

Local Administrator Password Solution” (LAPS) für Microsoft Endpoint (Intune)



Bernhard Köck

VIRTUALSCHOOL | MAI 2023

Inhaltsverzeichnis

1.	Windows LAPS (Local Administrator Password Solution)	1
2.	Voraussetzungen	1
3.	Lokales Admin Konto erstellen (optional)	2
4.	KONFIGURIEREN VON LAPS MIT INTUNE	9
4.1.	KONTOSCHUTZRICHTLINIE ERSTELLEN	9
4.2.	KONFIGURATIONSEINSTELLUNGEN	13
4.3.	ANZEIGEN DES LOKALEN ADMINISTRATORKENNWORTS EINES GERÄTS	16
4.3.1.	MICROSOFT ENTRA	16
4.3.2.	INTUNE-PORTAL	18
4.3.3.	PASSWÖRTER ROTIEREN	20
5.	FEHLERBEHEBUNG FÜR WINDOWS LAPS	21
5.1.	WINDOWS LAPS-EREIGNISPROTOKOLLE	21
5.2.	AZURE-ÜBERWACHUNGSPROTOKOLLE	24

1. Windows LAPS (Local Administrator Password Solution)

Windows Local Administrator Password Solution (Windows LAPS) ist ein Windows-Feature, mit dem IT-Administratoren lokale Administratorkennwörter sichern und schützen können. Dazu gehören die automatische Rotation von Kennwörtern sowie das Sichern der Kennwörter in Azure Active Directory oder Active Directory. Sie können Windows LAPS auf Ihren Windows-Endpunkten mithilfe von Microsoft Intune konfigurieren.

2. Voraussetzungen

Um Windows LAPS in Intune zu verwenden, stellen Sie sicher, dass Sie eine unterstützte Windows-Plattform verwenden:

Windows 10 20H2 und höher mit [installierten Sicherheitsupdates vom 11. April 2023](#)

Windows 11 21H2 und höher mit [installierten Sicherheitsupdates vom 11. April 2023](#)

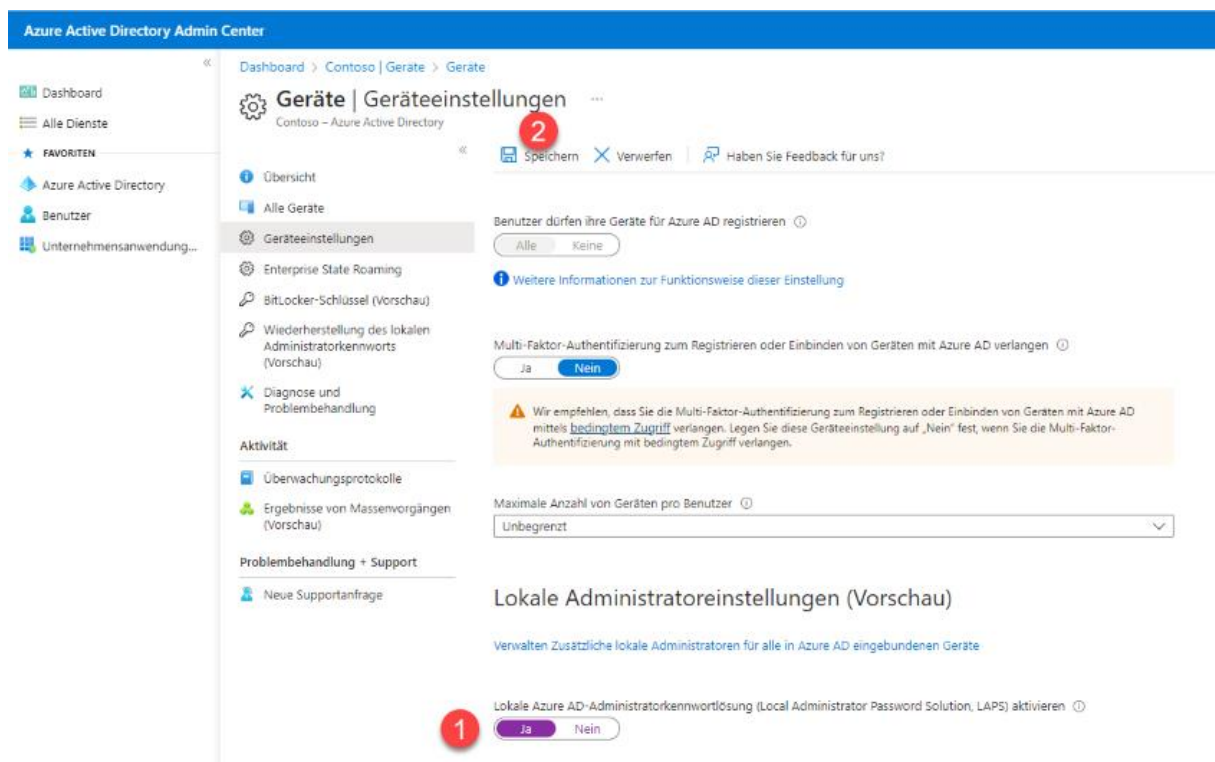
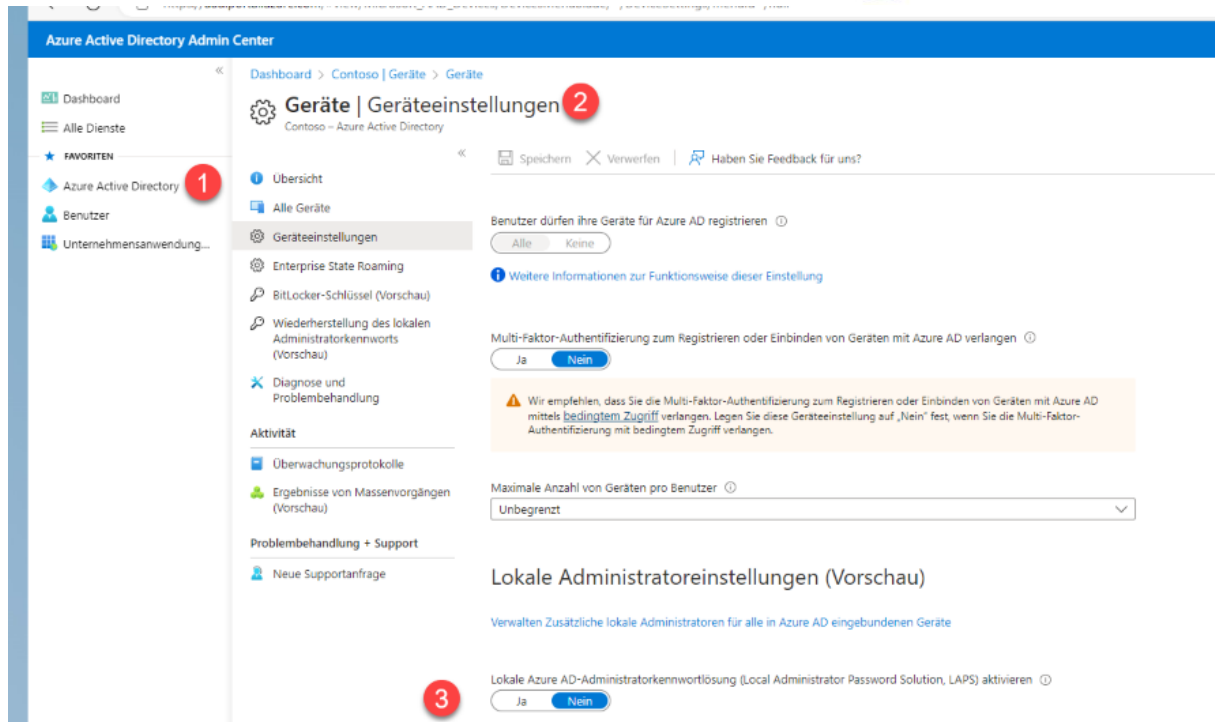
Windows Server 2019 und höher mit [installierten Sicherheitsupdates vom 11. April 2023](#)

Möglicherweise müssen Sie auch die Azure AD Local Administrator Password Solution (LAPS) in Ihrem Azure-Mandanten aktivieren.

Wichtig

Die Azure AD-Unterstützung für Windows Local Administrator Password Solution befindet sich derzeit in der Vorschauphase. Die **zusätzlichen Nutzungsbestimmungen für Microsoft Azure-Vorschauen** enthalten rechtliche Bedingungen. Sie gelten für diejenigen Azure-Features, die sich in der Beta- oder Vorschauversion befinden oder aber anderweitig noch nicht zur allgemeinen Verfügbarkeit freigegeben sind.

LAPS wird nur für in Azure AD eingebundene Geräte oder hybride, in Azure AD eingebundene Geräte unterstützt. In Azure AD registrierte Geräte werden nicht unterstützt.



- Melden Sie sich beim **Azure-Portal** an
- Navigieren Sie zu Azure Active Directory>Geräte>Geräteeinstellungen.
- Wählen Sie **Ja** für die Einstellung „Lokale Azure AD-Administratorkennwortlösung (LAPS) aktivieren“ aus, und wählen Sie **Speichern** aus.

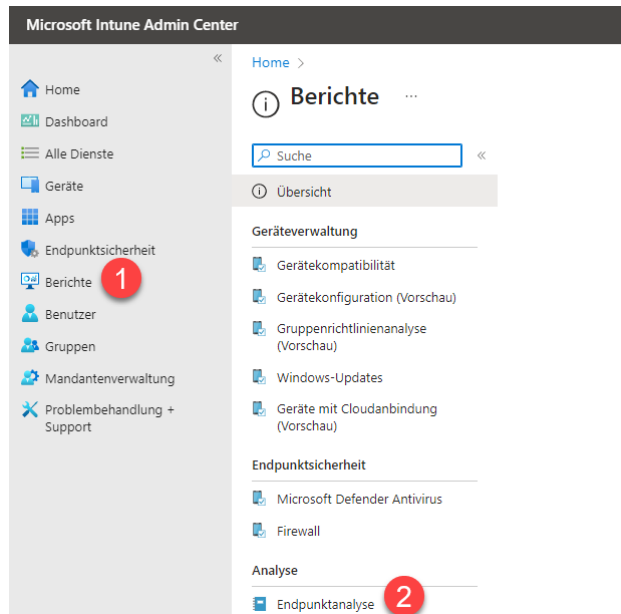
3. Lokales Admin Konto erstellen (optional)

Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)

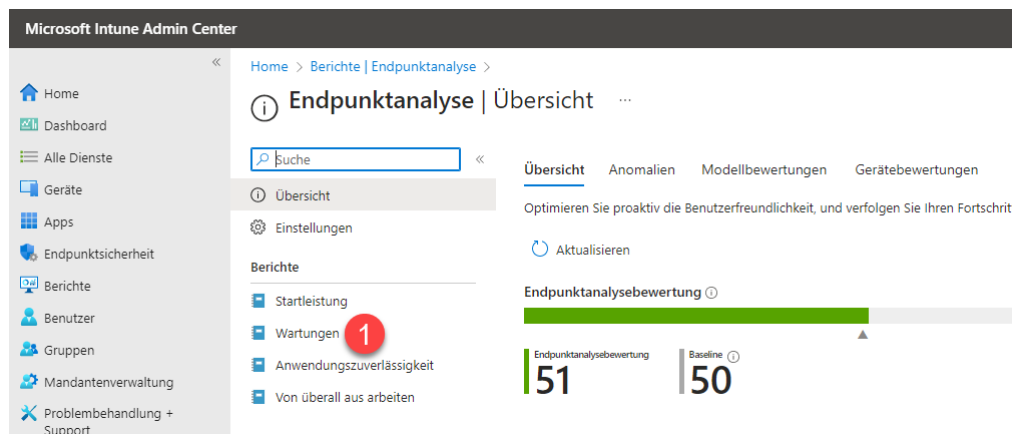
Microsoft verwendet für LAPS das integrierte Administratorkonto.

Für Laborumgebungen ist das sicherlich geeignet, aber für Produktivumgebungen empfehlen wir das Erstellen eines benutzerdefinierten Kontos.

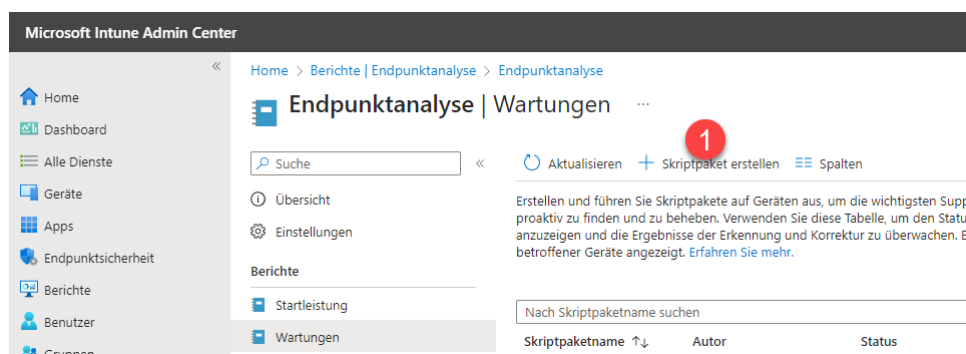
Im Folgenden wird auf den Geräten ein lokales Administratorkonto mithilfe von Powershell und Intune (proaktive PowerShell-Korrekturen) erstellt.



- Wechseln Sie im Intune Admin Center zu Berichte
- Klicken Sie Endpunktanalyse



- Klicken Sie Wartungen



Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)

Klicken Sie Skriptpaket erstellen

Microsoft Intune Admin Center

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Wartungen >

Benutzerdefiniertes Skript erstellen

1 Grundeinstellungen 2 Einstellungen 3 Bereichstags 4 Zuweisungen 5 Überprüfen + erstellen

Erstellen Sie ein neues benutzerdefiniertes Skriptpaket aus von Ihnen geschriebenen Skripts für Erkennung und Wartung.

Name * 1 Überprüfe lokales Admin Konto ✓

Beschreibung 2 Überprüft, ob das gewünschte lokale Admin Konto (clientadmin) vorhanden ist

Herausgeber MDM Admin

Version 1

3

Zurück Weiter

- Geben Sie einen Namen und eine Beschreibung für das Skriptpaket ein.
- Klicken Sie Weiter

Microsoft Intune Admin Center

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Wartungen >

Benutzerdefiniertes Skript erstellen

1 Grundeinstellungen 2 **Einstellungen** 3 Bereichstags 4 Zuweisungen 5 Überprüfen + erstellen

Erstellen Sie ein benutzerdefiniertes Skriptpaket aus Skripts, die Sie geschrieben haben. Standardmäßig werden Skripts täglich auf zugewiesenen Geräten ausgeführt.

Datei mit Erkennungsskript *

Erkennungsskript

```
i=; $username = "clientadmin"
try {
    $user = Get-LocalUser -Name $username -ErrorAction Stop
    if ($user.Enabled) {
        Write-Output ("User {0} present and enabled" -f $username)
        exit 0
    }
}
```

Datei mit Bereinigungsskript

Wiederherstellungsskript

```
i=; Add-Type -AssemblyName 'System.Web'

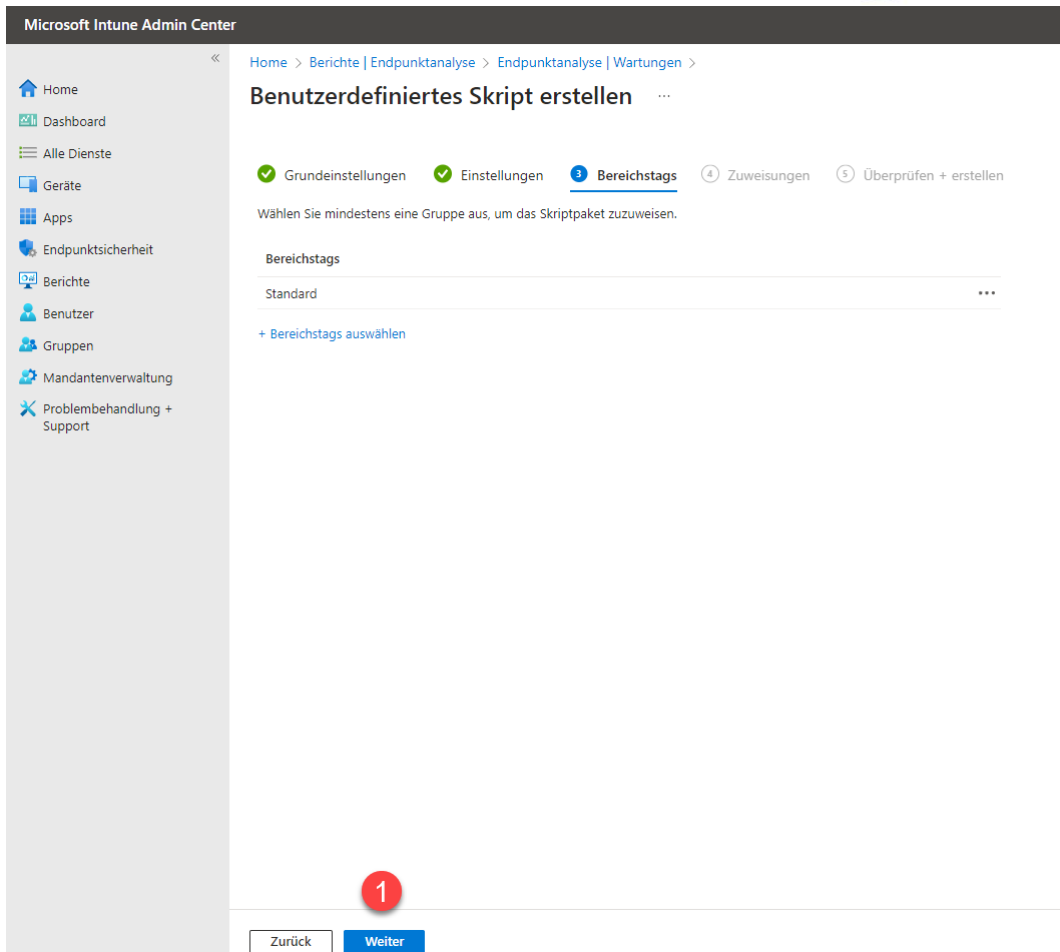
$userParams = @{
    Name = 'clientadmin'
    Description = 'LAPS Client Admin'
    Password = [System.Web.Security.Membership]::GeneratePassword(16, 0) |
    ConvertTo-SecureString -AsPlainText -Force
}
```

Dieses Skript mit den Anmeldeinformationen des angemeldeten Benutzers ausführen ☐ Ja ☒ Nein

Skriptsignaturprüfung erzwingen ☐ Ja ☒ Nein

Skript in 64-Bit-PowerShell ausführen ☒ Ja ☐ Nein

- Wählen Sie das **Erkennungsskript** aus. (Beispiel auf [Github](#))
- Wählen Sie das **Bereinigungsskript** aus. (Beispiel auf [Github](#))
- Stellen Sie den Schieberegler bei **Skript in 64-Bit-Powershell ausführen** auf **JA**.
- Klicken Sie Weiter



The screenshot shows the Microsoft Intune Admin Center interface. The left sidebar contains navigation links: Home, Dashboard, Alle Dienste, Geräte, Apps, Endpunktsicherheit, Berichte, Benutzer, Gruppen, Mandantenverwaltung, and Problembehandlung + Support. The main content area is titled "Benutzerdefiniertes Skript erstellen" and shows a progress bar with five steps: Grundeinstellungen, Einstellungen, Bereichstags (active), Zuweisungen, and Überprüfen + erstellen. Below the progress bar, it says "Wählen Sie mindestens eine Gruppe aus, um das Skriptpaket zuzuweisen." and displays a table with one row labeled "Bereichstags" and "Standard". A red circle with the number "1" is placed over the "Weiter" button at the bottom right of the interface.

- Klicken Sie Weiter

Microsoft Intune Admin Center

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Wartungen >

Benutzerdefiniertes Skript erstellen

✓ Grundeinstellungen ✓ Einstellungen ✓ Bereichstags **4 Zuweisungen** 5 Überprüfen + erstellen

Wählen Sie mindestens eine Gruppe aus, um das Skriptpaket zuzuweisen.

Eingeschlossene Gruppen

Zuweisen zu

Ausgewählte Gru...	Zeitplan	Filter	Filtermodus
Keine Gruppen ausgewählt			

+ Wählen Sie die Gruppen aus, die eingeschlossen werden sollen. **1**

Ausgeschlossene Gruppen

i Schließen Sie entweder Gerätegruppen oder Benutzergruppen ein oder aus. Innerhalb von Zuweisungen zum Einschließen oder Ausschließen dürfen Benutzer- und Gerätegruppen nicht kombiniert werden.

Ausgewählte Gruppen

Keine Gruppen ausgewählt

+ Wählen Sie die Gruppen aus, die ausgeschlossen werden sollen.

2

Zurück Weiter

- Weisen Sie das Skript einer Gerätegruppe zu
- Klicken Sie Weiter

Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)

Microsoft Intune Admin Center

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Wartungen >

Benutzerdefiniertes Skript erstellen

Grundeinstellungen Einstellungen Bereichstags Zuweisungen **Überprüfen + erstellen**

Zusammenfassung

Grundeinstellungen

Name	Überprüfe lokales Admin Konto
Beschreibung	Überprüft, ob das gewünschte lokale Admin Konto (clientadmin) vorhanden ist
Herausgeber	MDM Admin
Version	--

Einstellungen

Erkennungsskript	Ja
Wiederherstellungsskript	Ja
Dieses Skript mit den Anmeldeinformationen des angemeldeten Benutzers ausführen	Nein
Skriptsignaturprüfung erzwingen	Nein
Skript in 64-Bit-PowerShell ausführen	Ja

Bereichstags

Standard

Zuweisungen

Eingeschlossene Gruppen	Ausgewählte Grupp...	Zeitplan	Filter	Filterm
	Keine Ergebnisse.			
	<div></div>			
Ausgeschlossene Gruppen	Ausgewählte Gruppen			
	Keine Ergebnisse.			

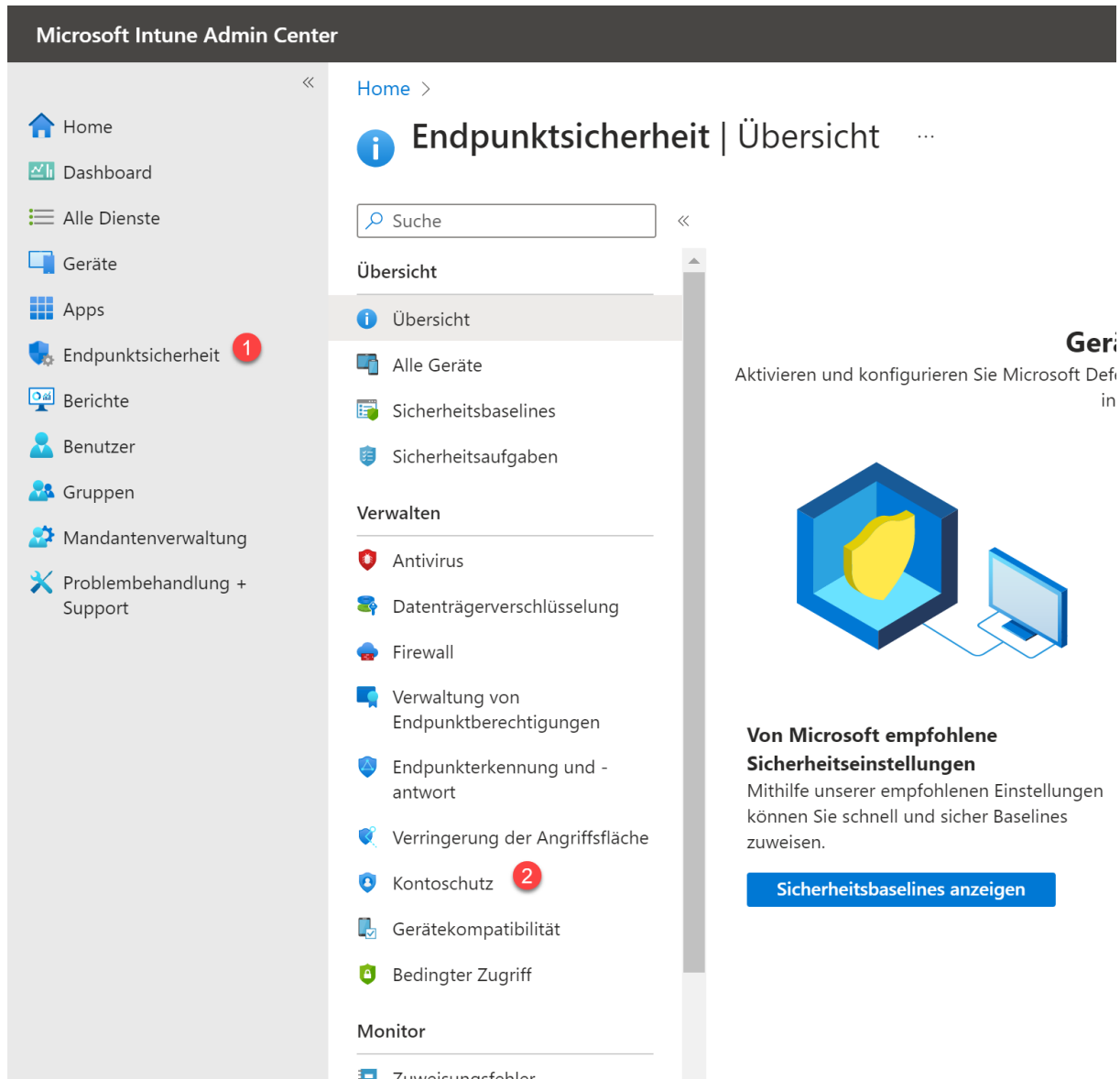
1

Zurück Erstellen

- Klicken Sie Erstellen

4. KONFIGURIEREN VON LAPS MIT INTUNE

4.1. KONTOSCHUTZRICHTLINIE ERSTELLEN



- Wechseln Sie im Microsoft Intune-Portal (Intune.Microsoft.com) zu Endpoint Sicherheit
- Klicken Sie Kontoschutz

Microsoft Intune Admin Center

Home > Endpunktsicherheit

Endpunktsicherheit | Kontoschutz

Suche

+ Richtlinie erstellen Aktualisieren Exportieren

Nach Profilnamen suchen

Richtlinienname	Richtlinientyp	Zugewiesen
Configure Windows Hi	Kontoschutz (Vorsch...	Nein
Windows Hello for Bus	Kontoschutz (Vorsch...	Nein
Manage local Adminis	Lokale Benutzergrup...	Ja

- Klicken Sie Richtlinie erstellen

Profil erstellen



Plattform

Windows 10 und höher

1



Profil

Local admin password solution (Windows LAPS)

2



Local admin password solution (Windows LAPS)

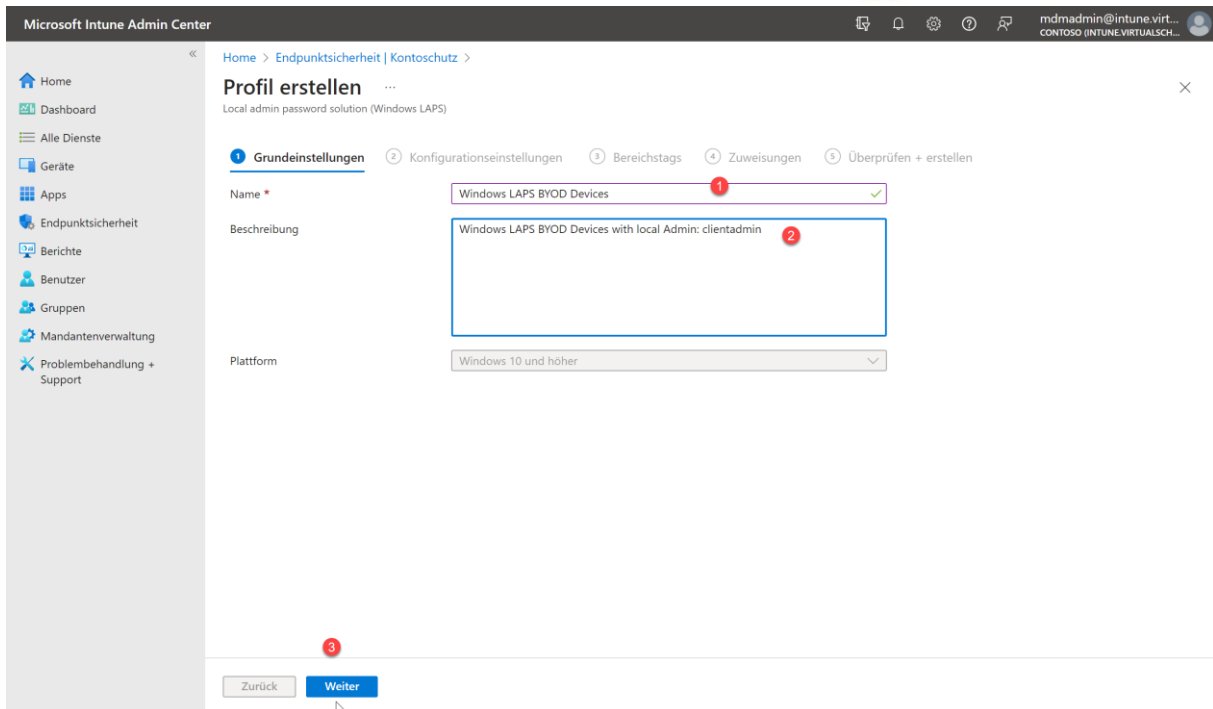
Windows Local Administrator Password Solution(Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on your Azure Active Directory - joined or Windows Server Active Directory - joined devices.

3

Erstellen

- Wählen Sie für die Plattform "Windows **10 oder höher**" und für das Profil die Option "**Lokal admin password solution (Windows LAPS)**" aus.
- Klicken Sie auf **Erstellen**

Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)



Microsoft Intune Admin Center

Home > Endpunktsicherheit | Kontoschutz >

Profil erstellen

Local admin password solution (Windows LAPS)

1 Grundeinstellungen 2 Konfigurationseinstellungen 3 Bereichstags 4 Zuweisungen 5 Überprüfen + erstellen

Name * Windows LAPS BYOD Devices 1

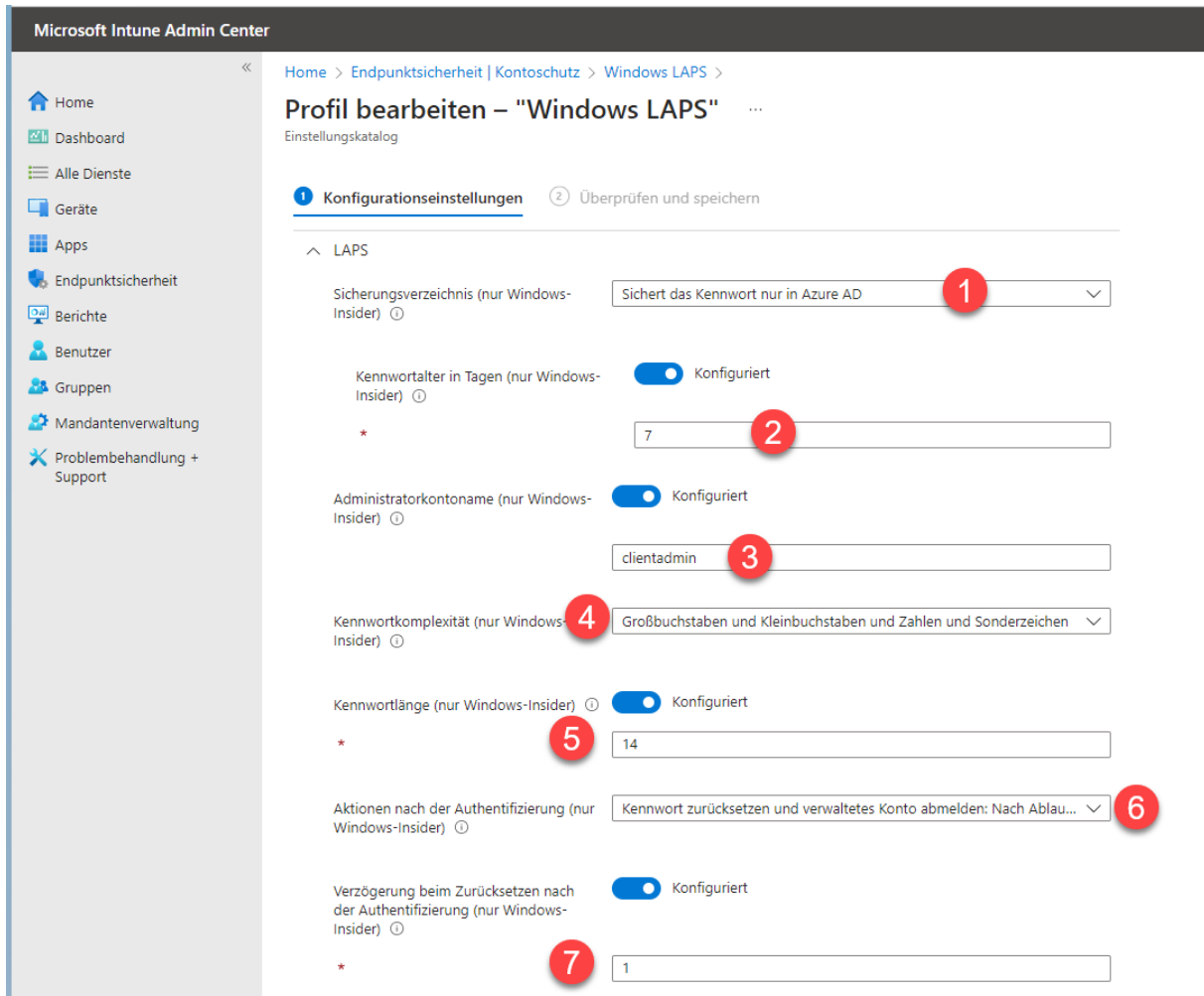
Beschreibung Windows LAPS BYOD Devices with local Admin: clientadmin 2

Plattform Windows 10 und höher

Zurück Weiter 3

- Geben Sie der neuen Richtlinie einen eigenen Namen und eine Beschreibung (optional)
- Klicken Sie auf **Weiter**

4.2. KONFIGURATIONSEINSTELLUNGEN



- Treffen Sie die gewünschten Einstellungen
- Klicken Sie Weiter

(1) Sicherungsverzeichnis: Verwenden Sie diese Einstellung, um zu konfigurieren, in welchem Verzeichnis das lokale Administratorkontokennwort gesichert wird.

Zulässige Einstellungen:

0=Deaktiviert (Kennwort wird nicht gesichert)

1=Das Kennwort nur in Azure AD sichern

2=Kennwort nur in Active Directory sichern.

Wenn nichts angegeben wird, ist diese Einstellung standardmäßig 0. Diese Einstellung ist nur für Windows-Insider verfügbar

(2) Kennwortalter in Tagen: Verwenden Sie diese Richtlinie, um das maximale Kennwortalter des verwalteten lokalen Administratorkontos zu konfigurieren. Wenn keine Angabe erfolgt, beträgt diese Einstellung standardmäßig 30 Tage. Diese Einstellung hat einen minimal zulässigen Wert von 1 Tag, wenn das Kennwort in das lokale Active Directory gesichert wird, und 7 Tage, wenn das Kennwort auf Azure AD gesichert wird. Dies hat einen maximal zulässigen Wert von 365 Tagen. Diese Einstellung ist nur für Windows-Insider verfügbar.

(3) Name des Administratorkontos: Verwenden Sie diese Einstellung, um den Namen des verwalteten lokalen Administratorkontos zu konfigurieren. Wenn keine

Angabe erfolgt, wird das standardmäßige integrierte lokale Administratorkonto über eine bekannte SID (auch bei Umbenennung) gefunden. Bei Angabe dieser Option wird das Kennwort des angegebenen Kontos verwaltet.

***Hinweis:** Wenn in dieser Einstellung ein benutzerdefinierter verwalteter lokaler Administratorkontoname angegeben ist, muss dieses Konto auf andere Weise erstellt werden. Wenn Sie in dieser Einstellung einen Namen angeben, wird das Konto nicht erstellt. (siehe Kapitel 3)*

- (4) Kennwortkomplexität:** Verwenden Sie diese Einstellung, um die Kennwortkomplexität des verwalteten lokalen Administratorkontos zu konfigurieren.

Zulässige Einstellungen:

1=Großbuchstaben

2=Großbuchstaben und Kleinbuchstaben

3=Großbuchstaben und Kleinbuchstaben und Zahlen

4=Großbuchstaben und Kleinbuchstaben und Zahlen und Sonderzeichen.

Wird nichts angegeben, ist diese Einstellung standardmäßig auf 4 festgelegt. Diese Einstellung ist nur für Windows-Insider verfügbar.

- (5) Passwortlänge:** Verwenden Sie diese Einstellung, um die Länge des Kennworts des verwalteten lokalen Administratorkontos zu konfigurieren. Wenn keine Angabe erfolgt, wird diese Einstellung standardmäßig auf 14 Zeichen festgelegt. Diese Einstellung hat einen zulässigen Mindestwert von 8 Zeichen. Diese Einstellung hat einen zulässigen Maximalwert von 64 Zeichen. Diese Einstellung ist nur für Windows-Insider verfügbar.

- (6) Post-Authentifizierungsaktionen:**

Verwenden Sie diese Einstellung, um die Aktionen anzugeben, die nach Ablauf des konfigurierten Aktivierungszeitraums ausgeführt werden sollen. Wenn keine Angabe erfolgt, wird diese Einstellung standardmäßig auf 3 festgelegt (Kennwort zurücksetzen und verwaltetes Konto abmelden). Diese Einstellung ist nur für Windows-Insider verfügbar.

- (7) Verzögerung beim Zurücksetzen der Authentifizierung:** Geben Sie mithilfe dieser Einstellung an, wie viel Zeit (in Stunden) nach einer Authentifizierung gewartet werden soll, bevor die angegebenen Aktionen nach der Authentifizierung ausgeführt werden. Wenn keine Angabe erfolgt, wird diese Einstellung standardmäßig auf 24 Stunden festgelegt. Diese Einstellung weist einen zulässigen Mindestwert von 0 Stunden auf (dadurch werden alle Aktionen nach der Authentifizierung deaktiviert). Diese Einstellung hat einen zulässigen Maximalwert von 24 Stunden. Diese Einstellung ist nur für Windows-Insider verfügbar.

Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)

Home > Endpunktsicherheit | Kontoschutz > Windows LAPS >

Profil bearbeiten – "Windows LAPS"

Einstellungskatalog

1 Zuweisungen 2 Überprüfen und speichern

Eingeschlossene Gruppen

Gruppen hinzufügen Alle Benutzer hinzufügen Alle Geräte hinzufügen

Gruppen	Gruppenmitglieder ⓘ	Filter	Filtermodus	Entfernen
mdm_all_Windows_company_devices	13 Geräte, 0 Benutzer	Keine	Keine	Filter bearbeiten Entfernen

Ausgeschlossene Gruppen

Beim Ausschließen von Gruppen können Benutzer- und Gerätegruppen in den Optionen "Einschließen" und "Ausschließen" nicht gemischt verwenden. [Klicken Sie hier, um weitere Informationen zum Ausschließen von Gruppen zu erhalten.](#)

Gruppen hinzufügen

Gruppen	Gruppenmitglieder ⓘ	Entfernen
Keine Gruppen ausgewählt		

3

Überprüfen und speichern

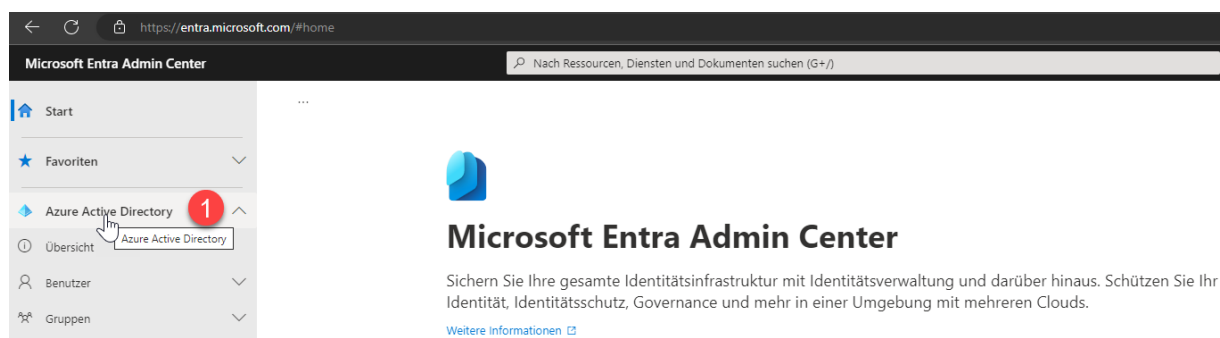
Abbrechen

- Weisen Sie die erstellte Richtlinie einer Gerätegruppe zu.

4.3. ANZEIGEN DES LOKALEN ADMINISTRATORKENNWORTS EINES GERÄTS

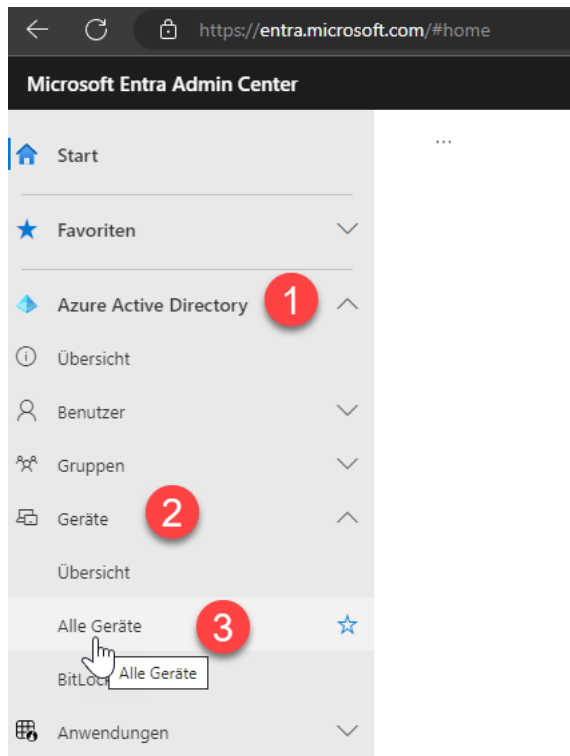
Es gibt mehrere Möglichkeiten, wie ein IT-Administrator das lokale Administratorkennwort eines Endpunkts anzeigen kann, vom Intune-Verwaltungsportal, Microsoft Entra bis hin zur Verwendung von PowerShell.

4.3.1. MICROSOFT ENTRA

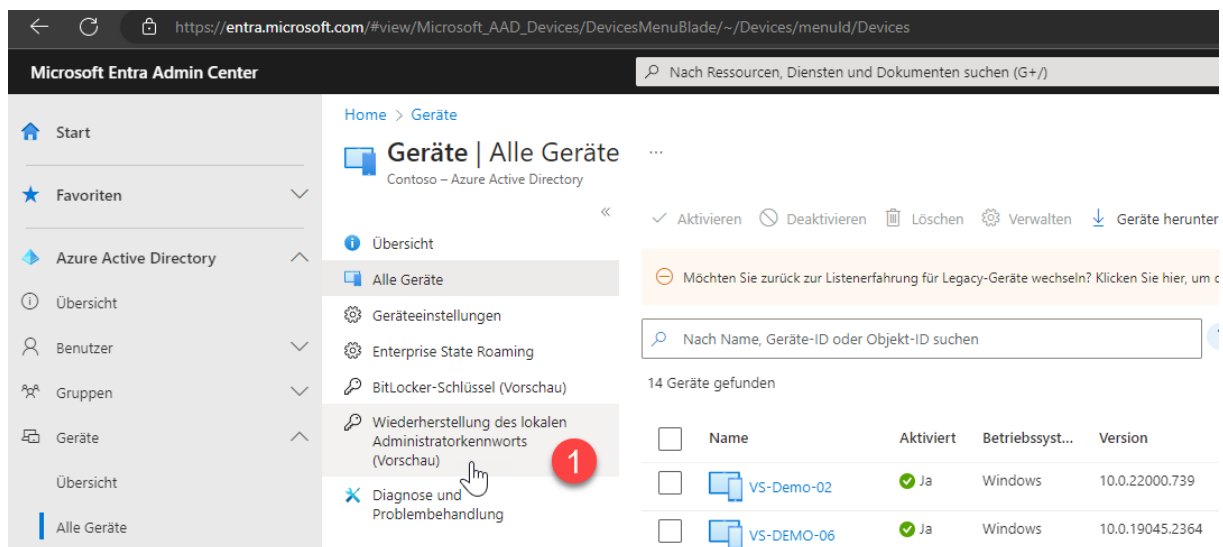


Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)

- Navigieren Sie zunächst [hier](#) zum Microsoft Entra-Verwaltungsportal.

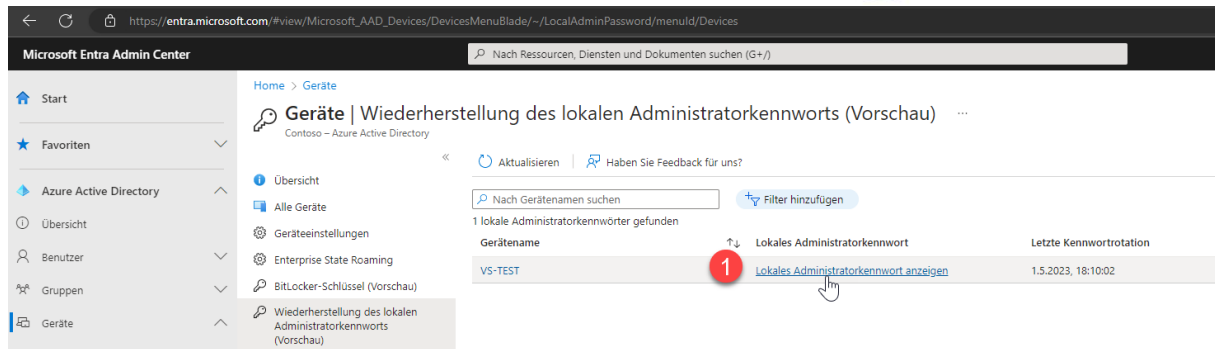


- Klicken Sie im linken Bereich unter **Azure Active Directory** Geräte
- Klicken Sie **Alle Geräte**



- Im linken Bereich können Sie **Wiederherstellung des lokalen Administratorkennworts** auswählen und von dort aus das Administratorpasswort anzeigen.

Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)



Microsoft Entra Admin Center

Home > Geräte

Geräte | Wiederherstellung des lokalen Administratorkennworts (Vorschau) ...

Contoso - Azure Active Directory

Übersicht

Alle Geräte

Geräteeinstellungen

Enterprise State Roaming

BitLocker-Schlüssel (Vorschau)

Wiederherstellung des lokalen Administratorkennworts (Vorschau)

Nach Gerätenamen suchen

Filter hinzufügen

1 lokale Administratorkennwörter gefunden

Gerätename	Lokales Administratorkennwort	Letzte Kennwortrotation
VS-TEST	Lokales Administratorkennwort anzeigen	1.5.2023, 18:10:02

- Klicken Sie Lokales Administratorkennwort anzeigen

Local administrator password ×

Account name

clientadmin

Security ID

1005

Local administrator password

***** Show 

Last password rotation

1.5.2023, 18:10:03

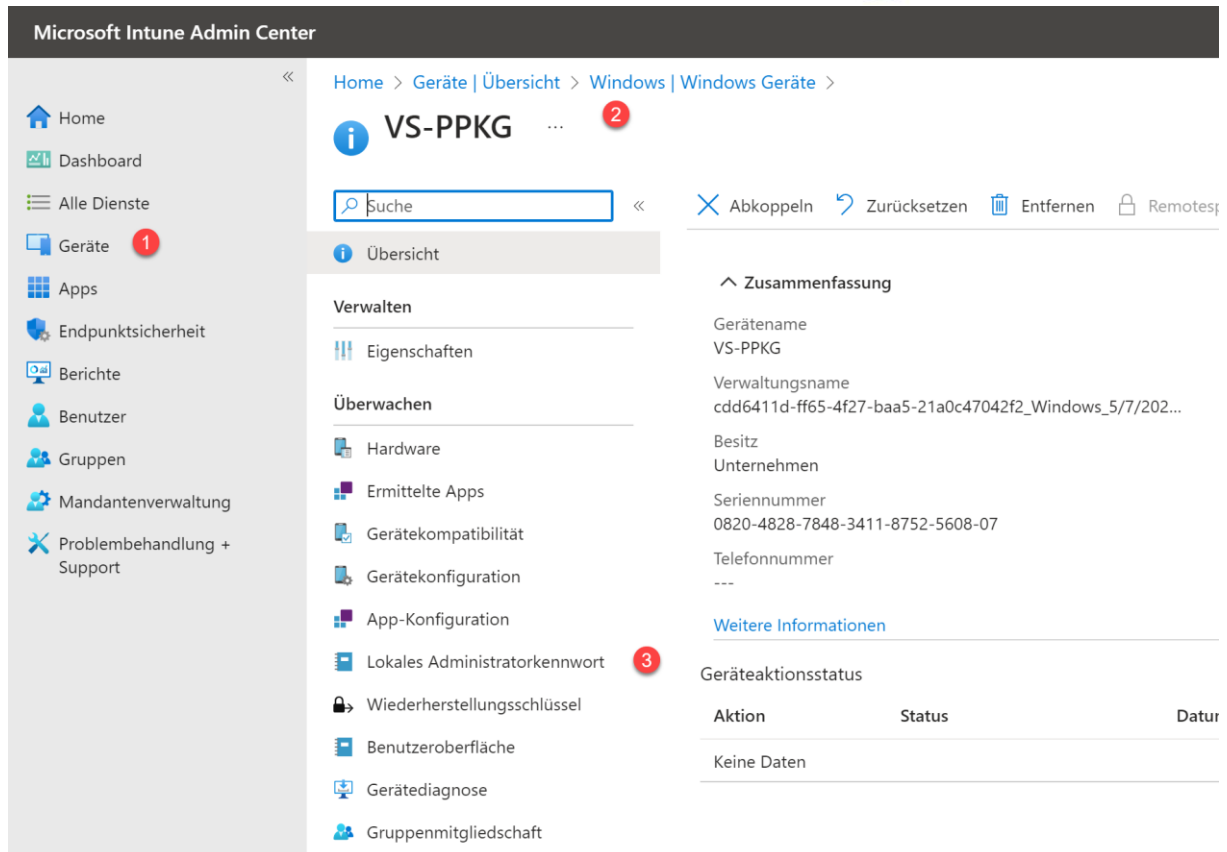
Next password rotation

8.5.2023, 18:10:02

- Klicken Sie auf die Schaltfläche „Show“

4.3.2. INTUNE-PORTAL

Local Administrator Password Solution" (LAPS) für Microsoft Endpoint (Intune)



Microsoft Intune Admin Center

Home > Geräte | Übersicht > Windows | Windows Geräte >

VS-PPKG

Suche

Übersicht

Verwalten

- Eigenschaften

Überwachen

- Hardware
- Ermittelte Apps
- Gerätekompatibilität
- Gerätekonfiguration
- App-Konfiguration
- Lokales Administratorkennwort**
- Wiederherstellungsschlüssel
- Benutzeroberfläche
- Gerätediagnose
- Gruppenmitgliedschaft

Zusammenfassung

Gerätename
VS-PPKG

Verwaltungsname
cdd6411d-ff65-4f27-baa5-21a0c47042f2_Windows_5/7/202...

Besitz
Unternehmen

Seriennummer
0820-4828-7848-3411-8752-5608-07

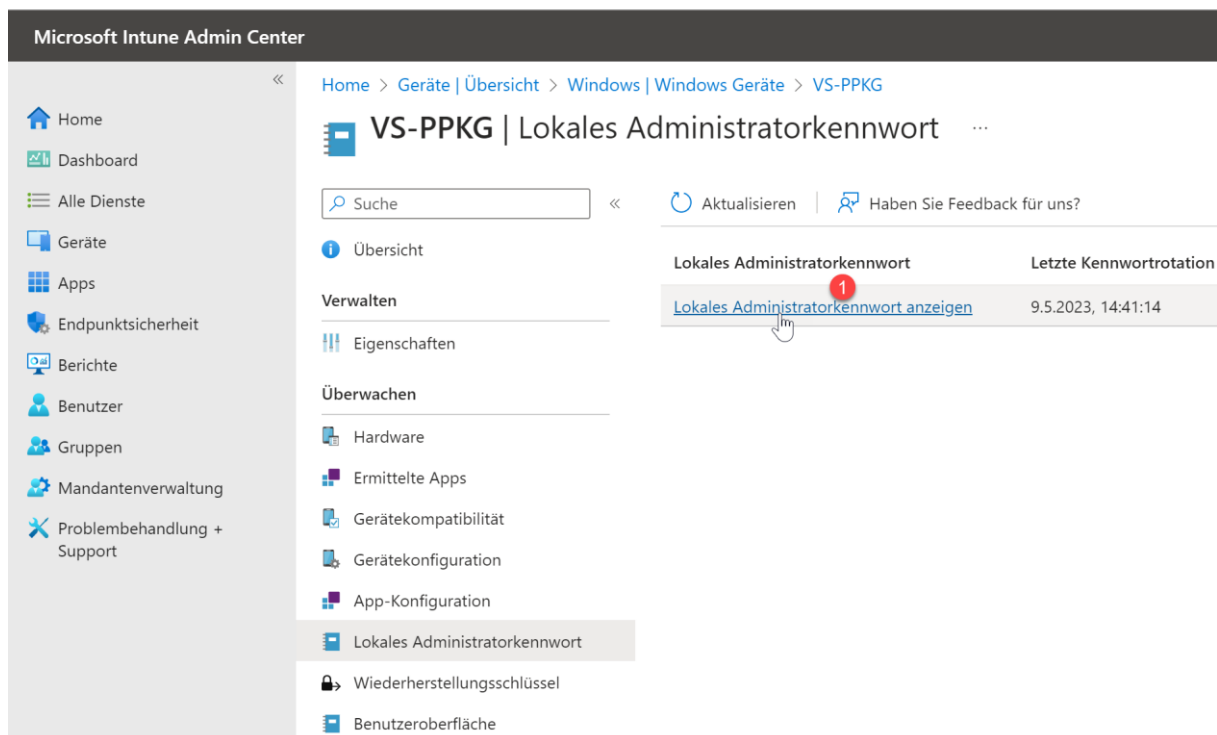
Telefonnummer

Weitere Informationen

Geräteaktionsstatus

Aktion	Status	Datum
Keine Daten		

- Navigieren Sie zu intune.microsoft.com
- Wechseln Sie zu **Geräte**
- Wählen Sie Ihr Gerät aus.
- Klicken Sie **Lokales Administratorkennwort**



Microsoft Intune Admin Center

Home > Geräte | Übersicht > Windows | Windows Geräte > VS-PPKG

VS-PPKG | Lokales Administratorkennwort

Suche

Übersicht

Verwalten

- Eigenschaften

Überwachen

- Hardware
- Ermittelte Apps
- Gerätekompatibilität
- Gerätekonfiguration
- App-Konfiguration
- Lokales Administratorkennwort**
- Wiederherstellungsschlüssel
- Benutzeroberfläche

Lokales Administratorkennwort

Letzte Kennwortrotation

[Lokales Administratorkennwort anzeigen](#)

9.5.2023, 14:41:14

- Klicken Sie **Lokales Administratorkennwort anzeigen**

Lokales Administratorkennwort ×

Kontoname

clientadmin

Sicherheits-ID

S-1-5-21-3800111666-3136795708-2151317961-1005

Lokales Administratorkennwort

***** 1 [Show](#) 

Letzte Kennwortrotation

9.5.2023, 14:41:14

Nächste Kennwortrotation

16.5.2023, 14:41:14

- Klicken Sie **“Show“**

4.3.3. PASSWÖRTER ROTIEREN

Home > Geräte | Übersicht > Windows | Windows Geräte >

VS-PPKG ... ×

Suche << Abkoppeln Zurücksetzen Entfernen Remotesperre Synchron. Passcode zurücksetzen ...

Übersicht

Verwalten

- Eigenschaften

Überwachen

- Hardware
- Ermittelte Apps
- Gerätekompatibilität
- Gerätekonfiguration
- App-Konfiguration
- Lokales Administratorkennwort
- Wiederherstellungsschlüssel
- Benutzeroberfläche

Zusammenfassung

Gerätename
VS-PPKG

Verwaltungsname
cdd6411d-ff65-4f27-baa5-21a0c47042f2_Windows_5/7/202...

Besitz
Unternehmen

Seriennummer
0820-4828-7848-3411-8752-5608-07

Telefonnummer

[Weitere Informationen](#)

Geräteaktionsstatus

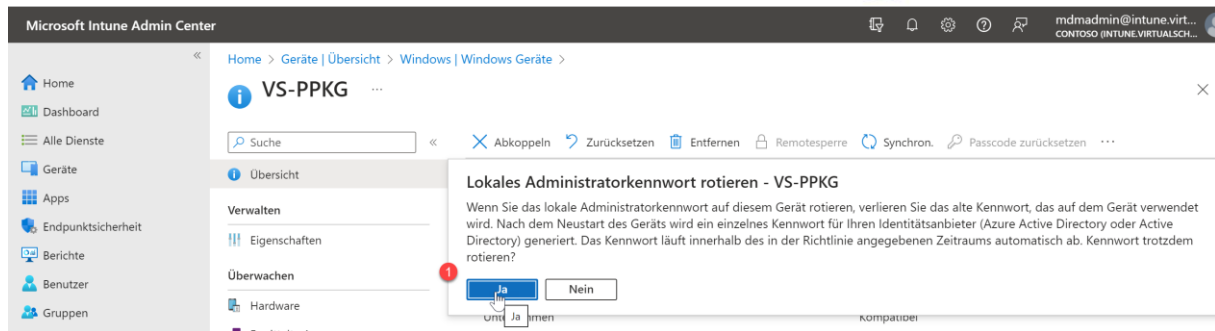
Aktion	Status	Datum/
Keine Daten		

Aktionen:

- Neu starten
- Diagnosedaten sammeln
- Sauberer Start
- Autopilot-Zurücksetzung
- Schnellüberprüfung
- Vollständige Überprüfung
- Windows Defender-Sicherheitsinformationen aktualisieren
- Lokales Administratorkennwort rotieren** 2
- BitLocker-Schlüsselrotation
- Gerät umbenennen
- Neue Remoteunterstützungssitzung
- Gerät suchen

Lokales Administratorkennwort rotieren

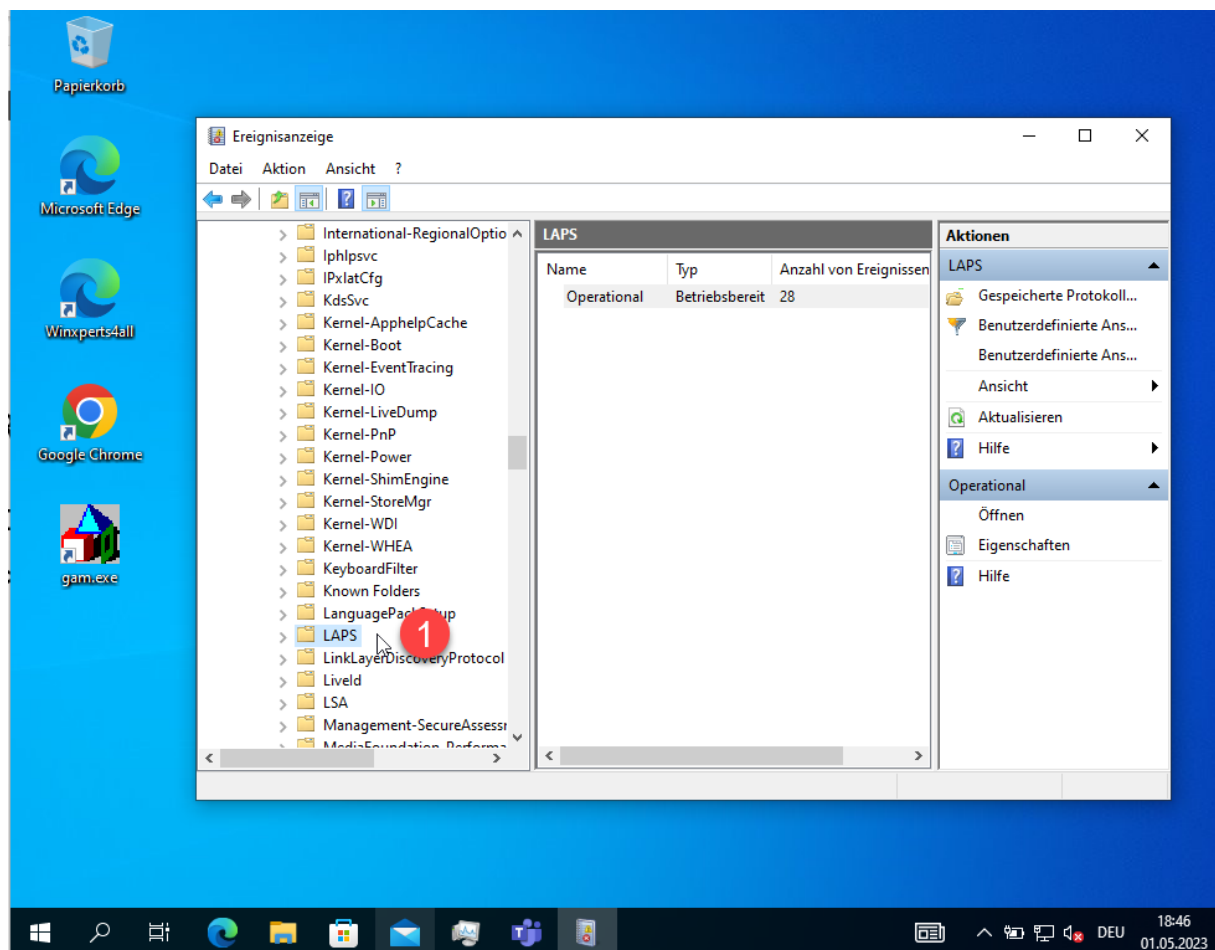
- Klicken Sie im Intune-Portal auf das Gerät, und klicken Sie dann auf die Auslassungspunkte in der Geräteübersicht.
- Klicken Sie **Lokales Administratorkennwort rotieren**



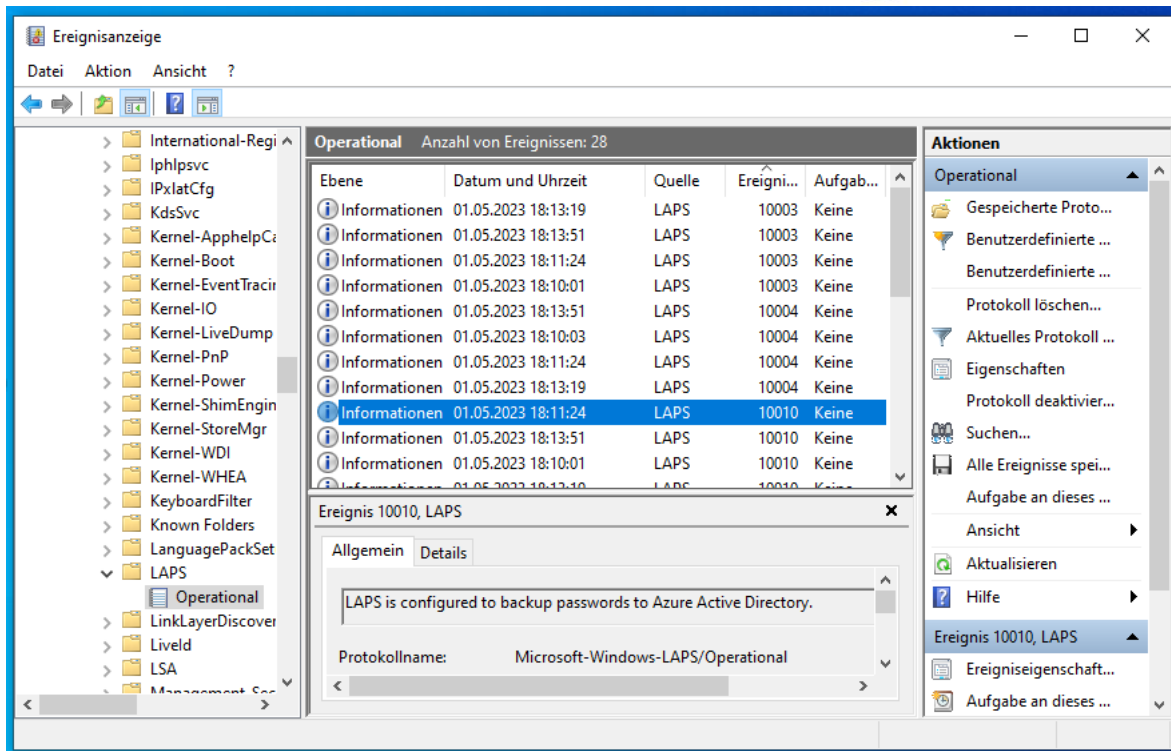
- Sobald der Endpunkt neu gestartet wird, wird das Kennwort geändert.

5. FEHLERBEHEBUNG FÜR WINDOWS LAPS

5.1. WINDOWS LAPS-EREIGNISPROTOKOLLE



Windows LAPS-Protokolle finden Sie in der Windows-Ereignisanzeige unter **Anwendungs- und Dienstprotokolle > Microsoft > Windows > LAPS**



Eine Übersicht über mögliche EventIDs in Bezug auf Windows LAPS finden Sie im Folgenden:

Ereignis-ID	Beschreibung
-------------	--------------

10003	Die Verarbeitung der LAPS-Richtlinie beginnt jetzt.
-------	---

10004	Die Verarbeitung der LAPS-Richtlinie war erfolgreich.
-------	---

10005	Die Verarbeitung der LAPS-Richtlinie ist mit einem Fehlercode fehlgeschlagen.
-------	---

10021	Die Richtlinie ist so konfiguriert, dass das Kennwort in Windows Server Active Directory gesichert wird.
-------	--

10022	Die Richtlinie ist so konfiguriert, dass das Kennwort in Azure Active Directory gesichert wird.
-------	---

10023	Windows LAPS ist so konfiguriert, dass eine ältere Microsoft LAPS-Richtlinie verwendet wird.
-------	--

10018	LAPS hat Active Directory erfolgreich mit dem neuen Kennwort aktualisiert.
-------	--

10029	LAPS hat Azure Active Directory erfolgreich mit dem neuen Kennwort aktualisiert.
-------	--

10020	LAPS hat das lokale Administratorkonto erfolgreich mit dem neuen Kennwort aktualisiert.
10031	LAPS blockierte eine externe Anforderung, die versuchte, das Kennwort des aktuell verwalteten Kontos zu ändern.
10041	LAPS hat eine erfolgreiche Authentifizierung für das aktuell verwaltete Konto erkannt, und es wurde eine Hintergrundaufgabe für Aktionen nach der Authentifizierung geplant.
10042	Der Kulanzzeitraum nach der Authentifizierung ist pro Richtlinie abgelaufen. Konfigurierte Aktionen nach der Authentifizierung werden nun ausgeführt.
10043	LAPS konnte das Kennwort für das aktuell verwaltete Konto nicht zurücksetzen. Das System wiederholt den Vorgang zum Zurücksetzen des Kennworts.
10044	LAPS hat das Kennwort für das aktuell verwaltete Konto erfolgreich zurückgesetzt und alle konfigurierten Aktionen nach der Authentifizierung abgeschlossen.
10033	Der Computer ist mit Legacy-LAPS-Richtlinieneinstellungen konfiguriert, es wird jedoch ein Legacy-LAPS-Produkt installiert. Das Kennwort wird von Windows erst verwaltet, wenn das Legacyprodukt deinstalliert oder neuere LAPS-Richtlinieneinstellungen konfiguriert wurden.
10066	LAPS hat eine LDAP_INSUFFICIENT_RIGHTS Fehlermeldung erhalten, als versucht wurde, das Kennwort mithilfe des LAPS-Kennwortattributs zu aktualisieren. Sie sollten die Berechtigungen für den Container dieses Computers mit dem Cmdlet Set-LapsADComputerSelfPermission aktualisieren
10017	LAPS konnte Active Directory nicht mit dem neuen Kennwort aktualisieren. Das aktuelle Passwort wurde nicht geändert.
10015	Das Kennwort für das verwaltete Konto muss aus einem oder mehreren Gründen aktualisiert werden: (0x1A06) Das Konto verfügt nicht über ein Kennwortablaufattribut Die Richtlinienautorität hat sich geändert Die Richtlinie ist für die Kennwortverschlüsselung konfiguriert, aber das verschlüsselte Kennwortattribut wurde nicht gefunden Die Richtlinie wurde geändert , um ein anderes Ziel für die Kennwortverschlüsselung anzugeben Der lokale Status fehlt und/oder stimmt nicht mit dem Verzeichnisstatus überein
10052	LAPS verarbeitet die aktuelle Richtlinie gemäß der normalen Hintergrundplanung.

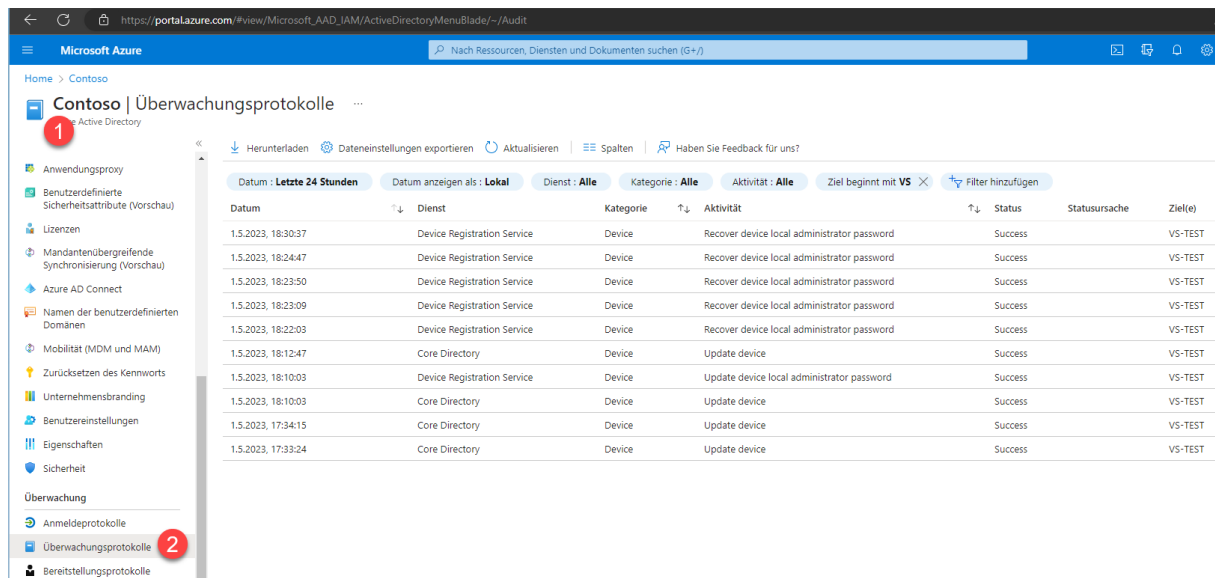
10011 LAPS ist bei der Abfrage von Active Directory nach dem aktuellen Computerstatus fehlgeschlagen. Fehlercode: 0x80070031

10054 LAPS verarbeitet die aktuelle Richtlinie als Reaktion auf eine Benachrichtigung über eine Gruppenrichtlinienänderung.

10057 LAPS konnte keine Bindung über LDAP an den Domänencontroller herstellen:

5.2. AZURE-ÜBERWACHUNGSPROTOKOLLE

Windows LAPS-Ereignisse werden auch an Azure-Überwachungsprotokolle gesendet, die im Azure-Portal angezeigt werden können.



Contoso | Überwachungsprotokolle

Datum: Letzte 24 Stunden | Datum anzeigen als: Lokal | Dienst: Alle | Kategorie: Alle | Aktivität: Alle | Ziel beginnt mit VS | Filter hinzufügen

Datum	Dienst	Kategorie	Aktivität	Status	Statusursache	Ziel(e)
1.5.2023, 18:30:37	Device Registration Service	Device	Recover device local administrator password	Success		V5-TEST
1.5.2023, 18:24:47	Device Registration Service	Device	Recover device local administrator password	Success		V5-TEST
1.5.2023, 18:23:50	Device Registration Service	Device	Recover device local administrator password	Success		V5-TEST
1.5.2023, 18:23:09	Device Registration Service	Device	Recover device local administrator password	Success		V5-TEST
1.5.2023, 18:22:03	Device Registration Service	Device	Recover device local administrator password	Success		V5-TEST
1.5.2023, 18:12:47	Core Directory	Device	Update device	Success		V5-TEST
1.5.2023, 18:10:03	Device Registration Service	Device	Update device local administrator password	Success		V5-TEST
1.5.2023, 18:10:03	Core Directory	Device	Update device	Success		V5-TEST
1.5.2023, 17:34:15	Core Directory	Device	Update device	Success		V5-TEST
1.5.2023, 17:33:24	Core Directory	Device	Update device	Success		V5-TEST