

Siemserva Claude Integration Quick Reference Instructions

Presumption:

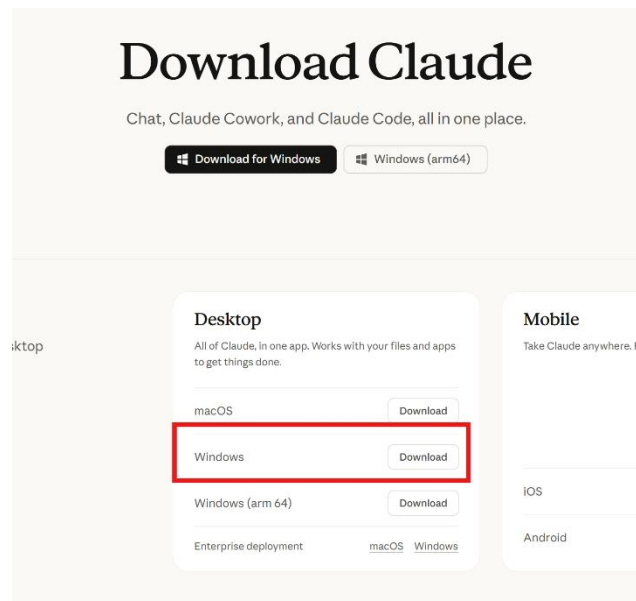
Running on Windows 11

Siemserva version 20260528.2323

Note: If you have completed the Claude setup and built the demo database previously, skip to the Claude prompting section in step 13.

Instructions:

- 1) Install Siemserva executable from the GetFree email which came in from tj@senserva.com
 - a. If previously downloaded: Verify your Siemserva version by 20260528.2323 by using the command `".\siemserva-win-x64.exe --version"`
 - i. **If non-current version:** Delete the file and click the **windows EXE** direct download from the GetFree email, which came in from tj@senserva.com.
- 2) Install Claude Desktop (Specifically Claude Desktop, not Claude Code). If already installed skip to step 3.
<https://claude.com/download>



- 3) If Claude desktop was previously installed: close Claude from Task Manager, the app runs some functions in the background that must be closed.
- 4) Move Siemserva executed from Downloads to a new file directory. **DO NOT run from downloads.**

- 8) You will see a message about setting up the MCP server and a message that Claude Desktop must be restarted. **Select either 'y' or 'n'.**
- If **'y'**: your Claude Desktop will close automatically. Once closed, manually reopen Claude.
 - If **'n'**: you will be directed to close Claude Desktop manually. Close Claude and reopen Claude manually.

```
>siemserva-win-x64.exe --claude self-install

Claude Self-Install
=====
Setting Claude up to drive Siemserva...

WARNING: Running from the Downloads folder
-----
siemserva-win-x64 is running from:
-----
Do NOT run siemserva-win-x64 from your Downloads folder. Problems this causes:
- macOS will prompt for Sandbox/TCC permissions every time
- The config file will embed a path inside Downloads, which breaks
  after you move or rename the binary
- The MCP server will fail to start once the binary is cleaned up

Move siemserva-win-x64 to a stable location first, then re-run install:
Windows: copy to C:\Tools\siemserva-win-x64.exe or C:\Users\<you>\bin\

Claude Desktop configured for Siemserva MCP
=====
Config:  claudes_desktop_config.json
Command: siemserva-win-x64.exe
Databases: 1
          zava-small.sqlite

Once Claude is restarted, just ask things like:

"How secure am I?"           - Claude builds a demo and walks you through it
"Reviewer's guide"          - guided tour of the top findings
"Run a compliance review"    - auditor walkthrough: GCC High? NIST 800-171? then SCuBA / MCSB / SOC 2 / ISO 27001
"Check NIST 800-171 compliance" - 14-family walk: compliant / partial / not-compliant per family with Siemserva evidence
"Show me what I need to fix" - prioritized fix list with PowerShell
"Build a Compliance report"  - branded HTML report you can share
"Shall We Play a Game"      - challenging interactive learning experience
"Open the help guide"       - full illustrated Siemserva docs in your browser
"Scan my tenant"            - real-tenant scan (license required)

No commands to memorize. Just talk to Claude.

-----
CLAUDE DESKTOP MUST BE RESTARTED FOR THE NEW MCP SERVER TO LOAD
-----
Claude Desktop reads its MCP config only at process startup.
Until you fully quit and reopen Claude, it cannot see Senserva.

Claude Desktop is not running. Open Claude Desktop now and the new
Siemserva MCP server will load on startup.

Watching for the restart (up to 60 seconds)...

Detected: Claude restarted, but no MCP log activity yet. The server
may still be starting. If Claude reports a problem, run:
siemserva-win-x64 --claude doctor

Bye!
```

- 9) Rerun the **“.\siemserva-win-x64-signed.exe --claude doctor”** command to see status. It may again prompt for Claude Desktop to be restarted, but this is optional.
- 10) Verify that the Configuration is updated in the Claude Desktop MCP settings at **“%AppData%\Claude\claude_desktop_config.json”**. When you view the JSON file in Notepad (or other viewer), the mcpServers property will be populated with a “Siemserva” configuration.

```
{
  "mcpServers": {
    "Siemserva": {
      "command": "C:\\<path_to_siemserva>\\siemserva-win-x64-signed.exe",
      "args": [
        "--accept-eula",
        "--mcp",
        "--reporter-db",
        "C:\\<path_to_siemserva>\\zava-small.sqlite"
      ]
    }
  }
}
```

11) Build the demo database by running “.\siemserva-win-x64-signed.exe demo build small”.

Note: if desired you may also build the medium and large databases using prompts:

“.\siemserva-win-x64-signed.exe demo build **medium**”

“.\siemserva-win-x64-signed.exe demo build **large**”

Or ““.\siemserva-win-x64-signed.exe demo build **all**”.



```
Siemserva, The AI
Cometh

First Scan in Minutes · Next Scans in Seconds · 7x24 SIEM Mode

By using Siemserva you agree to our EULA. Siemserva Beta 5 © Senserva, LLC
www.senserva.com. Provided as-is without warranty of any kind. Patent US11729201B2, and others.

Siemserva Beta 5 Build 20260523.0354 - up to date.

Small (250 users)
Generating zava-small.sqlite (250 users, 275 devices, 45 groups, 25 apps, 75 service principals).
Creating database schema
SQLite tables and indexes. Where the 580+ Siemserva checks land. Self-contained, single file, no server.
Zava Demo Seeding tenant
Tenant identity, domain, country. Every finding points back to one of these; lose the tenant id and multi-tenant
rollups break.abase schema 3% 00:00:01 00:00:28
Zava Demo Seeding 250 users
Real-looking names and UPNs, mix of admins and staff. Some lack MFA on purpose. Most breaches start at the
unprotected identity.chema 3% 00:00:01 00:00:28
```

12) When complete the build will say “bye”. Exit command prompt.

13) Open the Claude Desktop app.

14) Ask Claude “Do you have Siemserva?”

- If **yes**: interact with the demo following step 16.
- If **no**: open task manager and end all background Claude processes. This refreshes the MCP server configurations. Reopen Claude and retry the query.

i. If **no again**: reopen command prompt as described above and run

“.\siemserva-win-x64-signed.exe --claude doctor”

- Follow command prompt instructions.
- If no clear action is given reach out to tiffany@senserva.com for further assistance.

15) If Claude says Siemserva is available, it may ask you to enter the Demo Key. Follow Claude prompts.

- If Claude fails to recognize the demo SQLite file prompt Claude “**Look in the directory for the zava.sqlite database**”

i. If further assistance is required reach out to tiffany@senserva.com

16) Begin interacting with the Demo.

Below are some possible prompts and the Claude outputs. For pricing reach out to clay@senserva.com. For all other inquires reach out to tiffany@senserva.com

Can you tell me which tenants are available in Siemserva?

Loaded tools, used Siemserva integration >

There are 3 tenants currently available in Siemserva:

| # | Tenant Name | Tenant ID |
|---|----------------------|--------------------------------------|
| 1 | Zava Demo | 11111111-2222-3333-4444-555555555555 |
| 2 | Contoso Retail | 22222222-3333-4444-5555-666666666666 |
| 3 | Fabrikam Engineering | 33333333-4444-5555-6666-777777777777 |

Would you like to drill into any of these tenants — view findings, check severity summaries, or compare two of them side by side?



Please list the top 3 vulnerabilities.

Loaded tools, used Siemserva integration >

Here are the top 3 critical vulnerabilities across your tenants:

- 1. Missing Critical Windows Patch (Zava Demo)** A missing cumulative update for Windows 11 24H2 exposes the environment to CVE-2025-21298 and CVE-2025-21333, both of which are listed on CISA's Known Exploited Vulnerabilities (KEV) catalog — meaning they are being actively exploited in the wild.
- 2. Bulk Password-Change Operation (Zava Demo)** User Marcus Henderson was the entity associated with a bulk password-change targeting 100 users within 15 minutes — a strong indicator of a compromised account or an insider threat event.
- 3. App with High-Risk Permissions (Fabrikam Engineering)** Adobe Creative Cloud has been flagged for holding high-risk application permissions, which could allow it to access sensitive data or perform privileged actions beyond what's necessary.

There are 14 critical findings in total. Would you like to see more, get remediation guidance for any of these, or drill into a specific tenant?

