IT-Network DocuScanner

Installation and User Guide

Version 2.08.14

Sat-iTec Systemhaus GmbH
https://www.sat-itec.se

1. Overview

The IT-Network DocuScanner is a tool for the automated inventory and documentation of IT infrastructures. It captures hosts, installed software, license keys, Active Directory objects, network shares and IT security characteristics (BSI Grundschutz) and presents them in a web interface.

Main features

- Network scan via Ping/ARP, hostname resolution and MAC capture
- Software inventory via CIM/WMI with DCOM fallback
- License audit (Windows product keys, Office, WMI SoftwareLicensingProduct)
- Active Directory query through native Go-LDAP/LDAPS
- SMB shares with ACLs (CIM + net-view fallback) and NFS detection
- BSI Grundschutz heuristics derived from scan data
- REST API for external tools, automatic update check via GitHub releases

Architecture

The scanner consists of two components:

Component	Purpose	Platform
itscanner-server	Web UI, REST API, SQLite database, AD-LDAP client	Windows + Linux
Invoke-Scan.ps1	Network/software/license/share/NFS scan via CIM-WMI	Windows only

Note: The scan worker (Invoke-Scan.ps1) is Windows-specific. On Linux the server provides the web UI and AD query, while the actual scan must originate from a Windows node.

2. System requirements

Server (Web UI / API)

Platform	Minimum requirement
Windows	Windows 10 / Windows Server 2016 or newer, 64-bit
Linux	Distribution with systemd (Debian 11+, Ubuntu 20.04+, RHEL 8+, openSUSE Leap 15+), 64-bit
RAM	Minimum 512 MB, recommended 2 GB for large networks
Disk	200 MB program + SQLite DB growth (typically 50–500 MB)
Network	TCP/8585 reachable for the web UI

Scan node (Windows worker)

- Windows 10 / Server 2016 or newer with PowerShell 5.1
- Domain membership recommended; Domain Admin or equivalent rights for AD queries
- ActiveDirectory PowerShell module (RSAT) optional — ADSI/LDAP fallback is built in
- Services for NFS (Windows feature) optional, enables NFS mount listing via showmount.exe

Network requirements for target hosts

Port	Protocol	Purpose
135 / TCP	DCOM/RPC	Software inventory fallback
445 / TCP	SMB	Shares, net-view
5985 / TCP	WinRM	CIM sessions (preferred)
389 / TCP	LDAP	Active Directory query
636 / TCP	LDAPS	AD encrypted (recommended)
2049 / TCP	NFS	Linux NFS detection

3. Installation on Windows

The Windows installer is an NSIS setup that registers the server as a Windows service. The service starts automatically at system boot.

3.1 Step by step

1. Download ITScanner-Server-Setup-2.08.14.exe as Administrator
2. Download from the GitHub releases page or via the auto-update feature
3. Run the installer as Administrator (right-click → "Run as administrator")
4. Confirm install path (default: C:\Program Files\ITScanner-Server)
5. Finish the installation — the service "IT-Network DocuScanner Server" starts automatically
6. Open browser: http://localhost:8585

3.2 Service management

```
# Check status
sc query "IT-Network DocuScanner Server"

# Stop / start the service
net stop "IT-Network DocuScanner Server"
net start "IT-Network DocuScanner Server"

# Remove the service (for clean reinstall)
itscanner-server.exe --uninstall
```

3.3 Directories

Path	Contents
C:\Program Files\ITScanner-Server\	Program + scripts
C:\ProgramData\ITScanner-Server\	Database, configuration, logs
C:\ProgramData\ITScanner-Server\itscanner.db	Main SQLite database
C:\ProgramData\ITScanner-Server\scripts\	Invoke-Scan.ps1, ad_settings.json

4. Installation on Linux

The server runs on any Linux distribution with systemd. Two installation packages are available: a universal tar.gz with an install script, and a native .deb for Debian/Ubuntu.

4.1 Debian / Ubuntu (.deb)

```
sudo dpkg -i itscanner-server_2.08.14_amd64.deb
sudo systemctl status itscanner-server

# If dependencies are missing:
sudo apt-get install -f
```

The postinst hook automatically creates the system user itscanner, sets up /var/lib/itscanner-server, registers the systemd unit and starts the service.

4.2 Universal (tar.gz)

```
tar -xzf itscanner-server-linux-2.08.14.tar.gz
cd itscanner-server-linux-2.08.14
sudo ./install.sh
```

4.3 Directories on Linux

Path	Contents
/opt/itscanner-server/	Program binaries
/var/lib/itscanner-server/	SQLite DB, configuration
/var/log/itscanner-server/	Additional logs (otherwise 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
```

Important: On Linux the PowerShell scan worker is not active. Functional are: web UI with all tabs, REST API, AD live query via LDAP, subnet derivation, BSI heuristics, data display from prior scans. A Windows node is required for active scans.

5. Initial configuration

After installation the following settings should be configured so that the scanner can fully unfold its potential.

5.1 Connect Active Directory

7. Switch to Settings → AD / LDAP in the web UI
8. Enter the domain controller FQDN, e.g. dc01.company.local
9. Domain name (DNS form), e.g. company.local
10. Service account: preferably a dedicated account with read-only rights on the entire directory
11. Enter the password — it is stored encrypted in the DB
12. Trigger the connection test — should report a hit count

5.2 Scan credentials for CIM/WMI

For software inventory and share capture on remote hosts, credentials with local or Domain Admin rights are required.

13. Settings → Scan credentials
14. Enter Domain\\Administrator (or equivalent) as the username
15. Password: used exclusively for scan calls

Tip: Enable WinRM on the target hosts (Enable-PSRemoting) for significantly faster and more stable scans. Without WinRM the scanner attempts DCOM as a fallback (slower, less reliable).

5.3 Update server

By default the server checks github.com/satitec/itscanner for new releases. To use an internal mirror:

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

6. Using the web interface

The web UI is reachable at http://server:8585 and is divided into the following tabs:

6.1 Dashboard

Summary tiles with the most important metrics: number of hosts, software entries, AD objects, BSI status. The current server version and watchdog status are visible in the upper right.

6.2 Hosts

List of all devices captured in the network with hostname, IP, MAC, OS, domain and type (Server, Workstation, Switch, Firewall, NAS, Printer, Other). Filter dropdowns for type and status. Clicking a host opens the detail view with software list, license keys, open ports and server roles.

6.3 Software

Software inventory grouped by product name. Each entry shows on how many and which hosts the software is installed. Search, filter, export.

6.4 Shares

SMB network shares grouped by host. For each share the name, path, description and ACL are shown. If CIM access was not possible, the net-view fallback is used (without ACL details). Above the table a diagnostics row appears with values DB / API / Hosts. So when the tab is empty, it is immediately recognizable whether data is in the DB or the scan has not yet run. Linux hosts with NFS server (port 2049) are shown as an NFS server entry with available mounts, provided showmount.exe is available.

6.5 Licenses

Overview of all captured license keys with source (Registry, WMI), status (activated, grace, unlicensed) and activation channel (Volume, OEM, Retail, KMS).

6.6 Active Directory

Table with all AD objects (users, groups, computers, OUs, GPOs). Filter dropdown in the upper right to narrow down by object type. Full-text search across name, sAMAccountName and Distinguished Name. Above the table: "Load from AD" button (triggers a live LDAP query) and "Refresh" plus a diagnostics row DB / API / Displayed with active filter.

6.7 Subnets

Detected subnets with gateway, VLAN ID and host count. If no subnets were registered by a scan, the server derives them automatically from the host IP addresses (group by /24).

6.8 Server roles

Overview of all installed Windows server roles and optional features per host. On server operating systems the roles are read via Win32_ServerFeature (e.g. Active Directory Domain Services, DNS Server, DHCP Server, File Server, Web Server IIS, Hyper-V). On workstations the table shows Win32_OptionalFeatures such as Hyper-V Client, Telnet Client, Internet Information Services Express. The table shows five columns: Host, OS, Role / Feature (internal identifier), display name and status. The search filter searches hostname, role and display name in real time; the host filter dropdown in the upper right

narrows the display to a single server. Requirement: CIM access to the target host (WinRM on port 5985 or DCOM on port 135), plus admin rights for the WMI classes Win32_ServerFeature and Win32_OptionalFeature. Hosts without CIM access do not appear in this table.

6.9 BSI checks

IT-Grundschutz-compliant heuristics based on scan data. The tab shows the count of passed, warning and critical checks at the top in three cards. The table below lists the individual checks with category, status, finding and recommendation.

Examples of heuristics:

- End-of-life operating systems (Windows XP/7/8, Server 2003/2008/2012) → critical
- More than two hosts with open RDP (port 3389) → critical
- Telnet (port 23) on any host → critical
- Domain controller redundancy (≥ 2 DCs) → ok
- Backup software detected (Veeam, Acronis, Commvault, Nakivo, Macrium) → ok
- Disabled AD accounts → warning

6.10 Reports

Pre-built reports for download as PDF or DOCX, including: server/client overview, hardware inventory, software compliance, license audit, BSI Grundschutz report, network topology.

6.11 Scan management

Management of scan jobs with name, type, target subnets and schedule. Buttons to create, edit, trigger and delete. Default jobs are "Full network scan" (weekly), "Daily network status", "Software inventory" and "AD audit".

6.12 Scan history

Chronological list of all scan runs with start and end time, duration, number of hosts found and status. Clicking an entry opens the detail log of that run.

6.13 Log

Live log view with all server and scan events. Auto-refresh toggle in the upper right. Filter dropdown for log level (info / warning / error).

Tip: When troubleshooting, the Log tab is the most important diagnostic source. Search for "Share-Scan", "AD-Frueh-Import" or "NFS-/Linux-Scan" to follow the respective sub-phases.

6.14 Settings

Submenu with AD/LDAP connection, scan credentials, update server, report defaults and license activation.

7. Running a scan

7.1 Scan types

Type	Activity
full	Network + software + license + AD + shares + NFS
network	Ping/ARP/hostname resolution only
software	CIM/WMI + license on existing hosts
ad	AD live query via LDAP only
shares	SMB and NFS share capture only

7.2 Recommended flow for first deployment

16. Configure settings (AD connection, scan credentials)
17. Scan management → "Full network scan" → check targets → trigger
18. Watch progress in the Log tab — the AD early import reports after 10–30 seconds with "AD-Frueh-Import: X of Y objects in DB"
19. While the software/share scan runs (can take several minutes), already open the AD tab — the data is already visible there
20. When complete: check scan history, generate reports

7.3 Expected log sequence

```
Scan 'Default' started: type=full
N known hosts from DB passed to scan
AD scan finished: 66 objects (ou=2, user=7, ...)
AD-Frueh-Import: 66 of 66 objects in DB
Known hosts loaded from DB: 36 total, 2 new
Software inventory v2.08: CIM+StdRegProv...
Share-Scan: 36 hosts checked, 4 reached, 32 without CIM
NFS/Linux scan: 36 hosts checked, NFS=N, SMB-marker=M
Shares total: 7 SMB + N NFS/marker = X
Share import: X of X in DB
Scan 'Default' successful: 36 hosts, 374 software, ...
```

8. Update mechanism

Optionally the server checks the GitHub releases endpoint of satitec/itscanner and automatically detects a newer version. The correct download link is provided per platform (.exe for Windows, .deb for Debian/Ubuntu, .tar.gz universal).

8.1 Manual check

21. Settings → Updates
22. Click the "Check for updates now" button
23. If an update is available: the download link is shown
24. Download the file, run the installer — database and configuration are preserved

8.2 Automation behaviour

By default the server does not poll for updates regularly. A scheduled query can be configured via Scan management as a job, or via cron / Task Scheduler against the endpoint /api/update/check.

8.3 Version comparison (Semver)

The server compares version strings according to Semver rules: 2.08.10 vs. 2.04.00 yields 1 (a > b), the v prefix is ignored, suffixes such as -rc1 are stripped.

9. Troubleshooting

9.1 AD tab remains empty despite successful scan

Possible causes:

- Browser cache holds an old response → Ctrl+F5 forces reload
- Check diagnostics row: "DB: 66 | API: 0" → browser cache, "DB: 0 | API: 0" → scan was unsuccessful
- Search the log for "AD-Frueh-Import" or "AD-Partial file could not be written"

9.2 Shares tab empty

- Diagnostics row: "API: 0 shares | N hosts" → scan returned nothing
- Search the log for "Share-Scan: X reached, Y without CIM" — if all without CIM, permissions are missing
- Solution: enable WinRM on the target hosts (Enable-PSRemoting on the target)
- Alternatively: check scan credentials — the account must have admin rights on the target host

9.3 "No CIM access" for many hosts

- Common with workgroup hosts or hosts in foreign domains
- Enable the firewall rule "Windows Management Instrumentation (WMI-In)" on the target hosts
- On Linux servers "No CIM" appears → SMB probe fallback on port 445 shows them as an "SMB server" marker
- On NFS servers: TCP port 2049 is probed — if open, an NFS server entry appears

9.4 Telnet warning in BSI tab even though no Telnet is known

Some embedded devices (printers, older switches) have port 23 open. Check the ports table in the database, close the port on the device, or document the exception.

9.5 Service does not start (Linux)

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

Common causes: port 8585 occupied (stop the other service or adjust the --port flag in the systemd unit), wrong file permissions (chown -R itscanner:itscanner /var/lib/itscanner-server).

9.6 Service does not start (Windows)

```
# Open Event Viewer
eventvwr.msc

# Filter the Application log on "IT-Network DocuScanner"
# Common: database path not writable
# or port 8585 occupied
```

10. Appendix

10.1 REST API endpoints

Endpoint	Method	Purpose
/api/health	GET	Status + version
/api/dashboard	GET	Summary metrics
/api/hosts	GET	Host list
/api/software	GET	Software list
/api/shares	GET	Share list
/api/licenses	GET	License keys
/api/ad	GET	AD objects (filter: ?type, ?search)
/api/ad/stats	GET	AD counter
/api/ad/query	POST	Trigger live LDAP query
/api/subnets	GET	Subnets (with auto-derive)
/api/server-roles	GET	Server roles (filter: ?host, ?status)
/api/bsi	GET	BSI checks (with auto-derive)
/api/scans	GET	Scan history
/api/jobs	GET/POST	Scan jobs
/api/jobs/{id}/trigger	POST	Start scan
/api/update/check	GET/POST	Update check (GitHub)
/api/logs	GET	Log entries

10.2 Version scheme

Sat-iTec uses a three-part version scheme X.YY.ZZ:

- X = Major (rare, larger architecture changes)
- YY = Minor (new features, Y is written two digits)
- ZZ = Patch (bug fixes, Z is written two digits)

Example: 2.08.14 = Major 2, Minor 8, Patch 14. A new feature increases YY (e.g. 2.09.00), a bug fix increases ZZ (e.g. 2.08.15).

10.3 Support contact

Sat-iTec Systemhaus GmbH

Email: support@sat-itec.se

Web: https://www.sat-itec.se

GitHub releases: https://github.com/satitec/itscanner/releases