NICK INFORMATIONSTECHNIK GMBH

ZeroPortal – Administrationshandbuch

Installation, Einrichtung und Betrieb

Stand September 2026 (Server 1.0.30, Agent 1.0.36)

Dieses Handbuch führt in kompakter Form durch Installation, Einrichtung und Betrieb von ZeroPortal. Es richtet sich an Administratoren, die das Portal aufsetzen und betreuen. Wo ein Thema mehr Tiefe braucht, verweist der Text auf das jeweilige Detaildokument (siehe Kapitel 14).

Inhalt

1. Was ZeroPortal macht

ZeroPortal verteilt Anwendungen als **App-V-** und **MSIX-Pakete** an Windows-Geräte und setzt **Richtlinien** auf den Geräten durch. Die Pakete liegen auf einer Netzwerkfreigabe; das Portal verwaltet, wer welches Paket bekommt. Auf jedem Gerät läuft der **ZeroPortal-Agent**, der sich regelmäßig beim Portal meldet, die Zuweisungen abholt und Pakete installiert, aktualisiert oder wieder entfernt.

Die Bausteine:

- **Portal (Server):** Weboberfläche, Datenbank, Paketkatalog, Berechtigungen, Richtlinien. Läuft als Windows-Dienst mit eigenem Webserver.
- **MariaDB:** Datenbank des Portals. Für Hochverfügbarkeit repliziert.
- **Paketfreigabe:** SMB-Freigabe mit den App-V- und MSIX-Paketen. Die Clients laden Pakete direkt von dort, nicht über das Portal.
- **Agent:** Windows-Dienst plus Tray-Symbol auf jedem Gerät. Gleicht im Geräte- und im Benutzerkontext ab.
- **PowerShell-Modul:** Praktisch jede Verwaltungsaufgabe lässt sich auch per Cmdlet erledigen: Pakete, Zuweisungen, Gruppen und Rechte, Richtlinien, Lizenzen, Sicherung.

Die Anmeldung am Portal erfolgt mit dem Windows-Konto (Kerberos). Berechtigungen werden an AD-Gruppen vergeben.

2. Systemvoraussetzungen und Dimensionierung

Was Sie brauchen

Komponente	Anforderung
Portal-Server	Windows Server (64 Bit), Mitglied der Domäne. .NET bringt das Installationspaket mit.
Datenbank	**MariaDB 11.8 oder 12.3** (beide LTS), lokal auf dem Portal-Server oder auf eigener Maschine; getestet mit 11.8.6 und 12.3.3. Ältere Reihen (11.4, 10.x) sind nicht geeignet: Das Setup warnt nur, Datenbankwerkzeug und Portalstart brechen ab. **MySQL wird nicht unterstützt.** Im Cluster auf allen Knoten dieselbe Version.
Paketfreigabe	SMB-Freigabe, lesbar für Computerkonten (App-V, MSIX) und Benutzer
Clients	Windows 10/11 bzw. Windows Server (RDS) mit App-V-Client und/oder MSIX-Unterstützung
Netzwerk	Clients erreichen das Portal per HTTPS und die Paketfreigabe per SMB
Zertifikat	Serverzertifikat für die Portal-URL, das die Clients als vertrauenswürdig kennen

Welche MariaDB-Reihe? Immer eine **LTS-Reihe** (11.8 oder 12.3): mehrere Jahre nur Fehlerkorrekturen. Rolling-Reihen (12.0, 12.1, 12.2, 13.x) werden nur ein Jahr gepflegt und erzwingen alle drei Monate einen Reihenwechsel mit neuem Programmordner (Kapitel 12). Wartungsfristen: mariadb.org/about (Maintenance Policy).

Größe des Portal-Servers

Ein einzelner Portal-Knoten reicht für sehr große Umgebungen:

Endgeräte	Knoten	vCPU	RAM	Anmerkung
bis 10 000	1	2	8 GB	Auch 10 000 Anfragen innerhalb von 10 Minuten sind kein Problem
bis 50 000	1	6	16 GB	50 000 Anmeldungen innerhalb von 15 Minuten werden verarbeitet
bis 100 000	1	8	16 GB	100 000 Anmeldungen innerhalb von 15 Minuten werden verarbeitet

Ein zweiter Knoten dient vor allem der **Verfügbarkeit**; mit zufälliger Serverauswahl verteilt er zusätzlich die Abgleichlast (Kapitel 11). MariaDB auf demselben Server ist üblich; ab 50 000 Geräten empfiehlt sich eine SSD für das Datenverzeichnis. Ein Abgleich überträgt rund 5 KB (10 000 Abgleiche in 10 Minuten: unter 1 MBit/s); die Paketdaten gehen per SMB von der Freigabe zum Client, die Freigabe muss also die Paketgrößen und die gleichzeitigen Erstinstallationen tragen. Der Agent meldet sich alle 60 Minuten plus 0 bis 10 Minuten Zufall und 30 Sekunden nach dem Systemstart.

Virenschutz

Auf dem Portal-Server Installationsverzeichnis, MariaDB-Datenverzeichnis und Paketfreigabe vom Echtzeitscan ausnehmen. Mit Microsoft Defender:

```
Add-MpPreference -ExclusionPath "C:\Program Files\ZeroPortal"
Add-MpPreference -ExclusionPath "C:\Program Files\MariaDB*\data"
Add-MpPreference -ExclusionPath "D:\Packages"          # Paketfreigabe
Add-MpPreference -ExclusionProcess "C:\Program Files\ZeroPortal\zeroPortal.exe"
Add-MpPreference -ExclusionProcess "mysqld.exe"
```

Die Prozessausnahme für den Portaldienst ist die wichtigste: Ohne sie belegte der Virenscanner in unseren Messungen dauerhaft 7 bis 15 Prozent CPU.

Clients mit App-V: Der App-V-Client 5 braucht keine Ausnahmen; die Zeit beim Erststart steckt im Streaming des Pakets, nicht im Scanner. Ausnahmen nur in zwei Fällen:

Umgebung	Regel
Session Hosts und VDI mit Shared Content Store	Genau ein Pfad: `C:\ProgramData\App-V` (bei verlegtem Cache der Wert von `Get-AppvClientConfiguration -Name PackageInstallationRoot`), per GPO unter *Microsoft Defender Antivirus → Ausschlüsse → Pfadausschlüsse* oder lokal mit `Add-MpPreference -ExclusionPath 'C:\ProgramData\App-V'`; bei Manipulationsschutz nur per GPO oder Intune. Software-Inventur (z. B. ConfigMgr) mit einer leeren `skpswi.dat` in der Cache-Wurzel fernhalten.
Einzelne Anwendung	Nur nach Messung, wenn eine Anwendung beim Start selbst ausführbare Dateien erzeugt (Paint.NET mit Plugins): ihr Cache-Ordner, z. B. `C:\Users\*\AppData\Local\paint.net\AppCache`.

Nicht ausschließen: `C:\Users\*\AppData\Local\Microsoft\AppV`, `…\Roaming\Microsoft\AppV`, die Paketfreigabe vom Client aus sowie `AppVClient.exe` und `AppVStreamingUX.exe`. Für MSIX und App Attach gibt es keine gesonderte Empfehlung.

3. Installation des Servers

Reihenfolge

1. **MariaDB installieren:** Reihe 11.8 oder 12.3, Standardinstallation mit Zeichensatz UTF-8 (utf8mb4), Root-Passwort notieren. Programm- und Datenverzeichnis bei der Vorgabe des Installers belassen (`C:\Program Files\MariaDB 11.8` mit `data` neben `bin`); sonst finden die my.ini-Funktionen des Replikationsassistenten die Datei nicht. Der Dienst muss laufen, bevor das Portal eingerichtet wird.
2. **Portal-MSI installieren** (`ZeroPortal-<Version>.msi`) nach `C:\Program Files\ZeroPortal`. Das Setup legt den Dienst an und startet am Ende das Konfigurationstool (später: `C:\Program Files\ZeroPortal\ZeroPortalConfigTool.ps1` als Administrator).
3. **Paketfreigabe anlegen** und Berechtigungen setzen (siehe unten).
4. **Portal aufrufen** und die erste Einrichtung durchführen (Kapitel 4).

Das Konfigurationstool

Fünf Schritte:

1. **Certificate:** Zertifikat der eigenen PKI wählen oder PFX importieren. *Import to Trusted Root* vertraut einem selbst ausgestellten Zertifikat nur auf dem Server, nicht auf den Clients.
2. **Base Configuration:** Hostname und Port des mitgelieferten Webservers (z. B. `https://zeroportal.firma.local:8080`, kein IIS nötig), Kästchen *Open Windows Firewall for inbound traffic*, Datenbankverbindung und Replikationspasswort für den Clusterbetrieb.
3. **Admin Users:** AD-Gruppe der Voll-Administratoren (z. B. `Firma\ZeroAdmins`), optional eine Gruppe mit Lesezugriff. Ohne die erste Gruppe kommen Sie nicht hinein.
4. **Database Install / Update:** Legt Datenbank, Portal-Benutzer und Schema an.
5. **Service Control:** *Save & Restart Service*.

Die Einstellungen landen in `C:\Program Files\ZeroPortal\appsettings.json`. Diese Datei ist knotenspezifisch und gehört in jede Sicherung (Kapitel 12).

Paketfreigabe einrichten

Eine SMB-Freigabe, z. B. `\\fileserver\Packages`, mit Unterordnern für App-V und MSIX. Die Freigabe selbst lässt jeden durch, die eigentlichen Rechte vergibt NTFS. Zwei eigene Gruppen im Active Directory halten das wartbar, wenn später Server oder Paketierer dazukommen:

Gruppe	Mitglieder
`ZeroPortal-Server`	die **Computerkonten** aller Portal-Knoten
`ZeroPortal-Paketierer`	die Personen, die Pakete ablegen

Das Portal läuft als Systemdienst und greift mit dem Computerkonto des Servers auf die Freigabe zu, deshalb stehen in der ersten Gruppe Computer und keine Benutzer. Schreibrecht braucht es, weil es App-Attach-Images neben das Paket legt. Die Clients lesen als Computerkonto (maschinenweite Installation) und als angemeldeter Benutzer.

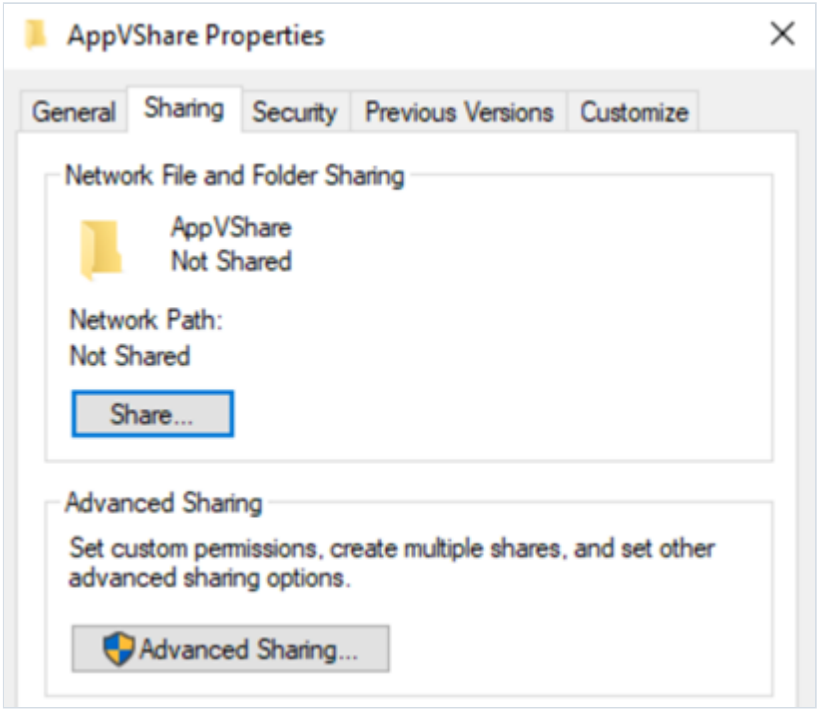
Freigabeberechtigung (Eigenschaften → *Freigabe* → *Erweiterte Freigabe* → *Berechtigungen*):

Konto	Berechtigung
Jeder	Ändern (Vollzugriff geht ebenso)

NTFS-Berechtigung (Eigenschaften → *Sicherheit* → *Erweitert*), jeweils anwenden auf *Diesen Ordner, Unterordner und Dateien*:

Konto	Berechtigung
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
`ZeroPortal-Server`	Vollzugriff
`ZeroPortal-Paketierer`	Ändern
Domänencomputer	Lesen, Ausführen
Domänen-Benutzer	Lesen, Ausführen

1. **Ordner anlegen** auf dem Dateiserver, etwa `D:\Packages`, mit den Unterordnern `AppV` und `MSIX`.
2. **Vererbung abschalten:** *Sicherheit → Erweitert → Vererbung deaktivieren → Vererbte Berechtigungen in explizite Berechtigungen konvertieren*, danach den Eintrag *Benutzer* entfernen. Sonst dürfen alle Benutzer im Paketordner Dateien anlegen, das ist das Standardrecht auf einem Datenlaufwerk.
3. **NTFS-Rechte** laut Tabelle eintragen.
4. **Freigeben:** Eigenschaften → *Freigabe* → *Erweiterte Freigabe*, Freigabename vergeben und die Freigabeberechtigung laut Tabelle setzen. Ein `$` am Ende versteckt die Freigabe im Netzwerk, das ist üblich, aber nicht nötig.



5. **Offlinedateien abschalten:** Im selben Dialog unter *Zwischenspeichern* den Haken *Zwischenspeichern der Freigabe zulassen* entfernen, oder per PowerShell `Set-SmbShare -Name Packages -CachingMode None`. Sonst können Clients Pakete aus einem veralteten lokalen Zwischenspeicher lesen statt von der

Freigabe.

6. **Portal-Knoten neu starten**, nachdem ihre Computerkonten in `ZeroPortal-Server` aufgenommen wurden; vorher trägt ihr Kerberos-Ticket die Gruppe noch nicht.

Das Portal liest die Freigabe danach als **Repository** ein (Kapitel 4). Pakete werden durch Kopieren in die Freigabe bereitgestellt, es gibt keinen Upload über den Browser.

Firewall und Ports

Alle Verbindungen gehen vom Client oder vom Knoten **ausgehend** zum Ziel; ZeroPortal verlangt keine Verbindung von außen nach innen.

Von → nach	Port	Wofür	Pflicht
Clients und Browser → Portal	Portal-Port, TCP (HTTPS), im Konfigurationstool festgelegt, z. B. 8080	Abgleich der Agenten, Weboberfläche, App-V-Reporting	ja
Clients → Paketfreigabe	TCP 445 (SMB)	Paketdaten laden, App-Attach-Images einhängen	ja
Portal → Paketfreigabe	TCP 445 (SMB)	Pakete einlesen, App-Attach-Images erzeugen	ja
Portal → Domänencontroller	TCP/UDP 389 (LDAP) oder der eingestellte Port, dazu TCP/UDP 88 (Kerberos) und 53 (DNS)	Anmeldung, Auflösung von Benutzern und Gruppen	ja, in der Domäne
Portal → MariaDB	TCP 3306	Datenbank; auf demselben Server bleibt der Verkehr lokal	ja
Replica → Primary	Portal-Port (HTTPS) **und** TCP 3306	Weitergeleitete Schreibvorgänge, Herzschlag, Datenbankreplikation	nur im Cluster
Primary → Replica	Portal-Port (HTTPS)	Erreichbarkeitsprüfung, Assistent, Wartungsmodus	nur im Cluster
Portal → Mailserver	TCP 587, alternativ der eingestellte Port	Benachrichtigungen per E-Mail	nur mit E-Mail
Clients → Internet	TCP 80 und 443	Sperrlistenprüfung der Paketsignatur; ohne Zugang siehe *Bekannte Fehlerbilder*	nein

Der Agent öffnet keinen eingehenden Port; auf den Clients ist keine Firewallregel nötig. Das Konfigurationstool legt die Regel `ZeroPortal Inbound <Port>` an, der Replikations-Assistent die Regel für Port 3306 auf beiden Knoten, beide nur in der **Windows-Firewall**. Bei einer Drittanbieter- oder Hardware-Firewall müssen der Portal-Port und im Cluster Port 3306 dort von Hand freigegeben werden.

Anmeldung ohne Passwortabfrage (SSO)

Damit sich Browser still mit dem Windows-Konto anmelden, muss die Portal-URL in der **Intranetzone** liegen. Einen SPN brauchen Sie in der Regel nicht:

- GPO: *Benutzerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Internet Explorer → Internetsystemsteuerung → Sicherheitsseite → Site-zu-Zone-Zuweisungsliste*, Portal-FQDN mit Wert **1**. Gilt auch für Edge und Chrome.
- SPN: Der Portaldienst läuft als lokales Systemkonto; für den eigenen Servernamen existiert der SPN am Computerkonto bereits. Nur wenn das Portal zusätzlich unter einem Alias erreichbar sein soll, gehört dieser an das Computerkonto: `setspn -S HTTP/zeroportal.firma.local SERVERNAME$`. Einen Load Balancer mit gemeinsamem Namen vor mehreren Knoten empfehlen wir nicht; der Agent schaltet selbst um (*Bekannte Fehlerbilder*).

Ein Anmeldefenster trotz korrekter Berechtigung bedeutet fast immer eine fehlende Intranetzone (Kapitel 13).

4. Erste Einrichtung

Nach dem ersten Aufruf mit einem Konto aus der Administratorengruppe:

1. **Repositories** (*Globale Konfiguration → Konfiguration*, Abschnitt *Paket-Repositorys*): Paketfreigabe als App-V- bzw. MSIX-Repository eintragen.
2. **E-Mail** (Abschnitt *E-Mail-Benachrichtigungen*): SMTP-Server, Absender, Empfänger. Über diesen Weg meldet das Portal ablaufende Zertifikate, Lizenzprobleme, eine nicht erreichbare Datenbank und abgeschaltetes Audit.
3. **Berechtigungen** (*Globale Konfiguration → Berechtigungen*): Weitere Gruppen anlegen (Kapitel 5). Mindestens eine Gruppe mit Leserechten für den Servicedesk ist sinnvoll.
4. **Lizenz** (*Globale Konfiguration → Lizenzierung*): 30 Lizenzen sind enthalten; darüber hinaus die Lizenzdatei hochladen und den Zählmodus wählen (Kapitel 6).
5. **Audit** (Abschnitt *Audit-Protokoll*): eingeschaltet lassen, Aufbewahrung festlegen.
6. **Agent-Download** (*Downloads*): Hier liegt die zur Serverversion passende Agent-MSI. Den Rollout beschreibt Kapitel 7.

5. Berechtigungen

Grundprinzip

Das Portal besteht aus acht **Bereichen**: App-V (Pakete und Verbindungsgruppen), MSIX (Pakete und App Attach), Richtlinien, Berichte (App-V-Reporting), Downloads (Agent-MSI), Konfiguration (portalweite Einstellungen, Repositories, E-Mail, Sicherung), Hochverfügbarkeit und Knoteneinstellungen. Für jeden Bereich vergeben Sie einer Gruppe eine **Stufe**:

Stufe	Was die Person darf
Keine	Der Bereich erscheint nicht im Menü und ist auch per Adresszeile gesperrt
Lesen	Alles ansehen, nichts verändern
Verwalten	Ansehen, anlegen, bearbeiten, löschen

Voll-Administratoren dürfen alles. Drei Dinge sind ihnen vorbehalten und lassen sich nicht delegieren: **Berechtigungen vergeben** (auch die Stufe *Verwalten* im Bereich *Konfiguration* erlaubt keine weiteren Rechte), **Sicherung und Wiederherstellung** (Kapitel 12) sowie **Benutzer, Geräte, Lizenzen und das Audit-Protokoll verwalten** (Portalgruppen, interne Konten, Rollout-Token, Lizenzierung, Audit).

> Die Stufe *Verwalten* im Bereich *Konfiguration* ist trotzdem weitreichend: Sie erlaubt das Ändern portalweiter Einstellungen einschließlich Repositories und E-Mail-Versand. Vergeben Sie sie nur an Personen, denen Sie den Betrieb des Portals anvertrauen.

Portalgruppen anlegen

Rechte hängen an **Portalgruppen**. Zwei davon legt das Portal selbst aus den Gruppen in `appsettings.json` an, also aus dem Schritt *Admin Users* des Konfigurationstools:

Portalgruppe	Rechte	Mitglieder	Verhalten
Portal administrators	Verwalten, alle Bereiche	AD-Gruppe aus `AccessGroups:FullAdmins`, dazu ein eingerichtetes `RootUser`-Konto	Bei jedem Dienststart geprüft; Fehlendes wird neu angelegt
Portal read-only	Lesen, alle Bereiche	AD-Gruppe aus `AccessGroups:ReadOnlyAdmins`	Einmalig beim ersten Start, nur wenn die Gruppe eingetragen ist; gelöscht bleibt gelöscht

Weitere Portalgruppen legen Sie selbst an. Eine Portalgruppe enthält AD-Gruppen (empfohlen), einzelne AD-Konten oder Geräte und Benutzer ohne AD (Kapitel 7). Unter *Globale Konfiguration → Portalgruppen* die Gruppe anlegen und Mitglieder hinzufügen, danach unter *Berechtigungen* je Bereich die Stufe wählen. Zum Beispiel:

Portalgruppe	Rechte	Mitglieder
Paketverwaltung	MSIX: Verwalten · App-V: Verwalten · Berichte: Lesen	`Firma\SW-Paketierer`
Servicedesk	MSIX: Lesen · App-V: Lesen · Berichte: Lesen	`Firma\Helpdesk`

Paketzuweisungen

Wer ein Paket **bekommt**, wird am Paket selbst festgelegt (Kapitel 8 und 9); die Berechtigungen aus diesem Kapitel regeln nur, wer im Portal **verwalten** darf. Für **MSIX** lassen sich AD-Gruppen und einzelne AD-Konten, Portalgruppen, interne Konten sowie Geräte und Benutzer aus dem Enrollment berechtigen, für **App-V** ausschließlich AD-Gruppen.

Nicht aussperren

Zwei Notausgänge stehen in `appsettings.json`: die Gruppe aus dem Konfigurationstool (`AccessGroups.FullAdmins`) und optional ein einzelnes Konto (`RootUser`). Beide gelten immer, auch wenn im Portal alle Rechte entfernt wurden. Nach einer Änderung den Dienst neu starten.

6. Lizenzierung

ZeroPortal zählt, es blockiert nicht. Bei Überschreitung der lizenzierten Zahl arbeitet die Verteilung weiter; das Portal meldet die Überschreitung per E-Mail und auf der Lizenzseite.

- Gezählt wird, was der **ZeroPortal-Agent** ausliefert (MSIX, App Attach und auch App-V): Geräte oder Benutzer, die sich über den Agenten in den **letzten 90 Tagen** gemeldet haben. Wer App-V ausschließlich mit dem Microsoft-App-V-Client bezieht, braucht keine Lizenz und wird nicht gezählt, unabhängig von der Zahl der Benutzer und Geräte; das App-V-Reporting ist ebenfalls kostenfrei.
- Der **Modus** auf der Lizenzierungsseite legt fest, ob Benutzer oder Geräte gezählt werden; er wird nicht automatisch erkannt. Für Terminalserver (RDS, AVD) empfiehlt sich *pro Benutzer*; im Modus *pro Gerät* zählt das Portal die Geräte, von denen aus verbunden wird, nicht den Sitzungshost.
- **30 Lizenzen sind enthalten** und laufen nicht ab. Darüber hinaus laden Sie vom Hersteller signierte **Lizenzdateien** hoch. Mehrere Dateien addieren sich, solange sie zum Modus passen; Dateien für den anderen Modus erscheinen grau, abgelaufene rot, beide zählen nicht mit.
- Die Lizenz wird beim Abgleich nebenbei gebucht und blockiert den Abgleich nie. Ist das Portal nicht erreichbar, entfernt der Agent nichts; alles Installierte läuft weiter.

Produktsupport über das Ticketsystem (Reaktionszeit 4 Stunden an Werktagen zu deutschen Bürozeiten) ist ab 20.000 lizenzierten Benutzern enthalten. Darunter, und für die 30 kostenfreien Lizenzen, wird Support als Paket oder nach Zeit abgerechnet; das gilt auch für Hilfe zu App-V- und MSIX-Paketen.

7. Clients anbinden

Der empfohlene Weg

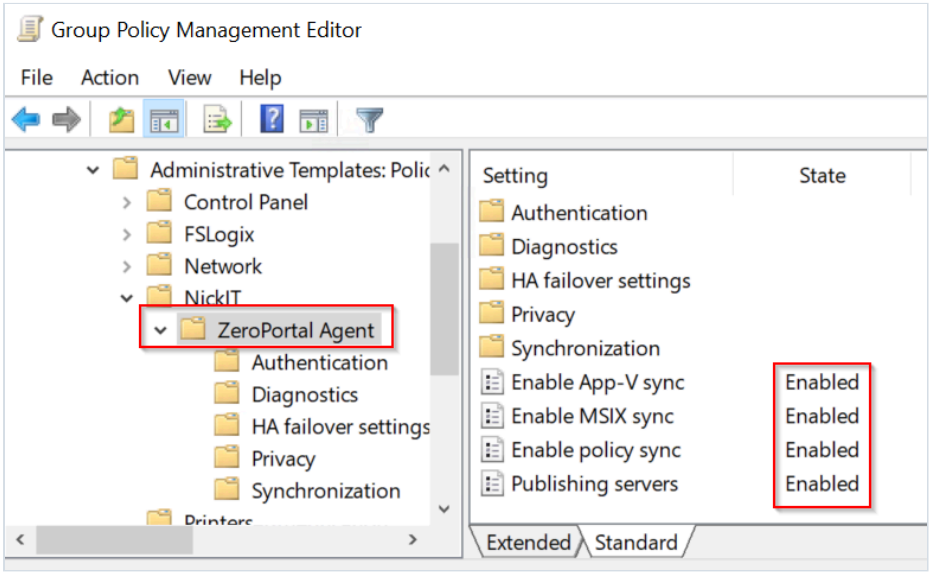
Der Agent wird ohne Parameter installiert; alle Einstellungen kommen per Gruppenrichtlinie. Nach der Installation sind App-V, MSIX und Richtlinien im Agenten **ausgeschaltet**, bis die Gruppenrichtlinie sie einschaltet.

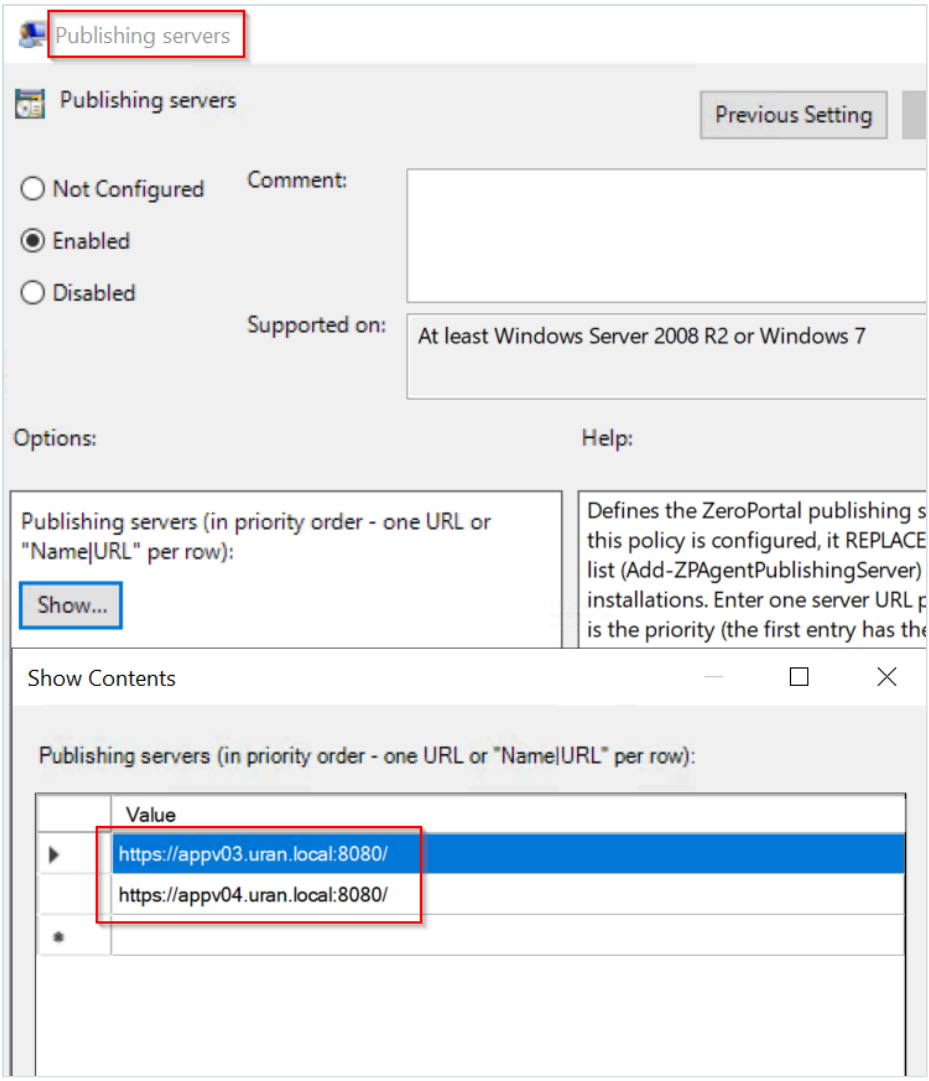
1. **ADMX-Vorlage** in den Central Store kopieren (`\\<Domäne>\SYSVOL\<Domäne>\Policies\PolicyDefinitions`). Die Einstellungen erscheinen unter *Computerkonfiguration → Administrative Vorlagen → NickIT → ZeroPortal Agent*.
2. **Eine GPO** für die Zielcomputer mit den vier Einstellungen, die über alles Weitere entscheiden:

Einstellung	Was sie bewirkt
Publishing-Server	Die Portal-URLs, je Zeile eine, in Prioritätsreihenfolge. Ohne sie weiß der Agent nicht, wen er fragen soll.
Sync MSIX einschalten	MSIX-Pakete und App Attach.
Sync App-V einschalten	App-V-Pakete und Verbindungsgruppen. Beachten Sie die Regel unten.
Sync Richtlinien einschalten	ZeroPortal-Richtlinien: Laufwerke, Drucker, Desktop, Skripte und die übrigen Vorlagen.

Bei eigener PKI verteilt dieselbe GPO das Serverzertifikat in die *Vertrauenswürdigen Stammzertifizierungsstellen* des Computers. 3. **Agent-MSI** ohne Parameter verteilen (GPO-Softwareinstallation, Intune oder ein beliebiger Softwareverteiler). Die MSI liegt im Portal unter *Downloads*. Der Agent registriert sich beim ersten Abgleich selbst; das Gerät erscheint unter *Bekannte Clients*. 4. **Feineinstellungen** (Abgleichintervall, Tray-Verhalten, laufende Anwendungen) über ZeroPortal-Richtlinien vom Typ *Agent-Konfiguration* (Kapitel 10).

> **Wo finde ich die ADMX-Vorlage?** Sie wird mit dem **Agenten** installiert und liegt auf jedem Gerät mit Agent unter `C:\Program Files\NickIT\ZeroPortalAgent\admx`, samt den Sprachordnern `de-DE` und `en-US`. Einen getrennten Download gibt es nicht.





> **App-V: immer nur ein Weg je Gerät.** Nutzt der **Microsoft-App-V-Client** das Portal selbst als Publishing-Server, bleibt *Sync App-V einschalten* **ausgeschaltet**. Übernimmt umgekehrt der ZeroPortal-Agent die App-V-Pakete, tragen Sie im Microsoft-Client **keinen** Publishing-Server ein. Laufen beide, veröffentlichen und entfernen sie dieselben Pakete abwechselnd: Verknüpfungen verschwinden und kommen wieder, die Protokolle laufen voll. MSIX und Richtlinien sind davon nicht betroffen und dürfen parallel laufen.

Rangfolge der Einstellungen: Gruppenrichtlinie vor ZeroPortal-Richtlinie *Agent-Konfiguration* vor lokalem Wert (`Set-ZPAgentConfiguration`, MSI-Parameter). Publishing-Server und Registrierungstoken gibt es nur in der Gruppenrichtlinie. Ist ein Schalter per GPO gesetzt, sind lokale Änderungen wirkungslos; `Get-ZPAgentConfiguration` zeigt das in der Spalte *SetByGroupPolicy*.

Agent installieren

```
msiexec /i ZeroPortalAgent-<Version>.msi /qn
```

Parameter sind nur nötig, wenn keine Gruppenrichtlinie greift (Test, Workgroup):

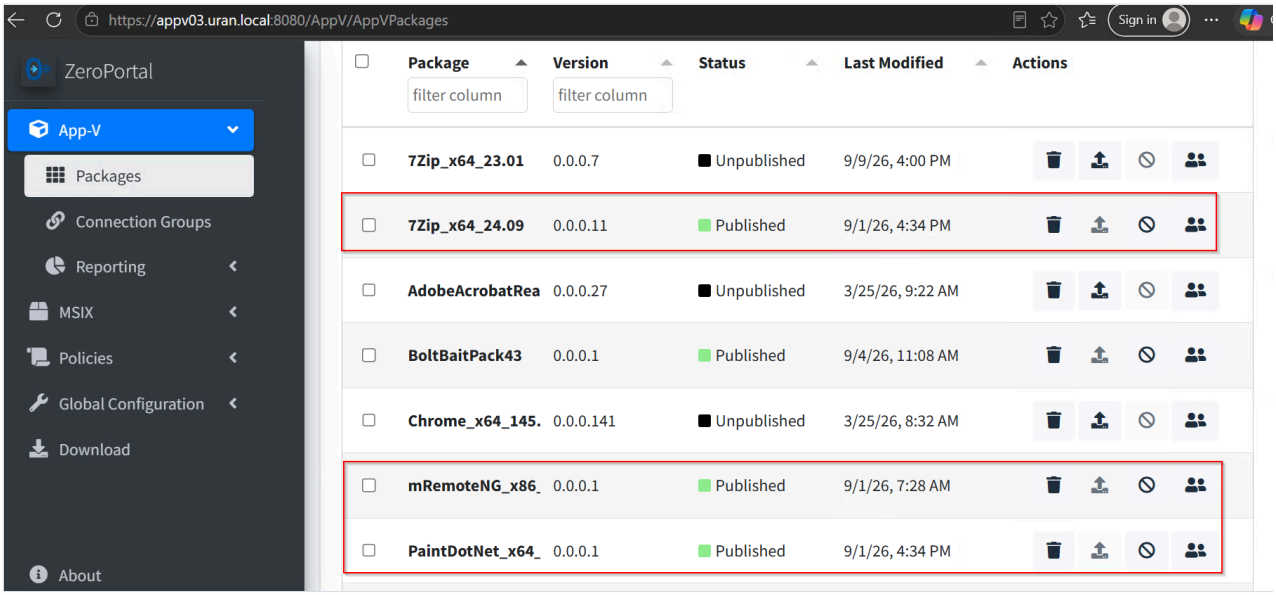
Parameter	Bedeutung
`SERVER=`	Portal-URL, wenn nicht per Gruppenrichtlinie gesetzt
`APPVSYNC=1` / `MSIXSYNC=1` / `POLICYSYNC=1`	Bereitstellung von App-V- bzw. MSIX-Paketen und Verarbeitung der Richtlinien einschalten
`TRUSTCERT=1`	Serverzertifikat nicht prüfen (nur Test)
`NOTRAY=1` / `NOTOASTS=1`	Kein Tray-Symbol bzw. keine Hinweisfenster
`ENROLLTOKEN=`	Einladungstoken für Geräte ohne AD (siehe unten)

Geräte ohne Active Directory melden sich mit einem Schlüssel an statt mit Kerberos: Unter *Globale Konfiguration → Agent-Registrierung* ein Token erzeugen und den Agenten mit `ENROLLTOKEN=<Wert>` installieren; beim ersten Abgleich tauscht das Gerät das Token gegen einen dauerhaften Schlüssel. Der Weg ist **experimentell**, für Pilotinstallationen und Einzelgeräte gedacht und liefert nur **MSIX-Pakete im Benutzerkontext** (kein App-V, kein App Attach, keine maschinenweite Installation); den Zugriff auf die Paketfreigabe stellt eine ZeroPortal-Richtlinie mit SMB-Zugangsdaten her. Details: *ZeroPortal mit API-Key*.

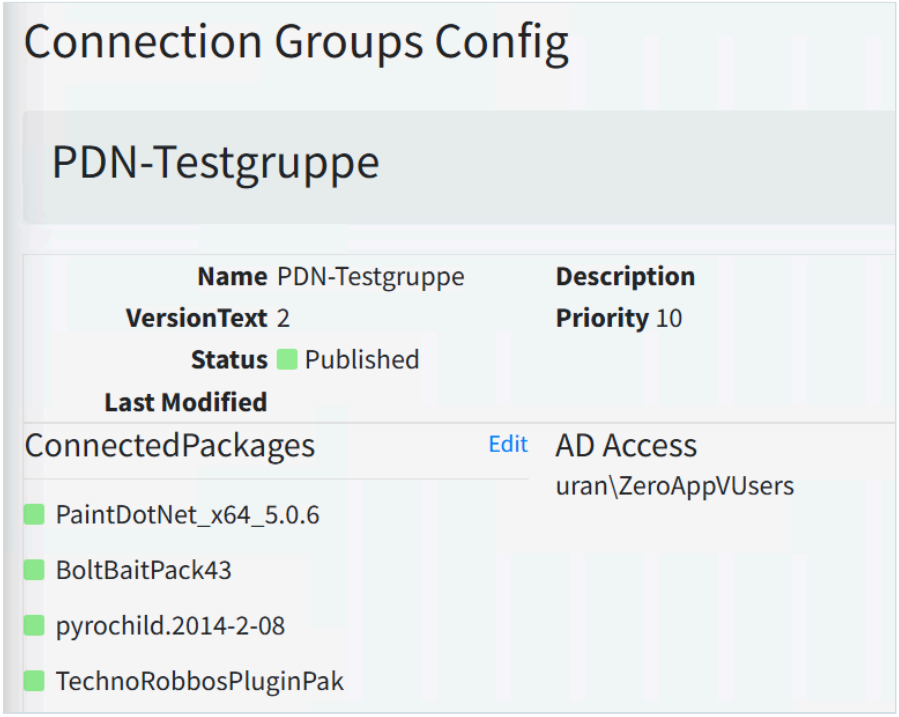
Alle Schalter, Cmdlets, Ereignis-IDs und den Registry-Aufbau des Agenten beschreibt *Client-Agent: Betrieb und Rollout*.

8. App-V-Pakete verteilen

1. **Paket bereitstellen:** Den Paketordner (`.appv`, `.xml`-Konfigurationen) in die App-V-Freigabe kopieren, dann unter *App-V → Pakete* auf **Pakete hinzufügen oder aktualisieren** klicken und das Paket im Repository auswählen. Das Portal durchsucht die Freigabe nicht von selbst.
2. **Zuweisen:** Paket öffnen und unter *Zugriff* die **AD-Gruppen** eintragen. Eine Gruppe mit Computerkonten liefert maschinenweit aus, eine Gruppe mit Benutzern im Profil des jeweiligen Benutzers.
3. **Veröffentlichen:** Paket auf *Veröffentlicht* setzen. Beim nächsten Abgleich holen die Clients das Paket; über das Tray-Symbol sofort.



4. **Verbindungsgruppen** (*App-V → Verbindungsgruppen*): Mehrere Pakete in einer gemeinsamen Umgebung ausführen, z. B. Anwendung plus Plugin. Zuweisung wie bei Paketen.



5. **Zurückziehen:** Veröffentlichung aufheben oder Zuweisung entfernen. Die maschinenweite Veröffentlichung nimmt der Agent sofort zurück; vollständig entfernt wird das Paket erst, wenn jeder Benutzer es beim nächsten Abgleich oder der nächsten Anmeldung freigegeben hat.

Den Microsoft-App-V-Client anbinden

Nutzen Sie App-V ohne den ZeroPortal-Agenten, tritt das Portal an die Stelle des App-V-Publishing-Servers. Zwei Adressen brauchen Sie dafür, beide auf Ihrem Portal:

Zweck	Adresse
Veröffentlichung	`https://<portal>:<port>/AppVPublishing`
Reporting	`https://<portal>:<port>/AppVReportReceiver`

Per Gruppenrichtlinie (der übliche Weg): *Computerkonfiguration → Administrative Vorlagen → System → App-V*. Unter *Publishing* tragen Sie bei *Publishing Server 1* die Veröffentlichungsadresse ein und schalten die Aktualisierung beim Anmelden für Computer und Benutzer an. Unter *Reporting* aktivieren Sie die Berichte und tragen die Reporting-Adresse ein. Unter *Streaming* entscheiden Sie über den Shared Content Store (siehe unten).

Per PowerShell auf dem Client, gleichwertig und gut für Tests:

```
Add-AppvPublishingServer -Name ZeroPortal -URL 'https://portal.firma.local:8080/AppVPublishing' `
    -GlobalRefreshEnabled $true  -GlobalRefreshOnLogon $true `
    -UserRefreshEnabled   $true  -UserRefreshOnLogon   $true
Set-AppvClientConfiguration -ReportingEnabled 1 `
    -ReportingServerURL 'https://portal.firma.local:8080/AppVReportReceiver'
Sync-AppvPublishingServer -ServerId 1
```

Ob Berichte ankommen, sehen Sie unter *Berichte* im Portal; einen Bericht sofort schicken können Sie mit `Send-AppvClientReport -URL '<Reporting-Adresse>' -DeleteOnSuccess:$false`.

Streaming: Shared Content Store oder vollständig laden?

Umgebung	Empfehlung
Terminalserver und VDI	**Shared Content Store** (`Set-AppvClientConfiguration -SharedContentStoreMode 1`). Die Pakete bleiben auf der Freigabe, auf dem Host liegt nichts. Voraussetzung ist eine schnelle, immer erreichbare Freigabe.
Arbeitsplätze und Notebooks	**Vollständig laden.** Ohne Shared Content Store lädt der Client das Paket beim ersten Start nach; mit `Mount-AppvClientPackage` holen Sie es vorab, dann startet die Anwendung auch offline.

> **Nur ein Weg je Gerät.** Holt der Microsoft-Client die Pakete selbst, bleibt im ZeroPortal-Agenten *Sync App-V einschalten* aus, und umgekehrt. Beides zusammen führt dazu, dass sich die zwei Wege gegenseitig die Pakete entziehen (Kapitel 7).

Der ZeroPortal-Agent statt des Microsoft-Clients: Dann tragen Sie im Microsoft-Client nichts ein. Die Portal-Adresse kommt aus der ADMX-Vorlage des Agenten, das Reporting läuft über den App-V-Client weiter und wird ebenfalls per Gruppenrichtlinie eingeschaltet. Alle Agenteneinstellungen finden Sie in Kapitel 7.

Versionswechsel: Für App-V gibt es keine Versionssperre. Die im Portal veröffentlichte Version wird auf dem Client hergestellt, auch wenn dort eine neuere liegt. Ein Wechsel zurück auf eine ältere Version ist also durch Veröffentlichen der älteren Version möglich.

Reporting: Die Berichtsdaten des App-V-Clients (Anwendungsnutzung, Paketstand je Gerät und Benutzer) sammelt das Portal unter *Berichte* (Kapitel 12).

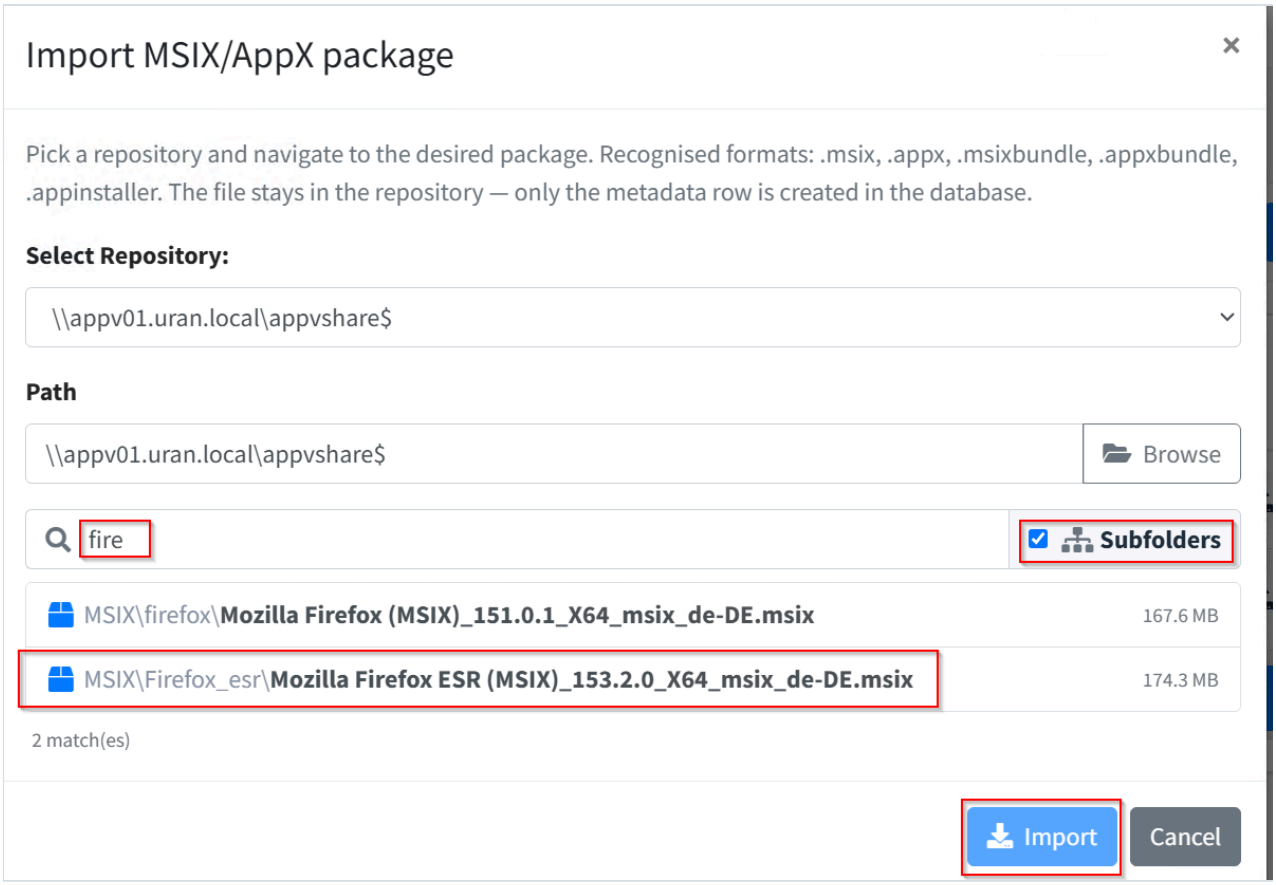
9. MSIX-Pakete verteilen

Voraussetzungen

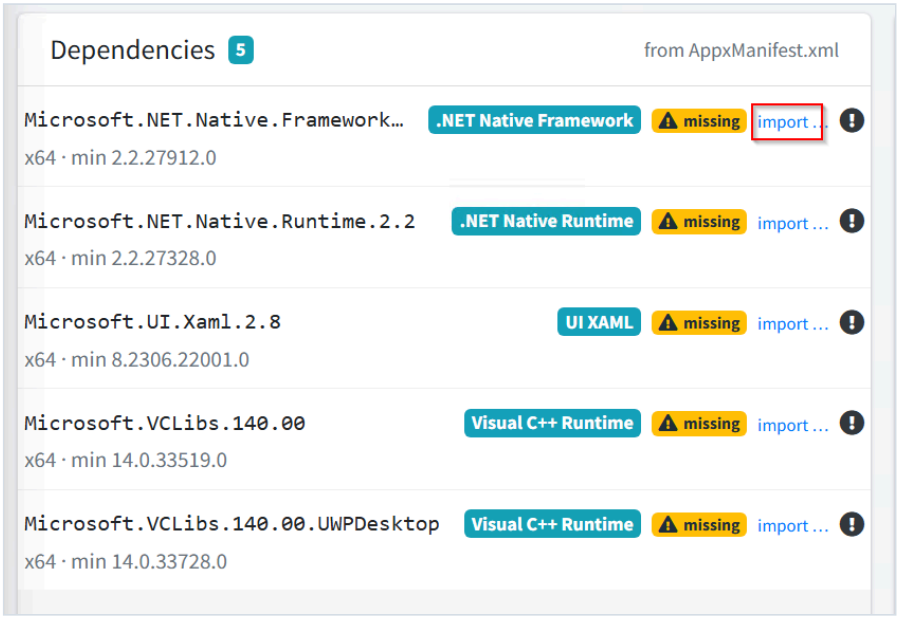
- In der Gruppenrichtlinie ist *Sync MSIX einschalten* aktiv (Kapitel 7).
- Das **Signaturzertifikat** des Pakets ist auf den Clients vertrauenswürdig: bei eigenen Paketen per GPO in *Vertrauenswürdige Personen* oder *Vertrauenswürdige Stammzertifizierungsstellen* verteilen. Clients ohne Internetzugang brauchen zusätzlich die Zwischen- und Stammzertifikate der Kette (*Bekannte Fehlerbilder*).
- Die Clients lesen die Paketfreigabe als Computerkonto (maschinenweite Installation) und als Benutzer. Für Außenstellen zeigt *Paketquellen-Stammpfad überschreiben* auf eine lokale Freigabe oder DFS; fehlt ein Paket dort, nimmt der Agent die zentrale Quelle.

Paket importieren und zuweisen

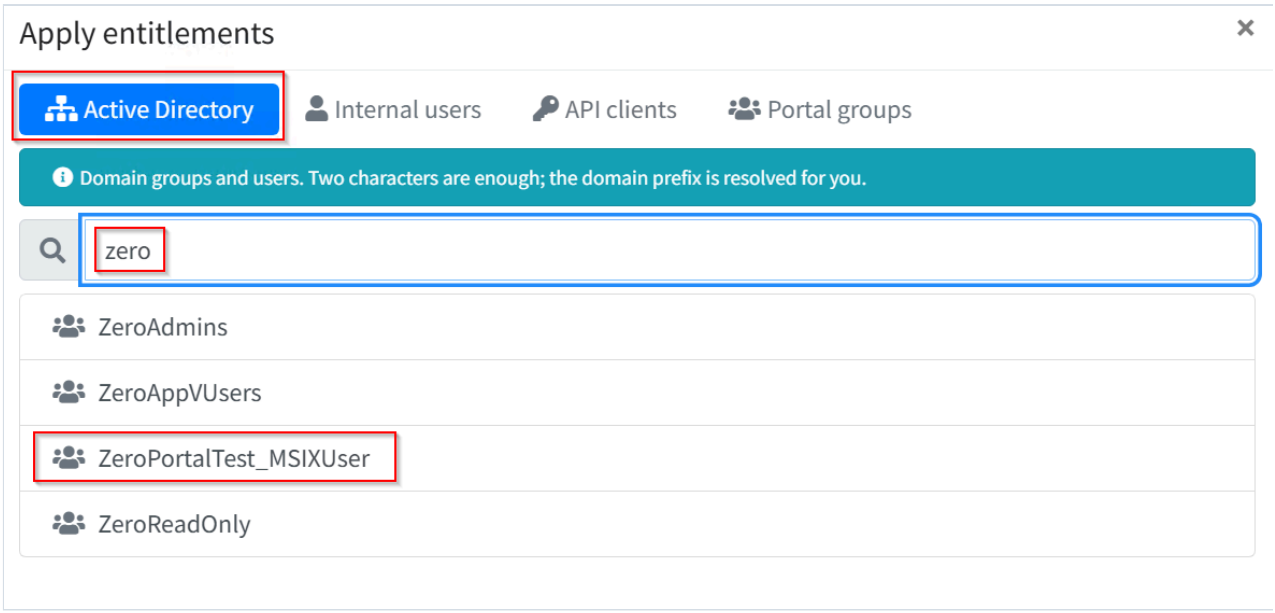
1. **Import** (*MSIX → Pakete → Import*): `.msix`, `.msixbundle`, `.appx` oder `.appxbundle` aus dem Repository wählen. Das Portal liest Name, Version, Architektur und Abhängigkeiten.

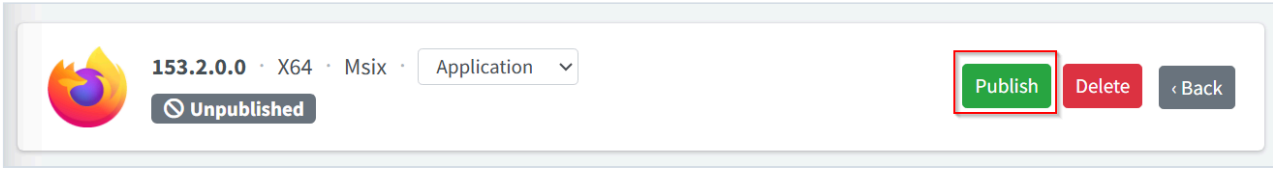


2. **Frameworks (Abhängigkeiten):** Fehlende Frameworks (`Microsoft.VCLibs`, `Microsoft.UI.Xaml`, …) zeigt die Paketseite an. *Import* sucht zuerst im Paketordner; sonst öffnet sich der Repository-Browser mit dem Framework-Namen vorbelegt. Frameworks liegen einmal im Repository und werden von allen Paketen gemeinsam genutzt.



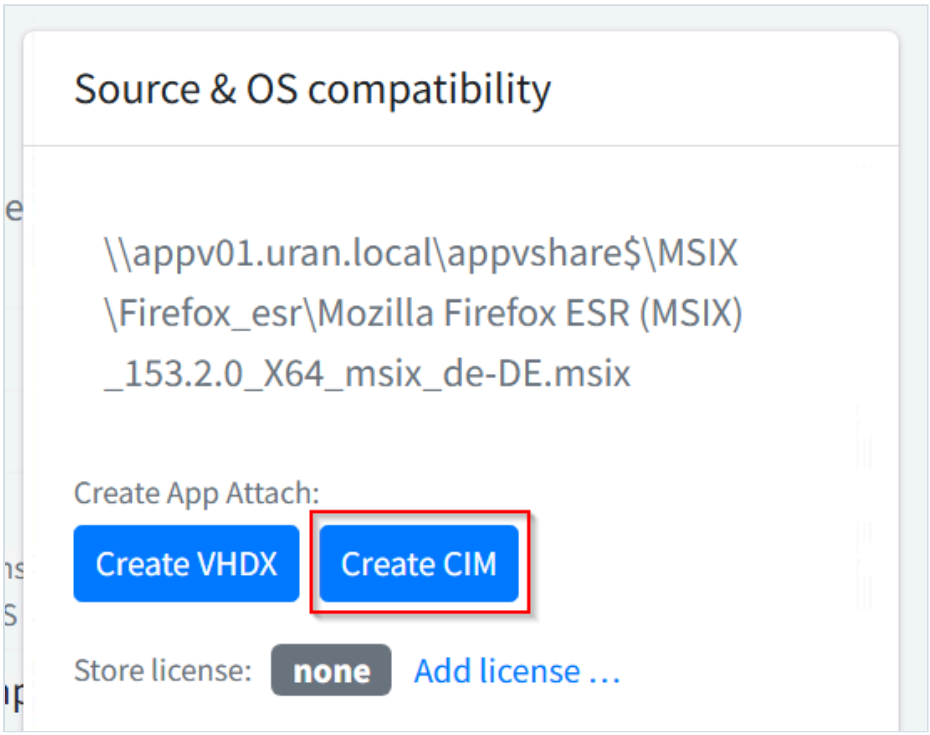
3. **Zuweisen und veröffentlichen:** In der Karte *AD-Berechtigungen* die Empfänger wählen: AD-Gruppen und einzelne AD-Konten, Portalgruppen, interne Konten sowie Geräte und Benutzer aus dem Enrollment. Computerzuweisungen installieren maschinenweit; jede Benutzeranmeldung registriert das Paket im Profil.





Bereitstellungsform: MSIX oder App Attach

Standard ist die klassische MSIX-Installation vom Repository. Alternativ wird ein Paket als **App Attach** (VHDX oder CIM) von der Freigabe eingehängt statt kopiert, was auf Terminalservern Platz und Zeit spart. Die Form legt die Richtlinie **MSIX-Bereitstellung** fest (Kapitel 10); das Portal erzeugt die Images auf Wunsch selbst (*MSIX → Paket → App Attach*).



Ältere Version verteilen (Downgrade)

Windows lehnt die Installation einer älteren MSIX-Version über eine neuere ab; der Agent versucht ein Downgrade nur, wenn es ausdrücklich erlaubt ist. **Standard:** verboten. Liegt auf dem Client eine neuere Version, gilt das Paket als erfüllt, ohne Fehlermeldung, auch bei reinem Formatwechsel (MSIX oder App Attach). **Empfehlung:** Downgrades je Paketfamilie über die Richtlinie **Paket-Downgrade-Steuerung** erlauben (Vorbelegung: alles verbieten); der Agentschalter `MSIX/AllowDowngrade` erlaubt pauschal, eine Richtlinienregel hat Vorrang.

Ein erlaubtes Downgrade entfernt zuerst die neuere Version und installiert dann die ältere; Nutzerdaten außerhalb des Pakets bleiben erhalten. **Frameworks werden nie zurückgestuft.** Läuft die Anwendung gerade, wird das Paket mit Grund im Agent-Log übersprungen und beim nächsten Abgleich erneut versucht; nur für einen Formatwechsel beendet der Agent die Anwendung (`MSIX/TerminateAppsForFormatSwitch`, Standard ein). Verlangt die ältere Version ältere Frameworks, die der Client nicht mehr hat, startet sie nicht: Downgrades vorher auf einem Testgerät prüfen.

Zurückziehen und Frameworks

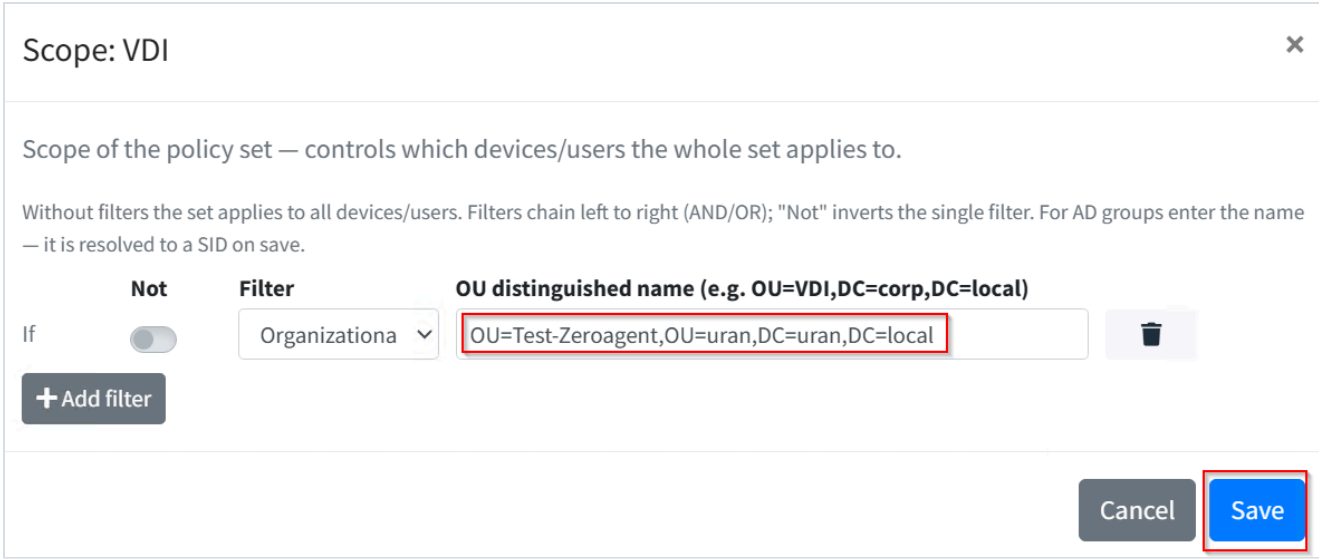
Beim Aufheben einer Veröffentlichung entfernt der Agent zuerst die Anwendungen, dann die Frameworks. Ein Framework bleibt ohne Fehlermeldung stehen, solange ein anderes Paket es benutzt (auch eines, das nicht aus dem Portal stammt); der nächste Abgleich prüft erneut. Frameworks, die der Microsoft Store aktualisiert hat, werden nicht angefasst.

10. Richtlinien

Richtlinien steuern Einstellungen auf den Geräten zentral aus dem Portal, unabhängig von der AD-Struktur. Der Agent holt sie beim Abgleich, wendet sie **vor** der Paketverarbeitung an und nimmt sie zurück, sobald ein Gerät oder Benutzer nicht mehr im Geltungsbereich liegt.

- **Richtliniensatz:** Behälter mit Priorität und einem Geltungsbereich (Filter), der für alle enthaltenen Richtlinien gilt.
- **Richtlinie:** Eine Einstellungsgruppe eines Typs (Registrierung, Laufwerke, Drucker, Skripte, Desktop, Agent-Konfiguration, MSIX-Bereitstellung, …), auf Wunsch mit eigenen Filtern.
- **Filter:** AD-Gruppe, OU (mit allen untergeordneten OUs), Computername (`*`, `?`), IP-Bereich, Umgebungsvariable, Betriebssystem, Sitzungstyp, Zeitfenster, Registrierungswert, Datei oder Ordner; mit UND/ODER verknüpft, einzeln negierbar.

Der Agent verarbeitet Computeranteile (Bereitstellungsregeln, Agent-Konfiguration, HKLM, Dienste) im Computer-Abgleich und Benutzeranteile (Laufwerke, Drucker, Desktop, HKCU) im Benutzer-Abgleich. Ein Satz, der auf Computer zielt (Computername, IP-Bereich, OU), bringt jedem Benutzer, der sich dort anmeldet, auch die Benutzeranteile mit (wie die Loopback-Verarbeitung von Gruppenrichtlinien); das ist der Normalfall für VDI und Terminalserver. Ein Satz, der nur auf Benutzer zielt (Benutzergruppe, Benutzer-OU), trägt keine Computeranteile; eine Computergruppe als einziger Filter nur die Computeranteile.



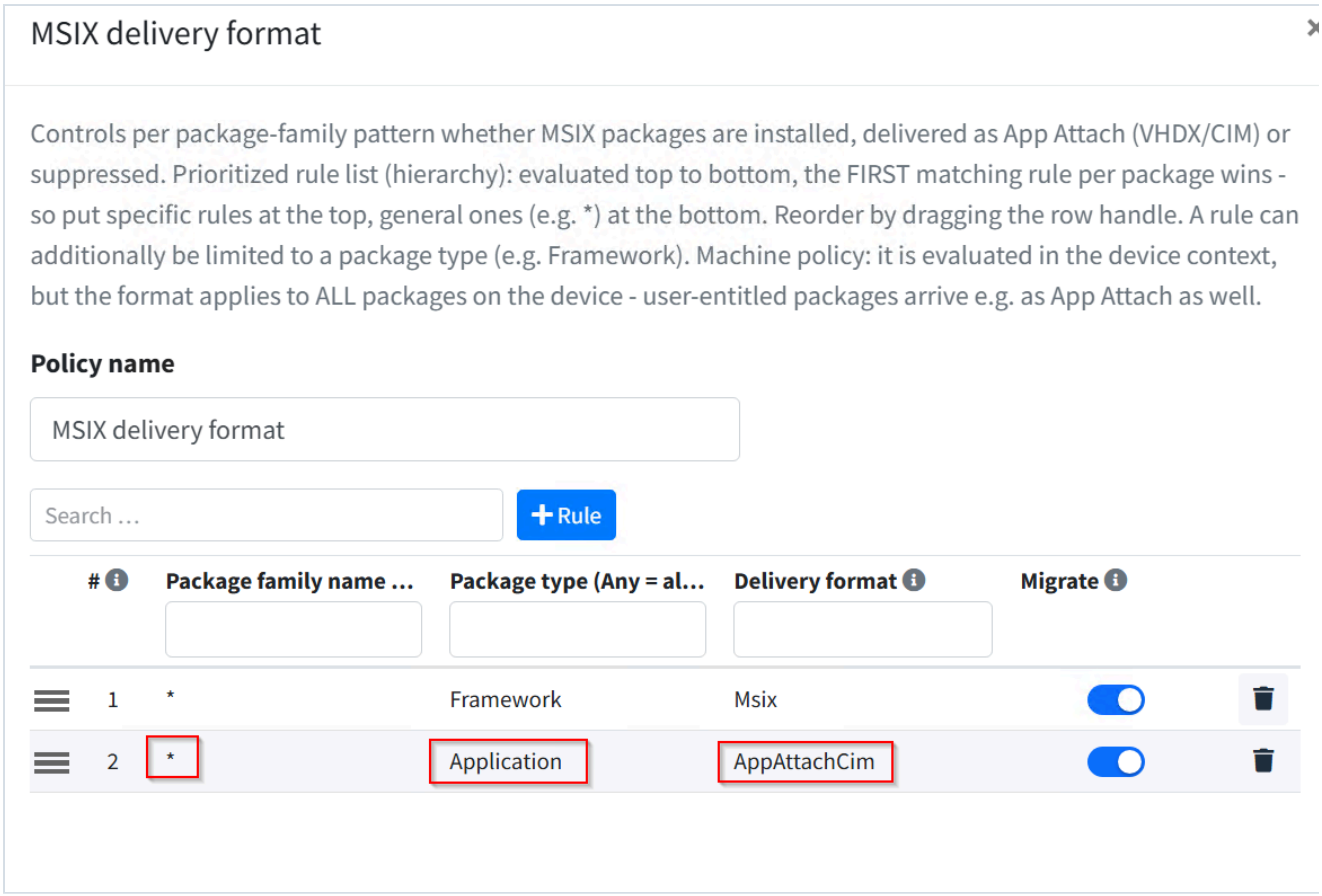
Richtliniensatz anlegen

1. *Richtlinien → Richtliniensatz anlegen*, Priorität und Geltungsbereich festlegen.
2. Im Satz *Richtlinie hinzufügen* und den Typ wählen. Listentypen bekommen neue Zeilen über **Eintrag hinzufügen**; bei Paketfamilien filtert die Liste beim Tippen.
3. Speichern. Jede Änderung erhöht die Revision der Richtlinie; die Historie lesen und einen früheren Stand zurückholen geht per PowerShell (`Get-ZeroPortalPolicyHistory`, `Restore-ZeroPortalPolicy`).

Widersprechen sich zwei Einstellungen, gewinnt der erste Treffer: zuerst nach Priorität des Richtliniensatzes, dann nach Priorität der Richtlinie im Satz; die kleinere Zahl gewinnt.

Bereitstellungsregeln für MSIX und App Attach

Die Richtlinie **MSIX-Bereitstellung** legt je Paketfamilie fest, ob ein Paket als `Msix` (Standard ohne Regel), als `AppAttachVhdx` oder `AppAttachCim` (Image von der Freigabe einhängen, z. B. für Terminalserver und AVD) oder gar nicht (`Deny`) ausgeliefert wird. Jede Regel: Muster auf den Familiennamen (`LibreOffice*`), optional Pakettyp, Format. Die Liste wird von oben nach unten ausgewertet, die erste passende Regel gewinnt; spezifische Regeln nach oben, die `*`-Regel nach unten. Es ist eine Maschinenrichtlinie und gilt auch für benutzerzugewiesene Pakete. Eine neue Richtlinie enthält bereits `*` / Framework → Msix, weil Frameworks immer als MSIX kommen.



Typischer Terminalserver-Satz: `Contoso.Legacy_*` → Deny, `*` / Framework → Msix, `*` → AppAttachCim. Arbeitsplätze ohne eigene Regel erhalten weiterhin klassisches MSIX.

Vorlagen, Felder und welcher Filter in welchem Abgleich greift: *Richtlinien und Vorlagen*.

11. Hochverfügbarkeit

Ein zweiter Portal-Knoten mit replizierter Datenbank hält den Abgleich bei Ausfall oder Wartung eines Servers am Laufen. Der **Primary** schreibt die Datenbank; alle Änderungen im Portal und alle Lizenzbuchungen laufen hier. Die **Replica** liest per MariaDB-Replikation mit; Clients gleichen hier ab, die Weboberfläche ist bedienbar, und Schreibvorgänge leitet der Knoten an den Primary weiter. Mit zufälliger Serverauswahl in der Gruppenrichtlinie des Agenten verteilen sich die Abgleiche auf beide Knoten. Der Primary prüft die anderen Knoten alle 10 Sekunden, jede Replica meldet sich alle 5 Minuten (einstellbar). Den Zustand zeigt *Globale Konfiguration → Hochverfügbarkeit*.

Einrichtung

1. Den zweiten Server wie in Kapitel 3 installieren.
2. Auf **beiden Knoten** im Konfigurationstool, Schritt *Base Configuration*, dasselbe **Replikationspasswort** eintragen; dort steht auch der Pfad zu den MariaDB-Programmdateien, den der Assistent braucht.
3. Den zweiten Knoten dem Cluster beitreten lassen (Adresse des Primary eintragen). Enthält der Primary bereits Daten, vorher einen vollständigen Abgleich der Datenbank durchführen (*Hochverfügbarkeit einrichten*).

4. Auf dem **zweiten Knoten** unter *Globale Konfiguration → Hochverfügbarkeit* den **Replikations-Assistenten**, Registerkarte *Replica*, ausführen: eindeutige Server-ID für beide Knoten, Host und Port des Primary.
5. Auf derselben Seite prüfen: beide Knoten grün, Replikationsverzögerung 0.

Clients auf beide Server verweisen

In der Gruppenrichtlinie *Publishing-Server* beide URLs eintragen, die Reihenfolge ist die Priorität; ohne Gruppenrichtlinie lokal mit `Add-ZPAgentPublishingServer`. Ist der erste Server nicht erreichbar, wechselt der Agent nach 10 Sekunden zum nächsten und meidet den ausgefallenen für 10 Minuten; das gilt für Pakete, App-V und Richtlinien gleichermaßen. Ein Server, der antwortet, aber einen Fehler meldet, wird nicht gesperrt, nur übersprungen.

Update im Cluster

1. **Primary zuerst** aktualisieren: MSI installieren, danach das Datenbankupdate mit `ZDBInstallUpdate.exe` (Befehl in Kapitel 12).
2. Dann die **Replicas**, jeweils ebenfalls mit `ZDBInstallUpdate.exe`. Niemals eine Replica vor dem Primary migrieren.
3. Cluster-Seite prüfen.

Ausfallszenarien und die Wiederherstellung eines ausgefallenen Primary beschreibt der *Hochverfügbarkeit einrichten*.

12. Betrieb: Sicherung, Logs, Audit, Updates

Sicherung und Wiederherstellung

Unter *Globale Konfiguration → Konfiguration*, Abschnitt *Sicherung und Wiederherstellung* (nur Voll-Administratoren), erzeugt **Download Backup** eine XML-Datei mit der gesamten Portal-Konfiguration in fünf Bereichen, die sich beim Zurückspielen einzeln abwählen lassen: Portal-Konfiguration (Repositories, E-Mail und Benachrichtigungen, Proxy, Lizenzdateien), Benutzer, Gruppen und Berechtigungen (Portalgruppen, Stufen, interne Konten, Anmeldeanbieter, API-Clients), Richtlinien, MSIX-Katalog und App-V-Katalog (Pakete, Verbindungsgruppen, Zuweisungen). **Restore** liest die Datei ein: Vorhandene Einträge werden anhand ihrer Kennung aktualisiert, fehlende neu angelegt, hinterlegte Kennwörter nie überschrieben. Dieselbe Datei verarbeitet das PowerShell-Modul (`Export-ZeroPortalConfiguration`, `Import-ZeroPortalConfiguration`), etwa für tägliche Sicherungen per Aufgabe.

Nicht in der Sicherung: Passwörter, Geheimnisse und API-Client-Schlüssel; knotenspezifische Einstellungen (`appsettings.json`, LDAP-Verbindung, Knoten- und Clusteridentität); Verlaufsdaten (Audit, Richtlinienverlauf, Versandhistorie, App-V-Reporting); bekannte Geräte und Benutzer, Rollout-Token; die Paketdateien selbst. Ein vollständiges Wiederherstellungskonzept umfasst deshalb:

1. Konfigurationssicherung aus dem Portal (regelmäßig, z. B. täglich per PowerShell).
2. `C:\Program Files\ZeroPortal\appsettings.json` je Knoten.
3. `C:\ProgramData\ZeroPortal\DataProtection` je Knoten (Schlüssel für gespeicherte Kennwörter; ohne diesen Ordner müssen hinterlegte Kennwörter neu eingegeben werden).

4. MariaDB-Dump (`mariadb-dump`), wenn Reporting- und Audit-Daten erhalten bleiben sollen.
5. Die Paketfreigabe.

Logs

Was	Wo	Hinweis
Portal	`C:\ProgramData\NickIT\ZPServer\Logs` (ältere Installationen: `C:\Windows\Temp\ZeroPortalLogs`)	Standardstufe *Warning*: nur Start, Warnungen, Fehler
Agent (Gerät)	`C:\ProgramData\NickIT\ZeroPortalAgent\Logs\agent-<Datum>.log`	eine Datei je Tag
Agent (Benutzer)	`usersync-<Benutzer>-<Datum>.log` im selben Ordner bzw. unter `%LocalAppData%\NickIT\ZeroPortalAgent\Logs`	eine Datei je Tag und Benutzer

- **Portal-Log:** Start und Stopp des Dienstes, Datenbank- und Zertifikatsprobleme, Fehler bei Anfragen; wer im Portal was geändert hat, steht im Audit. Mit Stufe *Warning* bleibt es klein (wenige KB im Quartal); wächst es schneller, steht darin ein Fehler, oder die Stufe (`Logging:Console:LogLevel:Default` in `appsettings.json`) wurde nach einer Fehlersuche nicht zurückgestellt. Nach einer Änderung den Dienst neu starten.
- **Agent-Log:** Je Paketvorgang eine Zeile mit Ereignis-ID, Paketname, Ergebnis und bei Fehlern dem Windows-Fehlercode, dazu Entscheidungszeilen und eine Zusammenfassung je Abgleich. Standardstufe *Information*; für eine Fehlersuche per Gruppenrichtlinie *Protokollierungsstufe* oder `Set-ZPAgentConfiguration -LogLevel Debug` auf *Debug* und danach zurück. Der Agent schreibt nicht in das Windows-Ereignisprotokoll. Die Logs werden nicht automatisch gelöscht: Dateien älter als 30 Tage per Richtlinie *Skripte* oder geplanter Aufgabe löschen; `Clear-ZPAgentLog` löscht alle auf einmal.

Audit

Das Portal protokolliert, wer wann was geändert hat: Zuweisungen, Veröffentlichungen, Richtlinien, Berechtigungen, Sicherungen. Die Einträge stehen unter *Globale Konfiguration → Audit-Protokoll*; ein- und ausschalten sowie die Aufbewahrung in Tagen einstellen lässt sich das auf der Konfigurationsseite im gleichnamigen Abschnitt (0 = unbegrenzt, Obergrenze 3650 Tage). Wird das Audit abgeschaltet, wird genau das noch protokolliert und eine Warn-E-Mail verschickt.

Benachrichtigungen

Das Portal verschickt vierzehn verschiedene Meldungen, jede einzeln ein- und ausschaltbar und mit eigener Wiederholsperre, damit ein Dauerzustand nicht das Postfach flutet:

- **Betrieb:** Datenbank nicht erreichbar, Serverzertifikat läuft ab, Audit abgeschaltet.
- **Lizenzen:** Lizenz läuft ab, Kontingent überschritten.
- **Cluster:** Knoten ausgefallen und wieder erreichbar, Replikation gestoppt, Failover (dieser Knoten ist jetzt Primary), Primary nicht erreichbar und wieder erreichbar.
- **Sicherheit und Wartung:** API-Schlüssel von einem fremden Rechner benutzt, App-V-Reportingdaten werden groß, Agent hat eine wiederholte Korrektur unterdrückt.

Reporting (nur App-V)

Berichte zeigt die Daten des App-V-Reportings: welche Anwendungen auf welchen Geräten und von welchen Benutzern gestartet wurden und welcher Paketstand dort liegt. Einrichtung und Aufbewahrung unter *Berichte → Konfiguration*. Für MSIX gibt es kein Reporting; dort sind das Agent-Log und die Tray-Meldungen die Auskunftsquelle.

Update eines Einzelknotens

1. Sicherung ziehen (Abschnitt *Sicherung und Wiederherstellung*).
2. Neue Server-MSI über die bestehende Installation installieren.
3. Datenbankupdate ausführen. Ohne diesen Schritt startet der Dienst mit einer veralteten Datenbank und meldet das im Log: `"C:\Program Files\ZeroPortal\ZDBInstallUpdate.exe" "C:\Program Files\ZeroPortal\appsettings.json" --admin-user root --admin-password <Passwort>`
4. Dienst neu starten, Portal aufrufen, Version in der Fußzeile und das Portal-Log prüfen.
5. Neue Agent-MSI aus dem Download-Center per GPO oder Softwareverteiler an die Clients verteilen. Sie kann über die vorhandene Version installiert werden; bei einem großen Versionssprung ist es sicherer, die alte Version zu deinstallieren und die neue frisch zu installieren.

Unverändert bleiben `appsettings.json`, das Zertifikat, die Datenbank (abgesehen vom Schemaupdate) und die Pakete auf der Freigabe. Im Cluster gilt die Reihenfolge aus Kapitel 11.

MariaDB aktualisieren

Das Portal kennt MariaDB über `MySqlSettings.BinPath` (Programmdateien, für Dump, Sicherung und den vollständigen Abgleich eines Replicas) und `MySqlSettings.DataPath` in der `appsettings.json`; der Portalstart prüft nur die Mindestversion.

Patch innerhalb der Reihe (11.8.6 auf 11.8.9): Installer laufen lassen, er aktualisiert denselben Ordner. In ZeroPortal ist nichts zu tun.

Reihenwechsel (11.8 auf 12.3; auch 12.1 auf 12.2, weil jede 12.x eine eigene Reihe mit eigenem Programmordner ist), je Knoten; im Cluster zuerst die Replicas, zuletzt der Primary (ein Replica darf vorübergehend neuer sein als sein Primary, nie älter):

1. Sicherung ziehen (Abschnitt *Sicherung und Wiederherstellung*).
2. Installer der neuen Reihe starten und *Upgrade existing instance* wählen. Er lässt das Datenverzeichnis, wo es ist, hängt den Dienst an die neuen Programmdateien unter `MariaDB <Reihe>\bin`, führt `mariadb-upgrade` aus und entfernt die alte Reihe.
3. Prüfen, dass der Dienst läuft und das Portal startet (`DB version OK` im Portal-Log).
4. Konfigurationstool starten, auf der Datenbankseite **Auto-detect** klicken, prüfen, dass `BinPath` auf `…\MariaDB <Reihe>\bin` zeigt, und speichern. Das Tool übernimmt den alten Pfad nicht von selbst.
5. Replikation, Heartbeat und Failover laufen ohne weitere Änderung weiter: Alles, was die Replikation braucht, steht in der my.ini im Datenverzeichnis, und das bleibt, wo es war.

Danach finden die my.ini-Funktionen des Replikationsassistenten die Datei nicht mehr, weil sie unter `…\MariaDB <neue Reihe>\data` suchen. Änderungen an der my.ini von Hand vornehmen oder das Datenverzeichnis samt `--defaults-file` im Dienstaufruf in den neuen Ordner verschieben.

Deinstallation

Server: Die Deinstallation über *Apps & Features* entfernt die Programmdateien unter `C:\Program Files\ZeroPortal`. Erhalten bleiben das Datenverzeichnis `C:\ProgramData\NickIT\ZPServer` mit den Logs, die MariaDB-Datenbank (MariaDB ist eine eigene Installation) und die Paketfreigabe.

Client: Die Agent-MSI über *Apps & Features* oder `msiexec /x` deinstallieren. Der Agent entfernt beim Deinstallieren keine Pakete; installierte App-V- und MSIX-Pakete bleiben auf dem Gerät. Sollen sie verschwinden, vorher die Veröffentlichung im Portal aufheben und einen Abgleich abwarten.

13. Notfälle und Fehlersuche

Niemand kommt mehr ins Portal

Bei **jedem Start** prüft der Dienst, ob die in der `appsettings.json` unter `AccessGroups:FullAdmins` eingetragene AD-Gruppe und das optionale Notfallkonto `RootUser` Vollrechte besitzen, und legt nur Fehlendes neu an (Portalgruppe *Portal administrators*, Mitgliedschaft, Berechtigung auf alle Bereiche); der Vorgang steht als Warnung im Portal-Log.

1. **Anmeldung oder Berechtigung?** Eine wiederholte Passwortabfrage ist ein Anmeldeproblem, meist die fehlende Intranetzone oder ein fehlender SPN für einen Aliasnamen (Kapitel 3). Die Meldung „kein Zugriff" heißt: angemeldet, aber nicht berechtigt.
2. **Gruppe prüfen:** Steht unter `AccessGroups:FullAdmins` die richtige AD-Gruppe, und sind Sie darin Mitglied? Dieser Eintrag gilt immer.
3. **Dienst neu starten.** Danach haben die Mitglieder der Gruppe wieder alle Rechte. Ist weder Gruppe noch Notfallkonto konfiguriert, repariert der Dienst nichts und schreibt einen Fehler ins Log: einen der beiden Werte eintragen und neu starten.
4. **Notfallkonto:** Ist ein `RootUser` eingerichtet, melden Sie sich damit an.

Nach der Rettung die Rechte wieder an einer Portalgruppe verankern, nicht an einer einzelnen Person.

Der Primary fällt aus (Cluster)

- Die **Paketverteilung läuft auf den Replicas weiter**, weil Lesen immer lokal geschieht. Verwaltung, Enrollment und Lizenzbuchungen warten; auf jeder Seite erscheint der Balken „Kein Primary erreichbar", und die Replica verschickt eine E-Mail.
- Kehrt der Primary zurück, holt der Cluster von selbst auf, in der Regel innerhalb einer Minute. Kommt er nicht zurück, auf der HA-Seite der Replica **Promote to Primary** ausführen.
- Eine Replica, die länger als sieben Tage fehlt oder aus einem Snapshot zurückgesetzt wird, braucht einen vollständigen Datenbankabgleich (*Hochverfügbarkeit einrichten*).

Weitere Notfälle

Fall	Vorgehen
Serverzertifikat abgelaufen	Konfigurationstool, Schritt *Certificate*, neues Zertifikat wählen, *Save & Restart Service*. Das Portal warnt vorher per E-Mail.

Fall	Vorgehen
Signaturzertifikat eines MSIX-Pakets abgelaufen	Mit Zeitstempel in der Signatur kein Problem, das Paket installiert sich weiter. Ohne Zeitstempel muss es neu signiert und erneut importiert werden. Die Paketseite zeigt, ob ein Zeitstempel vorhanden ist. Bereits installierte Pakete laufen weiter.
Konfiguration versehentlich zerstört	Sicherung zurückspielen (Kapitel 12). Hinterlegte Kennwörter bleiben dabei unverändert.
Datenbank verloren	MariaDB-Dump einspielen, danach die Konfigurationssicherung. Ohne Dump gehen Audit- und Reportingdaten verloren, die Konfiguration nicht.
Agent auf einem Client defekt	Agent deinstallieren und neu installieren (Kapitel 7). Installierte Pakete bleiben erhalten, der nächste Abgleich stellt den Sollzustand her.
Ein Paket verteilt sich fehlerhaft an viele Geräte	Veröffentlichung im Portal aufheben. Die Clients ziehen es beim nächsten Abgleich zurück. Soll es nur pausiert werden, stattdessen die Zuweisung entfernen.

Häufige Symptome

Symptom	Ursache und Lösung
Anmeldefenster beim Aufruf des Portals	Portal-URL nicht in der Intranetzone oder Aliasname ohne SPN (Kapitel 3). Fehlende Berechtigung wäre eine Fehlerseite, kein Anmeldefenster.
„Kein Zugriff" trotz Gruppenmitgliedschaft	Gruppe nicht in einer Portalgruppe oder Stufe *Kein Zugriff*. Neues Kerberos-Ticket nach Gruppenänderung: ab- und anmelden.
Portal startet nicht	`C:\ProgramData\NickIT\ZPServer\Logs\ZeroPortalLogs.log` lesen. Häufig: MariaDB nicht gestartet, Zertifikat abgelaufen, Datenbankupdate nach MSI-Update vergessen.
Paket kommt nicht auf dem Client an	Auf dem Client `Get-ZPAgentSync`: Ist MSIX bzw. App-V eingeschaltet? Nach der Installation sind alle drei Bereiche aus (Kapitel 7). Dann `Get-ZPAgentStatus` und `Sync-ZPAgentPublishingServer`, Zuweisung und Veröffentlichung im Portal prüfen, danach das Agent-Log des Tages.
Pakete fehlen einzelnen Benutzern	Berechtigung im Portal prüfen; neue AD-Gruppen wirken erst mit neuem Kerberos-Ticket (ADMX-Einstellung *Kerberos-Tickets des Benutzers vor dem Benutzer-Sync löschen*).
Tray meldet „failed"	Hinweisfenster anklicken: Es öffnet den Log-Ordner. Die Fehlerzeile nennt Paket, Fehlercode und Ursache.
MSIX-Fehler 0x800B0109	Signaturzertifikat auf dem Client nicht vertrauenswürdig (Kapitel 9).
MSIX-Fehler 0x80073D06	Downgrade von Windows abgelehnt. Downgrade per Richtlinie erlauben oder neuere Version veröffentlichen.
MSIX-Fehler 0x80073D02 beim Entfernen	Framework wird noch von einem anderen Paket benutzt. Kein Handlungsbedarf; es bleibt, bis es unbenutzt ist.
MSIX-Fehler 0x80073CF3 beim Installieren	Eine benötigte Abhängigkeit fehlt oder ist zu alt. Das passende Framework importieren und zuweisen (Kapitel 9).
App-V-Paket fehlt im Startmenü	Paket im Benutzerkontext prüfen (`Get-AppvClientPackage`). Der Verknüpfungs-Aufräumer ist standardmäßig aus; falls eingeschaltet, prüfen, ob er greift.

Symptom	Ursache und Lösung
App-V-Anwendung startet beim ersten Mal sehr langsam, Ladebalken bis 100 %	Das Paket streamt komplett, weil beim Sequenzieren kein Primary Feature Block aufgezeichnet wurde. Neu sequenzieren oder Shared Content Store einschalten. Virenscanner-Ausnahmen ändern daran nichts.
App Attach hängt nicht ein	Freigabe vom Client aus als Computerkonto lesbar? Image-Datei im Repository vorhanden? Agent-Log zeigt Pfad und Fehlercode.
Client-Zertifikatswarnung	Serverzertifikat nicht in der Vertrauenskette des Clients. Zertifikat per GPO verteilen; `TRUSTCERT=1` nur für Tests.
Lizenzseite zeigt Überschreitung	Zählung der letzten 90 Tage; ausgemusterte Geräte fallen nach 90 Tagen heraus. Lizenzdatei nachladen oder Modus prüfen.
Replica zeigt Verzögerung	MariaDB-Replikation prüfen (*Cluster*-Seite, `SHOW REPLICA STATUS`). Nach Netzunterbrechung holt sie in der Regel selbst auf.

Für Fehlermeldungen an den Hersteller: Portal-Version (Fußzeile), Agent-Version (`Get-ZPAgentStatus`), das Agent-Log des Tages und die betroffene Zeile aus dem Portal-Log.

14. Referenz

Pfade und Ports

	Wert
Portal-Installation	`C:\Program Files\ZeroPortal`
Portal-Konfiguration	`C:\Program Files\ZeroPortal\appsettings.json`
Schlüssel für gespeicherte Kennwörter	`C:\ProgramData\ZeroPortal\DataProtection`
Portal-Log	`C:\ProgramData\NickIT\ZPServer\Logs` (ältere Installationen: `C:\Windows\Temp\ZeroPortalLogs`)
Datenbankupdate	`C:\Program Files\ZeroPortal\ZDBInstallUpdate.exe`
Konfigurationstool	`C:\Program Files\ZeroPortal\ZeroPortalConfigTool.ps1`
Agent-Installation	`C:\Program Files\NickIT\ZeroPortalAgent`
Gruppenrichtlinienvorlage (ADMX)	`C:\Program Files\NickIT\ZeroPortalAgent\admx`
Agent-Logs	`C:\ProgramData\NickIT\ZeroPortalAgent\Logs`
Portal-Port	im Konfigurationstool festgelegt (HTTPS), z. B. 8080; Firewallregel `ZeroPortal Inbound <Port>`
MariaDB	3306, im Cluster zwischen den Knoten offen (Regel vom Replikations-Assistenten)

	Wert
Clients und Portal → Freigabe	SMB 445
Agent eingehend	kein Port; der Agent verbindet nur ausgehend
Alle Ports im Überblick	Kapitel 3, Abschnitt *Firewall und Ports*

Agentschalter (Auswahl)

Per Gruppenrichtlinie (ADMX, Kapitel 7), per ZeroPortal-Richtlinie *Agent-Konfiguration* oder lokal mit `Set-ZPAgentConfiguration -<Schalter> <Wert>`; die Gruppenrichtlinie hat Vorrang. Alle Schalter mit Erläuterung: *Client-Agent: Betrieb und Rollout*.

Schalter	Standard	Bedeutung
`MSIX/SyncIntervalMinutes`	60	Abstand des periodischen Abgleichs
`Agent/SyncJitterMinutes`	10	Zufällige Verzögerung 0 bis n Minuten
`Agent/ServerFailover`	an	Ein Server je Abgleich, bei Nichterreichbarkeit der nächste; aus = alle Server abarbeiten (unabhängige Portale)
`Agent/FailoverTimeoutSeconds`	10	Wartezeit je Server bis zum Wechsel; bei stark ausgelasteten Servern höher setzen, sonst gilt ein langsamer Server als tot
`Agent/ServerBlacklistMinutes`	10	Wie lange ein ausgefallener Server gemieden wird
`Agent/PurgeUserTicketsBeforeSync`	aus	Vor jedem Benutzer-Sync `klist purge`, damit neue Gruppenmitgliedschaften sofort wirken
`Agent/LogLevel`	Information	Protokollierungsstufe des Agenten (None bis Debug)
`MSIX/AllowDowngrade`	aus	Downgrade pauschal erlauben; Richtlinie hat Vorrang
`MSIX/DeferRemovalWhileInUse`	an	Entfernen aufschieben, solange die Anwendung läuft; spätestens nach `MSIX/RemovalIdleTimeoutHours` (24)
`MSIX/TerminateAppsForFormatSwitch`	an	Laufende Anwendung für einen Formatwechsel MSIX/App Attach beenden; aus = Wechsel verschieben, solange sie läuft

Wichtige Ereignisse im Agent-Log

ID	Bedeutung
2507	Framework wird im Gerätekontext noch gebraucht und bleibt installiert
2516	Dasselbe im Benutzerkontext
2538	Downgrade nicht erlaubt, Paket gilt als erfüllt; dieselbe ID meldet auch die Umstellung einer Benutzerregistrierung auf App Attach
3620	App Attach angefordert, aber kein erreichbares Image im gewünschten Format; Rückfall auf MSIX
4000	Startfehler des Dienstes mit vollständiger Fehlerursache

ID	Bedeutung
4501	Bereitstellung eines Pakets im Gerätekontext fehlgeschlagen (mit Fehlercode und Meldung)
4502	Rücknahme eines Pakets im Gerätekontext fehlgeschlagen
4512	Entfernen im Benutzerkontext fehlgeschlagen
4531	Einhängen eines App-Attach-Images fehlgeschlagen, Rückfall auf MSIX

Weiterführende Dokumente

Thema	Dokument
Erste Einrichtung Schritt für Schritt mit Bildschirmfotos: GPO, Agent, App-V, MSIX, Richtlinien	*Quick-Admin-Guide*
Agent: Installation, Schalter, Tray, Registry	*Client-Agent: Betrieb und Rollout*
Berechtigungen, Enrollment, Lizenzen, Audit	*Benutzer, Rechte, Lizenzen und Protokolle*
MSIX, Frameworks, App Attach, Downgrade	*MSIX-Pakete verteilen*
Richtlinien: Aufbau, Vorlagen, PowerShell	*Richtlinien und Vorlagen*
Cluster einrichten und betreiben	*Hochverfügbarkeit einrichten*
Geräte ohne AD	*Geräte ohne Domäne (API-Key)*
Anmeldeprobleme, langsame MSIX-Installation ohne Internet	*Bekannte Fehlerbilder*