



## **Active Directory Inventarisierung**

Inventarisierung des Active Directory Verzeichnisdienstes

<b>TITEL</b>	Active Directory Inventarisierung
<b>AUTOR</b>	Docusnap Consulting
<b>DATUM</b>	18.10.2022
<b>VERSION</b>	1.0   gültig ab 29.09.2022

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die itelio GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of itelio GmbH. All rights reserved.

## INHALTSVERZEICHNIS

1.	Einleitung	4
2.	Active Directory Inventarisierung	5
3.	Skriptbasierte Active Directory Inventarisierung	6
3.1	Skriptbasierte Inventarisierung durchführen	6
3.2	Inventarisierung importieren	7
3.3	Skriptausführung automatisieren	8
4.	Zusätzliche ADDS-Eigenschaften inventarisieren	10
4.1	Grundlagen	10
4.2	Notwendigen Werte sammeln	11
4.3	ADDS-Eigenschaft in Docusnap anlegen und zuordnen	12
5.	Auswertungsmöglichkeiten	13
5.1	Informationen in der Baumstruktur	13
5.2	Bericht – Veränderungen / Vergleichsbericht	13
5.3	Bericht – Objekte auflisten	14

## 1. Einleitung

Docusnap inventarisiert das Active Directory mit allen dazugehörigen Klassen wie Benutzer, Gruppen, Benutzer-Gruppenmitgliedschaften, Gruppenrichtlinien und Computerobjekte.

Für die eigentliche Inventarisierung der im Active Directory befindlichen Objekte werden LDAP / LDAPS Abfragen verwendet. Im Detail verwendete Ports und notwendige Berechtigungen werden im [Whitepaper für die Inventarisierungen](#) aufgelistet.

Neben der eigentlichen Inventarisierung des Active Directories ([Kapitel 2](#)) wird in diesem HowTo auch die Möglichkeit der skriptbasierten Inventarisierung beschrieben ([Kapitel 3](#)).

Docusnap inventarisiert, im Zuge der ADDS-Inventarisierung, u. a. die Benutzer Objekte mit einer Auswahl der dazugehörigen Eigenschaften. Sollten von Ihnen verwendete Eigenschaften nicht inventarisiert werden, können Sie diese nachträglich der ADDS-Inventarisierung hinzufügen ([Kapitel 4](#)).

In [Kapitel 5](#) finden Sie die beliebtesten Auswertungsmöglichkeiten zu Themen bzgl. Der Active Directory Inventarisierung.

## 2. Active Directory Inventarisierung

Für die Netzwerkinventarisierung des Active Directories starten Sie den entsprechenden Assistenten:

- Discovery – Alle Assistenten – Active Directory
- Inventar – Alle Assistenten – Active Directory
- Alle Aufträge – Alle Assistenten – Active Directory

In Schritt 1 wählen Sie Ihre Firma oder die Firma Ihres Kunden aus.

In Schritt 2 wählen Sie den Discovery Service aus, über den Sie die Inventarisierung durchführen möchten.

Für eine zeitgesteuerte Inventarisierung wählen Sie hier den Docusnap Server Discovery oder einen von Ihnen konfigurierten Discovery Service.

Weiterhin wählen oder geben Sie die Domäne und einen entsprechend berechtigten Benutzer mit dessen Passwort ein. Verwenden Sie für den Benutzer die NetBios Schreibweise (Domäne\Benutzer).

In Schritt 3 können nun die notwendigen Eigenschaften für die Inventarisierung gesetzt werden:

Über das Filterkriterium **Starte Suche bei** besteht die Möglichkeit, die Inventarisierung des AD auf eine bestimmte Organisationseinheit einzugrenzen.

Dies kann notwendig sein, wenn Ihre Benutzer, Gruppen und Computer etc. ab einer spezifischen Organisationseinheit in einem umfassenden Active Directory verfügbar sind, in dem Mutter / Tochtergesellschaften abgebildet sind.

**Ist dies nicht der Fall, dann sollten Sie hier keinen Filter setzen!**

Beachten Sie bei einer Filterung die standardmäßig aktive Option innerhalb der **erweiterten Optionen: Alle Benutzer, Gruppen und Computer auslesen!**

Diese Option sollte im Regelfall deaktiviert werden, da ansonsten doch wieder alles Benutzer, Gruppen und Computer der Gesamtstruktur inventarisiert werden.

Für die Inventarisierung der Gruppenrichtlinien (GPO) wird ein Host mit installierter Gruppenrichtlinienmanagementkonsole benötigt. In aller Regel einer der Domänen-Controller. Alternativ kann die Konsole auch auf sonstigen Systemen installiert werden.

Die Inventarisierung der GPOs wird mittels PSEXec durchgeführt. Sollte es bei der Prüfung zu einem Fehler kommen, können Sie die Fehleranalyse über das [HowTo Inventarisierungen per PSEXec](#) durchführen.

In den erweiterten Optionen können Sie aktivieren, dass die

- Domänenstruktur
- Active Directory Sites und
- Strukturberechtigungen

Inventarisiert werden.

### 3. Skriptbasierte Active Directory Inventarisierung

#### 3.1 Skriptbasierte Inventarisierung durchführen

Docusnap bietet die Möglichkeit, das Active Directory auch lokal, auf einem Domänencontroller, mittels einer skriptbasierten Inventarisierung zu erfassen.

Die Skriptdatei finden Sie im Installationsverzeichnis von Docusnap – im Standard:

- C:\Program Files\Docusnap 11\Tools\Scan-ADDS.exe

Im einfachsten Fall, ohne weitere Konfiguration und mit vollem Inventarisierungsumfang (Alle Klassen, Gesamtstruktur, GPOs, Domänenstruktur, Berechtigungen, Standorte) können Sie die Scan-ADDS.exe auf einen Domänencontroller kopieren und dort ausführen.

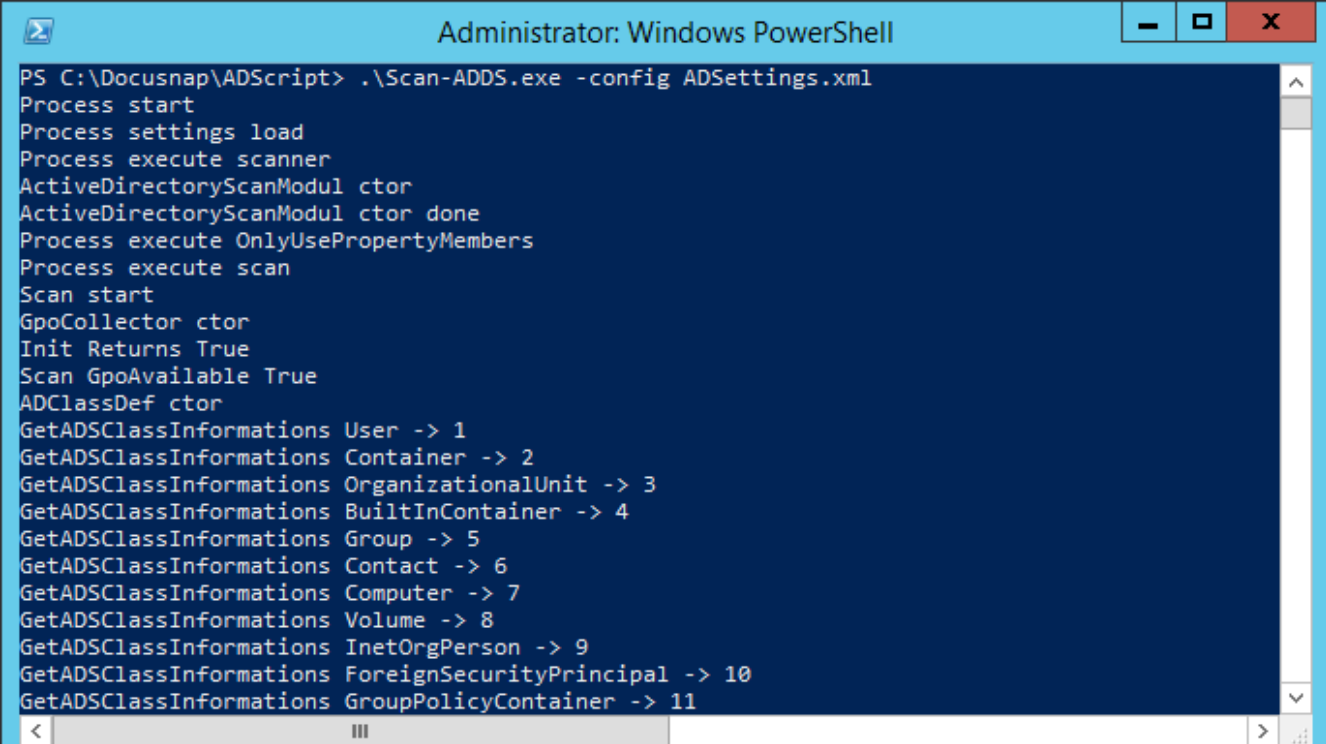
Sind weitere Einstellungen notwendig, kann die skriptbasierte Active Directory Inventarisierung auch angepasst werden. Hierzu nutzen Sie den Assistenten **AD-Einstellungen exportieren**:

- Discovery – Alle Assistenten – AD-Einstellungen exportieren
- Inventar – Alle Assistenten – AD-Einstellungen exportieren
- Alle Aufträge – Alle Assistenten – AD-Einstellungen exportieren

Innerhalb dieses Assistenten können Sie die gleichen Inventarisierungsoptionen wie beim zuvor behandelten Active Directory Inventarisierungsassistenten verwalten.

Nachdem alle Optionen gesetzt wurden, werden die Einstellungen in eine Zip-Datei exportiert. Transferieren Sie die Zip-Datei auf den Ziel-Domänencontroller und entpacken Sie diese.

Führen Sie die Scan-ADDS.exe nun zusätzlich mit dem Parameter `-config ADSettings.xml` aus.



```
Administrator: Windows PowerShell
PS C:\Docusnap\ADScript> .\Scan-ADDS.exe -config ADSettings.xml
Process start
Process settings load
Process execute scanner
ActiveDirectoryScanModul ctor
ActiveDirectoryScanModul ctor done
Process execute OnlyUsePropertyMembers
Process execute scan
Scan start
GpoCollector ctor
Init Returns True
Scan GpoAvailable True
ADClassDef ctor
GetADSClazzInformations User -> 1
GetADSClazzInformations Container -> 2
GetADSClazzInformations OrganizationalUnit -> 3
GetADSClazzInformations BuiltInContainer -> 4
GetADSClazzInformations Group -> 5
GetADSClazzInformations Contact -> 6
GetADSClazzInformations Computer -> 7
GetADSClazzInformations Volume -> 8
GetADSClazzInformations InetOrgPerson -> 9
GetADSClazzInformations ForeignSecurityPrincipal -> 10
GetADSClazzInformations GroupPolicyContainer -> 11
```

Abbildung 1 - Aufruf der Scan-ADDS.exe mit Parameter

## 3.2 Inventarisierung importieren

Je nach Konfiguration finden Sie nach Abschluss der Inventarisierung bis zu fünf JSON-Dateien mit den inventarisierten Informationen:

- Domains.json
- Objects.json
- Result.json
- Sites.json
- Trusts.json

Diese Daten können Sie mit Hilfe des Assistenten Skript Import nach DocuSnap importieren:

- Discovery – Alle Assistenten – Skript Import
- Inventar – Alle Assistenten – Skript Import
- Alle Aufträge – Alle Assistenten – Skript Import

**In Schritt 1** wählen Sie Ihre Firma oder die Firma Ihres Kunden aus.

**In Schritt 2** wählen Sie den Discovery Service aus, über den Sie die Inventarisierung durchführen möchten.

Für eine zeitgesteuerte Inventarisierung wählen Sie hier den DocuSnap Server Discovery oder einen von Ihnen konfigurierten Discovery Service.

Beachten Sie hierbei, dass der Benutzer, der einen der Dienste ausführt, Lese- und Schreibzugriffe auf den im nächsten Schritt ausgewählten Pfad besitzen muss.

Lokales System = Ablageverzeichnis kann nur lokal liegen

**In Schritt 3** wählen Sie das Verzeichnis aus, in dem Sie die erzeugten JSON-Dateien abgelegt haben.

Dieses Verzeichnis kann auch ein Netzlaufwerk sein. Beachten Sie die Freigabeberechtigungen.

**In Schritt 4** können Sie nun nach validen Skriptdateien suchen.

Sind in dem von Ihnen ausgewählten Ordner Dateien von weiteren Skriptinventarisierungen (DNS, DHCP, Windows etc.) vorhanden, werden auch diese berücksichtigt.

### 3.3 Skriptausführung automatisieren

Der große Vorteil von Docusnap besteht darin, dass regelmäßig und automatisch Daten inventarisiert werden und somit aktuell sind. Dies kann auch mit Skriptinventarisierungen erreicht werden.

Im ersten Schritt muss die Ausführung des Skripts automatisiert werden. Dies kann unter anderem mit einer Softwareverteilung erfolgen, wie auch mit Windows Bordmitteln – Aufgabenplanung.

Wechseln Sie in die Aufgabeplanung / Task Scheduler von Ihrem Domänen-Controller und erstellen Sie eine neue Aufgabe.

Im Tab **Allgemein** hinterlegen Sie einen Namen und wählen die Sicherheitsoptionen:

Folgendes Benutzerkonto verwenden: Benutzer mit vollständigen Leseberechtigungen auf das ADDS / lokales Systemkonto

Unabhängig von der Benutzeranmeldung ausführen

Mit höchsten Privilegien ausführen

Konfigurieren für: Das passende Betriebssystem auswählen

Im Tab **Trigger** können Sie den Zeitplan der Skriptausführung konfigurieren – beispielsweise:

Aufgabe starten: Nach einem Zeitplan

Wöchentlich, jede 1 Woche wiederholen am: Sonntag

Im Tab **Aktionen** definieren Sie die Ausführung der Scan-ADDS.exe

Wir empfehlen die Erstellung einer versteckten Freigabe auf dem Docusnap Server / System, dass den Docusnap Discovery Service ausführt.

Auf dieser Freigabe legen Sie die Scan-ADDS.exe und die JSON-Dateien ab

z. B. `\\SRV-Docu\DocusnapScript$\Scripts\ADS`

`\\SRV-Docu\DocusnapScript$\Firma#Domain.FQDN1`

Innerhalb dieser Freigabe / Unterordner kann der ausführende Benutzer Lesen und Schreiben

**Aktion:** Programm starten

**Programm / Skript:** `\\SRV-Docu\DocusnapScript$\Scripts\ADS\Scan-ADDS.exe`

**Argumente:** `-config ADSettings.xml -O "\\SRV-Docu\DocusnapScript$\Ihre Firma#intern.local"`

Der `-O` Parameter leitet die Ergebnisdateien auf den angegebenen Pfad um. Der Benutzer, der die Inventarisierung durchführt, muss auf diesem Pfad Schreibrechte besitzen.

Die neu erstellte Aufgabe sorgt dafür, dass die Inventarisierung regelmäßig und automatisch ausgeführt wird.

Es sollte immer sichergestellt sein, dass die aktuelle Version der Skriptdatei verwendet wird! Das bedeutet, dass Sie nach einem Update von Docusnap auch die Skriptdateien austauschen!

.....

<sup>1</sup> Die Angabe der Ordnerstruktur entspricht dem Standard des globalen Skript Imports und bewirkt, dass Sie auch für evtl. zukünftig auftretende Szenarien gerüstet sind.



Im nächsten Schritt wird der Import der Inventarisierung als Auftrag eingerichtet. Beachten Sie, dass Sie im Zuge eines Import-Auftrags auch die Ergebnisse der sonstigen skriptbasierten Inventarisierungen automatisch importieren können.

Öffnen Sie den Skript Import Assistenten:

- Discovery – Alle Assistenten – Skript Import
- Inventar – Alle Assistenten – Skript Import
- Alle Aufträge – Alle Assistenten – Skript Import

In Schritt 1 wählen Sie Ihre Firma oder die Firma Ihres Kunden aus.

In Schritt 2 wählen Sie den DocuSnap Server Dienst oder einen von Ihnen erstellten Discovery Service aus.

In Schritt 3 wählen Sie das Verzeichnis aus, in dem die erzeugten JSON-Dateien abgelegt werden:

In der empfohlenen Konfiguration liegt dieser Ordner lokal auf dem DocuSnap Server oder auf dem System, das den Discovery Service zur Verfügung stellt

Für die übrigen Skriptausführungen können auch weitere Verzeichnisse hinzugefügt werden

In Schritt 6 konfigurieren Sie die Zeitplanung.

Neben dem einfachen Skript Import können Sie auch den [globalen Skriptimport](#) verwenden. Durch diesen können Sie Skriptimporte für mehrere Firmen und / oder Domänen gleichzeitig durchführen.

## 4. Zusätzliche ADDS-Eigenschaften inventarisieren

### 4.1 Grundlagen

In der Docusnap-Administration finden Sie im Bereich Inventar die Active Directory Verwaltung. Innerhalb dieser können Sie

- ADDS-Klassen anpassen und erweitern
- ADDS-Eigenschaften anpassen und erweitern
- Neu hinzugefügte ADDS-Eigenschaften den dazugehörigen Klassen zuordnen (ADDS-Zuordnung)

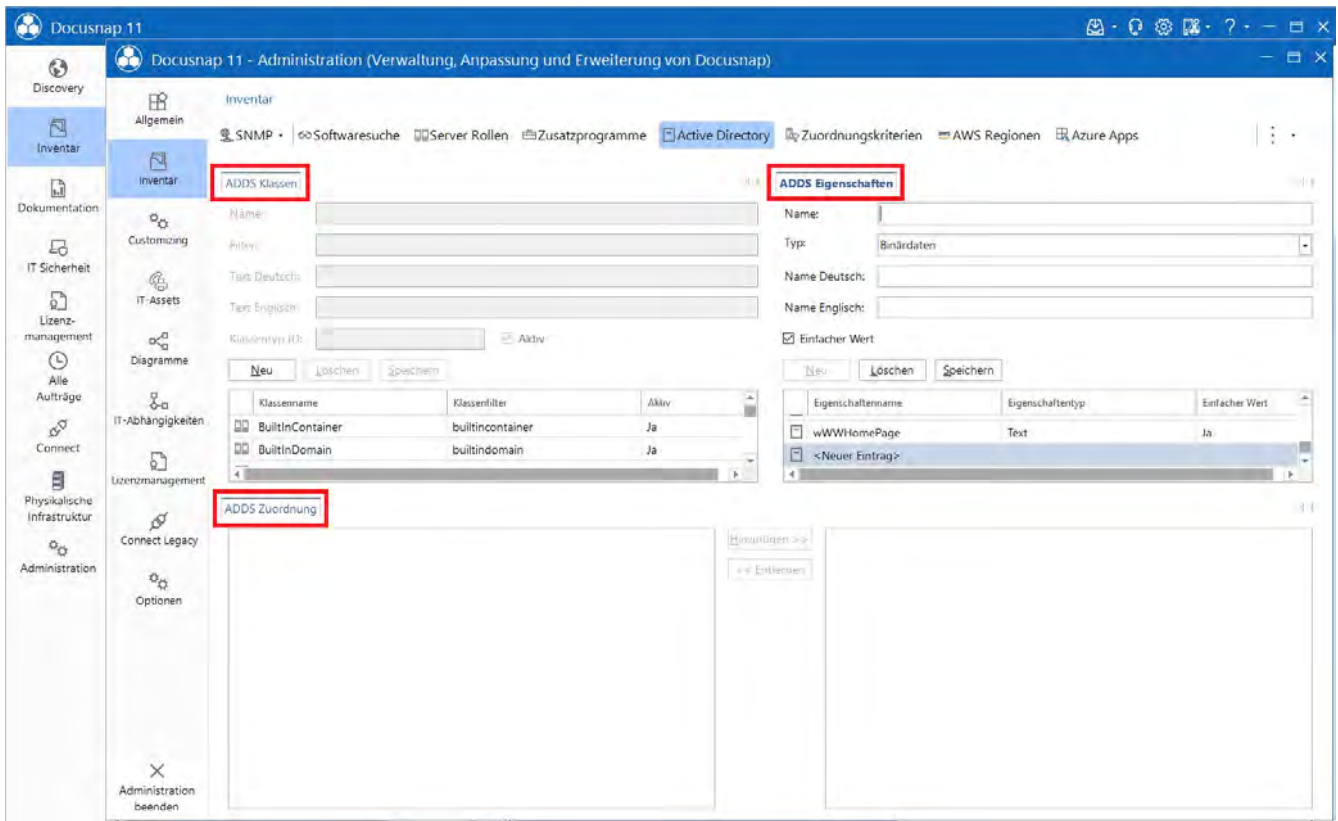


Abbildung 2 - Active Directory Verwaltung in der Docusnap-Administration

## 4.2 Notwendigen Werte sammeln

Der erste Schritt bei dem Hinzufügen neuer ADDS-Eigenschaften besteht darin, dass Sie die in DocuSnap notwendigen Informationen sammeln. DocuSnap benötigt für das Hinzufügen neuer ADDS-Eigenschaften folgende Werte:

- Name

Der Name der Eigenschaft muss der Bezeichnung, die die Eigenschaft bzw. das Attribut im Active Directory hat, entsprechen.

- Typ

Der Typ definiert den Wert der Eigenschaft.

- Name Deutsch / Name Englisch

Name der Eigenschaft, wie diese im Zuge der Inventarisierung in DocuSnap bezeichnet werden soll.

- Einfacher Wert

Das Kontrollkästchen gibt an, ob diese Eigenschaft pro Klasse mehrfach gefunden werden kann (z.B. Mailadressen) oder ob es diesen Wert nur einmal gibt (z.B. Name).

Microsoft bietet innerhalb der DOCS entsprechende Informationen - z. B. finden Sie folgend die Dokumentation für das Attribut [Employee-ID](#).

### 4.3 ADDS-Eigenschaft in DocuSnap anlegen und zuordnen

Nachdem die Werte gesammelt wurden, wechseln Sie in die Administration - Inventar - Active Directory und wählen unterhalb von ADDS Eigenschaften Neu.

In diesem Beispiel wird das extensionAttribute1 in DocuSnap aufgenommen:

- Name: extensionAttribute1
- Typ: Text
- Name Deutsch: Neu hinzugefügte ADDS-Eigenschaft
- Name Englisch: New added ADDS property
- Einfacher Wert: Ja (Aktiv)

Nach dem Speichern muss die Zuordnung der neuen Eigenschaft zur ADDS-Klasse(n) erfolgen.

Wählen Sie hierzu zunächst die entsprechende ADDS-Klasse aus - in diesem Beispiel sind es die User.

Nun werden Ihnen unterhalb der ADDS-Zuordnung, auf der linken Seite, alle vorhandenen und noch nicht zugeordneten ADDS-Eigenschaften aus DocuSnap aufgelistet. Suchen Sie die neu erstellte Eigenschaft heraus - markieren Sie diese und die Schaltfläche Hinzufügen fügt die neue Eigenschaft der Klasse hinzu.

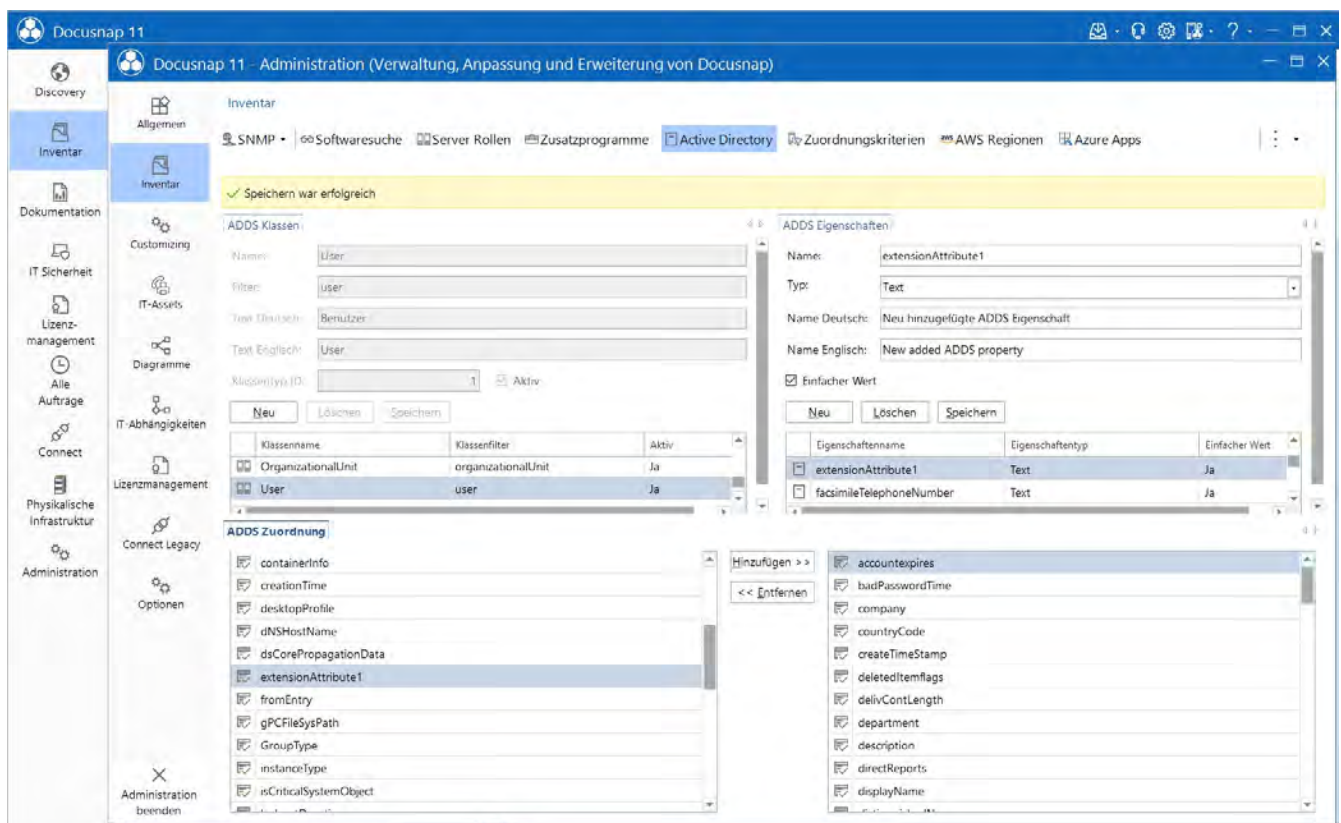


Abbildung 3 - ADDS Eigenschaft in DocuSnap anlegen und zuordnen

Wenn Sie nun eine neue Active Directory Inventarisierung durchführen, werden Sie daraufhin die neue Eigenschaft finden.

## 5. Auswertungsmöglichkeiten

### 5.1 Informationen in der Baumstruktur

Die inventarisierten Informationen der Active Directory Inventarisierung sind in der Baumstruktur wie folgt zu finden:

- *Ihre Firma* - Infrastruktur - *Ihre Domäne* – Active Directory

Hier können Sie nun durch die inventarisierte Struktur, samt der Gruppenrichtlinien, navigieren.

Unterhalb der Benutzer finden Sie alle aktiven wie auch deaktivierten Benutzer des Active Directories. In der nächsten Ebene können Sie die Eigenschaften und die direkten Gruppenmitgliedschaften des Benutzers auswerten.

Weiterhin haben Sie diese Informationen auch für Gruppen und Computerobjekte.

### 5.2 Bericht – Veränderungen / Vergleichsbericht

Der Bericht Veränderungen listet Ihnen alle Veränderungen zwischen der aktuellen und der vorherigen Active Directory Inventarisierung auf. Sie bekommen eine Übersicht über

- Hinzugefügte und gelöschte Benutzerkonten
- Hinzugefügte und gelöschte Gruppen
- Hinzugefügte und gelöschte Computerkonten
- Hinzugefügte und gelöschte Gruppenmitgliedschaften
- ADDS Container Veränderungen (Benutzer-, Gruppen oder Computerobjekte wurden verschoben)

Den Bericht finden Sie in der Baumstruktur wie folgt:

- *Ihre Firma* - Infrastruktur - *Ihre Domäne* - Berichte - AD DS Infrastruktur

Neben dem Bericht Veränderungen finden Sie dort auch den Vergleichsbericht. Dieser listet Ihnen die gleichen Veränderungen im Active Directory auf, jedoch besitzen Sie hier die Auswahl, welche Inventarisierungsstände miteinander verglichen werden sollen.

### 5.3 Bericht – Objekte auflisten

Der Bericht Objekte auflisten liefert Ihnen eine flexible Möglichkeit die inventarisierten Informationen aus dem Active Directory auszuwerten. Den Bericht finden Sie in der Baumstruktur wie folgt:

- *Ihre Firma* - Infrastruktur - *Ihre Domäne* - Berichte - AD DS Infrastruktur

Wenn der Bericht aufgerufen wird, erscheint zunächst ein Formularfeld.

- **Klasse:** Hier wählen Sie die Klasse, für die Sie eine Auswertung durchführen möchten (Benutzer)
- **Eigenschaft:** Hier wählen Sie die Eigenschaft, die ausgewertet werden soll (Neu hinzugefügte...)
- **Ansicht:** Hier können Sie weitere Eigenschaften auswählen, die angezeigt werden sollen

Mit dem Bericht können Sie beispielsweise folgende Fragen beantworten:

- Alle Benutzer einer Abteilung auflisten
- Alle aktiven Benutzer auflisten, deren Kennwort nicht abläuft
- Alle Benutzer auflisten, die seit X Tagen nicht angemeldet waren

## ABBILDUNGSVERZEICHNIS

ABBILDUNG 1 - AUFRUF DER SCAN-ADDS.EXE MIT PARAMETER .....	6
ABBILDUNG 2 - ACTIVE DIRECTORY VERWALTUNG IN DER DOCUSNAP-ADMINISTRATION .....	10
ABBILDUNG 3 - ADDS EIGENSCHAFT IN DOCUSNAP ANLEGEN UND ZUORDNEN .....	12

## VERSIONSHISTORIE

---

<b>Datum</b>	<b>Beschreibung</b>
29.09.2022	Erstellung des HowTos

---



