FIRST-TIME USER WALKTHROUGH

Running Siemserva & Generating Your First Report

A step-by-step guide to installing the scanner, running your first scan of Microsoft 365, Intune, Defender, and Entra ID, and producing a shareable security report.

Siemserva by Senserva, LLC • Microsoft Intelligent Security Association (MISA) Member • senserva.com

Siemserva is a lightweight, self-contained security scanner. There is no installer and no runtime to set up. Download one file, run it, and a guided wizard takes you from zero to a full HTML report in minutes. This walkthrough follows the recommended path for a brand-new user.

What you will accomplish

1. Install & launch
Download the single binary and start the first-run wizard.

2. Set up shared storage
Point Siemserva at a remote Azure Tables backend your team shares.

3. Run a scan
Try the built-in demo, or scan your real tenant.

4. Review findings
Navigate the live terminal dashboard by Severity.

5. Generate a report
Press `R` and produce a self-contained HTML report.

6. Connect Claude (MCP)
Query your scan data in plain English through the MCP server.

Before you begin

Requirement	Detail
Operating system	Windows 10+ or macOS (x64 / Apple Silicon)
Runtime	None. The binary is fully self-contained (about 50 MB disk).
Network	HTTPS access to the Microsoft Graph API (only needed for a real tenant scan, not the demo).
Permissions	Read-only Microsoft Graph access. No changes are ever written to your tenant.
AI (optional)	An Anthropic Claude API key enables AI-enhanced report sections. Not required to scan or report.

No tenant yet? You do not need a Microsoft 365 tenant or any credentials to try Siemserva. The built-in demo (three fictional tenants, around 280 findings) gives you the full dashboard and report experience with no login and no key.

Part 1 • Install and launch

1 Download the binary

Grab the latest signed release for your platform. There is no installer, just one executable.

Platform	How to get it
Windows (x64)	Download `siemserva-win-x64-signed.exe` from the Releases page, or `winget install Senserva.Siemserva`
macOS (Apple Silicon)	Download the `siemserva-osx-arm64.zip`, unzip, then run `run-siemserva.sh` on first launch (it clears the macOS quarantine flag)

> All releases are code-signed with Azure Artifact Signing. On Windows you can verify with `Get-AuthenticodeSignature .\siemserva.exe`.

2 Run it for the first time

Open a terminal in the folder where you saved the file and run it with no arguments. This starts the first-run wizard.

```
# Windows
siemserva.exe

# macOS
./siemserva
```

On first launch the wizard presents the End User License Agreement. Accept it once. Your acceptance is saved to a local `.eula-accepted` file so future runs start instantly. For automated or scheduled runs, pass `--accept-eula`.

3 Choose your setup path

The Welcome screen offers two ways forward. First-time users should pick **Quick Setup**.

Option	What it does
Recommended Quick Setup	One keypress builds the demo database (Zava, Contoso, Fabrikam), optionally wires Claude Desktop over MCP, and opens a personalized Next Steps page in your browser. Takes about 5 seconds. EULA required, license not.
Guided Setup	Step-by-step wizard for a real tenant: pick tenant, license, login method, scan depth, and add-ons, then review. Every step has Go Back, Cancel, and Help.

> You can re-run this wizard at any time with `siemserva --setup`, and reopen the Next Steps page with `siemserva --next-steps`.

> **Next, before scanning a real tenant:** set up shared remote storage so your team works from one set of scan data. See Part 2.

Part 2 • Set up shared remote storage Recommended

Do this before your first real scan. By default Siemserva keeps scan data in a local `senserva.sqlite` file, which only the one person on that one machine can see. Pointing Siemserva at **remote Azure Tables storage** lets your whole team scan and review the same tenants from any machine, with concurrent scans coordinated automatically. Set it up once and every later scan lands in shared storage.

1 Have an Azure Storage account ready

Remote storage uses an Azure Storage account that you own. Any general-purpose v2 account works; Table Storage is included with nothing extra to enable, and typical Siemserva usage costs well under a dollar per month. If you do not have one yet, create one first (Azure portal, about two minutes): learn.microsoft.com/azure/storage/common/storage-account-create.

2 Run the storage wizard

From the folder with the binary, launch the interactive storage setup. Choose **Azure Tables** when prompted, this is the shared, remote path.

```
siemserva setup-storage
```

> **SQLite vs. Azure Tables.** SQLite is a single local file for one operator on one machine. Azure Tables is the shared remote backend for teams. Pick **Azure Tables** here to get everyone on the same scan data.

3 Authenticate to the account

The wizard offers two ways to connect. Either works; the second avoids storing a secret.

Method	What you provide
Connection string (simplest)	Azure portal → Storage account → **Access keys** → Show keys → copy the key1 **Connection string** and paste it in. Treat it like a password.
Microsoft Entra sign-in (no stored secret)	The Table service URI `https://<account>.table.core.windows.net` and the owning Tenant ID. You need the **Storage Table Data Contributor** role; the wizard tries to assign it for you.

> **Secrets stay encrypted.** Credentials are saved only to the encrypted config (`~/.senserva/config.enc` , AES-256-GCM), never in plaintext. The wizard tests connectivity before saving. Entra role assignments can take up to two minutes to propagate, so if the test fails right after assigning the role, wait briefly and re-run `siemserva setup-storage` .

4 Confirm the local read cache

With Azure Tables selected, Siemserva mirrors the account into a small local SQLite cache (under `azure-cache/`) at scan startup so reads come from disk instead of the network. Keep the cache between scans (default, faster) or delete it after each scan on shared or locked-down machines. The cache is convenience data only; Azure remains the source of truth and scan locks are never cached.

You are now on the shared path. Every scan from here writes to your remote Azure Tables account, so teammates pointed at the same account see the same findings. Re-run `siemserva setup-storage` any time to switch back to local SQLite or reconfigure.

Part 3 • Run your first scan

Option A: Explore with the demo (no login, no key)

The fastest way to see everything. The demo builds a local database and opens the dashboard immediately, with the same findings, reports, and queries you get from a real scan.

```
# Build the demo database and open the dashboard
siemserva demo

# Explicit form (identical to above)
siemserva demo dashboard
```

Option B: Scan a real tenant

If you completed Guided Setup, the scan starts automatically. To scan directly without the wizard, pass your tenant ID:

```
# Scan a single tenant interactively
siemserva --tenantids <your-tenant-id>

# Scan several tenants at once
siemserva --tenantids <tenant-1> <tenant-2>
```

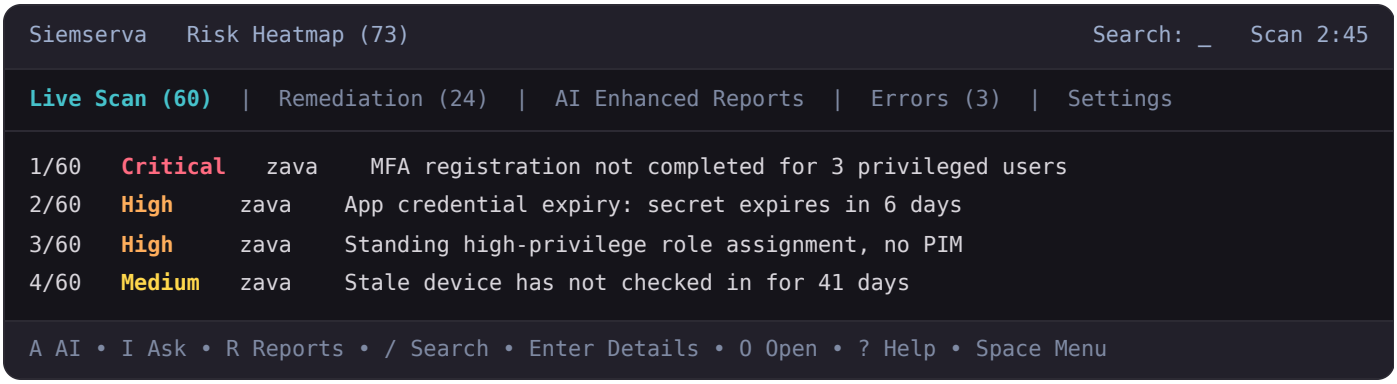
> **Read-only by design.** Siemserva only needs read scopes such as `User.Read.All`, `Policy.Read.All`, `Device.Read.All`, and `AuditLog.Read.All`. It never modifies your tenant. You sign in with your own account or an app registration during the wizard's login step.

What a scan covers

A single run executes 650+ checks across 18 domains, mapped automatically to the Microsoft Cloud Security Benchmark (MCSB) and CISA SCuBA frameworks. Coverage spans identity and MFA, Conditional Access, PIM, applications and service principals, Intune devices, Defender endpoint protection, sign-in and directory logs, and Purview.

Part 4 • Review results in the dashboard

As the scan runs, findings stream into the live terminal dashboard, sorted by Severity. Critical and High items rise to the top so you see what matters first.



Essential navigation keys

Key	Action
`Up` / `Down`	Move the cursor through findings
`Enter`	Open full detail for the selected finding
`/`	Search findings
`[` / `]`	Cycle the Severity filter (for example, show only High and above)
`I`	Ask a plain-language question about your scan data
`O`	Open the current tab or finding as HTML in your browser
`R`	Open the report picker (covered next)
`?`	Help overlay • `Q` Quit (double-tap to confirm)

Part 5 • Generate your first report

1 Open the report picker

From any tab in the dashboard, press `R`. Siemserva offers six report types, each tailored to a different audience.

#	Report	Best for
1	**Detailed**	Sysadmins and security engineers: every finding, with technical drill-down
2	**Compliance**	Compliance officers: MCSB and SCuBA control status and gap analysis
3	**Business Focused Review**	VPs, CFOs, IT directors: business risk and investment decisions
4	**Remediation**	SOC and IT ops: priority-ordered fixes with step-by-step instructions
5	**Audit**	Security auditors: a formal, branded audit trail
6	**Portfolio**	MSPs and MSSPs: a multi-tenant view across managed clients

> **New user tip.** Start with the **Detailed** or **Remediation** report. They give you the clearest, most actionable picture of what to fix first.

2 Pick a report and let it build

Select a number. Siemserva generates a self-contained HTML file with embedded CSS and inline graphics, then opens it in your default browser. No external assets, no internet needed to view it. To open the current view directly without the picker, press `O`.

3 Add AI insights (optional)

Two ways to enrich a report with AI analysis:

- **With an API key:** run `siemserva setup-ai` once (or set `ANTHROPIC_API_KEY`). Then press `R`, pick a report, and press `A` so AI analysis streams directly into the report.
- **Without a key (copy-paste):** press `A` to copy a PII-scrubbed prompt to your clipboard, paste it into any AI tool, copy the reply, and press `Ctrl+V` to import it. Then press `R` to build the report with those insights.

> **Privacy first.** Before anything leaves your machine, all PII (tenant names, user names, email addresses, and GUIDs) is replaced with anonymized session aliases.

4

Save or share as PDF

Every report is standard HTML. To share a fixed copy, open it in your browser and use **Print → Save as PDF**. For full native PDF and Excel exports plus trend comparison, the Senserva Manager add-on reads the same scan data.

Prefer the command line? Batch mode

You can split scanning and reporting into composable halves and generate all six reports in one command, no dashboard required:

```
# Scan once, then generate all 6 HTML reports from the result
siemserva --scan --tenantids <id> | siemserva --reporter

# Only specific reports, High severity and above
siemserva --reporter --reporter-reports Detailed,Remediation --reporter-severity High <
scan-results.json
```

Part 6 • Connect the MCP server to Claude

Siemserva can run as a **Model Context Protocol (MCP) server**, so Claude Desktop and the Claude Code CLI can query your scan data, look up remediation guidance, and build reports through 31 purpose-built tools. Once connected, you ask questions in plain English and Claude answers from your own findings.

1 Quickest path: demo + Claude (no login, no key)

One command builds a demo database, wires it into Claude Desktop, and opens Claude. Use this to confirm the connection works end to end.

```
# Build the demo db, install the MCP server, open Claude Desktop
siemserva demo claude

# Target the Claude Code CLI instead
siemserva demo claude --cli
```

2 Install MCP against your real scan data

If you have already run a scan, register the MCP server with your client directly. Run these from the folder that holds your scan files.

```
# Claude Desktop (Windows / macOS)
siemserva --claude mcp-install

# Claude Code (CLI)
siemserva --claude cli-install

# Uninstall later
siemserva --claude mcp-remove
```

> The connection is written to your Claude config file:
>
> - Windows: `%APPDATA%\Claude\claude_desktop_config.json`
> - macOS: `~/Library/Application Support/Claude/claude_desktop_config.json`

3 Point it at the right scan data

When the MCP server starts with no explicit database flag, it auto-discovers scan files in the current working directory: every `*.sqlite`, `*.db`, and `*.senserva-db` file is opened, and any `*.zip` archive is extracted so embedded databases load too. Start it from a folder holding your scans and they all load at once.

```
# Auto-discover and serve every scan file in this folder
siemserva --mcp

# Or name exactly which databases to load
siemserva --mcp --mcp-dbs scan-a.sqlite scan-b.sqlite
```

> **Explicit paths win.** Passing `--reporter-db <path>` or `--mcp-dbs <a> <b>` overrides auto-discovery and loads only the files you list.

4 Ask Claude about your tenant

Restart Claude Desktop (or your Claude Code session) so it picks up the new server, then ask in plain English. Claude answers from your scan data through the MCP tools:

- *"Which admins have no MFA?"*
- *"Summarize the top 5 risks in my Siemserva scan."*
- *"What CVEs affect my Windows fleet?"*

> **Tip.** If Siemserva is already on the shared remote storage path from Part 2, anyone with the MCP server pointed at the same scan data can ask Claude the same questions and get consistent answers.

You are done

You have installed Siemserva, run a scan, reviewed findings by Severity in the live dashboard, and produced a shareable report. From here:

- Run `siemserva --setup` any time to reconfigure, or `siemserva --full-help` for the complete in-browser guide.
- Use SIEM mode (`siemserva --siem --tenantids <id>`) to rescan on a schedule and watch posture over time.
- For deeper documentation, see the User's Guide, the checks reference, and the dashboard guide that ship with the product.