IT-Network DocuScanner

Installations- und Bedienungsanleitung

Version 2.08.14

Sat-iTec Systemhaus GmbH

https://www.sat-itec.se

1. Übersicht

Der IT-Network DocuScanner ist ein Werkzeug zur automatisierten Inventarisierung und Dokumentation von IT-Infrastrukturen. Er erfasst Hosts, installierte Software, Lizenz-Schlüssel, Active-Directory-Objekte, Netzwerkfreigaben und IT-Sicherheitsmerkmale (BSI-Grundschutz) und stellt sie in einer Web-Oberfläche bereit.

Hauptfunktionen

- Netzwerk-Scan via Ping/ARP, Hostname-Auflösung und MAC-Erfassung
- Software-Inventar via CIM/WMI mit DCOM-Fallback
- Lizenz-Auswertung (Windows-Produktschlüssel, Office, WMI SoftwareLicensingProduct)
- Active-Directory-Abfrage über natives Go-LDAP/LDAPS
- SMB-Freigaben mit ACLs (CIM + net-view-Fallback) und NFS-Detection
- BSI-Grundschutz-Heuristiken auf Basis der Scan-Daten
- REST-API für externe Tools, automatischer Update-Check über GitHub-Releases

Architektur

Der Scanner besteht aus zwei Komponenten:

Komponente	Aufgabe	Plattform
itscanner-server	Web-UI, REST-API, SQLite-Datenbank, AD-LDAP-Client	Windows + Linux
Invoke-Scan.ps1	Netzwerk-/Software-/Lizenz-/Share-/NFS-Scan über CIM-WMI	nur Windows

Hinweis: Der Scan-Worker (Invoke-Scan.ps1) ist Windows-spezifisch. Unter Linux läuft der Server für Web-UI und AD-Abfrage, der Scan selbst muss von einem Windows-Knoten ausgehen.

2. Systemvoraussetzungen

Server (Web-UI / API)

Plattform	Mindestanforderung
Windows	Windows 10 / Windows Server 2016 oder neuer, 64-Bit
Linux	Distribution mit systemd (Debian 11+, Ubuntu 20.04+, RHEL 8+, openSUSE Leap 15+), 64-Bit
RAM	Mindestens 512 MB, empfohlen 2 GB für große Netze
Festplatte	200 MB Programm + Wachstum der SQLite-DB (typisch 50–500 MB)
Netzwerk	TCP/8585 erreichbar für Web-UI

Scan-Knoten (Windows-Worker)

- Windows 10 / Server 2016 oder neuer mit PowerShell 5.1
- Domänen-Mitgliedschaft empfohlen, Domänen-Admin oder gleichwertige Rechte für AD-Abfragen
- ActiveDirectory-PowerShell-Modul (RSAT) optional — Fallback über ADSI/LDAP eingebaut
- Services for NFS (Windows-Feature) optional, ermöglicht NFS-Mount-Liste über showmount.exe

Netzwerk-Voraussetzungen für Ziel-Hosts

Port	Protokoll	Zweck
135 / TCP	DCOM/RPC	Software-Inventar Fallback
445 / TCP	SMB	Freigaben, net-view
5985 / TCP	WinRM	CIM-Sessions (bevorzugt)
389 / TCP	LDAP	Active-Directory-Abfrage
636 / TCP	LDAPS	AD verschlüsselt (empfohlen)
2049 / TCP	NFS	Linux-NFS-Detection

3. Installation unter Windows

Der Windows-Installer ist ein NSIS-Setup, das den Server als Windows-Dienst einrichtet. Der Dienst startet automatisch beim Systemstart.

3.1 Schritt-für-Schritt

1. ITScanner-Server-Setup-2.08.12.exe als Administrator herunterladen
2. Download von der GitHub-Releases-Seite oder über die Auto-Update-Funktion
3. Installer als Administrator ausführen (Rechtsklick → "Als Administrator ausführen")
4. Installationspfad bestätigen (Standard: C:\Program Files\ITScanner-Server)
5. Installation abschließen — der Dienst "IT-Network DocuScanner Server" startet automatisch
6. Browser öffnen: http://localhost:8585

3.2 Dienst-Verwaltung

```
# Status prüfen
sc query "IT-Network DocuScanner Server"

# Dienst stoppen / starten
net stop  "IT-Network DocuScanner Server"
net start "IT-Network DocuScanner Server"

# Dienst entfernen (für saubere Neuinstallation)
itscanner-server.exe --uninstall
```

3.3 Verzeichnisse

Pfad	Inhalt
C:\Program Files\ITScanner-Server\	Programm + Skripte
C:\ProgramData\ITScanner-Server\	Datenbank, Konfiguration, Logs
C:\ProgramData\ITScanner-Server\itscanner.db	SQLite-Hauptdatenbank
C:\ProgramData\ITScanner-Server\scripts\	Invoke-Scan.ps1, ad_settings.json

4. Installation unter Linux

Der Server läuft auf jeder Linux-Distribution mit systemd. Es stehen zwei Installationspakete bereit: ein universelles tar.gz mit Install-Skript sowie ein natives .deb für Debian/Ubuntu.

4.1 Debian / Ubuntu (.deb)

```
sudo dpkg -i itscanner-server_2.08.12_amd64.deb
sudo systemctl status itscanner-server

# Falls Abhängigkeiten fehlen:
sudo apt-get install -f
```

Die postinst-Hook legt automatisch den System-User itscanner an, erstellt /var/lib/itscanner-server, registriert die systemd-Unit und startet den Dienst.

4.2 Universell (tar.gz)

```
tar -xzf itscanner-server-linux-2.08.12.tar.gz
cd itscanner-server-linux-2.08.12
sudo ./install.sh
```

4.3 Verzeichnisse unter Linux

Pfad	Inhalt
/opt/itscanner-server/	Programm-Binaries
/var/lib/itscanner-server/	SQLite-DB, Konfiguration
/var/log/itscanner-server/	Zusätzliche Logs (sonst journalctl)
/etc/systemd/system/itscanner-server.service	systemd-Unit

4.4 Service-Management

```
sudo systemctl status   itscanner-server
sudo systemctl restart  itscanner-server
sudo systemctl stop     itscanner-server
sudo journalctl -u itscanner-server -f      # Live-Log
```

Wichtig: Unter Linux ist der PowerShell-Scan-Worker nicht aktiv. Funktionsfähig sind: Web-UI mit allen Tabs, REST-API, AD-Live-Abfrage über LDAP, Subnetze-Ableitung, BSI-Heuristiken, Daten-Anzeige aus früheren Scans. Für aktive Scans wird ein Windows-Knoten benötigt.

5. Erstkonfiguration

Nach der Installation sollten folgende Einstellungen vorgenommen werden, damit der Scanner sein volles Potenzial entfalten kann.

5.1 Active Directory verbinden

7. In der Web-UI auf Einstellungen → AD / LDAP wechseln
8. Domain-Controller-FQDN eintragen, z. B. dc01.firma.local
9. Domain-Name (DNS-Form), z. B. firma.local
10. Service-Account: bevorzugt ein eigener Account mit Read-only-Rechten auf das gesamte Verzeichnis
11. Passwort eingeben — wird verschlüsselt in der DB abgelegt
12. Verbindungstest auslösen — sollte einen Treffer-Zähler liefern

5.2 Scan-Credentials für CIM/WMI

Für Software-Inventarisierung und Freigaben-Erfassung auf Remote-Hosts werden Anmeldedaten mit lokalen oder Domänen-Admin-Rechten benötigt.

13. Einstellungen → Scan-Credentials
14. Domäne\\Administrator (oder gleichwertig) als Benutzername eintragen
15. Passwort: wird ausschließlich für Scan-Aufrufe verwendet

> **Tipp:** Auf Ziel-Hosts WinRM aktivieren (Enable-PSRemoting) für deutlich schnellere und stabilere Scans. Ohne WinRM versucht der Scanner DCOM als Fallback (langsamer, weniger zuverlässig).

5.3 Update-Server

Standardmäßig prüft der Server github.com/satitec/itscanner auf neue Releases. Falls ein interner Mirror genutzt werden soll:

```
# Anderes Repo
curl -X PUT -H "Content-Type: application/json" \
    -d '{"github_repo":"firma/itscanner-internal"}' \
    http://server:8585/api/settings/updates
```

6. Bedienung der Web-Oberfläche

Die Web-UI ist unter http://server:8585 erreichbar und gliedert sich in folgende Tabs:

6.1 Dashboard

Übersichtskacheln mit den wichtigsten Kennzahlen: Anzahl Hosts, Software-Einträge, AD-Objekte, BSI-Status. Rechts oben sieht man die aktuelle Server-Version sowie den Watchdog-Status.

6.2 Hosts

Liste aller im Netz erfassten Geräte mit Hostname, IP, MAC, OS, Domäne und Typ (Server, Workstation, Switch, Firewall, NAS, Printer, Other). Filter-Dropdowns für Typ und Status.

Klick auf einen Host öffnet die Detail-Ansicht mit Software-Liste, Lizenz-Schlüsseln, offenen Ports und Server-Rollen.

6.3 Software

Software-Inventar gruppiert nach Produktname. Pro Eintrag sieht man, auf wie vielen und welchen Hosts die Software installiert ist. Suchen, filtern, exportieren.

6.4 Freigaben

SMB-Netzwerkfreigaben gruppiert nach Host. Pro Freigabe wird der Name, der Pfad, die Beschreibung und die ACL angezeigt. Wenn der CIM-Zugriff nicht möglich war, wird der net-view-Fallback verwendet (ohne ACL-Details).

Über der Tabelle erscheint eine Diagnose-Zeile mit den Werten DB / API / Hosts. So ist bei leerem Tab sofort erkennbar, ob Daten in der DB liegen oder der Scan noch nicht gelaufen ist.

Linux-Hosts mit NFS-Server (Port 2049) werden als NFS-Server-Eintrag mit verfügbaren Mounts angezeigt, sofern showmount.exe verfügbar ist.

6.5 Lizenzen

Übersicht aller erfassten Lizenz-Schlüssel mit Quelle (Registry, WMI), Status (activated, grace, unlicensed) und Aktivierungs-Kanal (Volume, OEM, Retail, KMS).

6.6 Active Directory

Tabelle mit allen AD-Objekten (Benutzer, Gruppen, Computer, OUs, GPOs). Filter-Dropdown rechts oben zum Eingrenzen auf einen Objekt-Typ. Volltext-Suche über Name, sAMAccountName und Distinguished Name.

Über der Tabelle: Buttons "Vom AD laden" (löst eine Live-LDAP-Abfrage aus) und "Aktualisieren" sowie eine Diagnose-Zeile DB / API / Angezeigt mit aktivem Filter.

6.7 Subnetze

Erkannte Subnetze mit Gateway, VLAN-ID und Host-Anzahl. Wenn keine Subnetze von einem Scan eingetragen wurden, leitet der Server sie automatisch aus den IP-Adressen der Hosts ab (Gruppierung nach /24).

6.8 Server-Rollen

Übersicht aller installierten Windows-Server-Rollen und Optional-Features pro Host. Auf Server-Betriebssystemen werden die Rollen via Win32_ServerFeature ausgelesen (z. B. Active Directory Domain Services, DNS Server, DHCP Server, File Server, Web Server IIS, Hyper-V). Auf Workstations zeigt die Tabelle Win32_OptionalFeatures wie Hyper-V-Client, Telnet-Client, Internet Information Services Express.

Die Tabelle zeigt fünf Spalten: Host, OS, Rolle / Feature (interner Bezeichner), Anzeigename und Status. Der Suchen-Filter durchsucht Hostname, Rolle und Anzeigename in Echtzeit; das Host-Filter-Dropdown rechts oben grenzt die Anzeige auf einen einzelnen Server ein.

Voraussetzung: CIM-Zugriff auf den Zielhost (WinRM auf Port 5985 oder DCOM auf Port 135), plus Admin-Rechte für die WMI-Klassen Win32_ServerFeature bzw. Win32_OptionalFeature. Hosts ohne CIM-Zugriff erscheinen nicht in dieser Tabelle.

6.9 BSI-Checks

IT-Grundschutz-konforme Heuristiken auf Basis der Scan-Daten. Der Tab zeigt die Anzahl bestandener, warnender und kritischer Checks oben in drei Karten. Die Tabelle darunter listet die einzelnen Prüfungen mit Kategorie, Status, Befund und Empfehlung.

Beispiele für Heuristiken:

- End-of-Life Betriebssysteme (Windows XP/7/8, Server 2003/2008/2012) → kritisch
- Mehr als zwei Hosts mit offenem RDP (Port 3389) → kritisch
- Telnet (Port 23) auf irgendeinem Host → kritisch
- Domain-Controller-Redundanz (≥ 2 DCs) → ok
- Backup-Software erkannt (Veeam, Acronis, Commvault, Nakivo, Macrium) → ok
- Deaktivierte AD-Konten → warnung

6.10 Berichte

Vorgefertigte Reports zum Download als PDF oder DOCX, unter anderem: Server-/Client-Übersicht, Hardware-Inventar, Software-Compliance, Lizenz-Audit, BSI-Grundschutz-Bericht, Netzwerk-Topologie.

6.11 Scan-Verwaltung

Verwaltung der Scan-Jobs mit Name, Typ, Ziel-Subnetzen und Zeitplan. Buttons zum Erstellen, Bearbeiten, Triggern und Löschen. Standard-Jobs sind "Vollständiger Netzwerk-Scan" (wöchentlich), "Täglich Netzwerk-Status", "Software-Inventarisierung" und "AD-Audit".

6.12 Scan-Verlauf

Chronologische Liste aller Scan-Läufe mit Start- und Endzeit, Dauer, Anzahl der gefundenen Hosts und Status. Klick auf einen Eintrag öffnet das Detail-Log dieses Laufs.

6.13 Log

Live-Log-Ansicht mit allen Server- und Scan-Events. Auto-Refresh-Toggle rechts oben. Filter-Dropdown für Log-Level (info / warning / error).

Tipp: Bei Problemen ist der Log-Tab die wichtigste Diagnose-Quelle. Suche nach "Share-Scan", "AD-Frueh-Import" oder "NFS-/Linux-Scan" um die jeweiligen Sub-Phasen nachzuvollziehen.

6.14 Einstellungen

Untermenü mit AD/LDAP-Verbindung, Scan-Credentials, Update-Server, Berichte-Voreinstellungen und Lizenz-Aktivierung.

7. Scan ausführen

7.1 Scan-Typen

Typ	Aktivität
full	Netzwerk + Software + Lizenz + AD + Freigaben + NFS
network	Nur Ping/ARP/Hostname-Auflösung
software	CIM/WMI + Lizenz auf vorhandenen Hosts
ad	Nur AD-Live-Abfrage über LDAP
shares	Nur SMB- und NFS-Freigaben-Erfassung

7.2 Empfohlener Ablauf bei Erst-Inbetriebnahme

16. Einstellungen vornehmen (AD-Verbindung, Scan-Credentials)
17. Scan-Verwaltung → "Vollständiger Netzwerk-Scan" → Targets prüfen → Triggern
18. Im Log-Tab den Verlauf beobachten — der AD-Frühimport meldet sich nach 10–30 Sekunden mit "AD-Frueh-Import: X von Y Objekten in DB"
19. Während Software-/Share-Scan läuft (kann mehrere Minuten dauern) bereits den AD-Tab öffnen — die Daten sind dort schon sichtbar
20. Nach Abschluss: Scan-Verlauf prüfen, Berichte generieren

7.3 Erwartete Log-Sequenz

```
Scan 'Default' gestartet: Typ=full
N bekannte Hosts aus DB an Scan uebergeben
AD-Scan abgeschlossen: 66 Objekte (ou=2, user=7, ...)
AD-Frueh-Import: 66 von 66 Objekten in DB
Bekannte Hosts aus DB geladen: 36 gesamt, 2 neu
Software-Inventarisierung v2.08: CIM+StdRegProv...
Share-Scan: 36 Hosts geprueft, 4 erreicht, 32 ohne CIM
NFS-/Linux-Scan: 36 Hosts geprueft, NFS=N, SMB-Marker=M
Freigaben gesamt: 7 SMB + N NFS/Marker = X
Freigaben-Import: X von X in DB
Scan 'Default' erfolgreich: 36 Hosts, 374 Software, ...
```

8. Update-Mechanismus

Der Server prüft auf Wunsch den GitHub-Releases-Endpunkt von satitec/itscanner und erkennt automatisch eine neuere Version. Plattform-passend wird der richtige Download-Link bereitgestellt (.exe für Windows, .deb für Debian/Ubuntu, .tar.gz universell).

8.1 Manueller Check

21. Einstellungen → Updates
22. Button "Jetzt nach Updates suchen" klicken
23. Bei verfügbarem Update: Download-Link wird angezeigt
24. Datei herunterladen, Installer ausführen — Datenbank und Konfiguration bleiben erhalten

8.2 Automatik-Verhalten

Standardmäßig fragt der Server nicht selbst regelmäßig nach Updates ab. Eine geplante Abfrage kann über Scan-Verwaltung als Aufgabe konfiguriert werden, oder via Cron/Aufgabenplanung gegen den Endpunkt /api/update/check.

8.3 Versions-Vergleich (Semver)

Der Server vergleicht Version-Strings nach Semver-Regeln: 2.08.10 vs. 2.04.00 ergibt 1 (a > b), das v-Präfix wird ignoriert, Suffixe wie -rc1 werden abgeschnitten.

9. Troubleshooting

9.1 AD-Tab bleibt leer trotz erfolgreichem Scan

Mögliche Ursachen:

- Browser-Cache hält alte Antwort fest → Strg+F5 erzwingt Neuladen
- Diagnose-Zeile prüfen: "DB: 66 | API: 0" → Browser-Cache, "DB: 0 | API: 0" → Scan war erfolglos
- Im Log nach "AD-Frueh-Import" oder "AD-Partial-Datei konnte nicht geschrieben werden" suchen

9.2 Freigaben-Tab leer

- Diagnose-Zeile: "API: 0 Freigaben | N Hosts" → Scan hat nichts geliefert
- Im Log nach "Share-Scan: X erreicht, Y ohne CIM" suchen — wenn alle ohne CIM, fehlen Berechtigungen
- Lösung: WinRM auf Ziel-Hosts aktivieren (Enable-PSRemoting auf dem Ziel)
- Alternativ: Scan-Credentials prüfen — Account muss auf Ziel-Host Admin-Rechte haben

9.3 "Kein CIM-Zugriff" für viele Hosts

- Häufig bei Workgroup-Hosts oder Hosts in fremden Domänen
- Firewall-Regel für "Windows-Verwaltungsinstrumentation (WMI-In)" auf den Ziel-Hosts aktivieren
- Bei Linux-Servern erscheint "Kein CIM" → SMB-Probe-Fallback auf Port 445 zeigt sie als "SMB-Server"-Marker
- Bei NFS-Servern: TCP-Port 2049 wird gepingt — falls offen, erscheint NFS-Server-Eintrag

9.4 Telnet-Warnung im BSI-Tab obwohl kein Telnet bekannt

Manche Embedded-Geräte (Drucker, Switches älteren Typs) haben Port 23 offen. Prüfen Sie die ports-Tabelle der Datenbank, schließen Sie den Port am Gerät oder dokumentieren Sie die Ausnahme.

9.5 Service startet nicht (Linux)

```
sudo journalctl -u itscanner-server -n 50 --no-pager
```

Häufige Ursachen: Port 8585 belegt (anderen Dienst beenden oder --port-Flag in der systemd-Unit anpassen), Datei-Berechtigungen falsch (chown -R itscanner:itscanner /var/lib/itscanner-server).

9.6 Service startet nicht (Windows)

```
# Event-Viewer öffnen
eventvwr.msc

# Anwendungs-Log auf "IT-Network DocuScanner" filtern
```

```
# Häufig: Datenbank-Pfad nicht beschreibbar
#         oder Port 8585 belegt
```

10. Anhang

10.1 REST-API Endpunkte

Endpunkt	Methode	Zweck
/api/health	GET	Status + Version
/api/dashboard	GET	Übersichts-Kennzahlen
/api/hosts	GET	Host-Liste
/api/software	GET	Software-Liste
/api/shares	GET	Freigaben-Liste
/api/licenses	GET	Lizenz-Schlüssel
/api/ad	GET	AD-Objekte (Filter: ?type, ?search)
/api/ad/stats	GET	AD-Counter
/api/ad/query	POST	Live-LDAP-Abfrage triggern
/api/subnets	GET	Subnetze (mit Auto-Derive)
/api/server-roles	GET	Server-Rollen (Filter: ?host, ?status)
/api/bsi	GET	BSI-Checks (mit Auto-Derive)
/api/scans	GET	Scan-Verlauf
/api/jobs	GET/POST	Scan-Jobs
/api/jobs/{id}/trigger	POST	Scan starten
/api/update/check	GET/POST	Update-Check (GitHub)
/api/logs	GET	Log-Einträge

10.2 Versions-Schema

Sat-iTec verwendet ein dreistelliges Versionsschema X.YY.ZZ:

- X = Major (selten, größere Architektur-Wechsel)
- YY = Minor (neue Features, Y wird zweistellig geschrieben)
- ZZ = Patch (Bugfixes, Z wird zweistellig geschrieben)

Beispiel: 2.08.12 = Major 2, Minor 8, Patch 12. Eine neue Funktion erhöht YY (z. B. 2.09.00), ein Bugfix erhöht ZZ (z. B. 2.08.13).

10.3 Support-Kontakt

Sat-iTec Systemhaus GmbH

E-Mail: support@sat-itec.se
Web: https://www.sat-itec.se
GitHub-Releases: https://github.com/satitec/itscanner/releases