UNITED SECURITY PROVIDERS

USP Network Authentication System®

Spezifikation Inventarimport und NMS-Import

Version 18.2



United Security Providers AG
www.united-security-providers.ch
info@united-security-providers.ch

Headquarter Stauffacherstrasse 65/15 CH-3014 Bern Tel. +41 31 959 02 02
Baslerpark Mürtschenstrasse 27 CH-8048 Zürich Tel. +41 44 496 61 11



UNITED SECURITY PROVIDERS

Copyright © 2026 United Security Providers AG

This document is protected by copyright under the applicable laws and international treaties. No part of this document may be reproduced in any form and distributed to third parties by any means without prior written authorization of United Security Providers AG.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESSED OR IMPLIED REPRESENTATIONS AND WARRANTIES, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED TO THE EXTENT PERMISSIBLE UNDER THE APPLICABLE LAWS.

UNITED SECURITY PROVIDERS

Contents

1 Spezifikation Inventar-Import und NMS-Import **1**

2 Einführung **3**

2.1 Ausgangslage . . . 3
2.2 Hauptmerkmale von USP NAS . . . 3
2.3 Systemübersicht USP NAS . . . 3
2.4 Zweck des Dokuments . . . 4
2.5 Geschlechtsneutrale Formulierungen . . . 4

3 Schnittstelle für den Datenimport in USP NAS **5**

3.1 Ausgangslage . . . 5
3.2 Datentransfer . . . 5
3.3 Dateinamen . . . 6
3.4 Dateiformat . . . 7
3.4.1 Spezifischer Record-Separator . . . 7
3.5 Full Import und Delta Import . . . 8
3.6 Überprüfung des Inhalts . . . 8
3.7 Konflikte zwischen Quellsystemen . . . 8

4 Daten aus Inventarsystemen **9**

4.1 Format einer Datenzeile . . . 9
4.2 Erläuterungen . . . 10
4.2.1 Asset-ID . . . 10
4.2.2 Parent Asset-ID . . . 11
4.2.3 Offizieller DNS-Name des Geräts . . . 11
4.2.4 MAC-Adresse . . . 11
4.2.5 Darf das Gerät an das Netzwerk angeschlossen werden? . . . 11
4.2.6 Status gemäss Inventar . . . 11
4.2.7 Restriktionen . . . 11
4.2.8 Gerätetyp . . . 11
4.2.9 Geräteklasse . . . 12
4.2.10 Standort . . . 12
4.2.11 Owner . . . 12
4.2.12 Produktiv VLAN . . . 12
4.2.13 Mandant . . . 12
4.2.14 Aktivierung EPC-Scan . . . 12

Copyright © 2026 United Security Providers AG. All rights reserved.

4.2.15 Zusatzinformationen . . . 12
4.2.16 Gültigkeit Temporär . . . 12
4.2.17 Changed by . . . 13
4.2.18 Double Attached Node (DAN) . . . 13
4.3 Beispiel . . . 13
4.4 Geräte mit mehreren MAC-Adressen . . . 13
4.5 Komplette Assets pro Import . . . 13
4.6 Gleiche MAC-Adresse aus verschiedenen Inventarsystemen . . . 15
4.7 Funktionsweise Full Import . . . 15
4.8 Funktionsweise Delta Import . . . 18
4.9 Übersicht Ablauf des Inventarimports . . . 20

5 Daten aus NMS **21**
5.1 Format einer Datenzeile . . . 21
5.2 Erläuterungen . . . 22
5.2.1 DNS-Name . . . 23
5.2.2 IP-Adresse . . . 23
5.2.3 Typ des Netzwerkgeräts . . . 23
5.2.4 SNMP-Version . . . 24
5.2.5 SNMP Read Community (Public Community) . . . 24
5.2.6 SNMP Write Community (Private Community) . . . 24
5.2.7 Location . . . 24
5.2.8 In Scope . . . 25
5.2.9 Zugangskontrollvariante . . . 25
5.2.10 MPP-User / MPP-Passwort / MPP-Port (obsolet) . . . 25
5.2.11 SNMPv3 User . . . 25
5.2.12 SNMPv3 Authentication Passwort . . . 25
5.2.13 SNMPv3 Encryption Passwort . . . 25
5.2.14 Mandant . . . 25
5.2.15 WLAN ACL Filter Enforcement Flag . . . 26
5.2.16 802.1x Accounting . . . 26
5.3 Beispiel . . . 26
5.4 Format einer Datenzeile (Netzwerkports) . . . 27

Copyright © 2026 United Security Providers AG. All rights reserved.

6 Daten für Endpoint Profiling **28**
6.1 Format einer Datenzeile (PROFILERDEVICES) . . . 28
6.2 Erläuterungen . . . 28
6.2.1 Profilerdevice Name . . . 28
6.2.2 Profilerdevice Parent . . . 28
6.3 Format einer Datenzeile (PROFILERCOMBINATIONS) . . . 28
6.4 Erläuterungen . . . 29
6.4.1 Profilerdevice Name . . . 29
6.4.2 Version . . . 29
6.4.3 Score . . . 29
6.4.4 DHCP-Fingerprint . . . 29
6.4.5 DHCP-Vendor . . . 29
6.4.6 MAC Vendor Name . . . 29
6.4.7 MAC Vendor Präfix . . . 29

7 Daten für Port Konfiguration **30**
7.1 Format einer Datenzeile (PORTCONFIG) . . . 30
7.2 Erläuterungen . . . 30
7.2.1 Switch-DNS . . . 30
7.2.2 ifindex . . . 30
7.2.3 ifname . . . 30
7.2.4 Subzone . . . 30

8 Daten für Portgruppen Import **31**
8.1 Format einer Datenzeile (PORTGROUP) . . . 31
8.2 Erläuterungen . . . 31
8.2.1 Switch-DNS . . . 31
8.2.2 ifindex . . . 31
8.2.3 ifname . . . 31
8.2.4 Portgruppe . . . 32

9 DNS-Import über CSV **33**
9.1 Format einer Datenzeile (DNS) . . . 33
9.2 Erläuterungen . . . 33
9.2.1 DNS-Name . . . 33
9.2.2 IP-Adresse . . . 33
9.2.3 Typ . . . 33

Copyright © 2026 United Security Providers AG. All rights reserved.

10 Endgeräte-Detail Import **34**

10.1 Format einer Datenzeile (EPD) 34

10.2 Erläuterungen 34

10.2.1 Mac-Adresse 34

10.2.2 IP-Adresse 34

10.2.3 Key 34

10.2.4 Value 34

Copyright © 2026 United Security Providers AG. All rights reserved.

UNITED SECURITY PROVIDERS

1 Spezifikation Inventar-Import und NMS-Import

- Gilt ab USP NAS v18
- Nur für internen Gebrauch

Dokumentnummer: n/a	
Version: 2.35	20. August 2026

Dokumenthistory und –Status

Nr.	Datum	Version	Kapitel	Grund der Änderung	Autor
1	17.09.08	2.0	Alle	Übernahme von Version 1.12	M. Grossenbacher
2	17.09.08	2.0	2.3	Optionale Versionsbezeichnung am Ende des Dateinamens	M. Grossenbacher
3	17.09.08	2.0	4.1	Optionale Location und Inscope Felder zu NMS-Import hinzugefügt	M. Grossenbacher
4	18.09.08	2.0	Alle	Freigabe	M. Grossenbacher
5	12.01.09	2.1		Doppelte Interfaces ohne MAC-Adresse werden eliminiert, falls sich auch in den anderen Attributen kein Unterschied zeigt	M. Grossenbacher
6	12.01.09	2.1	Alle	Freigabe	M. Grossenbacher
7	12.03.09	2.2	4.1	Optionales Blockmechanismus Feld zum NMS-Import hinzugefügt	M. Grossenbacher
8	12.03.09	2.2	Alle	Freigabe	M. Grossenbacher
9	09.06.09	2.3	3.2	Optionales Produktiv VLAN für Inventarimport hinzugefügt	M. Grossenbacher
10	09.06.09	2.3	Alle	Freigabe	M. Grossenbacher
11	16.06.09	2.4	3.2	Erläuterungen erweitert	M. Grossenbacher
12	16.06.09	2.4	4.2	Erläuterungen erweitert	M. Grossenbacher
13	16.06.09	2.4	Alle	Freigabe	M. Grossenbacher
14	24.08.09	2.5	Alle	Überarbeitung	M. Grossenbacher
15	24.08.09	2.5	Alle	Freigabe	M. Grossenbacher
16	16.04.10	2.6	3.2	Optionales Feld Mandant zu Inventarimport hinzugefügt	M. Grossenbacher
17	14.07.10	2.6	3.2	Optionales Feld EPC Aktivierung zu Inventarimport hinzugefügt	M. Grossenbacher
18	24.08.10	2.7	5	Definition EPC Schnittstelle	T. Aebi
19	24.11.10	2.8	4.1	NMS Scope Import angepasst für MPP Devices und SNMPv3	M. Grossenbacher
20	24.11.10	2.8	Alle	Freigabe	M. Grossenbacher
21	27.07.11	2.9	4.1	NMS Scope Import angepasst damit Mandant angegeben werden kann	M. Grossenbacher
22	27.07.11	2.9	Alle	Freigabe	M. Grossenbacher
23	25.11.11	2.10	4.1	Umbenennen des Blockmechanismus zu Zugangskontrollvariante und Angabe von neuen Variantennamen	M. Grossenbacher
24	25.11.11	2.10	Alle	Freigabe	M. Grossenbacher
25	13.01.12	2.11	4.2	Erläuterungen zu Identifizierung im NMS-Import	M. Grossenbacher
26	13.01.12	2.11	Alle	Freigabe	M. Grossenbacher
27	16.02.12	2.12	4	Neue SNMPv3 Versionen mit AES-Verschlüsselung hinzugefügt	M. Grossenbacher
28	16.02.12	2.12	Alle	Freigabe	M. Grossenbacher

Copyright © 2026 United Security Providers AG. All rights reserved.

Nr.	Datum	Version	Kapitel	Grund der Änderung	Autor
29	24.04.12	2.13	3.2.15	Feld Zusatzinformationen hinzugefügt	M. Grossenbacher
30	24.04.12	2.13	Alle	Freigabe	M. Grossenbacher
31	25.05.12	2.14	4.2.3	Wert WLAN als Netzwerkgerätetyp hinzugefügt	M. Grossenbacher
32	25.05.12	2.14	Alle	Freigabe	M. Grossenbacher
33	28.02.13	2.15	4.2.3	Wert ACL Filter Flag hinzugefügt	M. Grossenbacher
34	28.02.13	2.15	Alle	Freigabe	M. Grossenbacher
35	04.03.13	2.16	4.2.16 -4.2.18	Beschreibung für ACL Filter Flag aktualisiert und 802.1x Accounting Feld hinzugefügt.	M. Grossenbacher
36	04.03.13	2.16	Alle	Freigabe	M. Grossenbacher
37	27.03.13	2.17	2.2	Poll-Intervall nicht konfigurierbar	T. Aebi
38	15.12.13	2.18	4	Erweiterung WTP Gerätetyp	T. Aebi
39	26.09.14	2.19	4.2.3	WTP-Gerät aufgelistet	M. Grossenbacher
40	10.03.16	2.20	2.1, 6	Endpoint Profiling hinzugefügt	T. Baumann
41	21.04.17	2.21	7	Import Portconfig hinzugefügt	T.Aebi
42	03.05.17	2.22	2,7,8	Import Portgroup hinzugefügt	T.Aebi
43	05.06.17	2.23	7	Gerätetyp statt Geräteklasse in Portconfig	T.Aebi
44	19.7.19	2.24	9,10	DNS und EPD-Imports hinzugefügt	T.Aebi
45	8.8.2019	2.25	2.4,4,10	Anpassung EPD, Erweiterung NMS mit L3-Modus, spezifischer Record-Separator	T.Aebi
46	11.12.19	2.26	3.2.16	Temporäre Gültigkeit Endgeräte	T.Aebi
47	22.06.22	2.27	4	SNMPV3 Felder immer optional wegen den neuen Werten in der globalen Konfiguration	T. Hubmann
48	20.09.22	2.28	4	Netzwerkgerätetyp erweitert mit RADIUSAUTH	T.Aebi
49	26.6.23	2.29	4	Maintenance Mode für Netzwergeräte	T.Aebi
50	29.4.24	2.30	4	Snmp versionen erweitert	T.Aebi
51	2.7.24	2.31	4	Portgroup import mit Port-Wildcard erweitert. Changed by Feld zu Endgeräte Inventar hinzugefügt.	T.Aebi
52	19.12.24	2.32	4	SNMP-Zugangsprofil zu Netzgeräten hinzugefügt	N. Perrenoud
53	25.7.25	2.33	3	Inventar-Feld «Produktiv-VLAN» und «Status gemäss Inventar» als obsolet markiert	N. Perrenoud
54	5.8.25	2.33	3	Netport-Feld «Typ» mit HSR-Option hinzugefügt	M. Schoen
55	6.8.25	2.33	3	Inventar-Feld «Double Attached Node» hinzugefügt	N. Perrenoud
56	8.1.26	2.34	5	Inventar-Feld «Richtliniengruppe» hinzugefügt	N. Perrenoud
57	20.4.26	2.35	3	Inventar-Feld «Aktivierung EPC Scan» entfernt	N. Perrenoud
58	27.5.26	2.35	3	Inventar-Feld-Name «Zusatzinformationen» durch «Attribute» ersetzt	N. Perrenoud
59	20.8.26	2.35	3	Inventar-Felder «Identitätstyp», «EAP Username» hinzugefügt	N. Perrenoud

Copyright © 2026 United Security Providers AG. All rights reserved.

2 Einführung

2.1 Ausgangslage

Das Network Authentication System (USP NAS) von United Security Providers verhindert den Anschluss von unerlaubten Endgeräten mit Ethernet-Schnittstelle an das Firmennetzwerk.

2.2 Hauptmerkmale von USP NAS

USP NAS überwacht mittels SNMP die Netzwerkgeräte und ermittelt beim Anschluss eines Clients die MAC-Adresse (Ethernet-ID) des Endgeräts. Ändert sich der Status eines überwachten Ports, wird USP NAS mittels SNMP-Trap benachrichtigt, so dass eine rasche Erkennung des neuen Zustands gewährleistet ist.

Das System sammelt die ermittelten Informationen in der USP NAS-Datenbank, was eine jederzeit aktuelle Übersicht der Endgeräte ermöglicht:

- Auflisten aller Geräte, welche im Netzwerk gesehen wurden
- Aufzeigen der Geräte, die zum aktuellen Zeitpunkt im Netz aktiv sind
- Ermöglicht die Abfrage der folgenden Detailinformationen: MAC-Adresse, Switchport, VLAN, Standort des Netzwerkgeräts, Zeitpunkt der letzten Aktivität auf dem Netz, benutzte IP-Adressen des Clients sowie die dazu passenden DNS-Hostnamen.

USP NAS überprüft laufend, ob die aktiven Geräte als erlaubte Clients eingestuft werden können. Der Entscheid basiert auf einem flexibel definierbaren Regelwerk. Das Netzwerk kann in verschiedene Portgruppen aufgeteilt werden. In Abhängigkeit vom Typ des Clients, seinem Status im Inventar und dem Ort des Anschlusses kann das Gerät als erlaubt oder nicht erlaubt behandelt werden.

Es stehen verschiedene Möglichkeiten zur Auswahl, um auf den Anschluss von nicht erlaubten Geräten zu reagieren:

- Automatisches und sofortiges Sperren des Zugangs zum Netzwerk
- Eintragen des Geräts in eine Worklist, welche durch einen Network-Operator behandelt wird (manueller Entscheid)
- Reines Monitoring der Vorgänge auf dem Netzwerk

Alle relevanten Ereignisse werden vom System geloggt. Die Informationen in der USP NAS-Datenbank ermöglichen die Erstellung von Reports über die Aktivitäten im Netzwerk und über die erkannten Endgeräte.

2.3 Systemübersicht USP NAS

Abbildung 1 zeigt die Schnittstellen von USP NAS zu den umliegenden Systemen:

Copyright © 2026 United Security Providers AG. All rights reserved.

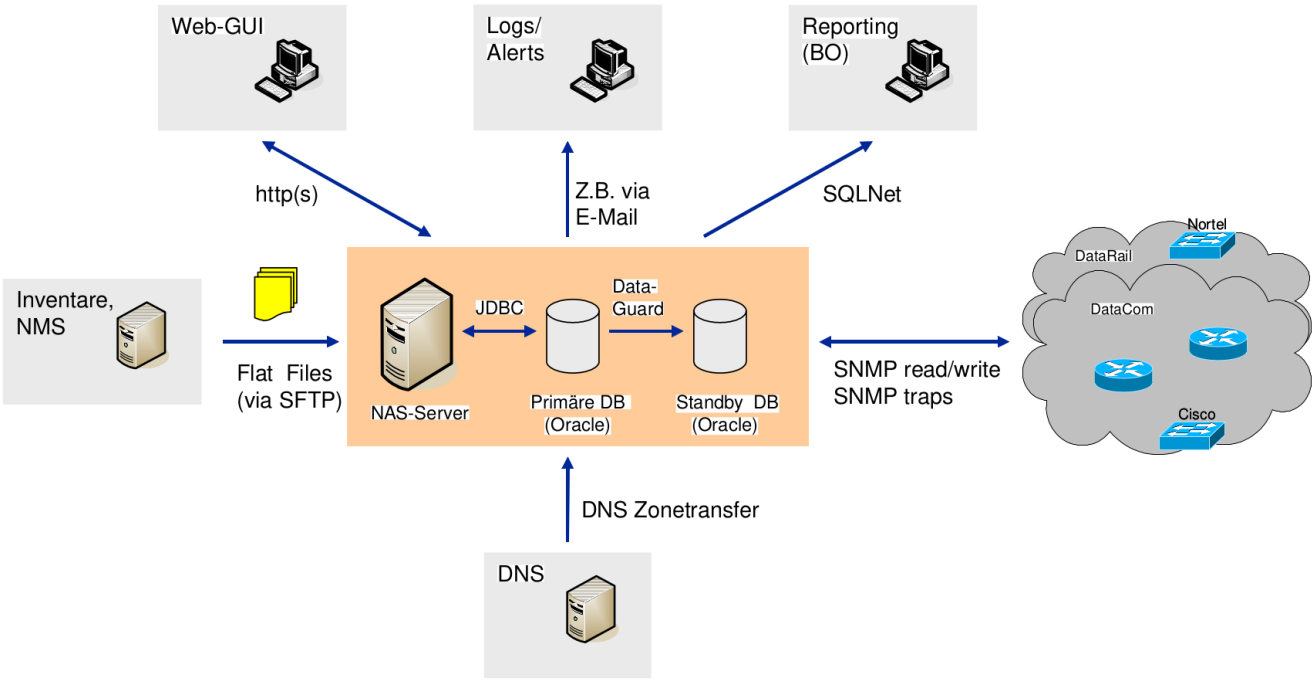

Figure 1: Abbildung 1: Schnittstellen von USP NAS

Auf die Netzwerkgeräte wird mittels SNMP zugegriffen, USP NAS empfängt zusätzlich auch SNMP-Traps von den Switches.

Inventarsysteme und NMS liefern Daten in Form von CSV-Flat-Files an USP NAS. Die Dateien werden via SFTP (SSH File Transfer Protocol) auf den USP NAS-Server übertragen.

USP NAS kann den auf dem Netzwerk ermittelten IP-Adressen den entsprechenden DNS-Hostname zuordnen. USP NAS bezieht die dafür notwendigen Informationen durch periodische Zonentransfers vom DNS und vermeidet dadurch eine übermässige Belastung des DNS-Servers durch Einzelabfragen.

2.4 Zweck des Dokuments

Das vorliegende Dokument „Inventarimport und NMS-Import“ beschreibt den technischen Ablauf des Importprozesses sowie das Datenformat der zu importierenden CSV-Dateien.

2.5 Geschlechtsneutrale Formulierungen

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsneutrale Differenzierung, z.B. Benutzer/innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich immer für beide Geschlechter.

Copyright © 2026 United Security Providers AG. All rights reserved.

3 Schnittstelle für den Datenimport in USP NAS

3.1 Ausgangslage

Über die Datenimport-Schnittstelle bezieht USP NAS die folgenden Informationen:

- Aus Inventarsystemen: die **registrierten Geräte** mit ihren MAC-Adressen
- Aus NMS-Systemen:
  - Zu überwachenden **Netzwerkgeräte** (Routers, Switches)
  - **Netzwerkports** (Ports, welche für die Verbindung zwischen Netzwerkgeräten verwendet werden, zum Beispiel Uplink Ports)
  - **Portkonfiguration** (erlaubte Geräteklasse an einem Port)
  - **Portgruppen**-Zugehörigkeit der Ports
- Aus Device Management Systemen: **Geräte-Profile** für das Endpoint Profiling Modul USP NAS

Für beide Arten von Informationen wird dieselbe technische Schnittstelle verwendet, welche grundsätzlich auf der Übertragung von CSV-Dateien zwischen dem Quellsystem und USP NAS aufbaut.

3.2 Datentransfer

Der Ablauf des Datentransfers ist in Abbildung 2 schematisch dargestellt. Das Quellsystem erzeugt das CSV-Datenfile (1), berechnet den MD5-Hash (*Message Digest Algorithm 5*) der CSV-Datei und speichert die MD5-Prüfsumme in der MD5-Datei (2).

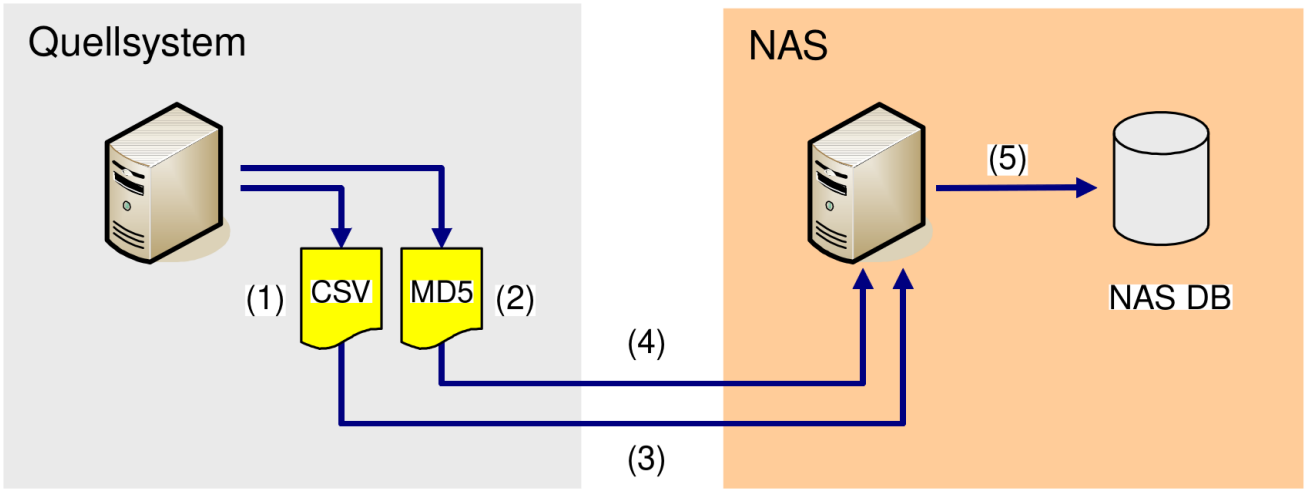

Figure 2: Abbildung 2: Ablauf des Datentransfers

Beide Dateien werden danach vom Quellsystem mittels SFTP (SSH File Transfer Protocol) in ein Verzeichnis direkt auf dem USP NAS-Server übertragen. Zur Authentisierung werden technische User für die Quellsysteme angelegt (für jedes Quellsystem ein eigener technischer User). Falls notwendig, werden auf Firewalls Punkt-zu-Punkt Verbindungen zwischen Quellsystem und USP NAS eingerichtet (TCP-Port 22).

Copyright © 2026 United Security Providers AG. All rights reserved.

Die Quellsysteme sind verpflichtet, zuerst die CSV-Datei vollständig zu übertragen (3) und erst danach die Datei mit der MD5-Prüfsumme (4). Bei Vorhandensein einer MD5-Datei darf also davon ausgegangen werden, dass eine dazu passende CSV-Datei zum Laden bereitsteht.

USP NAS prüft den Inhalt des Verzeichnisses in regelmässigen Intervallen (alle 60 Sekunden). Sind Dateien vorhanden, welche der Namenskonvention (siehe Abschnitt 2.3) entsprechen, so werden sie von USP NAS bearbeitet. USP NAS berechnet dabei zuerst die MD5-Prüfsumme der CSV-Datei und vergleicht sie mit der Prüfsumme aus der MD5-Datei. Stimmen die Prüfsummen überein, werden die Daten aus der CSV-Datei geladen und beide Dateien (CSV-Datei und MD5 Datei) nach erfolgter Verarbeitung entfernt.

3.3 Dateinamen

Die Namenskonvention sieht vor, dass die Namen der CSV-Dateien aus verschiedenen Feldern gebildet werden, welche durch Underscores getrennt werden:

`INHALT_QUELLE_MODUS_YYYYMMDDHHMMSS_VERSION.csv`

Die Bedeutung der verschiedenen Felder wird in Tabelle 1 näher erläutert.

Table 3: Tabelle 1: Bedeutung der Felder in den CSV-Dateinamen (Versionsangabe optional)

Feld	**Beschreibung**	**Werte**
INHALT	Handelt es sich um Informationen aus einem Inventarsystem, einem NMS (Netzwerkscope), Netport Informationen aus einem NMS oder Endpoint Profiling?	INVENTAR NMS NETPORTS PORTCONFIG PORTGROUP PROFILERCOMBINATIONS PROFILERDEVICES PORTCONFIG PORTGROUP DNS EPD
QUELLE	Der eindeutige Name des Quellsystems (wird bei der Anbindung eines neuen Quellsystems festgelegt, beinhaltet grundsätzlich: Kürzel des Providers, des Inventarsystems und des Mandanten).	Beispiele: SCIS-SC-BB TSS-AC-TS
MODUS	Handelt es sich um einen *Full-Export* oder um einen *Delta-Export*? (Full/Delta: siehe Abschnitt 2.5)	FULL DELTA
YYYYMMDDHHMMSS	Timestamp des Exports (gemäss Quellsystem)	Beispiel: 20061012172959
VERSION	Version der Importdatei (optional)	Beispiel: v2 Default = keine Versionsangabe

Als Beispiel hier der vollständige Dateiname eines Delta Exports aus dem Inventarsystem ABC-SC-BB, welcher am 12. Oktober 2006 um 17:29:59 Uhr vom Quellsystem erzeugt wurde:

`INVENTAR_ABC-SC-BB_DELTA_20061012172959.csv`

Copyright © 2026 United Security Providers AG. All rights reserved.

Sind mehrere Dateien von einem Quellsystem im Verzeichnis, so werden sie in zeitlich aufsteigender Reihenfolge geladen.

USP NAS speichert bei allen importierten Daten die Quelle in einem Datenbankfeld, so dass bei jedem Datensatz nachvollzogen werden kann, aus welchem Quellsystem er geliefert wurde.

USP NAS kann entweder mit einer Versionsangabe oder ohne arbeiten. Beispiel einer Datei mit Versionsnamen könnte folgendermassen aussehen:

`INVENTAR_ABC-SC-BB_DELTA_20061012172959_v2.csv`

oder

`INVENTAR_ABC-SC-BB_DELTA_20061012172959.csv`

Die MD5-Datei einer CSV-Datei hat den identischen Namen, aber es wird die Dateiendung .md5 anstatt .csv verwendet. Die MD5-Datei im oben genannten Beispiel würde also wie folgt heissen:

`INVENTAR_SCIS-SC-BB_DELTA_20061012172959.md5`

oder

`INVENTAR_SCIS-SC-BB_DELTA_20061012172959_v2.md5`

Eine MD5-Datei besteht aus einer Zeile mit dem folgenden Inhalt:

`<md5> <Dateiname>`

Es steht dabei `<md5>` für die MD5 Prüfsumme, welche als 32-stellige Hexadezimalzahl dargestellt wird, und `<Dateiname>` für den Namen der CSV-Datei.

Zwischen `<md5>` und `<Dateiname>` befinden sich exakt zwei Leerzeichen („Space“, ASCII Hex-Code: 0x20).

Der Inhalt der MD5-Datei könnte also beispielsweise wie folgt aussehen:

```
c5383772d856be5ebf23351a4ac62735 INVENTAR_SCIS-SC-BB_DELTA_20061012172959.csv
```

Dies entspricht genau dem Output des weit verbreiteten Tools „md5sum“.

3.4 Dateiformat

CSV-Dateien sollen die Zeichencodierung gemäss ISO-8859-1 verwenden. Das Zeilenende wird durch das ASCII-Zeichen *LF* („Line Feed“, Hex-Code 0x0A) signalisiert.

Als Trennzeichen der Felder wird das ASCII-Zeichen *RS* („Record Separator“, Hex-Code 0x1E) verwendet, um Konflikte mit Zeichen, welche in den Feldern vorkommen, möglichst ausschliessen zu können.

Die erste Zeile jeder CSV-Datei enthält keine Daten, sondern die Namen der Felder.

3.4.1 Spezifischer Record-Separator

Optional kann in der Datei ein spezifisches Spalten-Trennzeichen gesetzt werden, welches sowohl das Standard *RS* („Record Separator“, Hex-Code 0x1E) wie auch die globale Konfiguration (→ kann über das USP NAS WebGUI gesetzt werden) übersteuert.

Hierzu wird als erste Zeile in der import Datei (vor der Zeile mit den Spaltennamen) das Trenn-Zeichen festgelegt. Das Format muss folgendem Aufbau entsprechen damit es korrekt erkannt wird: SEPARATOR:<WERT>

Beispiel:

SEPARATOR:#

Copyright © 2026 United Security Providers AG. All rights reserved.

3.5 Full Import und Delta Import

Es sind zwei unterschiedliche Modi des Datenimports möglich:

1. *FULL*: Der Inhalt der Datei stellt einen kompletten Auszug der entsprechenden Daten aus dem Quellsystem dar. Der Inhalt der Datei ersetzt folglich alle bereits vorhandenen Datensätze von diesem Quellsystem. Nicht mehr in der Datei vorhandene Datensätze, welche vom entsprechenden Quellsystem stammen, werden dabei gelöscht.
2. *DELTA*: Der Inhalt der Datei beinhaltet nur ein Subset aller Datensätze, und zwar nur neue oder geänderte Datensätze.

Die Import-Schnittstelle ist so gestaltet, dass eine flexible Anpassung der Importfrequenzen an die Bedürfnisse möglich ist: so kann ein Quellsystem beispielsweise einmal täglich ein FULL-Update bereitstellen und zusätzlich geänderte Datensätze ad-hoc per DELTA-Update übermitteln.

Ein Quellsystem sollte nicht mehr als ca. 6 Full Imports in 24 Stunden übermitteln. Sind häufigere Updates notwendig, kann dies mittels DELTA Dateien erfolgen.

3.6 Überprüfung des Inhalts

Als Erstes wird der MD5-Hash der CSV-Datei berechnet und mit der MD5 Prüfsumme aus der MD5 Datei verglichen. Stimmen die Summen nicht überein, wird die Datei nicht geladen.

Der Inhalt der CSV-Datei (sprich: alle Zeilen ausser der ersten Zeile) wird von USP NAS zusätzlich mittels einer konfigurierbaren Regular Expression überprüft. Zeilen, welche nicht dem vereinbarten Format entsprechen, werden verworfen.

Weist eine Datei mit Importmodus *FULL* zu viele verworfene Datensätze auf (mehr als 10%), dann wird die gesamte CSV-Datei als inkorrekt betrachtet und nicht geladen. Die Prozentzahl bezieht sich dabei auf die Anzahl von Zeilen mit ungültigem Format, bezogen auf die gesamte Anzahl von Records der zu importierende Datei. Es wird kein Vergleich der Anzahl bereits in der Datenbank vorhandenen Records und der zu ladenden Records gemacht.

Erfolgreiche wie auch fehlgeschlagene Ladevorgänge werden von USP NAS geloggt.

3.7 Konflikte zwischen Quellsystemen

Wird ein Konflikt zwischen zwei Quellsystemen festgestellt (eine Quelle liefert einen Datensatz, welcher bereits aus einem anderen Quellsystem geliefert wurde), dann überschreiben die neu angelieferten Daten die bereits vorhandenen Daten.

Der Konflikt wird von USP NAS im Log festgehalten, so dass eine Abklärung der Ursachen durchgeführt werden kann.

Copyright © 2026 United Security Providers AG. All rights reserved.

4 Daten aus Inventarsystemen

4.1 Format einer Datenzeile

Im Fall eines Endgeräte-Inventarimports erwartet USP NAS die in Tabelle 2 aufgeführten Daten:

Table 4: Tabelle 2: Datenzeile für Inventar-Import

Feld	Beschreibung	Obligatorisch	Code	Werte
1	Asset-ID	Ja	NI	Beispiel: AC1000000004711
2	Parent Asset-ID	Ja	NI	Beispiel: AC1000000004712
3	Offizieller DNS-Name des Geräts	Nein	ZN	Beispiel: testsrv.firma.ch (Notation: korrekter DNS-Name)
4	MAC-Adresse (sofern bereits vorhanden)	Nein	ZN	Beispiel: 001143b47ae2
5	Darf das Gerät an das Netzwerk angeschlossen werden?	Ja	ZN	`0` (bedeutet „Nein“) `1` (bedeutet „Ja“)
6	Wird nicht mehr verwendet. Früher: Status gemäss Inventar	Nein	ZN	Wird nicht mehr verwendet und sollte leer gelassen werden.
7	Wird nicht mehr verwendet. Früher: Restriktionen bezüglich des Anschlusses des Geräts	Nein	ZN	Wird nicht mehr verwendet und muss leer gelassen werden.
8	Gerätetyp	Nein	NI	Freitextfeld Beispiele: DELL Latitude D620 DELL Inspiron 8200 Lexmark C734dn
9	Geräteklasse	Nein	NI	Freitextfeld Beispiele: Server Desktop Printer
10	Standort	Nein	EN	Standort
11	Owner (Organisationseinheit, welcher das Gerät gehört)	Nein	EN	Beispiel: IT-TEST-GRP
12	Wird nicht mehr verwendet. Früher: Compliant VLAN	Nein	ZN	Wird nicht mehr verwendet und sollte leer gelassen werden.
13	Mandant	Nein	NI	Textfeld. Der Mandantenname muss vorgängig in USP NAS erfasst werden. Ansonsten wird keine Verknüpfung gemacht
14	Wird nicht mehr verwendet. Früher: Aktivierung EPC-Scan	Nein	ZN	Wird nicht mehr verwendet und sollte leer gelassen werden.

Copyright © 2026 United Security Providers AG. All rights reserved.

Table 4: (continued)

Feld	Beschreibung	Obligatorisch	Code	Werte
15	Attribute	Nein	ZN	Textfeld. Hier können beliebig viele Key/Value Paare aufgelistet werden, die eine Zusatzinformation (Attribut) zu diesem Gerät enthalten. Key/Value-Paare werden durch eckige Klammern gekennzeichnet. Der Key wird vom Value mit einem doppelten = Zeichen getrennt (==). Zwischen den Key/Value Paaren muss zudem ein Semikolon stehen (;). Beispiel: `[Key==Value];[Key2==Value2]`
16	Temporär gültig	Nein	ZN	Gültigkeit endet am: YYYYMMDDHHMM Beispiel: 201912112359 Falls das Feld leer ist, gilt unbeschränkte Gültigkeit des Gerätes.
17	Changed by	Nein	NI	Textfeld Bsp. u12345
18	Double Attached Node (DAN)	Nein	NI	`true` `false` (default)
19	Identitätstyp	Nein	ZN	`0` (MAC, default) `1` (EAP LAN) `2` (EAP WLAN)
20	EAP Username	Nein	NI	Beispiel: nb001.example.com, hans@muster.com

Die Bedeutung der Spalte *Code* ist wie folgt:

- ZN: Zwingende Notation. Der Inhalt des Feldes muss sich nach der Beschreibung in der Spalte *Werte* und den Erläuterungen in Abschnitt 3.2 richten.
- NI: Notation gemäss Inventarsystem. Das Feld wird so geliefert, wie es im Inventarsystem geführt wird.
- EN: Empfohlene Notation. Das Feld wird so geliefert, wie es im Inventarsystem geführt wird, die Spalte *Werte* gibt aber eine Empfehlung dazu ab.

4.2 Erläuterungen

Die Felder 12, 13 und 14 sind gänzlich optional. Diese Felder müssen also nicht zwingend in der Importdatei vorhanden sein. Wenn jedoch vorhanden, dann müssen alle Felder existieren (dürfen jedoch leer sein).

4.2.1 Asset-ID

Die Asset-ID ist die eindeutige ID des Geräts („Configuration Item“) im Quellsystem. Kennt das Quellsystem hierarchische Beziehungen (Hauptkomponenten mit Sub-Komponenten), dann kann im Feld *Parent Asset-ID* dargestellt werden, zu

Copyright © 2026 United Security Providers AG. All rights reserved.

welcher Komponente eine Subkomponente gehört. Gibt es keine übergeordnete Komponente, dann haben die Felder *Asset-ID* und *Parent Asset-ID* den identischen Inhalt. Quellsysteme, die keine solchen Hierarchien führen, liefern im Feld *Parent Asset-ID* einfach immer die *Asset-ID*.

In der Importdatei ist die Asset-ID nicht eindeutig, denn wenn ein Asset mehrere Interfaces besitzt, dann wird pro Interface je eine Zeile in die Importdatei geschrieben.

4.2.2 Parent Asset-ID

Die Parent Asset-ID ist der eindeutige Bezeichner eines Assets, das z.B. ein PC darstellt. Ein PC kann mehrere Netzwerkkarten haben. Diese müssten dann mit unterschiedlicher Asset-ID unterschieden werden. Falls im Inventarsystem eine solche Gruppierung (Hierarchie) nicht gemacht wird, dann muss die Parent Asset-ID immer denselben Wert wie die Asset-ID bekommen.

4.2.3 Offizieller DNS-Name des Geräts

Der DNS-Name wird im Moment rein informeller Natur benötigt. Er wird nur für Lookups benötigt, bei dem man die MAC-Adresse noch nicht kennt. Dies ist insbesondere auch gerade im Inventarimportprozess der Fall. Trotzdem muss hier die korrekte Notation verwendet werden. Also: HOSTNAME.DOMAIN.TOPLEVELDOMAIN. wie zum Beispiel in: testserver.testdomain.ch. (Der abschliessende Punkt ist optional, wird aber empfohlen, um den Standard zu befolgen).

4.2.4 MAC-Adresse

Die MAC-Adresse (Feld 2) ist immer exakt 12 Buchstaben lang und darf nur die folgenden Zeichen enthalten: 0-9 und a-f (sprich: keine Grossbuchstaben zur Darstellung der Hexadezimalzahlen und keine Trennzeichen innerhalb der MAC-Adresse).

Die Media-Access-Control-Adresse ist die weltweit eindeutige Nummer einer Netzwerkkarte. Sie wird in USP NAS für die eindeutige Identifizierung eines Hosts benötigt. Anhand dieser MAC-Adresse wird dann entschieden, dass dieses Gerät im Netzwerk zugelassen oder (falls nicht autorisiert) gesperrt wird.

4.2.5 Darf das Gerät an das Netzwerk angeschlossen werden?

Ist die Information, ob ein Gerät das Netzwerk verwenden darf, im Inventarsystem nicht geführt, dann kann im Feld 3 systematisch der Wert 1 verwendet werden.

Dieses Feld wird benötigt, um die zugehörige MAC-Adresse im Netzwerk zuzulassen (Wert = 1) oder zu sperren (Wert = 0).

4.2.6 Status gemäss Inventar

Status gemäss Inventar (Feld 4) wird in immer leer gelassen, weil es obsolet ist und nicht mehr verwendet wird.

4.2.7 Restriktionen

Restriktionen (Feld 5) wird in immer leer gelassen, weil es obsolet ist und nicht mehr verwendet wird.

4.2.8 Gerätetyp

Frei wählbarer Gerätetyp. Meist wird hier der Herstellerspezifische Gerätetyp angegeben wie z.B. DELL Latitude D610.

Copyright © 2026 United Security Providers AG. All rights reserved.

4.2.9 Geräteklasse

Frei wählbare Geräteklasse. Meist wird hierfür ein Oberbegriff für den Gerätetypen verwendet wie z.B. Notebook, Printer, Server usw.

4.2.10 Standort

Die Standortinformation, welche aus dem Inventarsystem kommt. Diese Info wird in USP NAS nicht benötigt und ist rein informativ.

4.2.11 Owner

Der Eigentümer des Gerätes. Dies kann z.B. eine Abteilung oder eine Person sein. Diese Info wird in USP NAS nicht benötigt und ist rein informativ.

4.2.12 Produktiv VLAN

Produktiv VLAN (Feld 12) wird in immer leer gelassen, weil es obsolet ist und nicht mehr verwendet wird.

4.2.13 Mandant

Dieses Feld ist optional. Wenn es angegeben wird, muss jedoch zwingend das Feld 12 (Produktiv VLAN) in der Datenzeile vorhanden sein (leerer Inhalt)!

Der Mandant wird einem Gerät nur zugewiesen, wenn er vorgängig in USP NAS erfasst wurde. Dabei muss der Mandantenname, der in USP NAS verwendet wird, mit dem aus der Importdatei übereinstimmen. Falls der Mandant in USP NAS noch nicht erfasst wird, wird dieses Feld in der Datenbank leer gelassen und das Gerät dem Default Mandant zugeordnet.

4.2.14 Aktivierung EPC-Scan

Aktivierung EPC-Scan (Feld 14) wird in immer leer gelassen, weil es obsolet ist und nicht mehr verwendet wird.

4.2.15 Zusatzinformationen

Dieses Feld ist optional. Wenn es angegeben wird, muss jedoch zwingend auch das Feld 12 bis 14 in der Datenzeile vorhanden sein!

Diese Zusatzinformationen werden im USP NAS WebGUI eins zu eins wiedergeben. Das heisst, der Key und der Value werden nicht mehr formatiert, sondern gerade so ausgegeben, wie sie hier aufgelistet sind.

Key/Value Paare werden durch eckige Klammern gekennzeichnet. Der Key wird vom Value mit einem Doppelten = Zeichen getrennt (==). Zwischen den Key/Value Paaren muss zudem ein Semikolon stehen (;).

4.2.16 Gültigkeit Temporär

Dieses Feld ist optional. Wenn es angegeben wird, muss zwingend auch das Feld 12 bis 15 in der Datenzeile vorhanden sein.

Ein Eintrag im Feld definiert eine beschränkte Gültigkeit des Records. Das Gerät ist nur bis zum angegebenen Zeitpunkt als Gültig, danach gilt das Gerät als gelöscht.

Der Wert muss dem Format YYYYMMDDHHMM entsprechen. Ein Beispiel für einen gültigen Wert: 201912112359.

Copyright © 2026 United Security Providers AG. All rights reserved.

4.2.17 Changed by

Dieses Feld ist optional. Mit dem Feld kann angegeben werden, durch wen der Eintrag als letztes geändert/gespeichert wurde.

4.2.18 Double Attached Node (DAN)

In Hochverfügbarkeitsnetzen mit nahtloser Redundanz (High Availability Seamless Redundancy, HSR) ist ein Double Attached Node (DAN) ein Gerät, das zwei Netzwerkanschlüsse zur Redundanz nutzt. Diese Knoten sind entscheidend für die Schaffung einer Ringtopologie, in der Daten in beide Richtungen übertragen werden, um einen kontinuierlichen Betrieb zu gewährleisten, selbst wenn ein Pfad ausfällt.

USP NAS wird für DAN-Geräte keine Event-Nachricht `[1101] MAC found on multiple devices` auslösen, wenn dies entsprechend im Inventar markiert wird.

4.3 Beispiel

Beispiel für Dateinamen: `inventar_demo_full_20260501121401.csv`:

Minimales Beispiel:

```
SEPARATOR:,
asset id,parent asset id,client name (DNS),mac address,authorized
AC0001,AC0001,notebook001.example.com,123456789afe,1
AC0002,AC0002,notebook002.example.com,123456789aff,1
```

Erweitertes Beispiel:

```
SEPARATOR:,
asset id,parent asset id,client name,mac address,authorized,,,asset type,asset class, ↩
    location,owner,,tenant,,attributes,valid until
AC0003,AC0003,guest01.example.com,123456789abc,1,,,Laptop,BYOD,Bern,Hans Muster,,,,[Key== ↩
    Value];[Key2==Value1],202612112359
```

4.4 Geräte mit mehreren MAC-Adressen

Hat ein Gerät mehr als eine MAC-Adresse, dann sollen alle MAC-Adressen an USP NAS geliefert werden. In der CSV-Datei erscheinen in einem solchen Fall für ein Gerät mehrere Zeilen mit den verschiedenen MAC-Adressen des Geräts.

Liefert ein Inventarsystem hingegen dieselbe MAC-Adresse im selben Export mehr als einmal, dann wird dies von USP NAS als Fehler angesehen. Diejenige MAC-Adresse, welche zuerst gefunden wurde, wird beibehaltet, alle nachfolgenden werden verworfen. Die verworfenen Zeilen werden im Log festgehalten.

4.5 Komplette Assets pro Import

USP NAS nimmt an, dass die Assets in Full Imports immer komplett geliefert werden (ausgenommen bei Delta Imports). Ein Asset kann dabei aus 1 bis n Netzwerkinterfaces bestehen. Interfaces eines Assets müssen getrennt in einer eigenen Zeile stehen (zusammen mit den Assetinformationen). Daraus resultiert, dass ein komplettes Asset aus 1 bis n Zeilen besteht.

Copyright © 2026 United Security Providers AG. All rights reserved.

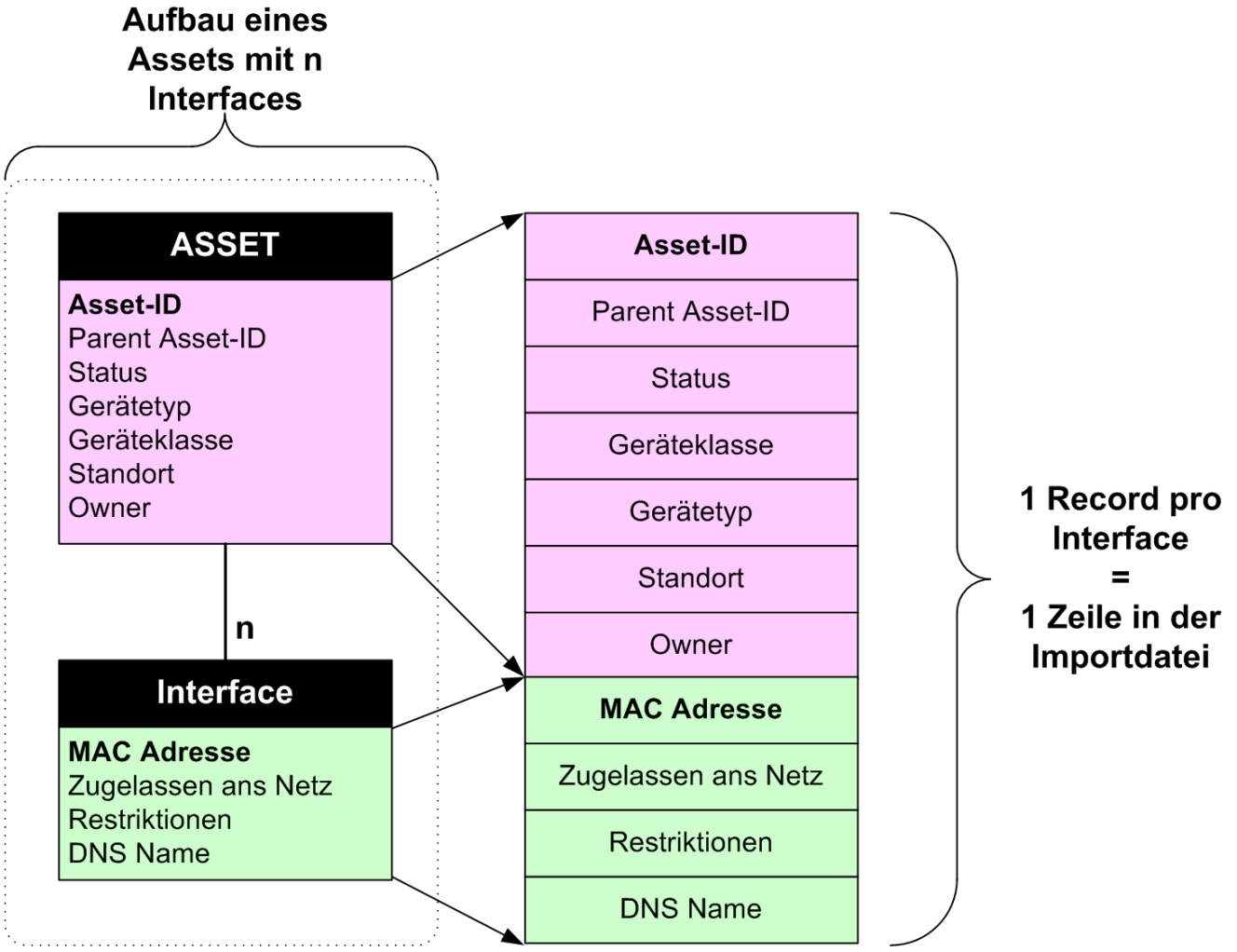

Figure 3: Abbildung 3: Zusammensetzung einer Datenzeile

Ein Asset wird eindeutig durch die Asset-ID und das zugehörige Inventarsystem (Quelle) gekennzeichnet. Das Interface wird eindeutig durch die gesetzte MAC-Adresse. Dies führt dazu, dass ein Interface immer eine MAC-Adresse beinhalten sollte. Falls es zwei Interfaces ohne MAC-Adresse gibt, so sollten sie sich in mindestens einem Attribut unterscheiden. Sonst muss USP NAS annehmen, dass ein Duplikat vorhanden ist und löscht eines der Interfaces aus dem Asset.

Ein Record (eine Datenzeile in der Importdatei) besteht aus einem Teil, der das Asset beschreibt, und einem Teil der spezifisch nur das Interface beschreibt. Ein Asset wird dabei durch die Asset-ID gekennzeichnet. Falls mehrere Records dieselbe Asset-ID haben, so gehören sie zu demselben Asset. Die übrigen Attribute des Assets sollten idealerweise für jedes Interface (eine Zeile in der Importdatei) dieselben sein, USP NAS kümmert sich jedoch nicht um Widersprüche innerhalb eines Assets und importiert sie wie sie sind.

Copyright © 2026 United Security Providers AG. All rights reserved.

1 komplettes Asset
(mit 3 Interfaces)

Asset-ID	Parent Asset-ID	Status	Geräteklasse	Geräte-typ	Stand-ort	Owner	DNS Name	MAC Adresse	Zuge-lassen	Restriktionen
A1	A1	AKTIV	HOMOLOGIERT	Server	Bern	Hans	server.test.ch		**1**	
A1	A1	AKTIV	HOMOLOGIERT	Server	Bern	Hans	server.test.ch	**00bb00bb00bb**	**1**	
A1	A1	AKTIV	HOMOLOGIERT	Server	Bern	Hans	server.test.ch	**00cc00cc00cc**	**1**	
A2	A2	AKTIV	HOMOLOGIERT	Printer	Bern	Peter	printer.test.ch	**00dd00dd00dd**	1	IP=192.168.1.40
A3	A3	AKTIV	HOMOLOGIERT	PC	Bern	Fritz	pc1.test.ch	**00ee00ee00ee**	0	

Figure 4: Abbildung 4: Ein komplettes Asset mit mehreren Interfaces

Wird beim Einlesen der Importdatei ein fehlerhafter Record entdeckt wird er aus dem Import entfernt und eine entsprechende Logmeldung generiert. Somit kann es vorkommen, dass ein Asset aus Sicht des Inventarsystems nicht mehr komplett ist, von USP NAS aus gesehen jedoch schon. Sobald der Record bei einem darauffolgenden Import gelesen werden kann, ohne verworfen zu werden, wird auch das Asset aus Sicht des Inventarsystems wieder komplett geladen.

Ein Asset kann mehrere Interfaces ohne MAC-Adresse beinhalten, jedoch müssen sich die anderen Attribute unterscheiden.

4.6 Gleiche MAC-Adresse aus verschiedenen Inventarsystemen

Falls ein Asset mit einer schon im USP NAS bestehender MAC-Adresse aus einem anderen Inventarsystem geliefert wird, überschreibt der neue Record den Alten. Beim schon bestehenden Record wird dabei die MAC-Adresse gelöscht und der UPDATED Timestamp auf dem ganzen Asset gesetzt.

4.7 Funktionsweise Full Import

In die Datenbank werden immer die kompletten Assets geladen. Inklusive Dateinzeilen, welche keine MAC-Adresse und somit keine eindeutigen Interface-Informationen beinhalten. Damit ist sichergestellt, dass auch Assets mit mehreren leeren MAC-Adressen immer komplett geladen werden.

Bei einem Full Import werden alle Assets logisch gelöscht, welche nicht mehr im Import vorhanden sind. Gelöscht wird mit dem Setzen des DELETED Timestamps in der Datenbank, die Assets werden also nicht per DB CleanUp entfernt, sondern bleiben bestehen, werden aber von USP NAS ausgeblendet und als nicht existent behandelt.

Beim erstmaligen Erstellen eines Assets wird der CREATED Timestamp gesetzt und wird nicht mehr verändert, auch wenn der DELETED Timestamp gesetzt wurde.

Bestehende Records werden aktualisiert, falls etwas im selben Asset geändert hat. Ist also mindestens eine Zeile eines Assets verändert im Import erschienen, wird das gesamte Asset upgedatet. Geprüfte Veränderungen sind fehlende oder hinzugefügte Records (Anzahl der Records stimmt nicht mit dem alten Stand der Datenbank überein), oder mindestens ein Attribut einer beliebigen Zeile des Assets hat den Wert geändert.

Falls ein Asset nicht dieselbe Anzahl Interfaces hat wie beim letzten Update, werden die überflüssigen Interfaces per DB CleanUp gelöscht oder fehlende Interfaces hinzugefügt. Beim Update wird immer der UPDATED Timestamp neu gesetzt und für die neuen Interfaces der CREATED Timestamp des Assets übernommen.

Copyright © 2026 United Security Providers AG. All rights reserved.

Falls ein Asset den DELETED Timestamp hat, aber wieder im Import auftaucht, wird der DELETED Timestamp entfernt und der UPDATED Timestamp neu gesetzt.

Wenn eine MAC-Adresse aus dem Import bereits in der Datenbank vorhanden ist, aber einem anderen Asset zugeteilt ist, so wird diejenige in der Datenbank überschrieben, resp. entfernt und eine entsprechende Logmeldung wird generiert.

Copyright © 2026 United Security Providers AG. All rights reserved.

FULL Import
INV_SYSTEM_A

Asset-ID	MAC Adresse
A1	aaaaaa000000
A1	00bb00bb00bb
A2	123456000000
A2	000000654321
A3	111122223333
A4	abcdefabcdef
AY	123abc123abc

NAS Datenbank vor Import

Asset-ID	Source	MAC Adresse	DELETED	UPDATED	CREATED
A1	INV_SYSTEM_A	aaaaaa000000		01.01.2007 12:00:00	01.01.2007 12:00:00
A1	INV_SYSTEM_A	00bb00bb00bb		01.01.2007 12:00:00	01.01.2007 12:00:00
A2	INV_SYSTEM_A	123456000000		01.01.2007 12:00:00	01.01.2007 12:00:00
A3	INV_SYSTEM_A	111122223333		01.01.2007 12:00:00	01.01.2007 12:00:00
A3	INV_SYSTEM_A	333322221111		01.01.2007 12:00:00	01.01.2007 12:00:00
AX	INV_SYSTEM_A	00cc00cc00cc		01.01.2007 12:00:00	01.01.2007 12:00:00
AX	INV_SYSTEM_A	00dd00dd00dd		01.01.2007 12:00:00	01.01.2007 12:00:00
AY	INV_SYSTEM_A	123abc123abc	06.09.2007 15:00:00	06.09.2007 15:00:00	01.01.2007 12:00:00

NAS Datenbank nach Import

Asset-ID	Source	MAC Adresse	DELETED	UPDATED	CREATED
A1	INV_SYSTEM_A	aaaaaa000000		01.01.2007 12:00:00	01.01.2007 12:00:00
A1	INV_SYSTEM_A	00bb00bb00bb		01.01.2007 12:00:00	01.01.2007 12:00:00
A2	INV_SYSTEM_A	000000654321		**13.03.2008 12:00:00**	**01.01.2007 12:00:00**
A2	INV_SYSTEM_A	123456000000		**13.03.2008 12:00:00**	01.01.2007 12:00:00
A3	INV_SYSTEM_A	111122223333		**13.03.2008 12:00:00**	01.01.2007 12:00:00
AX	INV_SYSTEM_A	00cc00cc00cc	**13.03.2008 12:00:00**	**13.03.2008 12:00:00**	01.01.2007 12:00:00
AX	INV_SYSTEM_A	00dd00dd00dd	**13.03.2008 12:00:00**	**13.03.2008 12:00:00**	01.01.2007 12:00:00
A4	INV_SYSTEM_A	abcdefabcdef		**13.03.2008 12:00:00**	**13.03.2008 12:00:00**
AY	INV_SYSTEM_A	123abc123abc		**13.03.2008 12:00:00**	01.01.2007 12:00:00

1 Interface zum Asset hinzugefügt mit Created Timestamp vom Asset

1 Interface vom Asset entfernt

Asset nicht in Import, daher Deleted

1 Asset hinzugefügt

Deleted Timestamp entfernt, da Asset bereits in der DB vorhanden (aber logisch gelöscht) war

Figure 5: Abbildung 5: Diverse Fälle im Full Import

Copyright © 2026 United Security Providers AG. All rights reserved.

FULL Import

Asset-ID	Source	MAC Adresse
A1	**INV_SYSTEM_A**	**aaaaaa000000**
A1	INV_SYSTEM_A	00bb00bb00bb

NAS Datenbank vor Import

Asset-ID	Source	MAC Adresse
A1	INV_SYSTEM_A	
A1	INV_SYSTEM_A	00bb00bb00bb
A2	**INV_SYSTEM_B**	**aaaaaa000000**
A2	INV_SYSTEM_B	00cc00cc00cc

NAS Datenbank nach Import

Asset-ID	Source	MAC Adresse
A1	**INV_SYSTEM_A**	**aaaaaa000000**
A1	INV_SYSTEM_A	00bb00bb00bb
A2	**INV_SYSTEM_B**	
A2	INV_SYSTEM_B	00cc00cc00cc

Figure 6: Abbildung 6: Full Import inkl. Überschreibung der MAC-Adresse in anderem Asset

4.8 Funktionsweise Delta Import

Beim Delta Import werden nur die einzelnen Records geladen und nicht die kompletten Assets. Falls ein Record keine MAC-Adresse beinhaltet, so wird dieser ignoriert. Geladen werden ausschliesslich nur Records mit MAC-Adressen.

Wenn eine MAC-Adresse aus dem Import bereits in der Datenbank vorhanden ist, wird diese mit NULL überschrieben. Und der UPDATED Timestamp gesetzt. Danach wird der Record aus dem Import mit einem Insert in die Datenbank geladen.

Standardmässig wird ein Delta Import immer per Insert in die Datenbank geladen. Dabei wird der CREATED und UPDATED Timestamp nur auf diesem Record gesetzt.

Einzige Ausnahme ist, wenn die vorhandene MAC-Adresse demselben Asset zugeordnet ist wie im Import. In diesem Fall wird ein Update durchgeführt und nur der UPDATED Timestamp gesetzt.

Der CREATED Timestamp eines per Delta Import geladenen Records ändert sich nicht, bis das zugehörige Asset bei einem Full Import zusätzliche Änderungen zum Delta Import und den schon bestehenden Daten aufweist und neu geladen wird.

Copyright © 2026 United Security Providers AG. All rights reserved.

DELTA Import

Asset-ID	Source	MAC Adresse
A1	**INV_SYSTEM_A**	**aaaaaa000000**

NAS Datenbank vor Import

Asset-ID	Source	MAC Adresse
A1	INV_SYSTEM_A	
A1	INV_SYSTEM_A	00bb00bb00bb
A2	**INV_SYSTEM_B**	**aaaaaa000000**
A2	INV_SYSTEM_B	00cc00cc00cc

NAS Datenbank nach Import

Asset-ID	Source	MAC Adresse
A1	INV_SYSTEM_A	
A1	INV_SYSTEM_A	00bb00bb00bb
A1	**INV_SYSTEM_A**	**aaaaaa000000**
A2	**INV_SYSTEM_B**	
A2	INV_SYSTEM_B	00cc00cc00cc

Figure 7: Abbildung 7: Delta Import inkl. Überschreibung der MAC-Adresse in anderem Asset

Copyright © 2026 United Security Providers AG. All rights reserved.

4.9 Übersicht Ablauf des Inventarimports

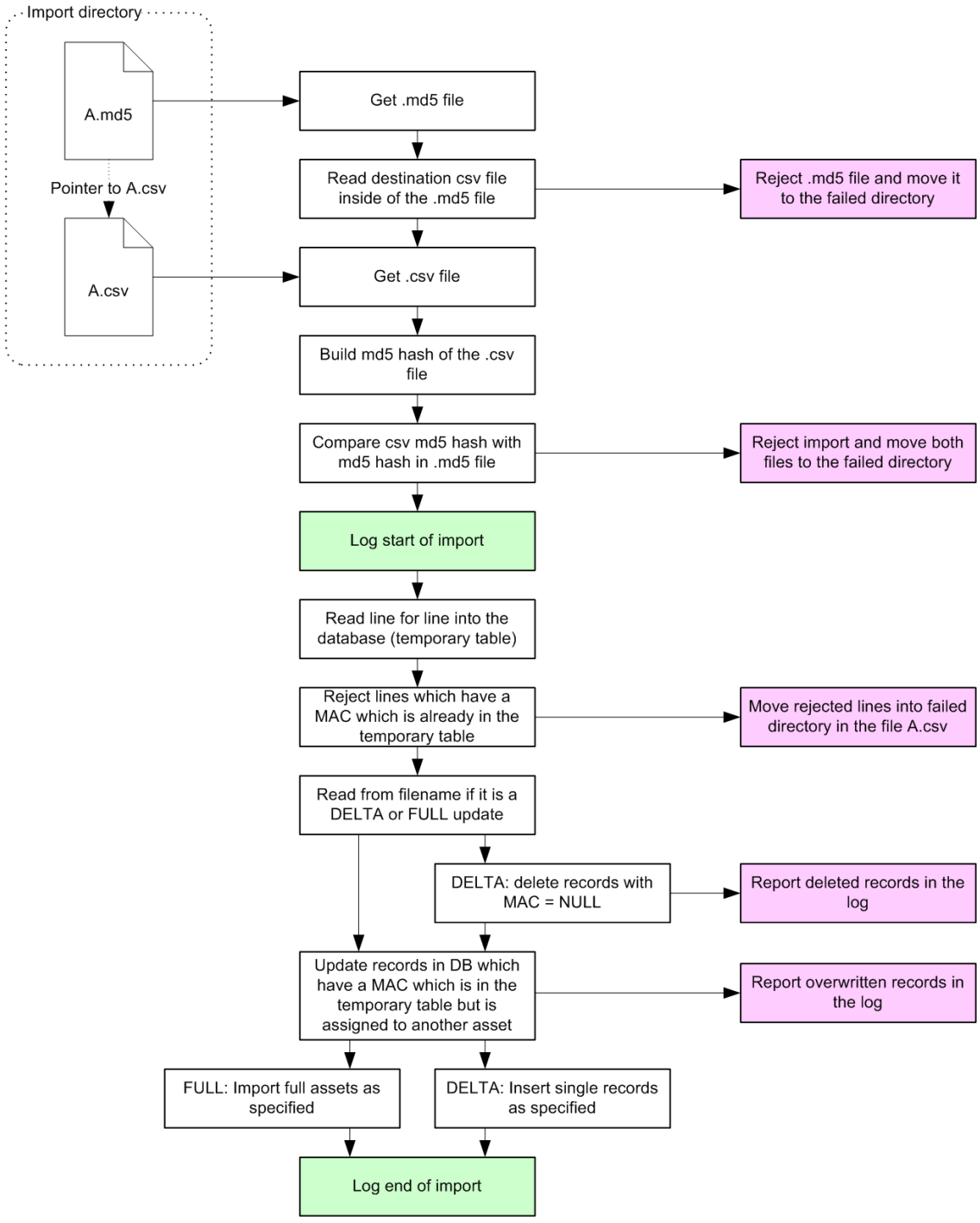

Figure 8: Abbildung 8: Ablauf des Inventarimports

Copyright © 2026 United Security Providers AG. All rights reserved.

5 Daten aus NMS

5.1 Format einer Datenzeile

Für den Import von Netzgeräten (Switche, Router, WLAN Access Points, . . .) werden die in Tabelle 3 aufgeführten Daten erwartet:

Table 5: Tabelle 3: Datenzeile für den Import von Netzgeräten

Feld	Beschreibung	Obligatorisch	Werte
1	Eindeutiger Name des Netzwerkgeräts (DNS-Name)	Ja	Beispiel: BONIN1.firma.ch.
2	IP-Adresse	Ja	Beispiel: 192.168.17.252 2001:db8::1
3	Typ des Netzwerkgeräts	Ja	ROUTER SWITCH ROUTER/SWITCH MPP (deprecated) WLAN WTP RADIUSAUTH

4	SNMP-Version für die Abfrage durch USP NAS	Nein	`1`
			`2c`
			`3_noauth`
			`3_auth_md5`
			`3_auth_sha`
			`3_auth_sha256`
			`3_priv_md5`
			`3_priv_sha`
			`3_priv_aes_md5`
			`3_priv_aes_sha`
			`3_priv_aes_sha224`
			`3_priv_aes_sha256`
			`3_priv_aes_sha384`
			`3_priv_aes_sha512`

5	SNMP Read community	Nein	Beispiel: comm-ro
6	SNMP Write community	Nein	Beispiel: comm-rw
7	Location des Netzwerkgerätes	Nein	Beispiel: 3000 Bern, Musterstr. 10, 3. OG, Raum 10, Schrank 2
8	In Scope (soll das Gerät überwacht werden)	Nein	0 (nicht überwacht) 1 (überwacht) 2 (Wartungsmodus: kein Alert falls per SNMP nicht erreichbar. RADIUS-Anfragen werden verarbeitet)

Copyright © 2026 United Security Providers AG. All rights reserved.

Table 5: (continued)

Feld	Beschreibung	Obligatorisch	Werte
9	Zugangskontrollvariante	Nein	SYSTEMDEFAULT PORTSHUTDOWN (früher SHUTDOWN) BLOCKVLAN (früher VLANMOVE) VLANASSIGNMENT (früher COMPLIANTVLAN und QUARANTINE_PRODUCTIVE_GUEST)
10	MPP-User	Nein	(deprecated)
11	MPP-Passwort	Nein	(deprecated)
12	MPP-Port	Nein	(deprecated)
13	SNMPv3 User	Nein	Beispiel: snmpv3user
14	SNMPv3 Authentication Passwort	Nein	Beispiel: snmpv3authpass
15	SNMPv3 Encryption Passwort	Nein	Beispiel: snmpv3privpass
16	Mandant	Nein	Textfeld. Der Mandantenname muss vorgängig in USP NAS erfasst werden. Ansonsten wird keine Verknüpfung gemacht
17	Benutze für WLAN Controller ACL Filter anstelle von VLAN Enforcements	Nein	0 (benutze VLAN) 1 (benutze ACL-Filter)
18	802.1x Accounting	Nein	0 (Accounting aus) 1 (nur Accounting Stop) 2 (Accounting ein)
19	Disconnect Message Port	Nein	1024 – 65535
20	WTP MAC-Adresse	Nein	Beispiel: 001143b47ae2
21	SSID	Nein	Textfeld
22	L3MODE	Nein	V4, V6, V4V6
23	SNMP-Zugangsprofil	Nein	Textfeld. Das Profil muss vorgängig mit einem eindeutigen Namen im USP NAS WebGUI erfasst werden. Ansonsten wird keine Verknüpfung gemacht. Wenn ein Profil angegeben wurde, werden die Einträge zu SNMP-Version, Community, V3 Username/Passwörter ignoriert.
24	Richtliniengruppe	Nein	Textfeld. Die Richtliniengruppe muss vorgängig mit einem eindeutigen Namen im USP NAS WebGUI erfasst werden. Wenn die Spalte leer gelassen wird, wird die Standardgruppe verwendet.

5.2 Erläuterungen

Der DNS-Name (Feld 1) dient zur Identifizierung des Records. Das heisst, ein Netdevice im Importfile wird immer über den DNS-Namen mit dem schon vorhandenen Record in der DB verglichen und so entschieden, ob ein neues Gerät erstellt werden muss oder das bestehende aktualisiert werden kann.

Copyright © 2026 United Security Providers AG. All rights reserved.

Für die Felder 4 bis 9 gilt: ist das Feld leer, dann werden die konfigurierten Default-Werte verwendet. Beim Feld 8 wird standardmässig 1 (überwacht) und beim Feld 9 wird SYSTEMDEFAULT verwendet.

Die Felder 7, 8, und 9 sind gänzlich optional. Diese Felder müssen also nicht zwingend in der Importdatei vorhanden sein. Wenn jedoch vorhanden, dann müssen alle drei Felder existieren (dürfen jedoch leer sein).

Die Felder 10, 11 und 12 sind ebenfalls optional. Sie müssen aber angegeben werden, wenn das Feld 3 (Typ des Netzwerkgeräts) ‚MPP' ist. Dabei müssen ebenfalls die Felder 7, 8 und 9 in der Importdatei vorhanden sein, dürfen aber leer sein.

Die Felder 13, 14 und 15 sind ebenfalls optional. Falls sie aber angegeben werden, müssen die Felder 7 – 12 ebenfalls in der Importdatei vorhanden sein, dürfen aber leer sein.

Das Feld 16 ist ebenfalls optional. Falls es aber angegeben wird, müssen die Felder 7 – 15 ebenfalls in der Importdatei vorhanden sein, dürfen aber leer sein.

Das Feld 17 ist ebenfalls optional. Falls es aber angegeben wird, müssen die Felder 7 – 16 ebenfalls in der Importdatei vorhanden sein, dürfen aber leer sein.

Das Feld 18 ist ebenfalls optional. Falls es aber angegeben wird, müssen die Felder 7 – 17 ebenfalls in der Importdatei vorhanden sein, dürfen aber leer sein.

Weil USP NAS per Default die Location Info per SNMP-Scan aktualisiert (also den Wert, der auf dem Switch definiert ist, in die Datenbank schreibt), kann man mit einer globalen Einstellung diesen Mechanismus deaktivieren. Danach wird nur noch die Info aus dem Import verwendet. Wird bei aktiviertem SNMP Location Update trotzdem die Location in der Importdatei mitgeliefert, wird diese trotzdem in die Datenbank geschrieben, wird jedoch beim nächsten SNMP-Scan überschrieben.

5.2.1 DNS-Name

Der DNS-Name des Switches/Routers. Er wird verwendet, um den Switch/Router eindeutig zu bezeichnen. Es sollte hier die korrekte Notation verwendet werden. Also: HOSTNAME.DOMAIN.TOPLEVELDOMAIN. wie zum Beispiel in: testserver.testdomain.ch. (Der abschliessende Punkt ist optional, wird aber empfohlen, um den Standard zu befolgen). Es ist jedoch möglich auch simple Namen zu verwenden wie: host1

Dieses Feld wird verwendet, um ein Gerät aus dem Import mit dem aus der DB zu identifizieren. Das heisst, wenn ein Gerät im Import denselben DNS-Namen wie ein Gerät in der DB hat, dann wird das Gerät in der DB durch dieses aus dem Import überschrieben.

5.2.2 IP-Adresse

Die IP-Adresse des Switches oder des Routers auf welchem das SNMP-Management zugelassen ist.

Dieses Feld wird nicht zur Identifizierung verwendet. Das heisst, wenn ein Gerät mit einer gleichen IP-Adresse wie ein anderes das bereits in der DB erfasst ist, jedoch einen anderen DNS-Namen hat, importiert werden soll, wird ein neuer Eintrag in der DB erstellt und das alte Gerät nicht überschrieben.

5.2.3 Typ des Netzwerkgeräts

Der Typ des Netzwerkgeräts kann drei verschiedene Stati annehmen:

Der **SWITCH** ist ein (OSI-)Layer 2 Netzwerkgerät, welcher als Access- (oder in Ausnahmefällen) als Core-Switch benutzt wird. Auf ihm werden die Endgeräte kontrolliert, welche ans Netz angeschlossen sind.

Der **ROUTER** ist ein (OSI-)Layer 3 Netzwerkgerät, welches über Routinginformationen verfügt. Er wird benötigt, um den IP Lookup für gefundene Endgeräte und deren MAC-Adressen zu machen.

Der **ROUTER/SWITCH** ist ein (OSI-)Layer 2/Layer 3 Switch. Das heisst, er verfügt über die Funktionalität eines Switches aber auch die eines Routers. Das heisst, auf einem solchen Gerät werden Scans durchgeführt, IP Lookups gemacht und zusätzlich, wenn Access-Ports definiert sind, auch ein Router Access-Port Scan.

Copyright © 2026 United Security Providers AG. All rights reserved.

Das **WLAN**-Gerät ist typischerweise ein WLAN-Controller oder WLAN-Accesspoint. USP NAS überwacht diese Geräte mittels 802.1x und fungiert dazu als Radius Proxy welcher die VLANs oder Filter-IDs in den Radius-Responses setzen kann.

Das **WTP**-Gerät (Wireless Termination Point) ist typischerweise ein WLAN-Accesspoint, welcher über einen zentralen WLAN-Access-Controller angeschlossen ist und nicht direkt mit USP NAS kommuniziert.

Das **RADIUSAUTH** Gerät ist ein Layer2 allgemein gehaltenes Netzwerkgerät welches als Access-Switch oder auch WLAN-Gerät eingesetzt wird. Für diesem Gerätetyp werden RADIUS-Anfragen beantwortet. Es erfolgt jedoch kein Enforcement über SNMP.

5.2.4 SNMP-Version

Die SNMP-Version mit welcher USP NAS den Scan oder sonstige SNMP-Funktionen durchführt. Empfohlen wird für diesen Punkt, wenn möglich immer die SNMP-Version 2c oder höher zu wählen. Bei fehlender Versionsangabe wird Version 2c verwendet.

Diese Einstellung ist nicht zu verwechseln mit der SNMP-Version der Traps. Denn diese sind unabhängig von dieser hier gemachten Einstellung.

Erläuterungen der Werte:

Konfigurationswert SNMP-Version	Beschreibung
`1`	SNMP v1
`2` oder `2c`	SNMP v2c
`3_noauth`	Keine Authentisierung und keine Verschlüsselung
`3_auth_md5`	Authentisierung über MD5, keine Verschlüsselung
`3_auth_sha`	Authentisierung über SHA, keine Verschlüsselung
`3_auth_sha256`	Authentisierung über SHA 256, keine Verschlüsselung
`3_priv_md5`	Authentisierung über MD5, Verschlüsselung über DES 56
`3_priv_sha`	Authentisierung über SHA, Verschlüsselung über DES 56
`3_priv_aes_md5`	Authentisierung über MD5, Verschlüsselung über AES 128
`3_priv_aes_sha`	Authentisierung über SHA, Verschlüsselung über AES 128
`3_priv_aes_sha224`	Authentisierung über SHA 224, Verschlüsselung über AES 128
`3_priv_aes_sha256`	Authentisierung über SHA 256, Verschlüsselung über AES 128
`3_priv_aes_sha384`	Authentisierung über SHA 384, Verschlüsselung über AES 128
`3_priv_aes_sha512`	Authentisierung über SHA 512, Verschlüsselung über AES 128

5.2.5 SNMP Read Community (Public Community)

Die (Public) Read Access Community für den SNMP-Lese-Zugriff. Im USP NAS und auf den Switches müssen dieselben SNMP-Communities eingetragen werden.

5.2.6 SNMP Write Community (Private Community)

Die (Private) Write Access Community für den SNMP-Schreib-Zugriff. Im USP NAS und auf den Switches müssen dieselben SNMP-Communities eingetragen werden.

5.2.7 Location

Der Standort des Switches. Wie oben beschrieben, kann dies durch einen SNMP-Scan überschrieben werden.

Copyright © 2026 United Security Providers AG. All rights reserved.

5.2.8 In Scope

Falls ein Switch oder Router 'In Scope' (Wert = 1) von USP NAS ist, heisst dies, dass diese nun aktiv gescannt, resp. für IP Lookups gebraucht werden. Falls ein Switch 'Out of Scope' (Wert = 0) ist, wird USP NAS die Traps dieses Switches nicht behandeln und auch keine Scans durchführen. Dasselbe gilt auch für den Router.

5.2.9 Zugangskontrollvariante

Die Zugangskontrollvariante beschreibt in welchem Modus USP NAS auf dem Switch operieren will.

`SYSTEMDEFAULT` ist der Standard und übernimmt die allgemeine Systemeinstellung.

`BLOCKVLAN` stellt sicher, dass auf diesem Switch nur VLAN's verschoben werden und keine Ports per Shutdown ausser Betrieb genommen werden. Früher hiess diese Einstellung `VLANMOVE`.

`PORTSHUTDOWN` versucht zu blockierende Ports mittels Shutdown ausser Betrieb zu nehmen. Falls ein Port aber als Voice-Port konfiguriert ist, wird diese Einstellung überschrieben und es wird in jedem Fall das VLAN verschoben anstelle des Shutdowns. Global kann man ein Shutdown auf allen Switches erreichen, indem 'Enforce Portblock' auf 'on' gestellt wird. Früher hiess diese Einstellung `SHUTDOWN`.

`VLANASSIGNMENT` verschiebt erlaubte und unerlaubte Geräte in die in den Access Profilen oder Endgeräten spezifizierten VLAN's. Diese Einstellung ist eine Zusammenfassung der früheren Werte `COMPLIANTVLAN` und `QUARANTINE_PRODUCTIVE_GUEST`.

5.2.10 MPP-User / MPP-Passwort / MPP-Port (obsolet)

Diese Datenfelder sind obsolet.

5.2.11 SNMPv3 User

Dies ist der SNMPv3 User (SNMPv3 Principal) welcher auf dem Switch oder Router definiert wurde.

5.2.12 SNMPv3 Authentication Passwort

Dies ist das Authentication Passwort für den SNMPv3 User (SNMPv3 Principal) welcher auf dem Switch oder Router konfiguriert wurde. Das Passwort kann leer gelassen werden, wenn ein SNMP Zugangsprofil mit dem entsprechenden Benutzernamen auf dem USP NAS konfiguriert ist.

5.2.13 SNMPv3 Encryption Passwort

Dies ist das Shared Secret zum Verschlüsseln der SNMPv3 Kommunikation. Dieses muss ebenfalls auf dem Switch oder Router konfiguriert werden. Das Passwort kann leer gelassen werden, wenn ein SNMP Zugangsprofil mit dem entsprechenden Benutzernamen auf dem USP NAS konfiguriert ist.

5.2.14 Mandant

Dieses Feld ist optional.

Der Mandant wird einem NetDevice nur zugewiesen, wenn er vorgängig in USP NAS erfasst wurde. Dabei muss der Mandantenname, der in USP NAS verwendet wird, mit dem aus der Importdatei übereinstimmen. Falls der Mandant in USP NAS noch nicht erfasst wird, wird dieses Feld in der Datenbank leer gelassen und das Gerät dem Default Mandant zugeordnet.

Falls ein NetDevice bereits in USP NAS erfasst ist und bereits eine Mandantenzuweisung besitzt, so wird diese NICHT überschrieben! Das heisst, man kann einem NetDevice genau einmal einen Mandanten zuweisen. Ausnahmen können nur noch über das USP NAS WebGUI gemacht werden.

Copyright © 2026 United Security Providers AG. All rights reserved.

5.2.15 WLAN ACL Filter Enforcement Flag

Dieses Feld ist optional.

Wenn der Typ des Netzwerkgerätes WLAN ist, kann hier angegeben werden ob anstelle von VLAN Enforcements ACL Filter Enforcements verwendet werden sollen.

Mögliche Werte:

- 0 (verwende VLAN Enforcements)
- 1 (verwende ACL Filter Enforcements)

5.2.16 802.1x Accounting

Dieses Feld ist optional.

Hier kann angegeben werden, ob USP NAS 802.1x Radius Accounting Informationen behandeln soll. Dieses Feature wird vor allem für die WLAN-Integration verwendet um in USP NAS tracken zu können, wann ein Endgerät sich vom Netz entfernt hat.

Mögliche Werte:

- 0 (Accounting ist ausgeschaltet)
- 1 (Accounting ist nur für Stop-Meldungen eingeschaltet)
- 2 (Accounting ist eingeschaltet und verarbeitet Start und Stop-Meldungen)

5.3 Beispiel

Beispiel für Dateinamen: `nms_demo_full_20260501121401.csv`:

Minimales Beispiel:

```
SEPARATOR:,
hostname,IP address,hardware class,SNMP version,SNMP read community
switch01,192.0.2.100,SWITCH,2c,public
```

Erweitertes Beispiel:

```
SEPARATOR:,
hostname,IP address,hardware class,SNMP version,SNMP read community,SNMP write community, ↩
    Location,InScope,,,,,snmpv3 user,snmp v3 auth pw,snmpv3 encription password,tenant
switch01,192.0.2.100,SWITCH,2c,public,private,Branch Office,1,,,,,,,,
switch02,192.0.2.101,RADIUSAUTH,3_priv_aes_sha512,,,,1,,,,,,johndoe,swordfish,swordfish,
```

Copyright © 2026 United Security Providers AG. All rights reserved.

5.4 Format einer Datenzeile (Netzwerkports)

Für den Import der Netzwerkports werden die Daten gemäss Tabelle 4 erwartet:

Table 7: Tabelle 4: Datenzeile für den Import von Netzwerkports

Feld	Beschreibung	Obligatorisch	Werte
1	Eindeutiger Name des Netzwerkgeräts (DNS-Name)	Ja	Beispiel: BONIN1.firma.ch
2	Interface Name	Nein	Beispiel: Fa0/1
3	Interface Index	Nein	Beispiel: 10001
4	Typ	Nein	Erlaubte Werte: `N` (= "Net-Port" / default) `A` (= "Access-Port") `H` (= "HSR-Port")

"HSR" steht für "High-availability Seamless Redundancy".

Der DNS-Name muss im USP NAS Scope vorhanden sein, damit die Netzwerkports korrekt zugeordnet werden können.

Empfehlung: Netzwerkports und Scope-Liste sollten immer zusammen exportiert werden, aber die Scope-Liste sollte einen leicht älteren Timestamp haben als die Netzwerkport-Liste, so dass zuerst die Scope-Liste verarbeitet wird. So kann sichergestellt werden, dass ein neues Netzwerkgerät bereits vorhanden ist, wenn die Netzwerkports des neuen Geräts eingelesen werden.

Es kann immer entweder der Interface Name (ifName) oder der Interface Index (ifIndex) angegeben werden. Es sollte jedoch nicht vorkommen, dass beide Felder (Feld 2 und Feld 3) gleichzeitig leer oder gleichzeitig ausgefüllt sind.

Copyright © 2026 United Security Providers AG. All rights reserved.

6 Daten für Endpoint Profiling

6.1 Format einer Datenzeile (PROFILERDEVICES)

Für den Import von PROFILERDEVICES werden die in Tabelle 6 aufgeführten Daten erwartet:

Table 8: Tabelle 6: Datenzeile für PROFILERDEVICES Import

Feld	Beschreibung	Obligatorisch	Werte
1	Profilerdevice Name	Ja	Beispiel: Windows 10
2	Profilerdevice Parent	Nein	Beispiel: Windows

6.2 Erläuterungen

Einem Endpoint wird nach erfolgreichem Profiling ein Profiling Device zugewiesen. Profiling Devices können eine Hierarchie aufweisen, zum Beispiel wird ein Endpoint erkannt als ‘Windows 10 Mobile’ mit aufsteigend ‘Windows 10’ und ‘Windows’ als Parent Profilerdevice.

6.2.1 Profilerdevice Name

Die Profilerdevice Bezeichnung, dies kann sowohl Aufschluss geben auf das erkannte Betriebssystem des Endpoints oder die Geräte-Art wie Switches, VoIP-Telefone oder Drucker.

6.2.2 Profilerdevice Parent

Der Name des übergeordneten Profilerdevice.

6.3 Format einer Datenzeile (PROFILERCOMBINATIONS)

Für den Import von PROFILERCOMBINATIONS werden die in Tabelle 7 aufgeführten Daten erwartet:

Table 9: Tabelle 7: Datenzeile für PROFILERCOMBINATIONS Import

Feld	Beschreibung	Obligatorisch	Werte
1	Profilerdevice Name	Ja	Beispiel: Windows 10
2	Version	Nein	Beispiel: 7.1.2
3	Score	Ja	0 - 100 Beispiel: 50
4	DHCP-Fingerprint	Nein	Beispiel: 1,33,3,6,15,28,51,58,59
5	DHCP-Vendor	Nein	Beispiel: dhcpcd-5.2.10

Copyright © 2026 United Security Providers AG. All rights reserved.

Table 9: (continued)

Feld	Beschreibung	Obligatorisch	Werte
6	MAC Vendor Name	Nein	Beispiel: Samsung Electro Mechanics co., LTD.
7	MAC Vendor Prefix	Nein	6-Stelliger HEX-String Beispiel: 000dcc

6.4 Erläuterungen

Eine Profiler Combination ist eine Zusammenstellung von Merkmalen, welche gewichtet nach einem Score ein am besten dazu passendes Profiler Device angibt. Nicht spezifizierte Merkmalsfelder treffen auf alle Inhalte zu, sind also eine Wildcard.

6.4.1 Profilerdevice Name

Das spezifierte Profilerdevice.

6.4.2 Version

Zusätzliche Versionsinformation zum erkannten Profilerdevice

6.4.3 Score

Die Gewichtung der Profilercombination, von 0=niedrigste Genauigkeit zu 100=exakter Match. Der Score kann verwendet werden zur Übersteuerung einer inkorrekten Erkennung.

6.4.4 DHCP-Fingerprint

Der DHCP-Fingerprint besteht aus dem Inhalt der DHCP-Option 55 und beschreibt die Reihenfolge und den Typ der angefragten Parameter seitens Endpoint.

6.4.5 DHCP-Vendor

Inhalt der DHCP-Option 60, beschreibt falls vorhanden den DHCP Client Hersteller.

6.4.6 MAC Vendor Name

Der Hersteller des Netzwerk-Adapters des Endpoints.

6.4.7 MAC Vendor Präfix

Die ersten 6 Stellen der MAC-Adresse des Endpoints.

Copyright © 2026 United Security Providers AG. All rights reserved.

7 Daten für Port Konfiguration

7.1 Format einer Datenzeile (PORTCONFIG)

Für den Import der Port-Konfiguration in Tabelle 8 aufgeführten Daten erwartet:

Table 10: Tabelle 8: Datenzeile für Portconfig import

Feld	Beschreibung	Obligatorisch	Beispielwert
1	Eindeutiger Name des Netzwerkgeräts (DNS-Name)	Ja	BONIN1.firma.ch
2	Interface Name	Nein*	Fa0/1
3	Interface Index	Nein*	10001
4	Subzone (Gerätetyp)	Ja	Printer

7.2 Erläuterungen

Mit dem Portconfig Import kann die gewünschte Port-Konfiguration eines Ports über ein Importfile von einem Fremdsystem in USP NAS importiert werden.

Jede Zeile beschreibt einen zugelassenen Gerätetyp eines einzelnen Netzwerk-Ports. Sind für einen Port mehrere Gerätetypen zugelassen, können für diesen Port mehrere Zeilen mit jeweils unterschiedlichem Gerätetyp importiert werden.

Der DNS-Name muss im USP NAS Scope vorhanden sein, damit die Netzwerkports korrekt zugeordnet werden können.

Es kann immer entweder der Interface Name (ifName) oder der Interface Index (ifIndex) angegeben werden. Es sollte jedoch nicht vorkommen, dass beide Felder (Feld 2 und Feld 3) gleichzeitig leer oder gleichzeitig ausgefüllt sind.

7.2.1 Switch-DNS

Switch-DNS enthält den DNS-Namen des Switches, für den der Port konfiguriert wird.

7.2.2 ifindex

Die Spalte ifindex definiert den Port am Switch, für den die Konfiguration gilt.

7.2.3 ifname

Die Spalte ifindex definiert den Port am Switch, für den die Konfiguration gilt.

7.2.4 Subzone

Die Subzone definiert den Gerätetyp, welche an diesem Port zugelassen ist.

Sind an einem Port mehrere Gerätetypen zugelassen, können mehrere Zeilen pro Port importiert werden mit jeweils unterschiedlichem Gerätetyp

Copyright © 2026 United Security Providers AG. All rights reserved.

8 Daten für Portgruppen Import

8.1 Format einer Datenzeile (PORTGROUP)

Für den Import der Portgruppen Konfiguration in Tabelle 8 aufgeführten Daten erwartet:

Table 11: Tabelle 9: Datenzeile für Portconfig import

Feld	Beschreibung	Obligatorisch	Werte
1	Eindeutiger Name des Netzwerkgeräts (DNS-Name)	Ja	Beispiel: BONIN1.firma.ch
2	Interface Name	Nein*	Beispiel: Fa0/1 Oder % für alle Ports des Switches
3	Interface Index	Nein*	Beispiel: 10001
4	Portgruppe	Ja	Beispiel: Printer (Die Portgruppe muss in USP NAS bereits konfiguriert sein. Wenn keine übereinstimmende Portgruppe existiert, wird der Eintrag verworfen.)

8.2 Erläuterungen

Mit dem Portconfig Import kann die gewünschte Port-Konfiguration eines Ports über ein Importfile von einem Fremdsystem in USP NAS importiert werden.

Jede Zeile beschreibt die Zugehörigkeit eines Ports zu einer Portgruppe. Falls im ifName Feld ein % angegeben wird, dann werden sämtliche Ports des Switches zu der entsprechenden Portgruppe hinzugefügt.

Der DNS-Name muss im USP NAS Scope vorhanden sein, damit die Netzwerkports korrekt zugeordnet werden können.

Es kann immer entweder der Interface Name (ifName) oder der Interface Index (ifIndex) angegeben werden. Es sollte jedoch nicht vorkommen, dass beide Felder (Feld 2 und Feld 3) gleichzeitig leer oder gleichzeitig ausgefüllt sind.

8.2.1 Switch-DNS

Switch-DNS enthält den DNS-Namen des Switches

8.2.2 ifindex

Die Spalte ifindex definiert den Port am Switch, welcher der Portgruppe zugeordnet werden soll

8.2.3 ifname

Die Spalte ifname definiert den Port am Switch, welcher der Portgruppe zugeordnet werden soll. Wenn in der Spalte % steht, werden sämtliche Ports des Switches der Portgruppe zugewiesen.

Copyright © 2026 United Security Providers AG. All rights reserved.

8.2.4 Portgruppe

Name der Portgruppe zu der dieser Port zugeordnet ist. Voraussetzung ist, dass bereits eine entsprechende Portgruppe in USP NAS definiert ist welcher dieser Port zugeordnet werden kann. Wenn keine entsprechende Portgruppe existiert, wird der Eintrag verworfen

Copyright © 2026 United Security Providers AG. All rights reserved.

9 DNS-Import über CSV

9.1 Format einer Datenzeile (DNS)

Für den Import der DNS-Records werden die in Tabelle 3 aufgeführten Daten erwartet:

Table 12: Tabelle 10: Datenzeile für DNS-Import über CSV

Feld	Beschreibung	Obligatorisch	Werte
1	DNS-Name	Ja	Beispiel: BONIN1.firma.ch.
2	IP-Adresse (v4/v6)	Ja	Beispiel: 192.168.17.252
3	Typ	Ja	A, A6, AAAA

9.2 Erläuterungen

Der DNS-Import über CSV ist neben dem Zonentransfer eine weitere Möglichkeit DNS-Namen im USP NAS zu ergänzen

9.2.1 DNS-Name

Der DNS-Name des Endgerätes

9.2.2 IP-Adresse

Die IP-Adresse des Endgerätes zu dem der DNS-Name aktualisiert werden soll

9.2.3 Typ

Dies gib den Typ der IP-Adresse an (v4 oder v6).

Copyright © 2026 United Security Providers AG. All rights reserved.

10 Endgeräte-Detail Import

10.1 Format einer Datenzeile (EPD)

Für den Import des EPD werden die in Tabelle 3 aufgeführten Daten erwartet:

Table 13: Tabelle 11: Datenzeile für EPD-Import

Feld	Beschreibung	Obligatorisch	Werte
1	MAC-Adresse	Nein*	Beispiel: 001143b47ae2
2	IP-Adresse	Nein*	Beispiel: 192.168.1.99
3	Key	Ja	Beliebiger Wert
4	Value	Ja	Beliebiger Wert

10.2 Erläuterungen

Mit dem EPD-Eigenschaften zu einem Endgerät importiert werden, welche einerseits im den Gerätedetail angezeigt werden oder für das Berechnen eines Profils verwendet werden können. Damit ein Datensatz zugeordnet werden kann, muss entweder die MAC-Adresse oder die IP-Adresse verfügbar sein. Fall beide Felder verfügbar sind, wird die MAC-Adresse für die Zuordnung verwendet.

10.2.1 Mac-Adresse

Die MAC-Adresse des Endgerätes zu dem die Eigenschaften hinzugefügt werden sollen

10.2.2 IP-Adresse

Die IP-Adresse des Endgerätes zu dem die Eigenschaften hinzugefügt werden sollen. Die IP-Adresse dient beim Einfügen der Eigenschaft für den Lookup der MAC-Adresse. Falls zum Zeitpunkt des Imports keine MAC/IP Zuordnung vorhanden ist, kann der Eintrag nicht eingefügt werden.

10.2.3 Key

Die Bezeichnung der Eigenschaft

10.2.4 Value

Der Wert der Eigenschaft

Copyright © 2026 United Security Providers AG. All rights reserved.