

# Active-Directory

- Active Directory Kennwort Änderung über Web-GUI
- Ordnerumleitung mit einer Gruppenrichtlinie konfigurieren

# Active Directory Kennwort Änderung über Web-GUI

## Einleitung

In diesem Beitrag erkläre ich kurz, wie wir es unseren Benutzern ermöglichen können, Ihr Kennwort über eine Weboberfläche zu ändern. Dies hat den entscheidenden Vorteil, dass die Benutzer dafür nicht zwangsweise am Rechner sein müssen. Sie können sich an jedem Endgerät befinden, der diesen Webserver erreichen kann.

## Kennwort Änderung ermöglichen

### Remotedesktop Web Access installieren

Im ersten Schritt müssen wir über den **Server-Manager** über die **Server-Rollen** den Serverdienst **Remotedesktopdienste** installieren. Im nächsten Schritt können wir die **Features** so lassen, wie diese eingestellt sind. Wir benötigen da keine weiteren Features.

Jetzt bei den **Rollendiensten** müssen wir den **Web Access für Remotedesktop** auswählen und dann das "Setup" weiter fortführen. Bei den folgenden Fenstern klicken wir diese durch, wie wir es aus anderen **Server-Rollen Installationen** kennen.

### DNS Eintrag für Webserver hinzufügen

Jetzt müssen wir auf unserem **DNS-Server** einen CNAME Eintrag erstellen. Dieser dient dazu, dass wir unsere Webseite nachher über eine "Domain" erreichen können. Falls wir unseren Server von Außen erreichbar machen möchten, müssen wir bei den öffentlichen DNS Anbietern, die Subdomain hinzufügen. Da wir aus Sicherheitsgründen die Seite nur aus dem **internen Netzwerk** erreichbar machen wollen, tragen wir einen **CNAME Eintrag** bei unserem lokalen **DNS-Server** ein.

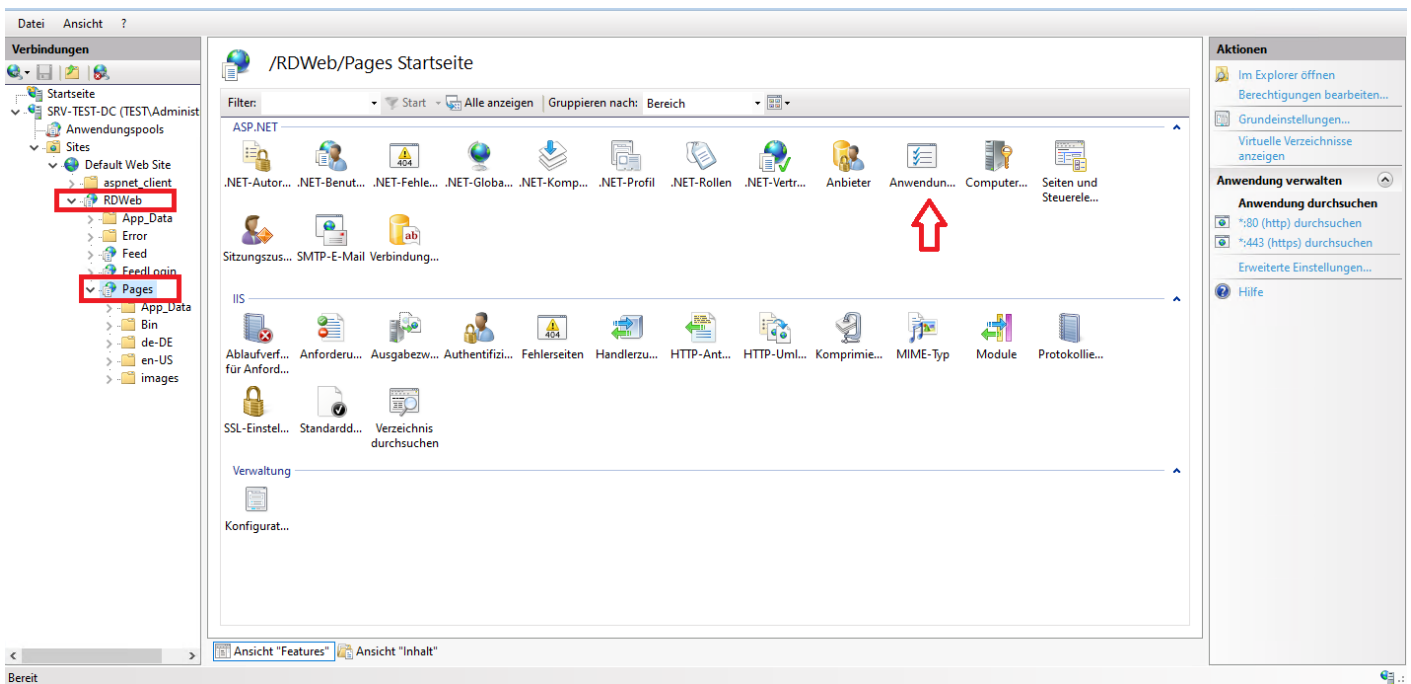
**Beachte:** Jeden Dienst den wir nach außen auf machen (Sprich, es kann sich jeder der unsere IP / Domain + ggf. Port kennt, die Seite öffnen), ist immer ein Sicherheitsrisiko. Hacker können so Sicherheitslücken ausnutzen, um so erheblichen Schaden anzurichten!

The screenshot shows a Windows dialog box titled "Eigenschaften von password". It has two tabs: "Alias (CNAME)" and "Sicherheit". The "Sicherheit" tab is selected. Inside the dialog, there are three text input fields and one button. The first field is labeled "Aliasname (bei Nichtangabe wird übergeordnete Domäne verwendet):" and contains the text "password". The second field is labeled "Vollqualifizierter Domänenname:" and contains the text "password.ad.test.local". The third field is labeled "Vollqualifizierter Domänenname des Zielhosts:" and contains the text "srv-test-dc.ad.test.local.". To the right of this third field is a button labeled "Durchsuchen...". At the bottom of the dialog are three buttons: "OK", "Abbrechen", and "Übernehmen".

Wenn wir jetzt, wie in meinem Beispiel die Domain `password.ad.test.local` anpingen, dann sollten wir eine Antwort erhalten. Damit stellen wir sicher, dass die Verbindung zum Server hergestellt werden kann.

## Internetdienst konfigurieren

Jetzt müssen wir den "**IIS Manager**" so konfigurieren, dass die Benutzer auf unserer Webseite Ihr Kennwort ändern können. Dazu öffnen wir jetzt den **IIS Manager** und navigieren zum letzten Unterpunkt **Pages** im Ordner **RDWeb** und öffnen dort die **Anwendungseinstellungen**.



In den **Anwendungseinstellungen** suchen wir dann den Wert **PasswordChangeEnabled** und ändern den Wert dann auf `true`. Jetzt können wir mit einer der nachstehenden URLs testen, ob wir die Seite öffnen können.

Auf dem Server: `https://localhost/RDWeb/Pages/de-DE/password.apsx`

Intranet: `https://password.ad.test.local/RDWeb/Pages/de-DE/password.aspx`

Es könnte sein das der Browser eine Fehlermeldung ausgibt das das **SSL Zertifikat** Fehlerhaft ist. Wenn dies der Fall ist, können wir im **IIS Manager** unter **SSL-Einstellungen** beim Punkt **SSL Erforderlich** den Haken entfernen. Wichtig ist, das wir uns dann später daru kümmern müssen eine **HTTPS Verbindung** herstellen zu können. Daher sollte dieser Weg nur zu Test Zwecken verwendet werden.

## Optional: HTTP Umleitung einstellen

Wenn wir ein funktionierendes Zertifikat haben, sollten wir dafür sorgen, dass die Verbindungen über HTTPS erfolgen. Dafür müssen wir lediglich wieder im **IIS Manager** unter dem Punkt **HTTP-Umleitung** den Haken bei *Anforderungen zu diesem Ziel umleiten*, und *alle Anforderungen an eigentliches Ziel (und nicht relativ zum Ziel) umleiten* setzen.

Im Anschluss tragen wir im ersten Textfeld den HTTPS Link ein. Und den Statuscode ändern wir auf **Dauerhaft (301)**.

## Optional: Anpassungen an der Weboberfläche

Jetzt können wir nach Belieben die Oberfläche anpassen. Die sieht so ja noch recht langweilig und alt aus! :)

Dazu öffnen wir die folgende Datei unter `C:\Windows\Web\RDWeb\Pages\de-DE\RDWAStrings.xml`

Dort können wir folgende Einträge ändern:

- **PageTitle:** "Passwort ändern"
- **HeadingRDWA:** "Passwort ändern"
- **HeadingApplicationName:** "Portal zur Passwortänderung"

Wenn man möchte, kann man noch in der Datei `C:\Windows\Web\RDWeb\Pages\de-DE\password.aspx` den String von `L_CompanyName_Text` auch auf "Passwort ändern" setzen.

Wer den Hintergrund ändern möchte, kann die Datei `C:\Windows\Web\RDWeb\Pages\images\bg_globe_01.jpg` austauschen.

Das Logo können wir ersetzen, indem wir die Datei `C:\Windows\Web\RDWeb\Pages\images\logo_02.png` ersetzen.

Wer will, kann sich bei der Seite noch mehr austoben! :)

# Ordnerumleitung mit einer Gruppenrichtlinie konfigurieren

## Einleitung

In diesem Beitrag erkläre ich kurz, wie wir mithilfe einer **Gruppenrichtlinie**, eine **Ordnerumleitung** einstellen können. Diese Art der Dateiablage für die Benutzerprofile hat einen enormen Geschwindigkeits-Vorteil und behebt einige Probleme im Vergleich zu den **Roaming Benutzerprofilen**.

## Durchführung

### Welche Ordner können umgeleitet werden?

Mithilfe der **Ordnerumleitung** können wir dann folgende Ordner auf einen **Netzwerk-Pfad** umleiten:

- ☒ AppData (Roaming)
- ☒ Desktop
- ☒ Startmenü
- ☒ Dokumente
- ☒ Bilder
- ☒ Musik
- ☒ Videos
- ☒ Favoriten
- ☒ Kontakte
- ☒ Download
- ☒ Verknüpfungen
- ☒ Suchvorgänge
- ☒ Gespeicherte Spiele

## Voraussetzungen

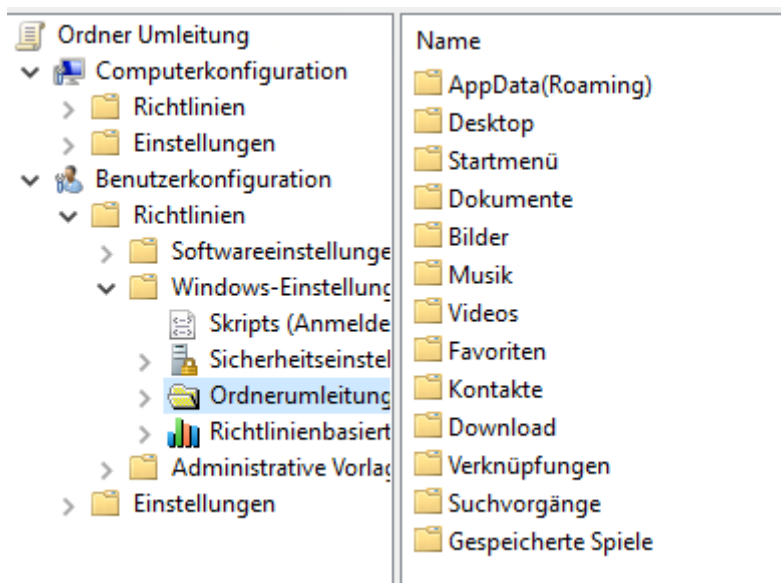
- Active Directory (Windows-Server 2016, Windows-Server 2019, Windows-Server 2022)
- Freigegebenen Netzwerk-Pfad mit entsprechenden Berechtigungen für die Benutzer
- Netzwerk muss bei der ersten Anmeldung vorhanden sein

## Ordnerumleitung einrichten

Um die Ordnerumleitung mittels der **Gruppenrichtlinien** einzurichten, müssen wir im ersten Schritt die **Gruppenrichtlinienverwaltung** öffnen.

Dort legen wir eine neue **Gruppenrichtlinie** an, und bearbeiten diese. Im Editor navigieren wir zum folgenden Pfad:

Benutzerkonfiguration / Richtlinien / Windows-Einstellungen / Ordnerumleitung



Dort angekommen, können wir allen dort angegebenen Ordnern eine Umleitung verpassen. Dazu markieren wir den ersten Ordner und öffnen durch einen *Rechtsklick* und dem folgenden *Klick* auf "*Eigenschaften*" die Einstellungen für diesen Ordner.

In der Eingabemaske entscheiden wir uns für einen von beiden "*Einstellungen*".

**Standard:** Für jeden Benutzer werden die Ordner auf den gleichen Pfad umgeleitet

**Erweitert:** Spezielle Gruppen werden auf spezielle Freigaben umgeleitet.

Wir verwenden **Standard**, da dies wohl die meist verwendete Art sein wird. Im nächsten Schritt unter **Zielordner** geben wir an, wie mit den Dateien umgegangen werden soll. In unserem Fall verwenden wir "*Einen Ordner für jeden Benutzer im Stammpfad erstellen*". Dies ermöglicht, dass der Benutzer einen **eigenen Ordner** hat, indem seine eigenen Dateien liegen. Der Server legt in diesem Fall bei einer neuen Anmeldung für den Benutzer eine **eigene Verzeichnisstruktur** in dem **Stammpfad** an.

Wahlweise können wir auch "*an folgenden Pfad umleiten*" verwenden, falls alle Benutzer dieselben Dateien und Dokumente haben sollen. Es ist vielleicht von Vorteil bei Favoriten oder Desktop.

Als letzten Schritt geben wir nur noch das **Stammverzeichnis** an. In diesem angegebenen Verzeichnis werden dann einzelne Ordner für die entsprechenden Benutzer angelegt.

Diese Schritte wiederholen wir mit allen benötigten Ordnern, die wir umleiten möchten.