AI Agent MCP Integration - Magento 2

- Installation
- Backend Configuration (Admin side)
- Backend Functionality
    - MCP Users
        - User Details
        - Edit User
    - Role-Based MCP Access Configuration
    - MCP Configuration in My Account
    - MCP Interaction Logs
- Frontend Functionality
    - Gemini CLI MCP Integration
    - OpenAI Codex MCP Integration
- Demo
- FAQs
- Support
- Additional Services

Installation

Before installing the extension, please make sure to **Backup your web directory and store database**

You will require to install MageDelight Base Extension first. If it is not installed then please download it from https://www.magedelight.com/pub/extensions/magedelight-base.zip and unzip the package file into the root folder of your Magento 2 installation.

Root Directory is - **"app/code/magedelight/#YourExtensionName#"**

- Unzip the extension package file into the root folder of your Magento 2 installation.
- Connect to SSH console of your server:
    - Navigate to the root folder of your Magento 2 setup
    - Run command as per below sequence,

```
php bin/magento setup:upgrade
```

```
php bin/magento setup:di:compile
```

```
php bin/magento setup:static-content:deploy
```

```
php bin/magento cache:clean
```

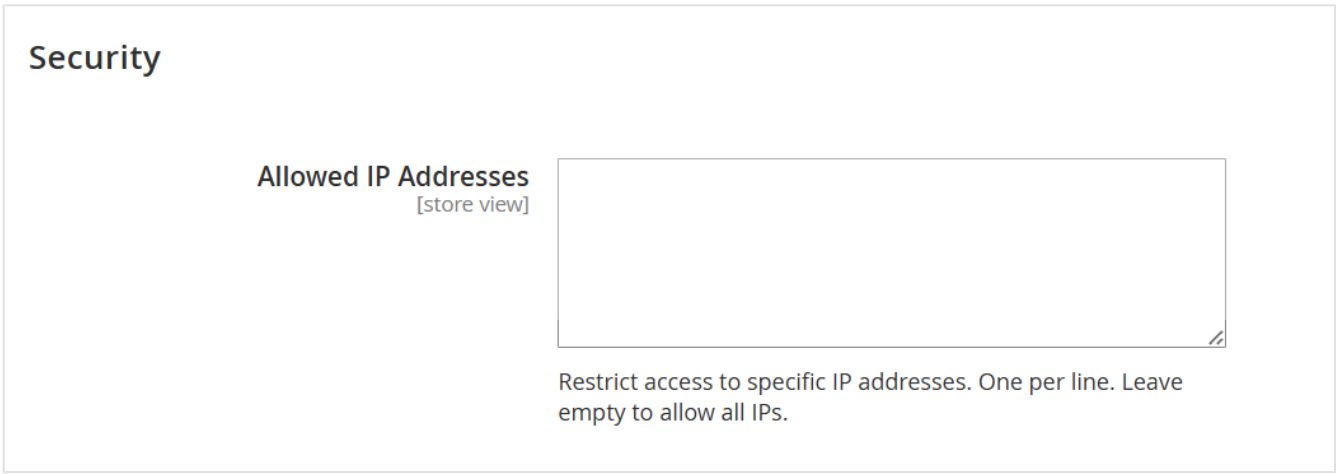
- log out from the backend and log in again

If you are using Magento 2.3 or later then you do not need to activate license. Extension will be activated with silent activation mechanism and does not require activation keys to be entered manually.

Copyright © 2021. MageDelight. All Rights Reserved.

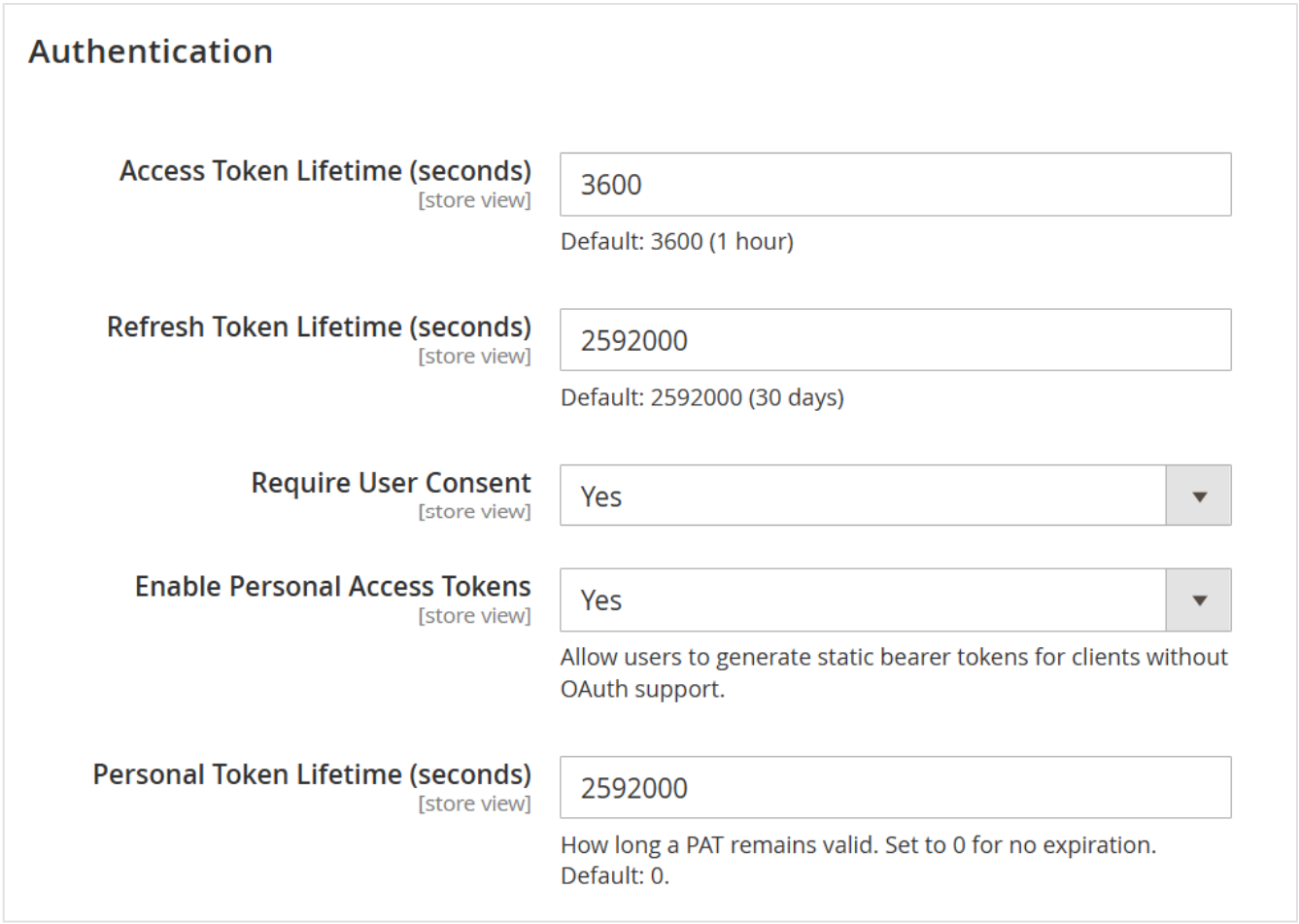
Backend Configuration (Admin side)

Field	Description
Enable MCP Server	This setting controls whether the MCP Server is active for the selected store view. When enabled, supported AI clients can connect to the store and interact with the available MCP features. When disabled, external AI connections through the MCP endpoint are blocked and the server will not respond to client requests. Default value: **Yes**.



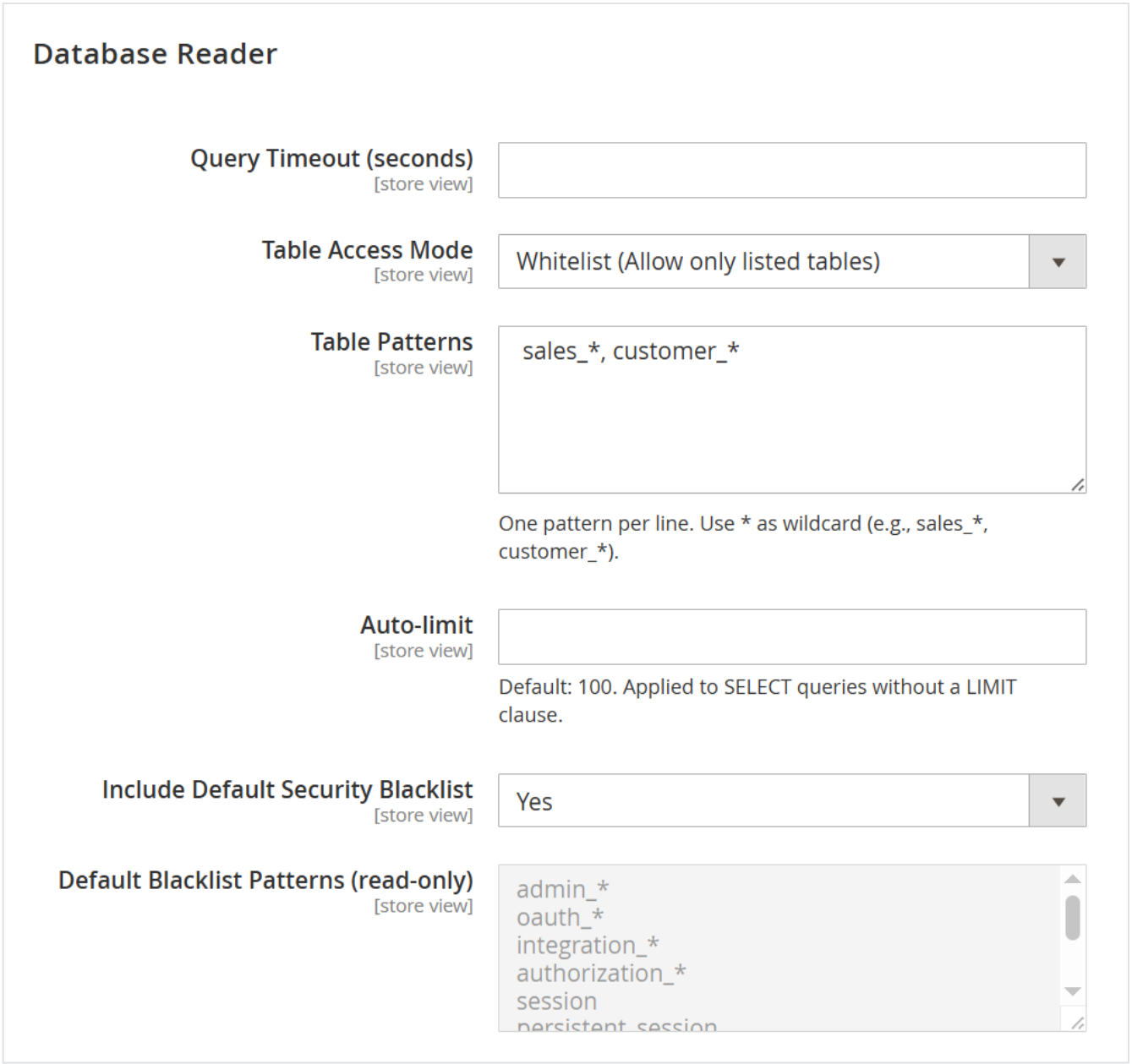
Field	Description
Allowed IP Addresses	Specify the IP addresses that are permitted to access the MCP Server. Add one IP address per line to restrict access only to trusted sources. If this field is left empty, the MCP Server will accept requests from all IP addresses.

Copyright © 2021. MageDelight. All Rights Reserved.



Field	Description
Access Token Lifetime (seconds)	Defines how long an issued access token remains valid before a new one must be obtained through the refresh flow. A shorter duration improves security, while a longer duration reduces the need for frequent token refresh requests.
Refresh Token Lifetime (seconds)	Specifies how long the connection can stay authorized without requiring the user to approve access again. Once this period ends, the client must complete the authorization process again to continue using the server.
Require User Consent	Determines whether users must explicitly approve access when an AI client attempts to connect. When enabled, a consent screen is shown before authorization is granted.
Enable Personal Access Tokens	Allows users to generate static bearer tokens for clients or tools that do not support OAuth-based authentication. This option is useful for external integrations that require direct token-based access.
Personal Token Lifetime (seconds)	Sets the validity period for generated personal access tokens. Enter **0** to keep the token active without expiration, or specify a duration in seconds to enforce automatic expiry.

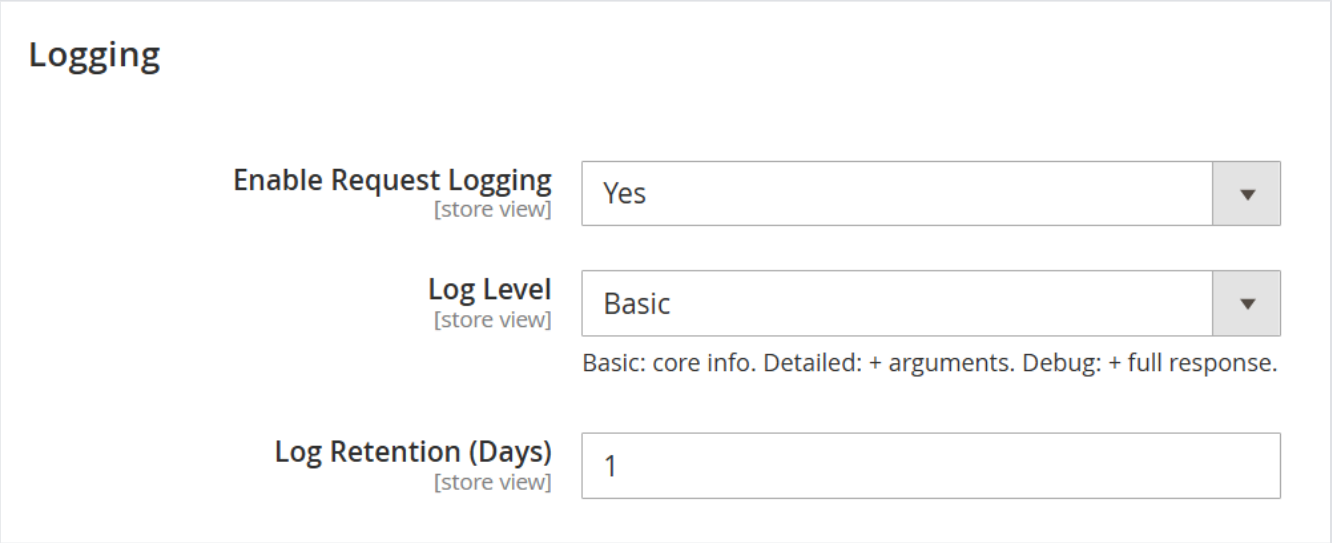
Copyright © 2021. MageDelight. All Rights Reserved.



Field	Description
Query Timeout (seconds)	Defines the maximum time allowed for a database query to run. If a query exceeds this limit, it is stopped automatically to help maintain performance and prevent long-running requests from affecting the system.
Table Access Mode	Controls how database table rules are applied. **Whitelist** allows access only to the tables that are explicitly listed, while **Blacklist** blocks the listed tables and keeps all other tables accessible.
Table Patterns	Use this field to define which tables should be allowed or blocked based on the selected access mode. Add one pattern per line, and use * as a wildcard to match multiple tables, such as `sales_*` or `customer_*`.
Auto-limit	Sets the default row limit for `SELECT` queries that do not already contain a `LIMIT` clause. This helps avoid returning very large result sets and keeps query responses more efficient.

Copyright © 2021. MageDelight. All Rights Reserved.

Include Default Security Blacklist	Enables the built-in protected table rules that automatically block access to sensitive database areas, such as tables containing credentials, tokens, sessions, and other restricted data.
Default Blacklist Patterns (read-only)	Displays the predefined restricted table patterns used by the default security blacklist. This field is for reference only and helps administrators understand which sensitive tables are protected by default.

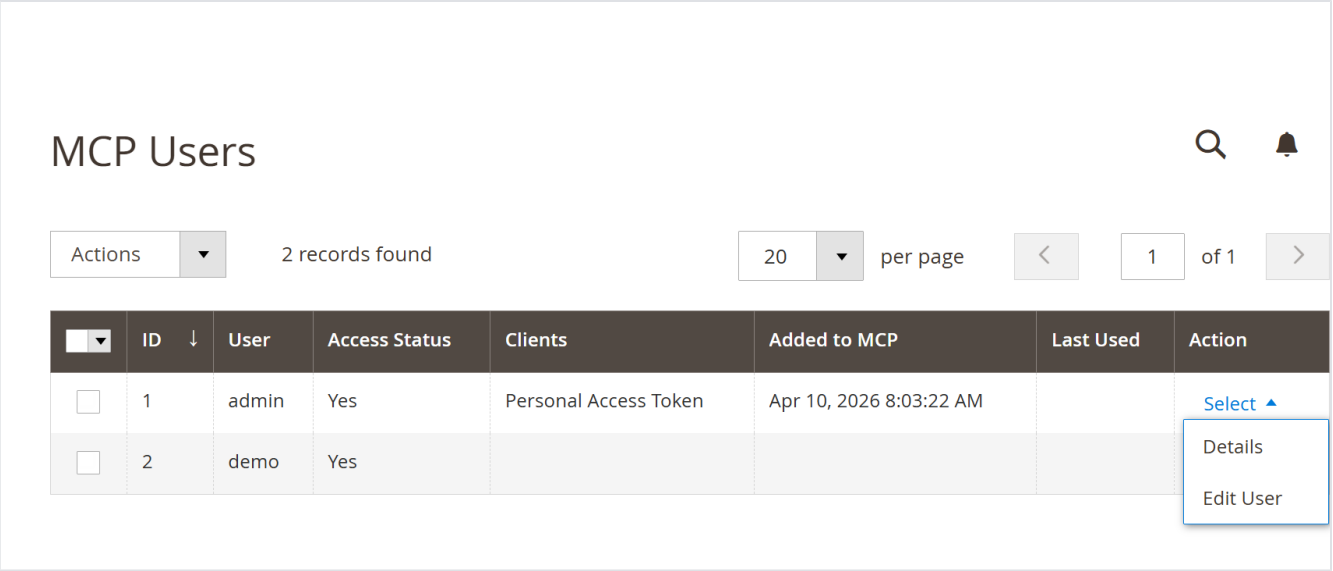


Field	Description
Enable Request Logging	Enables logging of MCP requests for monitoring and troubleshooting purposes. When enabled, the system records request activity so administrators can review interactions made through the MCP Server.
Log Level	Defines how much request information is stored in the logs. **Basic** records key request details, **Detailed** stores additional request arguments, and **Debug** captures the most complete response-level information for deeper analysis.
Log Retention (Days)	Specifies how long log records should be kept before cleanup. Set the number of days based on your monitoring needs, or use **0** to retain logs without automatic expiration.

Backend Functionality

MCP Users

Copyright © 2021. MageDelight. All Rights Reserved.

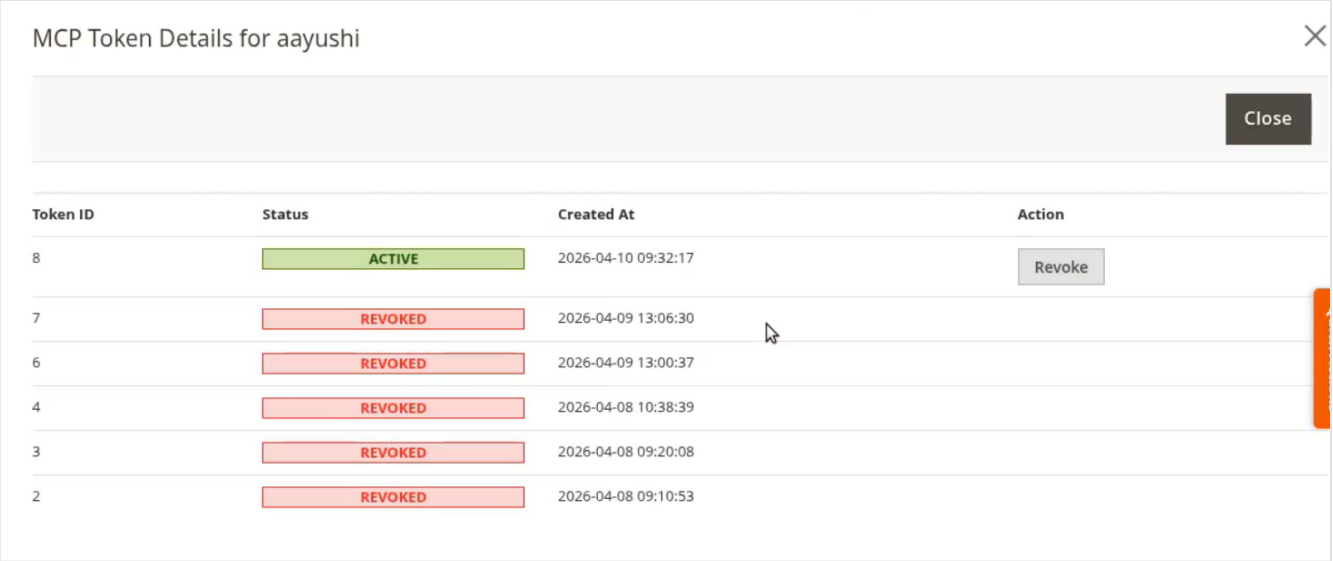


- The **MCP Users** grid is the central admin section for viewing and managing users who have access to the MCP Server. It gives administrators a quick overview of user access status, connected client types, and usage activity in one place. From this grid, admins can also take direct actions to review user connection details or open the user profile for further management.

Field	Description
ID	Displays the unique record identifier for each MCP user entry.
User	Shows the admin username associated with the MCP access record.
Access Status	Indicates whether MCP access is currently enabled or disabled for the user. This helps administrators quickly identify which users are allowed to connect.
Clients	Displays the connected client type associated with the user, such as a Personal Access Token or other authorized client connection.
Added to MCP	Shows the date and time when the user was first added to the MCP system.
Last Used	Displays the most recent date and time the user or connected client interacted with the MCP Server.
Action	Provides row-level management options for the selected user, such as viewing connection details or opening the related user record for further changes.
Actions	The top-left mass action control allows administrators to apply bulk operations to selected user records.
Records Found	Displays the total number of MCP user records currently available in the grid.
Per Page	Lets administrators control how many records are shown in the grid at one time.
Pagination	Allows navigation across multiple pages when the number of MCP users exceeds the selected per-page limit.

User Details

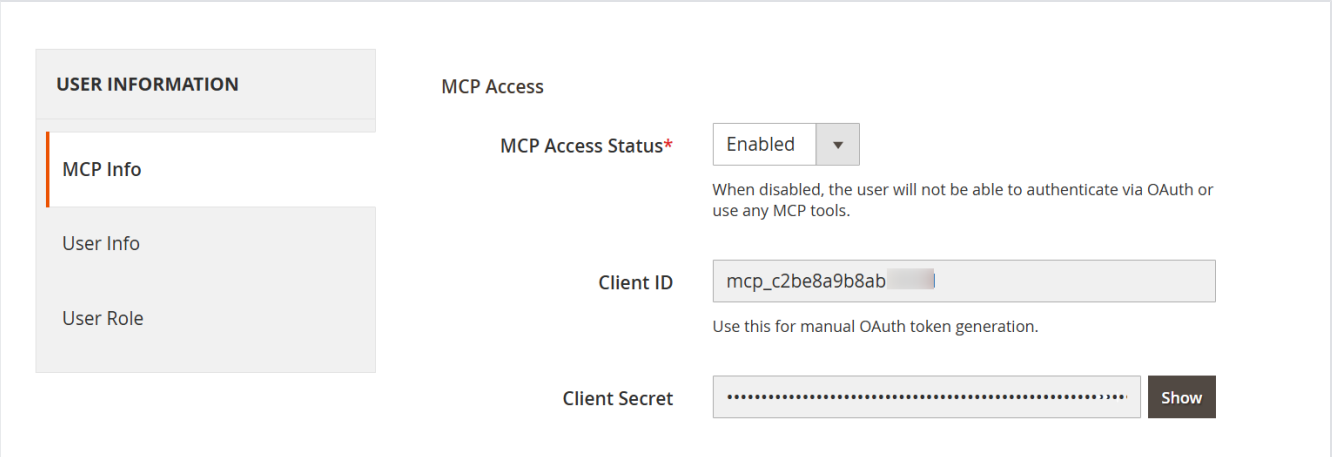
Copyright © 2021. MageDelight. All Rights Reserved.



- When the **Details** option is selected from the **Action** column in the **MCP Users** grid, a token details popup is opened for the selected user. This popup allows administrators to review all token records linked to that user, including their current status and creation date. It also provides a direct option to revoke an active token when required.

Field	Description
MCP Token Details	Displays a popup window containing the token history and status details for the selected MCP user.
Token ID	Shows the unique identifier assigned to each token record.
Status	Indicates the current state of the token, such as **Active** or **Revoked**.
Created At	Displays the date and time when the token was generated.
Action	Provides token-level management actions for the selected record.
Revoke	Allows administrators to manually revoke an active token to immediately disable its usage.
Close	Closes the popup window and returns to the MCP Users grid.

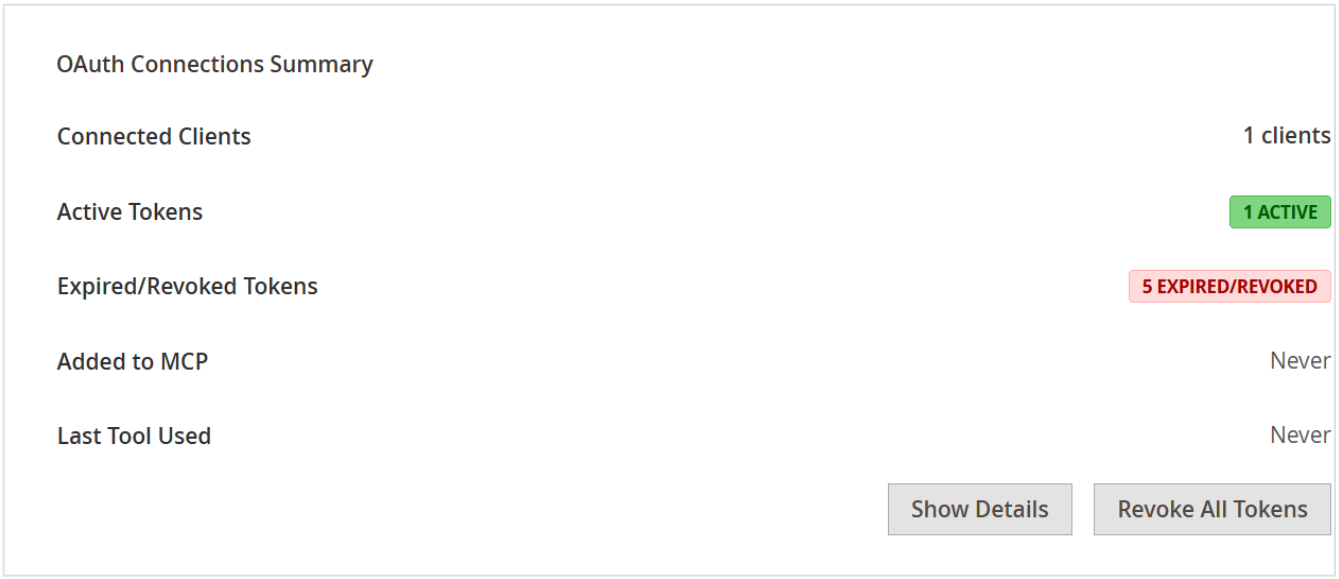
Edit User



- The **Edit User** screen opens when the administrator selects **Edit User** from the **Action** column in the **MCP Users** grid. This section is used to manage MCP access for a specific admin user and review authentication-related details linked to that user. It also allows the administrator to update the access status, view client credentials, and save changes directly from the user profile.

Copyright © 2021. MageDelight. All Rights Reserved.

Field	Description
MCP Access	Displays the MCP-related settings section for the selected admin user.
MCP Access Status	Allows the administrator to enable or disable MCP access for the user. When disabled, the user will not be able to authenticate through OAuth or use MCP tools.
Client ID	Shows the unique client identifier assigned to the selected user for MCP authentication. This value can be used for manual OAuth token generation.
Client Secret	Displays the secret key linked to the selected MCP client. It is masked by default for security purposes.
Show	Reveals the hidden client secret so the administrator can review it when needed.
Save User	Saves all changes made to the selected user profile.
Back	Returns to the previous screen without making further changes.
Delete User	Removes the selected admin user from the system.
Reset	Discards unsaved changes and restores the current form values.
Force Sign-In	Forces the selected user to sign in again for security or session control purposes.
MCP Info	Opens the MCP-specific configuration tab for the selected admin user.
User Info	Opens the general account information section for the selected user.
User Role	Opens the role assignment section where the administrator can manage permissions for the selected user.

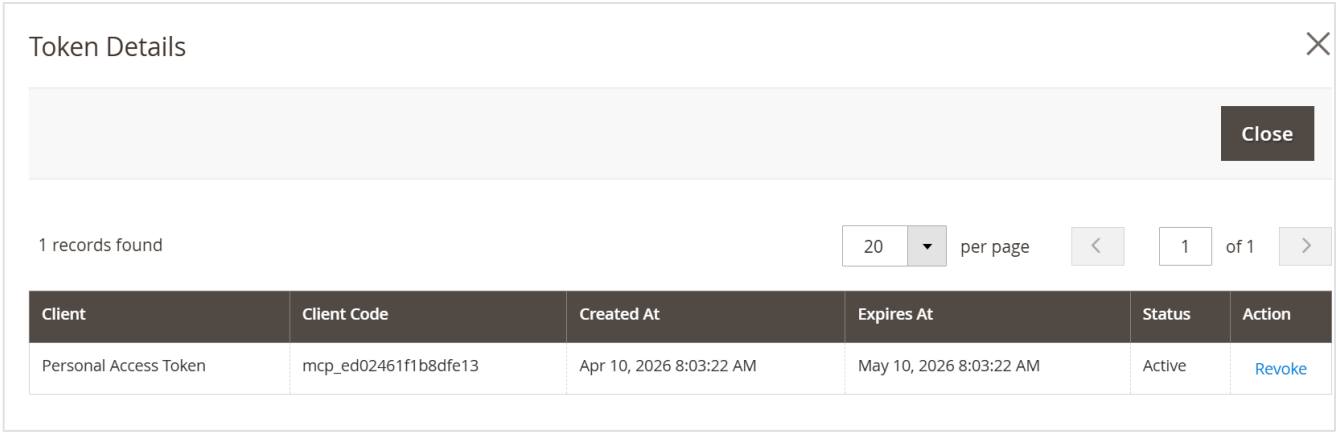


- The **OAuth Connections Summary** section under **MCP Info** gives administrators a quick overview of the selected user's MCP connection activity. It shows how many clients are connected, the current token status, when the user was added to MCP, and the latest usage activity. This section also provides direct actions to review token details or revoke all active tokens for that user.

Field	Description
Connected Clients	Displays the total number of AI clients currently connected for the selected user.
Active Tokens	Shows the number of currently valid and usable tokens linked to the user.
Expired/Revoked Tokens	Displays the total number of tokens that are no longer active due to expiration or manual revocation.
Added to MCP	Shows the date and time when the user was first added to the MCP system.

Copyright © 2021. MageDelight. All Rights Reserved.

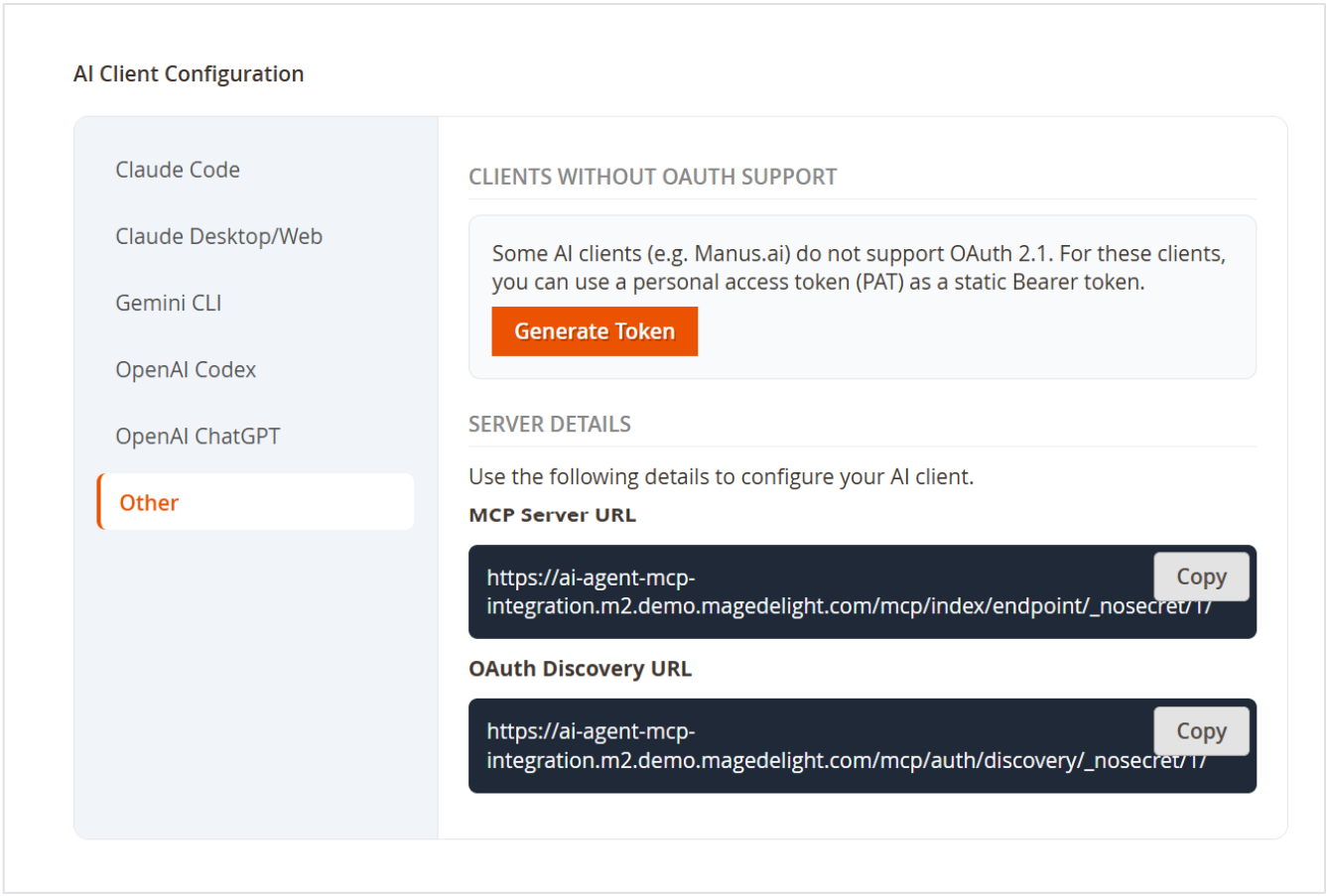
Last Tool Used	Displays the most recent MCP tool usage activity for the selected user. If no action has been performed yet, it shows **Never**.
Show Details	Opens the detailed token view for the selected user, where token-level records can be reviewed.
Revoke All Tokens	Revokes all active tokens associated with the selected user to immediately disable existing MCP connections.



- When the **Show Details** button is clicked in the **OAuth Connections Summary** section, a **Token Details** popup opens for the selected user. This popup provides a record-wise view of all connected MCP clients and their token information, helping administrators review token validity, expiry, and status from one place. It also allows direct revocation of an active token when required.

Field	Description
Client	Displays the type or name of the connected client associated with the token, such as a Personal Access Token.
Client Code	Shows the unique code assigned to the connected client for identification purposes.
Created At	Displays the date and time when the token was created.
Expires At	Shows the date and time when the token will expire and become unusable.
Status	Indicates the current condition of the token, such as **Active** or **Revoked**.
Action	Provides token-level actions for the selected client record.
Revoke	Allows administrators to immediately deactivate the selected active token.
Close	Closes the popup window and returns to the previous screen.
Records Found	Displays the total number of token records shown in the popup.
Per Page	Allows administrators to choose how many token records are displayed per page.
Pagination	Helps navigate between multiple pages if more token records are available.

Copyright © 2021. MageDelight. All Rights Reserved.

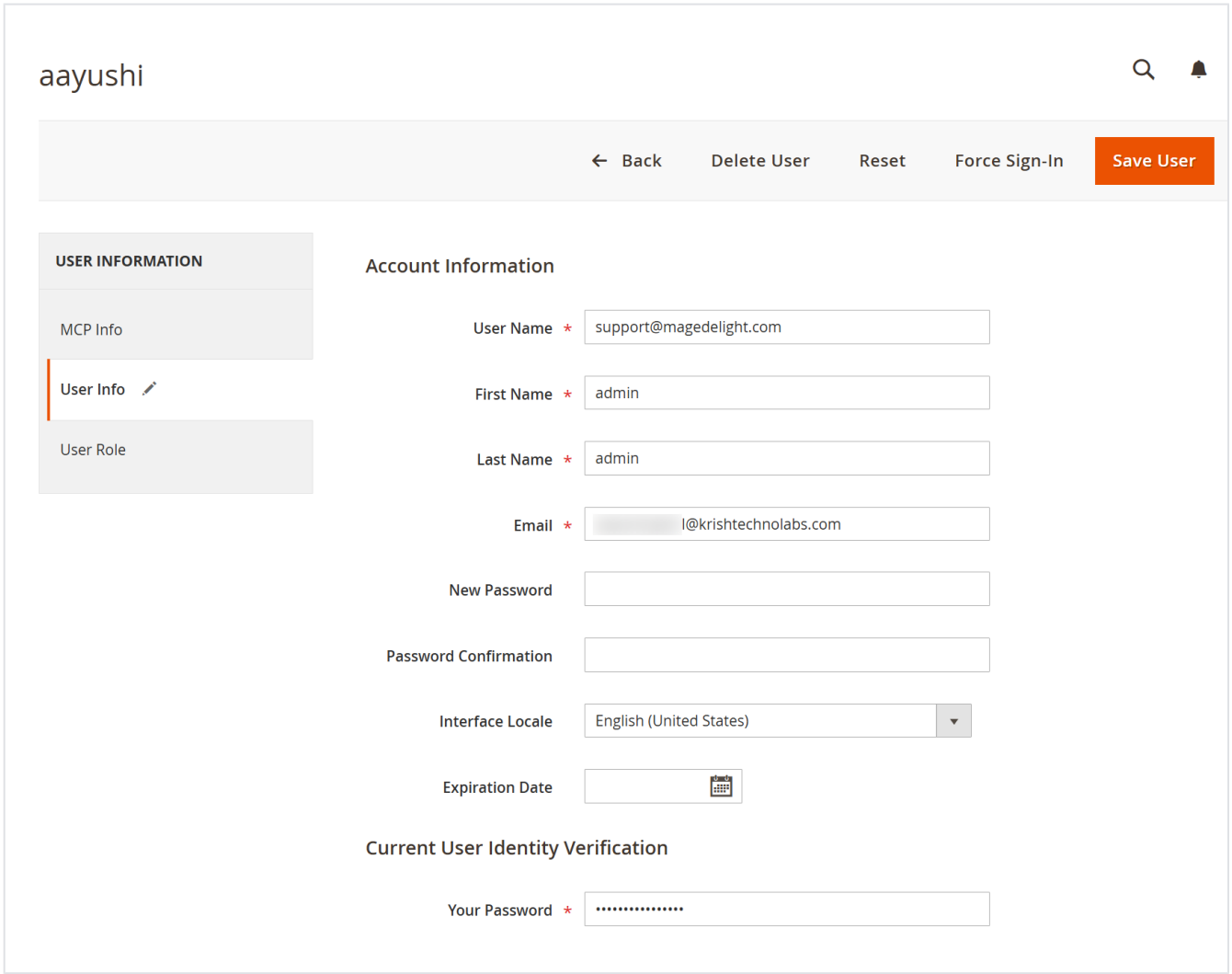


- The **AI Client Configuration** section under **MCP Info** provides ready-to-use connection instructions for supported AI clients in a tab-based layout. It helps administrators quickly connect an AI client by using prefilled server details, one-step setup commands, and manual configuration snippets. This makes the client onboarding process simpler and reduces the chance of configuration errors.

Field	Description
AI Client Configuration	Displays client-specific connection instructions for integrating supported AI tools with the MCP Server.
Claude Code	Shows setup instructions for connecting the store with Claude Code using command-line configuration.
Claude Desktop/Web	Provides guided connection details for Claude Desktop and Claude Web clients.
Gemini CLI	Displays setup instructions for connecting the store with the Gemini command-line client.
OpenAI Codex	Provides connection details for configuring the OpenAI Codex client with the MCP Server.
OpenAI ChatGPT	Shows setup instructions for connecting ChatGPT through the supported app-based MCP flow.
Other	Provides generic MCP connection details for other compatible AI clients. It can also be used for clients that require alternative connection handling.
Prerequisites	Lists any required tools, packages, or conditions that must be completed before configuring the selected AI client.

Copyright © 2021. MageDelight. All Rights Reserved.

MCP Server URL	Displays the prefilled MCP endpoint URL for the current store, which is used during client setup.
OAuth Authorization URL	Shows the authorization endpoint required for authenticated client connection.
Quick Setup Command	Provides a ready-to-copy command that allows the selected client to be configured in a single step.
Manual Setup Configuration	Displays the configuration snippet or structured setup block that can be added manually to the client configuration file.
Copy	Copies the related command, URL, or configuration block for faster setup.
Documentation Link	Opens the related client documentation for additional reference or advanced setup guidance.

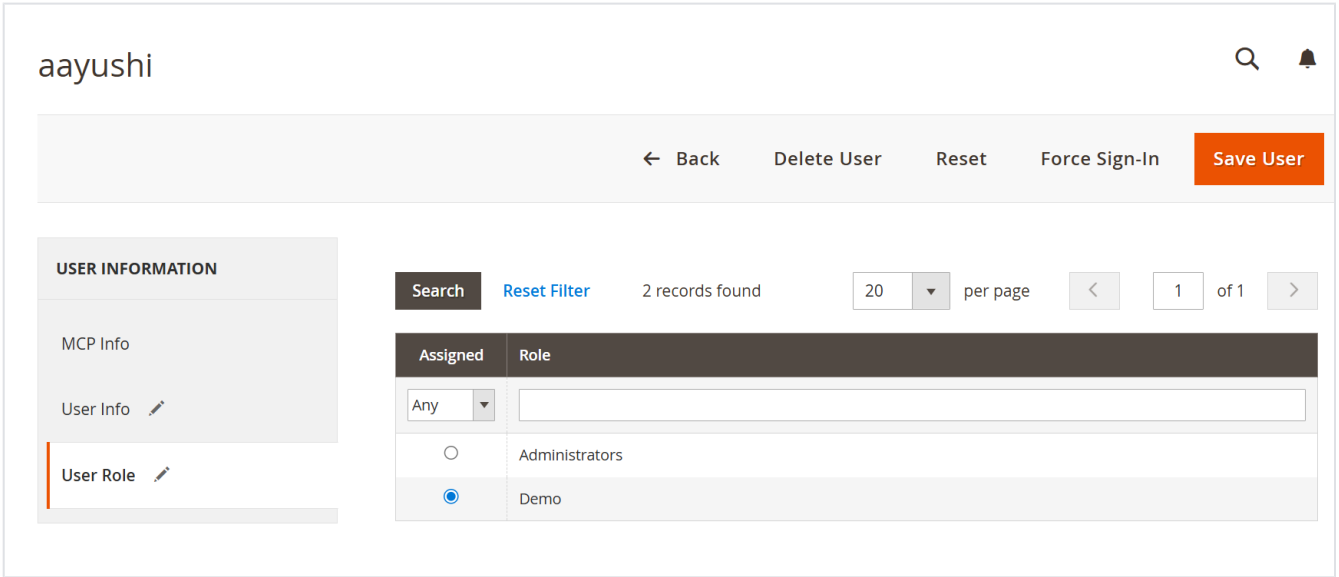


- The **User Info** tab is part of the admin user edit screen and is used to manage the selected user's general account details. Unlike the **MCP Info** tab, which focuses on MCP access and connection settings, this section is intended for standard user profile management such as login details, contact information, password updates, locale preference, and account validity.

Field	Description
User Name	Specifies the login username for the admin user account. This value is used when the user signs in to the admin panel.
First Name	Defines the first name of the admin user for identification within the system.

Copyright © 2021. MageDelight. All Rights Reserved.

Last Name	Defines the last name of the admin user for profile and record display purposes.
Email	Stores the email address associated with the admin user account. This is used for account-related communication and identification.
New Password	Allows the administrator to assign a new password for the selected user account.
Password Confirmation	Confirms the new password entry to avoid accidental password mismatches.
Interface Locale	Lets the administrator choose the language or locale used in the admin interface for the selected user.
Expiration Date	Sets the date until which the admin user account remains active. After this date, the account can be restricted based on system behavior.
Your Password	Requires the current administrator password to verify identity before saving sensitive account changes.
Save User	Saves all updates made in the User Info tab.
Back	Returns to the previous screen without continuing further actions.
Delete User	Removes the selected admin user account from the system.
Reset	Discards unsaved changes and restores the current form values.
Force Sign-In	Forces the selected user to sign in again, which is useful for session control or security purposes.
MCP Info	Opens the MCP-specific settings tab for the selected user.
User Info	Opens the general account information tab for the selected user.
User Role	Opens the role assignment tab where permissions and access levels can be managed for the selected user.



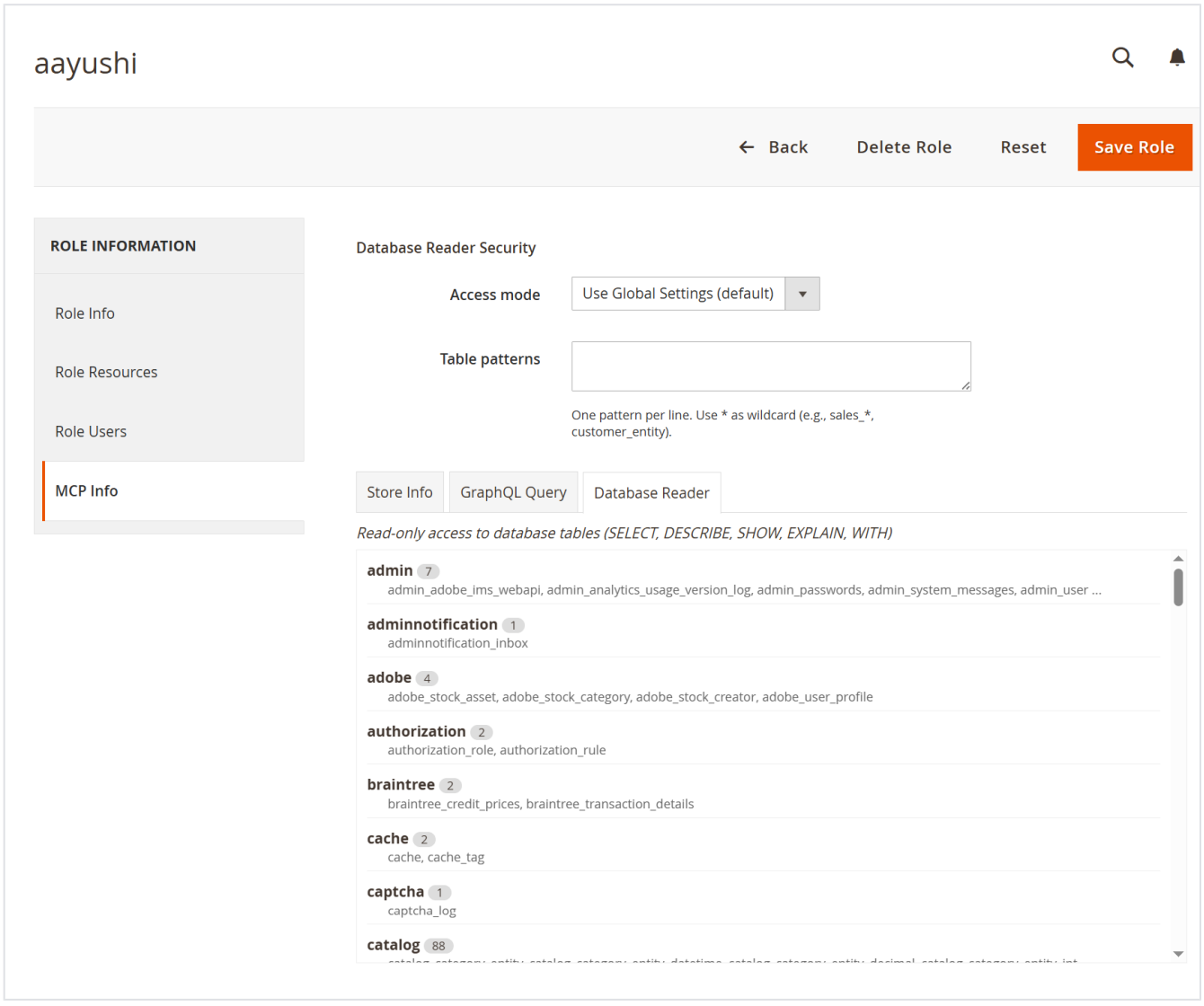
- The **User Role** tab in the **Edit User** section is used to assign or change the admin role for the selected user. It helps control what areas, tools, and permissions the user can access in the admin panel, including MCP-related capabilities based on the assigned role. This tab also includes basic grid controls to search and filter available roles before selecting one.

Field	Description
Assigned	Lets the administrator choose whether a role is assigned to the selected user. The radio option is used to select one role from the available list.
Role	Displays the list of available admin roles that can be assigned to the user.

Copyright © 2021. MageDelight. All Rights Reserved.

Search	Applies the selected filters and updates the role list accordingly.
Reset Filter	Clears the applied filters and restores the default role listing.
Records Found	Shows the total number of role records currently available in the grid.
Per Page	Lets the administrator define how many role records should be displayed per page.
Pagination	Enables navigation between pages when more role records are available than the selected page limit.
Save User	Saves the selected role assignment and any related changes made for the user.
Back	Returns to the previous screen.
Delete User	Deletes the selected admin user account.
Reset	Discards unsaved changes made on the current edit screen.
Force Sign-In	Forces the selected user to sign in again for security or session control purposes.
MCP Info	Opens the MCP-specific settings tab for the selected user.
User Info	Opens the general account information tab for the selected user.
User Role	Opens the role assignment tab where the user's admin role can be selected or updated.

Role-Based MCP Access Configuration



Copyright © 2021. MageDelight. All Rights Reserved.

- The **MCP Info** tab under **System Permissions User Roles** is used to manage MCP-related access rules at the role level. It lets administrators define how the **Database Reader** should behave for users assigned to that role and also provides a quick view of the MCP tools available to the role. This helps apply tighter access control without changing the global MCP configuration for all users.

Field	Description
MCP Info	Opens the role-level MCP configuration section for the selected admin role.
Database Reader Security	Displays role-specific security controls for database access through MCP.
Access Mode	Defines how database table restrictions are applied for the selected role. • **Use Global Settings** follows the system-wide configuration, • **Blacklist** blocks only the listed table patterns, • **Whitelist** allows access only to the listed table patterns.
Table Patterns	Lets administrators enter table name patterns to control database access for the role. Add one pattern per line and use * as a wildcard, such as `sales_*` or `customer_entity`.
Store Info	Shows the MCP tool access view for store configuration and store structure information available to this role.
GraphQL Query	Shows the MCP tool access view for GraphQL query capability available to this role.
Database Reader	Shows the MCP tool access view for database query access available to this role.
MCP Tools View	Displays the MCP tools assigned to the role, helping administrators quickly review what functionality is available under that role.
Save Role	Saves the MCP role settings and any other updates made to the selected role.
Back	Returns to the previous role management screen.
Delete Role	Removes the selected role from the system.
Reset	Discards unsaved changes and restores the current form values.
Role Info	Opens the general role information tab.
Role Resources	Opens the permissions tree where Magento and MCP resources can be assigned to the role.
Role Users	Opens the section showing users assigned to the selected role.

MCP Configuration in My Account

Copyright © 2021. MageDelight. All Rights Reserved.

MCP Access

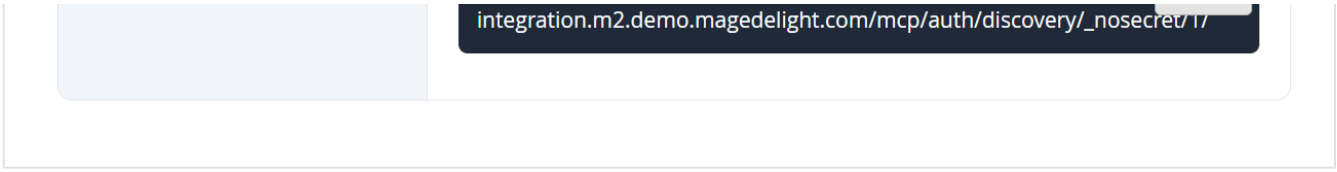
MCP Access Status* Enabled

When disabled, the user will not be able to authenticate via OAuth or use any MCP tools.

Client ID mcp_c2be8a9b8ab39871

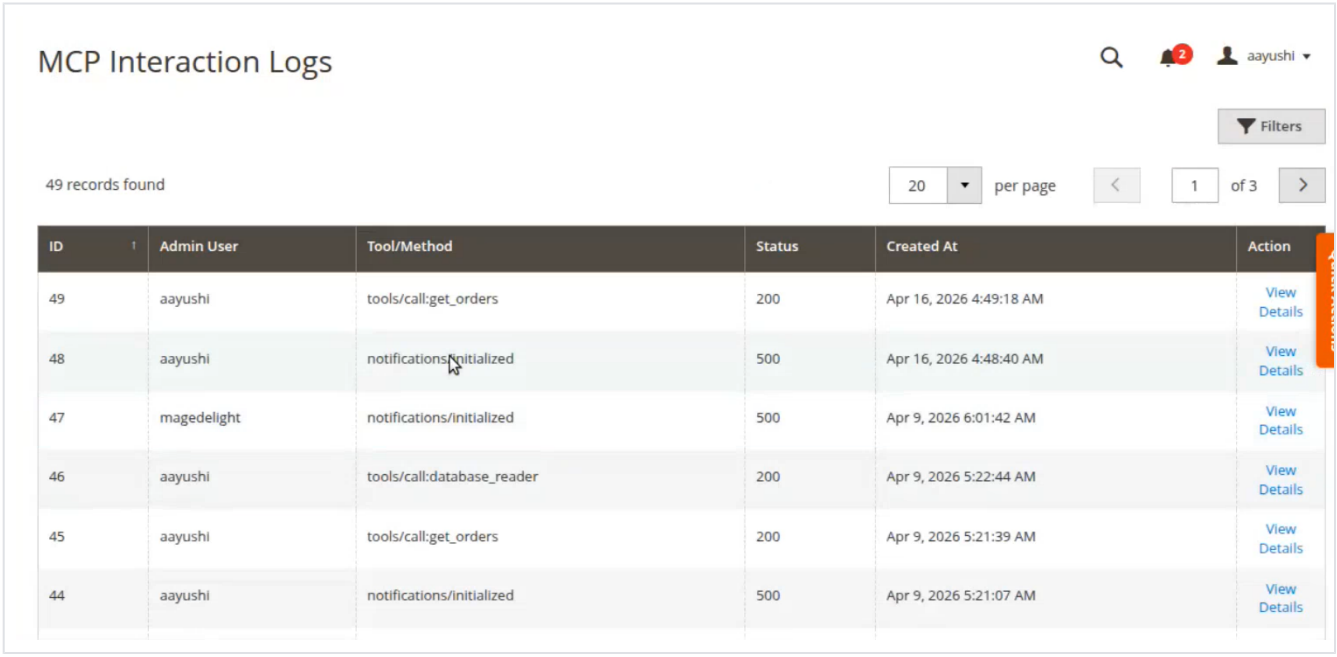
Use this for manual OAuth token generation.

Client Secret ••••••



- The **My Account** section also includes the same MCP-related settings and configuration options available for the logged-in admin user. From this screen, users can manage their **MCP access status**, review **OAuth connection details**, view token activity, and access **AI client configuration instructions** for supported clients such as Claude, Gemini, Codex, and ChatGPT. This provides a convenient self-service area where users can view and manage their own MCP setup without navigating to the broader user management section.
- **Path:** Admin Panel My Account

MCP Interaction Logs



- The **MCP Interaction Logs** section provides a centralized view of activity performed through the MCP integration. It helps administrators monitor which user triggered a request, which tool or method was used, the response status, and when the interaction occurred. This section is useful for audit tracking, debugging failed requests, and reviewing overall MCP usage history.

Field	Description
ID	Displays the unique identifier for each interaction log record.
Admin User	Shows the admin user who initiated the MCP request.
Tool/Method	Displays the MCP tool, endpoint, or method used during the interaction.
Status	Shows the response status code returned for the request, helping identify successful and failed interactions.
Created At	Displays the date and time when the interaction log was created.
Action	Provides the available action for the selected log record.
View Details	Opens the detailed view of the selected interaction log entry for further inspection.
Filters	Allows administrators to apply filter criteria to narrow down the displayed log records.
Records Found	Shows the total number of interaction log records available in the grid.
Per Page	Lets administrators choose how many log records are displayed on each page.
Pagination	Enables navigation through multiple pages of interaction logs.

Copyright © 2021. MageDelight. All Rights Reserved.

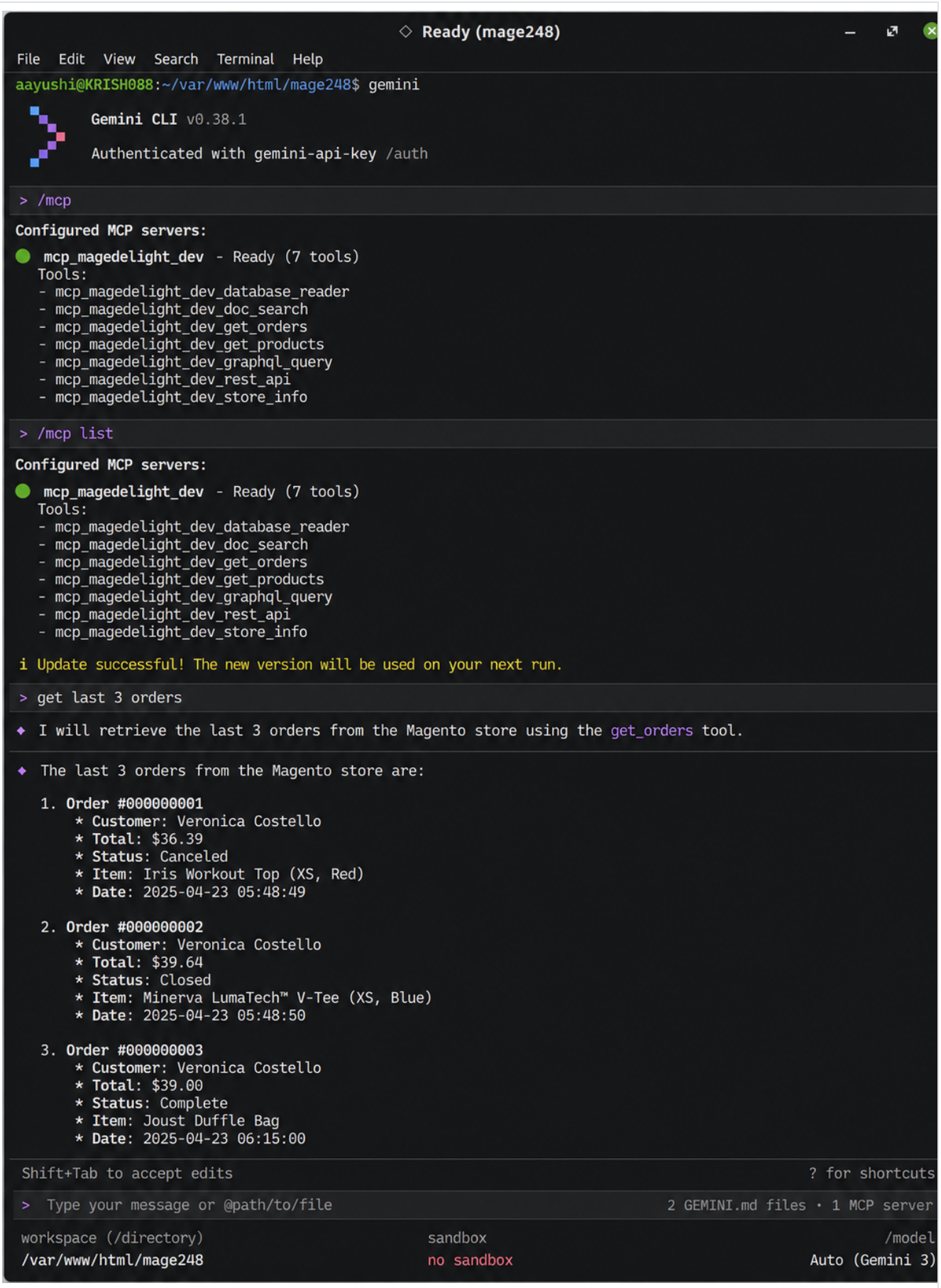
- When the **View Details** option is selected from the **Action** column in the **MCP Interaction Logs** grid, a detailed popup is opened for the selected log entry. This popup allows administrators to inspect both the request payload and the response returned for that interaction. It is especially useful for troubleshooting failed requests, reviewing API behavior, and validating MCP communication details.

Field	Description
MCP Interaction Log Details	Displays the detailed popup view for the selected interaction log record.
Request	Shows the request payload that was sent during the selected MCP interaction.
Response	Displays the response payload returned for the selected MCP interaction, including success or error details.
Close	Closes the popup window and returns to the interaction logs grid.

Frontend Functionality

Gemini CLI MCP Integration

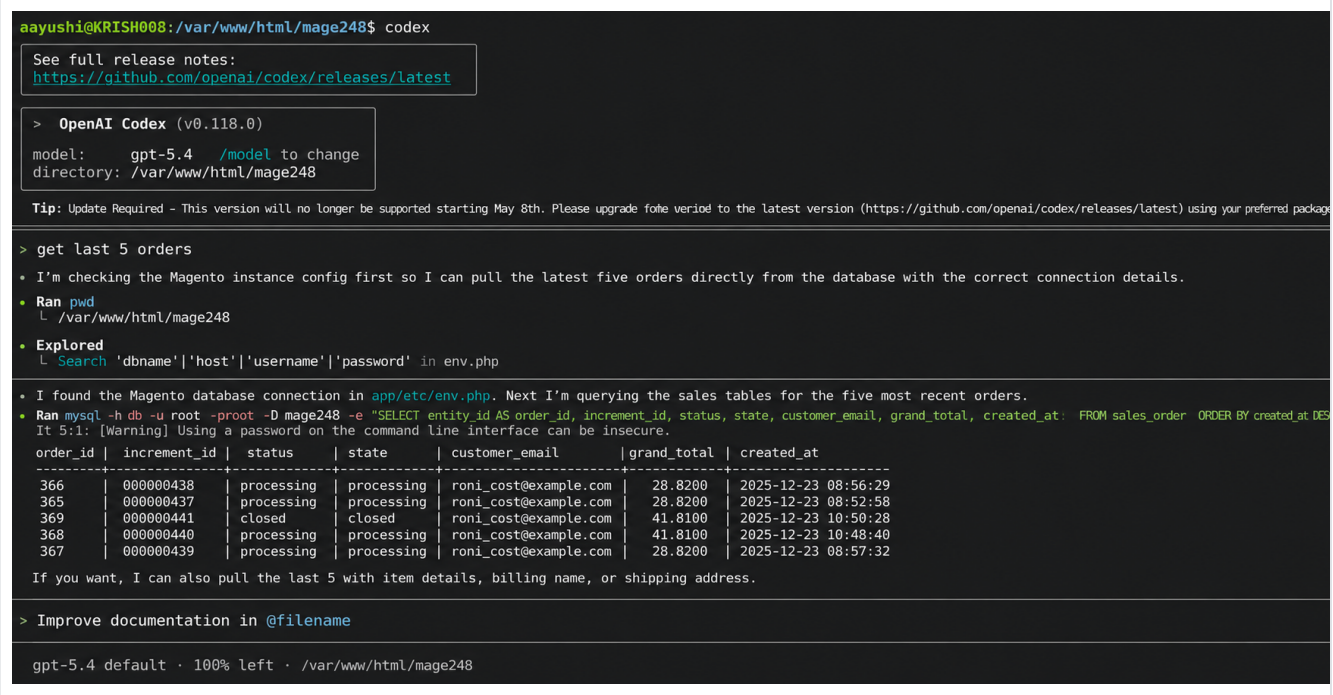
Copyright © 2021. MageDelight. All Rights Reserved.



Copyright © 2021. MageDelight. All Rights Reserved.

- The **Gemini CLI MCP integration** allows the Magento 2 store to connect with Google Gemini CLI through the configured MCP Server. Once the MCP Server is enabled and the required client setup is completed, Gemini CLI can access the available MCP tools and perform supported store operations directly from the command-line interface.
- In the displayed example, the Gemini CLI is successfully authenticated using the configured API key and connected to the Magento MCP Server. The MCP server is shown as **Ready**, confirming that the connection is active and the available tools can be used.
- The connected MCP server provides access to the following tools:
    - `database_reader` – Allows permitted database queries based on the configured access rules.
    - `doc_search` – Enables searching through available documentation or indexed content.
    - `get_orders` – Retrieves Magento order information.
    - `get_products` – Retrieves Magento product information.
    - `graphql_query` – Executes supported GraphQL queries.
    - `rest_api` – Allows supported Magento REST API interactions.
    - `store_info` – Retrieves store-related information.
- In this example, the user enters the command: get last 3 orders
- Gemini CLI uses the `get_orders` MCP tool to retrieve the latest three Magento orders from the store. The response displays key order details such as order number, customer name, order total, order status, purchased item, and order date.
- This functionality helps administrators and developers quickly fetch Magento store data through an AI-assisted command-line workflow without manually navigating the admin panel or writing direct queries. It is useful for checking recent orders, validating MCP tool connectivity, testing AI client integration, and confirming that the configured MCP permissions are working correctly.
- Before using this functionality, ensure that the MCP Server is enabled, the AI client is configured correctly, and the user has the required MCP access permissions. The extension documentation also includes MCP server configuration, MCP user access, role-based MCP permissions, AI client configuration, and interaction log management for monitoring requests.

OpenAI Codex MCP Integration



- The **OpenAI Codex MCP integration** allows administrators and developers to connect the Magento 2 store with OpenAI Codex through the configured MCP Server. Once the client is connected, users can enter natural language commands in the terminal to retrieve Magento store information using the available MCP tools.
- As shown in the example, the user enters the command: get last 5 orders
- Codex checks the Magento instance configuration, identifies the required database connection details, and retrieves the latest five orders from the Magento `sales_order` table. The response displays important order details such as order ID, increment ID, order status, customer email, grand total, and order creation date.
- This functionality helps users quickly access Magento store data directly from the command line without manually navigating the admin panel or writing database queries. It is useful for reviewing recent orders, validating MCP connectivity, testing database access, and confirming that the configured MCP permissions are working correctly.

Demo

Click here to visit backend admin panel.

FAQs

Click here to visit FAQs.

Support

Copyright © 2021. MageDelight. All Rights Reserved.

Click here to raise a support ticket using your MageDelight account.

Additional Services

Click here to get the customized solution for this extension.

Thank you for choosing MageDelight!

Copyright © 2021. MageDelight. All Rights Reserved.