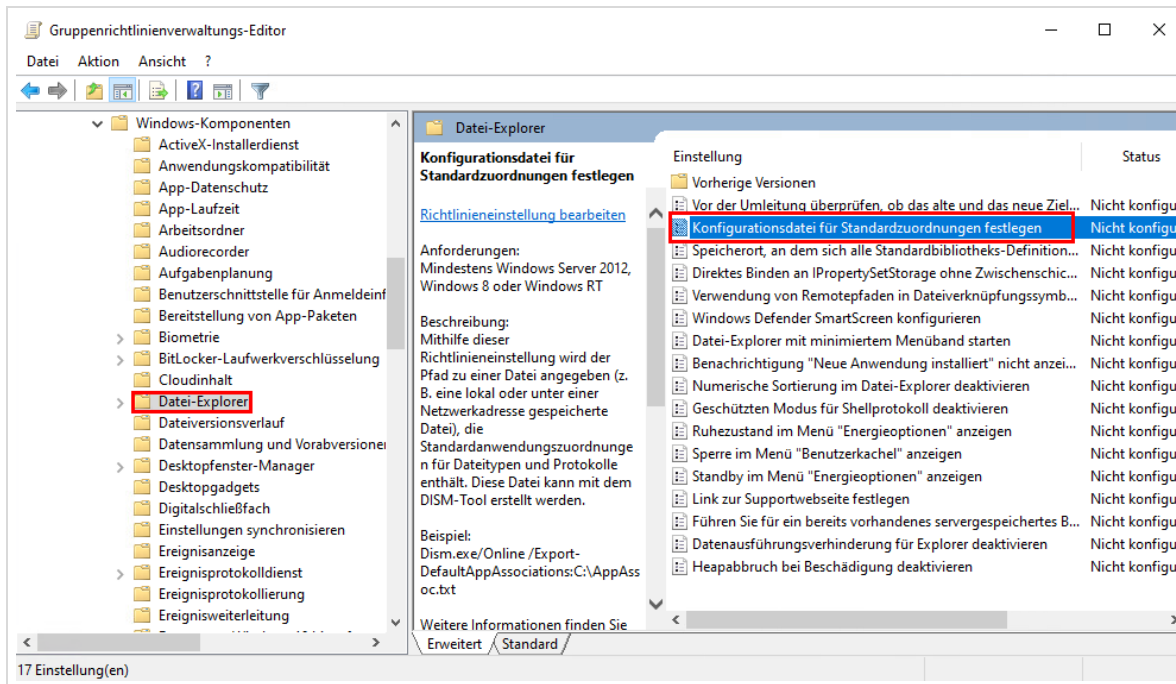


Abb. 104: Gruppenrichtlinie zum Festlegen von Standardprogrammen

5. Geben Sie den Pfad zu der vorher exportierten XML-Datei an und bestätigen Sie mit „OK“.

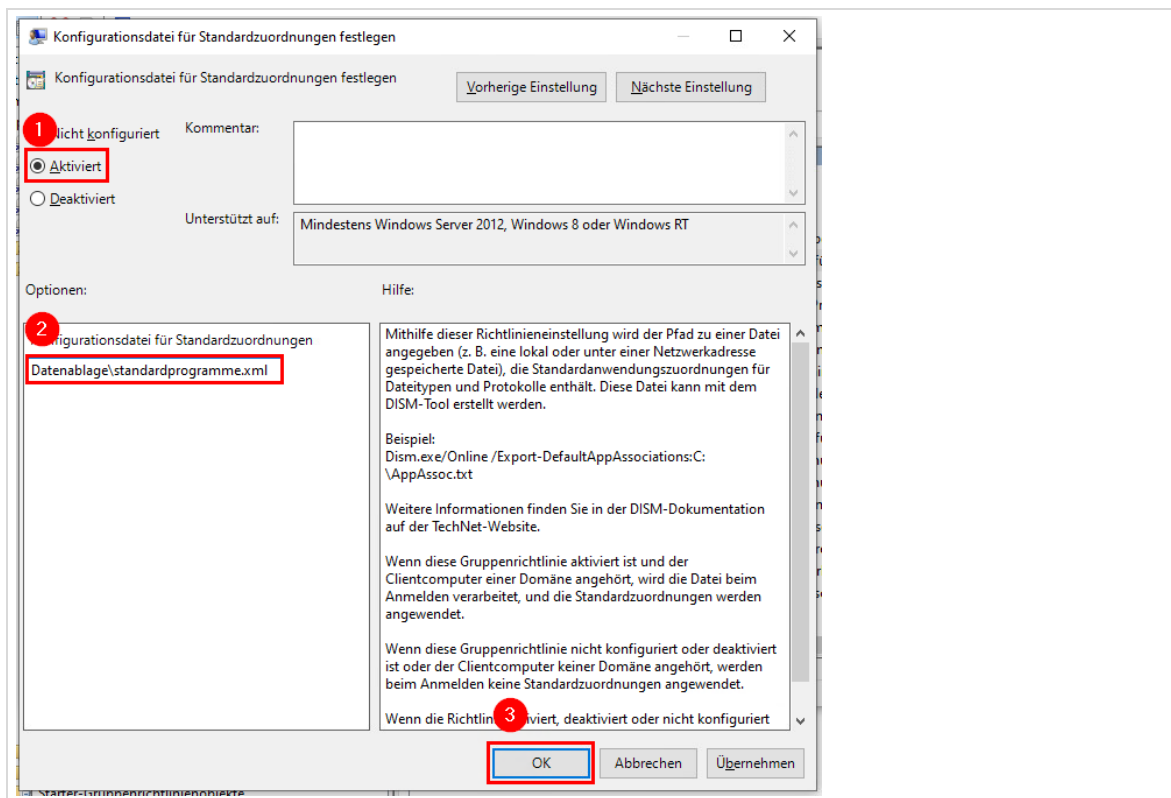


Abb. 105: Pfad der XML-Datei angeben.

6. Beim nächsten Start des Windows 10 Clients werden die neuen Standardprogramme gesetzt. Wenn sich ein Benutzer erstmalig an einem Windows 10 Client anmeldet muss er einmalig einen Haken bei „Immer diese App zum Öffnen von *-Dateien verwenden“ und mit „OK“ bestätigen:

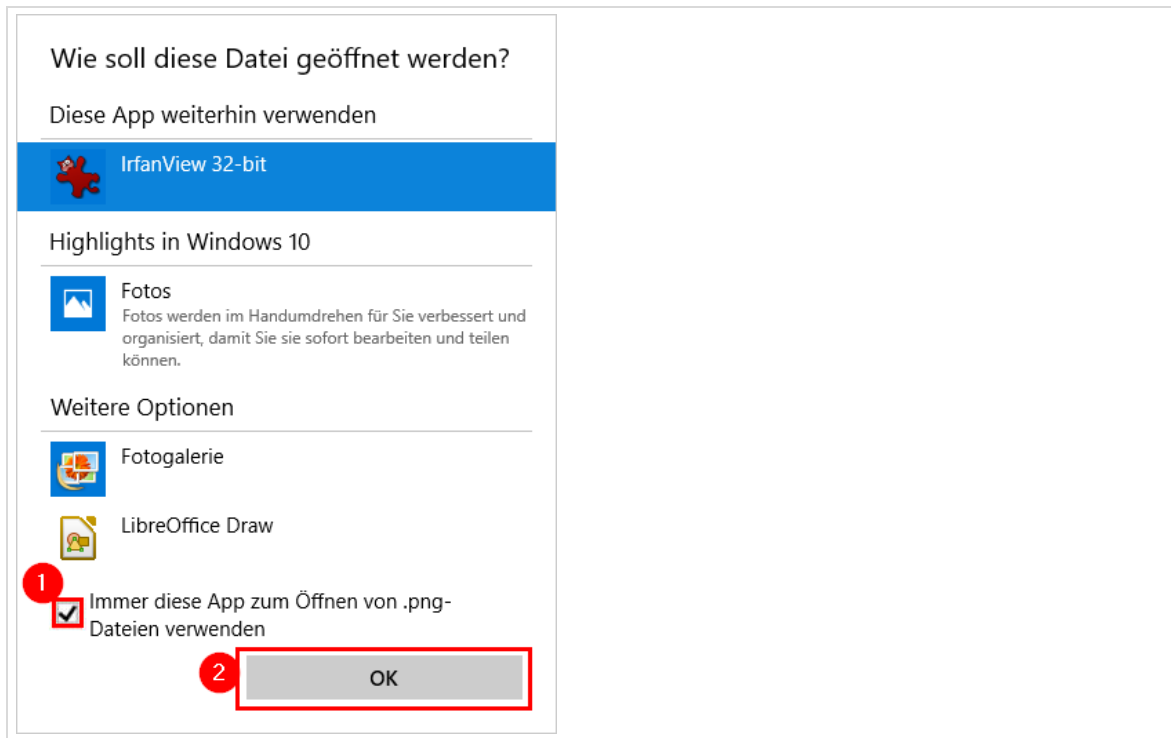


Abb. 106: Standardprogramm bestätigen

6.17 Neuinstallation von Rechnern



Dieses Kapitel ist nur dann relevant, wenn Sie Rechner neu aufsetzen und mit abweichender Software installieren wollen.

opsi speichert alle Informationen über verwaltete Rechner in einer Datenbank. Hier werden auch alle über *opsi* auf dem Rechner installierten Programme hinterlegt.

Wenn die Installationsdaten von Rechnern nicht – wie hier beschrieben – bereinigt werden, spielt *opsi* automatisch nach der Installation des Betriebssystems die für den Rechner hinterlegten Programme ein.

Vor einer kompletten Neuinstallation von Rechnern, die mit *opsi* verwaltet werden, sollte der Datensatz der betroffenen Geräte bereinigt werden. Alle Informationen zu *Localboot-Produkten* – also der von *opsi* installierten Software - der vorherigen *Windows*-Installation müssen hierbei gelöscht werden.

Um die *opsi*-Datenbank zu bereinigen, öffnen Sie zunächst den *opsi-configed*, wechseln Sie dann in die Rechner-Liste im Reiter „*Clients*“ und markieren Sie die Rechner, deren Informationen über installierte *Localboot-Produkte* gelöscht werden sollen.

Ein Klick auf die ausgewählten Rechner mit der rechten Maustaste öffnet ein Menü (1). Dort müssen Sie den Eintrag „*Localboot-Produkte zurücksetzen*“ auswählen (2).

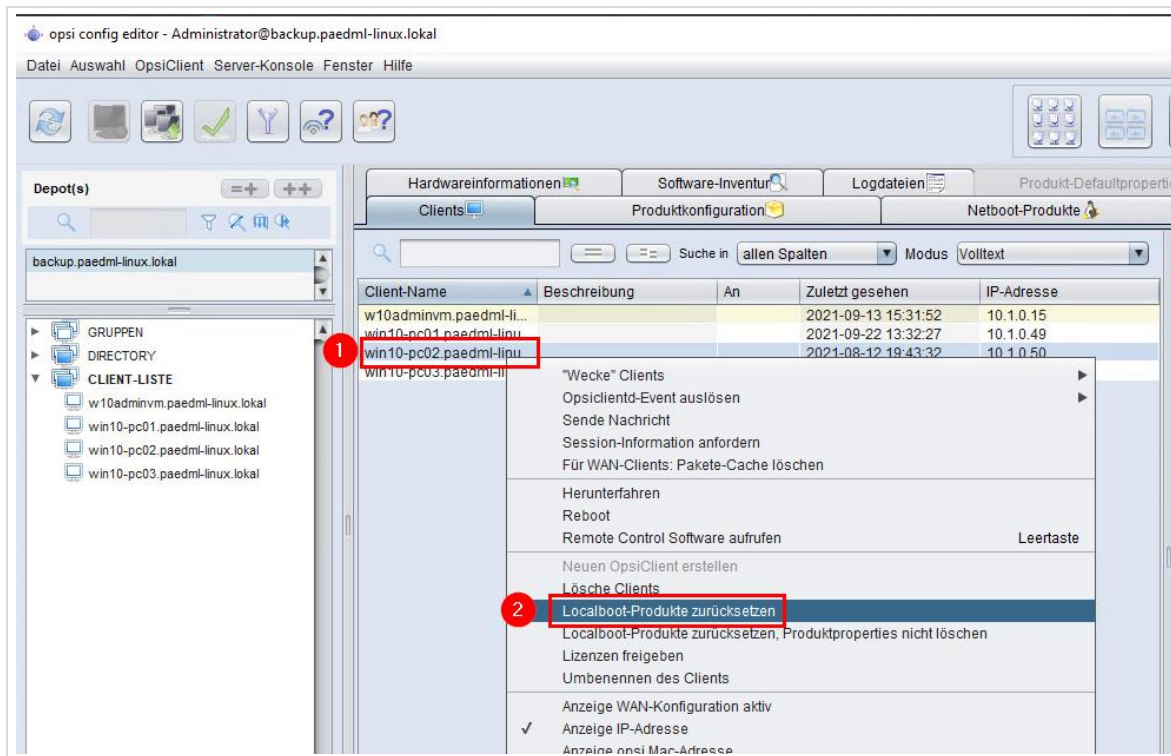


Abb. 107: „Localboot-Produkte“ zurücksetzen

Nun werden alle den Rechnern zugeordneten *Localboot-Produkte* aus der Datenbank gelöscht und *Windows* kann auf die Rechner neu ausgerollt werden.

6.18 Erstellen von opsi-Paketen

Das Erstellen von opsi-Paketen ist Aufgabe eines Dienstleisters.

Nähere Informationen zum Erstellen von opsi-Paketen entnehmen Sie dem „How To opsi“:

<https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-windows/#howtos>.



Die Erstellung, Einrichtung und Problembehandlung von *opsi-Paketen*, die nicht von Servern des Landesmedienzentrums bezogen werden, wird nicht durch die Mitarbeiter des *Support-Netzes* unterstützt.

6.19 Einbindung von opsi-Paketen

Alle Programme, die über opsi verteilt werden können, liegen auf dem Backup-Server im Verzeichnis `/var/lib/opsi/depot/PROGRAMMNAME`.

Unter `/var/lib/opsi/depot/` finden Sie alle opsi-Produkte, also Localboot-Produkte wie Programme (z.B. der Editor Notepad++) und Netboot-Produkte, die für die Installation benötigt werden (z.B. opsi-local-image-win10-x64).

opsi-Pakete können verschiedene Quellen haben:

- Die paedML Linux wird mit einigen opsi-Paketen ausgeliefert. Das Support-Netz stellt hierzu auf einem Updateserver Aktualisierungen zur Verfügung, die automatisch heruntergeladen und in das opsi-Depot aktualisiert werden. Das Angebot kann sich mit der Zeit ändern!

- Daneben können Inhalte aus anderen Quellen manuell eingebunden werden (z.B. Angebote der SoN-Gruppe). Diese Software muss in das opsi-Depot übertragen werden. Aktualisierungen müssen manuell vorgenommen werden.
- Darüber hinaus können Sie Dienstleister beauftragen, um Software für opsi zu paketieren oder eigene Pakete schnüren. Ein Dienstleister wäre die Firma uib (www.uib.de), die opsi entwickelt.
- Es gibt im Internet auch Paketquellen von opsi-Paketen. Informationen hierzu finden Sie unter anderem hier: https://wiki.opsi.org/userspace:free_opsi_repositories



Achtung! Das Einspielen von opsi-Paketen von Drittanbietern geschieht ausdrücklich auf eigene Gefahr.

Laden Sie die opsi-Datei herunter und speichern Sie diese zum Beispiel im Administrator-Homeverzeichnis.

Öffnen Sie den opsi-configed und führen Sie dort im Reiter *Server-Konsole* im Menü *opsi* den Befehl *Paket-Installation* aus.

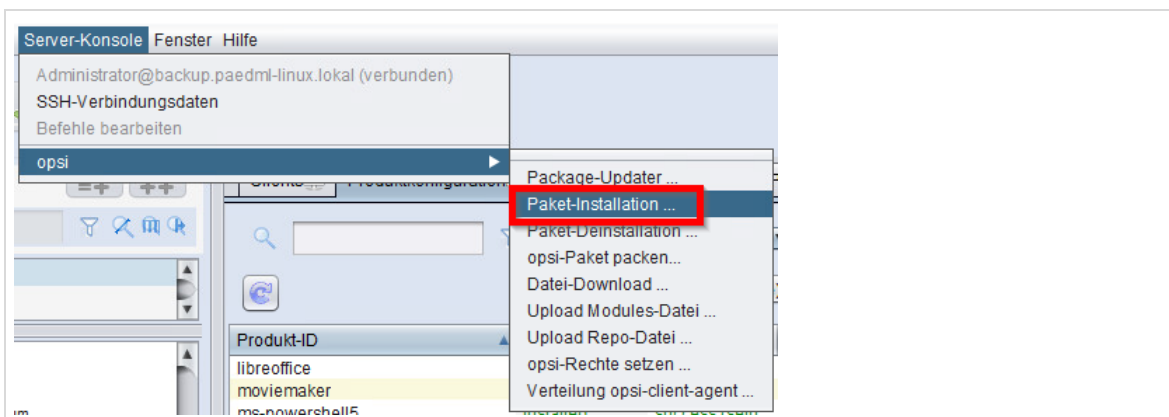


Abb. 108: Paket-Installation

Im folgenden Dialog können Sie den Pfad des zu installierenden opsi-Paketes angeben.

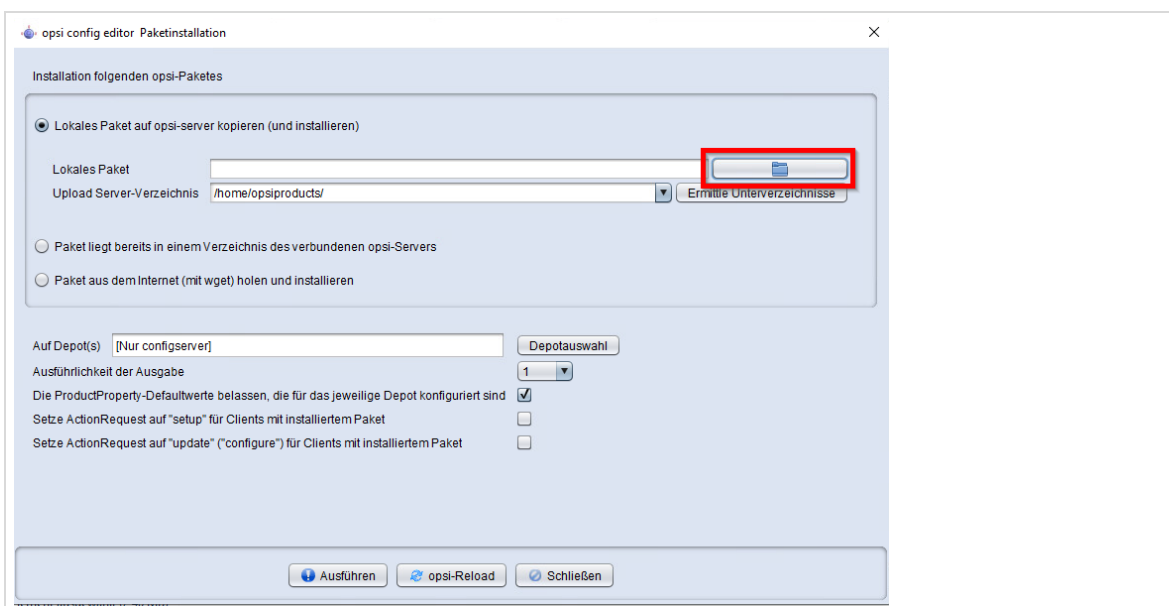


Abb. 109: Paket-Installation: Übersicht

In Unserem Beispiel soll das opsi-Paket *arduino_1.8.13-1* installiert werden. Dieses wurde zuvor als opsi-Datei heruntergeladen. Wählen Sie das Paket aus und klicken Sie auf „Übernehmen“.

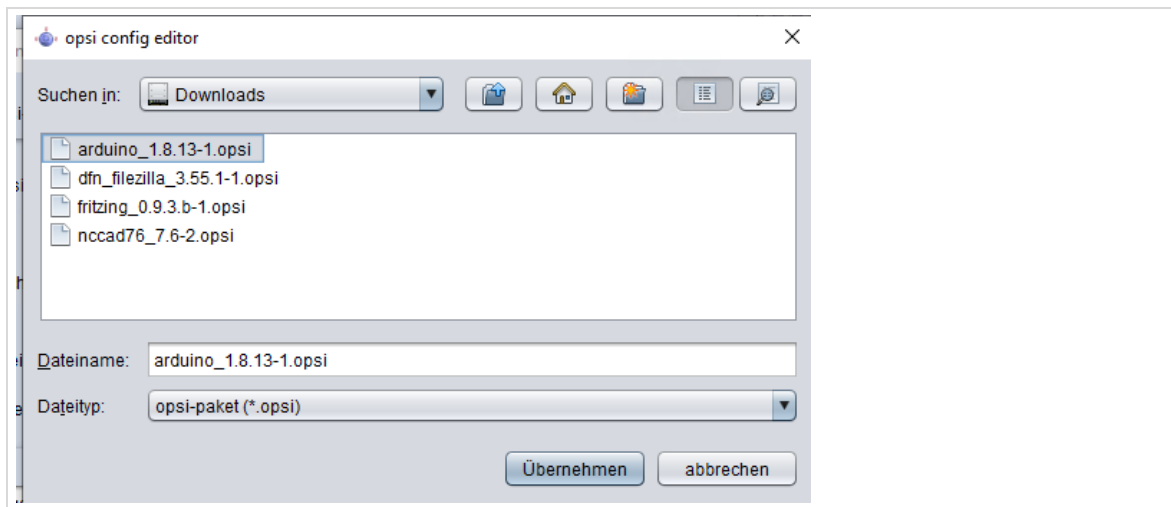


Abb. 110: Paket-Installation: Pfad zu opsi-Datei

Anschließend starten Sie die Installation mit *Ausführen*.

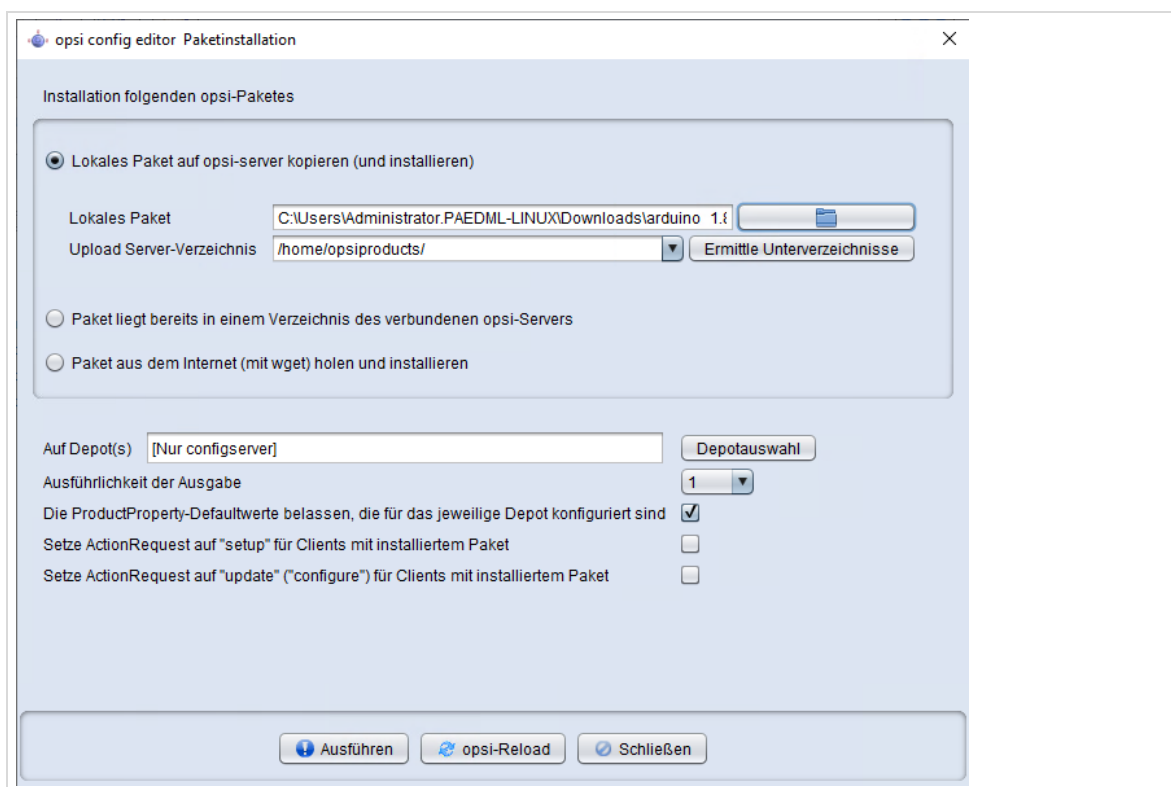


Abb. 111: Paket-Installation ausführen

Es öffnet sich ein Befehlsausgabe-Fenster. Nach beendeter Installation kann das Fenster durch einen Klick auf das blaue Symbol geschlossen werden.

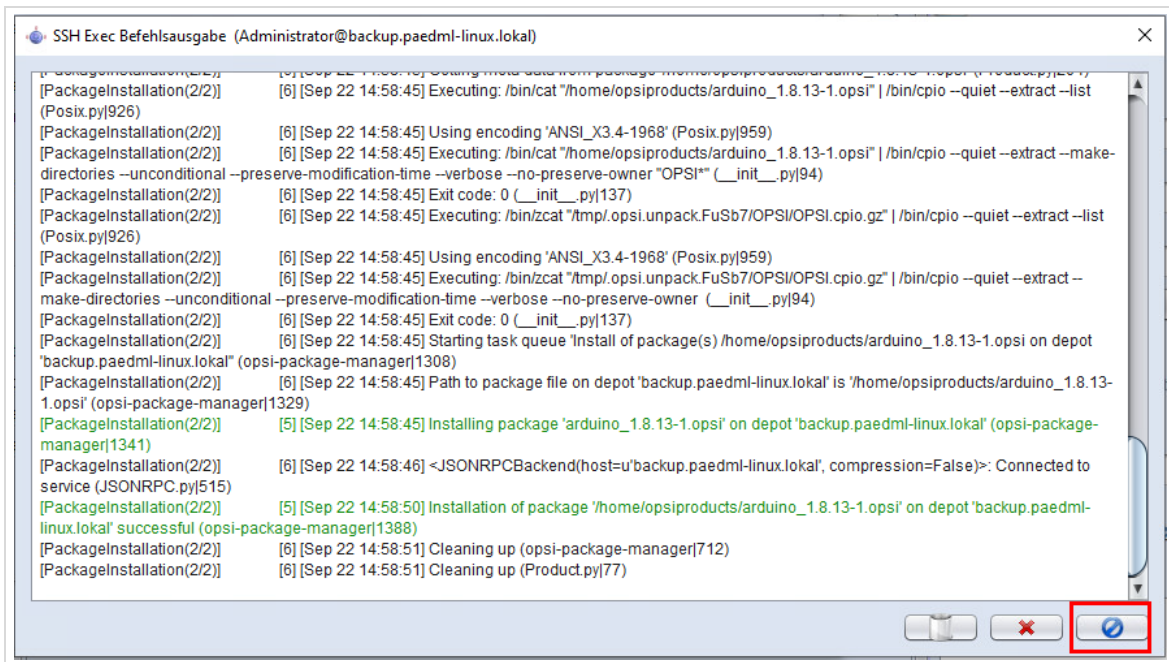


Abb. 112: Paket-Installation erfolgreich beendet

Anschließend können Sie das neu eingespielte Paket im Schulnetz verteilen. Damit das Paket im Reiter „Produktkonfiguration“ im Hauptfenster (5) angezeigt wird, muss der Datensatz von opsi neu eingelesen werden. Dies geschieht über die beiden blauen Pfeile im Schnellzugriffsmenü (2) oben links.



Abb. 113: opsi-Schnellzugriffsmenü – mit dem Symbol ganz links werden die opsi-Informationen neu geladen

6.20 Bearbeitung ganzer PC-Räume

Um ganze Rechnergruppen wiederherzustellen, müssen Sie mehrere Clients in der Clientliste markieren. Im Anschluss können Sie mit den opsi-Produkten wie oben beschrieben arbeiten. Sie können auf diesem Weg auch Software an mehrere Rechner verteilen.

Dies bedeutet, dass Sie bequem an der opsi-Konsole viele Rechner zeitgleich mit Betriebssystem und Software versorgen können. Sie können auf demselben Weg alle Rechner in die jeweilige Backuppartition sichern und wiederherstellen.

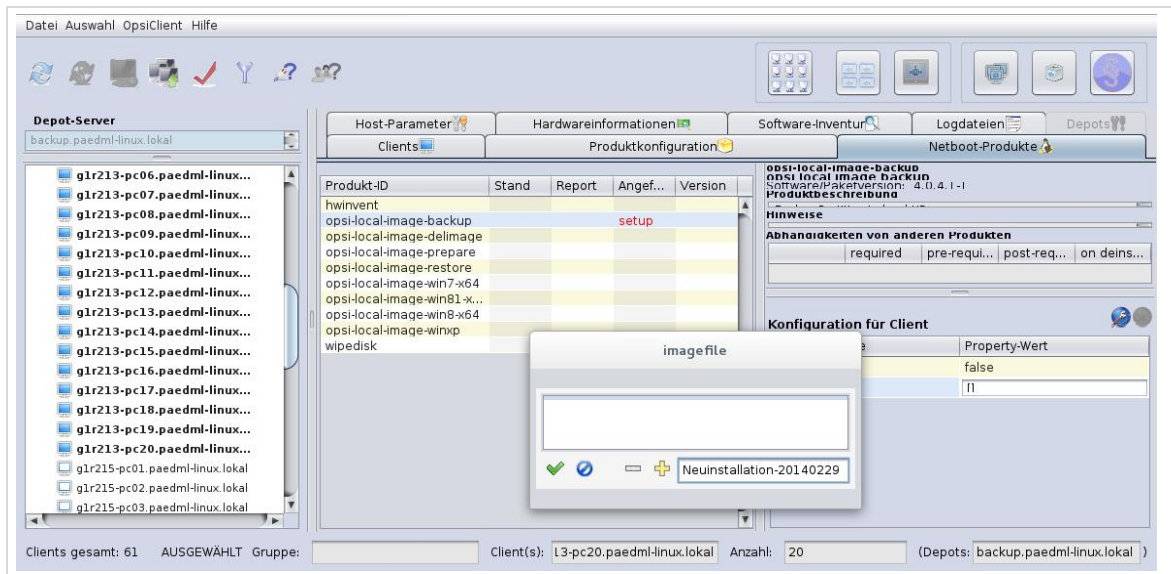


Abb. 114: Verwaltung mehrerer Rechner mit der opsi-Konsole..

Arbeiten mit Gruppen

Sie können – wie soeben beschrieben – mehrere Computer über die Client-Liste markieren oder über den Knopf „Gruppen“ in der Rechnerliste (4) auswählen. Hierbei können Sie die Auswahl auf Rechner eines Raumes oder andere beliebige Gruppen beschränken. Räume, die in der Schulkonsole definiert wurden, werden zurzeit nicht automatisch in opsi als Gruppe angezeigt. Dies wird aber in einem zukünftigen Update wieder möglich sein.

Um Gruppen in opsi benutzen zu können gehen Sie wie nachfolgend beschrieben vor:

1. Klicken Sie mit der rechten Maustaste auf „Gruppen“ (1) und dann im Kontextmenü auf „Untergruppe erzeugen“ (2)

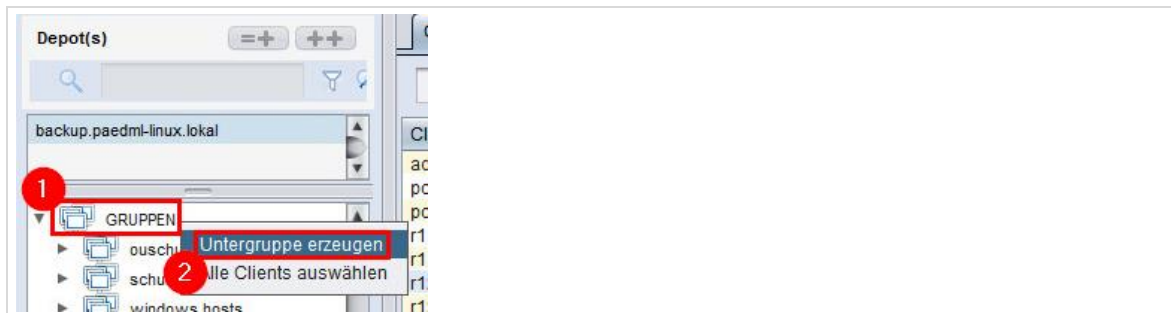


Abb. 115: Untergruppe erzeugen

2. Vergeben Sie einen aussagekräftigen Namen und eine optionale Beschreibung der Gruppe und speichern Sie die Gruppe mit einem Klick auf den roten Haken ab.

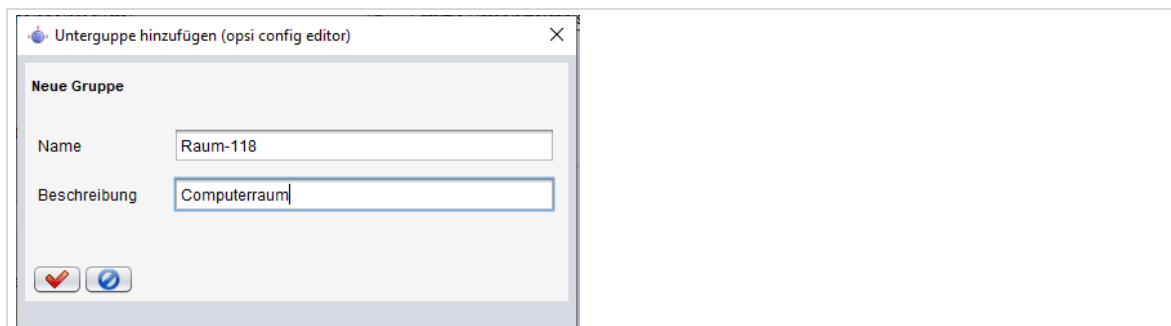


Abb. 116: Namen der Untergruppe vergeben

3. Sie können nun im Reiter „Clients“ (1) die Rechner markieren, welche der eben erstellten Gruppe angehören sollen (2). Danach können Sie mithilfe von „drag & drop“ die markierten Clients nach links (3) in die neue Gruppe (4) einfügen.

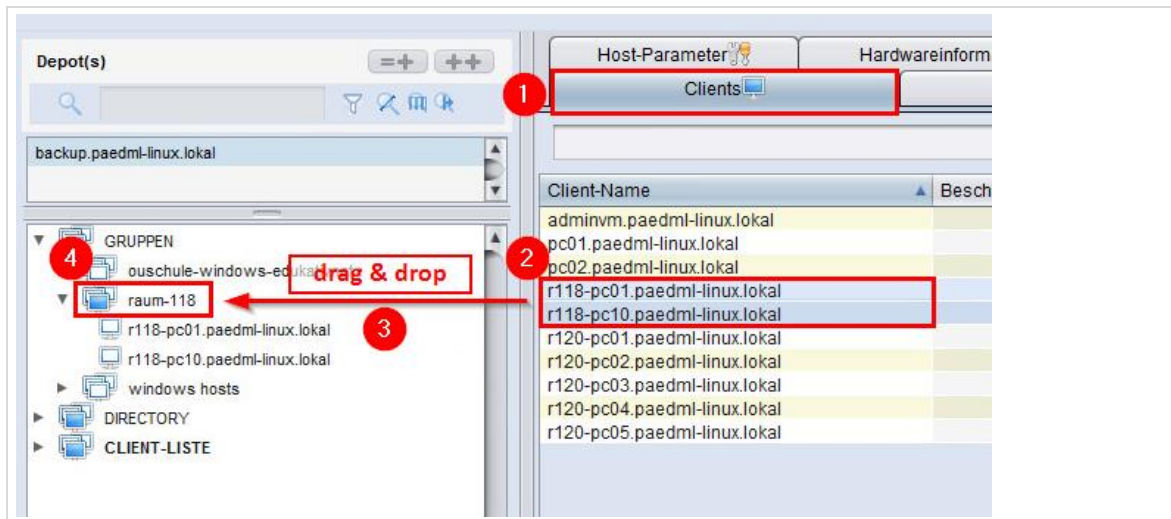


Abb. 117: Clients per „drag & drop“ in die Gruppe ziehen

4. Sie können nun mit dieser Gruppe arbeiten. Markieren Sie bitte hierfür die Kategorie „Gruppen“ und wählen Sie in der Liste (muss ggf. ausgeklappt werden) den Raum bzw. die Gruppe, die bearbeitet werden soll (im Beispiel der Raum „raum-118“).
5. Anschließend wechseln Sie im Hauptfenster (5) in den Reiter „Clients“ und markieren Sie alle Rechner, die Sie konfigurieren wollen. Sie können auch hier mit der **Strg**-Taste einzelne Clients an- bzw. abwählen oder mit der **Shift**-Taste Bereiche selektieren.
Die Rechner der Auswahl können nun über *opsi* mit Software versorgt werden.

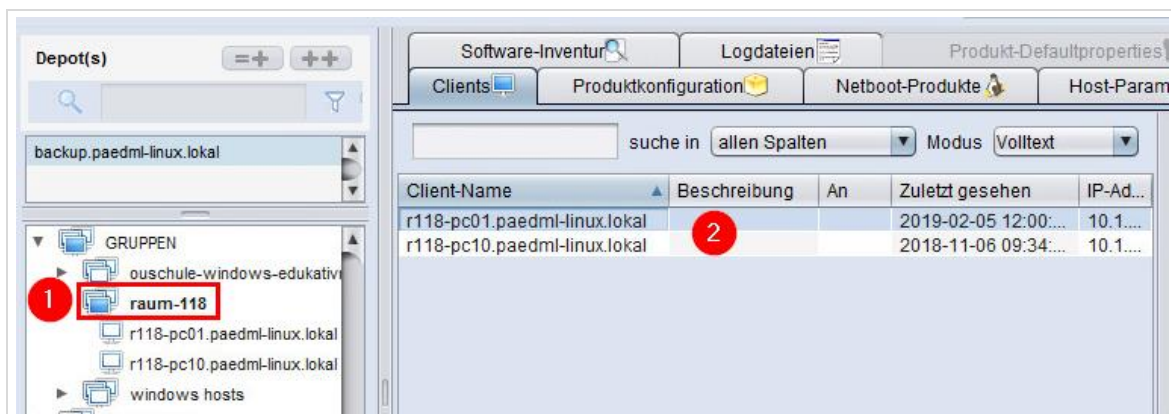


Abb. 118: Auswahl einer Rechnergruppe (entspricht Raum) (1) und darin befindlicher Clients (2)

6.21 PDF-Reports erstellen

Mit Hilfe von PDF-Dateien können Sie eine Übersicht der unter *opsi* verfügbaren „Clients“ (Geräteliste), „Produktkonfiguration“ (verfügbare opsi-Pakete), verfügbare „Netboot-Produkte“ und „Hardwareinformationen“ erstellen.

Erstellen eines PDF-Reports für „Clients“

Um eine Auswahl (oder alle Clients) als Liste im PDF-Format auszugeben, markieren Sie die Geräte im Reiter „Clients“. Klicken Sie dann im Hauptfenster mit der rechten Maustaste auf die Markierung, um das Kontextmenü zu öffnen. Dort finden Sie ganz unten die Funktion „PDF erzeugen“. Sie können nun

entscheiden, ob Sie die Datei direkt öffnen oder speichern möchten. Die erstellte PDF-Datei enthält alle Spalten des Fensterbereiches „Clients“.

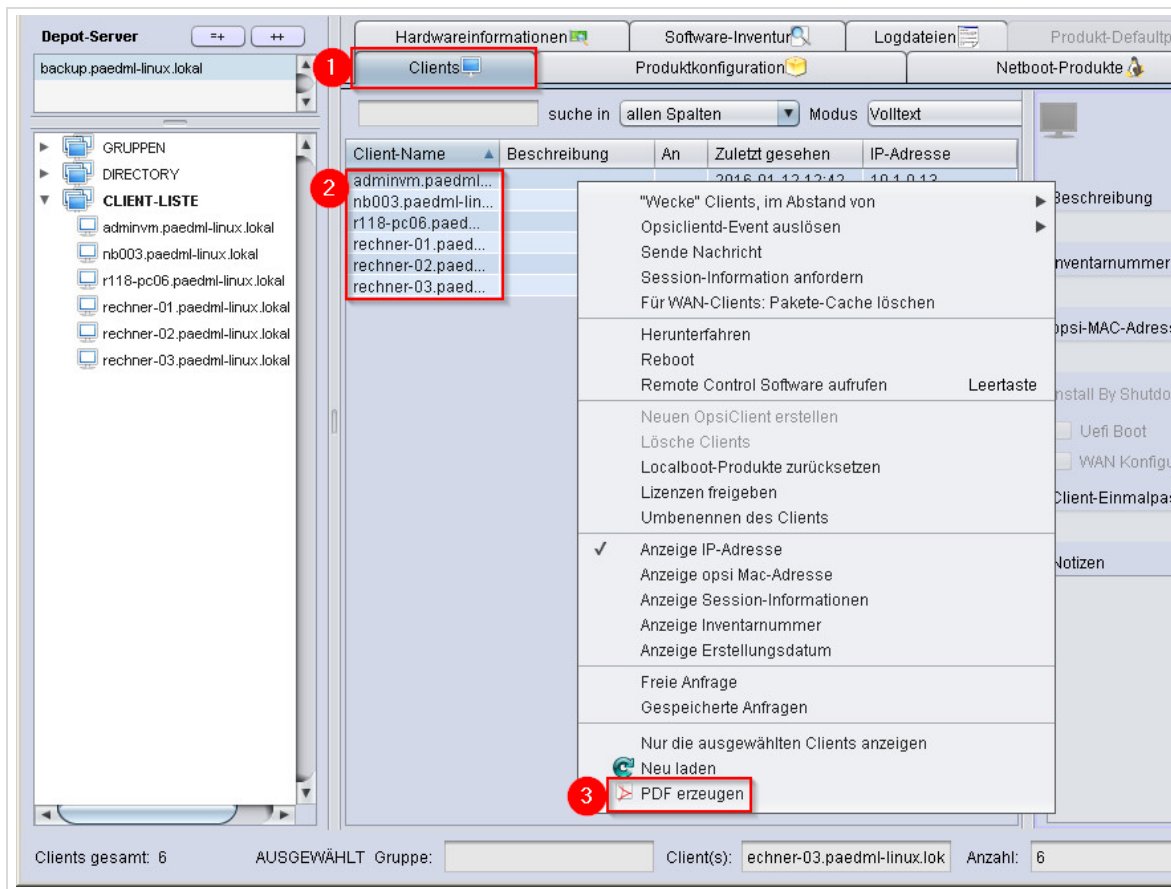


Abb. 119: PDF-Reports erstellen für „Clients“

Erstellen eines PDF-Reports für „Produktkonfiguration“ und „Netboot-Produkte“

Informationen des Reiters „Produktkonfigurationen“ können als PDF ausgegeben werden, indem Sie einen Client in der Rechnerliste (4) auswählen. Klicken Sie danach mit der rechten Maustaste auf die Liste der Produktkonfiguration im Hauptfenster (5), um das Kontextmenü zu öffnen. Dort finden Sie ganz unten die Funktion „PDF erzeugen, nur nicht leere Zeilen“. Sie können nun entscheiden, ob Sie die Datei direkt öffnen oder speichern möchten. Diese Vorgehensweise kann auch im Reiter „Netboot-Produkte“ angewendet werden.

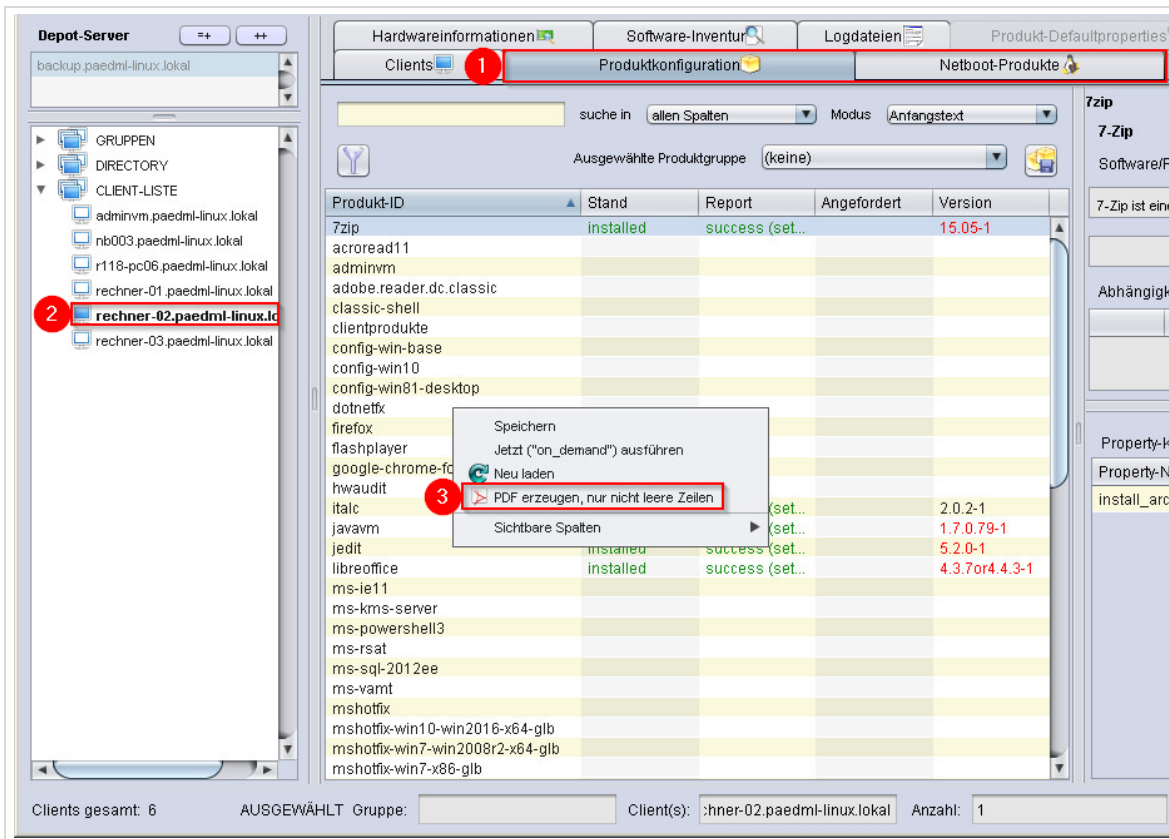


Abb. 120: PDF-Reports erstellen für „Produktkonfiguration“ und „Netboot-Produkte“

Erstellen eines PDF-Reports für „Hardwareinformationen“

Um Hardwareinformationen eines Clients als Liste im PDF-Format auszugeben, markieren Sie den gewünschten Client in der Rechnerliste (4). Klicken Sie danach mit der rechten Maustaste auf die Hardwareinformationen im Hauptfenster (5), um das Kontextmenü zu öffnen. Dort finden Sie ganz unten die Funktion „PDF erzeugen“. Auch hier können Sie dann entscheiden, ob Sie die Datei direkt öffnen oder speichern möchten.

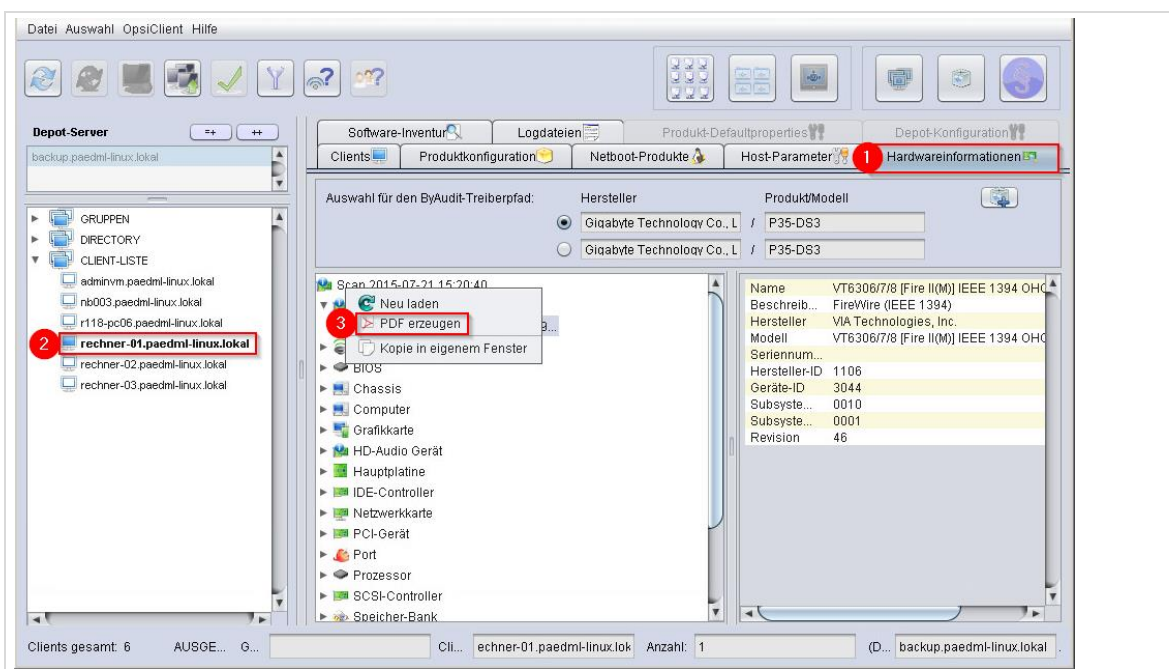


Abb. 121: PDF-Reports erstellen für „Hardwareinformationen“

6.22 Erneuerung des opsi-Lizenzschlüssel

Einmal jährlich im Februar muss der opsi-Lizenzschlüssel erneuert werden. Die Erneuerung erfolgt durch die Hilfsdatei „*opsiLizenzTausch.exe*“ auf dem opsi-Server unter `\\backup\opsi-depot-rw\update72\Skripte`.

Klicken Sie doppelt auf die Datei „*opsiLizenzTausch.exe*“.

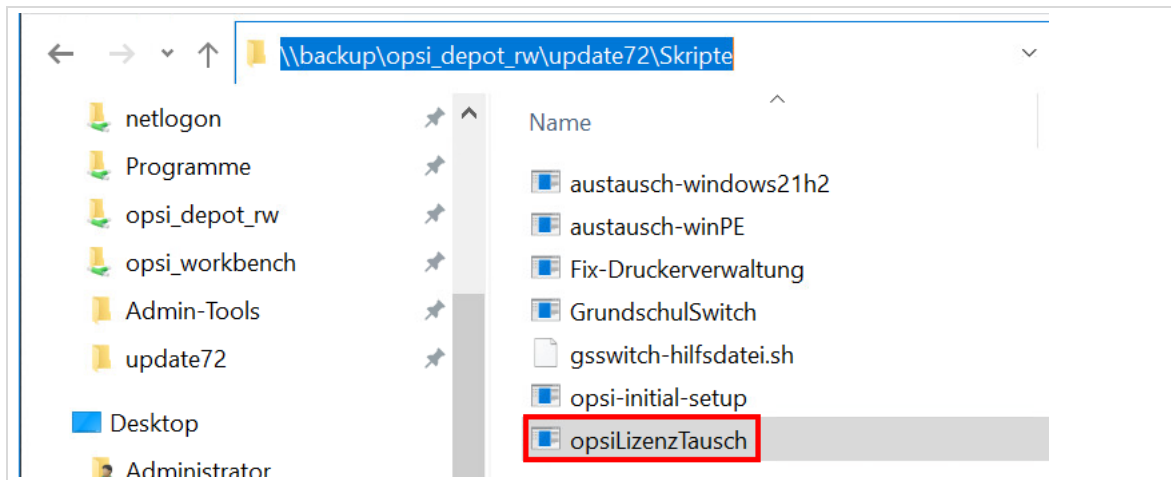


Abb. 122: *opsiLizenzTausch.exe* ausführen

Geben Sie nun das „root“-Passwort des opsi-Servers ein und folgen Sie den weiteren Anweisungen.

7 Übernahme alter Rechner in die Domäne

Es kommt immer wieder vor, dass bestehende Rechner(gruppen) ohne Anpassung am Image des Rechners in die neue Domäne übernommen werden sollen. Dies ist vor allem bei der Einrichtung eines neuen Netzwerkes der Fall.

Die Integration bestehender Rechner erfolgt in drei Schritten:

1. Rechner in die paedML aufnehmen.
2. Einspielen des opsi-client-agent
3. Rechner in die Domäne aufnehmen.



Rechner, die nicht mit opsi partitioniert wurden, können nicht mit opsi-local-image-Paketen versorgt werden. Dies bedeutet, dass (mittels opsi) keine Images erstellt und zurückgespielt werden können.

Unter opsi sind keine Informationen darüber verfügbar, welche Software auf dem Client installiert wurde. Nur Programme, die über opsi verteilt werden sind in der opsi-Maske als installiert sichtbar.

Wir empfehlen am Client das Paket „clientprodukte“ zu installieren.

7.1.1 Rechneraufnahme in die paedML

Zunächst müssen Sie den Rechner (wie in Kapitel 4 „Verwaltung von Geräten“ auf Seite 46 beschrieben) in die paedML aufnehmen. Bei der Rechneraufnahme muss der Rechnername des aufgenommenen Rechners (LDAP-Objekt) mit dem Windows-Rechnernamen übereinstimmen, ggf. muss vor der Aufnahme in die paedML der Windows-Rechnername an die Begebenheiten im Schulnetz angepasst werden.

Damit sind die Clients weder in die Domäne aufgenommen noch per opsi administrierbar. Um dies zu gewährleisten, muss zunächst der opsi-Client-Agent installiert werden. Anschließend können Sie den Client in die Domäne aufnehmen.

7.1.2 Einspielen von opsi-client-agent



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.

Achten Sie darauf, dass der Rechner denselben Namen unter Windows hat, unter dem er in die *paedML* aufgenommen wurde.

Auf dem opsi-Server („backup“) 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 einem Windows-Rechner an, öffnen Sie über den Windows-Explorer die Freigabe (Zugangsdaten des Domänenadministrators) und führen Sie das Skript aus.

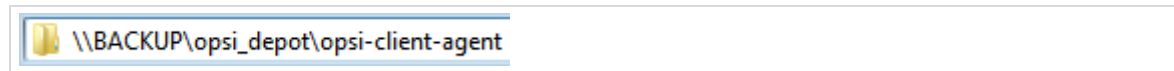


Abb. 123: Eingabe des Pfades in einen Windows-Explorer

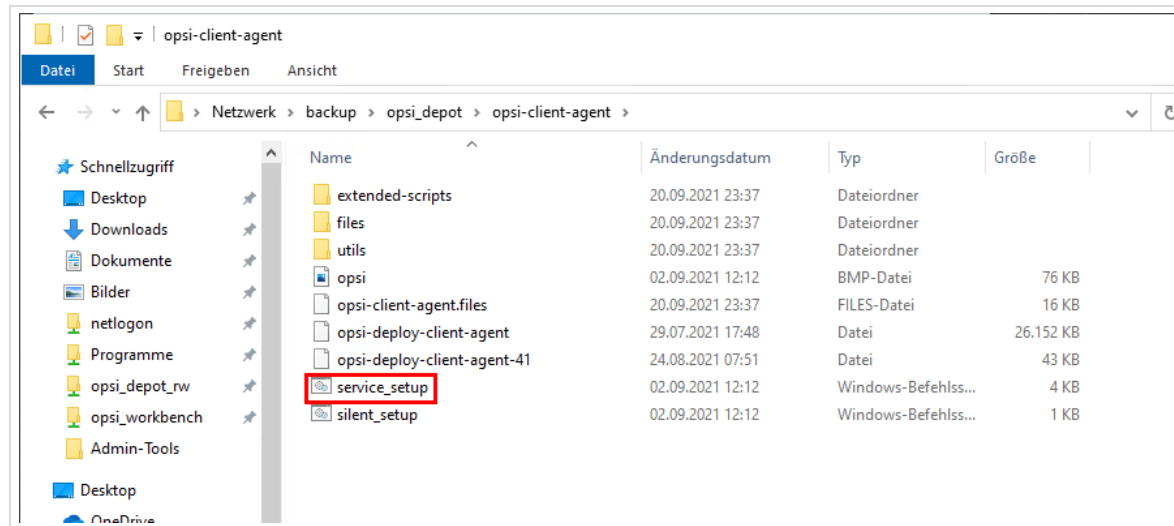


Abb. 124: Zugriff auf die Netzwerkfreigabe

Nach einem Doppelklick öffnet sich eine *Windows-Konsole*, in der Sie zur Bestätigung der Installation von „opsi-client-agent“ auf dem lokalen Rechner aufgefordert werden. Sollte der Zugriff auf [\\BACKUP\opsi-depot\opsi-client-agent](#) nicht möglich sein, können Sie versuchen die Freigabe [\\BACKUP\opsi_depot_rw\opsi-client-agent](#) zu verwenden.

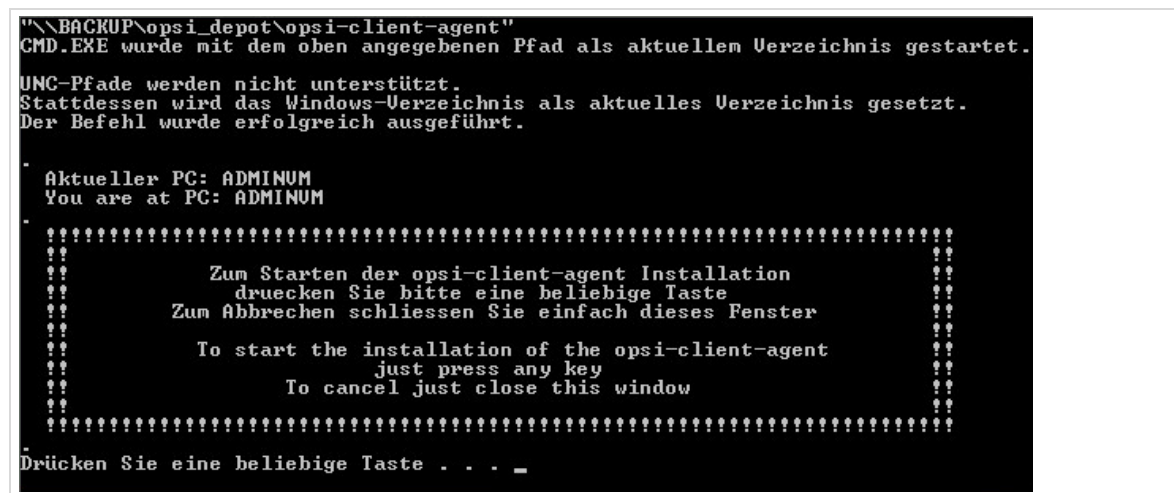


Abb. 125: Windows-Konsole vor Installation

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

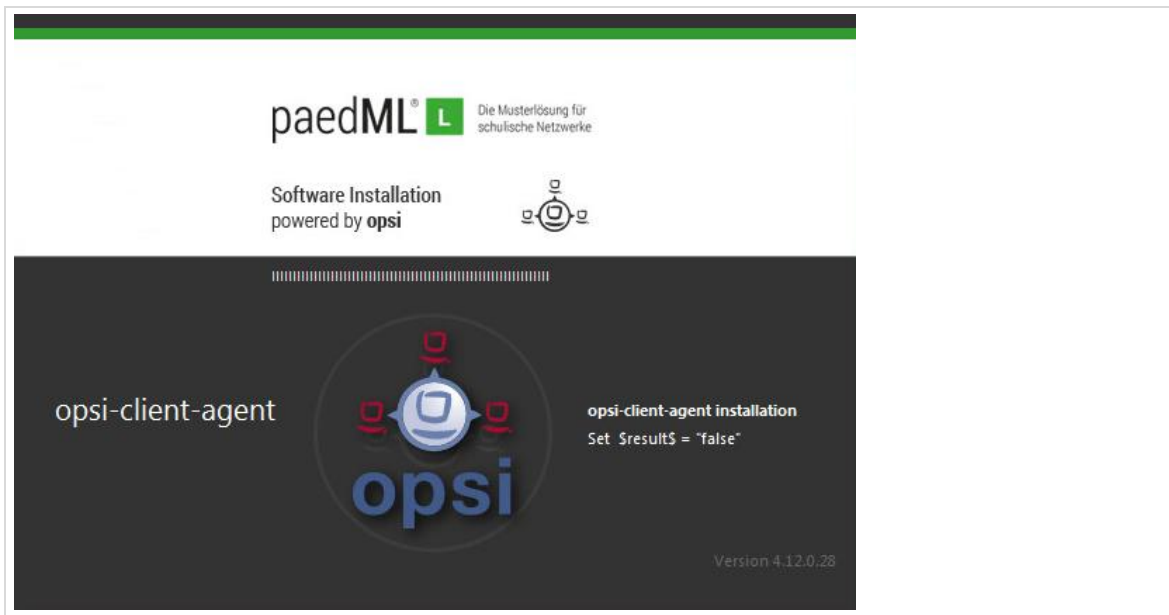


Abb. 126: Installation von opsi-client-agent

Um die Installation vollständig auszuführen, benötigt das Paket erneut die Eingabe der Zugangsdaten des Domänen-Administrators.

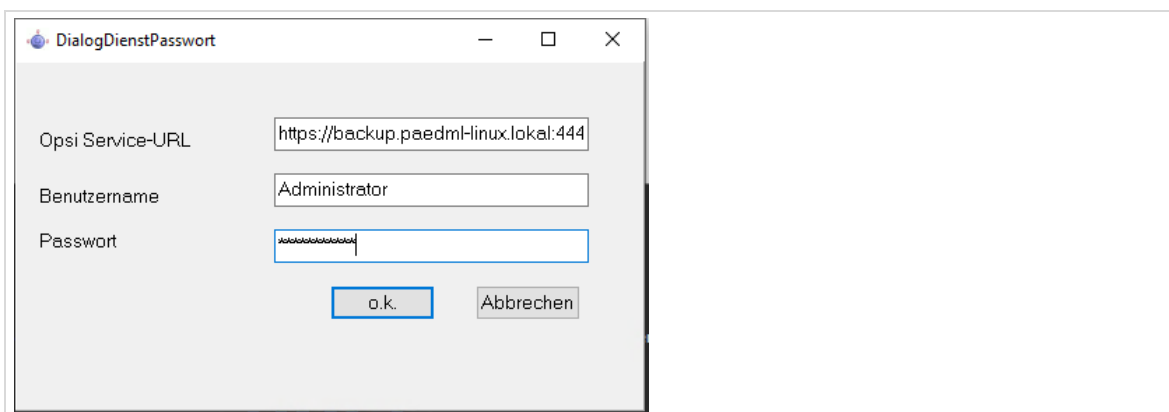


Abb. 127: Erneute Eingabe der Zugangsdaten von Domänenadministrator

7.1.3 Rechneraufnahme in die Domäne

Folgende Szenarien der Computeraufnahme in die Domäne sind möglich:

Variante 1 - Manuelle Aufnahme der Clients in die Domäne

Um einen Client manuell in die Domäne *paedml-linux.lokal* zu integrieren, müssen Sie sich als lokaler Administrator am Client anmelden.

Öffnen Sie die Systemsteuerung und dort den Menüpunkt „System“ (1). Im Abschnitt „Einstellungen für Computernamen, Domäne und Arbeitsgruppe“ finden Sie den Eintrag „Einstellungen ändern“ (2). Wenn Sie diesen Punkt ausgewählt haben, öffnet sich ein neues Fenster „Systemeigenschaften“. Klicken Sie auf „Ändern“ (3), um das nächste Dialogfenster „Ändern des Computernamens bzw. der Domäne“ aufzurufen.

Hierin überprüfen Sie, ob der Computernamen mit dem Namen des Rechners in der paedML übereinstimmt. Tragen Sie den Namen der Domäne „*paedml-linux.lokal*“ in das hierfür vorgesehene Feld ein (4).

Sie werden für den Domänenbeitritt nach einem Benutzer und einem Kennwort gefragt. Es handelt sich hierbei um den Administrator der Domäne, oder dem domadmin.

Bestätigen Sie die Eingaben jeweils mit „OK“ (5) und führen Sie im Anschluss einen Neustart aus, 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 und anschließend den Rechner neu starten, bevor Sie ihn schließlich in die Domäne „paedml-linux.lokal“ aufnehmen können.

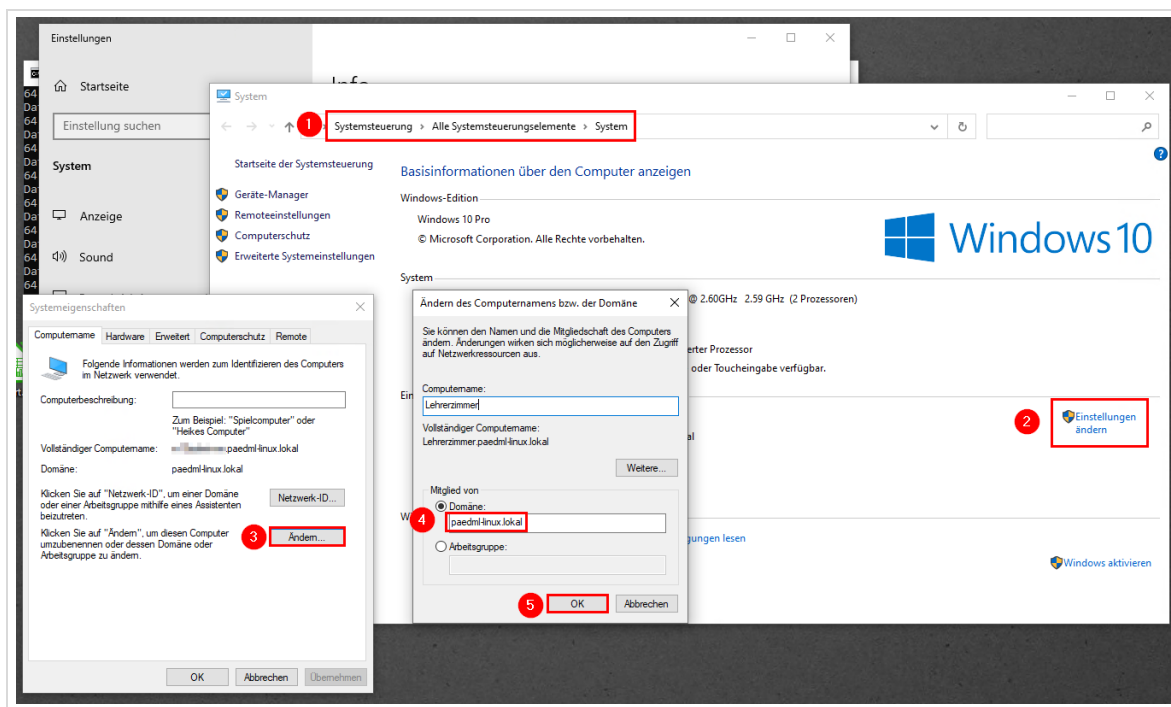


Abb. 128: Ändern der Domäne

Variante 2 - Domänenbeitritt über das opsi-Paket „windomain“

Für den neu in die paedML aufgenommen Client kann das Paket „windomain“ auf „setup“ gestellt werden. Hierdurch wird ein Domänenbeitritt angestoßen. Damit der Rechner über opsi verwaltet werden kann, muss – wie im vorigen Unterkapitel beschrieben – der opsi-client-agent auf dem Rechner vorher installiert sein.

paint-net				
putty				
rdp-zugriff				
schul-konsolen-grundschule	installed	success (setup)		1.0.0.33-1
scratch_3_desktop				
shutdownwanted				
swaudit				
teamviewer9				
thunderbird				
tonidix				
usbdm	installed	success (setup)		5.5.0-1
vic	installed	success (setup)		3.0.16-1
win10-sysprep-app-update-blocker				
windomain	installed	success (setup)	setup	# 1.0-11
windows-firewall-aus				

Property-Konfiguration	
Property-Name	Property-Wert
account_ou	
domain	PAEDML-LINUX.LOKAL
method	auto
passwd_one_time_use	false
password	*****
primarywinsserver	
samba_domain	false
secondarywinsserver	
username	domadmin@PAEDML-...

Abb. 129: Domänenbeitritt mittels opsi-Paket „windomain“



Nachdem die hier beschriebenen Schritte ausgeführt worden sind, können Sie den/ die Rechner in der opsi-Konsole aufrufen und mit Software versorgen.

8 Arbeiten mit lokalen Images von Rechnern



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 221.

Opsi ermöglicht Ihnen, lokale Images auf jedem Rechner zu speichern. Dadurch können Sie den Zustand jedes mit opsi verwalteten Rechners konservieren und bei Bedarf ohne nennenswerten Aufwand wiederherstellen.

Die Funktionen des Erstellens und Wiederherstellens eines Abbildes finden Sie in den „opsi-local-image“-Produkten. Im Zusammenhang mit lokalen Images sind die folgenden Netboot-Produkte relevant:

1. *opsi-local-image-prepare* – Dieses Modul hilft bei der Einrichtung der Festplatte bei der Erstinstallation.
2. *opsi-local-image-backup* – Hierüber wird ein Image erstellt.
3. *opsi-local-image-restore* – Mit diesem Modul kann ein Image wiederhergestellt werden.
4. *opsi-local-image-delimage* – Mit diesem Modul können alte Images gelöscht werden.

Produkt-ID	Stand	Report	Angefordert	Version
hwinvent				
opsi-local-image-backup				
opsi-local-image-delimage				
opsi-local-image-prepare				
opsi-local-image-restore				
opsi-local-image-win10-x64	installed	success		≠ 4.1.0.1-16
opsi-local-image-win10-x64-capture				
wipedisk				

Abb. 130: opsi-Produkte im Reiter „Netboot-Produkte“

Durch das Vorhalten lokaler Images ist eine schnelle Restauration von Rechnern möglich, ohne dass Daten über das Netzwerk verteilt werden müssen. Durch die Verteilung von Images wird in der Regel die Netzwerkperformanz in Mitleidenschaft gezogen, da große Datenmengen vom Server auf die Clients und zurück übertragen werden.

Das Vorhalten lokaler Images bietet die Möglichkeit, wertvolle Systemzustände, (z.B. Windows-Aktivierungen) zu erhalten, wenn die Images zurückgespielt werden.

8.1 opsi-local-image-prepare

Die Grundvoraussetzung für das Funktionieren der „opsi-local-image“-Produkte ist, dass der Rechner mit dem „Netboot-Produkt“ „opsi-local-image-prepare“ installiert wurde. Mit diesem opsi-Werkzeug wird eine Festplatte so eingerichtet, dass die Festplatte in verschiedene Bereiche partitioniert und eine Backup-Partition angelegt wird.

8.1.1 opsi-local-image-backup

Das Anlegen eines Images der Systempartition wird über dieses Modul bewerkstelligt. Ein Abbild wird in der Backuppartition abgelegt. Bei der Imageerstellung werden die folgenden Daten an- und in der Backuppartition des Rechners abgelegt:

- *master.log* – Wann wurde welches Netboot-Produkt mit welchen Optionen ausgeführt?
- *Name-des-Images* – Verzeichnis, das wie das erstellte Image heißt und dieses enthält
- *Name-des-Images/img.ini* – Informationen zum Image
- *Name-des-Images/Name-des-Images* – das Image
- *Name-des-Images/productOnClients.json* – Informationen darüber, welche opsi-Produkte auf dem Client installiert wurden (inkl. Version, Datum usw.)

opsi-local-image-backup

Sicherung der Systempartition

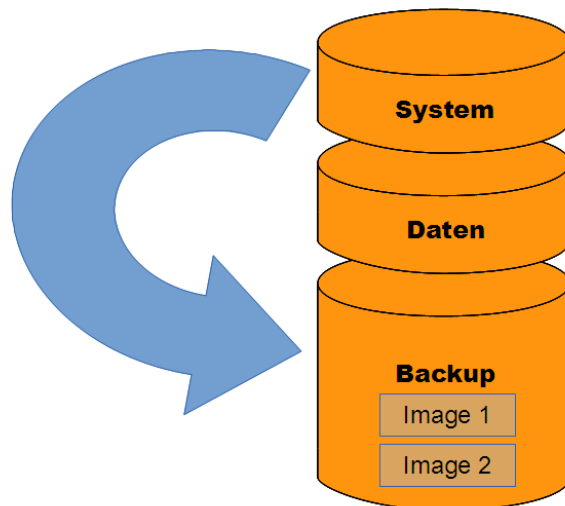


Abb. 131: Sicherung der Systempartition

Die folgenden Einstellungen können Sie für das Netbootprodukt „opsi-local-image-backup“ vornehmen:

Property-Name	Property-Wert
architecture	Belassen Sie es bitte auf dem Standardwert (64bit)
askbeforinst	Der Default-Wert (empfohlen) steht auf „false“. Wenn Sie die Wiederherstellung durch eine Benutzereingabe bestätigen wollen, ändern Sie den Wert auf „true“.
free_on_backup	Hier können Sie ablesen, wieviel freier Speicherplatz auf der Backuppartition verfügbar ist. Dieser Wert wird jedesmal aktualisiert, wenn ein Image erstellt wurde.
imagefile	Hier kann ein Name eingegeben werden.
setup_after_install	Mit diesem Parameter können Sie Aktionen nach dem Backup anstoßen. Diese Verkettung kann zum Beispiel dafür genutzt werden, dass nach der Sicherung des Rechners ein anderes Netboot-Produkt (z.B. eine andere Windows-Version) installiert wird.

Tabelle 12: Werte von opsi-local-image-backup

Beim Ausführen des Backups können Sie einen Namen für das zu erstellende Image eingeben. Sofern manuell kein Name vergeben wird, setzt das System den Namen des installierten „Netboot-Produkts“ als Imagennamen, zum Beispiel „opsi-local-image-win10-x64“.

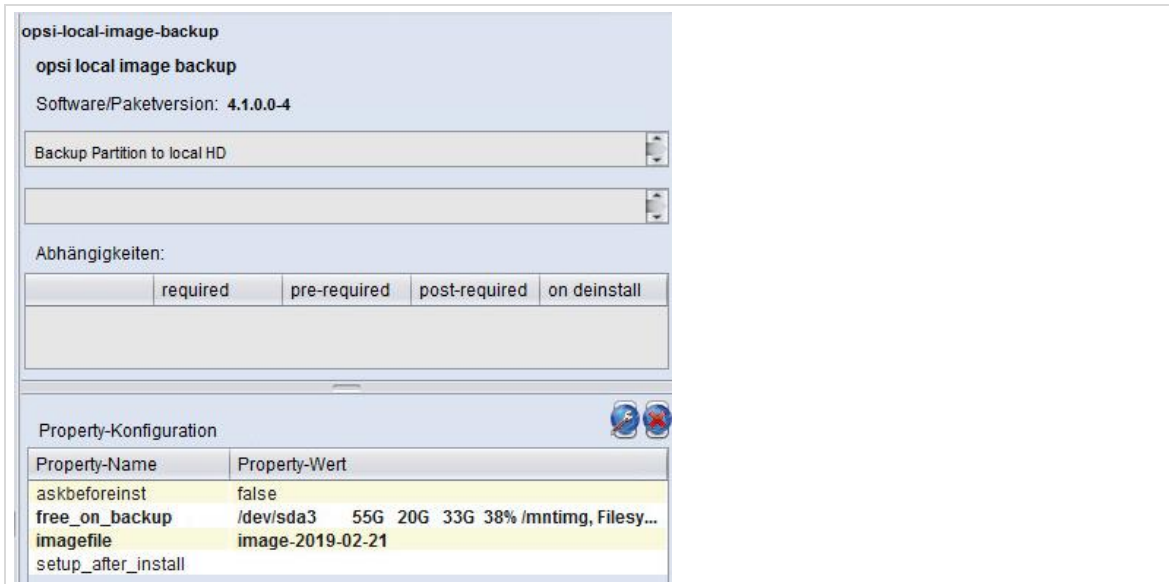


Abb. 132: Properties von „opsi-local-image-backup“ nach Erstellen eines lokalen Images

Um einen Namen einzugeben, klicken Sie auf den „Property-Wert“ von „imagefile“. In dem großen weißen Feld sehen Sie – sofern schon Abbilder der Systempartition erstellt wurden – die Namen der alten Images. Unten rechts können Sie den Namen des zu erstellenden Images eingeben. Drücken Sie auf das **PLUS**, um den Namen zu übernehmen. Er erscheint anschließend in dem großen weißen Feld. Sie müssen die Änderungen mit dem Haken übernehmen. Wenn Sie abbrechen wollen, drücken Sie auf den blauen Kreis.



Leerzeichen und Umlaute im Imagenamen führen zu Problemen und sollten daher generell vermieden werden!

Leerzeichen in opsi-Images können durch eine Unterstrich (_) ersetzt werden, Umlaute durch „ae“, „ue“ oder „oe“.

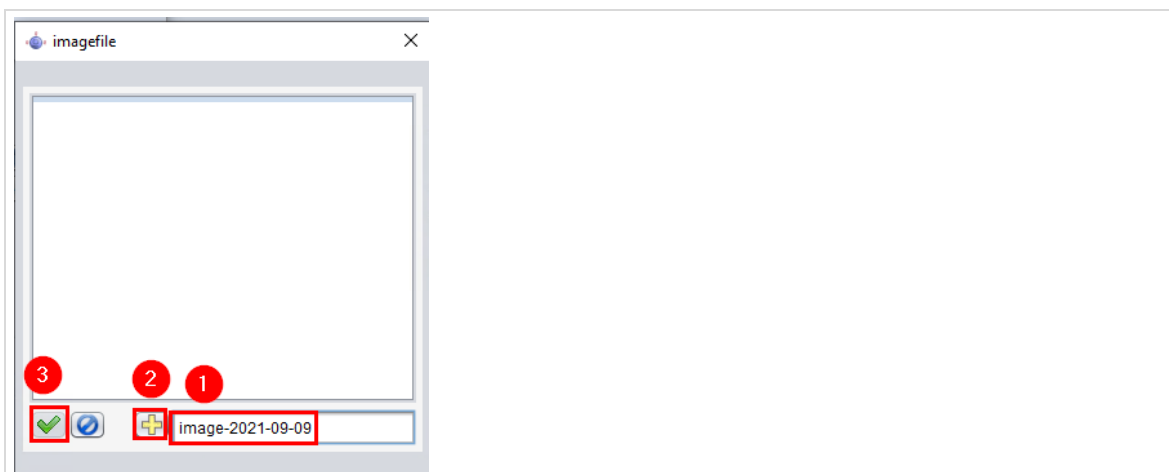


Abb. 133: Eintrag eines Imagenamens

Bitte dokumentieren Sie die Namen der erstellten Images, damit Sie später – wenn Sie mehrere Images haben – wieder darauf zugreifen können. Im Anhang ist eine Tabelle beigelegt, die Sie für die Dokumentation Ihrer Images nutzen können.



Bitte beachten Sie, dass der Imagename „case sensitive“ ist, d.h. dass zwischen Groß- und Kleinbuchstaben streng unterschieden wird und der Imagename später **genau** eingegeben werden muss.

Änderungen in der Konfiguration sind mit dem roten Haken (2) zu bestätigen.



Abb. 134: Geänderte Konfiguration bestätigen

Beim nächsten Systemstart wird das Image erstellt und in der Backup-Partition gespeichert.

Fahren Sie den Rechner vollständig herunter und starten Sie ihn anschließend neu. Ein Reboot kann dazu führen, dass das Backup nicht startet.

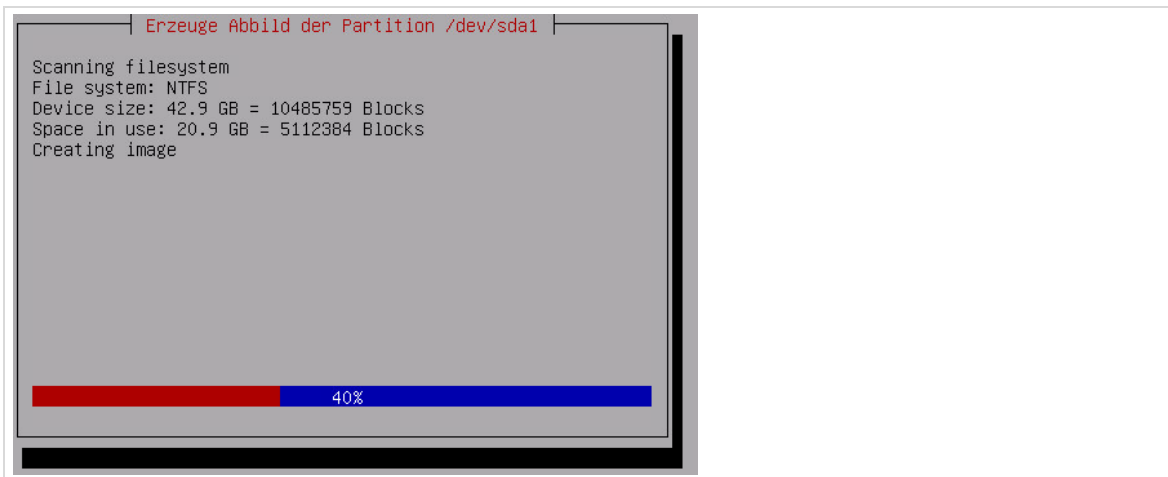


Abb. 135: Ein lokales Image wird erstellt



Wenn beim Erstellen eines Images kein Platz mehr in der Backup-Partition vorhanden ist, dann bleibt die Imageerstellung mit der Fehlermeldung „no space left on device“ stehen.

In diesem Fall müssten Sie mit *opsi-local-image-delimage* alte Abbilder löschen.

8.2 opsi-local-image-restore

Die Wiederherstellung eines Images wird mit dem Modul *opsi-local-image-restore* ausgeführt. Alle Abbilder, die zuvor in der Backup-Partition eines Rechners abgelegt wurden, können hiermit zurückgespielt werden. Sie können mehrere Images vorhalten und bei Bedarf wiederherstellen.

opsi-local-image-restore

Wiederherstellung der Systempartition

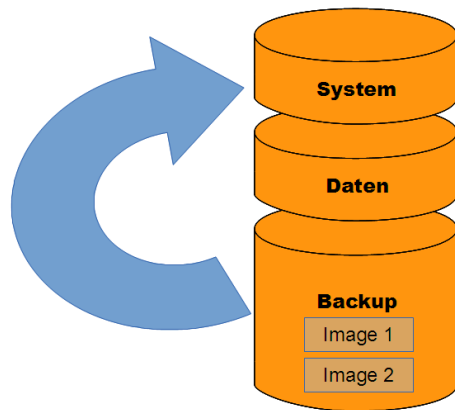


Abb. 136: Wiederherstellung der Systempartition

Die folgenden Einstellungen können Sie für das Netbootprodukt „opsi-local-image-restore“ vornehmen:

Property-Name	Property-Wert
architecture	Dieser Wert kann auf dem Default-Wert belassen werden.
askbeforinst	Der Default-Wert (empfohlen) steht auf „false“. Wenn Sie die Wiederherstellung durch eine Benutzereingabe bestätigen wollen, ändern Sie den Wert auf „true“.
imagefile	Dieser Wert bestimmt, welches Image wiederhergestellt werden soll. Hier ist immer der Wert des letzten Images eingetragen. Wenn Sie ein anderes Image wiederherstellen wollen, müssen Sie den genauen Imagennamen aus dem Feld „imagefiles_list“ in dieses Feld eintragen.
imagefiles_list	Hier sehen Sie eine Liste aller vorhandenen Images.
proxy	Dieses Feld bleibt leer.
setup_after_restore	Hier wird festgelegt, welche Produkte nach der Wiederherstellung konfiguriert bzw. ausgeführt werden sollen. Der Standard-Eintrag ist „windomain“ ³¹ .
update_and_backup	Default-Eintrag ist „false“. Wenn Sie den Wert auf „true“ stellen, überprüft opsi nach dem Wiederherstellen eines Images, ob es Softwareaktualisierungen für installierte opsi-Produkte gibt, aktualisiert diese und erstellt im Anschluss ein neues Abbild.

Tabelle 13: Werte von opsi-local-image-restore

³¹ Hierüber wird der Client erneut in die Domäne aufgenommen. Dies ist notwendig, da das Computerkontopasswort zwischen Client und Domäne regelmäßig neu verhandelt wird und der Computer das aktuelle Kennwort der Domäne unter Umständen nicht im Image hat.

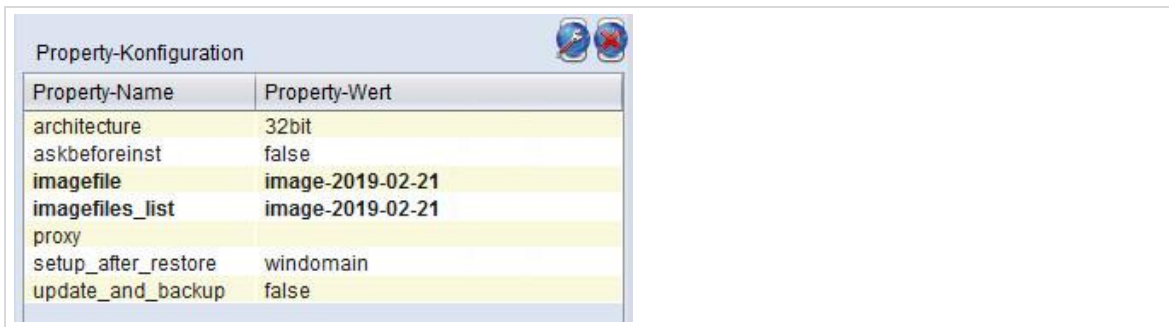


Abb. 137: Einstellungen von *opsi-local-image-restore*

Änderungen sind mit dem roten Haken zu bestätigen.

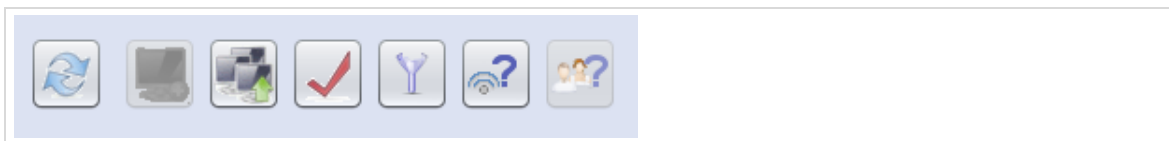


Abb. 138: Geänderte Konfiguration bestätigen

Beim nächsten Systemstart wird das Image wiederhergestellt.

8.3 opsi-local-image-delimage

Mit diesem Modul können alte Images aus der Backup-Partition gelöscht werden. Der Wert im Feld „*imagefile*“ ist nicht belegt. Dies bedeutet, dass Sie den Namen des Images wissen müssen, um das Image löschen zu können. Sie können Sich im Modul „*opsi-local-image-restore*“ die Imagennamen im Feld „*imagefiles_list*“ anzeigen lassen und dort abschreiben. Ein Doppelklick auf dieses Feld zeigt eine Liste aller Imagennamen, die in der opsi-Datenbank für den Client hinterlegt sind. Diese Werte werden nicht dynamisch aus dem Rechner ausgelesen! Wenn ein Rechner versehentlich aus opsi gelöscht und wieder angelegt wurde, sind hier keine Images hinterlegt, obwohl der Rechner gegebenenfalls lokale Images hat. Sofern der Name eines Images bekannt ist, kann es wiederhergestellt werden.

Um ein Image zu löschen, tragen Sie den Namen des Images in das Feld „*imagefile*“ ein.

Führen Sie hierfür einen Doppelklick auf das Feld aus. Anschließend können Sie den Namen des zu löschenden Images eintragen und mit dem gelben *PLUS-Symbol* übernehmen. Anschließend im Dialogfenster „*imagefile*“ den roten Haken (der Haken ist zunächst grün und wird nach dem Eintragen des Imagennamens rot) zur Bestätigung drücken.

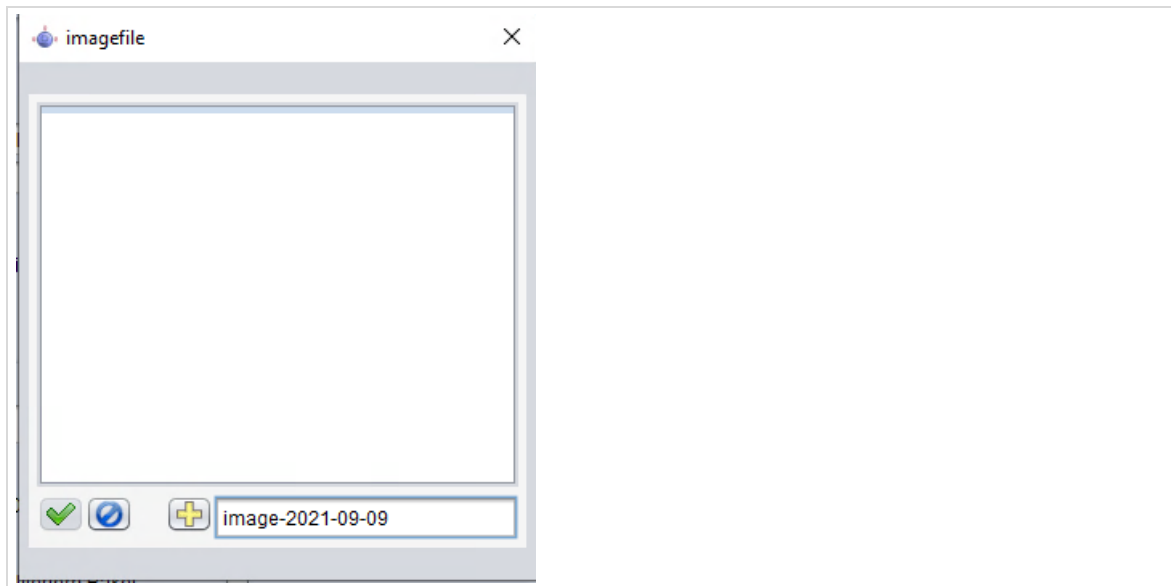


Abb. 139: Löschen eines Images aus dem Cache

Änderungen in der Konfiguration sind mit dem roten Haken (2) zu bestätigen.

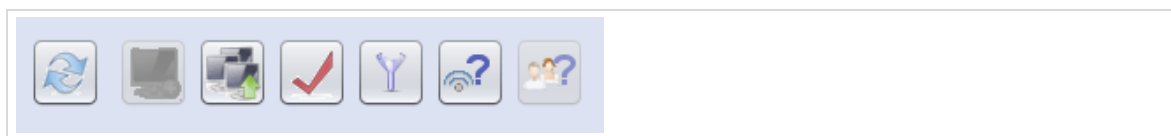


Abb. 140: Geänderte Konfiguration bestätigen

Beim nächsten Systemstart wird das Image aus der Backup-Partition gelöscht.

9 Capture-Images



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 221.

Das Software-Verteilungsverfahren mit *opsi* bietet etliche Vorteile. So können Rechner granular mit Software versorgt werden und der Lehrer-PC kann beispielsweise eine andere Software-Ausstattung als die Schüler-PCs eines Raumes erhalten. Dies geschieht ohne das Vorhalten mehrerer Images, zentral über die *opsi-Konsole*.

Für jedes *Windows*-Betriebssystem gibt es ein *opsi-Netboot-Produkt*, in dem die Installations-Dateien abgelegt werden. Installationsdateien werden als *.wim-Datei* – im *Windows-Imaging-Format*³² – auf dem *opsi-Server* abgelegt.

opsi bietet Ihnen die Möglichkeit über eine neue *.wim-Datei* Änderungen an einer Standard-Installation zu speichern (empfohlen). Hierbei werden nur die Differenzen zum bestehenden Image gespeichert. Die Images bleiben in der Summe schlank, da nicht jedes Mal ein neues Komplettimage erstellt wird, wie es etwa bei *Linbo* der Fall war.

Es ist aber auch möglich eine komplett neue *.wim-Datei* anzulegen, die die Standard-*Windows*-Installationsdatei überschreibt³³.

Wofür wird das Capture-Image benötigt?

In der Regel ist die Installation von Rechnern über die *opsi-Konsole* ausreichend, um alle Rechner im Schulnetz zu installieren. Es gibt Situationen, in denen die Softwareverteilung von *opsi* an ihre Grenzen kommt:

- Software, die installiert werden soll, liegt nicht als *opsi-Paket* vor. **In diesem Fall empfehlen wir die Verwedung von Virtuellen Maschinen als Muster-Clients. Dies hat den Vorteil, dass vor Capture-Prozessen, bzw. nach dem Installieren von Software Snapshots erstellt werden können.**
- In Ausnahmefällen: Die Installation von Treibern mit *opsi* setzt das Vorhanden-Sein einer *.inf-Datei* voraus. Leider gibt es Hardware, die mit Treibern ausgeliefert wird, die nur als ausführbare Datei (*.exe*) vorliegt. Diese Treiber müssen manuell auf den Clients installiert werden.

Hier kommt das *opsi-Capture-Image* ins Spiel, mit dessen Hilfe Sie von einem über *opsi* installierten Rechner ein Abbild, in Form eines angepassten *Windows*-Setups (*.wim-Datei*), erstellen und an andere Rechner im Netzwerk verteilen können.

³² http://de.wikipedia.org/wiki/Windows_Imaging_Format_Archive

³³ Der Parameter „*capture_mode*“ bestimmt das Verhalten des Capture-Prozesses. „*append*“ (s.u.) hängt neue Daten an das bestehende Image an, „*always_create*“ erstellt ein neues Image (möglich ab *Windows 8.1*).



1. Damit Sie mit *opsi-Capture-Image* ein Abbild erstellen und verteilen können, müssen die beteiligten Rechner mit *opsi* (*opsi-local-image-prepare*) installiert worden sein. Nur, wenn die *opsi*-Partitionierung vorliegt, kann mit *opsi* ein Capture-Image erstellt werden.

2. Die Rechner, von denen ein Abbild erstellt wird, werden mit *Sysprep*³⁴ entpersonalisiert. Hierbei werden alle Rechner-spezifischen Informationen gelöscht. Diese Geräte sollten automatisch lokal gesichert werden und nach dem Erstellen des Capture-Images sollten die Geräte aus dem lokalen Cache wiederhergestellt werden.

3. Ein Rechner, auf den das Image ausgespielt wird, muss im Anschluss erneut aktiviert werden³⁵, da es sich um eine quasi-Neuinstallation handelt.



Das hier beschriebene Verfahren hat den Vorteil, dass ein Hardware-unabhängiges Image erstellt wird. Wenn das Image auf eine andere Hardware installiert wird, installiert *opsi* - sofern hinterlegt - die hardware-spezifischen Treiber der neuen Hardware und das Image läuft auf einem anderen Gerät³⁶. Eine Ausnahme wäre natürlich die Verwendung von Capture Images zur Verteilung von Treibern (wie oben beschrieben).

9.1 Ablauf

Eine kurze Übersicht über den Ablauf der Image-Erstellung und –Verteilung:

- Der Muster-Client muss mit *opsi* installiert worden sein.
- **Der Muster-Client, von dem ein Abbild erstellt werden soll, muss komplett (Betriebssystem und Software, die nicht als *opsi*-Paket vorhanden ist) installiert werden. Direkt im Anschluss an die Installation muss das *opsi*-Paket *win10-sysprep-app-update-blocker* installiert werden.**
- Bevor ein *Capture-Image* erstellt wird, überprüft *opsi*, ob es bereits ein lokales Image (*local-image*) gibt. Sofern es kein lokales Image gibt und auch keines erstellt werden soll (Voreinstellung), bricht *opsi* den Vorgang ab.
Achtung: *opsi* überprüft hierbei nur, ob es ein Image gibt. Dieses Image muss nicht dem aktuellen Softwarestand des Clients entsprechen!
- (optional:) Vor der Imageerstellung wird ein neues Image erstellt (empfohlen).
- Im nächsten Schritt wird der Rechner mit Hilfe von *Sysprep* entpersonalisiert. Hierbei werden beispielsweise hardware-spezifische Informationen (u.a. auch Hardwaretreiber) und Lizenzinformationen gelöscht.
- Ein neues, entpersonalisiertes Abbild wird erstellt und die Image-Dateien werden auf den Server geladen.

³⁴ <http://de.wikipedia.org/wiki/Sysprep>

³⁵ Dies geschieht automatisch, wenn die Aktivierung von Windows/Microsoft Office, wie in Kapitel 0 beschrieben, eingerichtet ist.

³⁶ Je nach Hardware-Ausstattung müssen ggf. Treiber installiert werden.

- Nach der Erstellung des *Capture-Images* wird das letzte funktionierende Image des Muster-Clients wiederhergestellt (Auslieferungszustand).
- Das neu erstellte *Capture-Image* kann auf beliebige Rechner im Netzwerk ausgespielt werden.

9.2 Erstellen von Capture-Images



Die Erstellung des Capture-Images mit „*opsi-local-image-wim-capture*“ schlägt fehl, wenn Sie den Muster-Client mit einer Datenpartition angelegt haben. Installieren Sie in diesem Fall den Muster-Client neu mit dem „*opsi-local-image-prepare*“-Property *data_partition_size=0*.



Verwenden Sie bitte immer den gleichen Muster-Client für das Erstellen von Capture-Images. Wenn Sie unterschiedliche Muster-Clients verwenden, wird der Aktivierungszähler von Windows bei jedem Capture-Vorgang um eins hochgesetzt. Da der Aktivierungszähler nur dreimal zurückgesetzt werden kann, besteht die Gefahr, dieses Limit zu überschreiten und Windows dann nicht mehr aktiviert werden kann.³⁷



Es wird dringend empfohlen, dass Sie für das Erstellen von Capture-Images die gesonderten Capture-Produkte verwenden. Bei Capture-Images, die z.B. auf Windows 10 basieren, ist es das Produkt „*opsi-local-image-win10-x64-capture*“. Die Original-Windows-Installationen (z.B. „*opsi-local-image-win10-x64*“) bleiben dadurch unangetastet.

Wenn Sie Capture-Images verwenden, müssen die Zielprodukte – genauso wie „normale“ Windowsinstallationen – mit Windows-Installationsdateien versorgt werden.

Um ein Image vom Muster-Client zu erstellen, öffnen Sie die *opsi-Konsole*³⁸ und wählen Sie in der Rechnerübersicht (4) den Rechner, dessen Abbild Sie erstellen möchten.

Im Reiter „*Produktkonfiguration*“ des Hauptfensters (5) wählen Sie das Produkt „*opsi-local-image-wim-capture*“ aus und stellen dieses auf *setup*, und konfigurieren Sie die Produkt-Werte (siehe Tabelle 22).

³⁷ <https://technet.microsoft.com/de-de/library/cc766514%28v=ws.10%29.aspx>

³⁸ Die Ziffern in Klammern beziehen sich auf die Grafik aus Kapitel 1, ab Seite 128, in der die *opsi-Konsole* beschrieben wird. Sie finden die Grafik auch im Anhang.

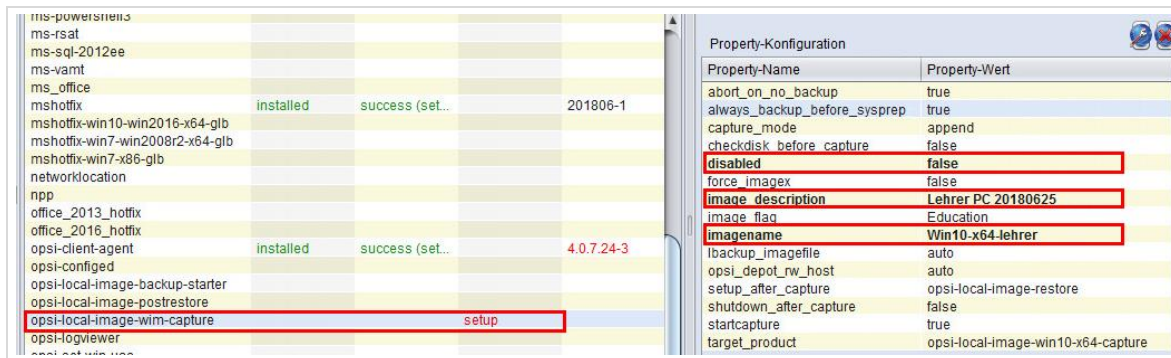


Abb. 141: Auswahl von *opsi-local-image-wim-capture*

Die folgenden *Produkt-Werte* können gesetzt werden.

Property-Name	Property-Wert
abort_on_no_backup	Steht dieser Wert auf „true“ so überprüft opsi, ob es ein lokales Image gibt, das benötigt wird, um den Rechner wiederherzustellen, nachdem die Installation mit Sysprep unbrauchbar gemacht wurde. Existiert kein solches Image, bricht der Vorgang ab. Dieser Wert MUSS auf „true“ belassen werden, andernfalls muss der Rechner nach dem Capture-Vorgang neu installiert werden.
always_backup_before_sysprep	Der Wert „true“ (empfohlen) bewirkt, dass ein neues lokales Image mit „opsi-local-image-backup“ erstellt wird, bevor mit Sysprep ein neues Abbild erstellt wird. Dieser Wert kann geändert werden.
capture_mode	Belassen Sie die Standard-Einstellung („append“), um die Differenz zu einem bestehenden Image hinzuzufügen (empfohlen). Sie haben die Möglichkeit ein neues Image zu erstellen („always_create“). Hierdurch wird die Original-Installationsdatei von Windows auf dem opsi-Server überschrieben. Dieser Modus ist erst ab Windows 8.1 möglich.
checkdisk_before_capture	Ist dieser Wert auf „true“ gesetzt, wird das Dateisystem des Clients überprüft, bevor das Capture Image erstellt wird. Standardmäßig ist der Wert auf „false“ eingestellt (empfohlen).
disabled	Dieses Feld deaktiviert sysprep, wenn der Wert „true“ eingetragen wird. Beim Muster-Client muss der Wert „true“ eingestellt sein, an den Clients immer „false“.
force_imagex	Als Standard (default=false), wird <i>dism</i> zur Erstellung des Capture-Images verwendet, wenn verfügbar. <i>Dism</i> ist schneller als <i>imagex</i> . Wenn das Property <i>force_imagex</i> den Wert „true“ hat, dann wird das <i>imagex</i> Programm des Produktes opsi-local-image-wim-capture zum Erstellen des Capture-Images verwendet, auch wenn Windows PE über das Programm <i>dism</i> verfügt.

image_description	Geben Sie hier eine aussagekräftige Beschreibung ein, um das Image später wieder zu erkennen. (z.B. Standard-Installation_ mit_Lehrer-Tools).
image_flag	Hier muss die eingesetzte Windows-Edition angegeben werden.
imagename	<p>Geben Sie hier einen aussagekräftigen Namen für das Image ein (z.B. Win10-x64-lehrer). Dieser Name wird später beim Zurückspielen des Images angezeigt.</p> <p>Leerzeichen und Sonderzeichen im Imagenamen führen zu Problemen und sollten daher generell vermieden werden!</p>
ibackup_imagefile	Der Name des lokalen Images muss auf „auto“ belassen werden.
opsi_depot_rw_host	Dieses Feld ist in der <i>paedML</i> nicht relevant, und sollte unangetastet bleiben.
setup_after_capture	<p>Hier wird ein Netboot-Produkt angegeben, das nach der Imageerstellung ausgeführt wird. Es wird empfohlen, den Standard-Wert („opsi-local-image-restore“) beizubehalten.</p> <p>„opsi-local-image-restore“ löst eine Wiederherstellung des Muster-Clients aus, der nach dem Ausführen von Sysprep unbrauchbar ist.</p>
shutdown_after_capture	<p>Herunterfahren des Rechners nach dem Capture-Vorgang.</p> <p>„setup_after_capture“ wird ignoriert, Defaultwert: „false“</p>
startcapture	<p>Dieser Wert ist der Auslöser für das Ausführen des Netboot-Produktes „opsi-local-image-wim-capture“, über das das Abbild des Rechners erzeugt wird. „True“ bewirkt das Erstellen des Capture-Images nach „Sysprep“, „false“ das Herunterfahren nach „Sysprep“. Der Wert muss auf „true“ belassen werden.</p>
target_product	<p>Geben Sie hier an, welchem zugrundeliegenden Betriebssystem das Image zugewiesen werden soll. Der Standardwert ist „opsi-local-image-win7-x64-capture“.</p> <p>Wenn Sie z.B. ein neues Image einer Windows 10 Installation erstellen, dann tragen Sie hier das Netbootprodukt opsi-local-image-win10-x64-capture ein.</p> <p>Bei Schreibfehlern wird kein Image erstellt.</p>

Tabelle 14: Konfigurationsparameter von opsi-local-image-wim-capture

Sobald Sie den Muster-Client neu starten, laufen die hier beschriebenen Prozesse ab und es wird ein Abbild erstellt, das auf den Server geladen wird. Der folgende Screenshot zeigt den Vorgang des Erstellens eines Capture-Images. Der Capture-Image-Vorgang dauert einige Zeit, in der nicht am Muster-Client gearbeitet werden kann. Der Muster-Client darf außerdem nicht ausgeschaltet werden.

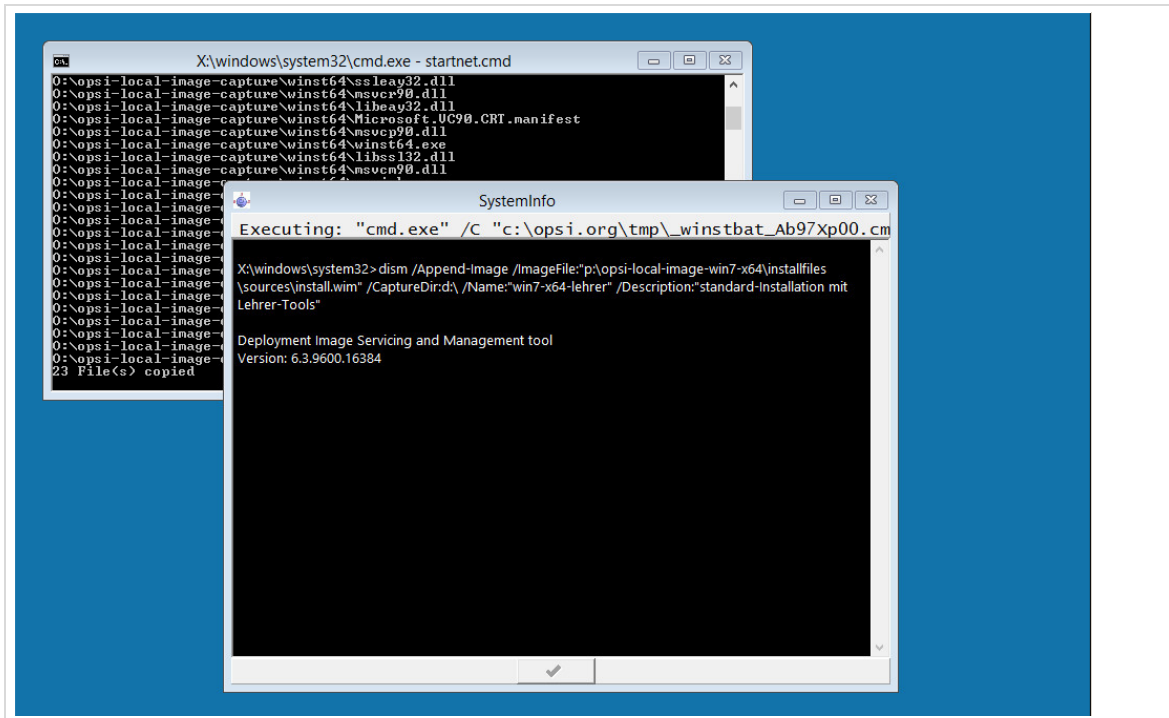


Abb. 142: Erstellen des Abbilds

9.3 Einspielen eines Capture-Images

Bitte beachten Sie, dass Capture-Images wie im Anhang B beschrieben, ebenfalls mit Windows-Installationsdateien versorgt werden müssen.



Die Windows 10-Version des Muster-Clients muss mit der Windows 10-Version der Windows-Installationsdateien übereinstimmen.

Das Einspielen eines Capture-Images entspricht einer Neuinstallation des Rechners, wobei der Rechner nicht mit dem Standard-Image (bzw. mit einer Standard-Windows-Installation), sondern mit einem durch Sie angepassten Capture-Image installiert wird.

Um einen Rechner mit dem neu erstellten Capture-Image zu installieren, wählen Sie den Rechner in der Rechner-Übersicht (4) aus und navigieren Sie im Hauptfenster (5) auf den Reiter „Netboot-Produkte“.

Stellen Sie das Produkt „opsi-local-image-prepare“ auf „setup“. Wählen Sie im Feld „Property-Konfiguration“ und dort in der Spalte „Property Name“ „start_os_installation“ das Netboot-Produkt, das Sie im vorherigen Abschnitt unter „target_product“ für das Speichern des Capture-Images gewählt haben.

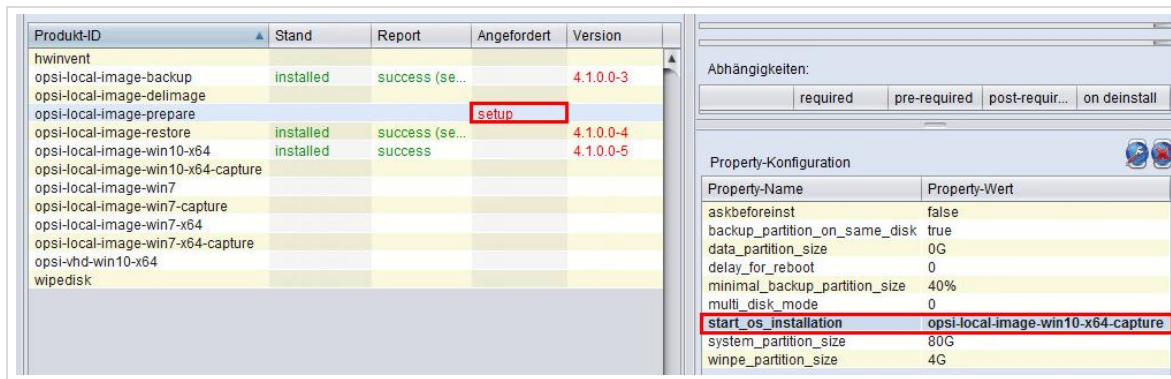


Abb. 143: Auswahl des Netboot-Produkts, das vorher als „target_product“ definiert wurde

Wählen Sie anschließend das „Netboot-Produkt“ („target_product“), dem Sie das Capture-Image zugewiesen haben, aus. Im hier beschriebenen Beispiel wurde das Capture-Image „Win10-x64-lehrer“ dem Netboot-Produkt „opsi-local-image-win10-x64-capture“ zugewiesen.

Überprüfen Sie die Werte im Feld „Property-Konfiguration“. Der Property-Name „imagename“ muss nun so angepasst werden, dass nicht die Standard-Windows-Installation, sondern das Capture-Image installiert wird. In diesem Beispiel das Image mit dem Namen „Win10-x64-lehrer“.

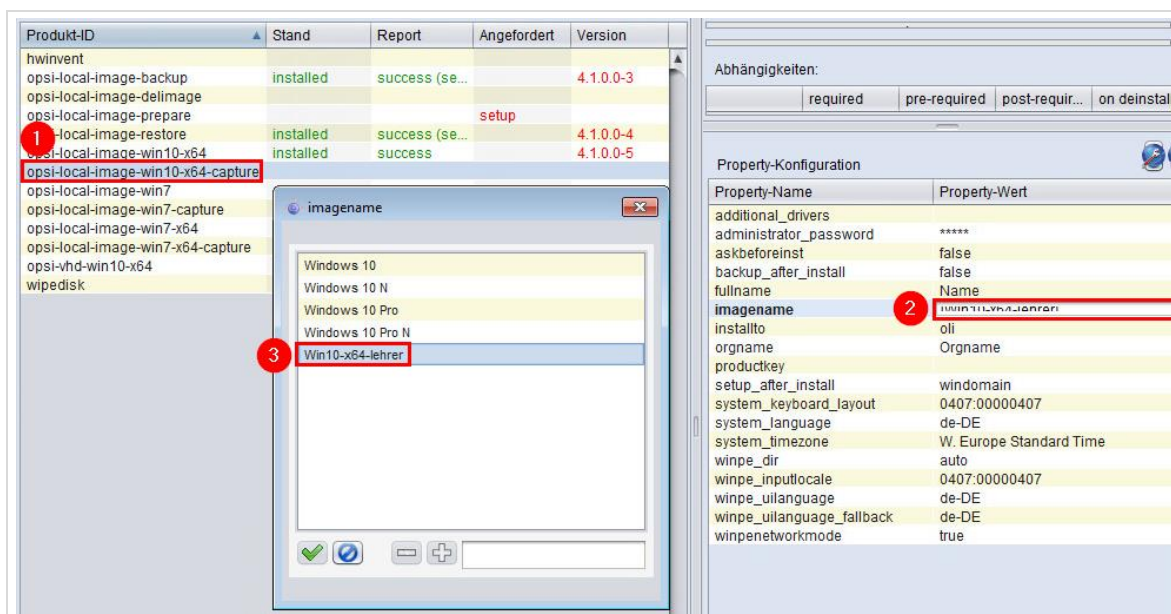


Abb. 144: Auswahl des Capture-Images

Wenn diese Einstellungen getätigt wurden, müssen Sie die Konfiguration abschließend speichern (roter Haken).

Beim nächsten Start über das Netzwerk des Clients wird dieser mit dem Capture-Image installiert.

10 Gruppenrichtlinien für Windows-Clients



Die Konfiguration von Gruppenrichtlinien ist komplex und benötigt Einarbeitung. Wenn Sie nicht wissen, wie die Konfiguration von Gruppenrichtlinien vorgenommen wird, steht Ihnen die Hotline beratend bei der Konfiguration der Gruppenrichtlinien zur Seite.

Wir empfehlen dringend, nur dann eigenständig in das System einzugreifen, wenn Sie wissen, was Ihre Änderungen bewirken.

Außerdem ist es ratsam, Änderungen zu dokumentieren, um im Fehlerfall die Suche zu vereinfachen.

Unter <https://technet.microsoft.com/de-de/library/hh147307> können Sie eine Anleitung für Anfänger abrufen.

10.1 Gruppenrichtlinien in der paedML Linux

Durch Gruppenrichtlinien kann zentral eingestellt werden, wie die Arbeitsplätze der Anwender konfiguriert werden. Hierdurch können Benutzer-Gruppen mit Programmen versorgt oder Drucker an Rechner zugewiesen werden. Sie können Rechte für das Ausführen von Funktionen beschränken oder für bestimmte Benutzer erweitern.

Die *paedML Linux* wird mit vordefinierten Windowsgruppenrichtlinien ausgeliefert, die bei der Installation von Windows-Clients auf den Arbeitsplatzrechnern eingerichtet werden.

Anmerkung: mit Hilfe der Gruppenrichtlinien werden beim Start von Windows-Sitzungen Skripte aufgerufen, die ihrerseits Anpassungen an den Einstellungen von Windows vornehmen und die Rechner für den Einsatz in der Schule konfigurieren.

Diese Skripte liegen in der Netzwerkfreigabe <\\server\netlogon\ScriptsML>. Dort gibt es den Ordner „StartUp“, der Skripte enthält, die beim Hochfahren des Rechners abgearbeitet werden und den Ordner „Login“, dessen Skripte bei der Anmeldung eines Benutzers ausgeführt werden.

10.1.1 Aufruf der Gruppenrichtlinienverwaltung

Für das Bearbeiten von Gruppenrichtlinien wird das Gruppenrichtlinienverwaltungs-Programm (*group policy management console*) von *Microsoft* verwendet.

Um Änderungen an den Gruppenrichtlinien vorzunehmen; Melden Sie sich als **Administrator der Domäne** an der W10AdminVM an.



Abb. 145: Anmelden als Administrator der Domäne

Sie erreichen das Programm Gruppenrichtlinienverwaltung über den Ordner Admin-Tools auf dem Desktop.

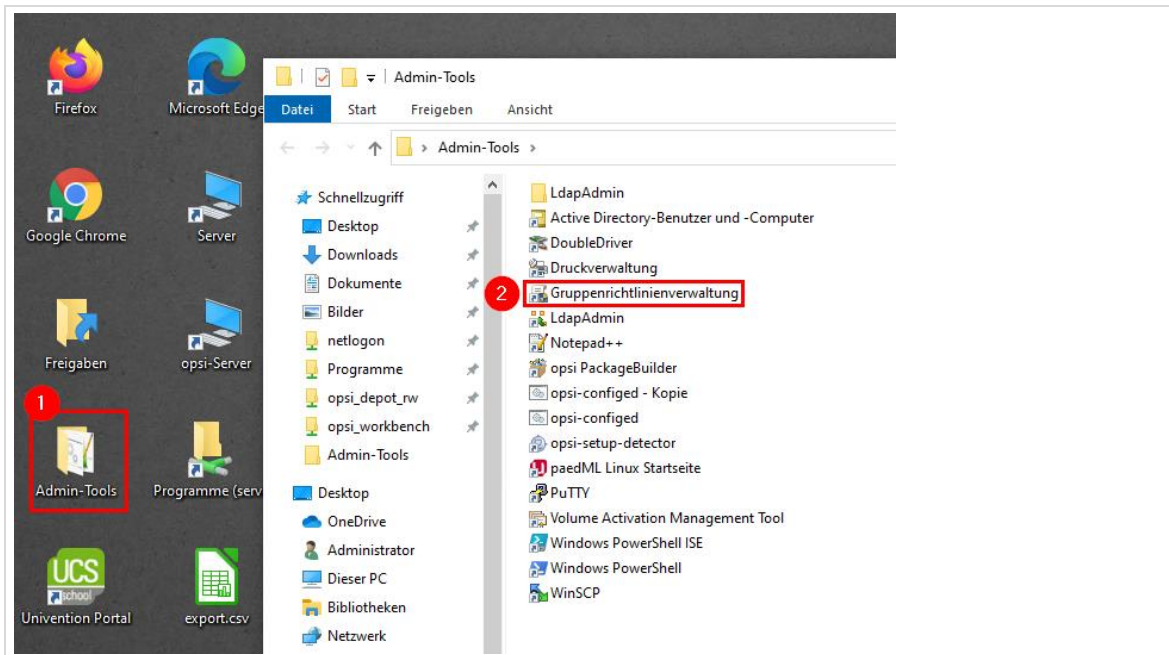


Abb. 146: Ein möglicher Weg den Gruppenrichtlinieneditor aufzurufen

Nach dem Start der Gruppenrichtlinienverwaltung können Sie die Gruppenrichtlinien der *paedML Linux* einsehen.

10.1.2 Aufbau der Gruppenrichtlinienverwaltung

Wenn Sie die Gruppenrichtlinienverwaltung öffnen sehen Sie auf der linken Seite eine Baumstruktur, über die verschiedene Ebenen aufgerufen werden können. Relevant für die Arbeit mit der *paedML* sind folgende zwei Bereiche:

- Im Container „*schule*“ (roter Kasten ❶) finden Sie alle Gruppenrichtlinien, die in Ihrem Schulnetz im Auslieferungszustand bereits aktiviert sind.
- Im Container „*Gruppenrichtlinienobjekte*“ (grüner Kasten ❷) finden Sie alle verfügbaren Gruppenrichtlinien (aktive und inaktive). Hier sind unter Umständen Gruppenrichtlinien vorhanden, die nicht im Netzwerk aktiv sind. Wenn Sie ein Upgrade von der Version 7.0 auf die Version 7.1 durchgeführt haben, finden Sie dort noch die „alten“ Gruppenrichtlinienobjekte, um eventuelle eigene Anpassungen auf die neuen Gruppenrichtlinien übertragen zu können. Bei einer Neuinstallation sehen Sie hier nur die neuen Gruppenrichtlinienobjekte.

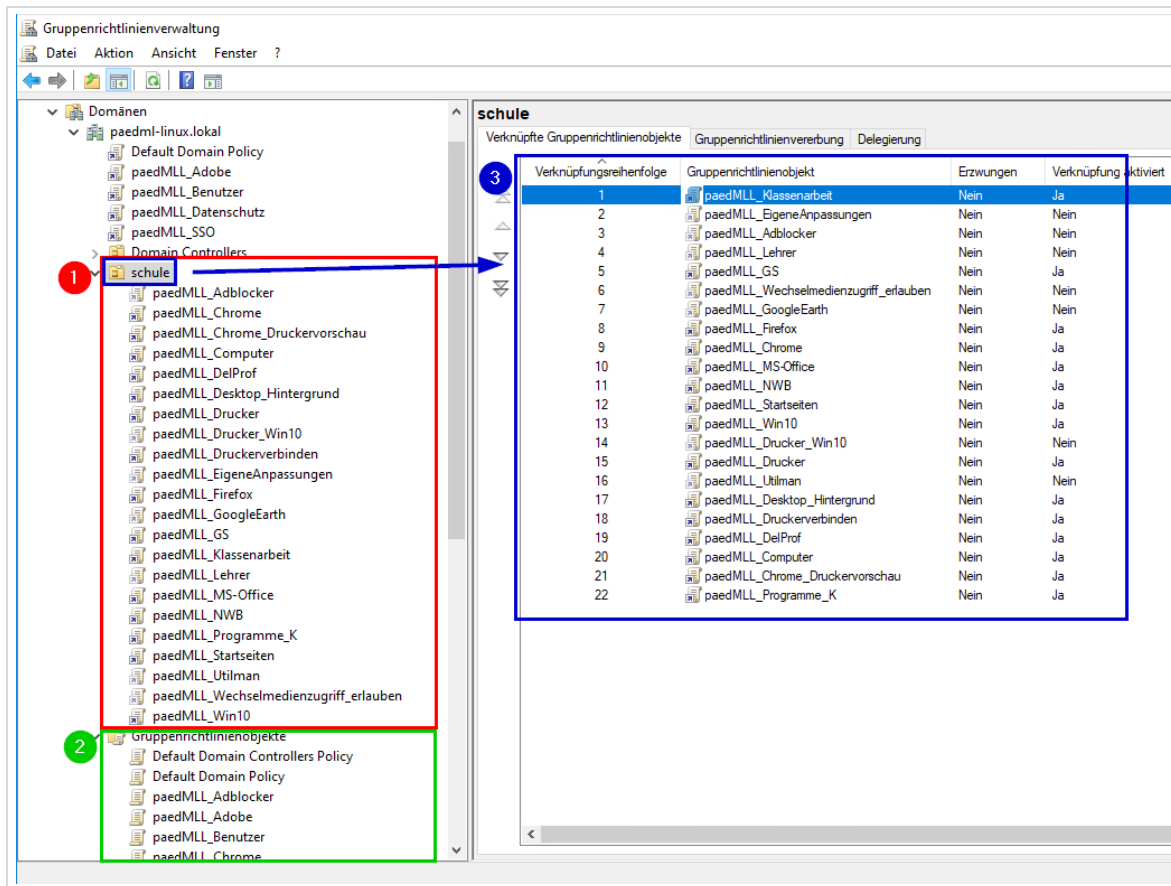


Abb. 147: Der Gruppenrichtlinieneditor und die Gruppenrichtlinien

Auf der rechten Seite sehen Sie – sofern der Container „schule“ angewählt ist – in welcher Reihenfolge die Gruppenrichtlinien abgearbeitet werden (blauer Kasten ③). Die Gruppenrichtlinien werden von unten nach oben abgearbeitet. Das heißt die Gruppenrichtlinie mit der kleinsten Nummer wird zuletzt bearbeitet.

Einige Gruppenrichtlinien sind optional und können bei Bedarf aktiviert werden.

PaedML Linux Kunden sollten die Grundschul-Gruppenrichtlinie nicht aktivieren.

Bei „widersprüchlichen“ Gruppenrichtlinien greift der letzte ausgeführte Gruppenrichtliniensatz. Diesen Mechanismus nutzen wir im Abschnitt „Änderungen der Gruppenrichtlinien“ (Kapitel 10.2).

10.1.3 Übersicht über die Gruppenrichtlinien der paedML Linux

Die Gruppenrichtlinien lassen sich in verschiedene Funktionen unterscheiden.

Eine Sonderstellung nehmen die Gruppenrichtlinien „Default Domain Controllers Policy“ und „Default Domain Policy“ ein, die für die Grundfunktionalität des UCS-Domänencontrollers benötigt werden.

10.2 Änderung der Gruppenrichtlinien



Nehmen Sie Änderungen bitte ausschließlich an paedMLL_EigeneAnpassungen vor oder erstellen Sie eine neue Gruppenrichtlinie.

Es ist notwendig, dass die Hotline bei Problemen im Zusammenhang mit Gruppenrichtlinien auf einen Standard zugreifen kann. Im Bedarfsfall werden die Standardgruppenrichtlinien wiederhergestellt, so dass Änderungen unwiderruflich verloren gehen.

10.2.1 Aktivieren und Deaktivieren von Gruppenrichtlinien

Um eine aktive Gruppenrichtlinie zu deaktivieren, klicken Sie mit der rechten Maustaste auf den Eintrag (im folgenden Beispiel „paedMLL_Wechselmedienzugriff_erlauben“). Ein Klick auf „Löschen“ (roter Rahmen) entfernt die Verknüpfung zur eigentlichen Gruppenrichtlinie aus der Liste der aktiven Gruppenrichtlinien des Containers „schule“. Die Gruppenrichtlinie ist dadurch jedoch NICHT im System gelöscht und kann jederzeit wieder zurückgeholt werden.



Beachten Sie unbedingt, dass im Bereich der Gruppenrichtlinienobjekte NIEMALS das Gruppenrichtlinienobjekt selbst (im folgenden Screenshot rot hinterlegte Fläche), sondern IMMER NUR die Verknüpfung zu einem Gruppenrichtlinienobjekt (im folgenden Screenshot grün hinterlegt) gelöscht werden darf.

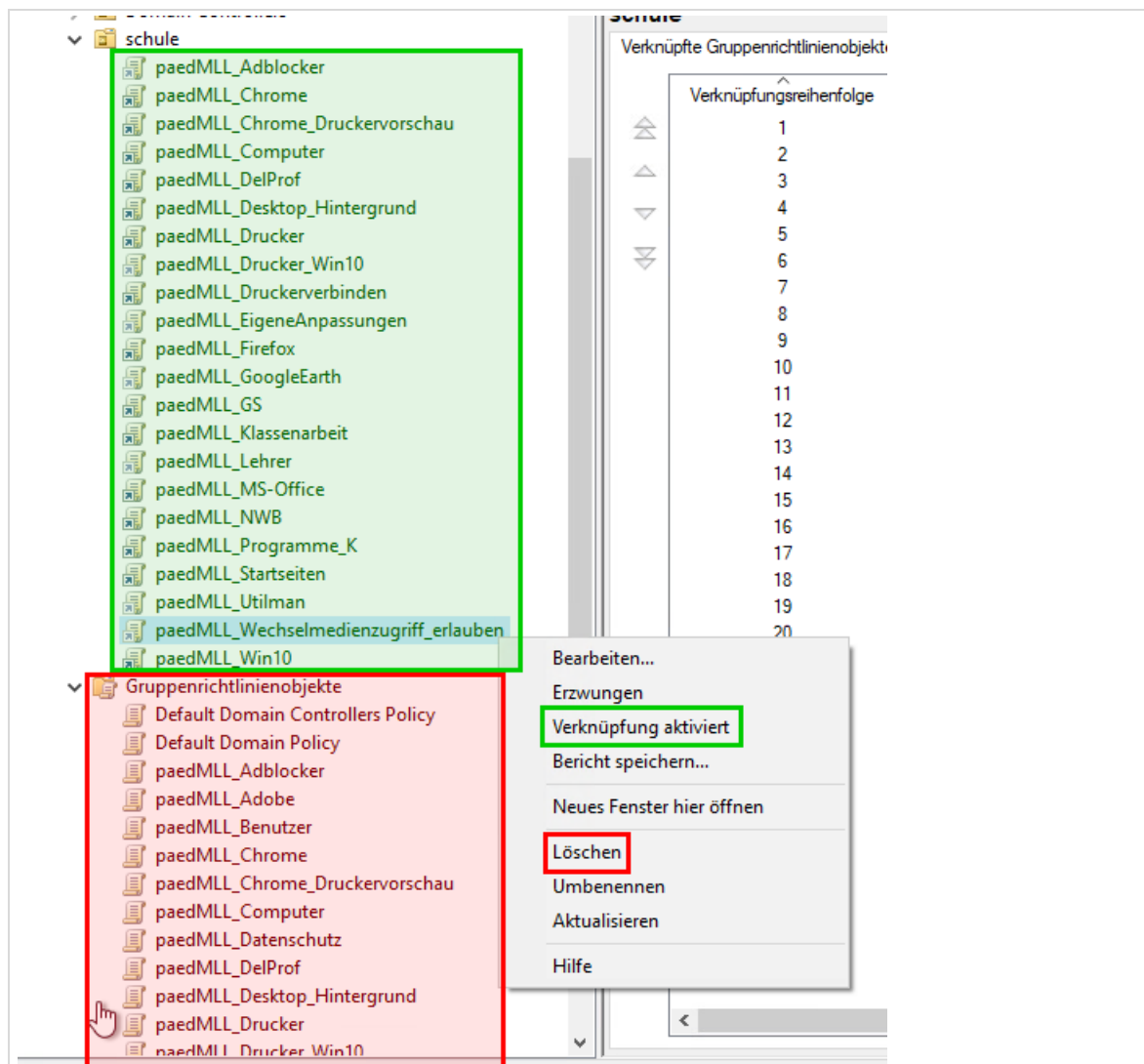


Abb. 148: Deaktivieren einer Gruppenrichtlinie –Achtung! Nicht das Gruppenrichtlinienobjekt selbst löschen!



Ein Haken vor dem Eintrag „*Verknüpfung aktiviert*“ zeigt an, dass die Verknüpfung aktiv ist. Sie können temporär auch den Haken deaktivieren.

Optionale Gruppenrichtlinien sind standardmäßig nicht aktiviert. Ob eine Gruppenrichtlinie aktiviert ist, können Sie in der Spalte „Verknüpfung aktiviert“ ablesen. Sollten Sie z.B. eine paedML für Grundschulen einsetzen, müssen Sie die Gruppenrichtlinie *paedMLL_GS* aktivieren.



Achtung! Die Reihenfolge der Gruppenrichtlinien ändert sich, wenn Sie Gruppenrichtlinien aktivieren und deaktivieren. Sie können die jeweils aktuelle Reihenfolge von Gruppenrichtlinien über die Auswahl des Containers „schule“ in der Gruppenrichtlinienverwaltung aufrufen. Gruppenrichtlinien werden von unten (größere Zahl) nach oben (kleinere Zahl) abgearbeitet.

Wir empfehlen dennoch die Reihenfolge des folgenden Screenshots einzuhalten:























Verknüpfungsreihenfolge	Gruppenrichtlinienobjekt
1	 paedMLL_Klassenarbeit
2	 paedMLL_EigeneAnpassungen
3	 paedMLL_Adblocker
4	 paedMLL_Lehrer
5	 paedMLL_GS
6	 paedMLL>Wechselmedienzugriff_erlauben
7	 paedMLL_GoogleEarth
8	 paedMLL_Firefox
9	 paedMLL_Chrome
10	 paedMLL_MS-Office
11	 paedMLL_NWB
12	 paedMLL_Startseiten
13	 paedMLL_Win10
14	 paedMLL_Drucker_Win10
15	 paedMLL_Drucker
16	 paedMLL_Utilman
17	 paedMLL_Desktop_Hintergrund
18	 paedMLL_Druckerverbinden
19	 paedMLL_DelProf
20	 paedMLL_Computer
21	 paedMLL_Chrome_Druckervorschau
22	 paedMLL_Programme_K

Abb. 149: Reihenfolge der Gruppenrichtlinien

10.2.2 Optionale Gruppenrichtlinie Wechselmedienzugriff

Möchten Sie den Zugriff auf Wechselmedien im Schulnetz erlauben, muss die Gruppenrichtlinie *paedMLL>Wechselmedien_erlauben* aktiviert werden.

10.2.3 Optionale Gruppenrichtlinie Lehrer

Einstellungen, die nur für Lehrer gelten sollen, können in der Gruppenrichtlinie *paedMLL_Lehrer* definiert werden. Anschließend muss die Gruppenrichtlinie aktiviert werden.

10.2.4 Optionale Gruppenrichtlinie Utilman

Verhindert bei Aktivierung die Ausführung der Datei Utilman.exe (Center für erleichterte Bedienung) und damit einen Missbrauch dieser. Die Aktivierung dieser Gruppenrichtlinie hat ggf. auch Auswirkung auf andere Anwendungen.

10.2.5 Bearbeiten von Gruppenrichtlinien

Beispiel: Festlegung der Startseite in verschiedenen Browsern

Die Startseiten der Browser Microsoft Edge, Internet Explorer, Google Chrome und Mozilla Firefox wird in der Gruppenrichtlinie „paedMLL_Startseiten“ definiert. Wenn Sie zunächst wissen möchten, welche Einstellungen in einer bestimmten Gruppenrichtlinie bereits vorgenommen wurden, können Sie wie nachfolgend beschrieben herausfinden:

1. Öffnen Sie den Gruppenrichtlinien-Verwaltungs-Editor.
2. Klicken Sie auf die entsprechende Gruppenrichtlinie im linken Bereich (im Beispiel „paedMLL_Startseiten“) und wählen Sie im rechten Bereich den Reiter „Einstellungen“ (2) aus. Hier können Sie alle vorgenommenen Konfigurationen sehen.
3. Mit einem Klick auf „show“ (3) können Sie weitere Einstellungen, z.B. bezüglich des Browsers Mozilla Firefox anzeigen lassen (3). „Show all“ (4) zeigt alle Einstellungen in der Gruppenrichtlinie.

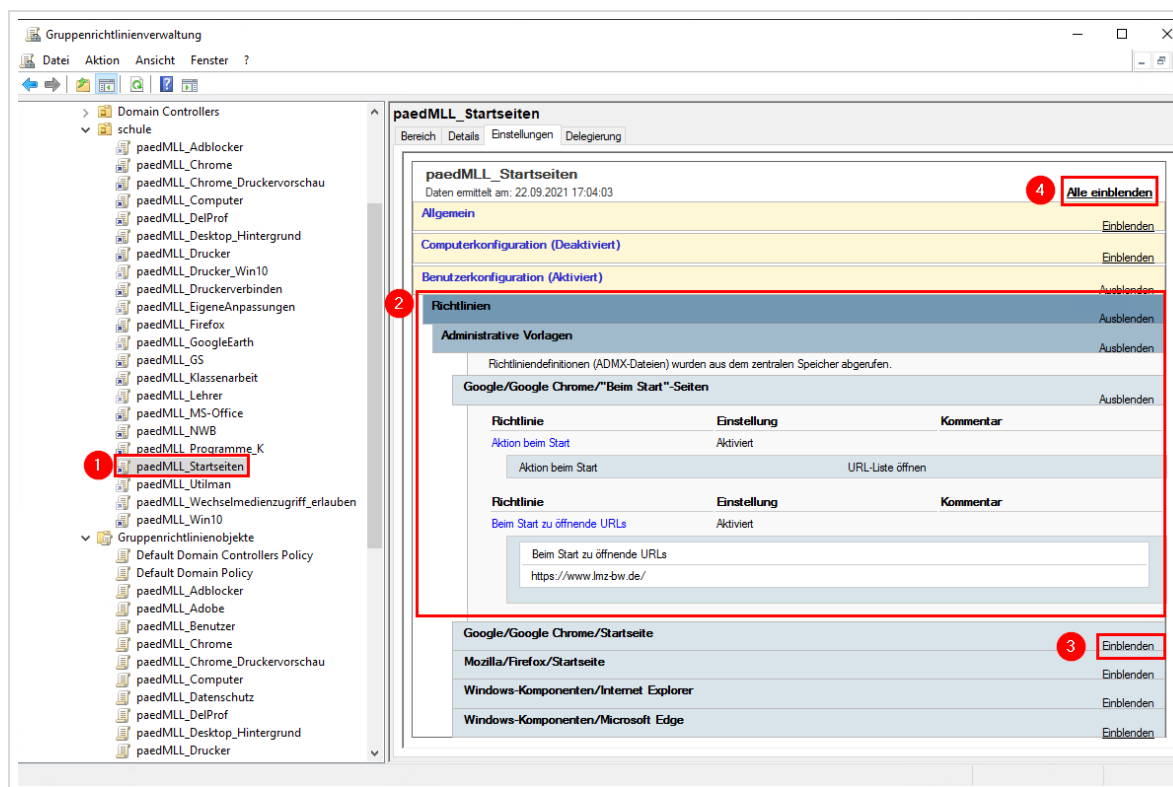


Abb. 150: Gruppenrichtlinien Einstellungen von paedMLL_Startseiten am Beispiel des Browsers Google Chrome

Wie Sie statt der Vorgabe eine eigene Startseite festlegen wird nachfolgend für den Browser Google Chrome beschrieben. Die Beschreibung bezieht sich im ersten Teil auf die Startseite, die geöffnet werden soll, wenn der „Home-Button“ im Browser angeklickt wird. Im zweiten Teil wird die Startseite festgelegt, die beim Start des Browsers automatisch aufgerufen wird.

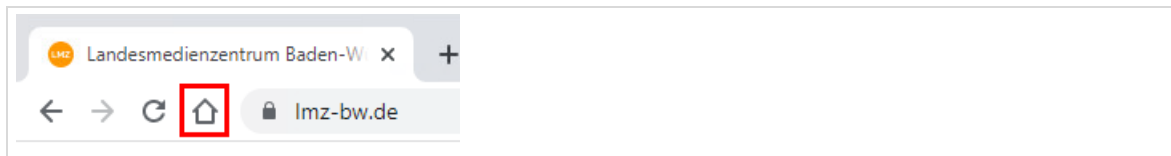


Abb. 151: Home-Button im Browser Google Chrome

1. Öffnen Sie den Gruppenrichtlinien-Verwaltungs-Editor.
2. Wählen Sie die zu bearbeitende Gruppenrichtlinie mit der rechten Maustaste aus und klicken Sie auf „Bearbeiten“.



Abb. 152: Aufruf einer zu bearbeitenden Gruppenrichtlinie

3. Es öffnet sich ein neues Fenster, in dem die Gruppenrichtlinie editiert wird. Sie sehen auf der obersten Ebene der linken Seite den Namen der Gruppenrichtlinie.
4. Die Einstellungen verbergen sich im Zweig „Benutzerkonfiguration | Richtlinien | Administrative Vorlagen | Google | Google Chrome“. Der Inhalt des rechten Fenster-Bereichs ist dynamisch und wird je nach Auswahl auf der linken Seite befüllt.
5. Wenn Sie den Eintrag „Startseite“ gewählt haben, dann bekommen Sie auf der rechten Seite in den Einstellungen den Eintrag „Startseiten-URL konfigurieren“ angezeigt. Ein Doppelklick führt Sie zu einem neuen Fenster, in dem die „Home“-Seite des Chrome-Browsers geändert werden kann.

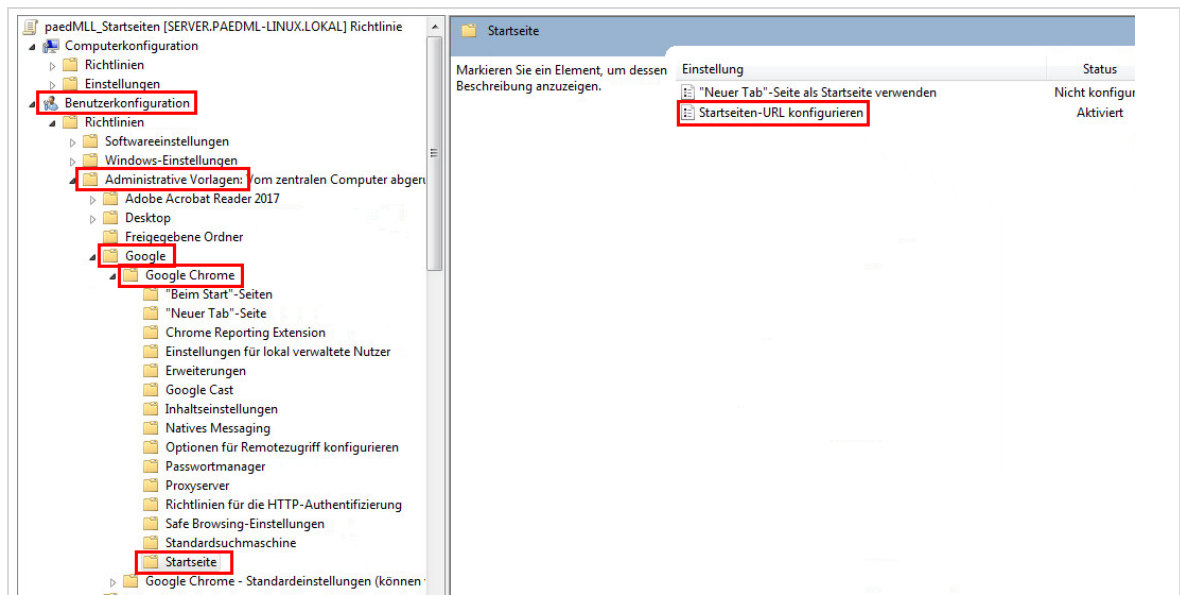


Abb. 153: Der Gruppenrichtlinienverwaltungs-Editor

6. Die Inhalte, bzw. die Konfigurationsmasken der einzelnen Einstellungen variieren – je nach Parameter, der eingestellt werden soll.
Im vorliegenden Fall wird die Startseiten-URL im Feld „Optionen“ definiert. Hier steht im Auslieferungszustand der Wert „www.lmz-bw.de“, den Sie anpassen können. Ein Klick auf „OK“ speichert die Änderungen.

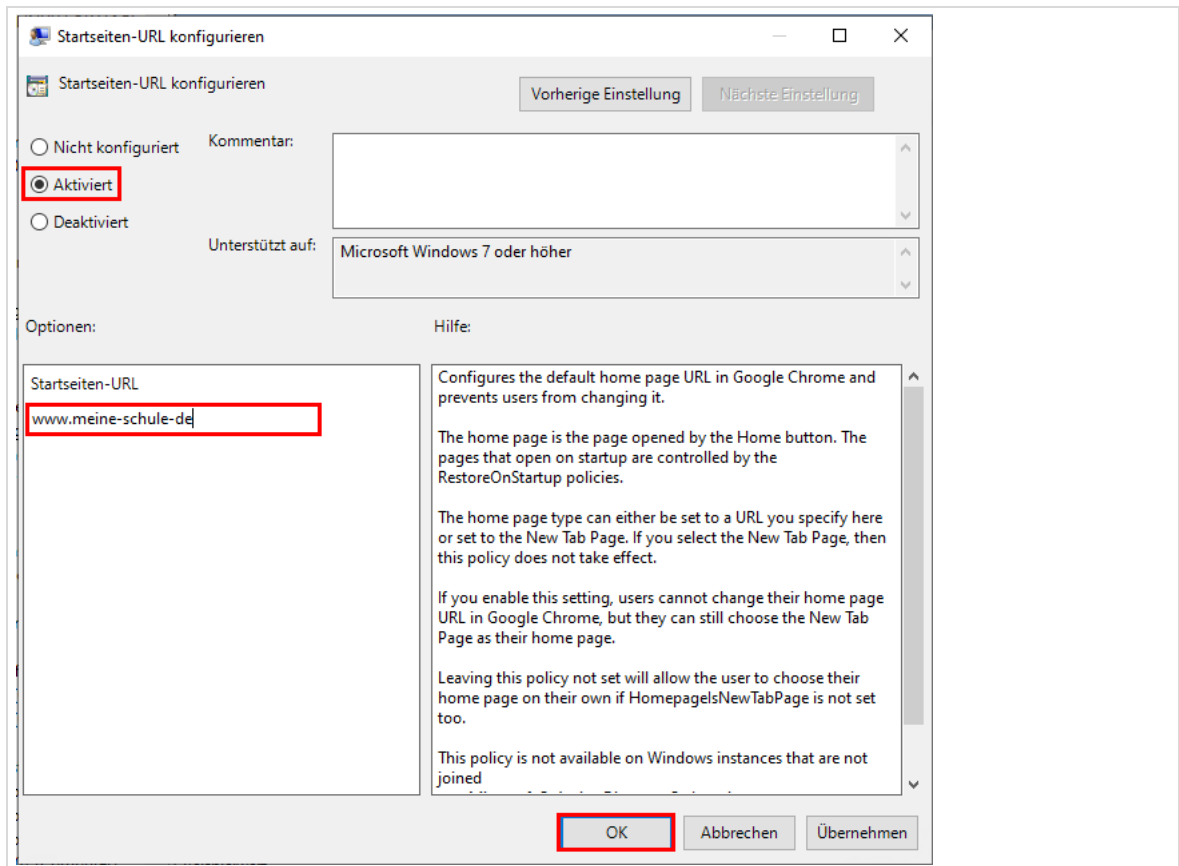


Abb. 154: Änderung der Home-Seite von google-chrome

Die Einstellungen der Startseite sind hiermit noch nicht abgeschlossen. Im nächsten Schritt wird die Startseite festgelegt, die automatisch beim Start des Browsers geöffnet werden soll.

1. Wählen Sie den Eintrag „Beim Start zu öffnende URLs“ und im Unterdialog „Beim Start zu öffnende URLs“ aus.

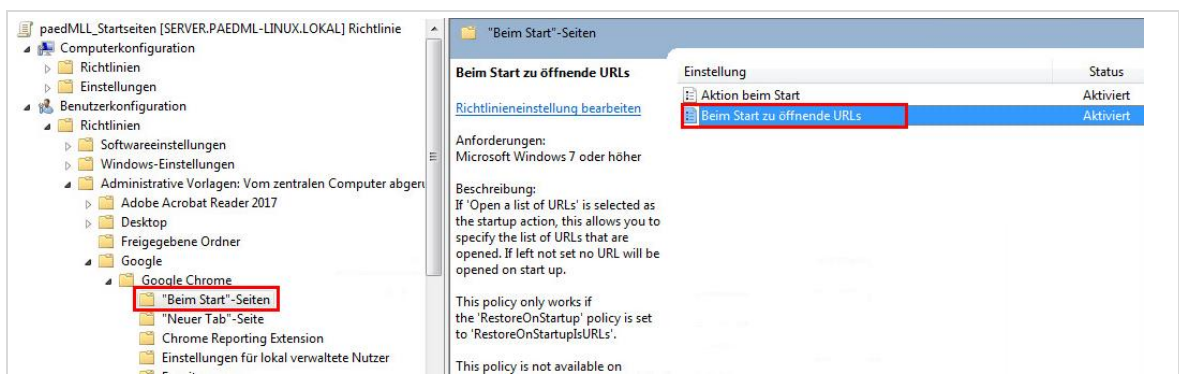


Abb. 155: Für die Startseite von chrome werden weitere Einstellungen benötigt.

2. Es öffnet sich ein Dialogfenster. Klicken Sie hier auf „Anzeigen...“, um die beim Start zu öffnenden URLs zu editieren.

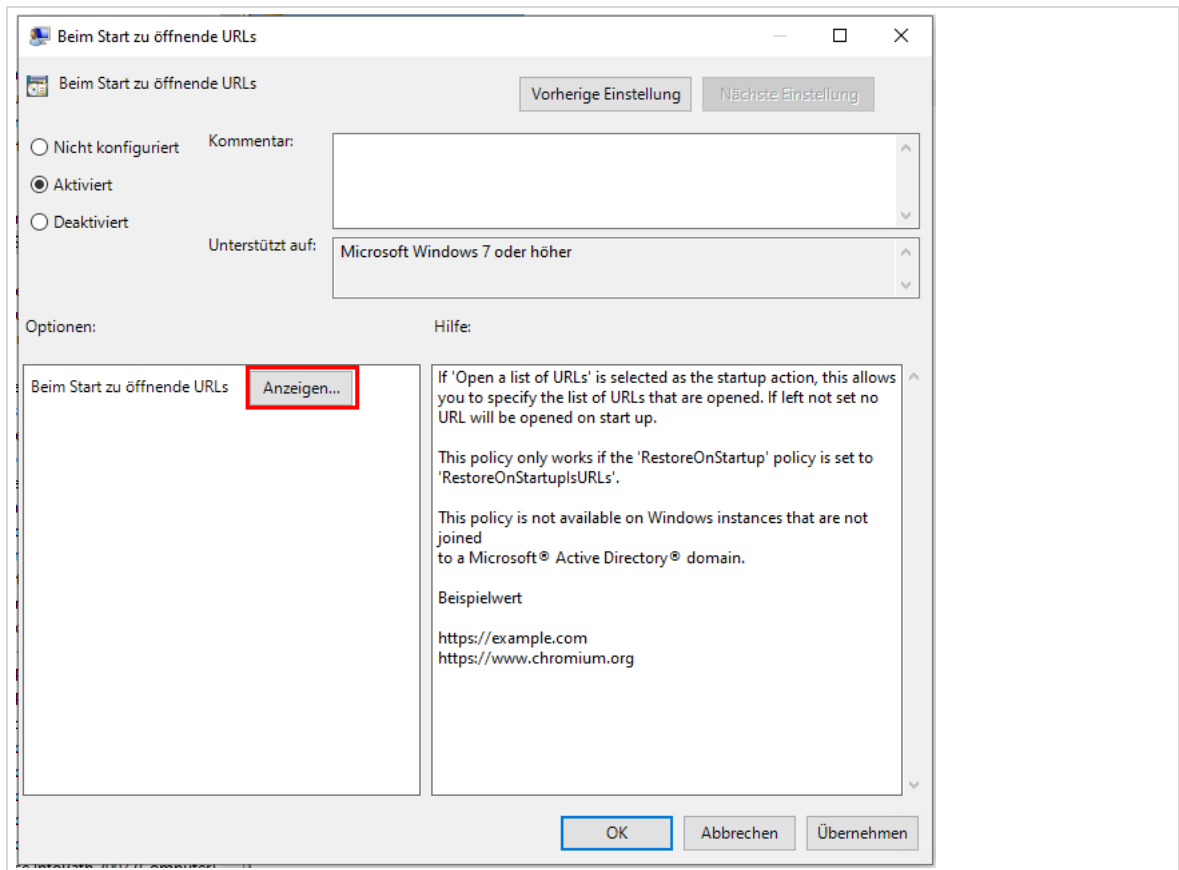


Abb. 156: Öffnen der Einstellungen von URLs beim Programmstart

3. Im Nächsten Fenster können Sie die Startseite(n) festlegen. Mehrere Seiten werden in mehreren Reitern (Tabs) angezeigt.

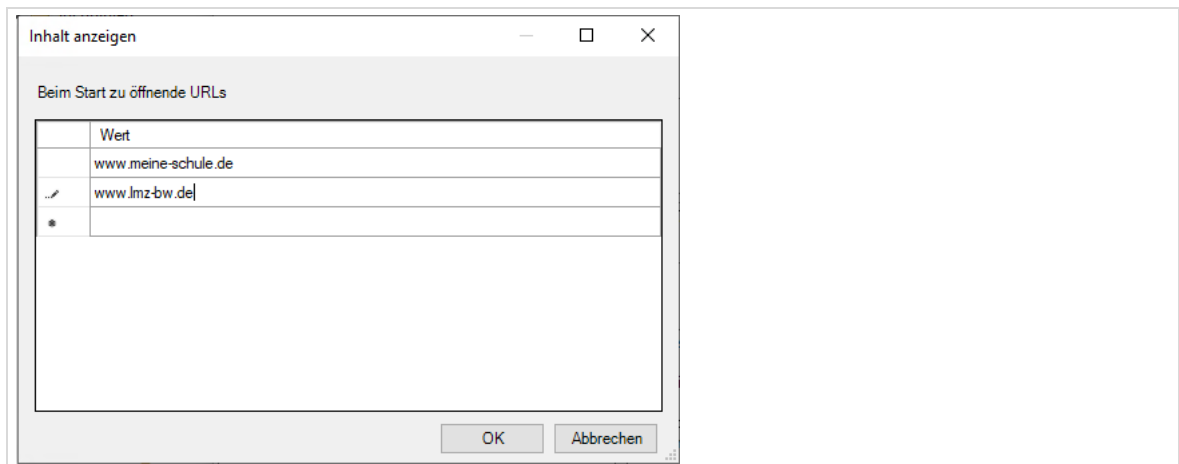


Abb. 157: Festlegen der Startseiten



Damit Änderungen unterhalb der „Benutzerkonfiguration“ angewandt werden, muss der Benutzer neu angemeldet werden. Bei Änderungen im Bereich „Computerkonfiguration“ müssen die Rechner neu gestartet werden.

Empfohlen wird folgender Konsolenbefehl, nach Arbeiten an den Gruppenrichtlinien, um Rechte im „sysvol“ neu zu setzen:

1. Melden Sie sich als „root“ am Server an.
2. Führen Sie den Befehl `samba-tool ntac1 sysvolreset` aus.

10.3 Desktop-Verknüpfungen mit Gruppenrichtlinien erstellen

1. Starten Sie die Gruppenrichtlinienverwaltung.
2. Legen Sie ein neues Gruppenrichtlinienobjekt an, indem Sie mit der rechten Maustaste auf „Gruppenrichtlinienobjekte“ und mit der linken Maustaste danach auf „Neu“ klicken.

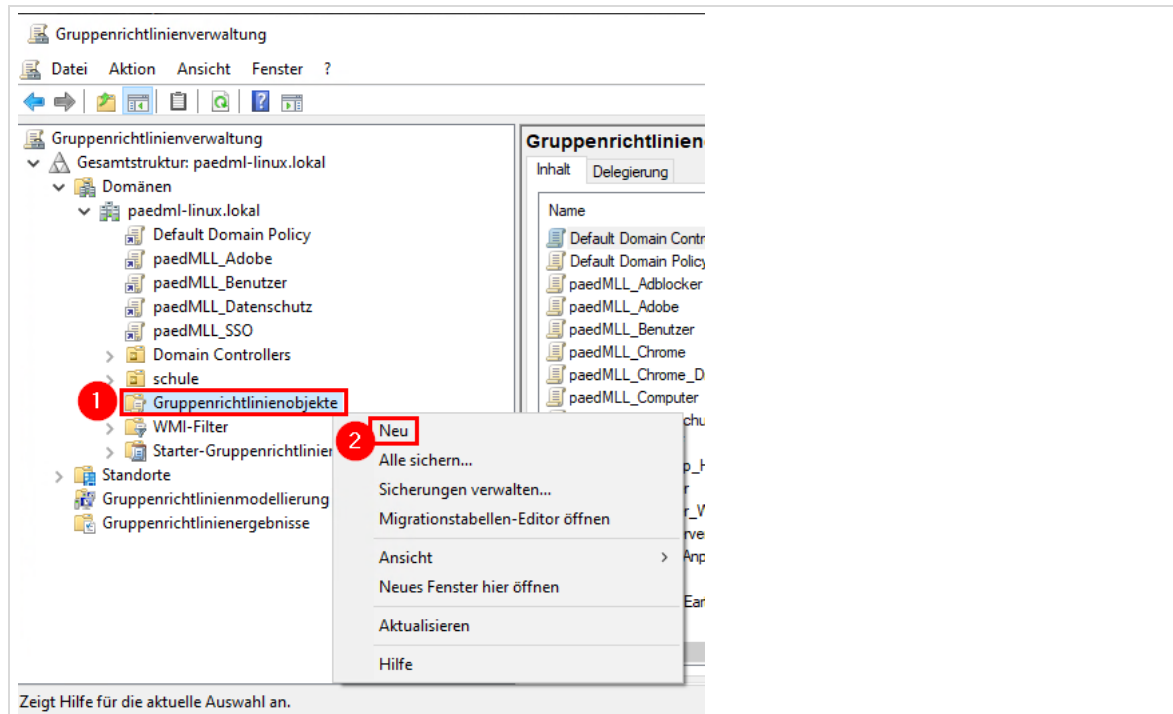


Abb. 158: Neues Gruppenrichtlinienobjekt

3. Vergeben Sie einen Namen, z.B.:

- Desktop_Allgemein
- Desktop_Lehrer
- Desktop_Schueler

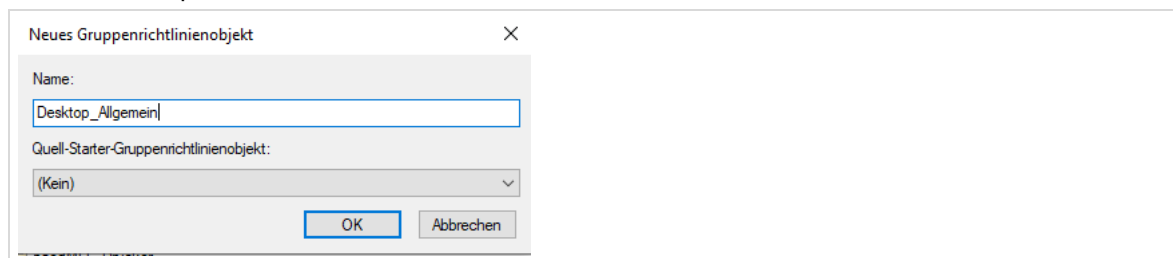


Abb. 159: Namen vergeben

4. Sicherheitsfilterung festlegen
- In der Sicherheitsfilterung wird festgelegt, für welche Gruppen, Benutzer und Computer das Gruppenrichtlinienobjekt angewendet wird.
 - Sie können neue Objekte zur Sicherheitsfilterung hinzufügen, indem Sie die Gruppenrichtlinie auswählen (1), im Reiter „Bereich“ auf „Hinzufügen“ klicken (2) und den Objektnamen eingeben (3). Mit „Namen überprüfen“ können Sie testen, ob der Objektnamen existiert. Mit „OK“ bestätigen Sie Ihre Auswahl.
 - Mögliche Einstellung für „Desktop_Allgemein“:

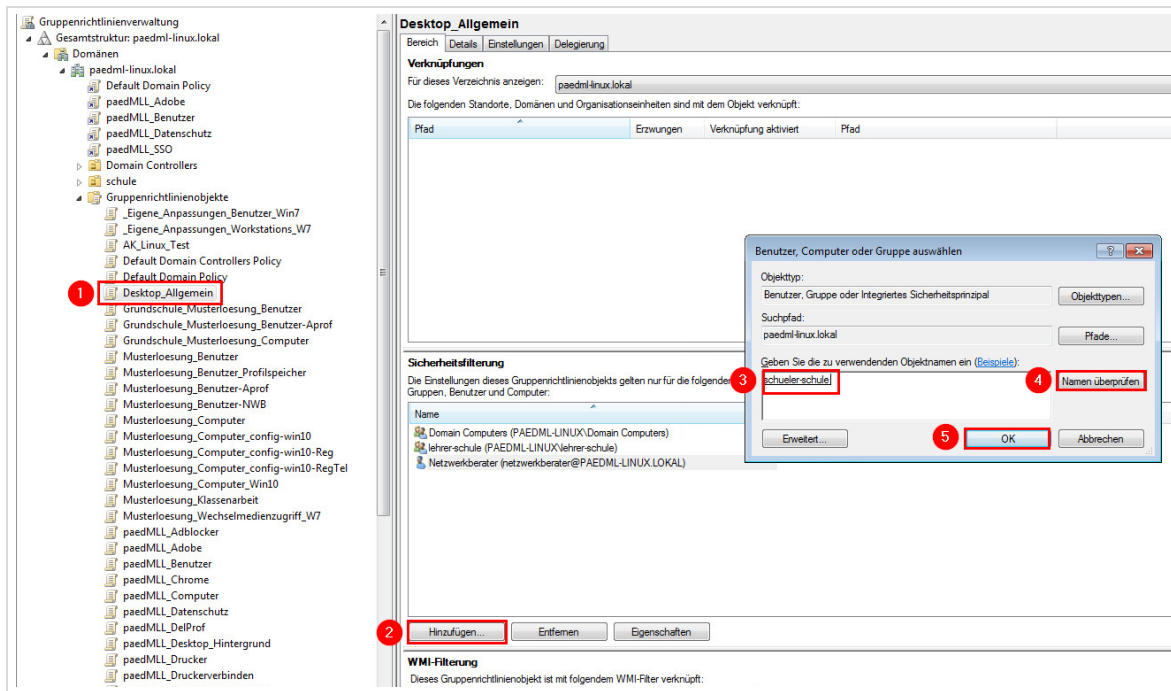


Abb. 160: Mögliche Sicherheitsfilterung

5. Objektstatus einstellen

Da es sich um eine Benutzerkonfiguration handelt, werden die Computerkonfigurationseinstellungen deaktiviert. Dies erfolgt im Reiter „Details“ unter „Objektstatus“.

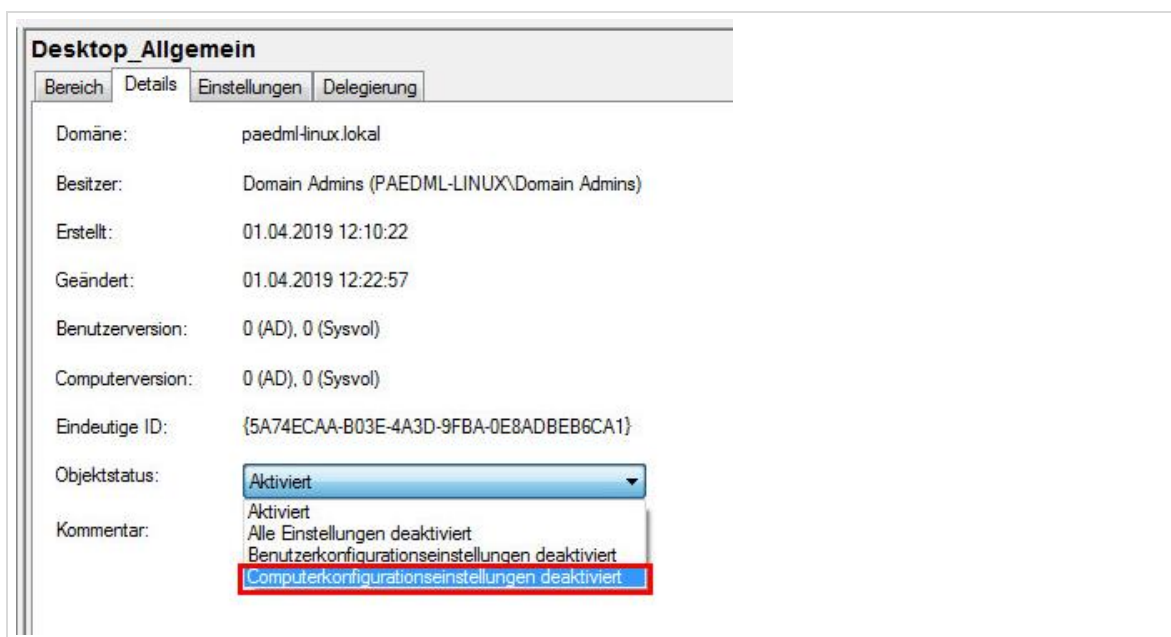


Abb. 161: Namen vergeben

6. Neue Desktopverknüpfung anlegen

- Wechseln Sie im Gruppenrichtlinienverwaltungs-Editor in der Benutzerkonfiguration der Gruppenrichtlinie in den Bereich „Einstellungen -> Windows-Einstellungen“
- Klicken Sie mit der rechten Maustaste auf Verknüpfungen und wählen Sie „Neu | Verknüpfung“

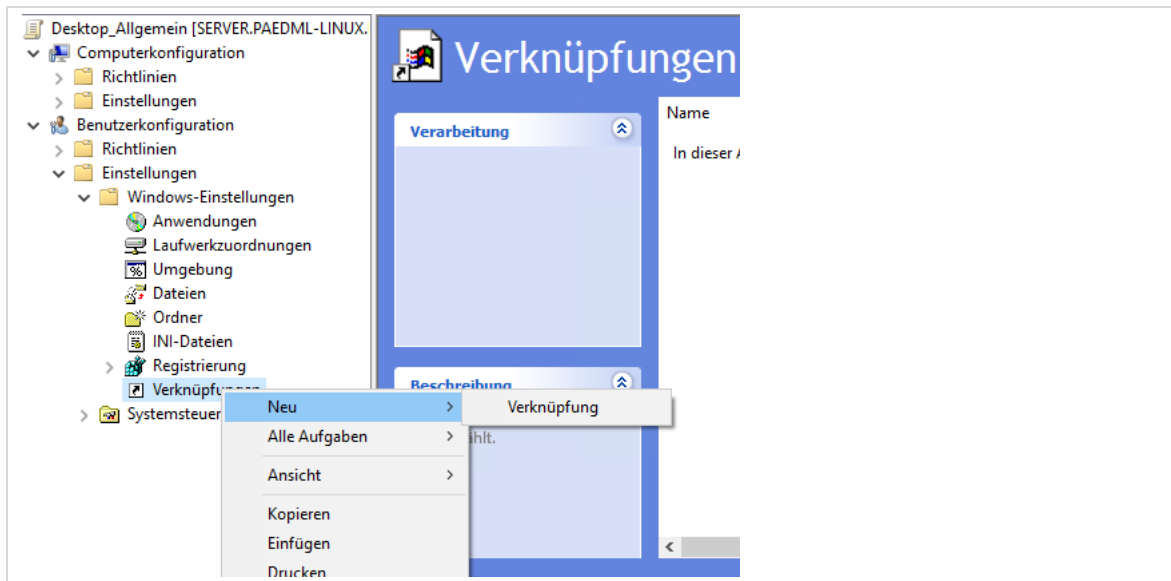


Abb. 162: Neue Verknüpfung erstellen

6.1. Verknüpfung zu einem Dateisystemobjekt

Ein Dateisystemobjekt kann z. B. eine ausführbare Datei sein. Um diese Art der Verknüpfung zu erstellen, müssen Sie bei „Aktion“ Erstellen, bei „Zielpfad“ die ausführbare Datei und unter „Name“ die Bezeichnung der Verknüpfung angeben. Im Symboldateipfad kann ein Verknüpfungssymbol (*.ico) hinterlegt werden.

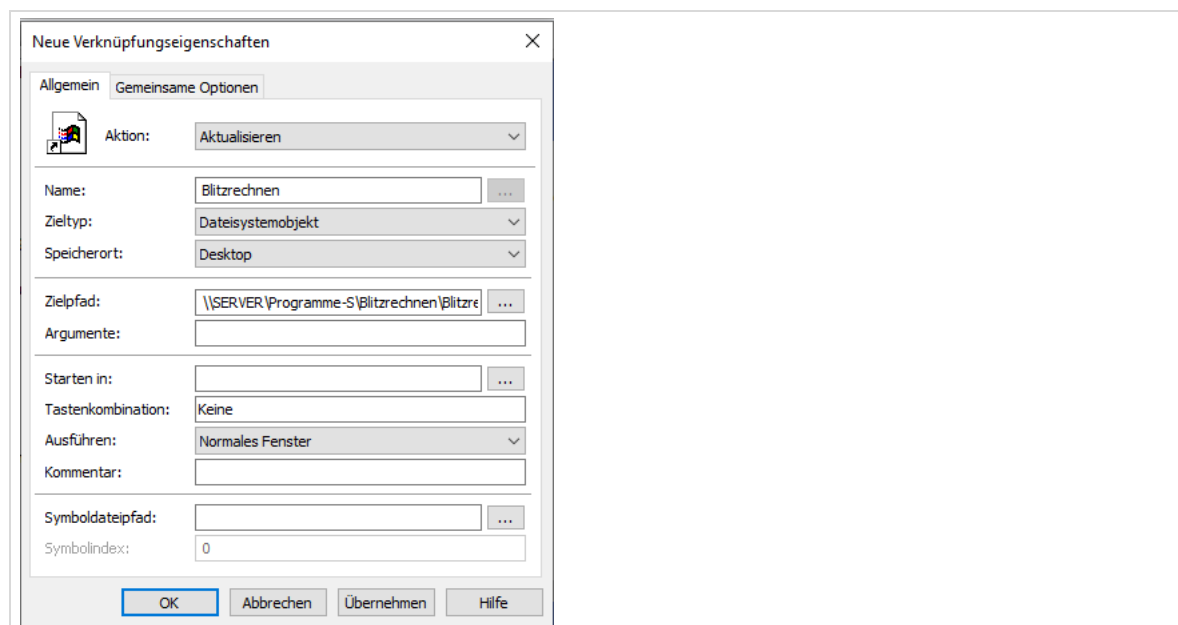


Abb. 163: Verknüpfung zu einer ausführbaren Datei

6.2. Verknüpfung auf eine URL

Um eine Verknüpfung auf eine Webseite zu erstellen, geben Sie unter „Aktion“ Erstellen, unter „Name“ den Namen der Verknüpfung ein und bei „Ziel-URL“ die Webseiten-URL. Im Symboldateipfad kann ein Verknüpfungssymbol (*.ico) hinterlegt werden.

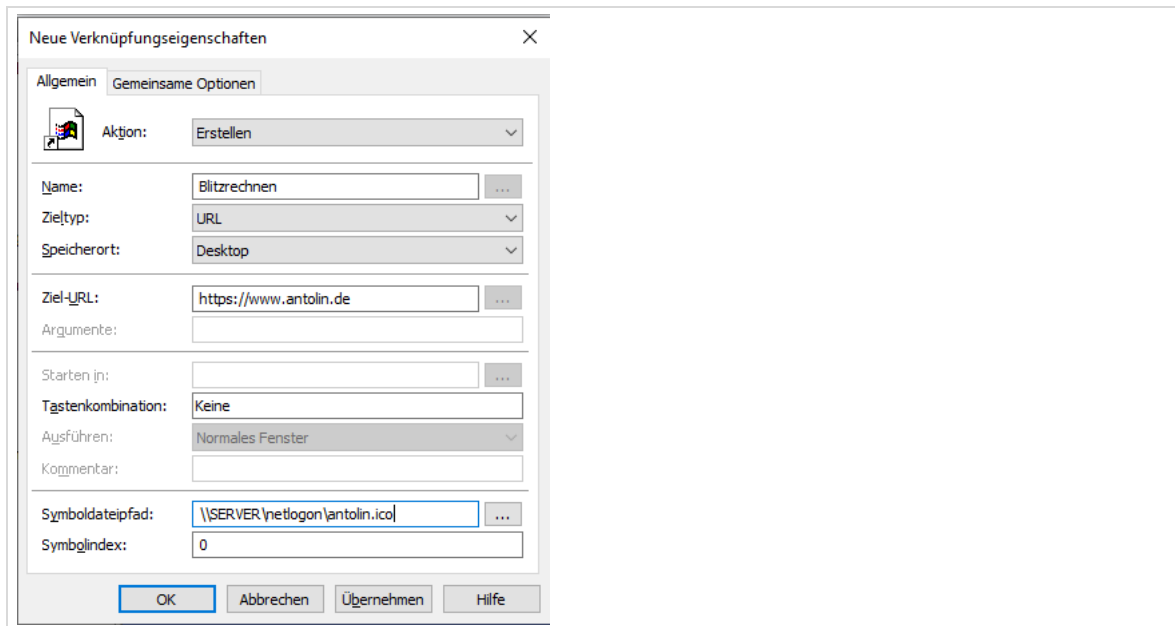


Abb. 164: Verknüpfung zu einer URL

7. GPO im Bereich Schule verknüpfen

- Rechtsklick auf „schule“ und „vorhandenes Gruppenrichtlinienobjekt verknüpfen ...“ wählen:

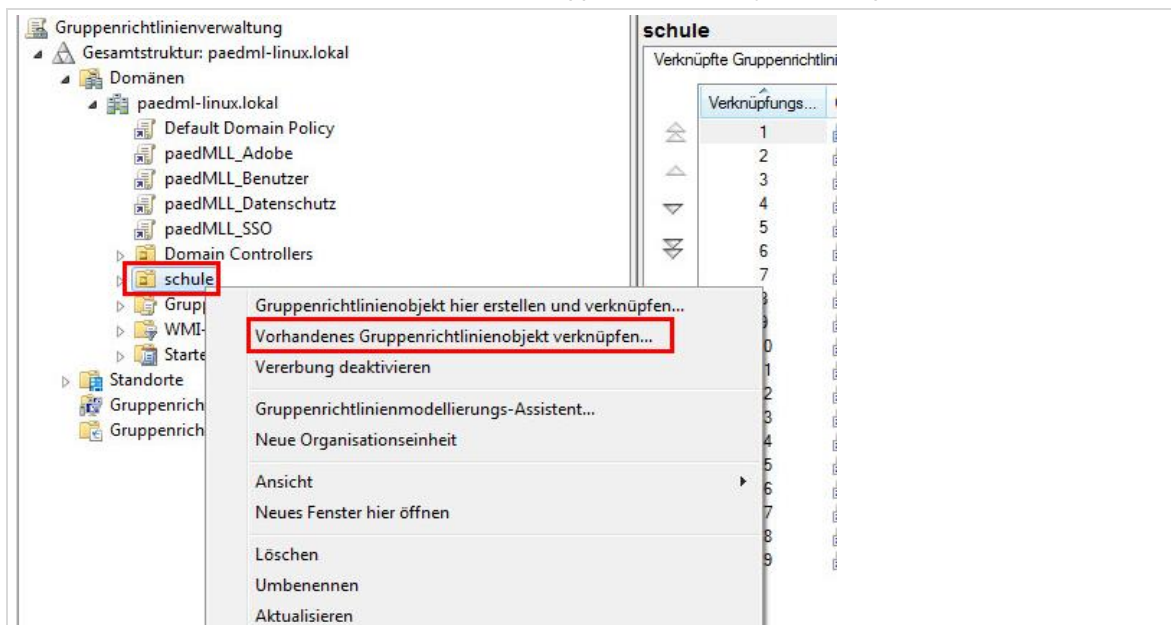


Abb. 165: GPO in „schule“ verknüpfen

- Wählen Sie die erstellte Gruppenrichtlinie aus und bestätigen Sie mit „OK“:

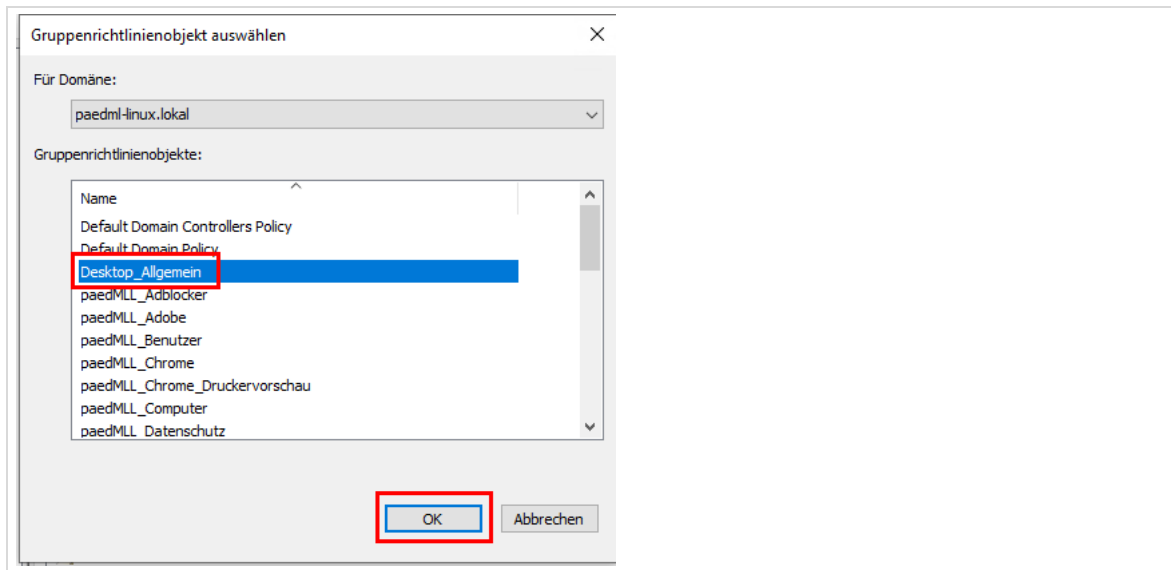


Abb. 166: GPO auswählen

- Die Gruppenrichtlinie ist verknüpft und somit aktiv:

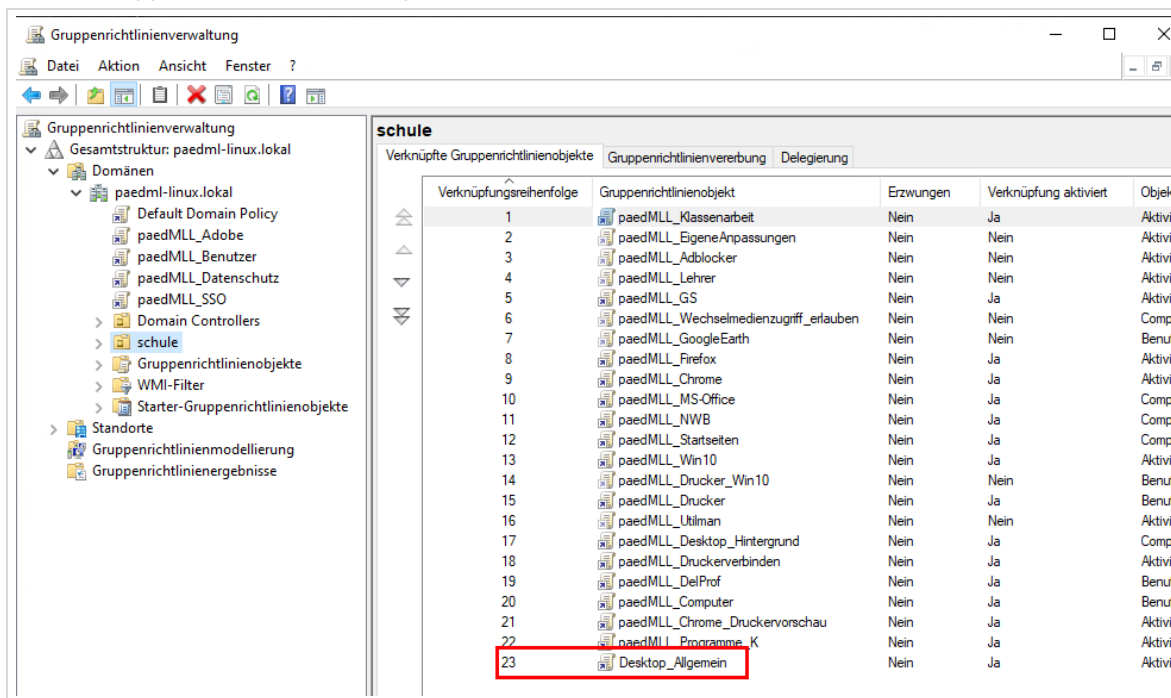


Abb. 167: Verknüpfte GPO

10.4 Festlegen eines eigenen Hintergrundbildes

Um ein eigenes Hintergrundbild zu definieren, wird empfohlen, dass Sie den Hintergrund mithilfe des opsi-Pakets „paedml-login“ ändern:

1. Erstellen Sie eine neue Datei „img0.jpg“ und kopieren Sie diese als Domänenadministrator auf den opsi-Server in die Freigabe `\\BACKUP\opsi_depot_rw\paedml-login\custom`.

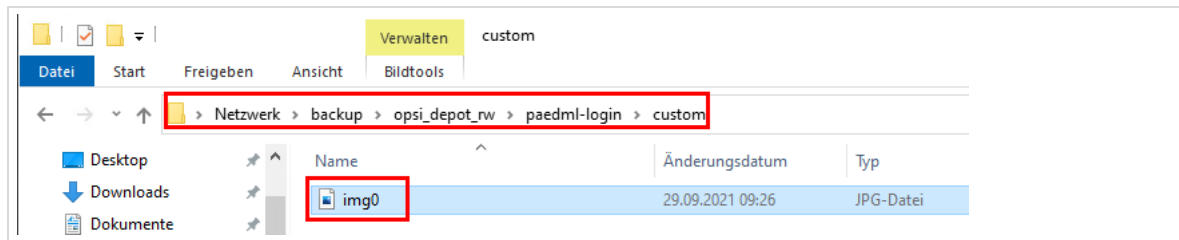


Abb. 168: Pfad des eigenen Hintergrundbilds auf dem opsi-Server

2. Setzen Sie das Paket „paedml-login“ für alle Rechner auf „setup“, die das Hintergrundbild bekommen sollen.
3. Starten Sie einen Rechner neu, und melden Sie sich als Domänenbenutzer an, um die Änderungen zu überprüfen.

10.5 Zugriff auf Wechselmedien

Die Gruppenrichtlinie „paedML_Wechselmedienzugriff_erlauben“ ist standardmäßig nicht aktiviert, der Zugriff auf externe Speichermedien ist für alle Benutzer unterbunden. Dies bedeutet im Klartext, dass Benutzer nicht in der Lage sind auf externe Datenträger (CDs, USB-Sticks, externe Festplatten) oder auf digitale Geräte (Handy, MP3-Player, ...), die an den PC angeschlossen werden, zuzugreifen.

Durch diese Einstellungen kann teilweise unterbunden werden, dass durch USB-Sticks oder ähnliches, Viren in das Schulnetz gebracht werden. Auch unerwünschtes File-Sharing kann durch ein Sperren der Datenträger unterbunden werden.

Negativer Seiteneffekt ist jedoch, dass es durchaus Situationen gibt, in dem Benutzer Dateien von/auf USB-Sticks ablegen sollen:

- Die Präsentation, die im Unterricht gehalten werden soll kann nicht im pädagogischen Netz abgelegt werden.
- Die Hausarbeit, die in der Schule und zu Hause bearbeitet werden soll kann nach der Fertigstellung nicht ins schulische Netz gesendet werden.
- Die in der Einführung angesprochene Datensicherung, die zum Ende des Schuljahres verhindern soll, dass die Schüler im neuen Schuljahr aller Daten verlustig gehen, da der Netzwerkberater Tabula Rasa macht und alle Daten aus den Home-Verzeichnissen löscht.

In einem dieser Fälle gilt es natürlich abzuwägen, ob die Sperre von externen Speichermedien (temporär) deaktiviert werden soll.

Im Klassenarbeitsmodus können Wechseldatenträger nicht freigegeben werden.

Sperren und Freigeben mithilfe von Gruppenrichtlinien

Das Aktivieren der Gruppenrichtlinie ist als Beispiel in Kapitel 10.2.1 auf Seite 143 beschrieben. Mithilfe der Sicherheitsfilterung können Sie festlegen, für welche Benutzer Wechseldatenträger freigegeben werden sollen. Zum Beispiel soll der Zugriff nur für Lehrer erlaubt sein, für Schüler nicht.

11 Einrichtung von Druckern

Bereitstellung von Druckertreibern via Samba

In der paedML Linux werden Druckaufträge über das Drucksystem CUPS (Common Unix Printing System)³⁹ ausgeführt. CUPS läuft als Systemdienst auf dem Server und dient als Warteschlange für die Verarbeitung von Druckaufträgen.

Beim Drucken spielt der Systemdienst Samba eine wichtige Rolle. Dort werden die Druckertreiber für die Windows-Rechner hinterlegt. Dies geschieht über die Windows-Freigabe „*print\$*“. Jede Druckerfreigabe wird mit Hilfe des von Windows bereitgestellten Point 'n' Print Verfahrens mit einem Treiber aus der „*print\$*“-Freigabe verknüpft.

Über eine Zuordnung in der Schulkonsole und zusätzlich über Gruppenrichtlinien bekommen Computerräume Drucker zugewiesen. Bei der Einrichtung der Computer wird – sofern ein Drucker zugewiesen ist – automatisch der Druckertreiber für den Client bereitgestellt. Hierdurch kann der Benutzer auf den entsprechenden Drucker zugreifen und über die Druckerfreigabe drucken.

Druckprozess

Nachdem die Druckertreiber auf dem Client installiert wurden, kann der Druckauftrag an den Drucker (bzw. die Druckerfreigabe) versandt werden (1). Windowsclients erkennen hierbei den Druckdienst CUPS an der von Samba bereitgestellten Druckerfreigabe und übertragen die Druckdaten an CUPS (2). Alle ankommenden Druckaufträge werden von CUPS in einer Warteschlange abgearbeitet und an die Drucker weitergeleitet (3).

Die folgende Grafik zeigt Ihnen schematisch wie das Drucken der *paedML Linux* funktioniert.

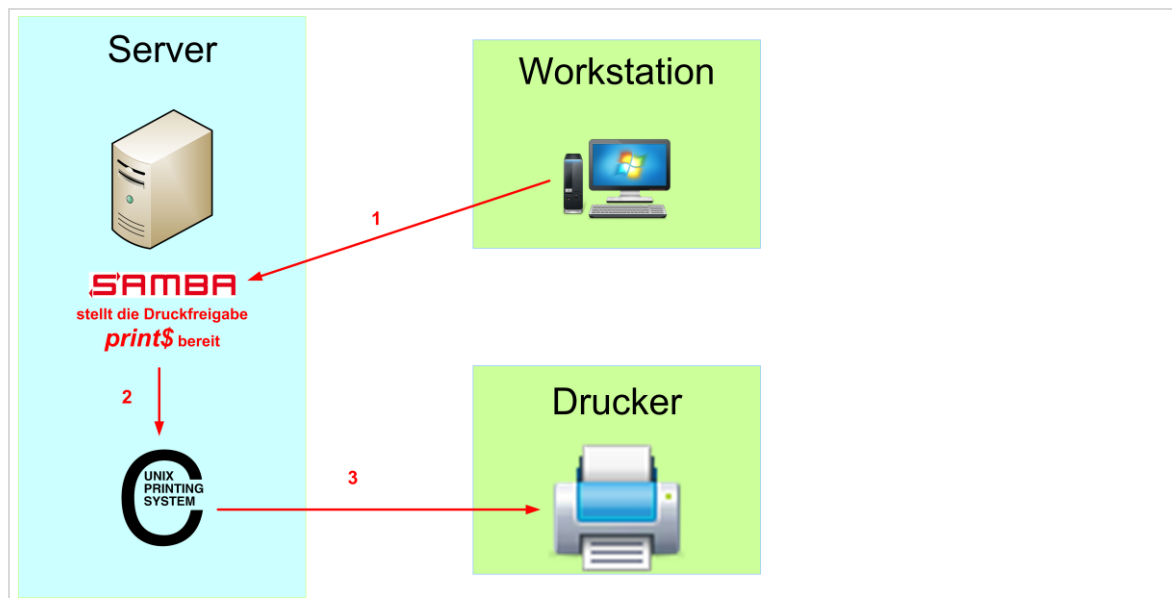


Abb. 169: Überblick über die Verwaltung von Druckaufträgen

³⁹ http://de.wikipedia.org/wiki/Common_Unix_Printing_System



Achten Sie bei der Anschaffung von Druckern darauf, dass diese netzwerkfähig und PCL/Postscriptfähig sind und ein netzwerkfähiger Treiber zur Verfügung steht.

Testen Sie vor dem Kauf, ob Sie die Druckertreiber in die Druckverwaltung einbinden können (siehe Kapitel 11.3 auf Seite 160). Dies ist die Voraussetzung für den uneingeschränkten Einsatz von Druckern in der *paedML Linux*.

(Optional, wenn auch *Linux*-Clients zum Einsatz kommen:

Achten Sie bei der Anschaffung von Druckern unbedingt darauf, dass diese mit Cups betrieben werden können. Es gibt Geräte, für die keine Treiber für *Linux* zur Verfügung stehen.

Eine Integration solcher Geräte in CUPS ist – wenn überhaupt – nur mit erheblichem Aufwand umsetzbar⁴⁰.

Es wird ausdrücklich empfohlen Drucker via Netzkabel an das Schulnetz anzuschließen und am Server einzurichten.

Checkliste: Ablauf der Druckereinrichtung

Die Einrichtung eines Druckers geschieht in vier Schritten:

- ☐ Aufnahme des Druckers in die Domäne („Gerät mit IP-Adresse“)
- ☐ Anlegen/Einrichten des Druckers im Drucker-Modul der Schulkonsole
- ☐ Bereitstellen von Druckertreibern für Windows
- ☐ Verteilung von Druckertreibern an die Clients über opsi
- ☐ Zuweisung der Drucker an Räume, damit der Druckertreiber an die Clients verteilt werden kann

11.1 Aufnahme des Druckers in die Domäne

Aufruf über Schulkonsole (netzwerkberater): Schul-Administration | Rechner (Schulen)

Bevor das Druckerprofil im System eingerichtet werden kann, muss das zugehörige Gerät (Drucker oder Printserver) in die *paedML* aufgenommen werden. Dies geschieht als netzwerkberater über die Rechnerverwaltung in der Schulkonsole im Menü „Schul-Administration | Rechner (Schulen)“.

Gehen Sie hierbei wie in Kapitel 4.2.2 „Rechneraufnahme über die Schulkonsole“, Seite 50 beschrieben vor. Der Unterschied zur Aufnahme eines Rechners liegt darin, dass für Drucker kein Computerkonto erstellt wird.

⁴⁰ Informationen zur Unterstützung durch CUPS und – sofern verfügbar – Treiber gibt es bei <http://www.linuxprinting.org>

Sie wählen also in der Maske, in der der Computertyp definiert wird, den letzten Eintrag „Gerät mit IP-Adresse“. Dieser ist für Netzwerkgeräte – in diesem Fall ein Drucker. Anschließend wird für das Gerät eine DHCP-Adresse reserviert und ein DNS-Eintrag erstellt.



Abb. 170: Drucker haben den Typ Gerät mit IP-Adresse, sonst ist die Einrichtung gleich wie in Kapitel 4.2.1

Wenn der Drucker in das Netzwerk aufgenommen wurde, muss das Gerät so konfiguriert werden, dass es die in der Schulkonsole zugewiesene IP-Adresse erhält und dadurch im Netzwerk erreichbar ist. Das Gerät sollte hierfür so konfiguriert sein, dass es seine Netzwerkeinstellungen über DHCP bezieht. Nähere Informationen hierzu entnehmen Sie bitte dem Handbuch Ihres Druckers.



Falls der Drucker nicht über eine Netzwerkkarte verfügt, können Sie mit einem Druckserver (Printserver) arbeiten, der die Daten für den Drucker über ein Netzwerkkabel entgegennimmt und an den Anschluss des Druckers weiterleitet.

11.2 Anlegen einer Druckerfreigabe

Aufruf über Schulkonsole (als Administrator): Geräte | Drucker

Die Verwaltung von Druckern geschieht ebenfalls über die Schulkonsole. Öffnen Sie hierfür den Menüpunkt „Geräte | Drucker“ als Administrator. Sie erhalten eine Auswahl von im System hinterlegten Druckern (mindestens ein „PDFDrucker“, der mit der paedML Linux ausgeliefert wird).

Beim Hinzufügen, Entfernen oder Bearbeiten einer Druckerfreigabe wird der Drucker automatisch auch in CUPS konfiguriert. Die Druckerfreigaben werden automatisch auch für Windows-Clients bereitgestellt. Dies geschieht mit dem Systemdienst Samba.

Über „Hinzufügen“ können Sie einen neuen Drucker einrichten.

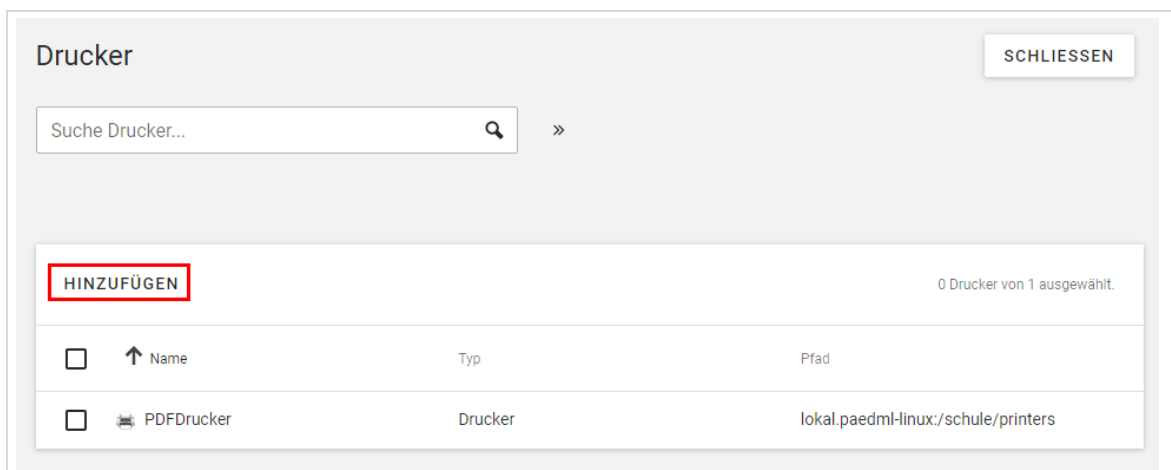


Abb. 171: Druckerverwaltung in der Schulkonsole

In den Einstellungen der nächsten Maske wählen Sie bitte unbedingt den Container „lokal.paedml-linux/schule/printers“ aus, damit der Drucker in der Schuldomäne verwaltet werden kann. Der Eintrag im Dropdownmenü „Druckertyp“ bleibt auf der Vorgabe „Druckerfreigabe: Drucker“. Weiter mit „Weiter“.



Abb. 172: Systemeigenschaften des Druckers (hier bitte den Container ändern)

Über die folgende Maske wird das Druckerprofil angelegt. Bitte tragen Sie hierbei die Werte ein, die für Ihren Drucker zutreffend sind. Die für die Konfiguration notwendigen Werte finden Sie in Tabelle 15: Attribute für die Einrichtung eines Druckerprofiles (Attribute mit * müssen eingetragen werden) auf Seite 160.

Der Eintrag für „Protokoll“ ist davon abhängig, wie Sie den Drucker an das Netzwerk anschließen. Drucker, die an einer Netzwerkdose hängen, werden anders angesprochen als Drucker, die mit Computern verbunden sind. Das Protokoll ist in diesem Fall abhängig vom Drucker. Die meisten Modelle nutzen das Protokoll „socket://“, einige neuere Modelle arbeiten mit dem Protokoll „http://“.

Entnehmen Sie bitte dem Handbuch des Druckers die genaue Protokollunterstützung.

Die IP-Adresse („Ziel“) entspricht dem Wert, den Sie bei der Aufnahme des Gerätes in die Domäne vergeben haben (Vgl. Kapitel 11.1 auf Seite 156).

Als Drucker-Hersteller müssen Sie den Wert „misc“ und als Modell den Wert „None“ eintragen. Falls Sie Linux-Clients und/oder die Druckermoderation nutzen wollen, müssen hier die richtigen Einstellungen für den benutzten Drucker eingetragen werden. Abschließend speichern Sie mit einem Klick auf „Drucker erstellen“.

Drucker: drucker-bib

DRUCKER ERSTELLEN

HILFE

ZURÜCK

Allgemein

Zugriffskontrolle

Richtlinien

Grundeinstellungen

Informationen über die Verwaltung von Windows-Druckertreibern und eine Anleitung zur Fehlerbehebung finden Sie [hier](#).

Grundeinstellungen - Druckerfreigabe ⌵

Name *

Windows-Name

⌵

Druckserver

✖

NEUER EINTRAG

⌵

Protokoll *

Ziel *

⌵

Drucker-Hersteller

⌵

Drucker-Modell *

Standort

Beschreibung

Abb. 173: Eingabe der Druckereinstellungen

Die folgende Tabelle gibt eine Übersicht über die einzelnen Felder, die in der Maske der Druckergrundeinstellungen vorhanden sind.

Attribut	Beschreibung
Name (*)	Dieses Feld enthält den Namen für die Druckerfreigabe. Dieses Feld wird nach dem Speichern gesperrt. Unter diesem Namen erscheint der Drucker unter Windows und Linux. Der Name der Druckerfreigabe darf nur Buchstaben und Zahlen sowie Binde- und Unterstriche enthalten.
Windows-Name	Lassen Sie dieses Feld leer!
Server (*)	Der Druckdienst muss auf dem Master-Server („server“) ausgeführt werden.
Protokoll und Ziel (*)	In diesem Feld wird definiert, wie der Druckserver auf den Drucker zugreift.
Drucker-Hersteller (*)	Der empfohlene Wert: „misc“.
Drucker-Modell (*)	Der empfohlene Wert: „None“
Quota aktivieren	Wird i.d.R. nicht verwendet.
Preis pro Druckauftrag	Wird i.d.R. nicht verwendet.
Standort	Diese Angabe wird von einigen Anwendungen bei der Druckerauswahl angezeigt. Sie kann mit einem beliebigen Text gefüllt werden.

Attribut	Beschreibung
Beschreibung	Diese Angabe wird von einigen Anwendungen bei der Druckerauswahl angezeigt. Sie kann mit einem beliebigen Text gefüllt werden.

Tabelle 15: Attribute für die Einrichtung eines Druckerprofiles (Attribute mit * müssen eingetragen werden)

11.3 Bereitstellen von Druckertreibern für Windows⁴¹



Testen Sie vor dem Kauf, ob Sie die Druckertreiber in die Druckverwaltung einbinden können (siehe Kapitel 11.3.1 auf Seite 161). Dies ist die Voraussetzung für den uneingeschränkten Einsatz von Druckern in der paedML Linux.

Achten Sie bei der Bereitstellung von Treibern auf jeden Fall darauf, dass diese aktuell sind.

Bitte verwenden Sie nur Treiber vom „Typ 3“.

Vorgehensweise

Doppelklicken Sie auf die Verknüpfung „Druckverwaltung“ in „Admin-Tools“.

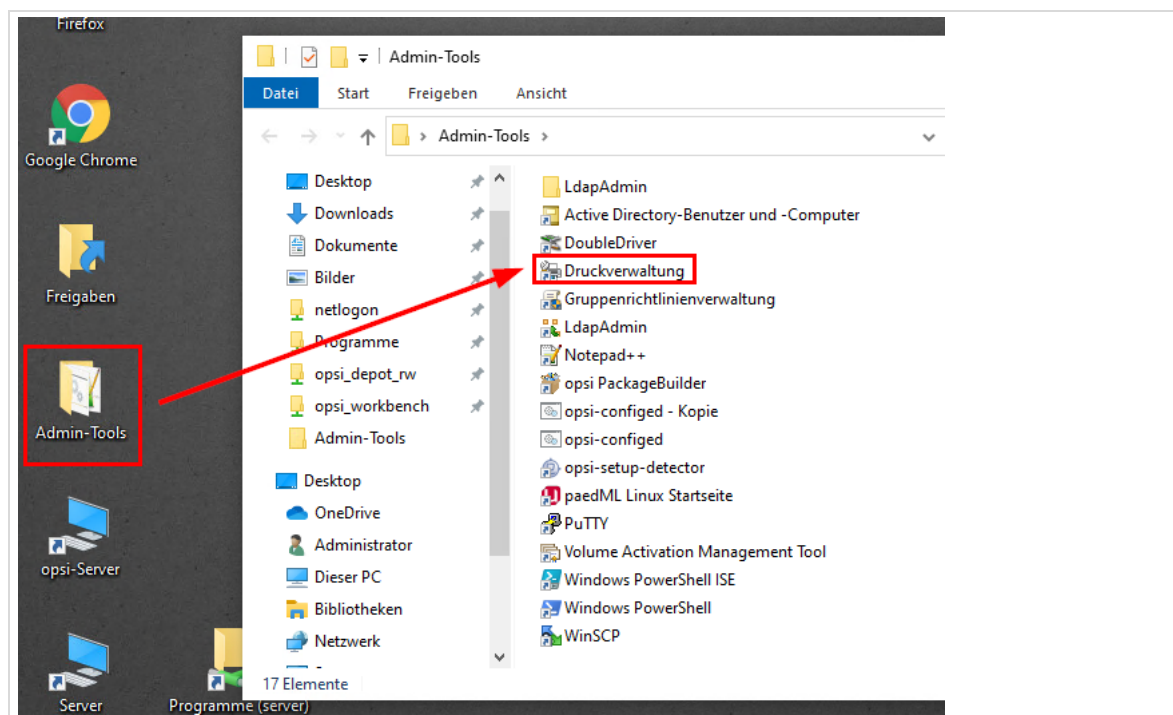


Abb. 174: Starten der Druckverwaltung

⁴¹ Ein weiteres Verfahren, um Druckertreiber auf den Server zu laden, ist unter <http://sdb.univention.de/1309> beschrieben. Dieses Verfahren kann Anwendung finden, wenn das hier beschriebene Prozedere fehlschlägt.

Es öffnet sich das Fenster „Druckerverwaltung“.

11.3.1 Treiber hochladen

Ein Rechtsklick auf den Eintrag „Druckerverwaltung | Druckserver | SERVER | Treiber“ und die Auswahl von „Treiber hinzufügen“ startet den Dialog für die Treiberinstallation.

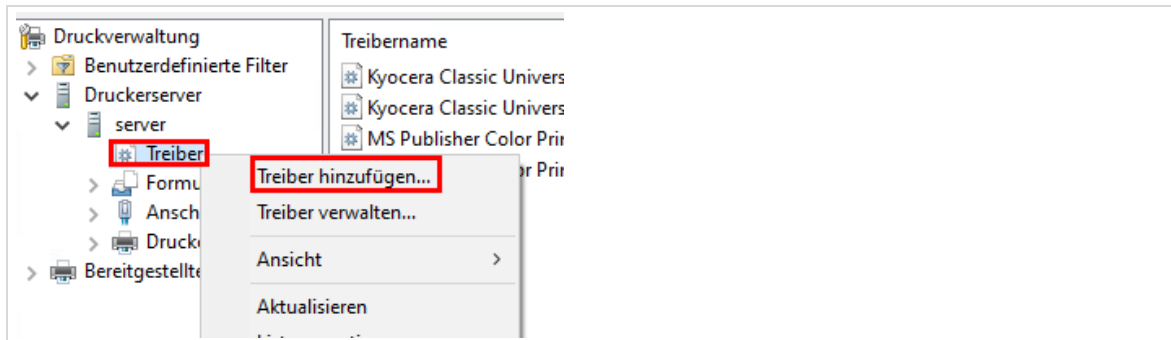


Abb. 175: Treiber hinzufügen

Es öffnet sich ein Dialogfenster „Assistent für die Druckertreiberinstallation“. Drücken Sie hier auf „Weiter“.

Im nächsten Dialog werden Sie nach der Prozessor-Architektur gefragt. Wählen Sie den Prozessor-Typ, bzw. die Windows-Version (x64).

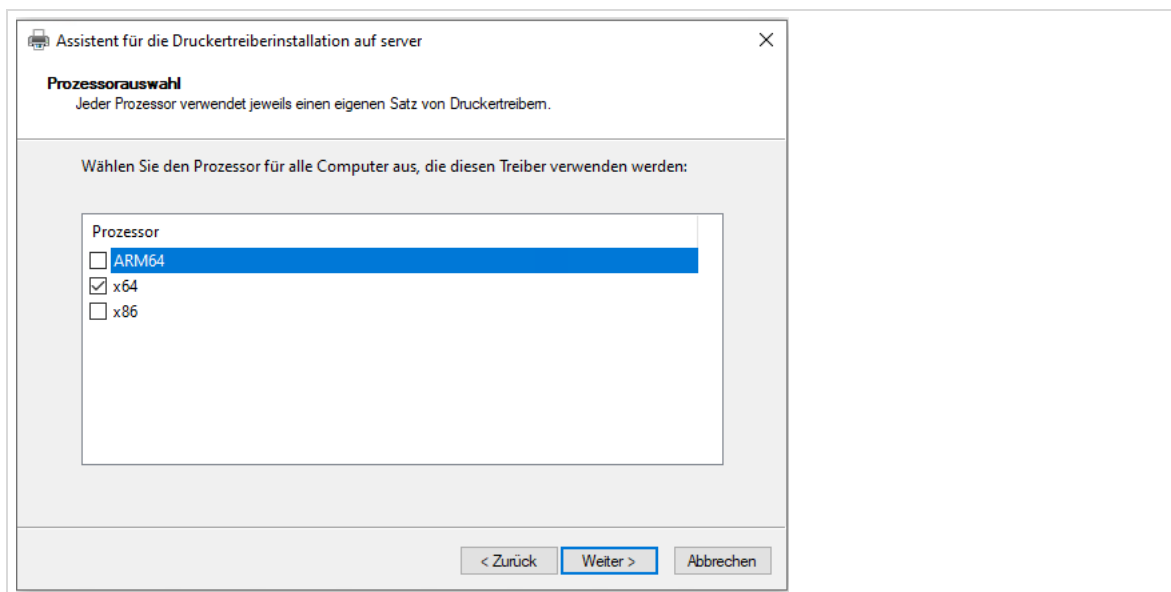


Abb. 176: Prozessorauswahl, bzw. Auswahl des eingesetzten Betriebssystems

Im nächsten Dialog wird der Speicherort des Treibers ausgewählt. Gegebenenfalls muss noch das Druckermodell ausgewählt werden. Installieren Sie den Treiber für Ihr Druckermodell.



Es wird ausdrücklich empfohlen den aktuellen Treiber vom Druckerhersteller zu laden und zu installieren.

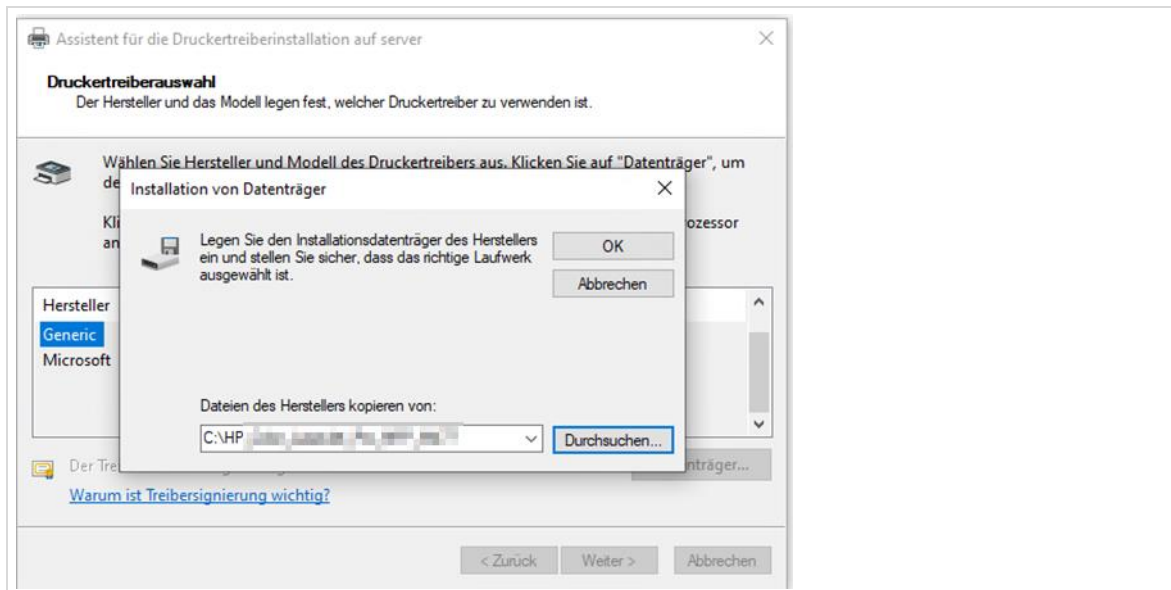


Abb. 177: Treiberauswahl

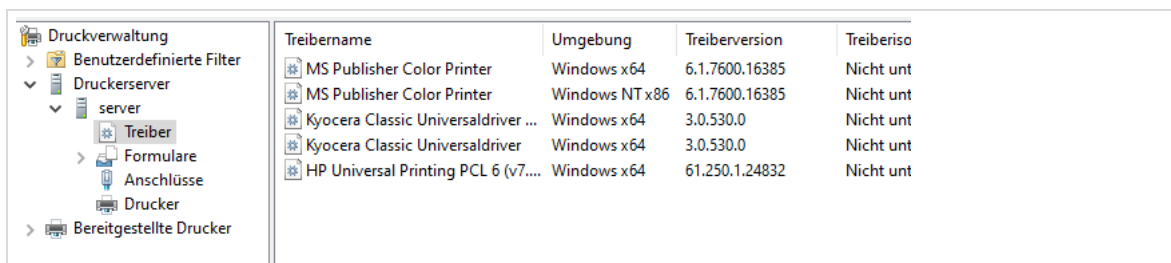


Abb. 178: Der Treiber wurde erfolgreich auf den Server geladen

11.3.2 Treiber an Drucker zuweisen

Wählen Sie den einzurichtenden Drucker, drücken Sie die rechte Maustaste und wählen Sie „Eigenschaften“.

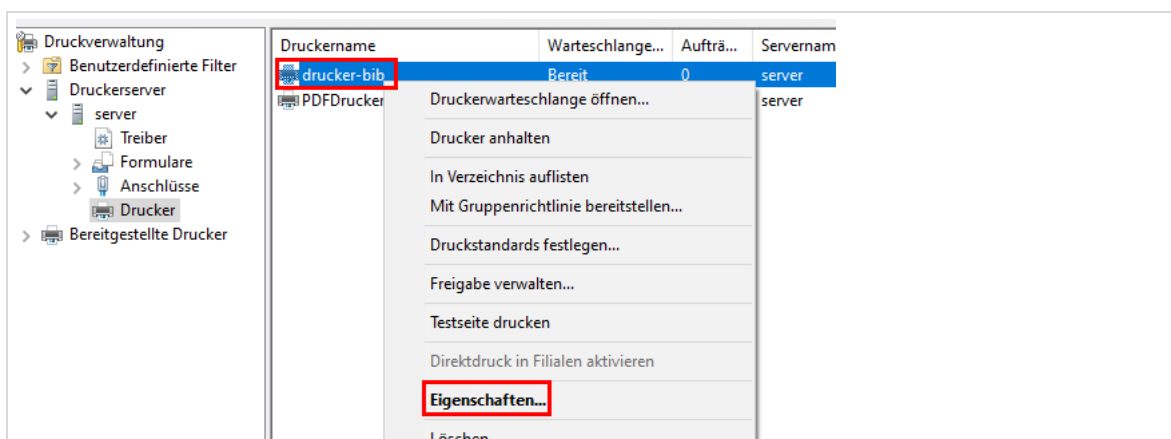


Abb. 179: Auswahl des Druckers

Es erscheint ein Dialogfenster, in dem darauf hingewiesen wird, dass kein Treiber installiert ist. Bestätigen Sie den Dialog mit „Nein“, da der Treiber bereits im vorigen Abschnitt hochgeladen wurde.

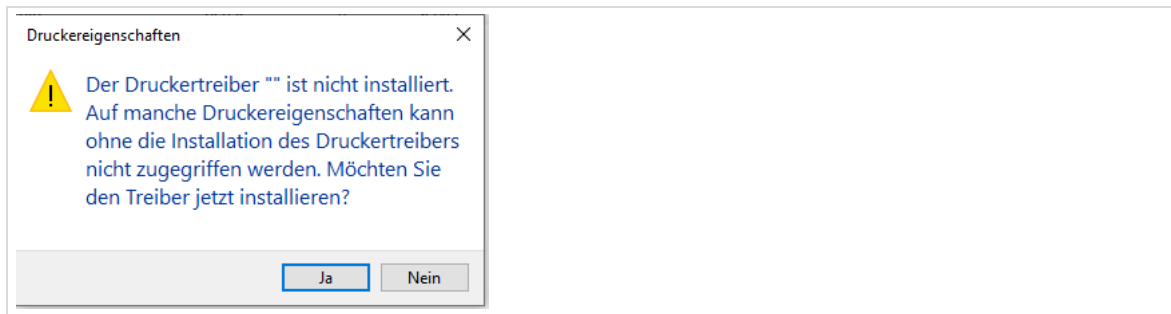


Abb. 180: Kein Druckertreiber? Kein Problem!

Anschließend öffnet sich ein Fenster mit den „Eigenschaften von ‚NEUER DRUCKER‘ an SERVER“. Öffnen Sie dort den Reiter „Erweitert“ und wählen Sie den im vorigen Abschnitt hinterlegten „Treiber“.

Wenn der Treiber eingetragen wurde, können Sie den Dialog mit „OK“ schließen. Die Einrichtung des Druckers unter Samba ist hiermit abgeschlossen.

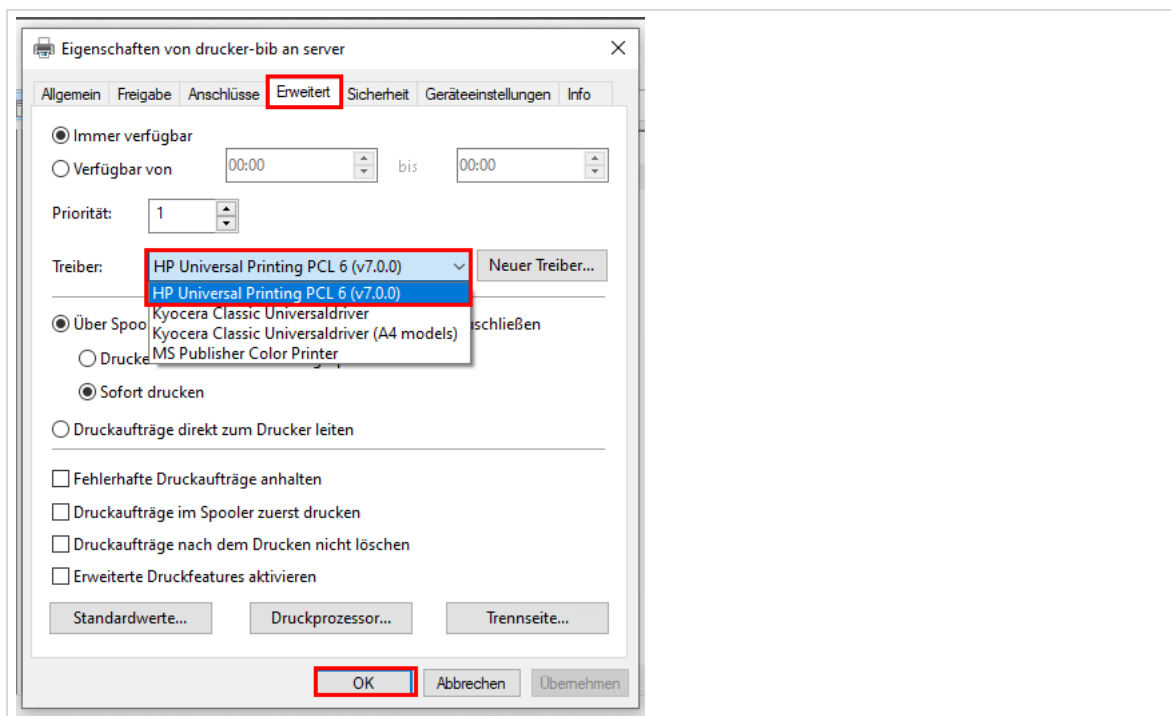


Abb. 181: Überprüfen des Druckertreibers

Eventuell erscheint eine Warnmeldung „Vertrauen Sie diesem Drucker?“. Bestätigen Sie die Meldung mit „Treiber installieren“.

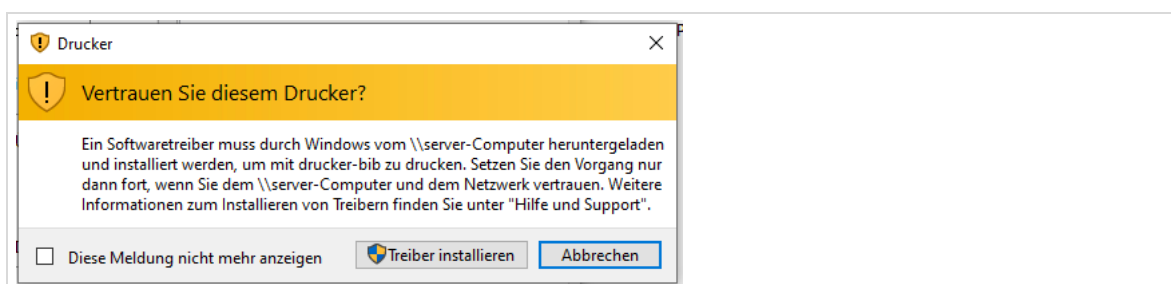


Abb. 182: Warnmeldung

11.3.3 Standardeinstellungen setzen

Manchmal ist es nötig, die Standardeinstellungen in einem Druckertreiber zu verändern. Es kann zum Beispiel vorkommen, dass anstatt des Papierformats „A4“ das Format „Letter“ eingestellt ist. Um diese Einstellung zu korrigieren, klicken Sie in der Druckerverwaltung mit der rechten Maustaste auf den Drucker (1), wählen dann im Reiter „Geräteeinstellungen“ (2) das gewünschte Papierformat aus (3) und bestätigen Sie den Dialog mit „OK“. Selbstverständlich können an dieser Stelle, je nach Druckertreiber, weitere Einstellungen gesetzt werden. Die Einstellungen gelten dann für alle Clients im Netzwerk, die sich mit diesem Drucker verbinden.

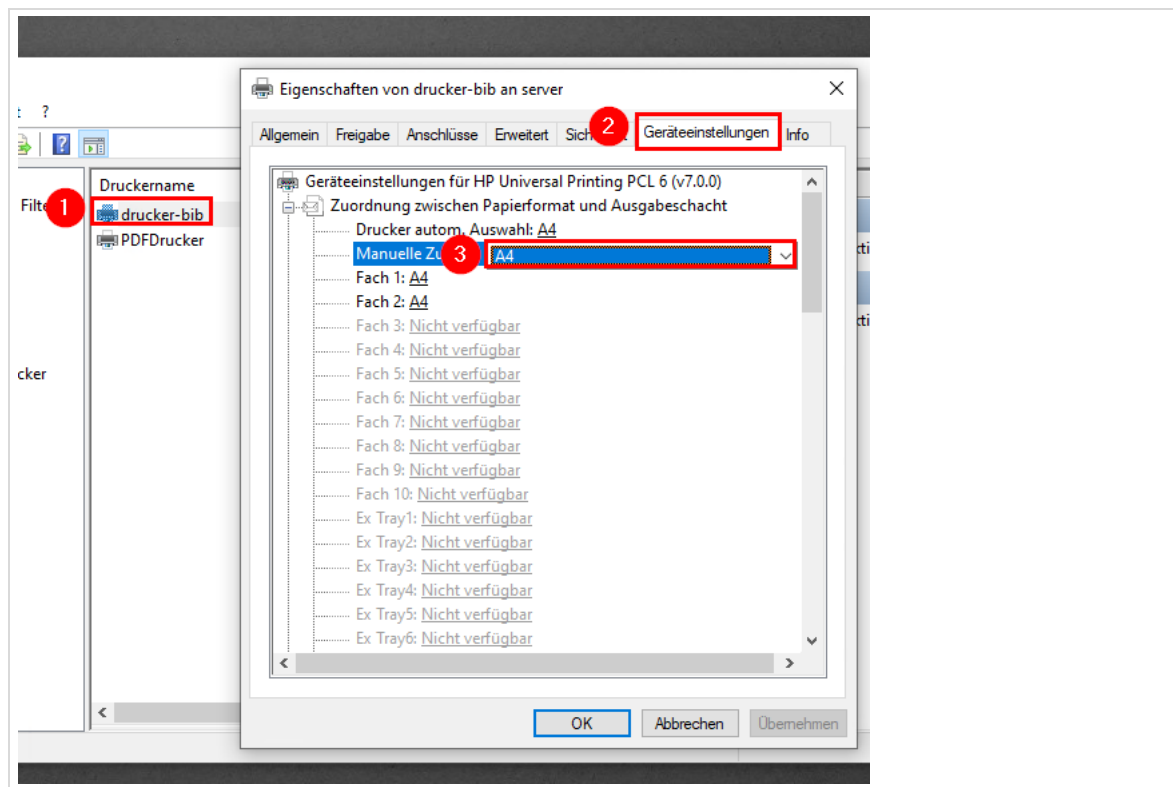


Abb. 183: Papierformat ändern

11.4 Verteilung von Druckertreibern an Clients über opsi

Das opsi-Paket „druckertreiber“ installiert die sich auf dem opsi-Depot im Verzeichnis „files“ befindenden Druckertreiber auf Windows-Clients. Die Auswahl der Treiber, die installiert werden sollen, erfolgt im opsi-configed über die Property „treiberliste“ - dort sind die Pfade zu den Inf-Dateien der Druckertreiber unterhalb von „druckertreiber“ einzutragen.

Vorgehensweise:

1. opsi-Paket „druckertreiber“ auf den Clients einspielen (z.B. mit Hilfe des opsi-configed), es entsteht der Ordner „druckertreiber“ auf dem opsi-Depot (`\\backup\opsi_depot-rw`)

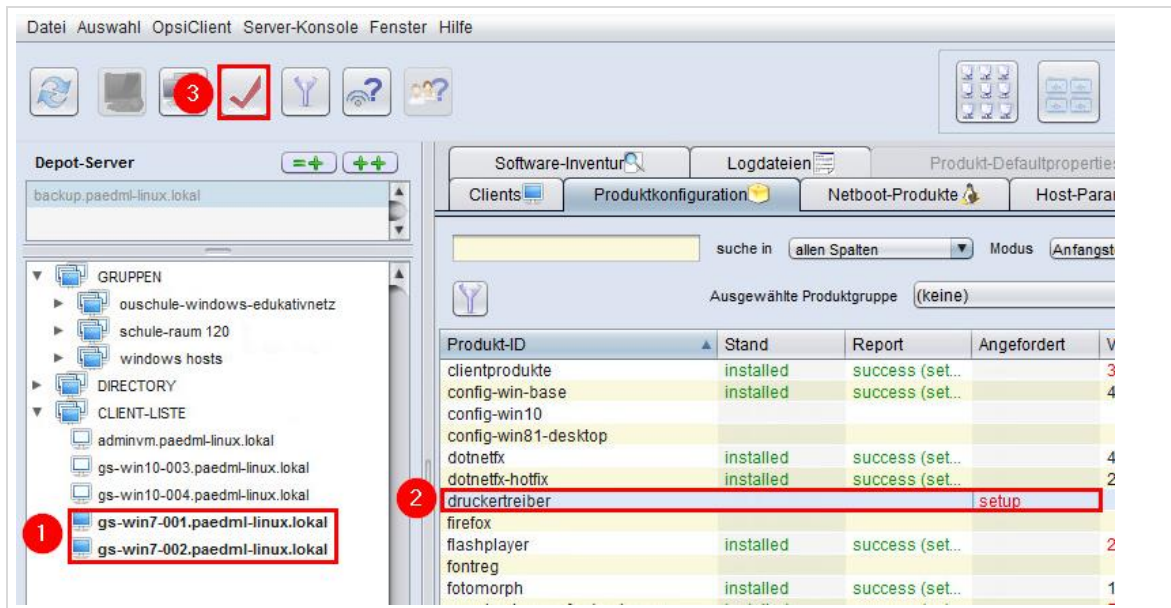


Abb. 184: opsi-Paket „druckertreiber“ auf den Clients installieren

2. Gesamten Druckertreiber (nicht nur die Inf-Datei) entpackt ablegen in eigenem Verzeichnis passend zum Druckernamen (keine Umlaute, Leer- oder Sonderzeichen. z.B. „brotherHL3040cn“) unterhalb von `\\backup\opsi_depot_rw\druckertreiber\druckertreiber`.

Dieser Treiber muss derselbe sein, der auch in der Druckverwaltung verwendet wurde!

3. Opsi-Rechte über den opsi-config-editor setzen.

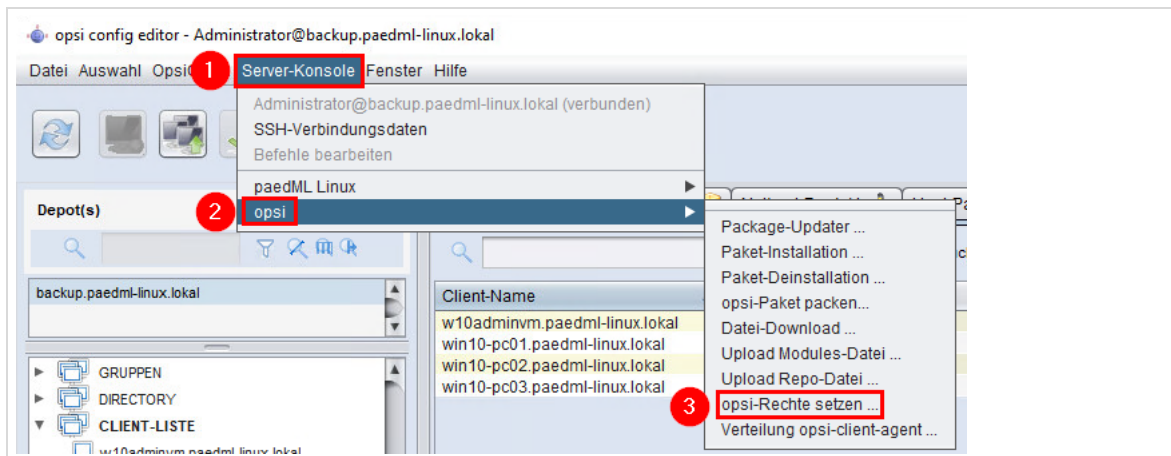


Abb. 185: Opsi-Rechte setzen

4. Im opsi-Configed unter Produkteigenschaften beim Produkt „druckertreiber“ die Property „treiberliste“ mit den Verzeichnisnamen (ggf. mit Pfad bei Unterverzeichnissen) füllen, in der die Inf-Dateien des jeweiligen Druckertreibers liegen.
 - **Beispiel:** Die Inf-Dateien liegen unter `\\backup\opsi_depot_rw\druckertreiber\druckertreiber\brotherHL3040cn`
 - Somit wird in die Property „treiberliste“ eingetragen: `brotherHL3040cn`
Erstellen Sie pro Verzeichnis einen neuen Eintrag (Plus-Zeichen), dann wählen Sie alle zur Installation gewünschten Einträge außer „beispieltreiber“ aus.

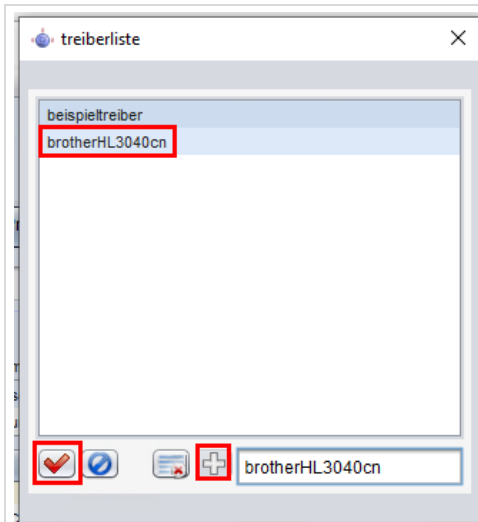


Abb. 186: Eintrag erstellen

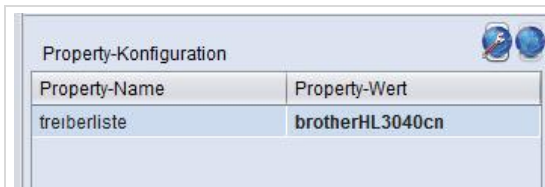


Abb. 187: Eintrag in „treiberliste“

5. Setzen Sie das Paket „druckertreiber“ auf „setup“ und speichern Sie die Konfiguration.

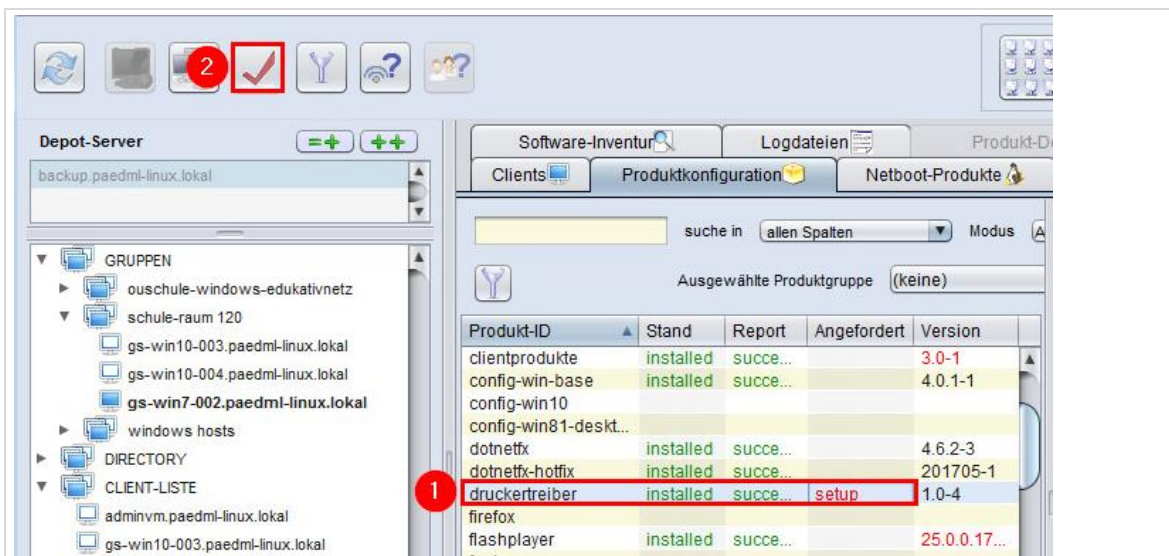


Abb. 188: Druckertreiber auf die Clients verteilen

11.5 Druckerzuordnung an Räume

Aufruf über Schulkonsole (als Administrator): Benutzer | Gruppen

Die Zuordnung von Druckern an Räume geschieht über das Schulkonsolenmenü „Benutzer | Gruppen“.

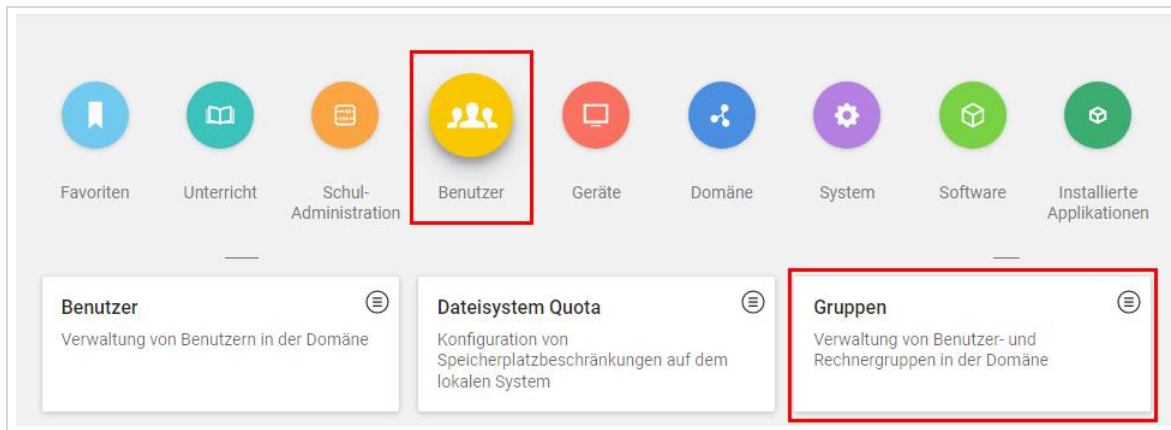


Abb. 189: Drucker werden über Gruppen an Räume zugewiesen

Wenn Sie dieses Modul öffnen, dann bekommen Sie alle Gruppen der *paedML Linux* angezeigt. Hierzu gehören Benutzergruppen, Klassen und Räume. Letztere benötigen wir, um einen Drucker einem Raum zuzuweisen.

Sie können die Anzeige auf Räume begrenzen, indem Sie auf das Feld „Erweiterte Optionen“ klicken...

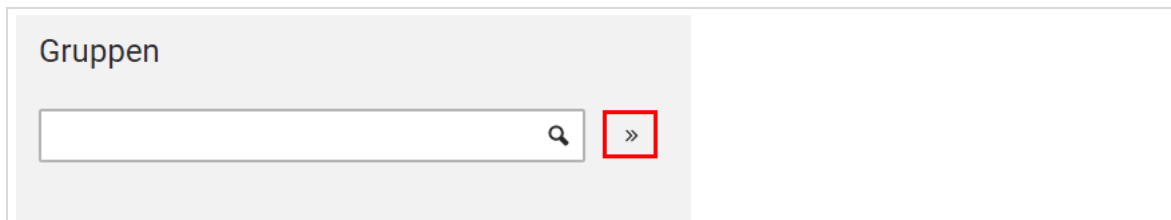


Abb. 190: Erweiterte Optionen

...und im Dropdown-Menü „Suche In:“ den Container „*lokal.paedml-linux:/schule/groups/raeume*“ auswählen. Wenn Sie auf „Suche“ klicken, werden nur noch Computerräume angezeigt. Räume haben das Präfix „*schule-*“, zum Beispiel „*schule-PC-Raum*“.

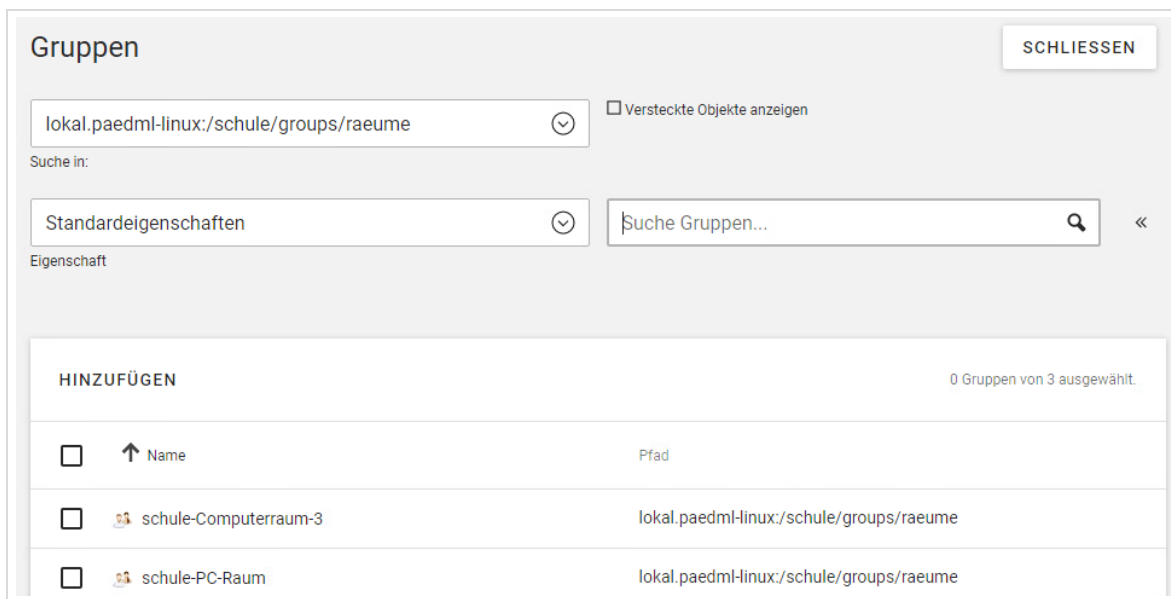


Abb. 191: Einschränken der Anzeige auf Computerräume

Anschließend können Sie den Raum auswählen, dem Sie den Drucker zuordnen wollen. Klicken Sie auf den Raum und navigieren Sie zum Reiter „Druckerzuordnung“. Im Drop-Down-Menü „Zugewiesene Drucker“ können Sie einen Drucker auswählen und mit „Speichern“ dem Raum zuweisen.



Abb. 192: Auswahl des Druckers

Führen Sie abschließend bitte eine exe-Datei aus, die die Drucker zusätzlich über Gruppenrichtlinien verbindet. Führen Sie die Datei jedes Mal aus, wenn Sie Änderungen an Druckerzuordnungen vornehmen.

Sie finden die Datei in `\\backup\opsi_depot_rw\update72\DruckerSetup`.

1. Führen Sie die Datei aus, indem Sie auf die Datei doppelklicken.

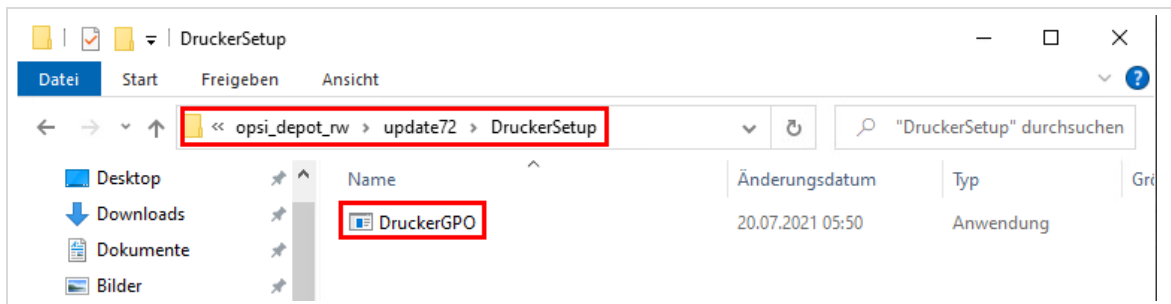


Abb. 193: Starten der ausführbaren Datei

2. Es öffnet sich ein Konsolenfenster. Folgen Sie den Anweisungen. Es schließt sich selbst, nachdem alle Befehle ausgeführt wurden.
3. Drucker werden nun zusätzlich über Gruppenrichtlinien verbunden.



Hinweis: Die Datei DruckerGPO.exe muss nach jeder Veränderung der Druckerzuordnung, nach dem Anlegen oder Löschen von Druckern erneut ausgeführt werden. Dies kann automatisiert werden, indem die Datei zeitgesteuert z.B. alle 15 Minuten an der AdminVM ausgeführt wird.

Der Drucker ist anschließend dem Raum zugeordnet. Beim Login der Benutzer wird der dem Raum zugeordnete Drucker auf dem Rechner eingerichtet und der Treiber wird installiert.

12 Aktivierung von Windows / MS-Office

Die Aktivierung eines frisch installierten Microsoft-Produktes kann grundsätzlich mit einem der nachstehend genannten Verfahren durchgeführt werden:

- Händisch an jedem Client (nicht empfohlen, wird im Folgenden nicht beschrieben)
- Zentral über einen KMS-Server (Volumenlizenz-Kunden)
- Zentral über einen MAK-Proxy (Volumenlizenz-Kunden)



Um *Microsoft*-Produkte – wie hier beschrieben – zu lizenzieren benötigen Sie **Volumenlizenzen**. Diese erhalten Sie in der Regel über Ihren Schulträger.

Die Lizenzierung von *Microsoft*-Produkten ist in der Regel Aufgabe des Dienstleisters. Das Support-Netz haftet nicht für etwaige Folgen einer fehlerhaften Anwendung der hier beschriebenen *Microsoft*-Aktivierungswerkzeuge. Informieren Sie sich ausgehend, zum Beispiel unter:

<https://docs.microsoft.com/de-de/licensing/products-keys-faq#what-are-product-keys>

Bitte beachten Sie, dass Office 2019 **nicht** mit dem MAK-Proxy-Verfahren aktiviert werden kann. Die Aktivierung ist nur per KMS-Server möglich (siehe Kapitel 12.2 auf Seite 179.)

12.1 MAK-Proxy und VAMT-Service

Die Aktivierung von Clients über einen *MAK-Proxy* erfolgt mithilfe des auf der *W10AdminVM* bereits vorinstallierten und vorkonfigurierten *Volume Activation Management Tools*.



Um das Schulnetz nach lizenzpflichtigen *Microsoft*-Produkten zu durchsuchen, müssen alle Rechner, die lizenziert werden sollen, eingeschaltet sein.

12.1.1 Suche nach *Microsoft*-Produkten

Öffne Sie das *Volume Activation Management Tool* im Ordner *Admin-Tools* auf der *W10AdminVM*.

Das *Volume Activation Management Tool* startet beim ersten Aufruf ohne Wissen um die installierten Programme. Dies kann im mittleren Fenster abgelesen werden. Die Einträge unter „*VAMT Inventory*“ und „*Licence overview*“ sind jeweils mit „0“ befüllt.

Es empfiehlt sich zunächst eine Neue „*Database*“ anzulegen. Klicken Sie dazu auf den Link „*Successfully connected to Server...*“

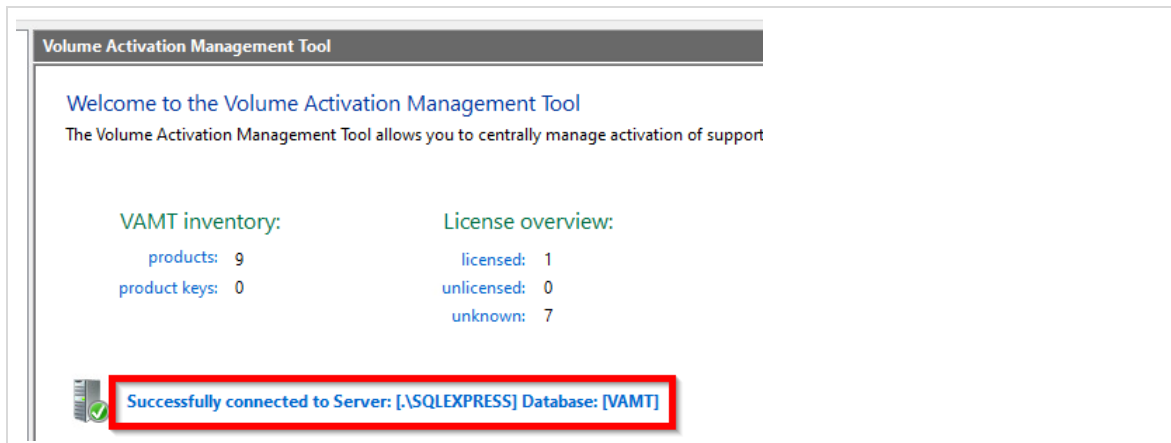


Abb. 194: Erster Aufruf von VAMT

Erstellen Sie nun eine neue „Database“. Wählen Sie dazu einen aussagekräftigen Namen.

Um das Netzwerk nach Rechnern zu scannen, drücken Sie im linken Bereich des Fensters mit der rechten Maustaste auf den Eintrag „Products“ und im Kontextmenü auf „Discover Products“.

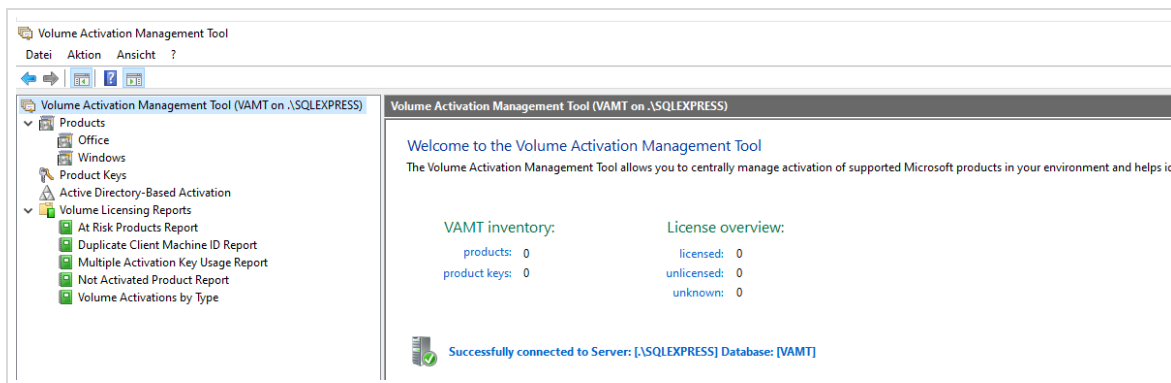


Abb. 195: Erster Aufruf von VAMT

Es geht ein neues Fenster auf. Achten Sie darauf, dass die Felder – wie im folgenden Screenshot mit „Search for computers in the Active Directory“ und dem Namen der Domäne im Feld „Search for computers in this domain“ befüllt sind.

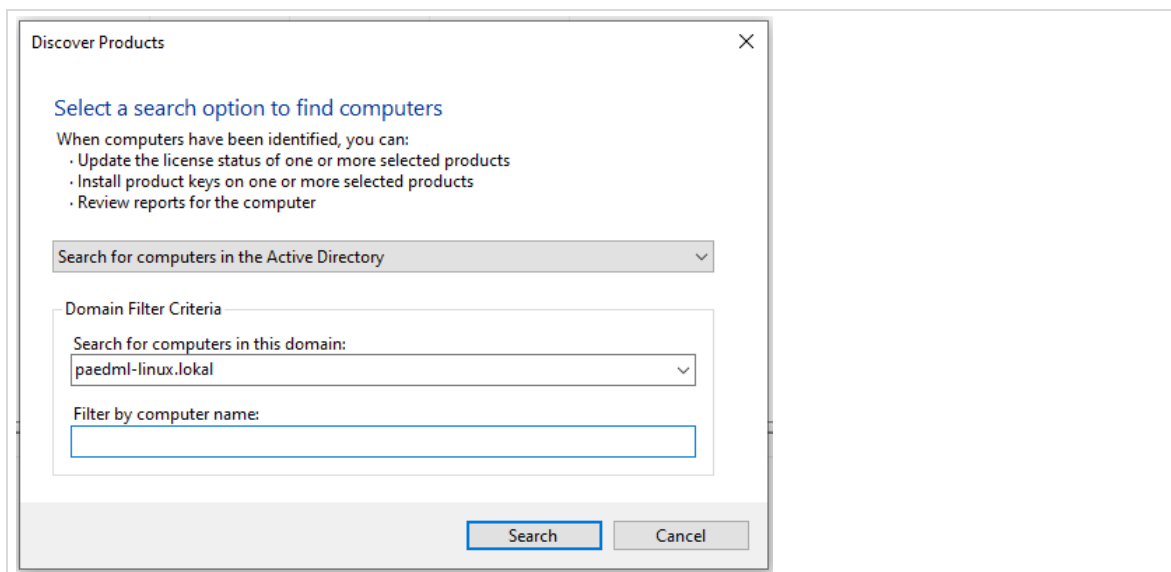


Abb. 196: Suchen nach eingeschalteten Computern

Im mittleren Bereich des VAMT-Fensters werden nun die erkannten Rechner angezeigt, wobei noch keine Informationen über die installierten Produkte vorliegen.

Products						
Group by: Product ▾						
Computer Name	Product Name	Product Key Ty...	License Status	Genuine Status	Status of Last Action	Date of Last License Stat...
Windows (8)						
backup		Unknown	Unknown	Not available		Not available
ersatz07		Unknown	Unknown	Not available		Not available
Ersatz08		Unknown	Unknown	Not available		Not available
horde-52296866		Unknown	Unknown	Not available		Not available
SERVER		Unknown	Unknown	Not available		Not available
ter03		Unknown	Unknown	Not available		Not available
ter04		Unknown	Unknown	Not available		Not available
w10adminvm		Unknown	Unknown	Not available		Not available

Abb. 197: VAMT zeigt nach Suchvorgang alle Rechner der Domäne, die an und somit erreichbar sind

Markieren Sie den Rechner und wählen Sie (entweder über das Kontextmenü – mit der rechten Maustaste über markierte Rechner – oder im rechten Bereich des VAMT-Fensters) den Eintrag „Update license status / Update current credential“. Hier können auch mehrere Rechner gleichzeitig bearbeitet werden.

Wählen Sie nun *Close*.

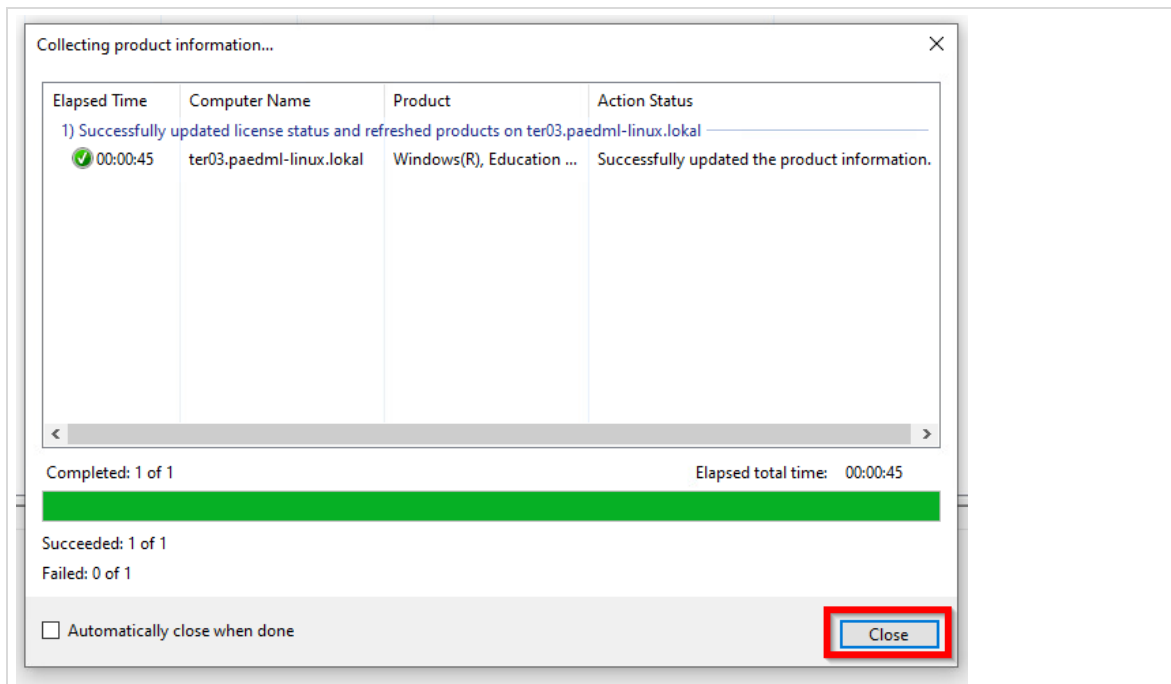


Abb. 198: Ergebnis Collecting product information

An dieser Stelle sei nochmal der Hinweis gegeben, dass die Rechner an sein müssen, um auf diesem Wege erreichbar zu sein.

Im Beispiel wurden Informationen über den Rechner *ter03* eingeholt.

Products						
Group by: Product						
Computer Name	Product Name	Product Key Ty...	License Status	Genuine Status	Status of Last Action	Date of Last License Stat
Office (1)						
ter04.paedml-linux.lokal	Office 16, Office160365ProPlusR...	Retail	Notification	Non Genuine	Successfully updated the product informat...	05.02.2021 16:25:40
Windows (7)						
backup		Unknown	Unknown	Not available		Not available
ersatz07		Unknown	Unknown	Not available		Not available
Ersatz08		Unknown	Unknown	Not available		Not available
ccoupe		Unknown	Unknown	Not available		Not available
ter03.paedml-linux.lokal	Windows(R), Education edition	GVLK	Licensed	Genuine	Successfully updated the product informat...	12.02.2021 11:54:56
ter04.paedml-linux.lokal	Windows(R), Education edition	GVLK	Licensed	Genuine	Successfully activated the product with Kivi...	05.02.2021 16:26:03
w10adminvm		Unknown	Unknown	Not available		Not available

Abb. 199: Der Rechner ter03

12.1.2 Eingabe der Lizenzschlüssel

Nachdem nun die Produktinformationen gesammelt wurden, können Sie Ihre Lizenzschlüssel eingeben.

Dies geschieht über den Menüpunkt „Product Keys“ im linken Feld des VAMT-Fensters. Aktivieren Sie diesen Eintrag und klicken Sie entweder mit der rechten Maustaste darauf oder wählen Sie im linken Bereich des Fensters den Menüpunkt „Add Product Keys“.

Es öffnet sich ein neues Fenster, in dem Sie einen oder mehrere Lizenzschlüssel untereinander eingeben können. Bestätigen Sie die Eingabe mit „Add Key(s)“.

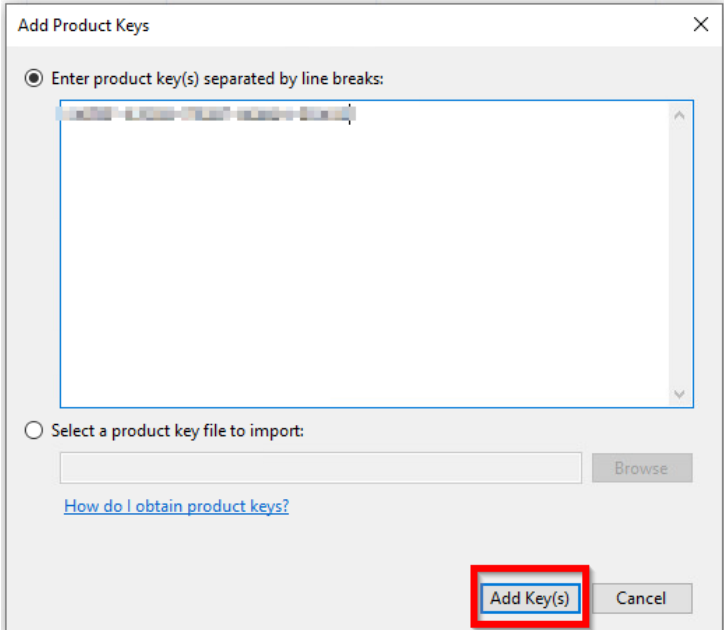


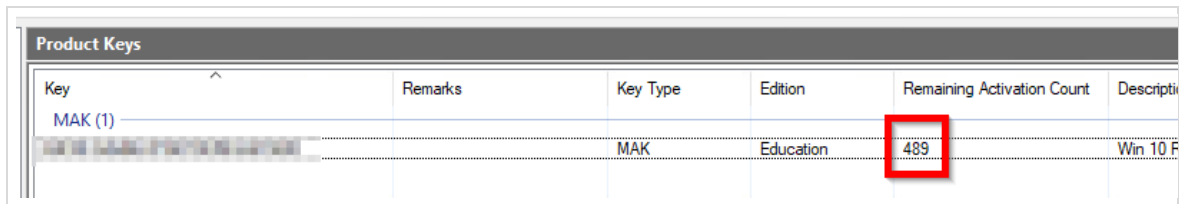
Abb. 200: Eingabe der Lizenzschlüssel

Die Lizenzschlüssel werden bei Microsoft auf Gültigkeit überprüft und – sofern diese Überprüfung erfolgreich ist – in VAMT hinterlegt. Sie sehen im Anschluss im vorher leeren Feld „Product Keys“ Informationen zu den eingetragenen Lizenzschlüsseln.

Product Keys					
Key	Remarks	Key Type	Edition	Remaining Activation Count	Description
MAK (1)		MAK	Education	Not available	Win 10 RTM Education Volume:MAK

Abb. 201: Informationen zum Lizenzschlüssel – ohne Angabe über verbleibende Aktivierungen

Die Spalte „Remaining Activation Count“ zeigt an, wie oft der eingegebene Schlüssel noch aktiviert werden kann. Sollte hier kein Wert eingetragen sein, können Sie mit der rechten Maustaste und dem Eintrag „Refresh product key data online“ die Lizenzinformationen aktualisieren.



Key	Remarks	Key Type	Edition	Remaining Activation Count	Description
MAK (1)		MAK	Education	489	Win 10 F

Abb. 202: Informationen zum Lizenzschlüssel – mit Angabe über verbleibende Aktivierungen

12.1.3 Aktivierung der Lizenzen

Nachdem nun zunächst die Informationen über die Rechner gesammelt wurden und anschließend die Lizenzschlüssel hinterlegt haben, geht es darum, die beiden zu verheiraten und die Software zu lizensieren.

Um die Lizenz auf den Rechnern auszuspielen, wählen Sie im linken Fenster von VAMT den Menüpunkt „Products“ und wählen Sie die zu aktivierenden Maschinen. Mit dem Eintrag „Install Product Key“ (rechte Maustaste oder Einträge im rechten Bereich des Fensters) können Sie den ausgewählten Rechnern einen Produktschlüssel zuweisen. Drücken Sie auf „Install Product Key“, um den Schlüssel zu verteilen.

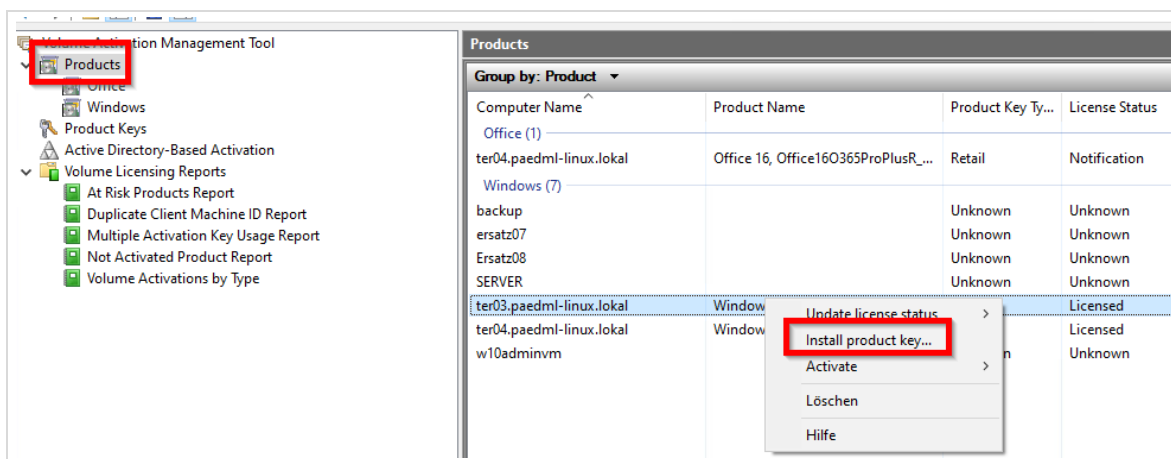


Abb. 203: Zuweisung eines Lizenzschlüssels

Es öffnet sich ein Fenster mit den im System hinterlegten Lizenzschlüsseln. Hier müssen Sie den Schlüssel wählen, den Sie auf den Rechner einspielen wollen. Es kann immer nur ein Schlüssel ausgespielt werden. Daher muss der Vorgang für Betriebssystem und Office-Programm getrennt voneinander ausgeführt werden.

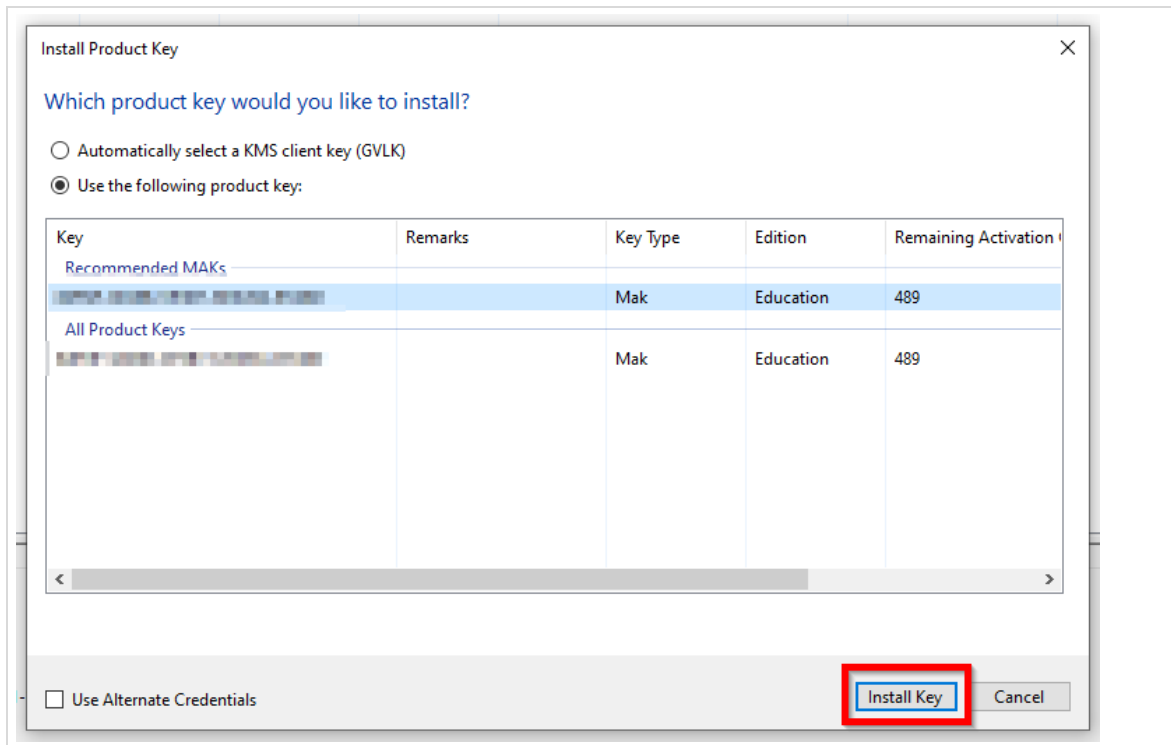


Abb. 204: Auswahl des Lizenzschlüssels

Wählen Sie das Produkt, das Sie installieren wollen und drücken Sie auf „Install Key“.

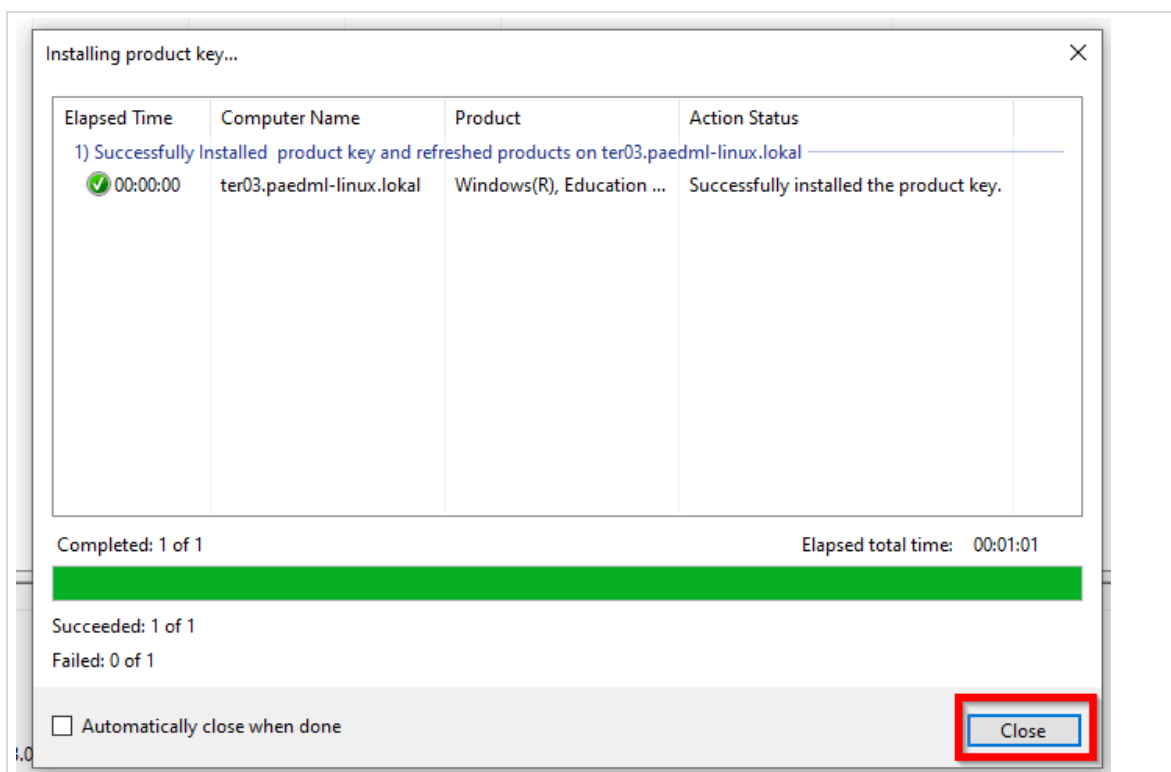


Abb. 205: Schlüssel erfolgreich auf dem Rechner installiert.

Nun ist der Lizenzschlüssel auf den Rechnern hinterlegt und muss im letzten Schritt nur noch aktiviert werden. Hierfür sind wiederum die zu aktivierenden Rechner zu markieren und mit dem Kontextmenü der rechten Maustaste ist der Eintrag „Activate | Proxy activate“ zu wählen.

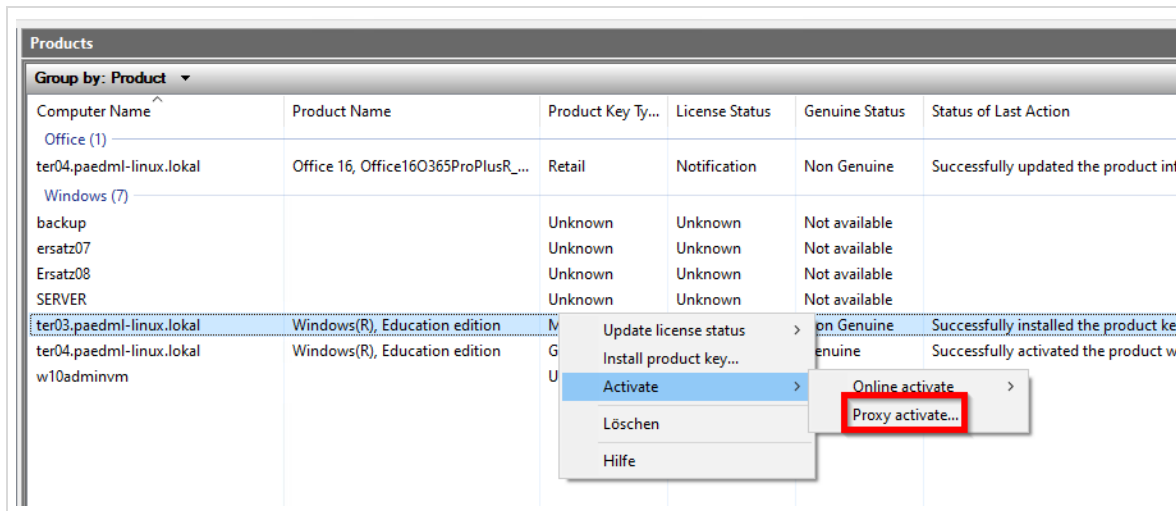


Abb. 206: Aktivierung über Proxy

Im nächsten Dialog werden Sie gefragt, ob Sie die Aktivierungsinformationen nur herunterladen oder das Gerät auch gleich aktivieren wollen. Wir empfehlen Ihnen die Aktivierung gleich durchzuführen. Hierfür muss das Optionsfeld „Acquire confirmation ID, apply to selected machine(s) and activate“ ausgewählt werden.

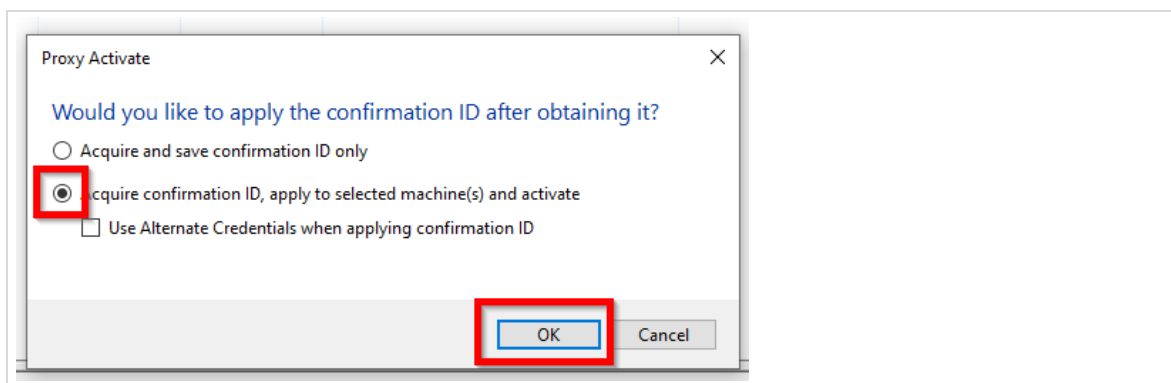


Abb. 207: Soll das die Software gleich aktiviert werden?

Wenn Sie auf „OK“ drücken, fragt das Programm zunächst nach einer „confirmation Id“ (Bestätigung), die auf den Rechner ausgespielt wird.

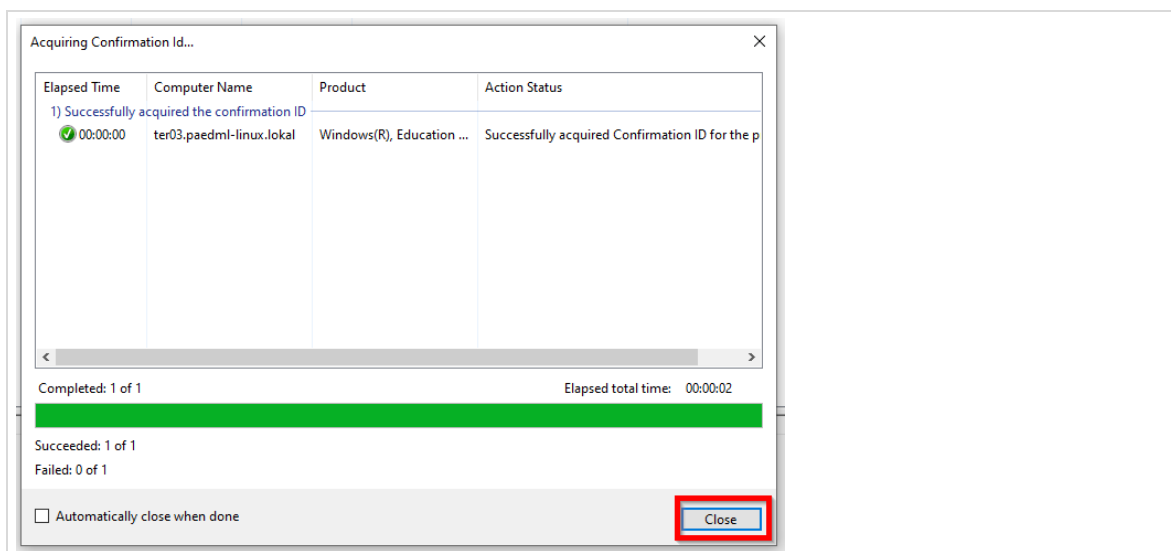


Abb. 208: Einspielen der Bestätigungs-ID

Nach erfolgreicher Bestätigung wird die Lizenz im nächsten Schritt aktiviert.

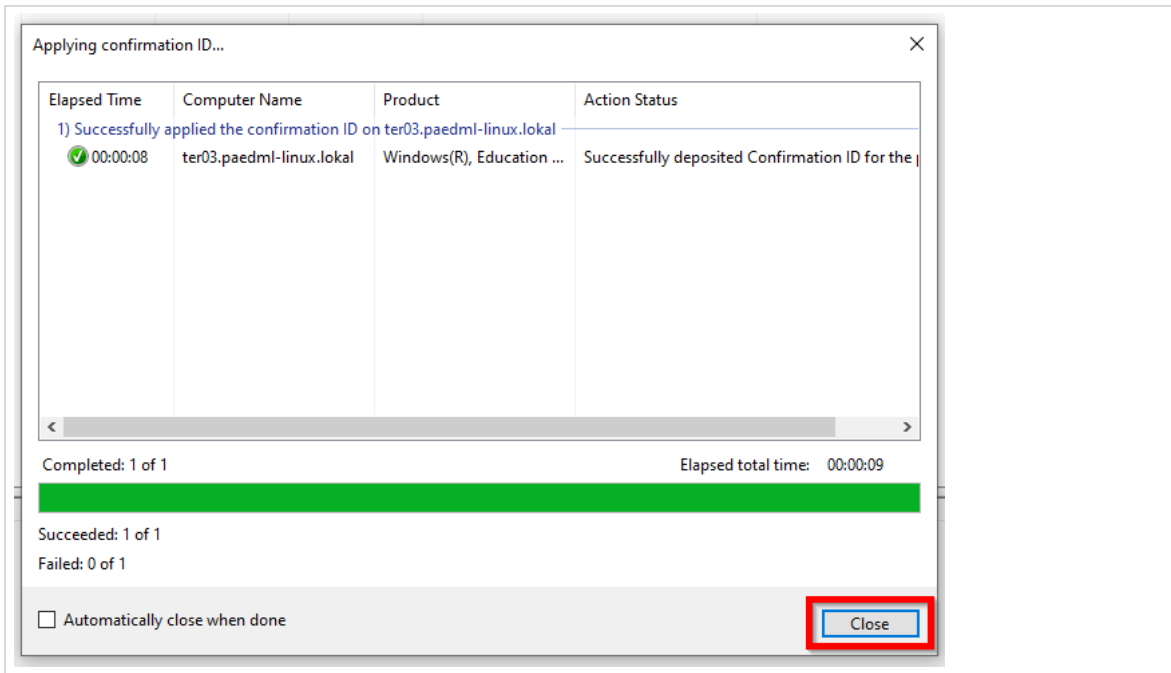


Abb. 209: Aktivierung der Lizenz

Nach dem Aktivieren ist der Rechner in den Produktdetails mit dem „Licence Status“ „Licensed“ versehen.

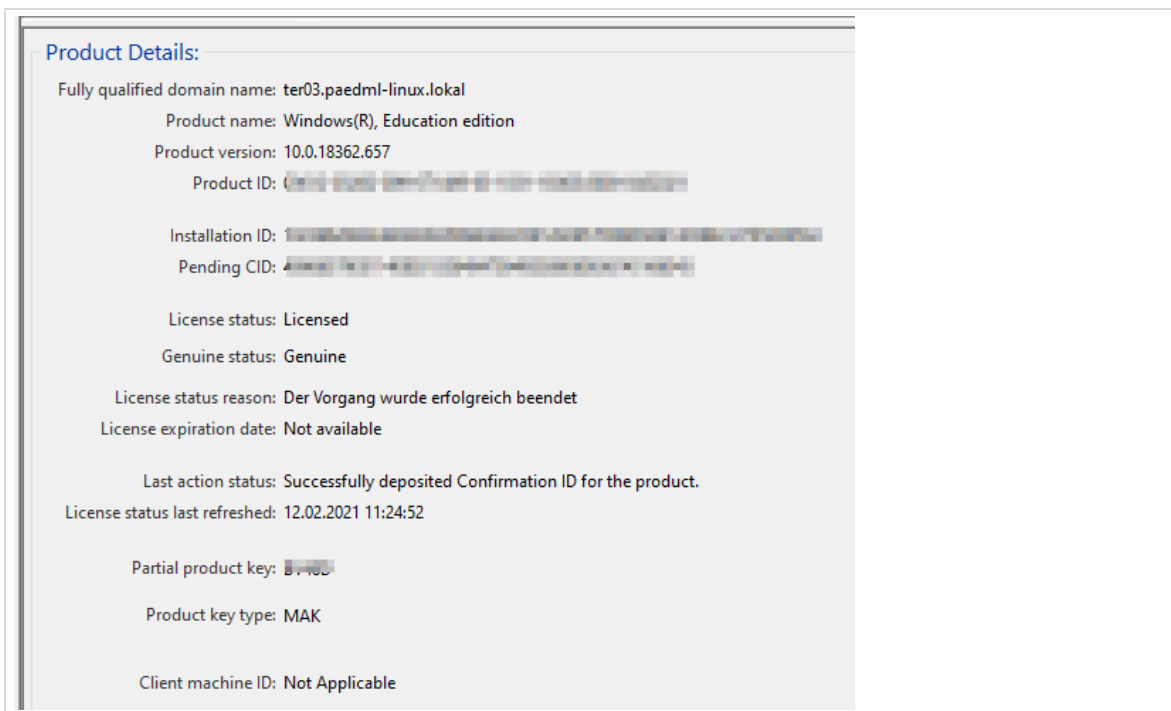


Abb. 210: In der Übersicht ist der Rechner mit dem Lizenzstatus „licensed“ versehen.

12.1.4 Sicherung der Lizenzinformationen

12.1.4.1 Sicherung über ein lokales Image auf den Rechnern

Die Aktivierung der Clients sollte nun nach Möglichkeit in lokalen Images auf den Rechnern gespeichert werden. Hierfür sollten je Maschine die folgenden Schritte durchgeführt werden:

1. Installation des Rechners
2. Aktivierung der Lizenz auf dem Gerät
3. Erstellung eines lokalen Images wie in Kapitel 1 ab Seite 183 beschrieben

Anschließend können Sie den Rechner jederzeit aus dem lokalen Image wiederherstellen, ohne dass die Lizenzinformationen verloren gehen.

12.1.4.2 Sicherung der Lizenzinformationen von VAMT

Die Lizenzinformationen von VAMT können Sie in eine Textdatei exportieren und später – im Fall einer defekten *AdminVM* – in eine neue VAMT-Instanz importieren.

Öffnen Sie hierfür in der Menüleiste von VAMT den Eintrag „Aktion / Export List“.

In dem sich neu öffnenden Fenster müssen Sie einen Namen für die Sicherungsdatei eingeben. Sie können den Sicherungspfad anpassen.

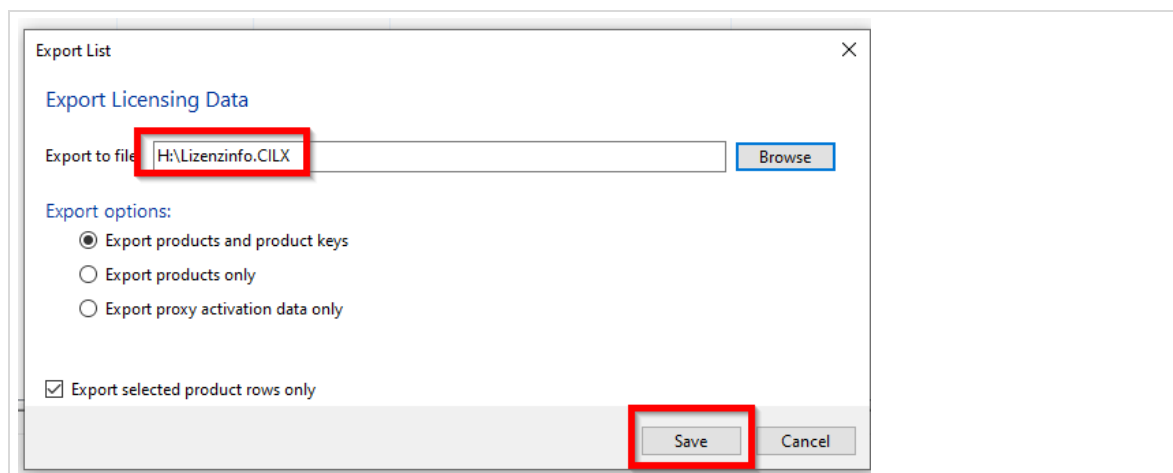


Abb. 211: Wohin sollen die Lizenzdaten gesichert werden?

Die Datei wird im „*.cilx“-Format gespeichert und kann per Mausklick in eine bestehende VAMT-Instanz übertragen werden.

12.1.5 Reaktivierung von Lizenzen nach Neuaufsetzen

Wie oben beschrieben, wird empfohlen, dass Sie nach der Aktivierung eines Clients ein Image erstellen. Dadurch werden die Lizenzinformationen in das Image des jeweiligen Rechners geschrieben und sind nach der Imagewiederherstellung verfügbar.

Eine Reaktivierung von Lizenzen ist nur notwendig, wenn Clients neu installiert – anstatt vom lokalen Image wiederhergestellt – wurden.



Voraussetzung für die Reaktivierung ist, dass sich die Hardware der Clients nicht geändert hat.

Microsoft überprüft anhand von Rechnermerkmalen, an welches Gerät eine Lizenz gebunden wird. Geänderte Hardware (z.B. eine andere Festplatte) führt unter Umständen dazu, dass die Lizenz nicht mehr für das Gerät gültig ist.

Die Reaktivierung beim MAK-Aktivierungs-Verfahren geschieht nicht automatisch, sondern muss manuell ausgeführt werden. Das Verfahren ist ähnlich dem der Erstaktivierung.

Wählen Sie die zu reaktivierenden Clients im VAMT aus und öffnen Sie das Kontextmenü mit der rechten Maustaste.

Die folgenden Schritte sind nacheinander auszuführen:

1. „Update license status | Current credential“

Hiermit wird der Rechner nach installierten Microsoft-Produkten untersucht.

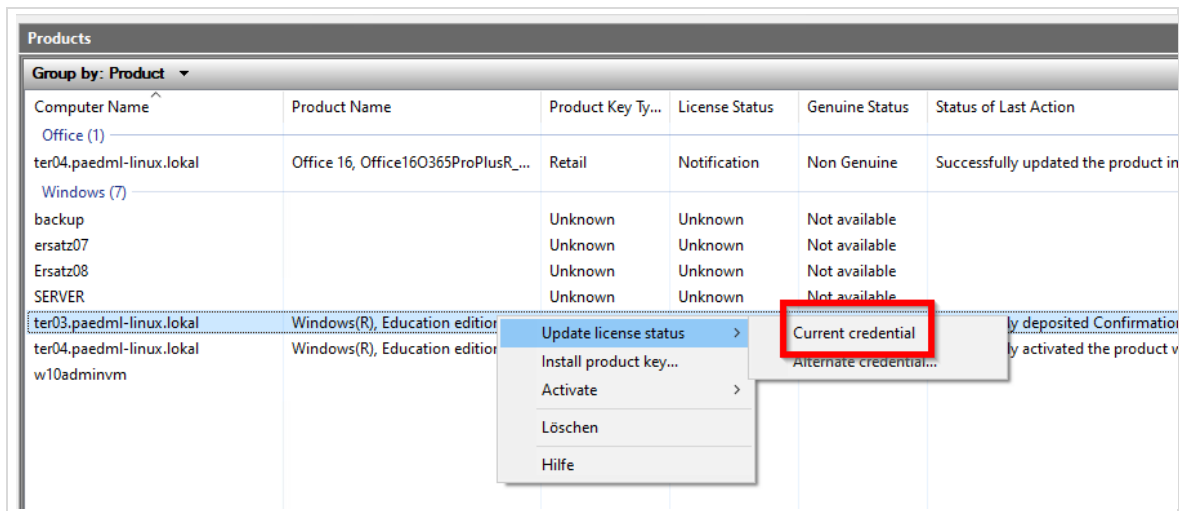


Abb. 212: Erster Schritt der Reaktivierung

2. „Install product key“

Nachdem die Lizenzinformationen für den Rechner abgefragt wurden, installieren Sie den Produkt-Schlüssel. Für diesen Schritt muss der Client erneut ausgewählt und mit der rechten Maustaste bearbeitet werden. Mit dem Eintrag „Install product key...“ werden die Lizenz-Daten auf den Rechner überspielt.

3. „Activate | Apply confirmation ID | Current credential“

Im letzten Schritt (der nur möglich ist, wenn das Gerät bereits aktiviert war – andernfalls ist der Menü-Eintrag nicht verfügbar) wird der Rechner (erneut) aktiviert. Dabei wird die bestehende Lizenz verwendet und der Lizenzzähler nicht erhöht.

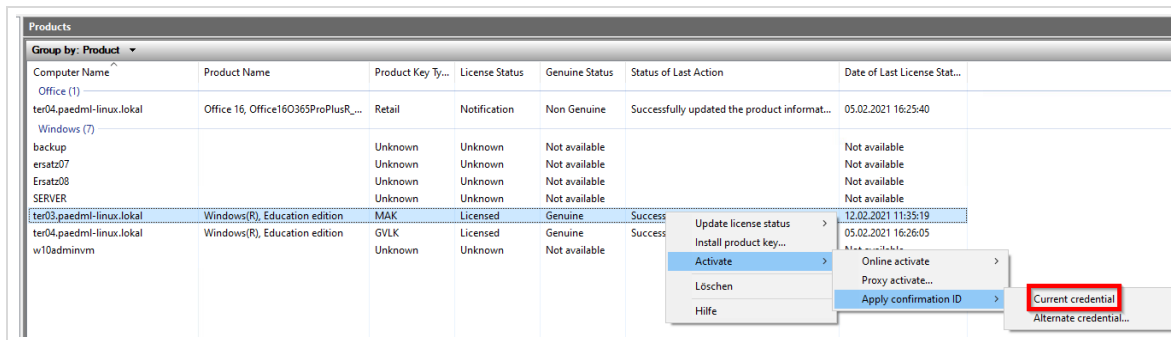


Abb. 213: Zuweisen der bestehenden Lizenz an den Client

12.2 KMS-Server

Bei Verwendung von MAK nehmen Clients einzeln Verbindung zu Microsoft-Servern auf. Der Schlüssel muss über das VAMT installiert werden.

Neben dem MAK-Verfahren gibt es allerdings noch eine weitere Möglichkeit Windows zu aktivieren, den Key Management Service (KMS). Bei Verwendung von KMS gibt es einen KMS-Server. In der *paedML Linux* soll dieser KMS-Server die *W10AdminVM* sein. Dieser stellt eine Verbindung zu Microsoft her. Die zu aktivierenden Clients verbinden sich lediglich mit diesem KMS-Server.

Die Aktivierung erfolgt nach der Neuinstallation von Windows automatisch. Sie ist 180 Tage gültig und wird dann in der Regel automatisch erneuert.



Damit ein KMS-Server aktiv werden kann sind jedoch mindestens 25 Anfragen von zu aktivierenden Clients nötig.

Der KMS kann also nur von Schulen mit mehr als 25 Clients betrieben werden.

12.2.1 Aktivierung des KMS auf der W10AdminVM

In der *paedML Linux* bietet es sich an, den KMS auf der *W10AdminVM* zu aktivieren. Dazu melden Sie sich als Administrator an der AdminVM an.

1. Starten Sie zunächst die Windows-Eingabeaufforderung.
2. Für die Einrichtung des KMS ist das Script „*slmgr.vbs*“ zuständig. In der Eingabeaufforderung wird der Befehl

```
slmgr /ipk <KMS-Schlüssel>
```

eingetragen und durch Drücken der Eingabetaste ausgeführt. Anschließend muss man den Schlüssel aktivieren. Dazu verwendet man den Befehl:

```
slmgr /ato
```

Nun sollte überprüft werden, ob die Einrichtung von KMS erfolgreich war. Dazu den Befehl

```
slmgr /dlv
```

eingeben. Nach kurzer Wartezeit erscheint ein Statusfenster mit dem Hinweis „Der Schlüsselverwaltungsdienst ist auf diesem Computer aktiviert.“

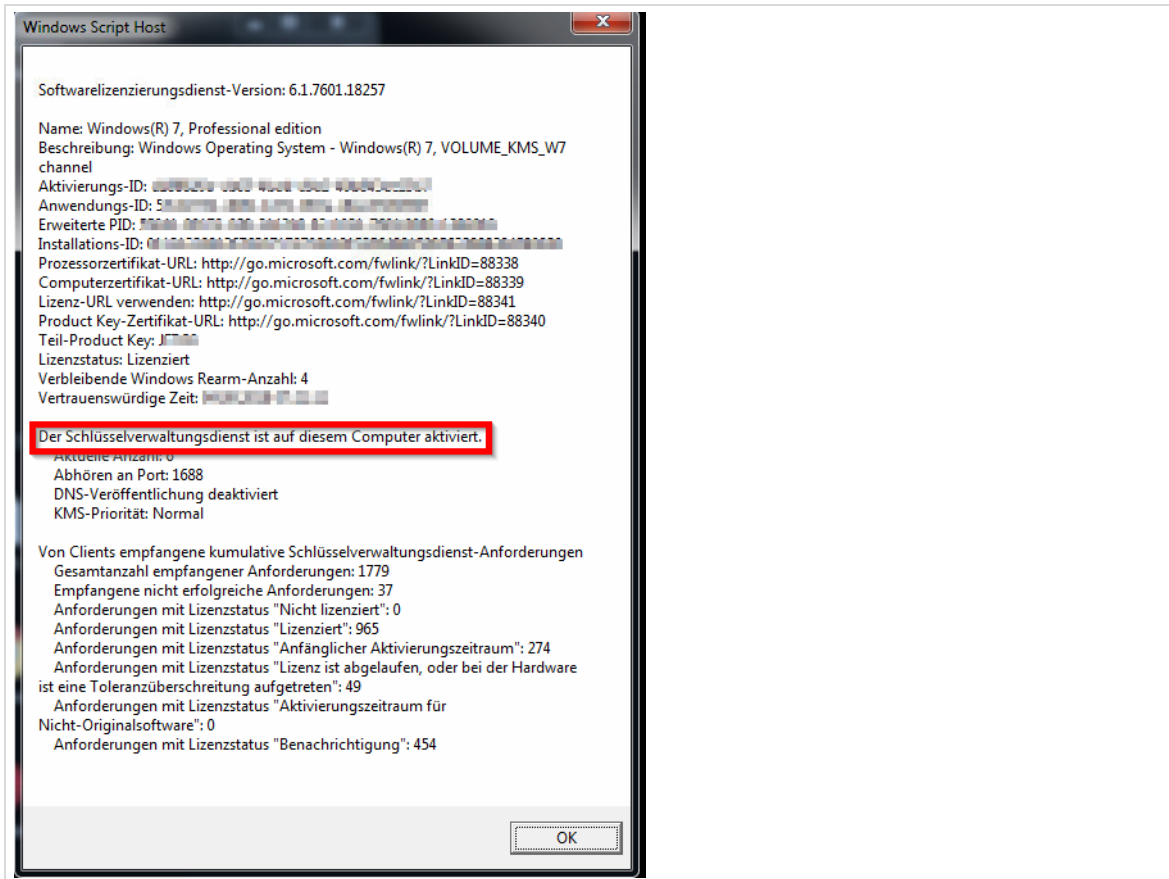


Abb. 214: Ausgabe von `slmgr /dlv`

Die AdminVM ist damit als KMS-Server aktiviert.

12.2.2 Veröffentlichung des KMS

Damit neu installierte Clients den KMS-Server erreichen können muss der DNS um einen entsprechenden Eintrag ergänzt werden.

Melden Sie sich dazu als Administrator an der Schulkonsole an. Navigieren Sie zu Domäne und klicken Sie auf das Feld DNS.

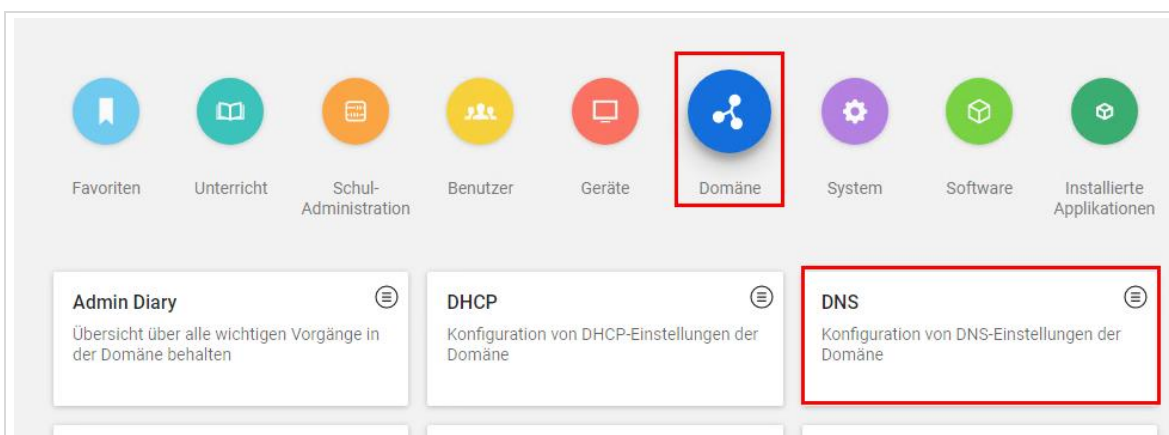


Abb. 215: DNS

Fügen Sie der Domäne `paedml-linux.lokal` einen DNS-Eintrag hinzu.

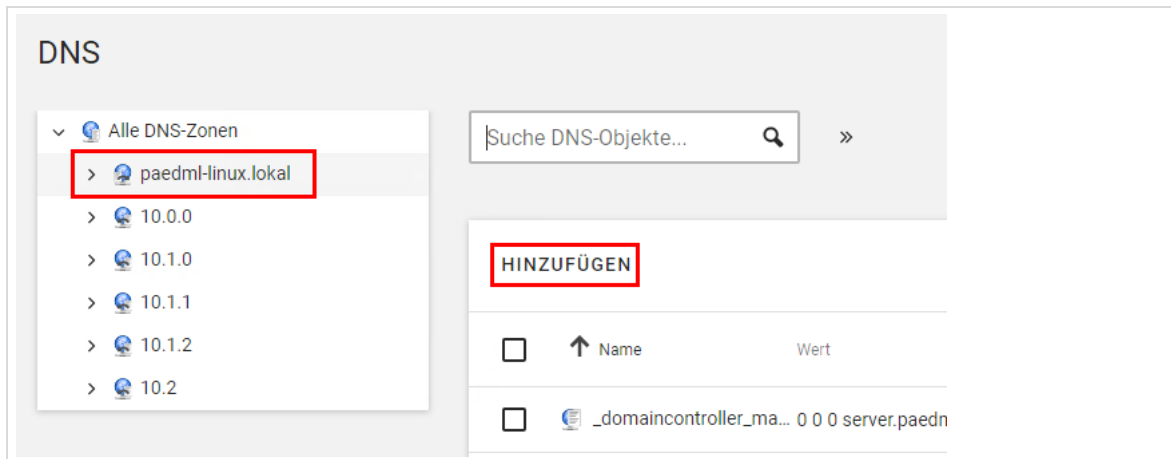


Abb. 216: DNS-Eintrag hinzufügen.

Wählen Sie im nächsten Fenster „DNS: Service Record“ aus und klicken Sie auf „Weiter“.



Abb. 217: DNS: Service Record

Es öffnen sich Felder, in denen Grundeinstellungen vorgenommen werden müssen:

Feld-Name	Feld-Wert
Dienst	vlmcs
Protokoll	Hier bleibt der Standardwert TCP.
Priorität	0
Gewichtung	100
Port	1688
Erweiterung	w10adminvm.paedml-linux.lokal. (Der Punkt am Ende des Eintrags muss gesetzt werden.)

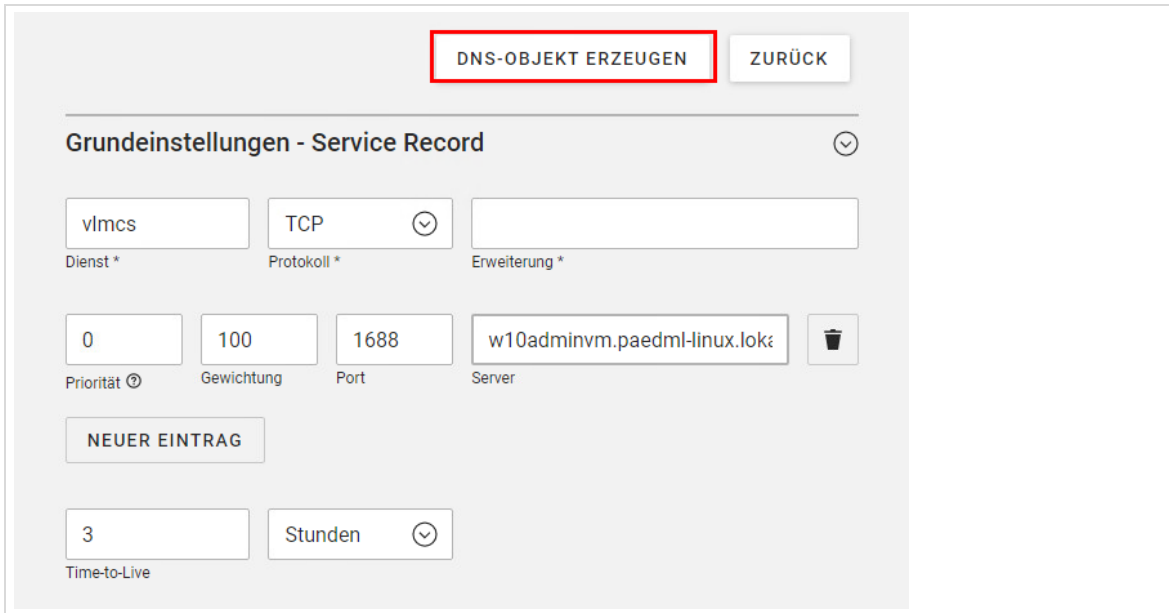


Abb. 218: Grundeinstellungen vlmcs

Durch „DNS-OBJEKT-ERZEUGEN“ bestätigen Sie die Eingaben. Anschließend können Sie sich aus der Schulkonsole abmelden.

Starten Sie die Eingabeaufforderung und deaktivieren Sie mit dem Befehl

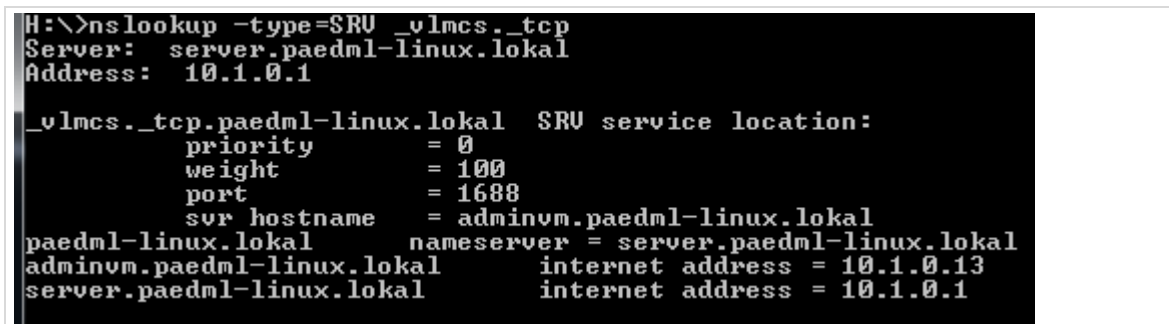
```
slmgr.vbs /cdns
```

die KMS-eigene DNS-Veröffentlichung.

Testen Sie, ob Ihr Vorgehen erfolgreich war, indem Sie in der Eingabeaufforderung

```
nslookup -type=SRV _vlmcs._tcp
```

eingeben.



```
H:\>nslookup -type=SRV _vlmcs._tcp
Server:  server.paedml-linux.local
Address:  10.1.0.1

_vlmcs._tcp.paedml-linux.local SRV service location:
        priority      = 0
        weight         = 100
        port           = 1688
        svr hostname   = adminvm.paedml-linux.local
paedml-linux.local    nameserver = server.paedml-linux.local
adminvm.paedml-linux.local internet address = 10.1.0.13
server.paedml-linux.local internet address = 10.1.0.1
```

Abb. 219: nslookup-type=SRV_vlmcs_tcp

Ab jetzt werden Clients automatisch aktiviert, sobald mehr als 25 Anfragen beim KMS-Server eingegangen sind.

12.2.3 KMS-Aktivierung über das Volume Activation Management Tool (VAMT)



Eine Übersichtliche Darstellung des Status der Lizenzierung der einzelnen Clients bietet das Volume Activation Management Tool (VAMT).

In kleineren Umgebungen, etwa im Grundschul-Bereich, ist ggf. die Mindestanzahl von 25 Clients für die automatisierte KMS-Aktivierung nicht erfüllt. Hier kann über das VAMT eine KMS-Aktivierung händisch für jeden Client angestoßen werden. Hier empfehlen wir jedoch das oben beschriebene MAK-Verfahren, da die Vorteile des KMS in solch kleineren Umgebungen nicht tragen.

Öffnen Sie das Volume Activation Management Tool. Befolgen Sie die in Kapitel 12.1 beschriebenen Schritte bis zur Aktivierung.

Klicken Sie im mittleren Produkte-Fenster des (VAMT) den Client, den Sie aktivieren möchten, rechts an und wählen Sie Activate | Volume Activate | Current Credential.

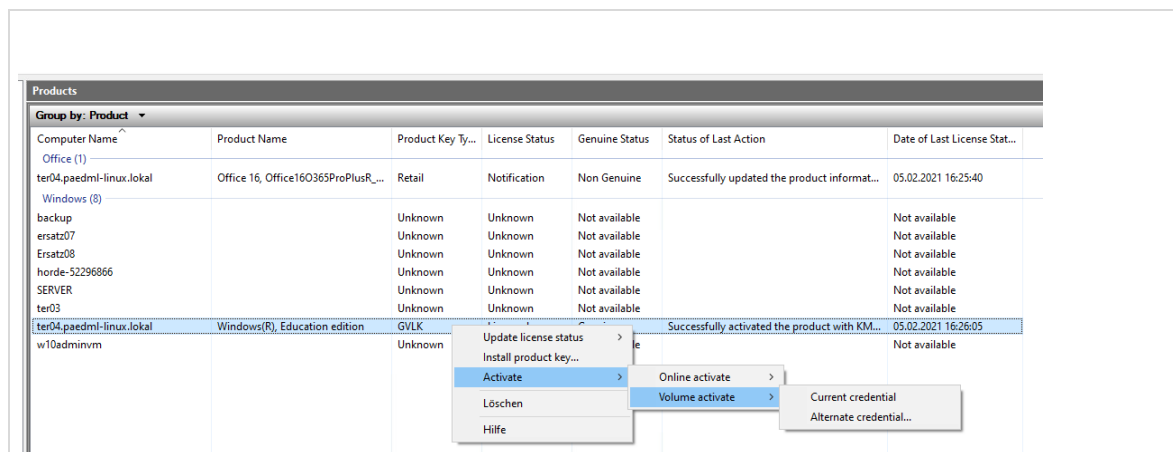


Abb. 220: VAMT: Activate | Volume Activate | Current Credential

13 Updates für die paedML Linux

13.1 paedML Linux Server

Updates für die paedML Linux Server werden automatisch über einen zentralen Updateserver im Support-Netz bezogen.



Nach erfolgreichem Update müssen die Systeme regelmäßig neu gestartet werden.

Melden Sie sich regelmäßig als „Administrator“ an der Schulkonsole vom Server und vom opsi-Server an, um zu überprüfen, ob ein System-Neustart notwendig ist.

„Benachrichtigungen“ oben rechts in der Schulkonsole zeigen an, ob ein Neustart notwendig ist. Um die Meldung anzuzeigen, klicken Sie auf das Glockensymbol.



Abb. 100.1: Benachrichtigungen

13.2 pfSense-Firewall

Das Update der Firewall ist im Installationshandbuch beschrieben. Die Firewall sollte regelmäßig auf aktuelle Versionen geprüft und diese installiert werden.

13.3 Updates/Hotfixes für Windows und opsi-Pakete



Windows 10-Updates dürfen ausschließlich über das opsi-Paket „mshotfix“ und „windows10-upgrade“ ausgespielt werden. Weitere Informationen diesbezüglich finden Sie in Kapitel 6.12 ab Seite 99 und in Kapitel 6.13 ab Seite 100.

Manuell auf Rechnern installierte Windows-Updates führen zu Problemen.

Standard-Pakete der paedML Linux

Wenn Sie ein frisch installiertes paedML Linux System haben, dann befinden sich in Ihrem opsi-Depot einige Softwareprodukte wie z.B. Google Chrome oder Mozilla Firefox, die Sie auf den Arbeitsstationen Ihres Schulnetzwerks einspielen können.

Auf dem opsi-Server vorinstallierte opsi-Produkte werden automatisch aktualisiert. Diese Paketaktualisierungen müssen manuell über die opsi-Konsole auf die Clients ausgespielt werden.

Um zu überprüfen, ob es Updates für installierte opsi-Produkte gibt, müssen Sie in der opsi-Oberfläche alle Rechner markieren, die Sie überprüfen wollen. Klicken Sie anschließend auf den Reiter „Produktkonfiguration“ des Hauptfensters. Sie bekommen installierte Software angezeigt. Sofern es Updates für die Software gibt, wird in der Spalte „Version“ ein roter Wert angezeigt, der die neue Versionsnummer der Software anzeigt. Bei verschiedenen Softwareständen steht in der Spalte „Version“ der Eintrag „mixed“, der ebenfalls rot angezeigt wird.

Um die Software zu aktualisieren, klicken Sie mit der linken Maustaste im Reiter „Produktkonfiguration“ in das Feld der Spalte „Angefordert“ des zu aktualisierenden Produktes. Die Auswahl von „setup“ und die Bestätigung der Änderung führen dazu, dass die Software beim nächsten Systemstart aktualisiert wird.

Produkt-ID	Stand	Report	Angefordert	Version
google-chrome-for-business	installed	success (setup)	setup	# 93.0.4577.82-1
opsi-client-agent	installed	success (setup)	setup	# 4.1.1.32-1
windomain	installed	success (setup)	setup	# 1.0-11
firefox	installed	success (setup)		78.14.0esr91.1.0e...
nccad76	installed	success (setup)		7.6-2
clientprodukte	installed	success (setup)		7.2-5

Abb. 100.1.1: Es gibt Updates für Clientsoftware

Nachträglich installierte opsi-Pakete

Auf dem Server der SON-Gruppe werden opsi-Pakete für registrierte paedML Kunden bereitgestellt. Diese Pakete und Pakete, die von Drittanbietern bezogen werden, müssen manuell im opsi-Depot auf dem Backup-Server aktualisiert werden.



Wir empfehlen Ihnen generell das folgende Vorgehen beim Einspielen von Produktupdates in Ihrem Netzwerk:

1. Installieren Sie Updates auf einem Testclient bevor Sie diese im gesamten Netzwerk verteilen.
2. Wenn alles funktioniert, werden die Updates auf allen Clients der Schule ausgerollt.
3. Aktualisieren Sie anschließend – sofern vorhanden – das lokale Image im Cache der Arbeitsstationen.

13.4 Übersicht über Updatezeiten

Es gibt im System verschiedene cron-jobs – das sind zu bestimmten Zeiten wiederkehrende Aufgaben – mit denen verschiedene Elemente der *paedML Linux* aktuell gehalten werden.

Server-Updates	Die Installation von Updates der <i>paedML</i> Server wird automatisch ausgeführt. Hierfür gibt es einen cron-job, der freitags um 22:05 Uhr nach neuen Updates sucht und diese gegebenenfalls installiert.
opsi-Produkte	Hierfür gibt es einen cron-job, der von Montag bis Donnerstag um 22:00 Uhr nach neuen opsi-Paketen sucht und diese in das opsi-depot auf dem Backup-Server lädt.

Tabelle 16: Übersicht über Update-Zeiten

14 Steuerung der Internetzugriffe



Bevor im Folgenden das Thema Steuerung des Internetzugriffs erörtert wird, sei die Bemerkung gestattet, dass technische Mechanismen dem Erfindungsreichtum der Schüler vermutlich immer unterlegen sein werden.

Es wird immer wieder Schlupflöcher geben, die Schüler finden, um gesperrte Internetseiten aufzurufen:

- Webproxy-Dienste
- https-Zugriff
- ...

Neben technischen Vorkehrungen, die das Surfverhalten kontrollieren sollen, sollten Sie sich pädagogische Ansätze (Ge- und Verbote, Aufklärungsarbeit, ...) überlegen und die eigene Frustrationstoleranz erhöhen.

14.1 Definition von Internetregeln

Aufruf über Schulkonsole (netzwerkberater): Schul-Administration | Internetregeln definieren



Wir empfehlen unseren Kunden grundsätzlich, den Internetzugang mit einem externen Jugendschutzfilter zu kombinieren. Seit der Ankündigung, dass BelWü mittelfristig den Jugendschutzfilter nicht mehr anbieten wird, empfehlen wir den Einsatz von JusProgDNS. Ein HowTo diesbezüglich ist unter <https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#howtos> abrufbar. Aber auch andere externe DNS-basierte Jugendschutzfilter Ihrer Wahl sind verwendbar.

Bitte beachten Sie, dass JusProg kostenpflichtig ist. Weitere Informationen erhalten Sie unter <https://www.jusprogdns.com/schulen/> und <https://www.jusprogdns.com/premium>.

Das folgende Bild zeigt die zwei Standardeinstellungen des Menüs „Schul-Administration | Internetregeln definieren“:

- „Kein Internet“ – wenn diese Regel aktiviert wird, kann keine Seite im Internet aufgerufen werden.
- „Unbeschränkt“ – Der Zugriff funktioniert auf alle Internetseiten (außer die durch den Jugendschutzfilter gesperrten).

Internetregeln definieren SCHLIESSEN

🔍

Suchbegriff ⓘ

REGEL HINZUFÜGEN
0 Einträge von 2 ausgewählt

<input type="checkbox"/> ↑ Name	Typ	WLAN	Priorität
<input type="checkbox"/> Kein Internet	Freigabeliste	deaktiviert	0
<input type="checkbox"/> Unbeschränkt	Sperrliste	aktiviert	0

Abb. 100.1.2: Standardregeln für den Internetzugriff

Sie können über den Knopf „Regel hinzufügen“ eigene Regelwerke definieren. Hierbei gibt es die Möglichkeit, eigene Black- (Sperrliste) und Whitelists (Freigabeliste) anzulegen. Eine Blacklist sperrt bestimmte Seiten, eine Whitelist lässt **nur** den Zugriff auf in der Whitelist eingetragene Seiten zu.

Zuerst ist ein „Name“ für die neue Regel einzugeben. Danach wird der „Regeltyp“ („Freigabeliste“ oder „Sperrliste“) definiert.

Im Feld „Internet-Domänenliste“ wird festgelegt, welche Seiten aufgerufen werden dürfen oder vom System gesperrt werden. Hier können mehrere Seiten hintereinander eingetragen werden. Es wird empfohlen, den Domänenanteil der Adresse anzugeben, also lmz-bw.de statt www.lmz-bw.de. Tragen Sie jede Domäne in ein eigenes Feld ein.

Internetregeln definieren

SPEICHERN

ZURÜCK ZUR ÜBERSICHT

Regeleigenschaften ⌵

Name ⓘ

Regeltyp ⓘ

Internet-Domänenliste ⌵

🗑️

Internet-Domänen (z.B., wikipedia.org, facebook.com) ⓘ

🗑️

Internet-Domänen (z.B., wikipedia.org, facebook.com) ⓘ

NEUER EINTRAG

Erweiterte Einstellungen ⌵

☐ WLAN-Authentifizierung aktiviert

Priorität ⓘ

Abb. 100.1.3: Anlegen eigener Freigabeliste

Der Haken bei „WLAN-Authentifizierung aktiviert“ definiert, ob die Gruppe, der die Regel zugewiesen ist, auf ein vorhandenes WLAN zugreifen darf. Wenn der Haken nicht gesetzt ist, Kann sich ein Benutzer nicht am WLAN anmelden, sobald die Regel aktiv ist.

Die „Priorität“ der Regel legt fest, wie Regeln abgearbeitet werden. Dies ist vor allen dann interessant, wenn Anwender in verschiedenen Gruppen (Klasse und Arbeitsgruppe) Mitglied sind und widersprüchliche Regeln erhalten.

Regeln mit hohen Prioritäten (z.B. 10 (hoch)) überschreiben niedrig priorisierte Regeln (z.B. 0 (niedrig)).



Abb. 100.1.4: Anlegen eigener Sperr- oder Freigabelisten

14.2 Internetregeln zuweisen

Aufruf über Schulkonsole (netzwerkberater): Schul-Administration | Internetregeln zuweisen

Die *paedML Linux* ermöglicht Ihnen die Verwaltung mehrerer Internetregeln, die an verschiedene Benutzergruppen zugewiesen werden können. So können Sie beispielsweise für Unterstufenschüler den Internetzugriff stärker eingrenzen als für Oberstufenschüler.

Die im letzten Abschnitt beschriebene Priorität der Listen entscheidet, welche Inhalte ein Benutzer zu sehen bekommt, wenn er Mitglied verschiedener Gruppen ist.

Die Zuweisung einer Regel erfolgt als Netzwerkberater über das Menü „Schul-Administration | Internetregeln zuweisen“. Sie können hier Gruppen auswählen, denen eine bestimmte Regel zugewiesen werden soll. Im folgenden Screenshot wurde das Internet für die fünften Klassen gesperrt. Die sechsten Klassen sollen einen Zugriff auf die Sendung mit der Maus erhalten.

Wählen Sie zunächst die zu ändernden Klassen aus und drücken Sie anschließend auf „Regeln zuweisen“. Es öffnet sich ein neues Dialogfenster.

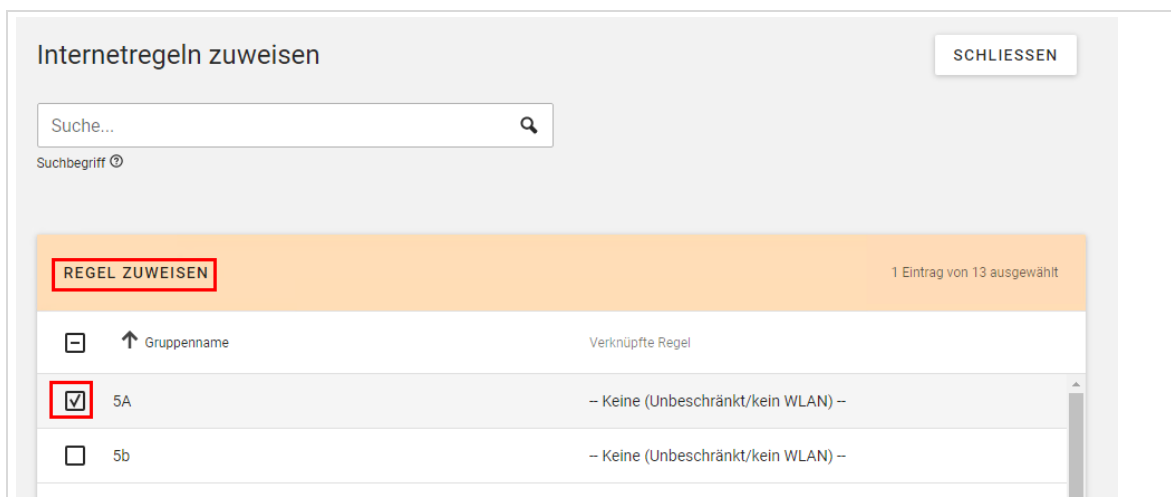


Abb. 100.1.5: Zuweisen von Internetregeln an Gruppen

Sie können im nächsten Dialog eine Internetregel an die ausgewählten Gruppen zuweisen. Ein Klick auf „Regel zuweisen“ übernimmt die Änderungen.

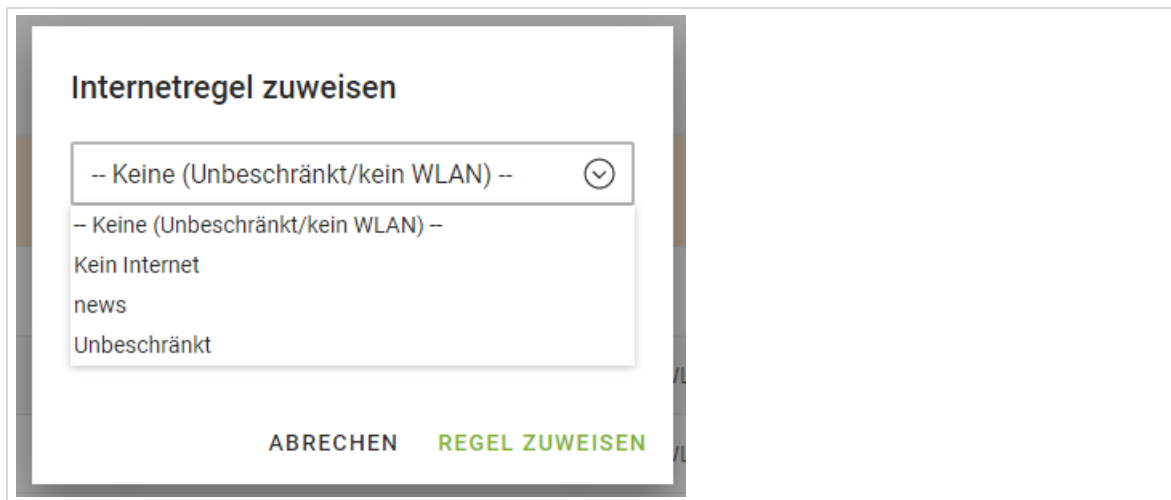


Abb. 100.1.6: Auswahl der Internetregel

14.3 Unbeschränkten Internetzugriff für Lehrer

Wird die Regel einer Klasse oder Arbeitsgruppe zugewiesen, betrifft dies auch die der Klasse zugewiesenen Lehrer. Um zu verhindern, dass Lehrer den gleichen Beschränkungen unterliegen, kann Lehrern eine Regel mit höherer Priorität zugewiesen werden. Im nachfolgenden Beispiel soll der Lehrer unbeschränkten Internetzugriff erhalten:

1. Definieren Sie eine Internetregel mit hoher Priorität (z.B. 10) und benennen Sie die Regel eindeutig.

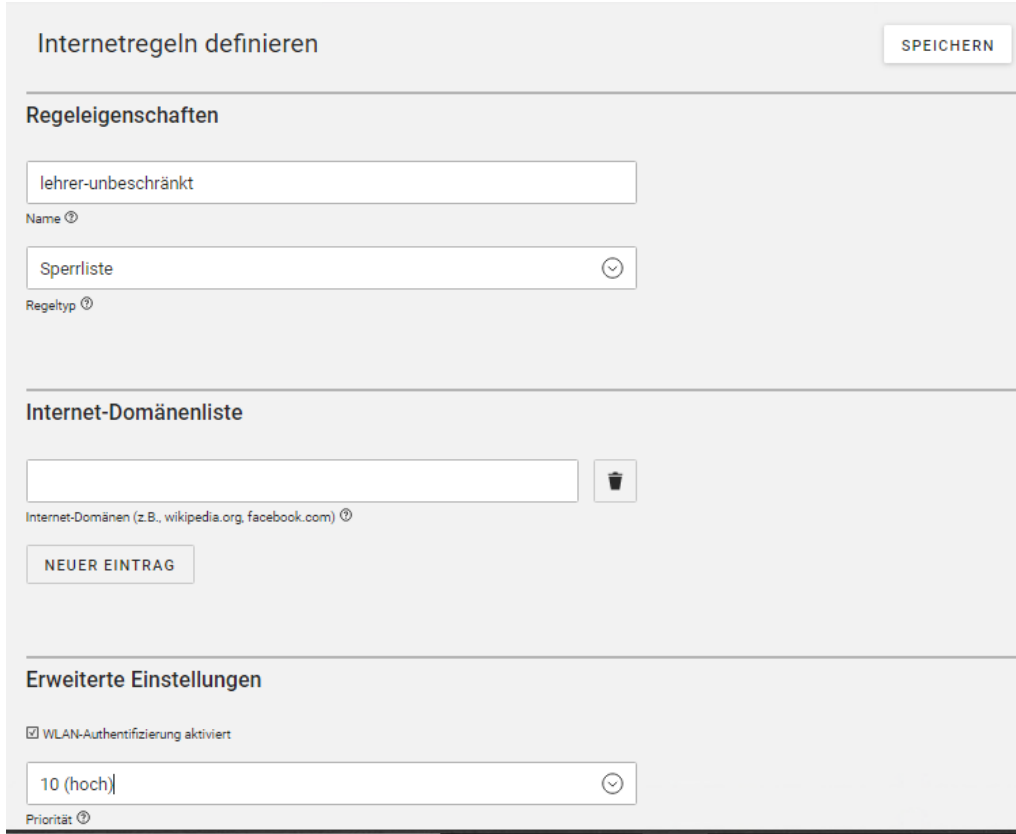


Abb. 100.1.7: Internetregel für Lehrer erstellen

2. Weisen Sie die eben erstellte Regel der Gruppe „Lehrer“ zu.

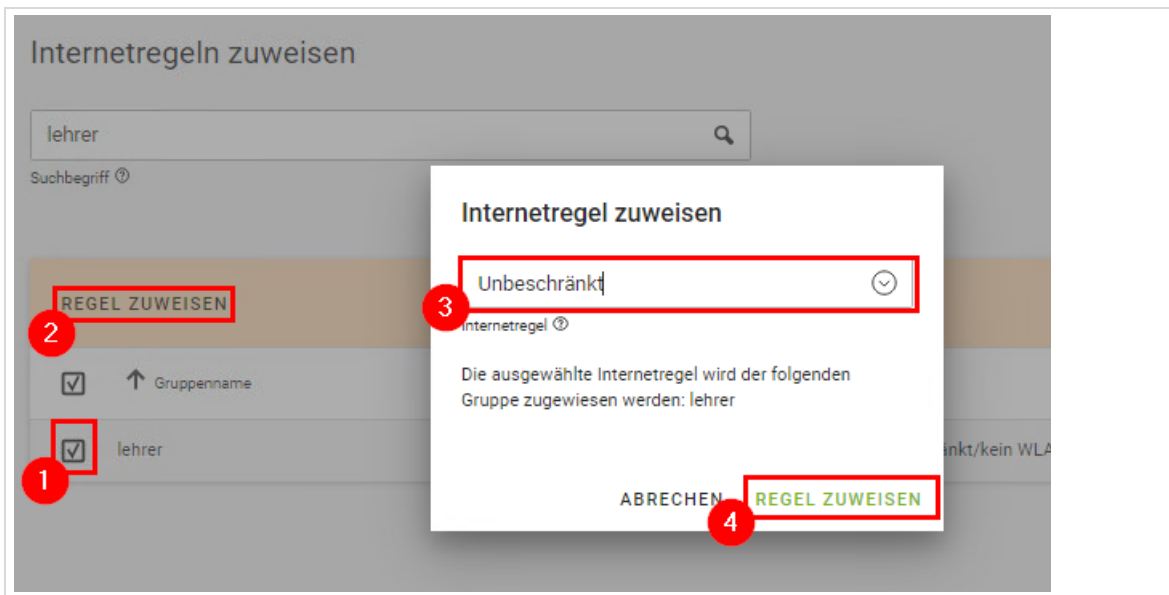


Abb. 100.1.8: Internetregel mit höherer Priorität an Lehrer zuweisen

14.4 Verwendung eines externen Jugendschutzfilters (DNS-Filter)

Um einen externen DNS-Server einzutragen, über den der Netzverkehr des schulischen Netzes gefiltert werden kann, müssen Sie diesen in der Firewall eintragen.

Beachten Sie bitte, dass der Jugendschutzfilter in diesem Fall für alle Benutzer greift.

Unter <https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#howtos> ist beschrieben, wie Sie den Jugendschutzfilter JusProgDNS in der paedML Linux / GS einsetzen können.

Eintrag eines externen DNS-Servers

1. Melden Sie sich als Administrator an der Firewall an (<https://firewall.paedml-linux.lokal>).

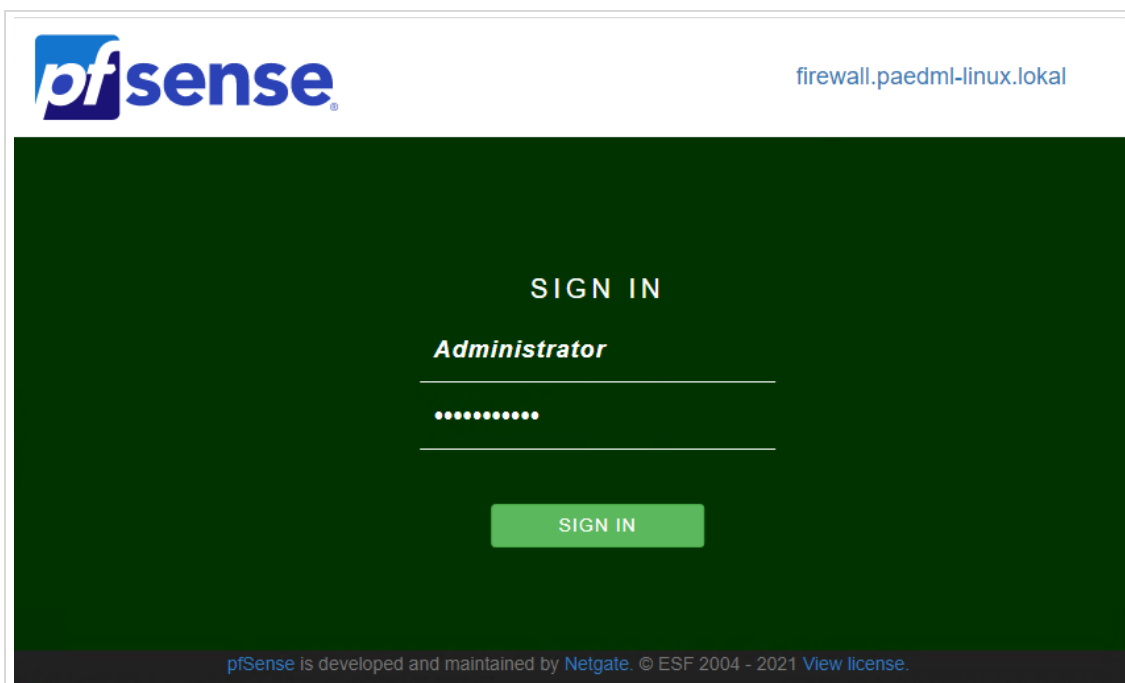


Abb. 100.1.9: An der Firewall anmelden Update Screenshot

2. Navigieren Sie zu „System | Allgemeine Einstellungen“. Tragen Sie bei (1) die Adresse des externen Jugendschutzfilters ein und löschen Sie einen evtl. eingetragenen zweiten DNS-Server (2).

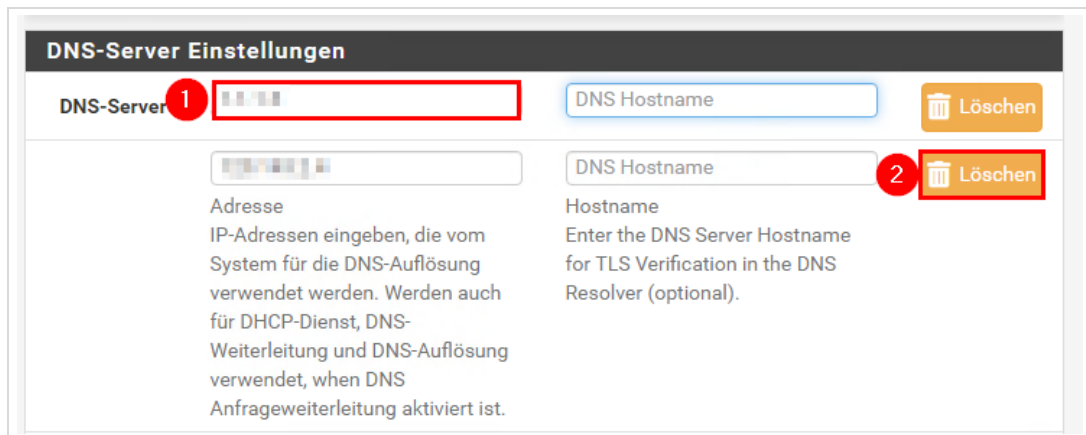


Abb. 100.1.10: An der Firewall anmelden

3. Scrollen Sie auf der Seite nun bis nach unten und klicken Sie auf „Speichern“.

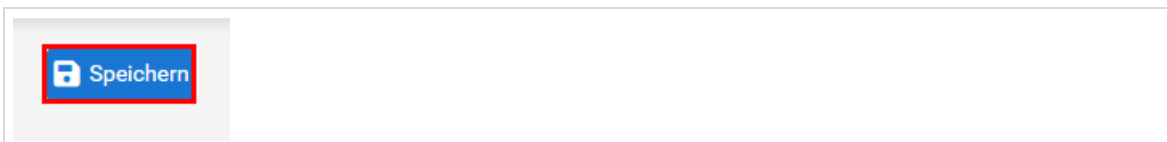


Abb. 100.1.11: Speichern nicht vergessen

14.5 Protokollierung von Internetzugriffen

Leider kommt es immer wieder vor, dass aus dem Schulnetz heraus Missbrauch betrieben wird, der die Ermittlungsbehörden auf den Plan ruft. In einem solchen Fall muss in Erfahrung gebracht werden, welcher Benutzer wann an einem Rechner angemeldet war und welche Seiten aufgerufen wurden.

Die folgende Tabelle listet auf, welches Benutzerverhalten in welchen Dateien protokolliert wird.



Aus datenschutzrechtlichen Gründen ist zur Kontrolle dieser Log-Dateien die Anordnung der Schulleitung einzuholen und das Vier-Augen-Prinzip zu wahren.

Wir empfehlen außerdem, die Benutzer durch eine Benutzerordnung darauf hinzuweisen, dass im Bedarfsfall Log-Dateien ausgewertet werden können.

Protokollgruppe	Verzeichnis	Dateiname	Was wird protokolliert?	Frist
Arbeitssitzung	/home/Administrator/	logon.txt	An- und Abmelden von Benutzern an Clients	30 Tage ⁶⁰
	/home/netzwerkberater/ /		Datum , Uhrzeit, IP, Benutzername	
	/var/log/	auth.log	System-Log-Datei Linux-Logins von Diensten (cron,...) und root	30 Tage
Intranet-Webseiten	/var/log/apache2/	access.log	Webseitenname, zugreifende IP, Datum, Uhrzeit	30 Tage
		other_vhosts_access.log	Webseitenname, zugreifende IP, Datum, Uhrzeit	30 Tage
		error.log		30 Tage
Internet-Webseiten	/var/log/squid/	access.log	Benutzername, Webseitenname, zugreifende IP, Datum, Uhrzeit	30 Tage

Tabelle 17: Log-Dateien zu Benutzerverhalten

Ein Auszug einer Log-Datei zur Veranschaulichung:

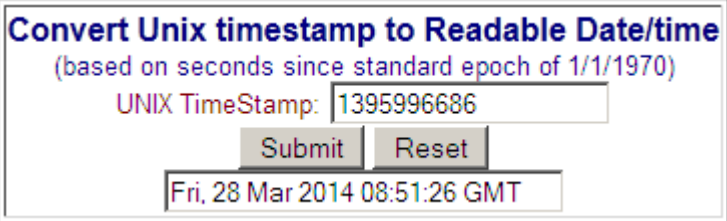
Die Informationen zu Seitenaufrufen stehen in der Datei /var/log/squid/access.log.

Ein Auszug aus der Log-Datei sieht folgendermaßen aus:

⁶⁰ Bei stark frequentierten Netzwerken können die Dateien weniger als 30 Tage vorgehalten werden, da ein wöchentlicher Austausch der Log-Dateien stattfindet und zusätzlich ab einer Größe von 50 kB eine neue Log-Datei angelegt wird.

```
(...)  
  
1395996686.010      40 10.1.0.222 TCP_MISS/200 931 GET  
http://www.google.com/complete/search? felix.gengler DIRECT/173.194.113.148  
text/javascript  
  
1395996686.980      577 10.1.0.222 TCP_MISS/200 25918 GET  
http://www.tagesschau.de/ felix.gengler DIRECT/23.74.202.240 text/html  
  
(...)
```

Squid loggt die Zeitstempel in Sekunden seit 1970, so dass eine Umrechnung vorgenommen werden muss, wenn die genaue Zeit ermittelt werden soll. Hierfür gibt es im Internet Angebote, die Sie mit Hilfe der Suchbegriffe „Timestamp & Rechner“ oder „Timestamp & Calculator“ aufrufen können.



Convert Unix timestamp to Readable Date/time
 (based on seconds since standard epoch of 1/1/1970)
 UNIX TimeStamp:

Abb. 100.1.12: Umrechnung des Zeitstempels

15 Nagios

15.1 Funktionsweise

Adresse: <https://server.paedml-linux.lokal/nagios>

Mit der Monitoring-Software *Nagios* werden verschiedene Serverdienste überwacht. *Nagios* ist im Auslieferungszustand so konfiguriert, dass alle drei in der *paedML Linux* eingesetzten Server (Server, opsi-Server und pfSense) überwacht werden.

Im Fehlerfall generiert Nagios eine Mail, die an den Netzwerkberater gesendet wird. Sobald der Fehler behoben wurde, sendet Nagios eine erneute Meldung an den Netzwerkberater.

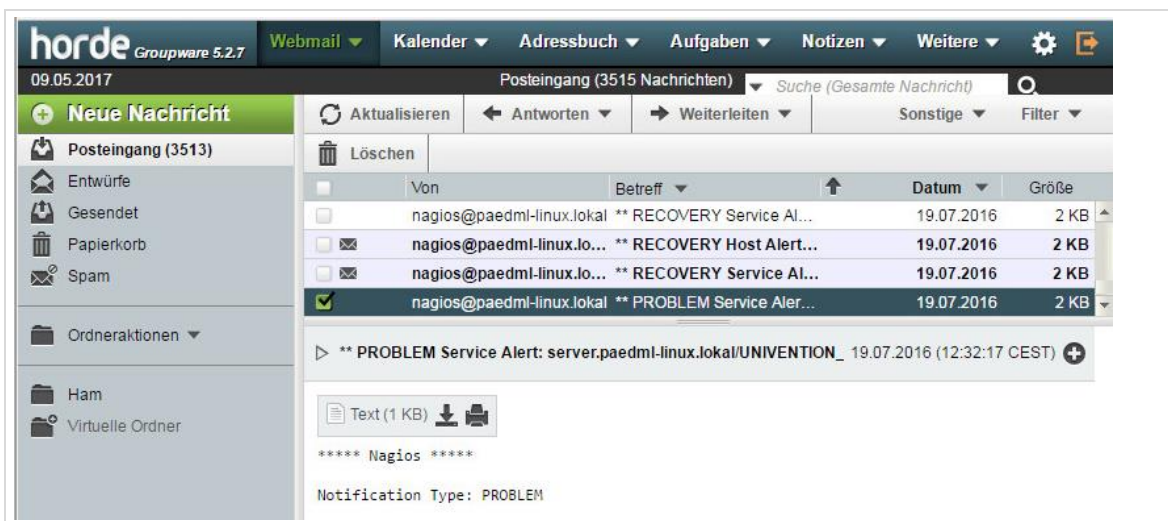


Abb. 100.1.13: Nagios-Mail für den Netzwerkberater



Hinweis für alle anderen Kunden:

Nagios ist als Dienst auf Ihrem Server vorkonfiguriert. Das Programm kann beliebig modifiziert und an Ihre Bedürfnisse angepasst werden. Da es sich um ein mächtiges Programm mit vielfältigen Einstellungsmöglichkeiten handelt, können wir hierfür keinen Support anbieten.

Eigene Anpassungen an der Nagios-Installation werden nicht durch die Hotline unterstützt.

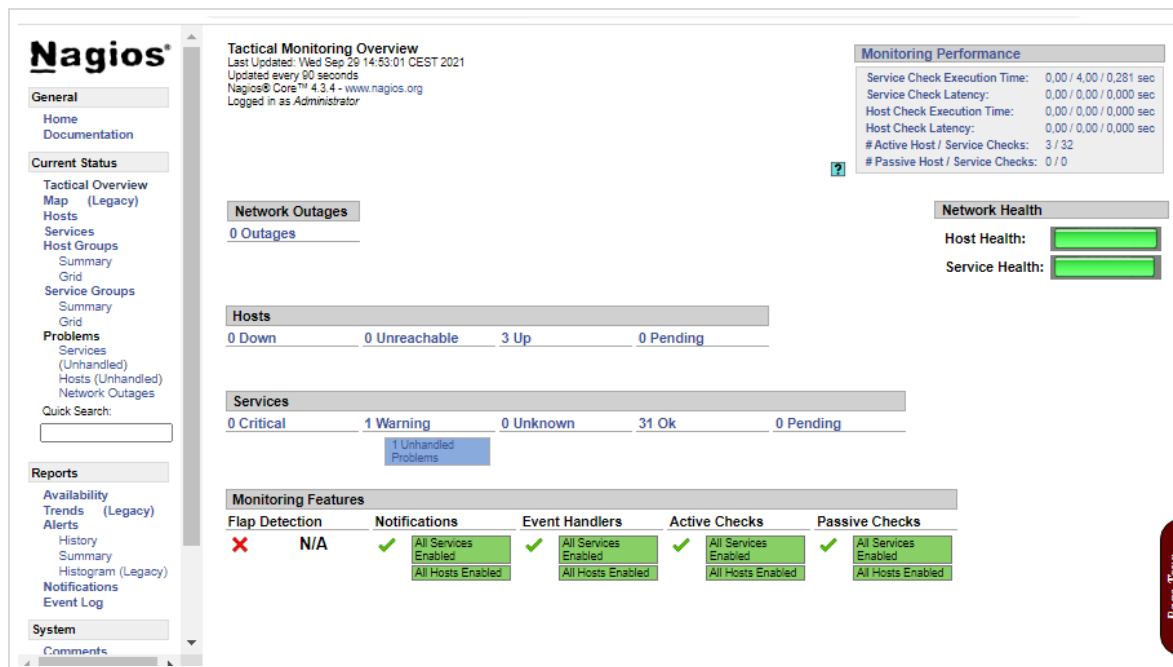
Wir bitten Sie um Verständnis. Danke.

Mehr Informationen zu *Nagios* finden Sie unter <http://www.nagios.org/> oder unter <https://docs.software-univention.de/handbuch-4.3.html#nagios::general>

15.2 Die Nagiosübersichtsseiten

Auf der linken Seite haben Sie eine Navigationsleiste mit verschiedenen Menüs.

Unter *Current Status* / *Tactical Overview* wird eine Übersicht über den Zustand der überwachten Maschinen angezeigt.





Nagios®

Tactical Monitoring Overview
 Last Updated: Wed Sep 29 14:53:01 CEST 2021
 Updated every 90 seconds
 Nagios® Core™ 4.3.4 - www.nagios.org
 Logged in as Administrator

Monitoring Performance

Service Check Execution Time:	0.00 / 4.00 / 0.281 sec
Service Check Latency:	0.00 / 0.00 / 0.000 sec
Host Check Execution Time:	0.00 / 0.00 / 0.000 sec
Host Check Latency:	0.00 / 0.00 / 0.000 sec
# Active Host / Service Checks:	3 / 32
# Passive Host / Service Checks:	0 / 0






Network Outages
0 Outages

Network Health
 Host Health: 
 Service Health: 

Hosts
 0 Down 0 Unreachable 3 Up 0 Pending

Services
 0 Critical 1 Warning 0 Unknown 31 Ok 0 Pending

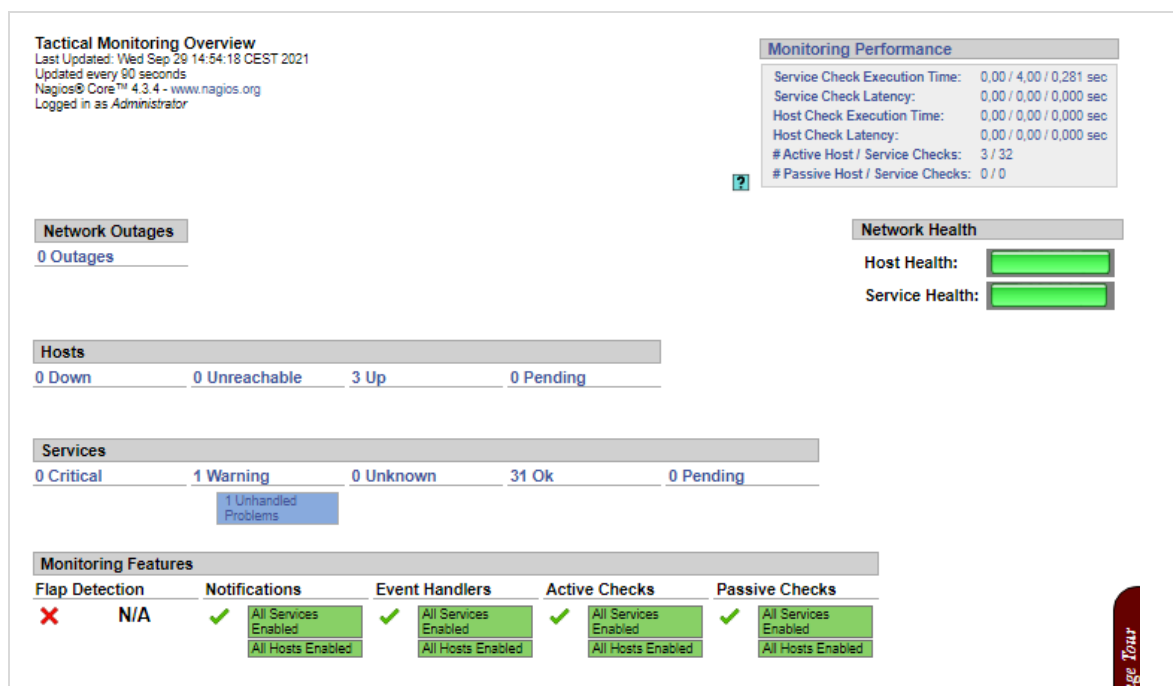
Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
 N/A	 All Services Enabled All Hosts Enabled	 All Services Enabled All Hosts Enabled	 All Services Enabled All Hosts Enabled	 All Services Enabled All Hosts Enabled

Page Tour

Abb. 100.1.14: Nagios-Startseite

Im Menü „Current Status“ können Sie verschiedene Sichten für Nagios einsehen. „Tactical Monitoring Overview“ ist der Standard-Startbildschirm von Nagios. In dieser Ansicht sehen Sie einen Überblick über alle überwachten Rechner („Hosts“), alle überwachten Dienste („Services“), sowie die Einstellungen der Systemüberwachung („Monitoring Features“).





Tactical Monitoring Overview
 Last Updated: Wed Sep 29 14:54:18 CEST 2021
 Updated every 90 seconds
 Nagios® Core™ 4.3.4 - www.nagios.org
 Logged in as Administrator

Monitoring Performance

Service Check Execution Time:	0.00 / 4.00 / 0.281 sec
Service Check Latency:	0.00 / 0.00 / 0.000 sec
Host Check Execution Time:	0.00 / 0.00 / 0.000 sec
Host Check Latency:	0.00 / 0.00 / 0.000 sec
# Active Host / Service Checks:	3 / 32
# Passive Host / Service Checks:	0 / 0






Network Outages
0 Outages

Network Health
 Host Health: 
 Service Health: 

Hosts
 0 Down 0 Unreachable 3 Up 0 Pending

Services
 0 Critical 1 Warning 0 Unknown 31 Ok 0 Pending

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
 N/A	 All Services Enabled All Hosts Enabled	 All Services Enabled All Hosts Enabled	 All Services Enabled All Hosts Enabled	 All Services Enabled All Hosts Enabled

Page Tour

Abb. 100.1.15: Die „taktische Übersicht“ von Nagios

Unter „Services“ erhalten Sie eine Liste über die einzelnen Dienste (Spalte „Service“) aller überwachten Maschinen (Spalte „Host“). Fehler werden in der Spalte „Status“ rot unterlegt, im oberen Bereich der Übersicht finden Sie kleine Tabellen, die auf den ersten Blick anzeigen, ob es Probleme gibt und – für den Fall, dass alles in Ordnung ist – das nach unten Scrollen überflüssig machen.

Current Network Status
 Last Updated: Wed Sep 29 14:55:24 CEST 2021
 Updated every 90 seconds
 Nagios® Core™ 4.3.4 - www.nagios.org
 Logged in as Administrator

View History For all hosts
 View Notifications For All Hosts
 View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
3	0	0	0

All Problems All Types

0	3
---	---

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
31	1	0	0	0

All Problems All Types

1	32
---	----

Service Status Details For All Hosts

Limit Results:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
backup.paedml-linux.local	LMZ_DISK_VAR	OK	2021-09-29 14:51:07	209d 5h 18m 53s	1/10	DISK OK - free space: /var 188157 MB (86% inode=99%):
	UNIVENTION_DISK_ROOT	OK	2021-09-29 14:53:34	209d 5h 15m 30s	1/10	DISK OK - free space: / 15085 MB (79% inode=91%):
	UNIVENTION_DNS	OK	2021-09-29 14:46:08	110d 6h 35m 52s	1/10	DNS OK: 0.009 seconds response time. www.univention.de returns 78.47.199.152
	UNIVENTION_JOINSTATUS	OK	2021-09-29 13:48:28	40d 1h 6m 57s	1/1	OK: system joined successfully
	UNIVENTION_LOAD	OK	2021-09-29 14:52:10	132d 7h 8m 22s	1/1	OK - load average: 0.00, 0.00, 0.00
	UNIVENTION_NSCD2	OK	2021-09-29 14:49:41	209d 5h 7m 35s	1/2	OK: nsd is running.
	UNIVENTION_NTP	OK	2021-09-29 14:46:54	40d 3h 58m 49s	1/10	NTP OK: Offset -1,177191734e-05 secs
	UNIVENTION_PACKAGE_STATUS	OK	2021-09-29 13:58:37	358d 20h 45m 2s	1/1	OK: Package status OK
	UNIVENTION_PING	OK	2021-09-29 14:53:27	108d 15h 40m 31s	1/10	PING OK - Packet loss = 0%, RTA = 0.27 ms
	UNIVENTION_REPLICATION	OK	2021-09-29 14:54:41	40d 4h 15m 57s	1/5	OK: replication complete (nid=12162 lid=12162)
server.paedml-linux.local	LMZ_DISK_HOME	OK	2021-09-29 14:54:20	948d 0h 8m 40s	1/10	DISK OK - free space: /home 161708 MB (99% inode=99%):
	LMZ_DISK_VAR	OK	2021-09-29 14:46:58	948d 0h 13m 37s	1/10	DISK OK - free space: /var 41885 MB (78% inode=95%):

Abb. 100.1.16: Details zu den überwachten Diensten Update Screenshot

Das Menü „Host Detail“ schließlich zeigt eine Übersicht über alle verfügbaren Maschinen, jedoch ohne die einzelnen Services und deren Status anzuzeigen.

Current Network Status
 Last Updated: Wed Sep 29 14:55:34 CEST 2021
 Updated every 90 seconds
 Nagios® Core™ 4.3.4 - www.nagios.org
 Logged in as Administrator

View Service Status Detail For All Host Groups
 View Status Overview For All Host Groups
 View Status Summary For All Host Groups
 View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
3	0	0	0

All Problems All Types

0	3
---	---

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
31	1	0	0	0

All Problems All Types

1	32
---	----

Host Status Details For All Host Groups

Limit Results:

Host	Status	Last Check	Duration	Status Information
backup.paedml-linux.local	UP	2021-09-29 14:54:50	188d 20h 45m 59s	PING OK - Packet loss = 0%, RTA = 0.25 ms
firewall.paedml-linux.local	UP	2021-09-29 14:55:14	84d 2h 7m 32s	PING OK - Packet loss = 0%, RTA = 0.30 ms
server.paedml-linux.local	UP	2021-09-29 14:55:12	948d 1h 20m 13s	PING OK - Packet loss = 0%, RTA = 0.10 ms

Results 1 - 3 of 3 Matching Hosts

Abb. 100.1.17: Übersicht über die überwachten Server

Das Menü „Reporting“ bietet Ihnen vielfältige Möglichkeiten über den Status Ihrer Systeme auszuwerten. Sie können sich hier Ansichten erstellen, die beispielsweise zeigen, wie häufig es in einem bestimmten Zeitraum Fehler gab. Dadurch können zum Beispiel regelmäßig auftretende Probleme erkannt und es kann gegengesteuert werden.

Im Menü „*Configuration*“ sollten – wie Eingangs beschrieben – keine Änderungen vorgenommen werden, da Nagios nur im Auslieferungszustand von der Hotline unterstützt wird.



Bei Nagios handelt es sich um ein hochkomplexes Werkzeug zur Überwachung von Computern.

Wenn Sie tiefer in die Materie einsteigen wollen, bitten wir Sie darum die Homepage von Nagios (<http://www.nagios.org/>) oder einschlägige Internetforen zu besuchen.

Auf der rechten Bildschirmseite sehen Sie eine Übersicht über den Zustand Ihres Netzwerks. Vollständige grüne Balken signalisieren, dass alles in Ordnung ist. Wenn es Probleme gibt, dann werden die Balken kleiner, bzw. rot.



Abb. 100.1.18: Alles in Ordnung

15.3 Übersicht über die überwachten Dienste

Für das Monitoring bringt *Nagios* eine umfassende Sammlung an Überwachungsmodulen mit. Diese können neben der Abfrage von Systemkennzahlen (z.B. CPU- und Speicherauslastung, freie Festplattenkapazität) auch die Erreichbarkeit und Funktion unterschiedlicher Dienste (z.B. SSH, SMTP, HTTP) testen.

Für die Funktionstests werden in der Regel einfache Programmschritte wie das Ausliefern einer Testmail oder das Auflösen eines DNS-Eintrags durchgeführt. Neben den in *Nagios* enthaltenen Standardmodulen werden auch *paedML*-spezifische Überwachungsmodule mitgeliefert.

Nagios unterscheidet drei grundlegende Betriebszustände für einen Dienst:

„OK“ ist der Regelbetrieb

„*CRITICAL*“ beschreibt einen aufgetretenen Fehler, z.B. ein Webserver, der nicht erreichbar ist

„*WARNING*“ deutet auf einen möglicherweise bald auftretenden Fehlerzustand hin und ist somit eine Vorstufe zu „*CRITICAL*“.



Beispiel: Der Test für ausreichend freien Speicherplatz auf der Root-Partition löst erst ab 90 Prozent Füllstand einen Fehler aus, aber bereits ab 75 Prozent eine Warnung.

An diesem Beispiel kann man sehen, dass *Nagios*-Meldungen immer im Kontext des jeweiligen Systems gelesen werden müssen. Ein 75%-ige Festplattenbelegung bei einem System mit 200 GB Festplattenspeicher ist kritischer als wenn ein System mit 2 TB Festplattenspeicher zu 75% belegt ist.

Nagios ist also so konfiguriert, dass Dienste überwacht werden, die für die Funktionsfähigkeit der *paedML*-Server benötigt werden. *Nagios* überprüft regelmäßig den Zustand der überwachten Dienste und gibt eine Fehlermeldung aus, wenn es Probleme gibt.

Nagios-Dienst	Funktion
LMZ_DISK_VAR	Überwacht den freien Plattenplatz auf der /var-Partition.
LMZ_DISK_HOME	Überwacht den freien Plattenplatz auf der /home-Partition.
UNIVENTION_PING	Testet die Erreichbarkeit des überwachten UCS-Systems mit dem Kommando ping. In der Standardeinstellung wird der Fehlerzustand erreicht, wenn die Antwortzeit 50ms bzw. 100ms überschreitet oder Paketverluste von 20% bzw. 40% auftreten.
UNIVENTION_DISK_ROOT	Überwacht den Füllstand der root-Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% bzw. 10% wird der Fehlerzustand gesetzt.
UNIVENTION_DNS	Testet die Funktion des lokalen DNS-Servers und die Erreichbarkeit der öffentlichen DNS-Server durch die Abfrage des Rechnernamens www.univention.de. Ist für die UCS-Domäne kein DNS-Forwarder definiert, schlägt diese Abfrage fehl. In diesem Fall kann www.univention.de z.B. gegen den FQDN des Domaincontroller Master ersetzt werden, um die Funktion des Namensauflösung zu testen.
UNIVENTION_LOAD	Überwacht die Systemlast.
UNIVENTION_LDAP	Überwacht den auf Domänencontrollern laufenden LDAP-Server.
UNIVENTION_NTP	Fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 bzw. 120 Sekunden auf, wird der Fehlerzustand erreicht.
UNIVENTION_SMTP	Testet den Mailserver.
UNIVENTION_SSL	Testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Domänencontroller Master- und Domänencontroller Backup-Systeme geeignet.
UNIVENTION_SWAP	Überwacht die Auslastung der Swap-Partition. Unterschreitet der verbleibende freie Platz den Schwellwert (in der Standardeinstellung 40% bzw. 20%), wird der Fehlerzustand gesetzt.
UNIVENTION_REPLICATION	Überwacht den Status der LDAP-Replikation, erkennt das Vorhandensein einer failed.Idif-Datei sowie den Stillstand der Replikation und warnt vor zu großen Differenzen der Transaktions-IDs.

UNIVENTION_NSCD	Testet die Verfügbarkeit des Name Server Cache Dienstes. Läuft kein NSCD-Prozess wird ein CRITICAL-Event ausgelöst, läuft mehr als ein Prozess ein WARNING-Event.
UNIVENTION_WINBIND	Testet die Verfügbarkeit des Winbind-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_SMBD	Testet die Verfügbarkeit des Samba-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_NMBD	Testet die Verfügbarkeit des NMBD-Dienstes, der in Samba für den Netbios-Dienst zuständig ist. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_JOINSTATUS	Prüft den Join-Status eines Systems. Ist ein System noch nicht Mitglied der Domäne, wird ein CRITICAL-Event ausgelöst, sind nicht-aufgerufene Joinskripte vorhanden, wird ein WARNING-Event zurückgeliefert.
UNIVENTION_KPASSWD	Prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Domänencontroller Master/Backup). Läuft weniger oder mehr als ein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_CUPS	Überwacht den CUPS-Druckdienst. Läuft kein cupsd-Prozess oder ist die Weboberfläche auf Port 631 ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_DANSGUARDIAN	Überwacht den Webfilter Dansguardian. Läuft kein Dansguardian-Prozess oder ist der Dansguardian-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_SQUID	Überwacht den Proxy Squid. Läuft kein Squid-Prozess oder der Squid-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_LIBVIRT_KVM	Prüft den Status eines KVM-Virtualisierungs-Servers über eine Anfrage an virsh und gibt den Status CRITICAL zurück, wenn die Rückmeldung mehr als zehn Sekunden dauert.
UNIVENTION_LIBVIRT_XEN	Prüft den Status eines Xen-Virtualisierungs-Servers über eine Abfrage an virsh und gibt den Status CRITICAL zurück, wenn die Rückmeldung mehr als zehn Sekunden dauert.
UNIVENTION_UVMMD	Prüft den Status des UCS Virtual Machine Managers über eine Anfrage der verfügbaren Nodes. Können sie nicht aufgelöst werden, wird der Status CRITICAL zurückgegeben.
UNIVENTION_opsi	Überwacht den opsi-Daemon. Läuft kein opsi-Prozess oder die opsi-Weboberfläche ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.

Tabelle 18: Nagios Dienste der paedML Linux

16 Horde Groupware

Auf dem *paedML Linux Server* läuft *Horde*. *Horde* ist eine Groupware-Lösung, die neben dem Mailversand auch Kalender und andere Funktionen für die Zusammenarbeit im Team anbietet. Mit diesem Programm kann im Unterricht das Thema E-Mail gelehrt und gelernt werden⁶¹. Bitte beachten Sie die folgenden Hinweise:

1. **Die Einrichtung von Horde ist NUR für den internen Gebrauch konfiguriert.** Eine Öffnung nach außen ist seitens des Support-Netzes nicht vorgesehen und wird nicht durch die Hotline unterstützt.
2. Die Verfügbarkeit der Mailadresse eines Benutzers hängt davon ab, ob der Benutzer beim Anlegen eine Adresse zugewiesen bekommen hat. Benutzer können auch nachträglich über die Schulkonsole (Modul: „Domäne | Benutzer“) eine Mailadresse zugewiesen bekommen.
3. **Der Support seitens der Linux-Hotline beschränkt sich auf den Einsatz von Horde als Mailclient zur Verwendung im Schulnetz. Andere Funktionen – wie das Versenden und der Empfang von Mails außerhalb des Schulnetzes, die Kalenderfunktion oder weitere Features von Horde werden nicht unterstützt.**

Weiterführende Informationen zur Bedienung *Horde* finden Sie unter <http://www.horde.org/>.

16.1 Aufruf von Horde

Adresse: <https://server.paedml-linux.lokal/horde>

Sie können die Webseite von *Horde* von jedem Rechner im Schulnetz über die Adresse <https://server.paedml-linux.lokal/horde> erreichen. Sofern für den jeweiligen Benutzer ein Mailkonto im System angelegt ist, kann sich dieser mit seinem Kennwort an Horde anmelden.

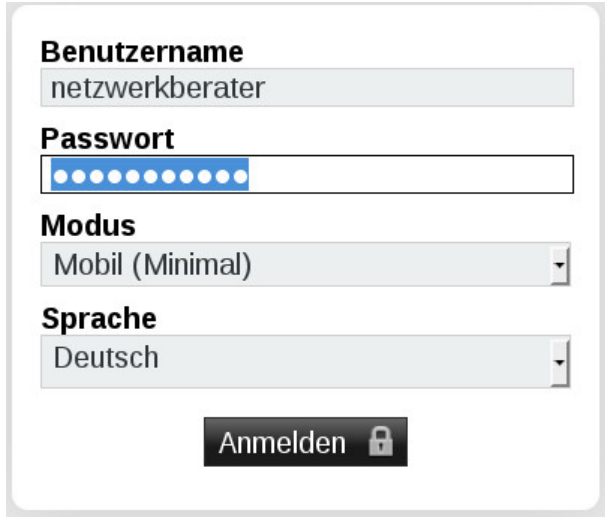


Abb. 100.1.19: Anmeldebildschirm von Horde

⁶¹ Bitte beachten Sie hierfür die Hinweise unter http://lehrerfortbildung-bw.de/sueb/recht/ds_neu/daten/email_unter/ und unter <http://www.it.kultus-bw.de/Lde/830504>

Nach dem erfolgten Login sehen Sie die Übersichtsseite. Diese gliedert sich grob in zwei Bereiche.

1. Die obere Leiste (1) bietet den Zugriff auf die verschiedenen Horde Module. Hier finden Sie Informationen wie das aktuelle Datum und den eingewählten Benutzer. Auf der linken Seite (3) können Sie das Programm konfigurieren oder sich über den orangenen Knopf abmelden.
2. Das Hauptfenster des Programmes (4) zeigt den Inhalt des jeweiligen Moduls an. Im folgenden Screenshot sehen Sie die Übersichtsseite, die Sie nach erfolgtem Login oder durch einen Klick auf das „Horde“-Logo oben links aufrufen können. Die Übersichtsseite kann von jedem Benutzer an die eigenen Bedürfnisse angepasst werden. Hierfür klicken Sie bitte auf den Knopf „Inhalt hinzufügen“ (2).



Abb. 100.1.20: Startseite von Horde

16.2 Posteingang

Im vorigen Bild sehen Sie in der Übersicht unter „Webmail“ den Status Ihres Posteingangs. Mit einem Klick auf „Posteingang“ gelangen Sie in Ihr Postfach.



Abb. 100.1.21: Weiter zum eigenen Postfach

Das Postfach gliedert sich in drei Bereiche.

1. Auf der linken Seite (1) sehen Sie die Ordnerstruktur. Hier können Sie zum Beispiel auf gesendete Mails zugreifen.
2. In der Mitte der rechten Seite (3) des Fensters sehen Sie eine Übersicht über Ihre E-Mails.
3. Im unteren Drittel der rechten Seite des Fensters sehen Sie die jeweils ausgewählte Mail angezeigt.

Ein Klick auf „Neue Nachricht“ (4) öffnet ein neues Fenster für die Eingabe einer neuen Nachricht.

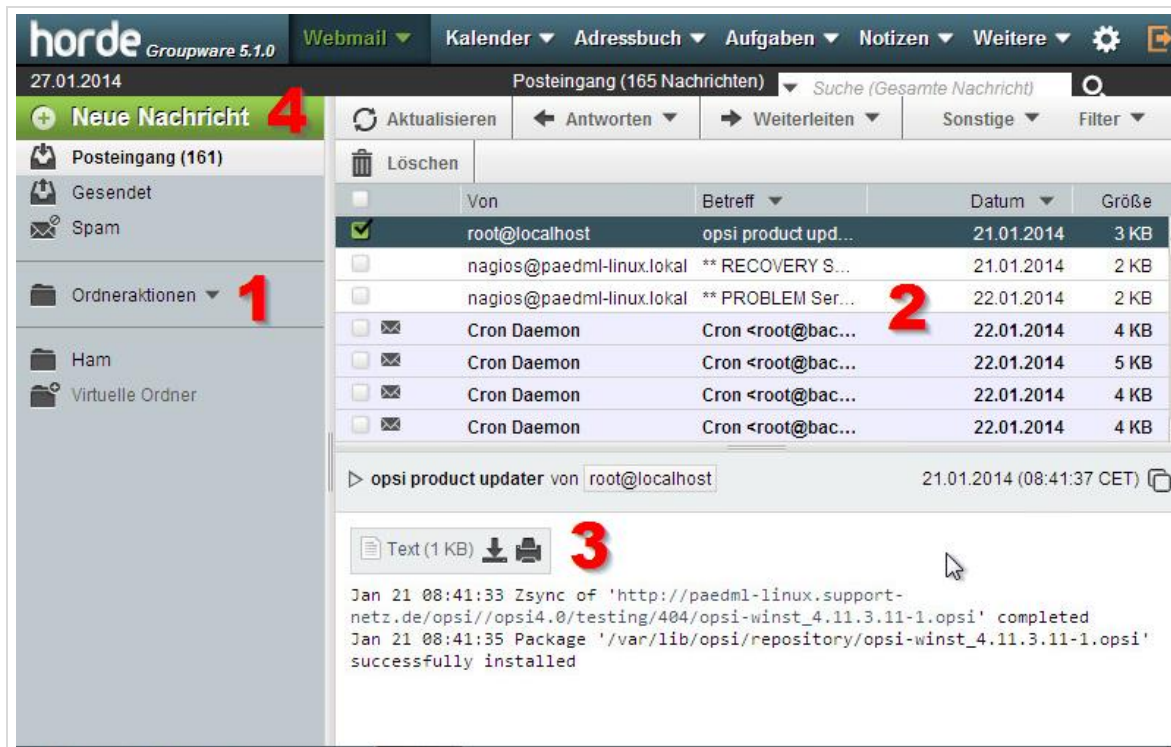


Abb. 100.1.22: Der Posteingang

Im Posteingang finden Sie zwei Ordner, die einer kurzen Erläuterung bedürfen:

1. Der erste Ordner „Spam“ hilft bei der Einordnung von nützlichen und unerwünschten Mails. Der Ordner „Ham“ dient dazu Mails, die als „Spam“ markiert wurden, aber nicht als solche behandelt werden sollen, künftig zu erhalten. Hierfür gibt es die Möglichkeit, E-Mails mit einem Bayes-Klassifikator bewerten zu lassen. Dieser vergleicht eine eingehende E-Mail mit statistischen Daten, die er aus bereits verarbeiteten E-Mails gewonnen hat und kann so seine Bewertung an die Mailgewohnheiten anpassen. Die Bayes-Klassifizierung wird vom Benutzer selbst gesteuert, in dem nicht als Spam erkannte E-Mails in den Unterordner Spam verschoben und eine Auswahl legitimer Mails in den Unterordner Ham kopiert werden. Diese Ordner werden täglich ausgewertet und noch nicht erfasste oder bisher falsch klassifizierte Daten in einer gemeinsamen Datenbank erfasst. Diese Auswertung ist in der Grundeinstellung aktiviert und kann mit der Univention Configuration Registry-Variable `mail/antispam/learndaily` konfiguriert werden.
2. Der virtuelle Posteingang („Virtuelle Ordner“) ist eine gespeicherte Suchabfrage, die es Ihnen abnimmt, in allen Ordnern nach neuen Nachrichten zu schauen. Stattdessen werden alle Ordner, die Sie für diesen Zweck in der Ordner Navigation ausgewählt haben, automatisch nach neuen Nachrichten durchsucht und in einer einzigen Übersicht angezeigt. Diese Funktion ist nützlich, wenn Sie mehrere Mailkonten über Horde abrufen. Da in der *paedML Linux* nur jeweils ein Mailkonto pro Nutzer aktiv ist; empfehlen wir Mails nur über den Standardordner „Posteingang“ zu lesen.

16.3 Versand von E-Mails

Es gibt zwei Wege eine neue Mail zu erstellen. Entweder Sie klicken in der Kopfleiste auf „Webmail | Neue Nachricht“ oder Sie benutzen den „Neue Nachricht“-Knopf im Posteingangsfenster.

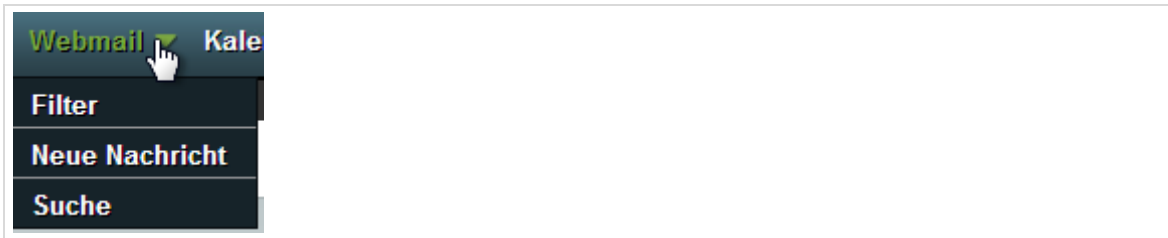


Abb. 100.1.23: Detail der Kopfleiste.

Wenn Sie eine neue Nachricht erstellen, dann wird ein neues Browserfenster geöffnet, in dem Sie die Mail bearbeiten können. Für den Versand einer neuen Mail geben Sie den Empfänger (Feld: „An“) ein. Hierbei reicht es Teile des Namens einzutippen (1), der Rest des Namens und die zugehörige E-Mailadresse werden automatisch mit den Daten, die im Adressbuch gespeichert sind, vervollständigt und können mit einem Klick ausgewählt werden (2). Geben Sie einen „Betreff“ und einen Nachrichtentext ein.

Sie haben verschiedene weitere Optionen wie eine „Rechtschreibprüfung“, die Möglichkeit einen „Anhang hinzu(zu)fügen“ oder Sie können den „HTML-Modus“ aktivieren und die Darstellung Ihrer Mail aufhübschen.

Ein Klick auf „Senden“ (oben links) verschickt die erstellte Nachricht.

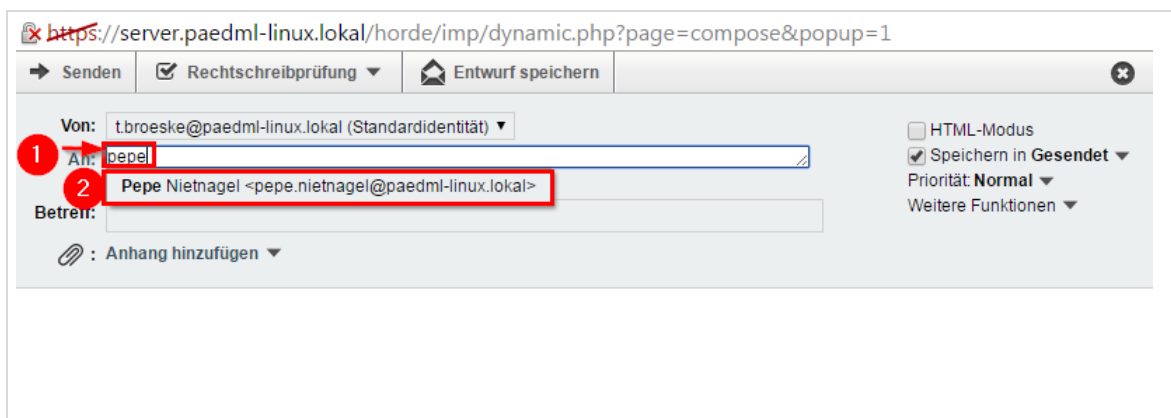


Abb. 100.1.24: Fenster für das Erstellen einer neuen Mail

16.4 Adressbuch

Um auf das Adressbuch zuzugreifen, gibt es in der Kopfleiste den Menüpunkt „Adressbuch“ dort können neue Kontakte angelegt werden und das persönliche Adressbuch verwaltet werden. Im Schul-Adressbuch sind alle Benutzer der Schule zu finden, die in der paedML aufgenommen wurden. Unter „Häufigste Empfänger“ sind die Kontakte zu finden, die am häufigsten kontaktiert wurden.

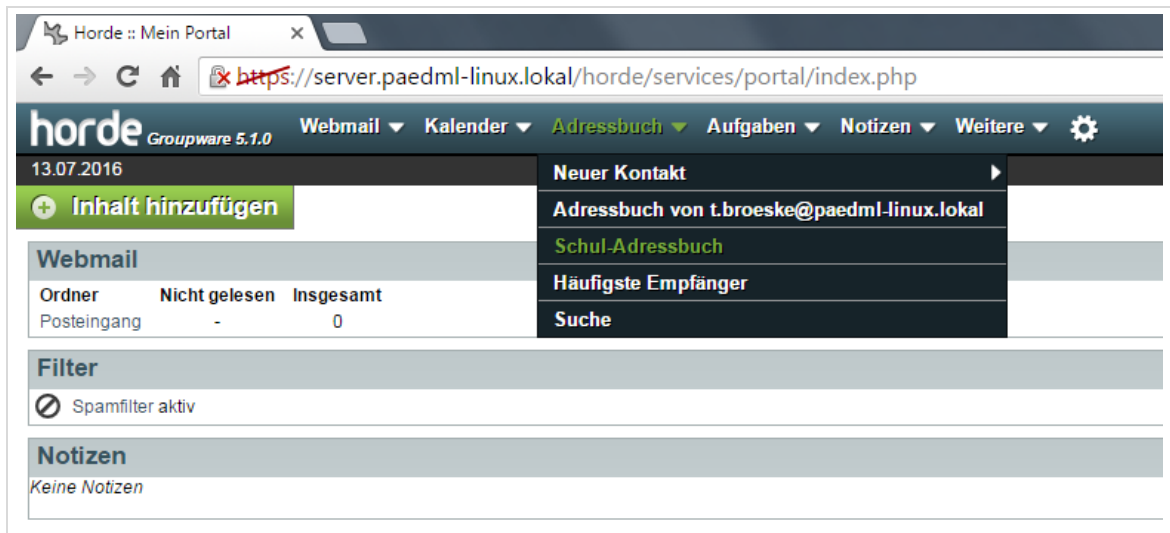


Abb. 100.1.25: Horde Adressbuch

16.5 Änderung von Anhangsgrößen (Attachments)

Die Größen der Anhänge von E-Mails in Horde sind beschränkt auf 10 MB. Eigentlich sollte dieser Wert ausreichend sein, zumal es Tauschverzeichnisse gibt, über die größere Dateien getauscht werden können.

Wenn Sie die Größe der Anhänge in Horde ändern wollen, geschieht dies über die UCR-Variable:
 horde/php/apache/cfg/upload_max_filesize

17 Verzeichnisstruktur Nutzerdaten

Bei der Anmeldung an einem Rechner bekommen die Benutzer – abhängig von Ihrer Benutzerrolle (vgl. Kapitel 1.2, Seite 17) Freigaben des *paedML* Servers auf ihren Desktop eingebunden.

Hierbei handelt es sich um das Homeverzeichnis des angemeldeten Benutzers, Freigaben von Gruppen, deren Mitglied der Benutzer ist (z.B. Lehrer-Tauschverzeichnis – bei Lehrern, Arbeitsgruppen- und Klassentauschverzeichnisse – bei Schülern) sowie die Programmlaufwerk *K:* und das Laufwerk *Programme-S*⁶².



Bitte speichern Sie als Administrator angemeldet keine Daten auf *\\SERVER\netlogon*. Dieses Verzeichnis wird täglich nach „*/var/univention-backup/samba/sysvol-DATUM.tar.bz2*“ gesichert. Sollten Sie dort größere Datenmengen speichern, wird sich der freie Speicher der „*/var*“-Partition immer mehr verkleinern, was zur Instabilität des Systems führen kann. Legern Sie Daten stattdessen auf dem Programme-Share (*K:*) ab.

Im Folgenden erhalten Sie eine Übersicht über die Verzeichnisse der *paedML Linux*, in denen Daten abgelegt werden. Es handelt sich hierbei um lokale Laufwerke, die Home-Verzeichnisse der Benutzer und um Tauschlaufwerke.

Verzeichnis	Inhalt
C:\	Lokale Festplatte Inhalte, die hier von Anwendern lokal abgelegt werden, werden nicht in das Benutzerprofil auf dem Server synchronisiert und gehen verloren!
H:\	Home-Laufwerk Benutzerdaten- und -profil
K:\	Laufwerk für die zentrale Installation von Programmen
T:\	Tauschlaufwerk (bei Lehrern: Lehrer-Tauschlaufwerk; bei Schülern: Klassen-Tauschlaufwerk)
Optional: Freigabe für alle beschreibbar	Kann bei Bedarf eingerichtet werden (s.u.)
Optional:	Weitere lokale Laufwerke (Festplattenpartitionen, Wechseldatenträger,...)

⁶² Dieses Laufwerk ist für alle Anwender sichtbar, muss aber – sofern Sie damit arbeiten wollen – gesondert eingerichtet werden.

Diese Laufwerke – und der Zugriff – sind abhängig von der Konfiguration der Arbeitsplatzrechner.

Tabelle 19: Laufwerke unter Windows

Außerdem finden Sie auf dem Desktop und im Windows-Dateimanager eine Verknüpfung namens „Freigaben“. Als Schüler angemeldet enthält der Ordner die Verknüpfungen zu „Meine Dateien“, PDF Drucker, Programme-S und dem Klassen-Tauschlaufwerk.

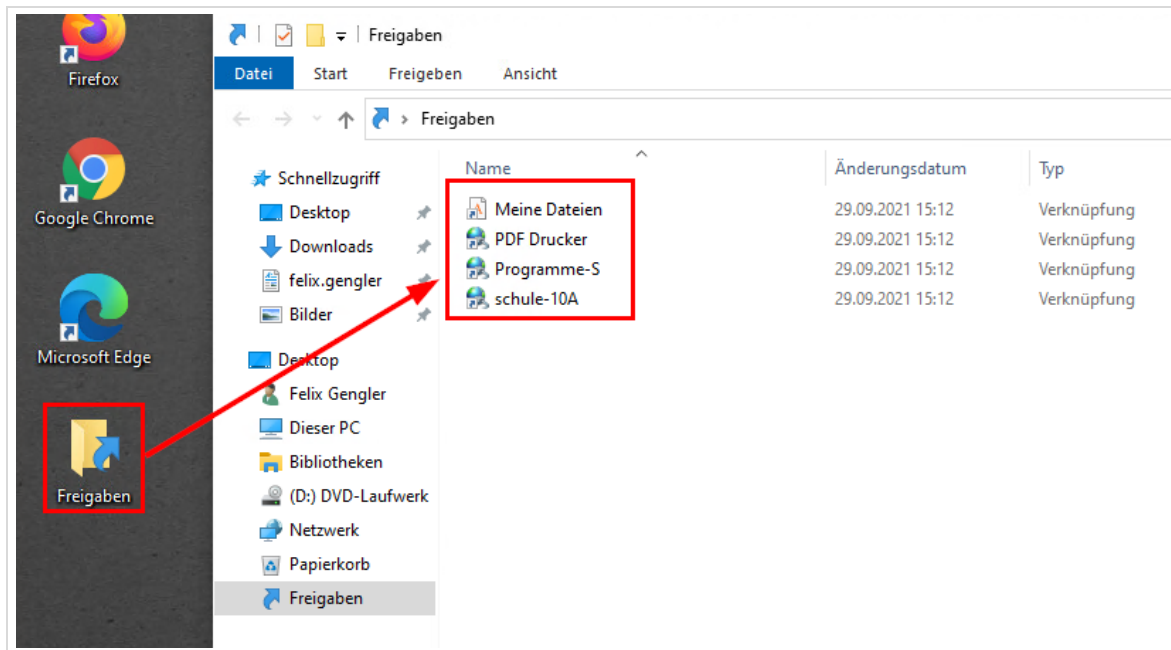


Abb. 100.1.26: „Freigaben“ eines Schülers

17.1 Anwendersicht auf Home-Verzeichnisse (H:\)



Home-Verzeichnisse von Benutzern werden auf dem Server erst angelegt, wenn sich Benutzer im System mindestens einmal angemeldet haben.

Vorher ist kein Zugriff auf diese Verzeichnisse möglich, da die Verzeichnisse nicht vorhanden sind.

Für jeden Benutzer der *paedML Linux* wird ein Home-Verzeichnis angelegt. Unter *Windows* wird das Laufwerk *H:* mit dem Homeverzeichnis des angemeldeten Benutzers verknüpft. Dabei werden die von *Windows* angelegten Ordner⁶³ in diesen Ordner umgeleitet. **Alle Daten, die nicht unter „H:\“ (bzw. in einem Tauschlaufwerk) gespeichert werden, werden gelöscht, wenn sich der Benutzer vom Rechner abmeldet.**

⁶³ Hierbei handelt es sich ab *Windows 7* um die sogenannten „special folders“ *Windows* inklusive dem „Desktop“ (vgl. <http://de.wikipedia.org/wiki/Sonderverzeichnis>).

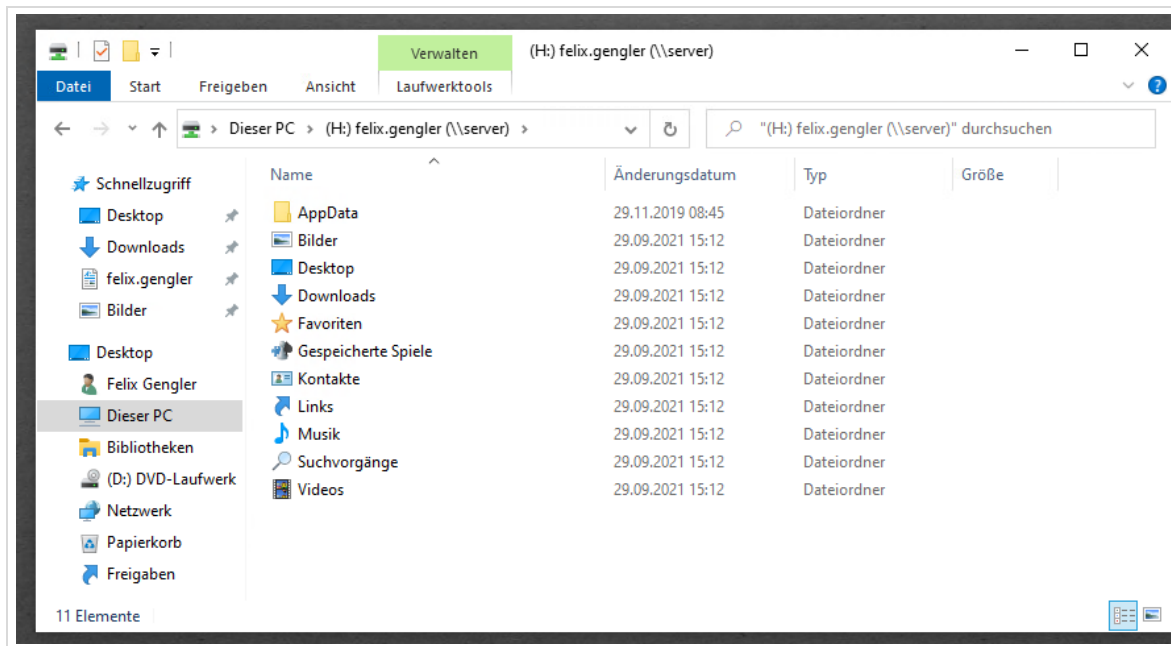


Abb. 100.1.27: Inhalt eines neu angelegten Home-Verzeichnisses Neuer Screenshot unter Windows 10

Der Zugriff auf `H:\` kann für alle Benutzer alternativ über den Aufruf der Desktop-Verknüpfung „Freigaben / Meine Dateien“ erfolgen.

17.2 Administratorsicht auf `/home`

Sie finden auf dem Server die folgenden Verzeichnisse unter `/home`:

Verzeichnisname	Inhalt
<code>/home/Administrator</code>	Home-Verzeichnis des Benutzers <i>Administrator</i> Windows-Freigabe <code>H:\</code> Speichern Sie hier alle Dateien, die Sie als Administrator auch im Netz verfügbar haben wollen. Alle Dateien von Administrator, die im eigenen Profil gespeichert werden, werden jeweils lokal auf dem Arbeitsplatz abgelegt und nicht auf den Server übertragen.
<code>/home/backup/BENUTZERNAME</code>	Daten gelöschter Benutzer
<code>/home/domadmin</code>	Der Benutzer domadmin sollte NUR für die Aufnahme von Clients in die Domäne genutzt werden!
<code>/home/groups</code> <code>/home/groups/klassen</code> <code>/home/groups/schule-ARBEITSGRUPPENNAME</code>	Ablageort für Tauschverzeichnisse (vgl. nächster Abschnitt)
<code>/home/groups/programme</code>	Ablageort für Programme, die auf dem Server installiert werden (vgl. Seite 209 ff.)

Optional: `/home/groups/programme-s`

<code>/home/lehrer/NACHNAME.VORNAME</code>	Home-Verzeichnisse der Lehrer Home-Verzeichnis des Benutzers <i>Windows-Freigabe H:\</i>
<code>/home/netzwerkberater</code>	Home-Verzeichnis des Benutzers „netzwerkberater“
<code>/home/schueler/_klassen</code>	Im Ordner „_klassen“ befinden sich alle angelegten Klassen (z.B. „5a“). Innerhalb der einzelnen Klassen werden Verknüpfungen zu den Home-Laufwerken der einzelnen Schüler angezeigt.
<code>/home/schueler/VORNAME.NACHNAME</code>	Home-Verzeichnisse der Schüler Home-Verzeichnis des Benutzers <i>Windows-Freigabe „H:“</i>

Tabelle 20 Verzeichnisse unter `/home` auf dem Server

17.3 Tauschverzeichnisse für Gruppen (T:\)

Die in der Schulkonsole angelegten Gruppen erhalten je ein Verzeichnis, in dem sich das Tauschlaufwerk der Gruppe befindet. Die Verzeichnisse liegen unter `/home/groups`.

- `/home/groups/klassen`
 - `/home/groups/klassen/lehrer-schule` – Tauschverzeichnis der Lehrer
 - `/home/groups/klassen/schule-KLASSENAME` – Klassentauschverzeichnis
- `/home/groups/schule-ARBEITSGRUPPENNAME` – Tauschverzeichnis der Arbeitsgruppe

Der Zugriff auf die Tauschverzeichnisse erfolgt über die Verknüpfung „Freigaben“, die sich auf dem Desktop befindet.

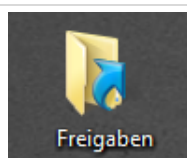


Abb. 100.1.28: Verknüpfung zu den Tauschlaufwerken

Die Inhalte der Verknüpfung sind – wie gesagt – abhängig von der Benutzerrolle. Sowohl Lehrer, als auch Schüler erhalten über die Verknüpfung „Meine Dateien“ Zugriff auf das eigene Homeverzeichnis und können über „PDF Drucker“ den PDF-Drucker einsehen.

Lehrer sehen die Klassen und Projekte, denen Sie zugeordnet sind und das Lehrer-Tauschverzeichnis („*Lehrer-schule*“).

Über die Verknüpfung „*Home-Verzeichnisse Schüler*“, der in „Freigaben“ liegt gelangen Sie zu den Homeverzeichnissen aller Schüler.

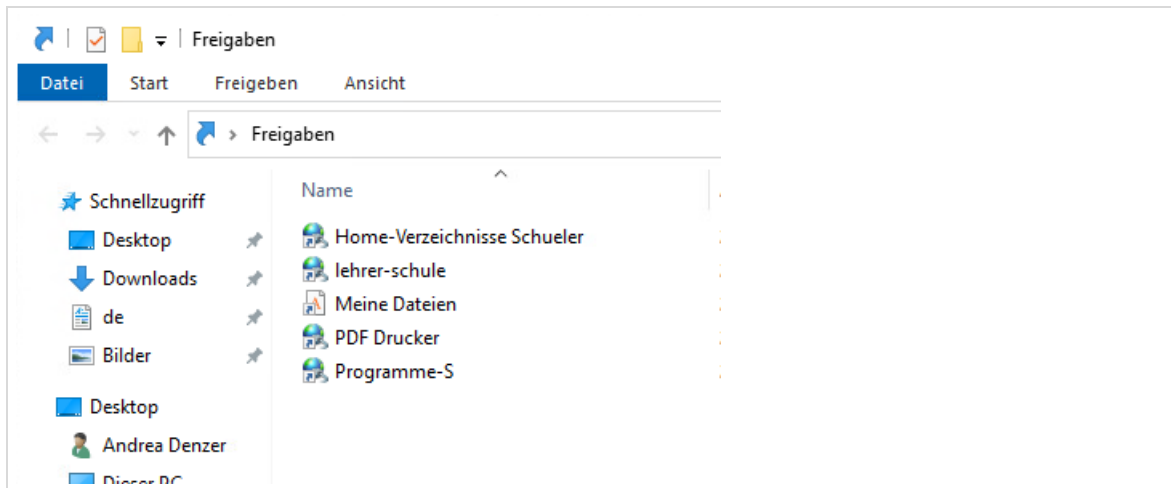


Abb. 100.1.29: Freigaben einer Lehrkraft

Bei Schülern sind jeweils nur die eigene Klasse, sowie die Arbeitsgruppen sichtbar.

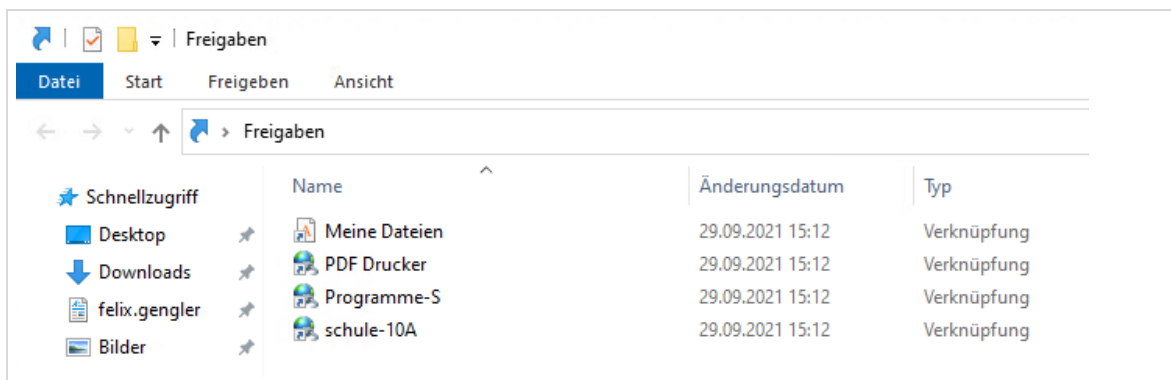


Abb. 100.1.30: Tauschlaufwerke eines Schülers.

17.4 Programmverzeichnis (K:\)

Unter `/home/groups/programme` werden auf dem Server Programme abgelegt, die über das Netzwerk ausgeführt werden können. Hierdurch entfällt die Installation auf den Clients. Die Installation des Programmes muss nur einmal durchgeführt werden und die Images der Arbeitsplatzrechner bleiben schlank.

Nachteil dieser Installationsart ist, dass bei Ausführen der Programme Last auf dem Netzwerk entstehen kann. Insbesondere wenn mehrere Nutzer gleichzeitig Programme auf dem Server ausführen.

Schreibenden Zugriff auf den Programme-Ordner hat die Gruppe „admins-schule“, also die Benutzer *netzwerkberater* und *Administrator*.

Wenn Sie ein Programm auf `K:\` installieren wollen, dann wählen Sie dieses Laufwerk als Installationsort während der Installationsroutine des Programmes aus.

Geben Sie als Installationspfad den UNC-Pfad der Verknüpfung „Programme“, sowie einen Namen für das Programm ein. Am Beispiel der Installation von Gimp-Portable ist der UNC-Pfad, in den das Programm installiert wird `\\server\Programme\gimp2`.

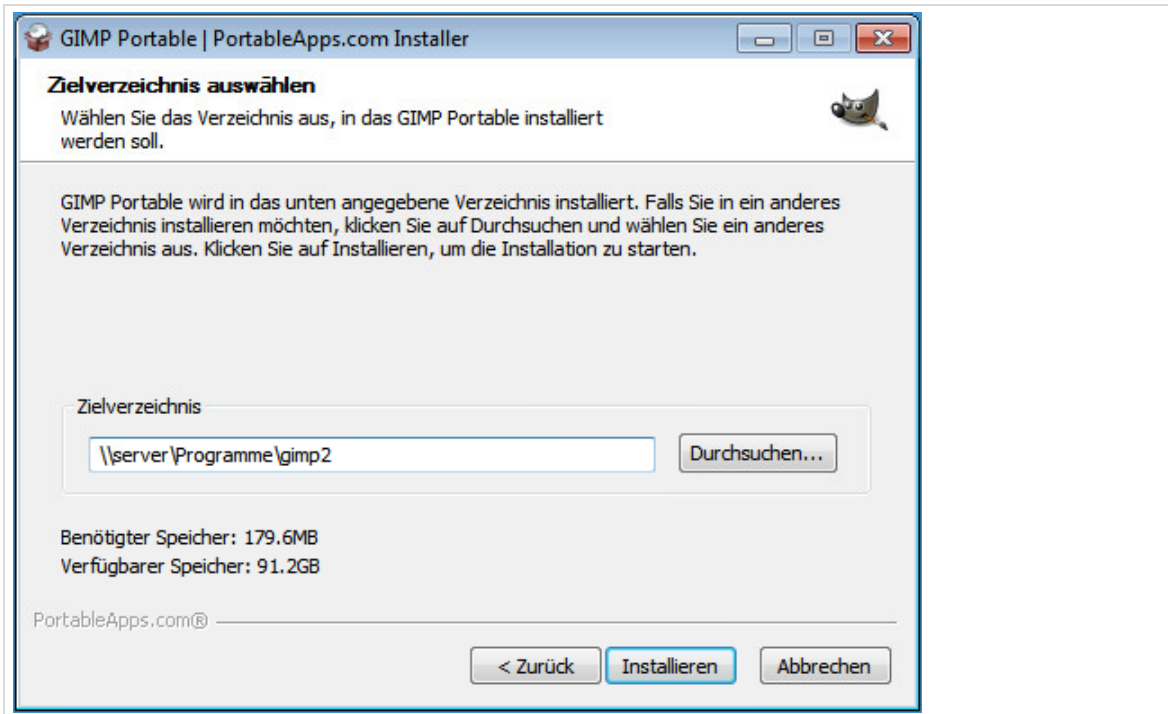


Abb. 100.1.31: Installation nach Programme (K:\)

In K:\ installierte Programme sind für alle Domänenbenutzer verfügbar.



Damit ein Programm über das Programmlaufwerk verfügbar gemacht werden kann, muss es die Netzwerkinstallation unterstützen.

Viele Programme benötigen eine lokale Installation, um lauffähig zu sein!

17.5 Für alle beschreibbares Share

Unter /home/groups/programme-s gibt es einen Ordner, der für alle Domänenbenutzer beschreibbar frei gegeben werden kann.

Hintergrund hierfür ist, dass es Programme gibt, die nur dann ausgeführt werden können, wenn der ausführende Benutzer auch Schreibzugriff auf den Installationsordner des Programmes hat. Ein prominentes Beispiel aus der Grundschule ist das Programm „Lernwerkstatt“.

Eine Standardinstallation in das Laufwerk K:\ würde verhindern, dass Schüler mit dem Programm arbeiten können, da sie keine Schreibrechte für die Freigabe haben.



Ein für alle Anwender beschreibbares Share hat nicht nur Vorteile:

- Neben nützlichen Dateien kann hier jeder Anwender auch unnütze Daten ablegen. Dieses Verzeichnis sollte regelmäßig aufgeräumt werden!
- Wenn alle Benutzer schreibend auf das Verzeichnis zugreifen können, dann können sie Daten auch (vorsätzlich oder versehentlich) löschen. Sie sollten das Verzeichnis ggf. gesondert sichern, um die Daten schnell wieder herstellen zu können.

Das für alle beschreibbare Verzeichnis ist im Auslieferungszustand aktiviert.

Die Installation in die Freigabe „Programme-S“ erfolgt analog zur Installation von Software in das Programmlaufwerk K:\ (vgl. Kapitel 17.4, Seite 209). Geben Sie als Installationspfad den UNC-Pfad der Verknüpfung „Programme-S“, sowie einen Namen für das Programm ein. Am Beispiel der Installation von Gimp-Portable ist der UNC-Pfad, in den das Programm installiert wird \\server\Programme-S\gimp2.

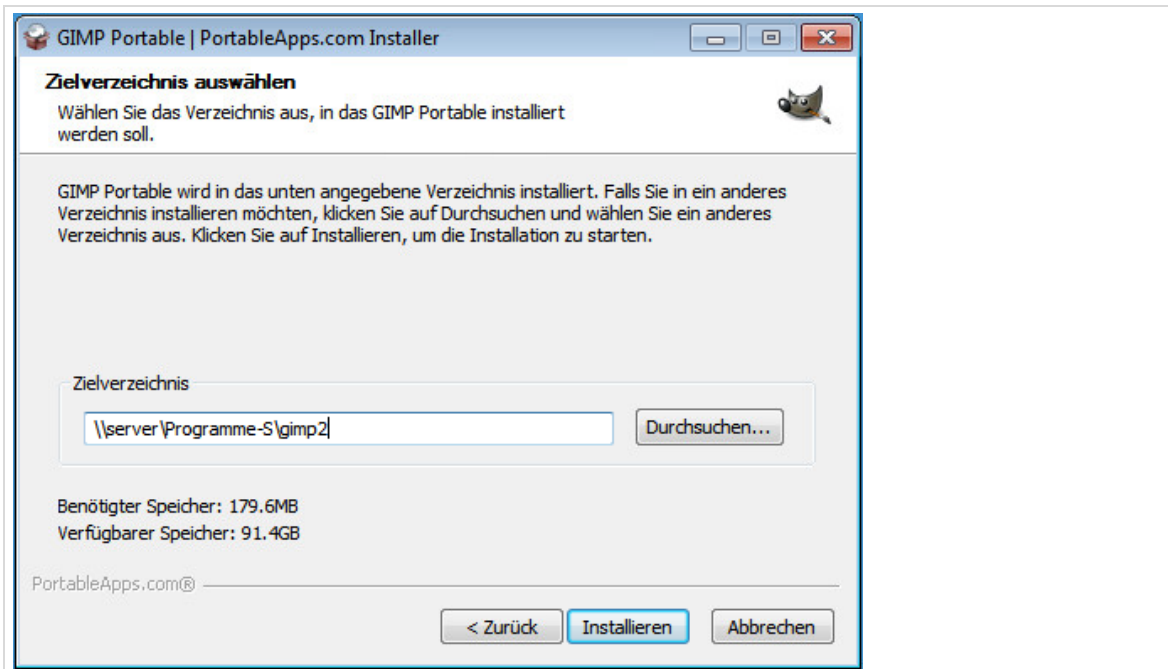


Abb. 100.1.32: Installation nach Programme-S

Um das Laufwerk zu deaktivieren, melden Sie sich als Benutzer *Administrator* an der *Schulkonsole* an. Navigieren Sie in das Menü „Domäne“ und wählen Sie dort den Eintrag „Freigaben“.

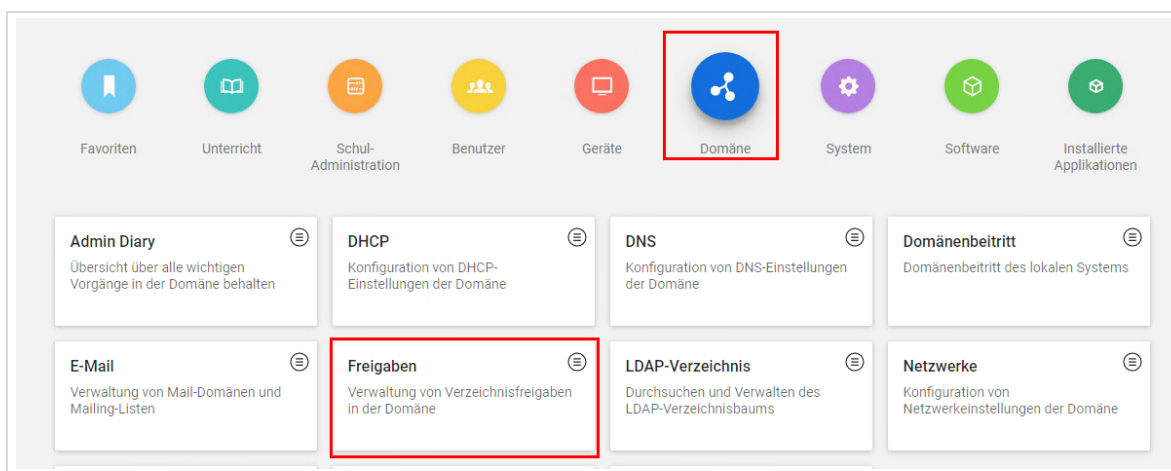


Abb. 100.1.33: Öffnen von „Domäne | Freigaben“

Es öffnet sich eine Liste mit allen im System eingerichteten Freigaben. **Hier darf außer dem beschriebenen Eintrag KEINE ÄNDERUNG vorgenommen werden!** Navigieren Sie zum Eintrag „Programme-S (/home/groups/programme-s...)“ und wählen Sie die Freigabe durch das Aktivieren der Checkbox vor dem Eintrag (Haken). Klicken Sie anschließend auf „Bearbeiten“.

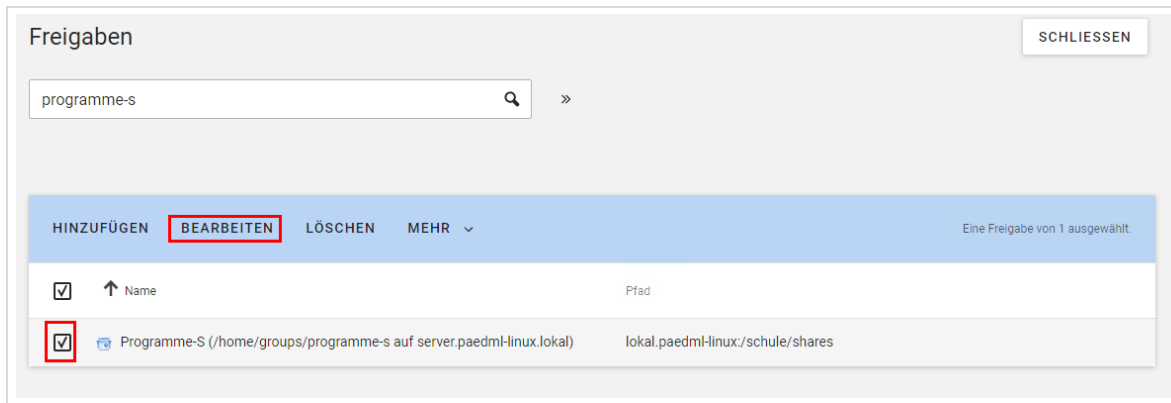


Abb. 100.1.34: Ändern der Freigabe „Programme-S“

Es öffnet sich ein neues Fenster, das verschiedene Reiter enthält. Die Aktivierung der Freigabe geschieht über den Reiter „Samba“. Die erste Checkbox muss für den Eintrag „Samba-Schreibzugriff“ deaktiviert werden, damit der Schreibzugriff für alle Benutzer deaktiviert wird.

Klicken Sie anschließend auf „Speichern“.

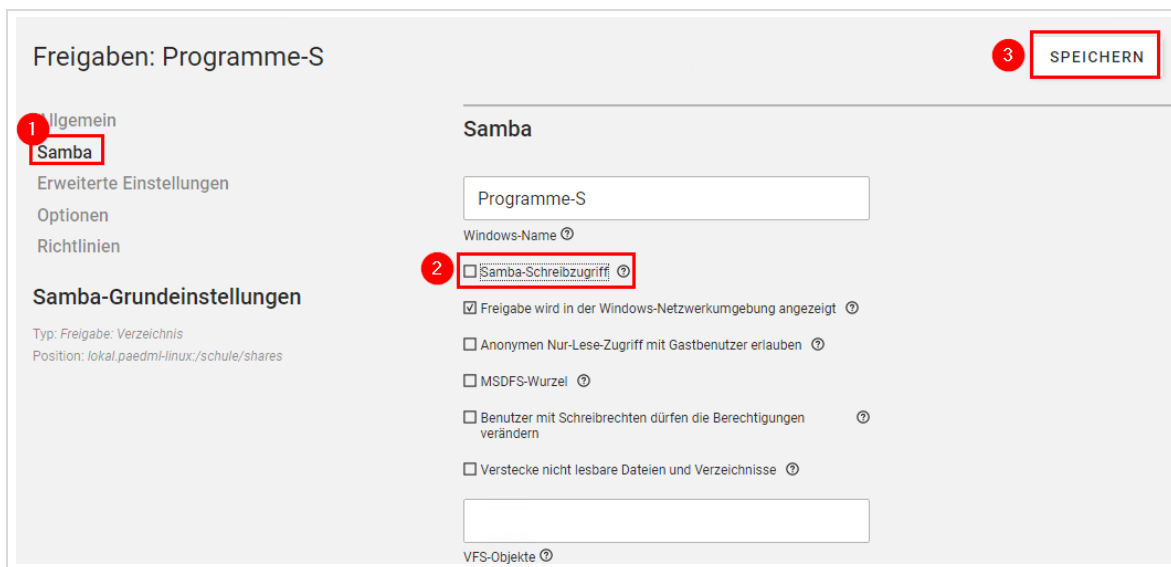


Abb. 100.1.35: Deaktivieren des Werts „Samba-Schreibzugriff“

Wenn diese Änderungen durchgeführt werden, dann können alle Benutzer – nach einer Neuansmeldung am Windows-Rechner nicht mehr auf das Verzeichnis *Programme-S* zugreifen, nachdem sie auf den Link „Freigaben“ auf dem Desktop geklickt haben.

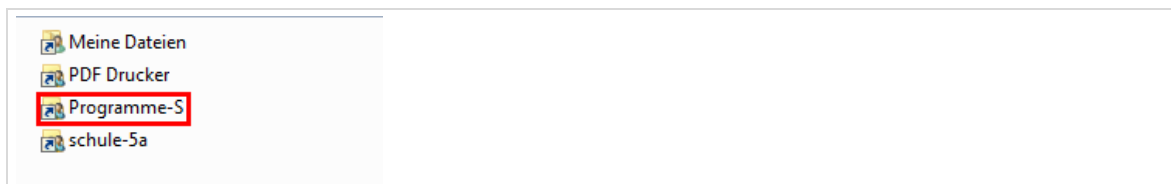


Abb. 100.1.36: Programme-S kann nicht mehr aufgerufen werden, wenn es deaktiviert wurde.

18 Datensicherung und Datenwiederherstellung



Wir empfehlen dringend die Sicherung des gesamten Systems. Eine ausführliche Anleitung (HowTo: Vollbackup und Wiederherstellung mit Veeam) kann hier abgerufen werden:

<https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#howtos>

19 Fernzugriff zur Wartung

Der Fernzugriff durch die Mitarbeiter der Linux-Hotline erfolgt über das Programm Teamviewer. Durch Teamviewer kann – ohne Einrichtung von Firewallregeln – direkt aus dem Internet auf einen Rechner zugegriffen und eine Fernwartung durchgeführt werden.

Das Programm liegt als opsi-Paket vor und kann über opsi installiert werden oder Sie können es unter www.teamviewer.com herunterladen und auf den fern zu steuernden Rechner einspielen.



Die Software *Teamviewer* ist NUR für den privaten Gebrauch kostenlos. Für die kommerzielle Nutzung – und hierzu zählt auch der Einsatz in der Schule – muss eine Lizenzgebühr an den Hersteller abgeführt werden.

19.1 Zugriff auf Teamviewer

Nachdem *Teamviewer* installiert wurde, können Sie das Programm auf dem fernzusteuenden Rechner ausführen, z.B. auf der W10AdminVM.

Das Hauptfenster des Programmes zeigt eine ID und ein zugehöriges Kennwort. Mit diesen Daten kann eine Remote-Verbindung zu dem Rechner aufgebaut werden. Das Kennwort ändert sich, sobald das Programm neu gestartet wird.

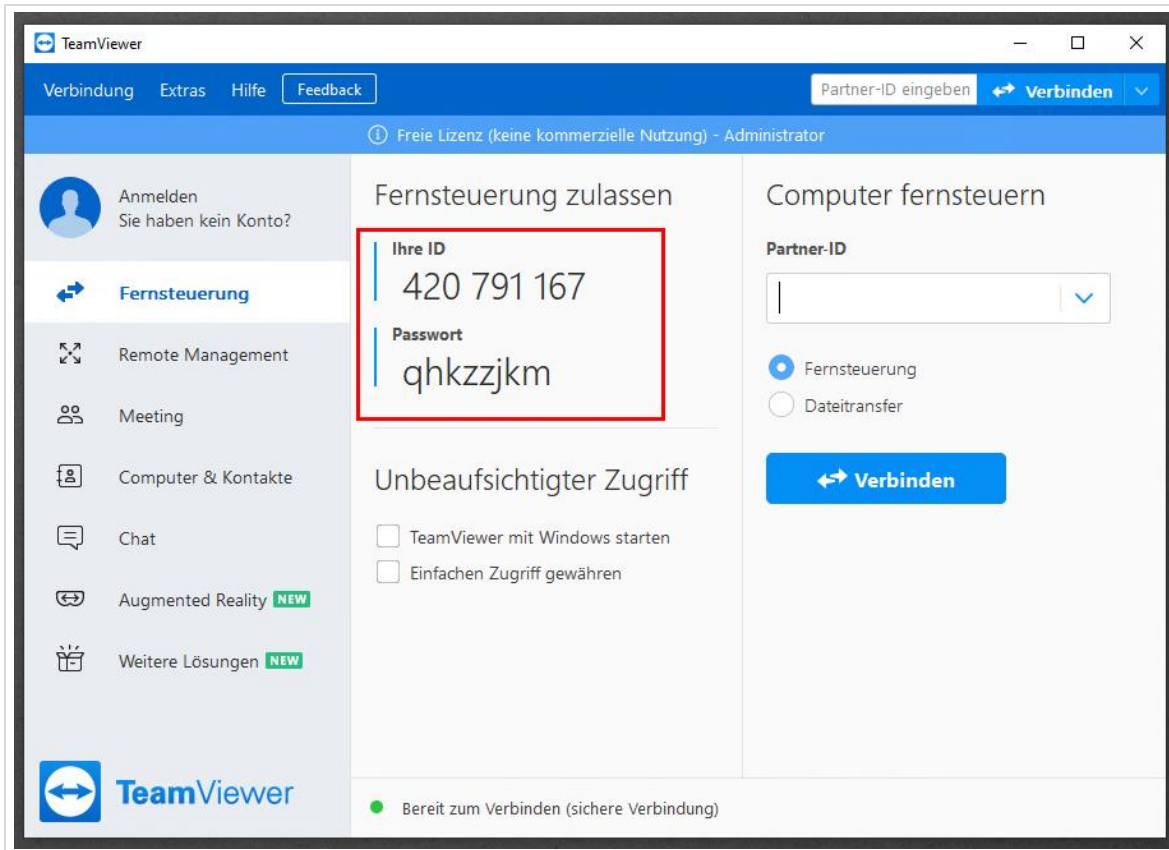


Abb. 100.1.38: Teamviewer

Es gibt zwei Optionen, wie die Hotline auf Ihren Rechner zugreift:

- Sie richten Teamviewer als Systemdienst ein, der automatisch beim Systemstart des Rechners gestartet wird (empfohlen).
- Sie müssen der Hotline jedes Mal den Zugriff gewähren, in dem Sie die ID und das tagesaktuelle Kennwort an den Hotline-Mitarbeiter übermitteln.



Wir empfehlen Ihnen ausdrücklich *Teamviewer* als Systemdienst zu installieren.

Dies hat den entscheidenden Vorteil, dass die Hotline jederzeit auf das System zugreifen kann, selbst wenn Sie nicht vor Ort sind. Somit kann eine Fehleranalyse durch die Hotline auch in Ihrer unterrichtsfreien Zeit erfolgen.

19.2 Einrichtung von Teamviewer als Systemdienst

Damit die Hotline-Mitarbeiter jederzeit auf Ihr System zugreifen können, müssen Sie *Teamviewer* als Systemdienst mit *Windows* starten. Öffnen Sie hierfür das Menü „Extras | Optionen“

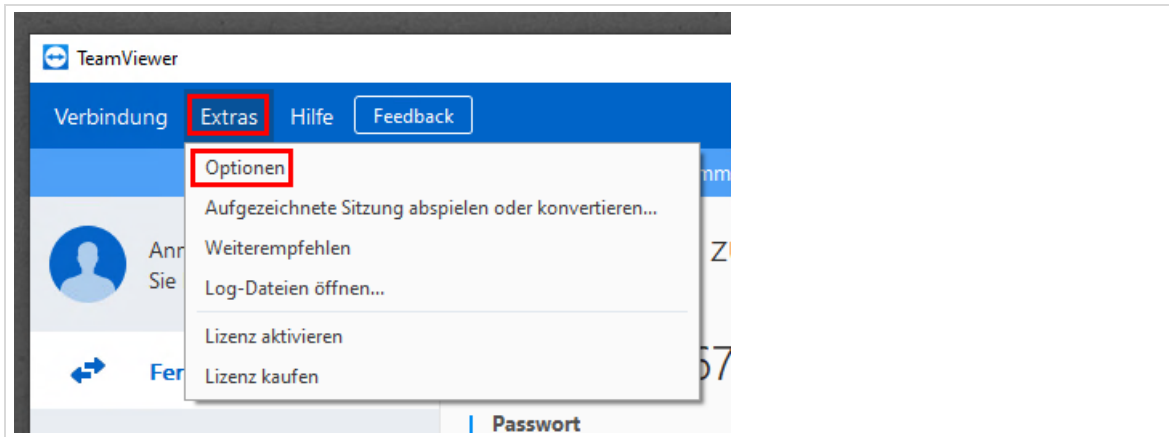


Abb. 100.1.39: Einrichtung Teamviewer als Systemdienst

Klicken Sie dann auf „Erweitert“ → „Erweiterte Einstellungen anzeigen“.

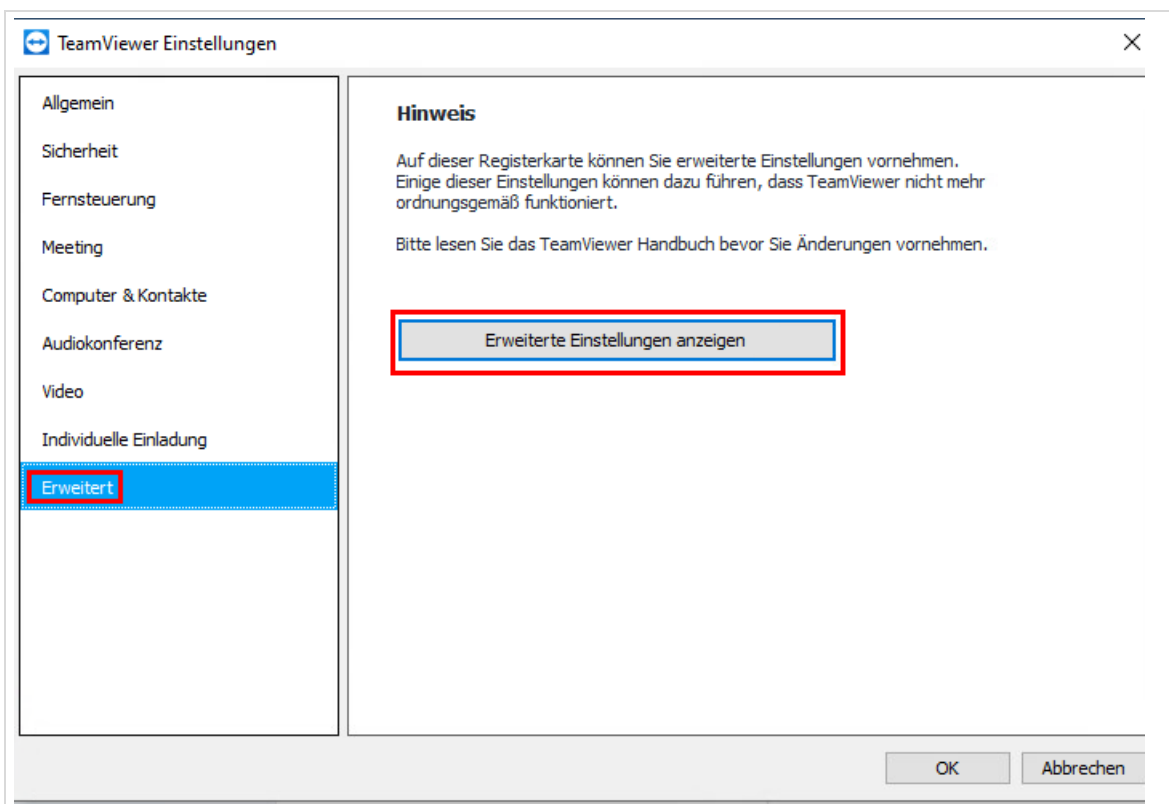


Abb. 100.1.40: Einrichtung Teamviewer als Systemdienst 1

Scrollen Sie dann bis zum Abschnitt „Persönliches Kennwort“. Geben Sie hier ein Kennwort ein, bestätigen Sie mit „OK“ und teilen Sie das Kennwort der Hotline mit.

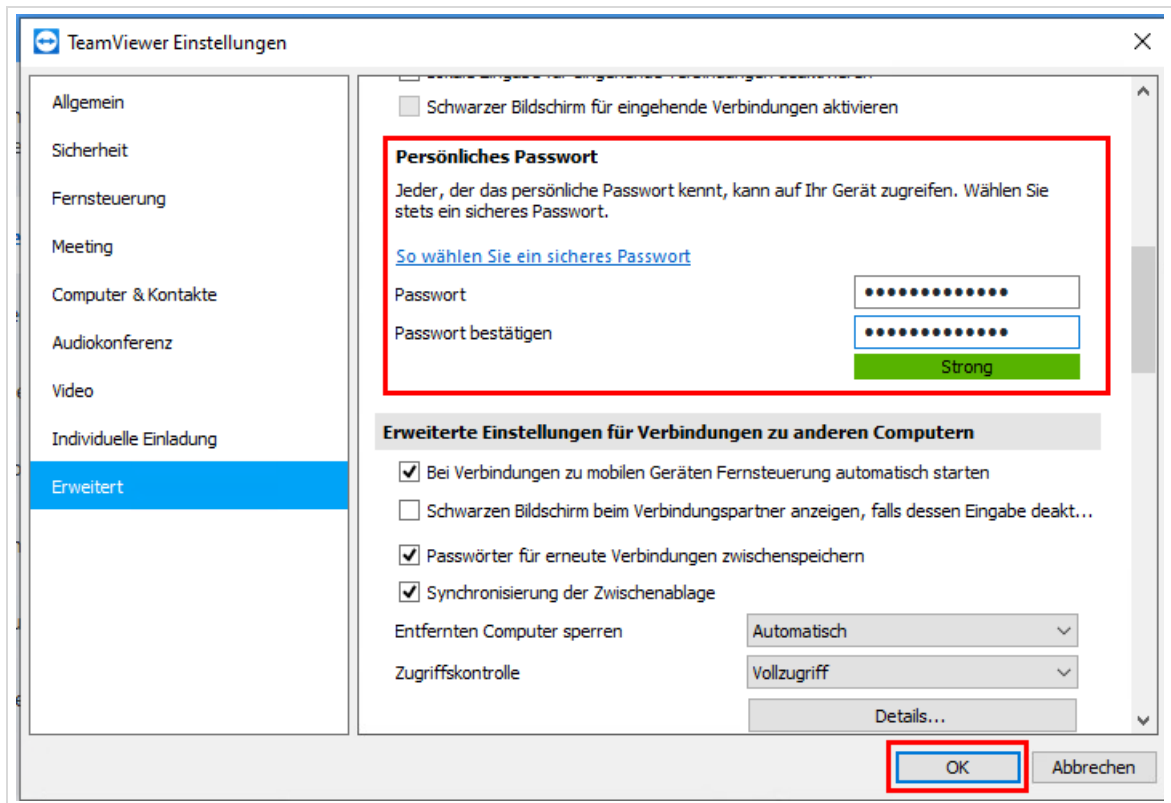


Abb. 100.1.41: Einrichtung Teamviewer als Systemdienst 2

20 Unterrichtzeiten



Da die Unterrichtszeiten in den Schulen variieren, ist es uns nicht möglich jede Situation vor Ort abzubilden. Im System sind vordefinierte Zeiten hinterlegt, die Sie in der *Schulkonsole* geändert werden sollten.

Die Einstellung der Unterrichtszeiten, können Sie in der Schulkonsole unter "*Schul-Administration / Unterrichtszeiten*" einsehen und ändern.

Beschreibung	Beginn	Ende	
1. Stunde	08:00	08:45	
2. Stunde	08:50	09:35	
3. Stunde	09:50	10:35	
4. Stunde	10:40	11:25	
5. Stunde	11:40	12:25	
6. Stunde	12:30	13:15	

Abb. 100.1.42: Definition der Unterrichtszeiten in der Schulkonsole

Die vorgegebenen Zeiten definieren die Unterrichtszeit. Nach Ablauf einer definierten Unterrichtsstunde werden im Computerraummodul („*Unterricht | Computerraum*“) vorgenommene Änderungen („*Benutzerdefinierte Einstellungen*“) automatisch zurückgesetzt.

Der Zeitraum, in dem eigene Einstellungen im Computerraummodul aktiv sind, kann auch händisch eingestellt werden. Dadurch kann der Automatismus des Zurücksetzens auf die Standardwerte zu einer im System festgelegten Uhrzeit umgangen werden. Dies ist beispielsweise dann interessant, wenn Sie eine Doppelstunde im Computerraum unterrichten.

Sie finden diese Einstellungsmöglichkeit im Computerraummodul über den Knopf „*Einstellungen ändern*“. Im obersten Feld „*Gültig bis*“ können Sie eine Uhrzeit festlegen, bis zu der die Einstellungen aktiv bleiben. Anschließend können Sie die Einstellungen ändern und mit „*Setzen*“ aktivieren.

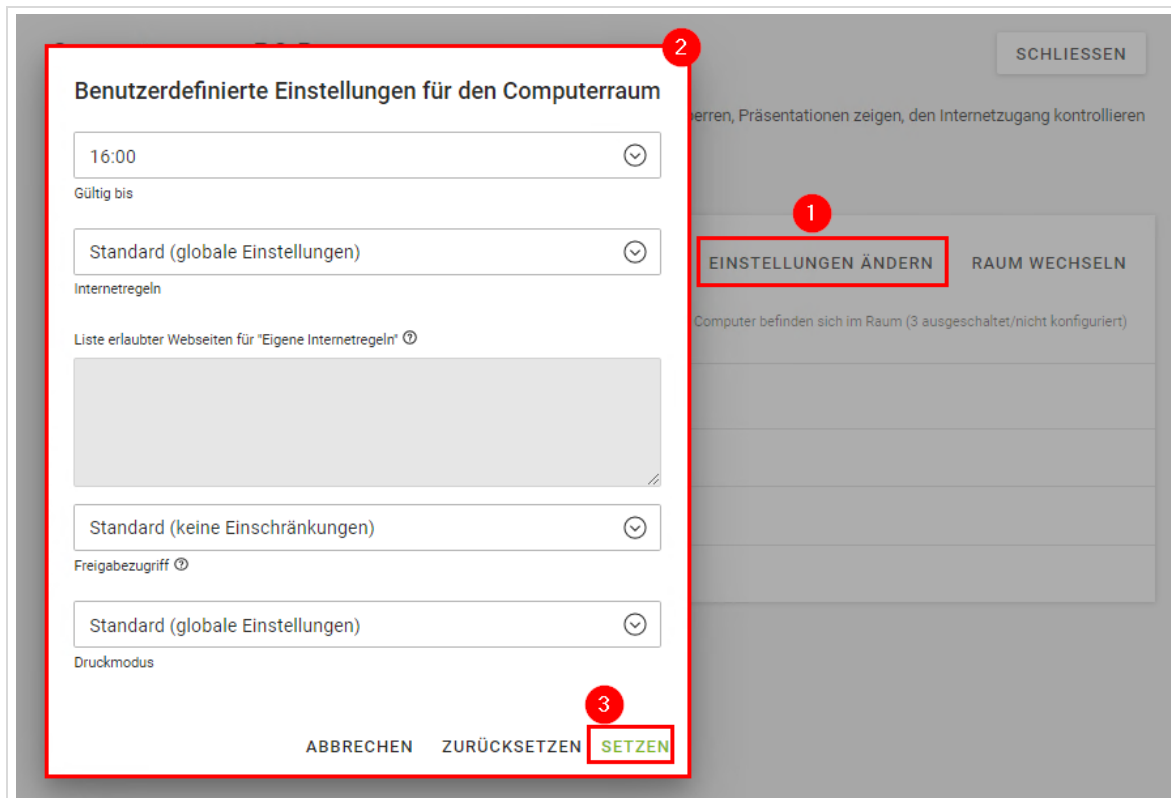


Abb. 100.1.43: Festlegen von Einstellungen für den Computerraum

Folgende Regeln greifen bei der Arbeit in Computerräumen

1. Internetregeln

Die Definition der Internetregeln geschieht über das Schulkonsolenmodul "Schuladministration / Internetregeln". Dort werden global Regeln für den Internetzugriff definiert. Die Zuweisung der Regeln für Klassen/Gruppen geschieht in der Schulkonsole unter „Schuladministration / Internetregeln zuweisen“. Computerraumregeln überschreiben die Werte für angemeldete Benutzer, sofern durch die unterrichtende Lehrkraft "Benutzerdefinierte Einstellungen" im Computerraummodul vorgenommen werden.

2. Ein Beispiel zur Illustration:

In einem Computerraum eines Gymnasiums ist eine AG mit Schülern der Klassen 5, 7 und der Jahrgangsstufe 2 angemeldet.

- Die Schüler der Klassen 5 und 6 dürfen im global definierten Filter nur auf die Schulhomepage zugreifen.
- Die Schüler der Klassen 7 bis 10 dürfen auf alle Seiten außer auf Facebook zugreifen.
- Die Jahrgangsstufen 1 und 2 haben unbeschränkten Zugang.
- Wenn im Computerraummodul der Wert für die Internetregeln auf „Unbeschränkt“ gesetzt wird, können alle Schüler auf alle Seiten zugreifen, solange sie im Computerraum angemeldet sind.

3. Druckmodus

Die Default-Einstellungen erlauben das Drucken in dem Raum. Der Druckerzugriff kann aber auch durch die Lehrkraft unterbunden werden (Feld: *Druckmodus*, Wert: *Drucken deaktiviert*).

4. Freigabezugriff

In den Standardeinstellungen wird der Zugriff auf Freigaben („Tauschverzeichnisse“) gewährt. Dieser Freigabezugriff kann aber auch beschränkt werden.

21 Known Issues

21.1 Lehrertauschverzeichnis

Es kann passieren, dass Lehrer in der Festplattenübersicht unter „Computer“ nicht das Lehrer-Tauschlaufwerk unter T:\ sondern ein Klassentauschlaufwerk einer Klasse, der sie zugewiesen sind, angezeigt bekommen.

Workaround:

Unterhalb der Desktop-Verknüpfung „Freigaben“ befindet sich eine Verknüpfung zum „richtigen“ Lehrer-Tauschlaufwerk.

21.2 Probleme bei der Domänenanmeldung

Windows-Rechner erhalten in einem Zyklus von 30 Tagen ein neues Computerkonto-Kennwort für die Anmeldung an der Domäne. Wenn ein Rechner mehr als 60 Tage nicht an der Domäne angemeldet war, erscheint beim Versuch sich an der Domäne anzumelden eine Fehlermeldung „die Vertrauensstellung mit der Domäne konnte nicht hergestellt werden“. Dieses Problem kann bei selten genutzten Systemen oder nach den Sommerferien auftreten.

Lösung

An den betroffenen Systemen muss via opsi-Konsole das Paket „windomain“ ausgespielt und dadurch ein erneuter Domänenbeitritt initiiert werden.

21.3 Internetzugriff für Apps

Die nachfolgende Beschreibung gilt auch für iOS und Android.

Mit Windows 10 wurde der App Store eingeführt, mit dem kostenlose und kostenpflichtige Apps von Microsoft und Drittanbietern installiert werden können. Manche Apps bereiten Probleme, da sie nicht auf das Internet zugreifen können. Ursache ist der Proxy-Server der *paedML Linux*, der eine Authentifizierung verlangt. Apps, die die automatische Weitergabe der Windows-Anmeldung nicht unterstützen, kommen nicht ins Internet. Auftreten kann das Problem sowohl im pädagogischen wie im Gäste-Netz. Microsoft-Apps sind hiervon nicht betroffen (z.B. der Browser Microsoft Edge).

Mögliche Lösungen:

1. Eintragen von URL-Ausnahmen im Proxyserver (Squid), so dass der Zugriff ohne Anmeldung möglich ist. Die Ausnahmen müssen in die Datei `/etc/squid/local.conf` eingetragen werden. Dies muss für jede URL durchgeführt und manuell gepflegt werden.

In diesem Beispiel wird der Zugriff auf die Domäne des LMZ eingetragen:

```
acl LMZ dstdomain .lmz-bw.de
http_access allow LMZ
```

2. Es kann eine Ausnahmeregel in der Firewall definiert werden, was allerdings dazu führt, dass der Jugendschutzfilter umgangen wird. Die Eintragung der Ausnahmeregel wird in der Firewall pfSense unter *Firewall | Rules* vorgenommen.

21.4 Materialverteilung – Dateigröße

Beim Verteilen von Material über die Schulkonsole ist eine Größenbeschränkung aktiv. Diese verhindert, dass zu große Dateien verteilt werden.

In der UCR-Variable „*umc/server/upload/max*“ kann dieser Wert bei Bedarf angepasst werden.

Im Auslieferungszustand ist der Wert auf 512MB gesetzt ($512 \cdot 1024 = 524288$). Der Wert wird in Kilobyte in die UCR-Variable eingetragen. Zur Umrechnung von Megabyte in Kilobyte multiplizieren Sie den gewünschten Wert mit 1024. Der errechnete Wert ist in die Variable einzutragen.

Anhang A Nomenklatur



1. Bitte beachten Sie unbedingt, dass die Vergabe von Sonderzeichen in Namen zu Problemen führen kann. Es sollten daher keine Sonderzeichen und Umlaute verwendet werden. Dies gilt insbesondere für folgende Zeichen: äöüÄÖÜß
2. Bitte beachten Sie außerdem, dass wir vom Umbenennen von Benutzern, Geräten, Räumen, Projekten ausdrücklich abraten. Bitte löschen Sie stattdessen das entsprechende Objekt⁶⁴ und legen Sie es neu an.
3. Achten Sie beim Import von Listen (Benutzerlisten/Gerätelisten) auf die richtige Zeichencodierung⁶⁵ (Character Encoding) der Dateien. Unterstützt wird nur der Zeichensatz utf-8. Bei anderen Zeichensätzen kann es zu Problemen beim Import von Daten kommen.
4. Die Namen aller „Objekte“ (Geräte sowie Benutzer), die im Server angelegt werden, müssen eindeutig sein. So darf beispielsweise ein Laptop des Kollegen Netzwerkberaters nicht als Computer „Netzwerkberater“ angelegt werden. Die Namen von Rechnern, Klassen und Benutzer dürfen jeweils NUR EINMAL vergeben werden!
5. „Case sensitivity“⁶⁶, also die Unterscheidung von Groß- und Kleinbuchstaben ist ein wichtiges Thema in Linux. Ein Objekt PC01 ist unter Umständen nicht dasselbe wie das Objekt pc01.
Wir empfehlen dringend die konsequente Kleinschreibung aller Namen für Objekte, die Sie in der paedML anlegen (Benutzernamen, Klassenräume, Geräte,...).

Global sind die folgenden Zeichen erlaubt:

Großbuchstaben, Kleinbuchstaben, - (Bindestrich), _ (Unterstrich – **außer in Geräte- und Raumnamen**) und Ziffern. Bitte vermeiden Sie Sonderzeichen (zum Beispiel Umlaute (ä, ö, ü), scharfes S (ß), Akzente (é, è,...), Satzzeichen und Leerzeichen). Leerzeichen in Benutzer- und Objektnamen.

⁶⁴ Alternativ empfehlen wir zu überlegen, ob eine Änderung überhaupt notwendig ist. Wenn sich bspw. der Nachname eines Benutzers ändert, dann kann dieser unter Umständen auch mit dem alten Namen im System geführt werden. Zum Thema Daten gelöschter Benutzer beachten Sie bitte die Hinweise in Kapitel 3.3.1 auf Seite 39.

⁶⁵ <http://de.wikipedia.org/wiki/Zeichencodierung>

⁶⁶ http://de.wikipedia.org/wiki/Case_sensitivity

Objekte	Hinweise
Benutzernamen	<p>Umlaute und das scharfe S (ß) werden beim Import von Benutzern vom System verarbeitet.</p> <p>Achten Sie darauf, dass keine Sonderzeichen (?, !,...) Accents oder ähnliches in den Benutzernamen vorkommen dürfen.</p> <p>Die Zeichenlänge von Benutzernamen sollte auf 15 Zeichen beschränkt werden, sofern Sie den Klassenarbeitsmodus nutzen wollen. Hierfür müssen der Import-Liste Benutzernamen mitgegeben werden.</p>
Rechner- und Gerätenamen	<p>Die Länge von Gerätenamen darf 14 Zeichen nicht überschreiten!</p> <p>Vorsicht: In Rechner- und Gerätenamen dürfen keine Unterstriche verwendet werden. Der Unterstrich wird zwar von der Schulkonsole akzeptiert, die Rechner/Räume werden dann allerdings nicht nach opsi synchronisiert!</p> <p>es muss mind. ein Buchstabe im Namen des Gerätes enthalten sein (unzulässig: „12345678“ / zulässig: „r12345678“)</p>
Arbeitsgruppen	Hier sind keine Sonderzeichen, Leerzeichen oder Umlaute erlaubt.
Imagennamen	<p>Hier sind keine Unterstriche erlaubt.</p> <p>Hier sind keine Sonderzeichen erlaubt.</p>
Raumbezeichnungen	s. Rechner- und Gerätenamen

Tabelle 21: Besonderheiten bei Namen von Objekten

Einträge von opsi-Werten



Alle opsi-Felder dürfen **KEINE SONDERZEICHEN, KEINE UMLAUTE UND KEINE LEERZEICHEN** beinhalten. Erlaubt ist der Bindestrich (-) und der Unterstrich (_).

Anhang B Vervollständigen der opsi-Pakete für die Windows-Installation



Die folgende Beschreibung bezieht sich auf die Verwendung der W10AdminVM auf Windows 10 1909 Basis. Es wird empfohlen bei der Umstellung auf Clients mit Windows 10 auch diese neue AdminVM zu installieren. Informationen zur W10AdminVM erhalten sie [hier](#).



Auf den ausgelieferten Sticks befinden sich noch *Windows 10 Education 1803* Installationsdateien. Diese sollten durch die Installationsdateien von *Windows 10 Education 1909* ersetzt werden.

Sie erhalten die Windows10-Installationsdateien (im Folgenden iso-Datei genannt) direkt bei Microsoft als Download nur dann, wenn Sie über den entsprechenden Zugang verfügen. Sollten Sie einen solchen Zugang nicht besitzen, nehmen Sie Kontakt zu Ihrem Schulträger bzw. Ihrem Dienstleister auf.

Im Folgenden wird von einer iso-Datei ausgegangen, die zuvor von Microsoft heruntergeladen wurde.

Speichern Sie die iso-Datei z. B. in Ihrem Administrator-Homeverzeichnis.

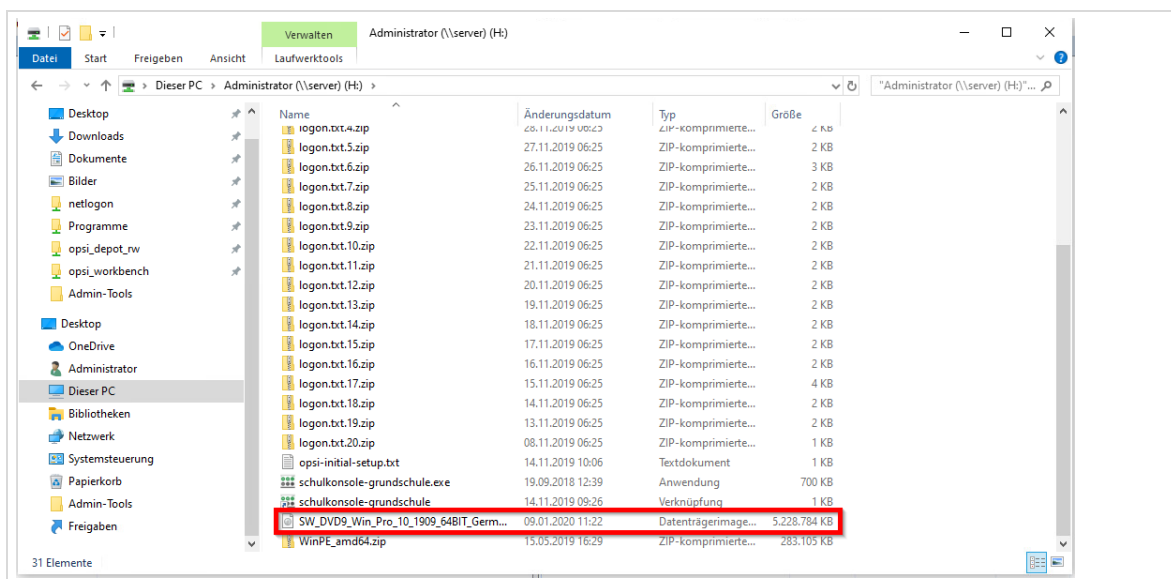


Abb. 100.1.44: Die Windows 10 iso-Datei im Administrator-Home

Durch Doppelklick auf die iso-Datei wird deren Inhalt als DVD-Laufwerk bereitgestellt.

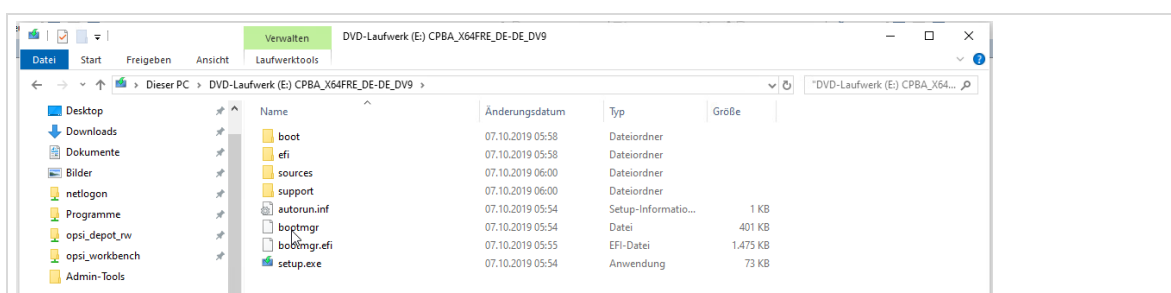


Abb. 100.1.45: Der Windows 10 iso-Datei-Inhalt als DVD-Laufwerk

Öffnen Sie das Programm WinSCP. WinSCP ist auf der AdminVM bereits vorinstalliert. Auf Rechnern mit opsi-client-agent kann das entsprechende opsi-Paket ausgerollt werden. Das Programm ist jedoch auch als Download kostenlos erhältlich. Der Rechnername lautet backup, die Portnummer 22 und der Benutzer root.

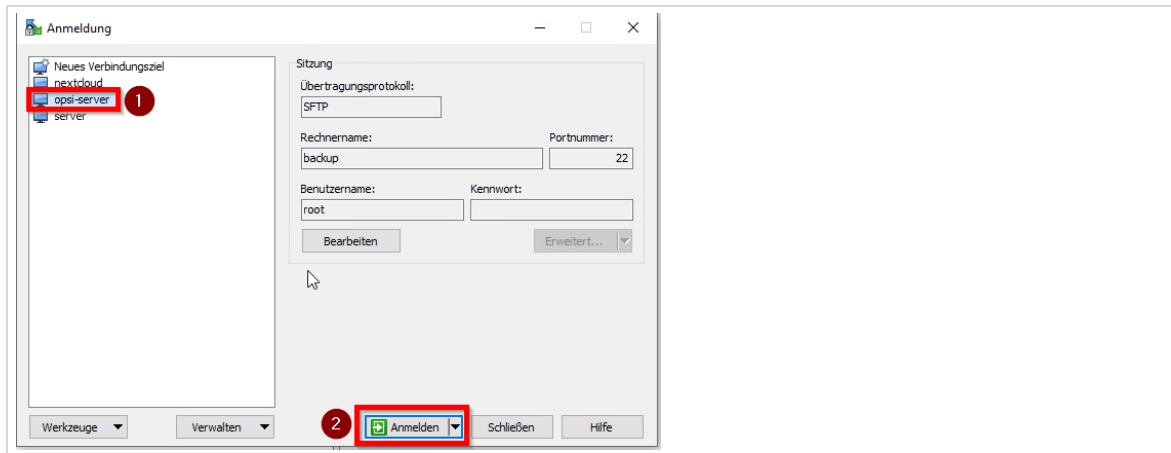


Abb. 100.1.46: Verbindung zu opsi-Server mit WinSCP

Anschließend müssen Sie das root-Passwort eingeben.

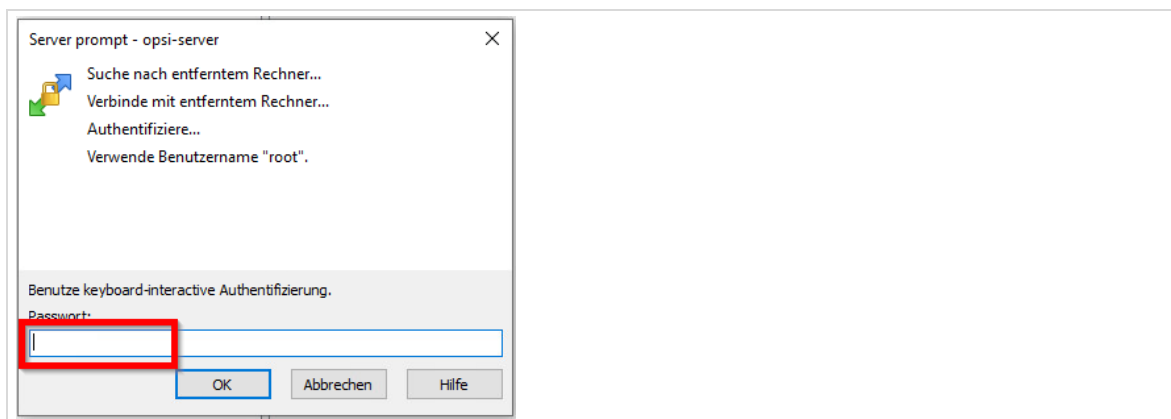


Abb. 100.1.47: Verbindung zu opsi-Server mit WinSCP: root-Passwort

Sie gelangen zur Übersicht von WinSCP. Im linken Bereich finden Sie die Quell-Dateien, rechts sind die Zieldateien (opsi-Server).

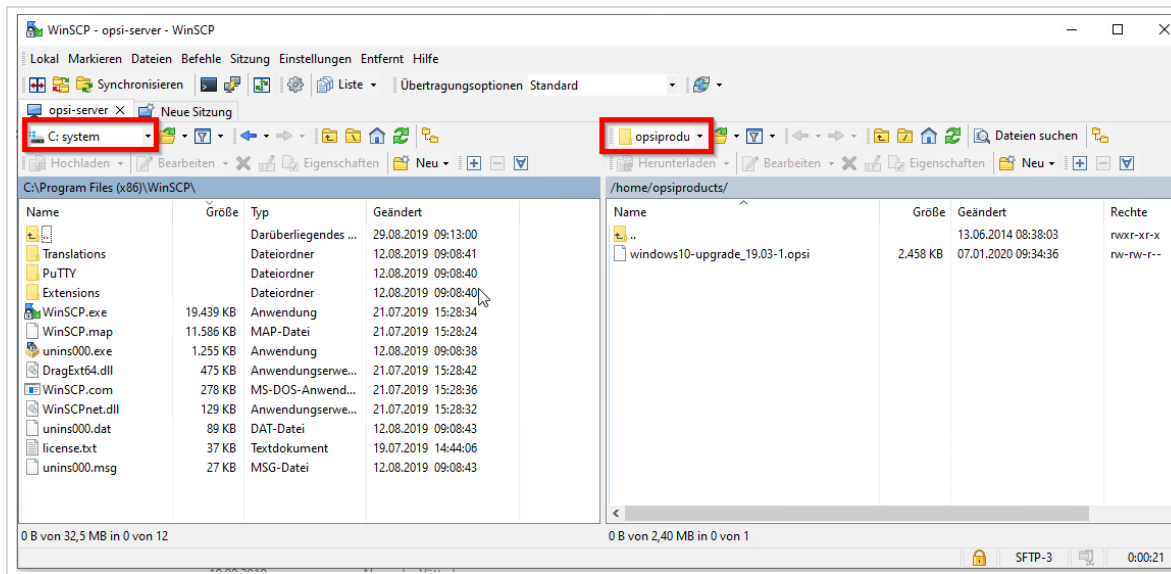


Abb. 100.1.48: WinSCP Übersicht

Navigieren Sie links zum DVD-Laufwerk mit den Windows 10-Installationsdateien und rechts nach `/var/lib/opsi/depot/opsi-local-image-win10-x64/installfiles` und laden Sie die Dateien hoch.

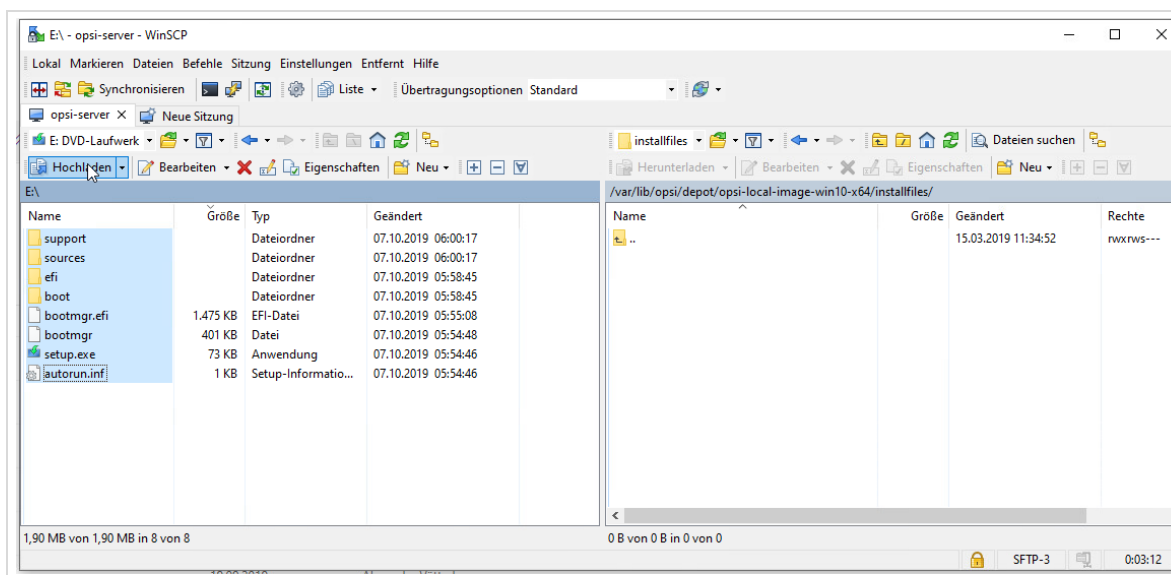


Abb. 100.1.49: WinSCP: Hochladen der Installationsdateien.

Nach erfolgreichem Hochladen müssen noch die opsi-Rechte gesetzt werden. Öffnen Sie dazu den `configd` und wählen Sie im Reiter `Server-Konsole` im Menüpunkt `opsi` den Befehl `opsi-Rechte setzen...`

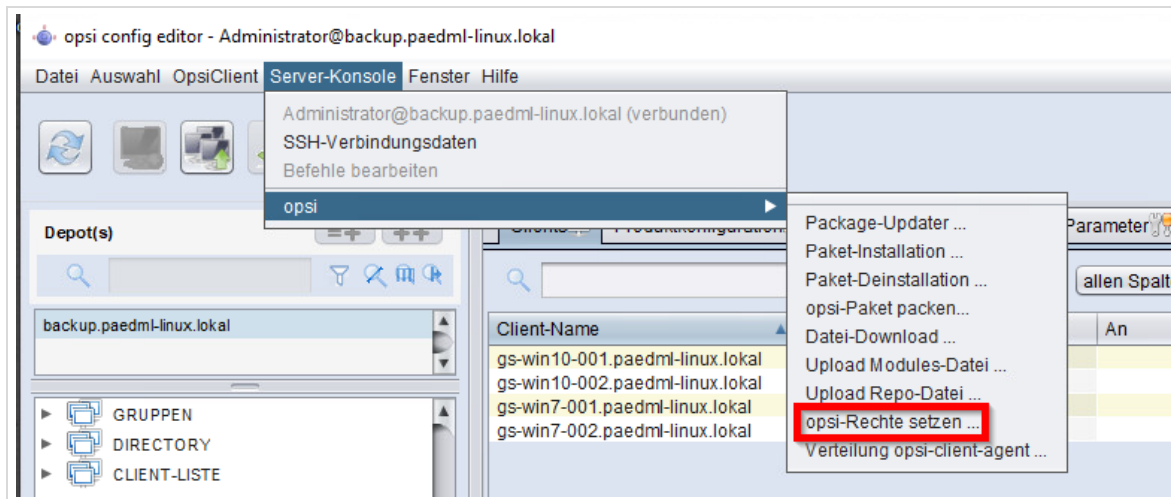


Abb. 100.1.50: Configed: opsi-Rechte setzen

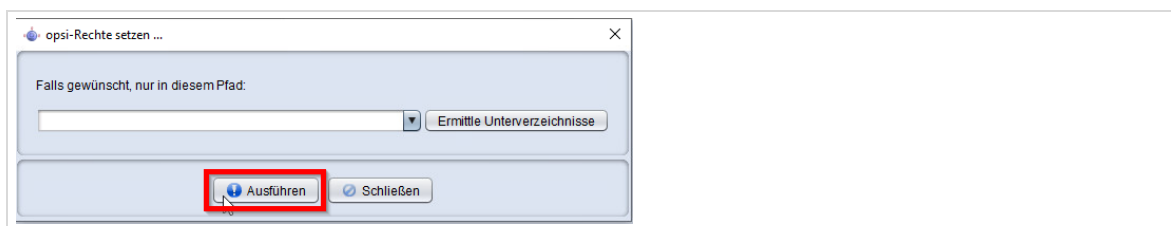


Abb. 100.1.51: Configed: opsi-Rechte setzen

Schließen Sie anschließend die Befehlsausgabe.



Sollen Capture-Images verwendet werden, müssen die Installationsdateien analog auch in *opsi-local-image-win10-x64-capture* hinterlegt werden.

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

© Landesmedienzentrum Baden-Württemberg, 2024