

Connecting to an AI server



AI Overview

Connecting to an AI server involves configuring network access, using SDKs or APIs, and optionally setting up a local server for secure and high-performance AI operations.

Network and Access Requirements To connect to an AI server, ensure your network allows outbound traffic to the server's domain and port. For example, Burp AI requires HTTPS access to `ai.portswigger.net` on port 443, and firewalls or content filters may need to allowlist the server domain. If your network uses an upstream or intercepting proxy, you may need to configure your client to trust the proxy's certificate or provide proxy credentials.

Using an AI Server SDK Many AI servers provide SDKs for programmatic access. For instance, the `ai-server-sdk` Python package allows you to connect to an AI server using a `ServerClient` object. You provide your server URL, access key, and secret key to authenticate. Once connected, you can run queries, retrieve JSON responses, or integrate with frameworks like `LangChain` for advanced workflows. Example usage includes creating a `ModelEngine` instance and executing queries or database operations through the SDK.

```
PythonCopyfrom ai_server import ServerClient, ModelEngineloginKeys = {"secretKey":"","accessKey":""}server_connection = ServerClient(base="", access_key=loginKeys['accessKey'], secret_key=loginKeys['secretKey'])model = ModelEngine(engine_id="", insight_id=server_connection.cur_insight)response = model.run_query("Your query here")
```

Setting Up a Local AI Server For high-performance or private AI operations, you can build a local AI server. A typical setup includes a powerful CPU (e.g., AMD Ryzen 9 7950X), large RAM (128GB DDR5), and GPUs (e.g., dual NVIDIA RTX 4090) to handle large models efficiently. Operating systems like `Pop!_OS` or `Ubuntu` are commonly used. Once installed, you can access an admin portal to configure AI providers, generate API keys, and manage requests locally.

Admin Portal and API Access After installation, AI servers often provide a we...

Article Content

Connect to external tools with MCP

The Model Context Protocol (MCP) is an open standard for connecting AI agents to external tools and data sources. With MCP, your agent can query databases, integrate with APIs like Slack and GitHub,

Connect MCPs to AI assistants and coding agents

See managed MCP servers, MCP Services, and Databricks-hosted MCP servers for each feature's current stage. Connect clients, AI assistants, and IDEs that support Model Context

How to build a high-performance AI server locally

Building and setting up your very own high-performance local AI server offers a fantastic solution to this. Enabling you to tailor your server to your budget as well as keep all your...

A Jargon-Free Guide on How AI Server Architecture Works

Whether you're deploying AI in your business, tinkering with a project, or just want to understand the tech shaping our world, this guide discusses what

Home Assistant MCP Server – Connect Your AI | raspberry.tips

What is the Home Assistant MCP server? The MCP server (Model Context Protocol) is an interface that lets AIs like Claude, ChatGPT, or Gemini talk directly to your Home Assistant. Instead

Introducing the Model Context Protocol Anthropic

The Model Context Protocol (MCP) is an open standard for connecting AI assistants to the systems where data lives, including content

Local AI Server A Step by Step Guide to Setup and Use

Learn to set up and use your local AI server with this comprehensive guide. Enhance your projects today—read the article for step-by-step instructions!

MCP and Connectors | OpenAI API

Remote MCP servers can be any server on the public Internet that implements a remote Model Context Protocol (MCP) server. This guide will show how to use

Home AI Server Build Guide 2026 — Always-On Local

Build a dedicated home AI server that runs 24/7 — serving LLMs to every device on your network. Hardware picks, networking, storage, remote

Quick Start

The installer will detect common environment variables for its supported AI Providers including OpenAI, Anthropic, Mistral AI, Google, etc. and prompt if you would like to include any others in your AI

Higgsfield MCP | AI Image & Video Generation for Any

Add the Higgsfield MCP server to Claude, OpenClaw, Hermes Agent, NemoClaw, or any MCP-compatible client. 30+ models for image and video generation, no API

How I Connected Claude AI to My SAP ABAP System Us...

Introduction The SAP developer community has been buzzing about connecting Claude AI directly to live SAP ABAP systems using MCP (Model Context Protocol) — reading code, modifying

Self-Hosted AI: A Complete Roadmap for Beginners

In this article, I will walk you through building a self-hosted AI workflow hub on a home server, giving you complete control, greater privacy, and powerful

Connect to the NetSuite AI Connector Service

Connect to the NetSuite AI Connector Service Important Before connecting to the NetSuite AI Connector Service, it's important to familiarize yourself with Associated Risks, Controls, and Mitigation

What is an AI Server? AI Server Architecture Explained

In this quick guide, we'll walk you through everything you need to know before deploying your first AI server configuration, covering most of your burning questions.

Get started with AI and MCP

MCP client-server architecture MCP uses a client-server architecture that enables an AI-powered app (the host) to connect to multiple MCP servers

Clari + Salesloft Introduce MCP Server to Expand AI

Clari and Salesloft introduce MCP Server and new tools, connecting revenue intelligence to execution and expanding AI-driven insights.

Remote connections - Codex | OpenAI Developers

Remote connections let you use Codex from another device or another machine. Use Codex in the ChatGPT mobile app to work with Codex on a connected Mac

New in Claude Managed Agents: self-hosted sandboxes

Rogo, an AI platform for institutional finance, is building an analyst agent on Managed Agents and Vercel Sandbox to handle their proprietary data

Databricks managed MCP servers | Databricks on AWS

Reference for Databricks-managed MCP servers that connect AI agents to Unity Catalog data, AI Search, Genie Spaces, and custom functions with no setup.

Extend Atlassian into any AI assistant using MCP | Atlassian

The Atlassian Rovo MCP server connects to your preferred external AI clients, so you can securely access Atlassian data and context through MCP tools.

XBTFX Launches AI Trading Stack Connecting Compatible AI

XBTFX launches an AI trading stack connecting compatible AI agents to live crypto and CFD accounts via MCP Server, Skills Hub, and Trading API.

Unity AI Open Beta: How to get started

Unity AI is a suite of tools built into the Unity Editor for developers using Unity 6 or later. Unity AI includes the AI Assistant (Ask, Plan, and Agent modes), the MCP Server for connecting IDE

Comfy MCP: Turn Your AI Agent Into a Creative Technologist

Comfy Org launches Comfy MCP, connecting AI agents to ComfyUI via the Model Context Protocol. Agents can now search models, execute workflows, and generate images, video,

Connect MCPs to AI assistants and coding agents

The Databricks MCPs you can connect to are in different release stages. See managed MCP servers, MCP Services, and Databricks-hosted MCP servers for each feature's current stage.

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: <https://www.mr-security.co.za>

Email: info@mr-security.co.za

Phone: +33 1 45 23 67 81

Address: 10 Rue de la Paix, 75002 Paris, France

This document is for informational purposes only. Specifications subject to change without notice.

