Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

How-To-Anleitung

Drucken auf Netzwerkdrucker funktioniert nach der Installation von Microsoft Hotfix KB5005652 nicht mehr

Stand 10.09.2021 / V 1.0.0

paedML® Windows

Version: 4.x

paedML

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG

Impressum

Herausgeber

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

70190 Stuttgart

Autoren

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

Martin Ewest
Markus Finkenbein
Ulrich Hollritt
Soo-Dong Kim
Antonius Schnetter

Endredaktion

Redaktion Support Netz

Bildnachweis Symbole Titelseite

CC By 3.0 US von Gregor Cresnar, The Noun Project

Weitere Informationen

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

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2021

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 Störung

Ein bisher funktionierender Netzwerkdrucker fordert Benutzer auf, einen Druckertreiber zu installieren. Die Benutzer können den Treiber jedoch nicht installieren, da ihnen die erforderlichen Adminrechte fehlen.

Folge: Es kann weder der Drucker verbunden noch auf dem Drucker Dokumente ausgedruckt werden.

2 Ursache

Um die unter dem Namen *Printnightmare* bekanntgewordene Sicherheitslücke zu schließen, hat Microsoft im August 2021 ein weiteres Sicherheitsupdate veröffentlicht: KB5005652

Microsoft hat mit dem Update KB5005652 laut eigener Aussage die Art und Weise geändert, wie Druckertreiber installiert werden:

> *Windows Updates, die am 10. August 2021 und höher veröffentlicht wurden, erfordern standardmäßig Administratorrechte, um Treiber installieren zu können. Wir haben diese Änderung im Standardverhalten vorgenommen, um das Risiko auf allen Windows-Geräten zu minimieren, einschließlich Geräten, die keine Punkt- und Druck- oder Druckfunktionen verwenden. Weitere Informationen finden Sie unter Ändern des **Standardverhaltens]** von Point and Print und **CVE-2021-34481**. (Auszug aus KB5005652)*

Das heißt konkret: Die bis vor dem Erscheinen des Microsoft Sicherheitsupdates funktionierende Methode, als Benutzer ohne Adminrechte einen Drucker über den "Point and Print"-Mechanismus zu installieren, funktioniert nicht mehr, weswegen es zu der eingangs beschriebenen Störung kommt.

3 Wer ist davon betroffen?

- Kunden, die PCs, Notebooks oder Tablets (neu) installieren und dabei *mshotfix, Version 202108-1* über opsi installiert haben.
- Kunden, die *mshotfix* in der Version 202108-1 auf allen PCs installiert haben und neue Drucker installieren bzw. Druckertreiber aktualisieren wollen.

Das Sicherheitsupdate KB5005652 ist als ein Teil im kumulativen Update KB5005031 von Microsoft enthalten, welches wiederum im opsi-Produkt mshotfix in der Version 202108-1 enthalten ist.

4 Behelfslösung/Workarounds

Hier beschreiben wir zwei Behelfslösungen von Microsoft, wobei wir die paedML-spezifischen Eigenschaften berücksichtigen.

Microsoft sagt selbst, dass durch diese Behelfslösung die Computer *„angreifbar werden“* und empfiehlt diese Lösung nur vorübergehend zu verwenden. (Siehe auch KB5005652 Abschnitt *Ändern des Standardverhaltens der Treiberinstallation mithilfe eines Registrierungsschlüssels*)

Wir informieren Sie, sobald wir erfahren, dass Microsoft diesbezüglich weitere Sicherheitsupdates bzw. weitere Informationen zur Behebung der Sicherheitslücke Printnightmare veröffentlicht hat.

Im Wesentlichen geht es bei dem Workaround darum, das durch KB5005652 geänderte Standardverhalten der Treiberinstallation mithilfe eines speziellen Registrierungsschlüssel rückgängig zu machen.
Das heißt konkret: Die Einschränkung, dass nur Benutzer mit Adminrechten Treiberinstallationen vornehmen können, wird explizit aufgehoben.

4.1 Registrierungsschlüssel mit GPO verteilen

1. Melden Sie sich als Domänenadministrator an DC01 an.
2. Öffnen Sie die Konsole Gruppenrichtlinienverwaltung.

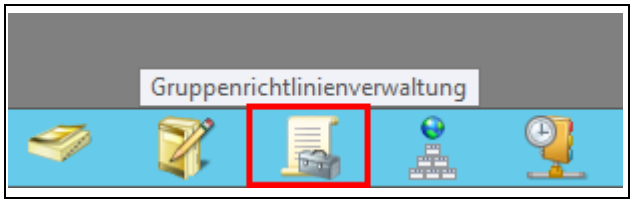

Abb. 1: Gruppenrichtlinienverwaltung (GPMC) öffnen

3. Klicken mit der rechten Maustaste auf den Ordner Computer und wählen Sie die Option Gruppenrichtlinienobjekt hier erstellen und verknüpfen… aus.

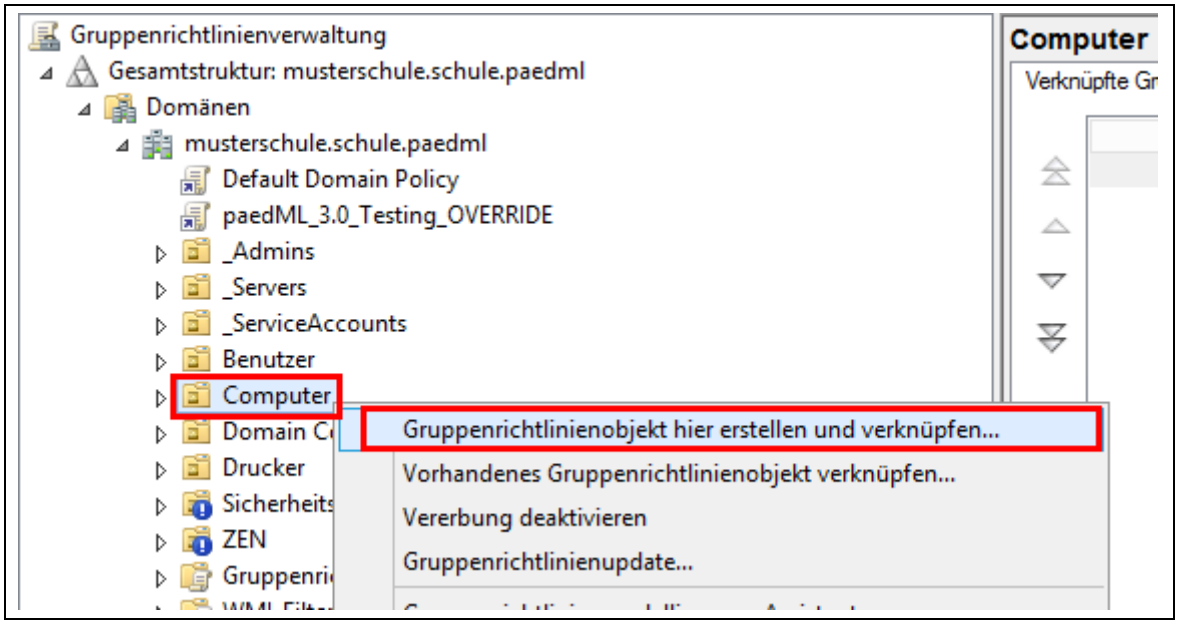

Abb. 2: GPMC -> OU Computer -> GPO hier erstellen und verknüpfen

4. Geben Sie dem neuen Gruppenrichtlinienobjekt (GPO) einen Namen, anhand dessen Sie das GPO leicht nachvollziehen können, und klicken Sie auf OK.

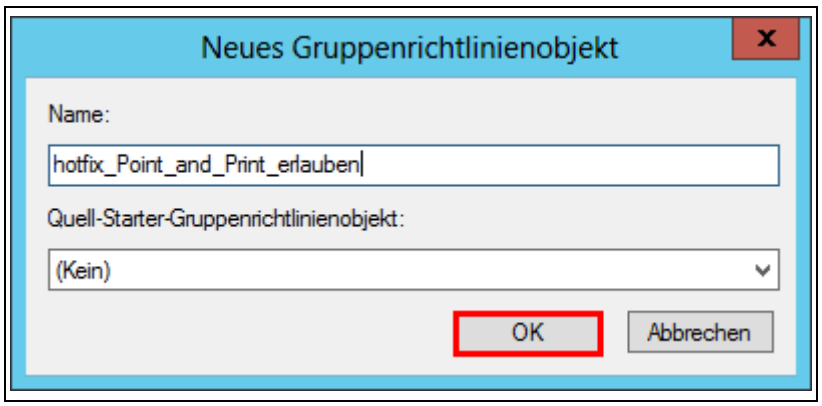

Abb. 3: Neues GPO

5. Klicken Sie auf das neu erstellte GPO und öffnen Sie die Registerkarte Details. Stellen Sie anschließend den **Objektstatus** auf Benutzerkonfigurationseinstellungen deaktiviert um.

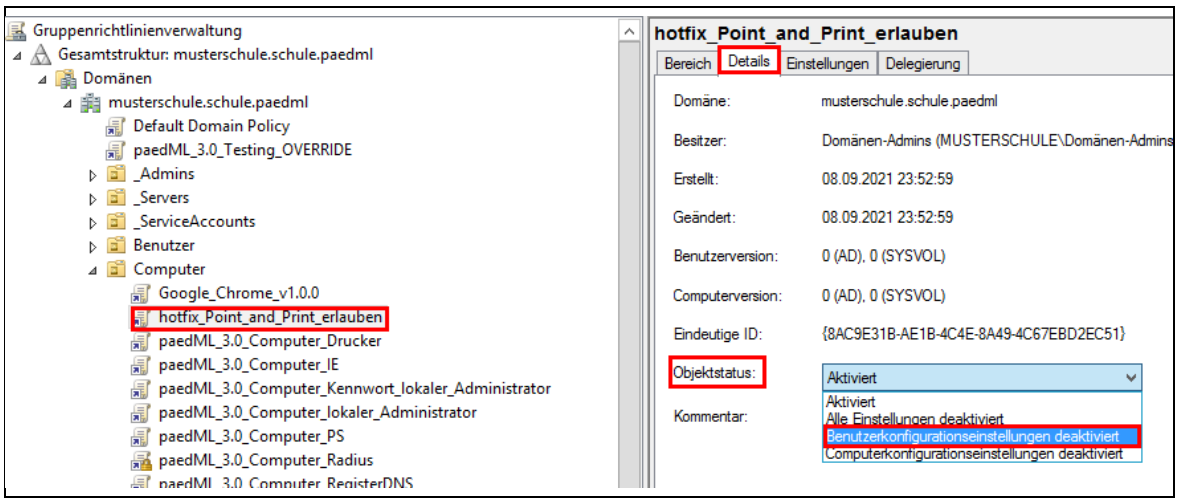

Abb. 4: Neues GPO -> Objektstatus ändern

6. Bestätigen Sie die Aktion mit OK.

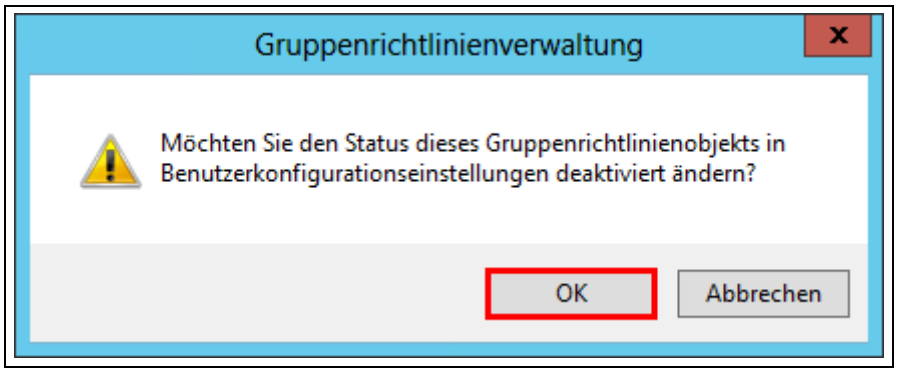

Abb. 5: Änderung des Objektstatus bestätigen

7. Klicken Sie mit der rechte Maustaste auf das oben erstellte GPO und wählen Sie die Option Bearbeiten... aus.

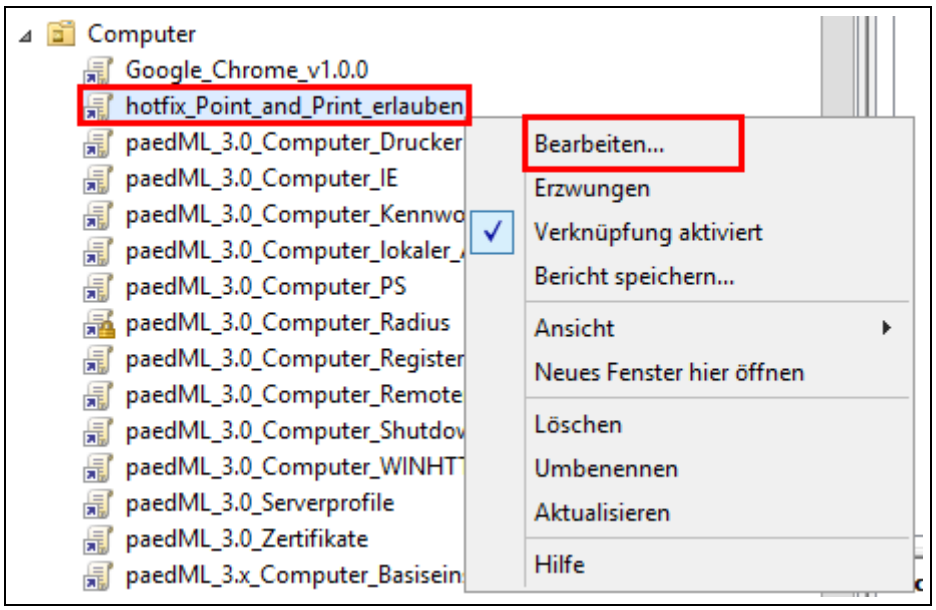

Abb. 6: Neues GPO

8. Öffnen Sie nacheinander die Ordner **Computerkonfiguration, Einstellungen**, **Windows-Einstellungen**. Klicken Sie anschließend mit der rechten Maustaste auf Registrierung. Wählen Sie aus dem Kontextmenü Neu → Registrierungselement aus.

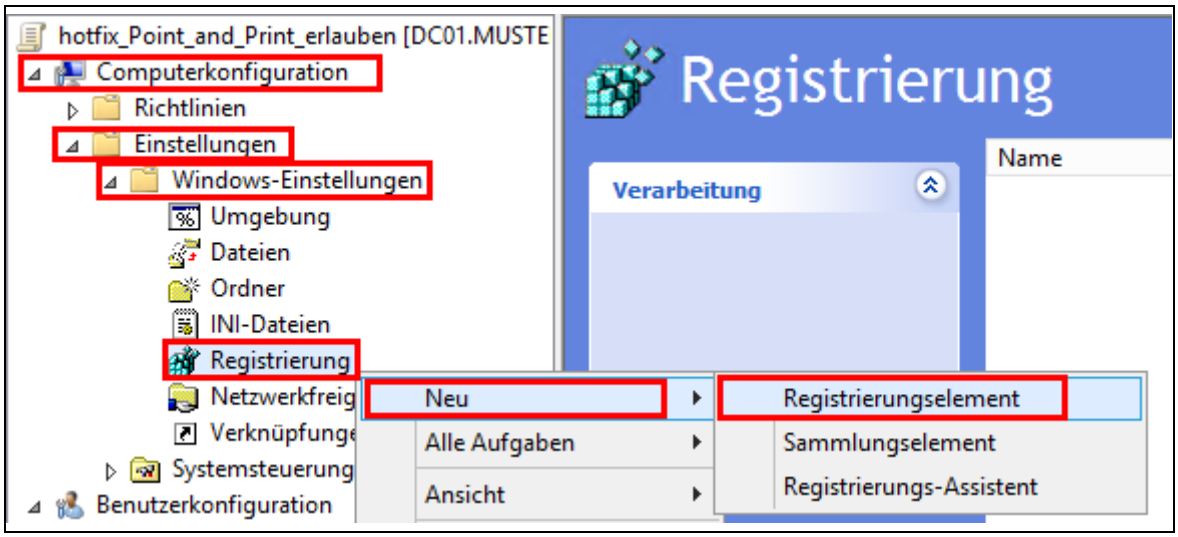

Abb. 7: Neues Registrierungselement hinzufügen

9. Legen Sie folgende Eigenschaften für das neue Registrierungselement fest:

- Aktion: Aktualisieren
- Struktur: HKEY_LOCAL_MACHINE
- **Schlüsselpfad: Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint**
- **Name: RestrictDriverInstallationToAdministrators**
- **Werttyp: REG_DWORD**
- **Wertdaten: 0**
- **Basis: Dezimal**

Wenn Sie den Schlüsselpfad mithilfe des Registrierungselementbrowser einfügen wollen, werden Sie feststellen, dass Sie den oben genannten Schlüsselpfad nicht finden. Das ist kein Bug. Tippen Sie den Pfad in das Eingabefeld direkt ein.

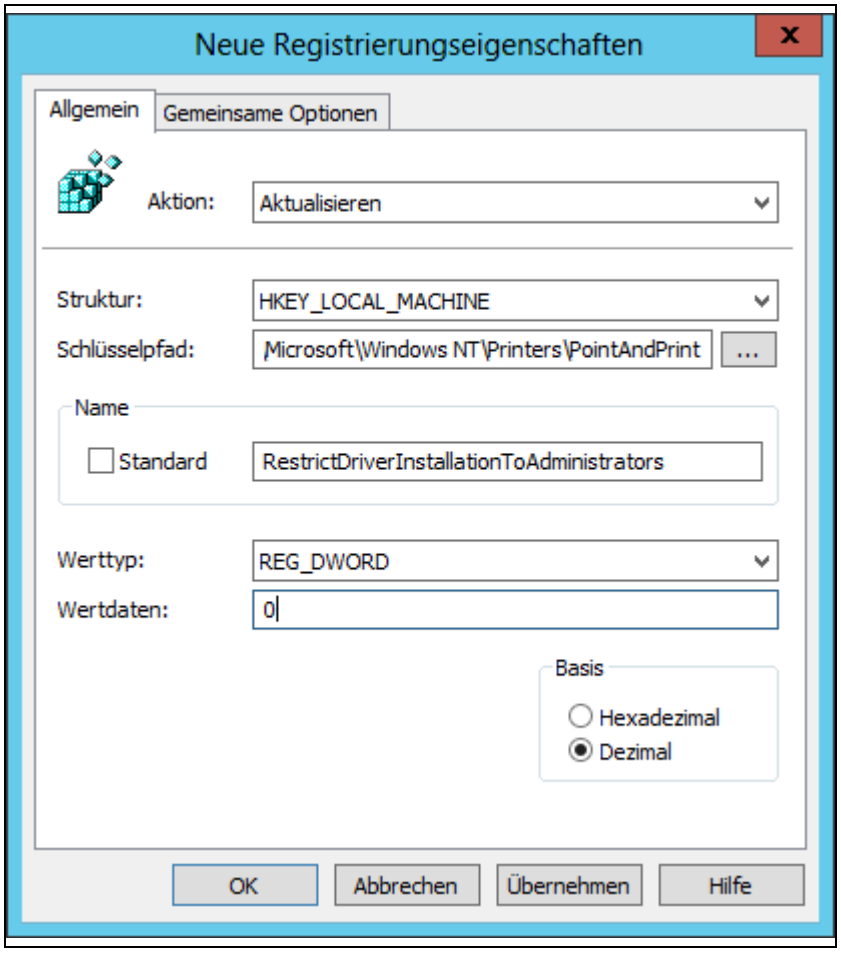

Abb. 8: Eigenschaften des neuen Registrierungselements

10. Klicken Sie auf OK, um das Dialogfenster zu schließen.
11. Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.

Damit haben Sie den wesentlichen, von Microsoft in KB5005652 beschriebenen Workaround umgesetzt. Er wird angewendet, sobald Ihre PCs (neu) gestartet werden.

Wie Sie anhand des Schlüsselnamens erkennen können, dürfen ab sofort Benutzer ohne Adminrechte Druckertreiber auf den PCs installieren, wodurch die beabsichtigte Schutzmaßnahme praktisch aufgehoben wird. Microsoft empfiehlt deshalb zusätzliche Maßnahmen zu ergreifen, um einen minimalen Schutz vor der Sicherheitslücke Printnightmare gewährleisten zu können. Das beschreiben wir im nächsten Kapitel.

4.2 Abmilderung bei Dauereinsatz der Behelfslösung

1. Öffnen Sie die Konsole Gruppenrichtlinienverwaltung, falls Sie sie geschlossen haben.

2. Klicken mit der rechten Maustaste auf den Ordner Computer und wählen Sie die Option Gruppenrichtlinienobjekt hier erstellen und verknüpfen… aus.
3. Geben Sie dem neuen Gruppenrichtlinienobjekt (GPO) einen Namen, anhand dessen Sie das GPO leicht nachvollziehen können, und klicken Sie auf OK. Den anschließend geöffneten Bestätigungsdialog schließen Sie ebenfalls mit OK.

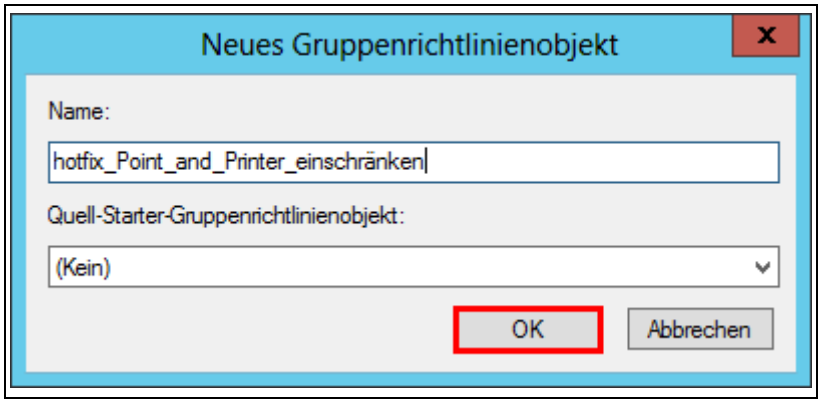

Abb. 9: Ein neues GPO zur Abmilderung der Behelfslösung erstellen

4. Klicken Sie auf das neu erstellte GPO und öffnen Sie anschließend die Registerkarte Details. Ändern Sie den **Objektstatus** auf Benutzerkonfigurationseinstellungen deaktiviert.

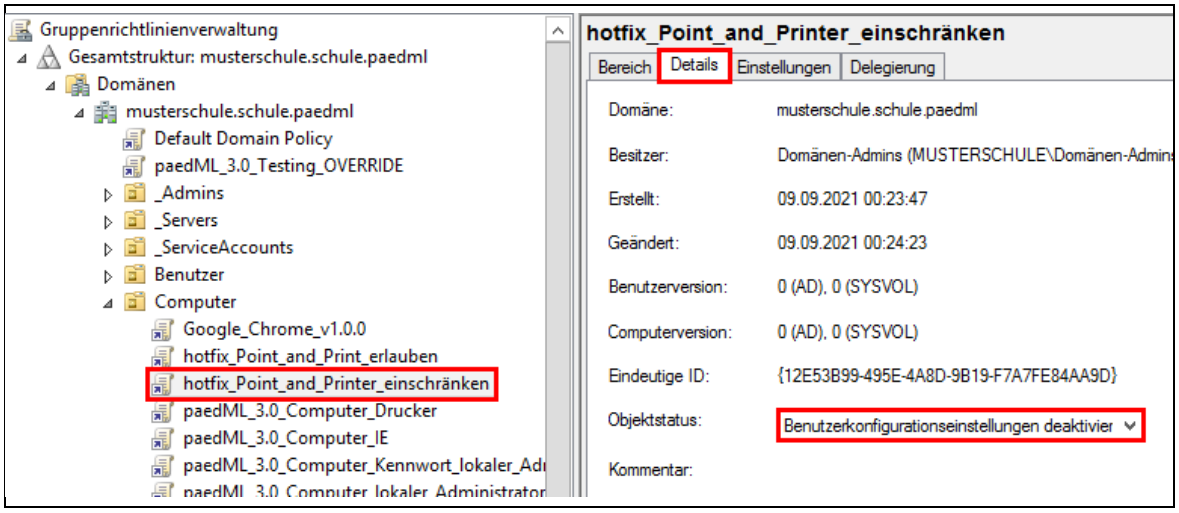

Abb. 10: Objektstatus des neuen GPO bearbeiten

5. Klicken Sie mit der rechten Maustaste auf das GPO und anschließend auf Bearbeiten….

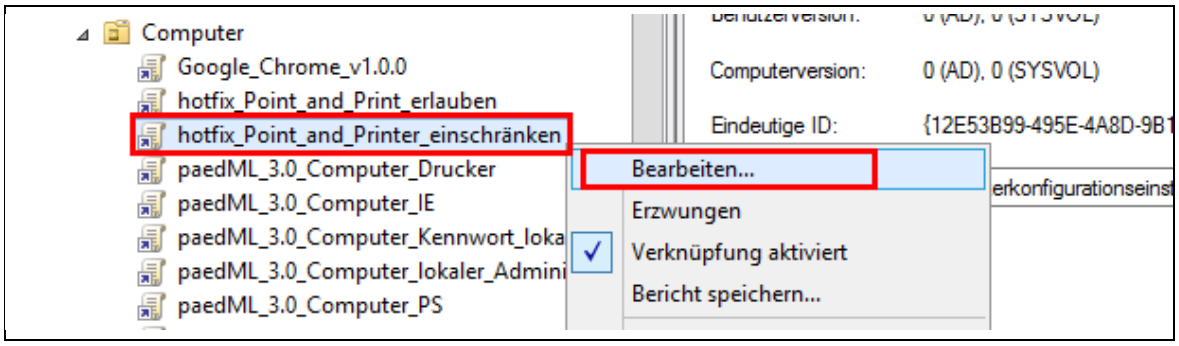

Abb. 11: GPO beabreiten

6. Öffnen Sie nacheinander die Ordner **Computerkonfiguration**, **Richtlinien**, **Administrative Vorlagen** und **Drucker**. Öffnen Sie die Richtlinie Point-and-Print-Einschränkungen mit einem Doppelklick.

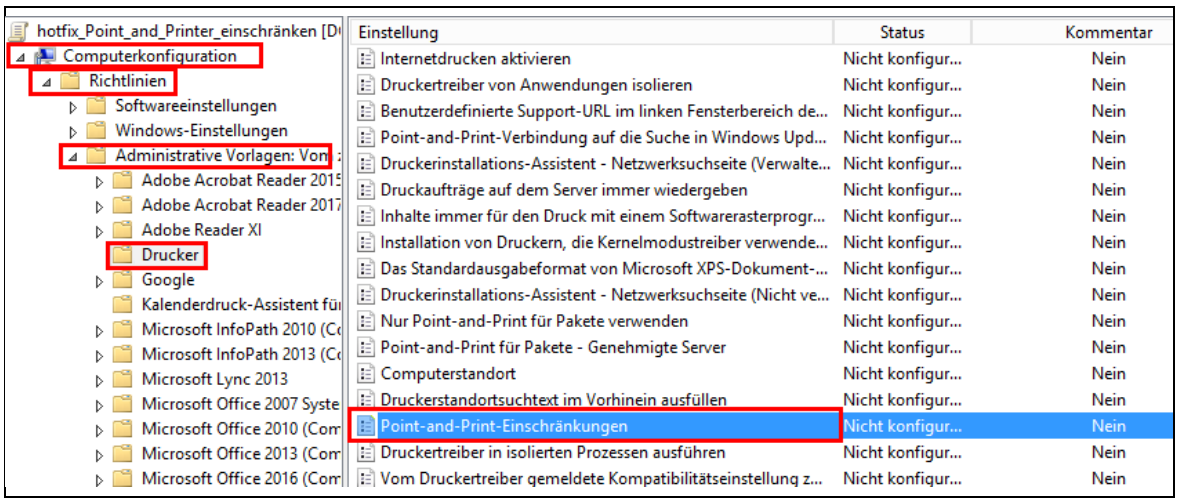

Abb. 12: Richtlinie Point-and-Print-Einschränkungen

7. Wählen Sie den Radio-Button Aktiviert aus. Setzen Sie ein Häkchen bei Benutzer können Point-and-Print nur mit folgenden Servern verwenden. Tragen Sie `sp01.musterschule.schule.paedml` in das Eingabefeld ein. Setzen Sie die beiden Sicherheitshinweise jeweils auf **Warnung oder Aufforderung nicht anzeigen**. Schließen Sie den Vorgang mit OK ab.

Hier weichen wir bewusst von Microsofts Vorschlag ab.

Denn: Wir halten das Anzeigen eines Sicherheitshinweises im schulischen Umfeld für ungeeignet, da es bei den meisten Benutzern für eine Verunsicherung sorgen wird. Außerdem werden die Drucker in der paedML® durch ein Benutzeranmeldeskript installiert bzw. verbunden.

Eine auf diese Art und Weise erzwungene Benutzerinteraktion durch das Anzeigen eines Sicherheitshinweises kann zu einer teils massiven Verzögerung der Benutzeranmeldung führen. Denn der Hinweis erscheint im Hintergrund, so dass der angemeldete Benutzer ihn nie zu sehen bekommt. Folglich kann er nicht bestätigt werden und der Anmeldevorgang wird unter Umständen für mehrere Minuten unterbrochen.

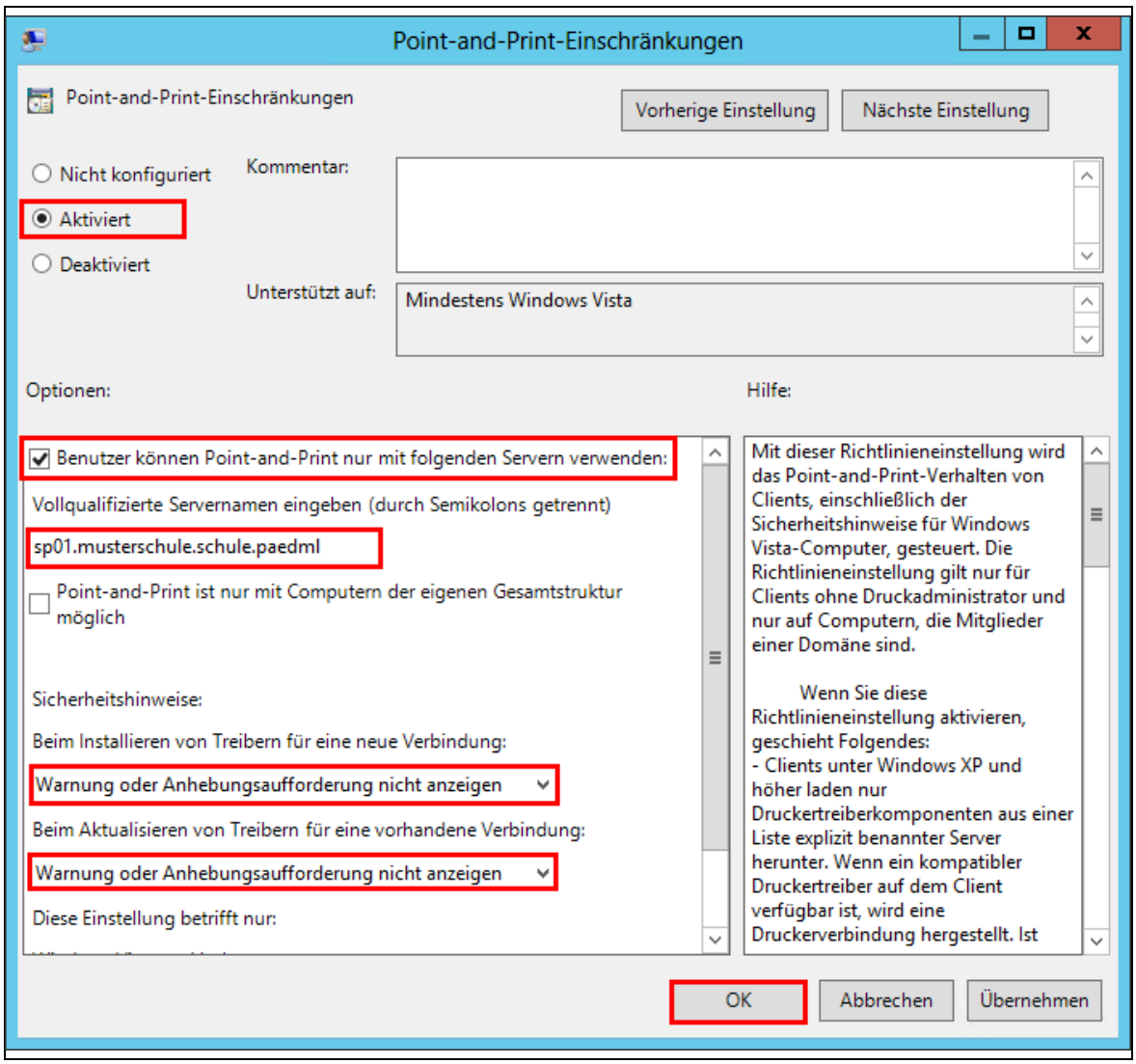

Abb. 13: Eigenschaften der Richtlinie Point-and-Print-Einschränkungen

8. Öffnen Sie anschließend die Richtlinie Point-and-Print für Pakete – Genehmigte Server mit einem Doppelklick.

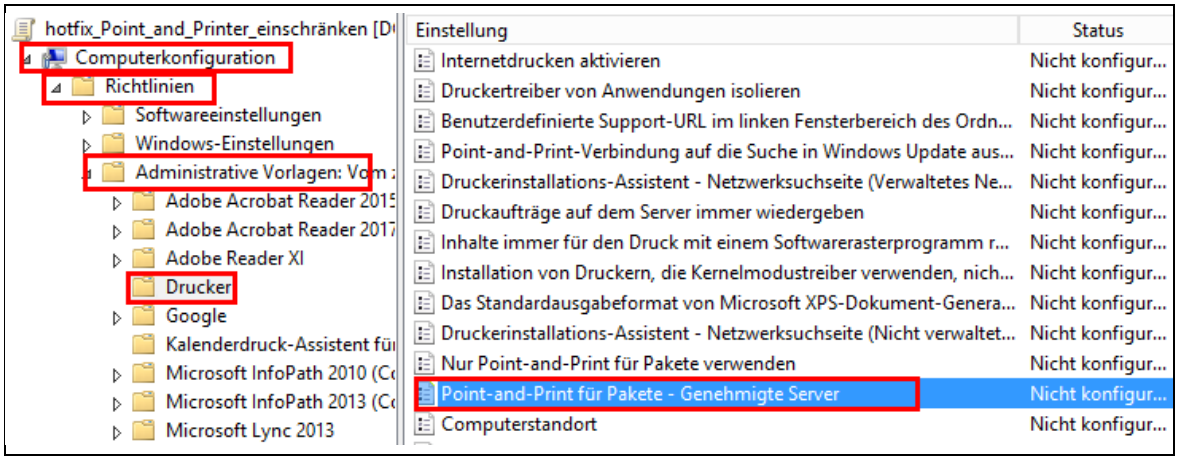

Abb. 14: Richtlinie Point-and-Print für Pakete – Genehmigte Server

9. Aktivieren Sie die Richtlinie und klicken Sie auf Anzeigen....

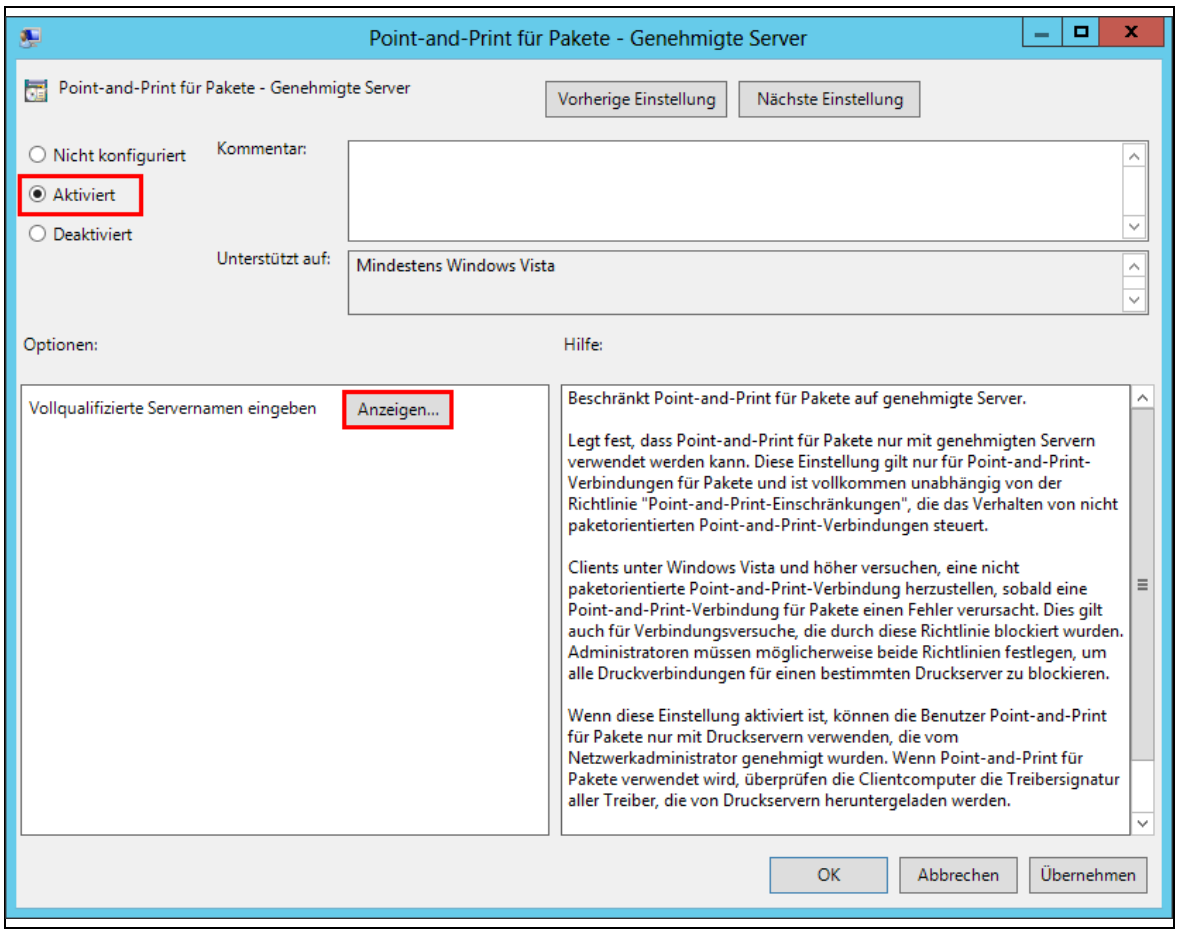

Abb. 15: Eigenschaften der Richtlinie Point-and-Print für Pakete – Genehmigte Server

10. Tippen Sie in die Spalte **Werte** den vollqualifizierten Servernamen `sp01.muster-schule.schule.paedml` ein und schließen Sie das Dialogfenster mit OK.

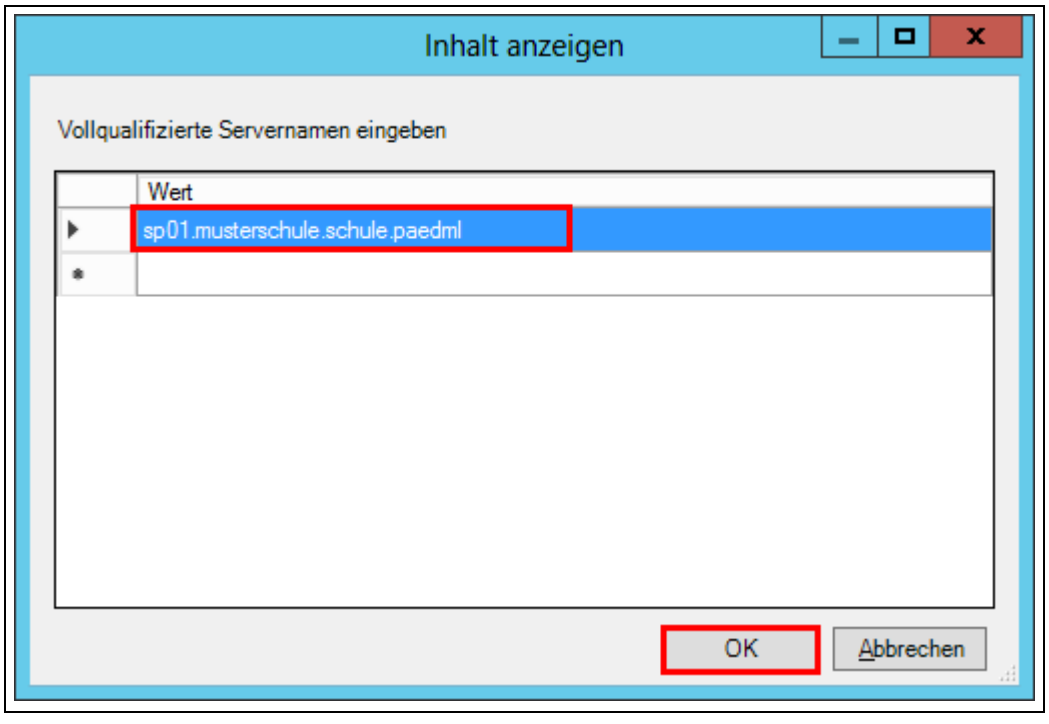

Abb. 16: Vollqualifizierter Name eines genehmigten Servers

11. Schließen Sie das Bearbeitungsfenster mit OK.
12. Klicken Sie in der Konsole Gruppenrichtlinienverwaltung auf den Ordner Computer und öffnen Sie die Registerkarte Verknüpfte Gruppenrichtlinienobjekte. Ändern Sie die Reihenfolge der GPOs derart, dass dieses neu erstellte GPO über den beiden vorhandenen GPOs *paedML_3.0_Computer_Drucker* und *paedML_3.x_Computer_Win10_Basis_Version* steht.

Das Ändern der Reihenfolge ist entscheidend dafür, ob die in dem neuen GPO festgelegten Maßnahmen von Ihren PCs übernommen werden.

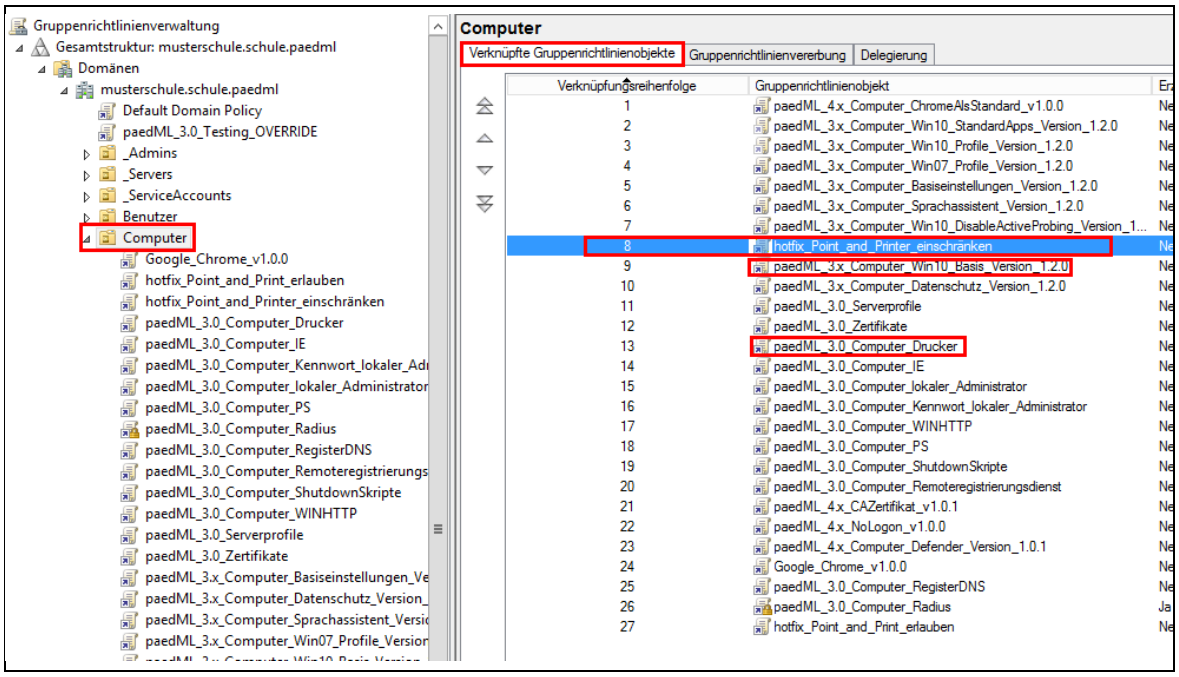

Abb. 17: Richtlinie Point-and-Print-Einschränkungen

5 Änderungsdokumentation

Version	Geänderte oder ergänzte Kapitel
Stand 09.09.2021	Initialversion

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2021

paedML

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG

paedML

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG