

MCP szerver: telepítés és üzemeltetés

Ez az oldal a **rendszergazdának** szól: az [eVIR MCP szerver](#) modul telepítése, webszerver-konfigurációja és üzemeltetése. A felhasználói oldal — csatlakozás az AI-alkalmazásból — külön oldalon: [Hozzáférés engedélyezése](#).

<note warning>**A modul webszerver-oldali beállítás nélkül NEM működik.** A telepítés önmagában kevés: az Apache alapértelmezésben nem adja át a CGI-nek azt a fejléctet, amiben a hozzáférési kulcs utazik, így minden hívás elutasításra kerülne.</note>

1. A modul telepítése

```
cd install
TESTNONINTERACTIVE=1 NOSUDO=1 ./control /path/to/instance install_module ai_mcp
</dev/null
```

Ez létrehozza az `ai_mcp_*` táblákat, bekapcsolja a modult, felveszi a karbantartó job ütemezését, majd automatikusan lefuttatja a menu és adminjog lépéseket is.

Ellenőrzés: a Rendszer → Beállítások → AI MCP hozzáférés menücsoporthoz meg kell jelennie (am01-am05 jogkódok).

2. Webszerver-konfiguráció

Minta a példány forrásában: `install/modules/ai_mcp/apache-mcp.conf.sample`. Nem automatikusan telepítendő fájl — másold az ügyfél vhostjába és igazítsd az útvonalakat.

Két dolog kell mindenképpen:

1. **CGIPassAuth On** a `cgi-bin` könyvtárra (Apache 2.4.13+). A Bearer token az Authorization fejlécben utazik, amit az Apache alpból nem ad át a CGI-nek. Régebbi Apache-hoz tartalék: `RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]` — a `mcp.cgi` mindhárom változatot megnézi.
2. **Rewrite** a `/mcp` útvonalról a `cgi-bin/mcp.cgi`-re.

<note>**Telepítés előtt ellenőrizd, hogy a /mcp útvonalat nem használja-e már valami** az adott példányon (webshop, CMS).</note>

Alkönyvtáras vs. gyöker-telepítés

	alkönyvtáras (https://host/ugyfel/)	gyöker (saját vhost)
base URL	https://host/ugyfel/mcp	https://ugyfel.pelda.hu/mcp
.well-known	a példány alatt	a host gyökerében is

A szabvány (RFC 9728, RFC 8414) szerint path-komponenses issuernél a metadata a **host gyökerében** lenne, amihez alkönyvtáras telepítésnél nincs feltétlenül hozzáférésünk. Ezért a `mcp.cgi` az elutasító válasz `WWW-Authenticate` fejlécében **explicit megadja** a metadata URL-jét (`resource_metadata=„...”`), és a kliensek azt követik — a példány alatti útvonal így elegendő, gyöker-hozzáférés nem kell. A minta a gyöker-szintű változatot is tartalmazza (kikommentelve), az ACME/Let's Encrypt kivétellel együtt.

3. Beállítások

Rendszer → Beállítások → Rendszerbeállítások → **eVIR MCP szerver (AI hozzáférés)**.
Részletesen: [Beállítások: eVIR MCP szerver](#).

Telepítés után jellemzően csak egyet kell átnézni: **az MCP végpont publikus URL-jét**. Üresen hagyva a `setup.pm web_url_host` értékéből származik, `/mcp` végződéssel — ez a szokásos esetben helyes.

<note important>A base URL egyben az OAuth **issuer és resource azonosító** is. Utólagos megváltoztatása **érvényteleníti a már kiadott hozzáféréseket**, a felhasználóknak újra kell engedélyezniük.</note>

4. Ki kaphat hozzáférést

MCP privilégium kell hozzá (`users.privek`). Enélkül a felhasználó látja az engedélyező képernyőt, de nem tud hozzáférést adni. A privilégiumot a [Felhasználók](#) felületen lehet megadni; adminisztrátoroknak a `control adminjog` automatikusan adja.

<note important>A privilégium ellenőrzése **minden egyes hívásnál** megtörténik, nem csak a hozzáférés kiadásakor. Ha egy felhasználótól elveszik az MCP privilégiumot, a már kiadott hozzáférés **azonnal** érvénytelenné válik — nem kell megvárni a lejáratát.</note>

5. Karbantartó job

Nincs vele teendő: a telepítés felveszi. A modul telepítő SQL-je aktív crontab sort hoz létre (naponta 03:17), ami a lejárt technikai sorokat — függő kérések, felhasznált kódok, lejárt tokenek, hívásszám-számlálók — takarítja.

Ellenőrzés:

```
SELECT ct_min,ct_hour,dok,megj,aktiv FROM crontab WHERE dok LIKE 'ai_mcp%';
```

Az időpont a Rendszer → Beállítások → [Ütemezett feladatok](#) menüpontban módosítható, és a job ki is kapcsolható.

<note>A job a **hívásnaplóhoz nem nyúl**. A napló törlése tudatos adminisztrátori döntés, nem automatizmus — lásd [MCP hívásnapló](#).</note>

6. Ellenőrzés telepítés után

```
# metadata (nem igényel bejelentkezést)
curl -s https://<host>/<ugyfel>/mcp/.well-known/oauth-protected-resource

# az MCP végpont token nélkül: 401 + WWW-Authenticate
curl -si -X POST https://<host>/<ugyfel>/mcp \
  -H 'Content-Type: application/json' \
  -d '{"jsonrpc":"2.0","id":1,"method":"tools/list"}' | head -20
```

Az elutasító válaszban **kötelezően** ott kell lennie a `WWW-Authenticate: Bearer ... resource_metadata=,,,"` fejlécnek — ez indítja a kliens oldali bejelentkezést. Ha hiányzik, az AI-alkalmazás nem tud csatlakozni.

Hibakeresés

Tünet	Legvalószínűbb ok
A bejelentkezés <i>után</i> is elutasítás jön	hiányzik a CGIPassAuth → az Authorization fejléc nem jut el a CGI-hez
A kliens nem talál metadatát	a .well-known rewrite hiányzik, vagy rossz a base URL beállítás
„Ismeretlen alkalmazás,” a visszatéréskor	a base URL megváltozott a hozzáférés kiadása óta
A felhasználó nem tud engedélyezni	nincs MCP privilégiuma
Egyes funkciók hiányoznak a kliensben	az adott modul nincs telepítve, vagy a felhasználónak nincs rá menü-jogosultsága — ez helyes működés , lásd Elérhető funkciók

7. Több példány egy ügyfélnél (teszt + éles)

Technikailag tiszta: az audience-ellenőrzés miatt egy hozzáférési kulcs **nem használható másik példányon**. Feltétel, hogy a két base URL különbözzön — ha a teszt példány ugyanarról a hostról, más alkönyvtárból megy, ez magától teljesül; ha nem, állítsd be kézzel. Az AI-alkalmazásban két külön kapcsolat lesz belőlük.

Kapcsolódó oldalak:

- [eVIR MCP szerver \(áttekintés\)](#)
- [Beállítások: eVIR MCP szerver](#)
- [Adatbiztonság](#)
- [Felhasználók](#)

From:

<https://www.doc.evir.hu/> - **eVIR tudásbázis**

Permanent link:

https://www.doc.evir.hu/doku.php/evir:rendszer:ai_mcp:telepites

Last update: **2026/08/28 16:03**

