Model Context Protocol (MCP) Integration & Operations Guide

This guide outlines the configuration, architecture, security controls, and operational responsibilities required to set up and integrate with the Oak MCP service.

Setup & Configuration Guidelines

Prerequisites

- Separate client registrations for each client application/platform (e.g., Copilot Studio, Claude, n8n).
- Oak Tenant ID and appropriate administrative privileges.
- Access to your Identity Provider (e.g., Microsoft Entra ID) to configure SAML app definitions.
- To use the MCP Aria Search tool, Aria Search must be enabled and areas approved for indexing on the Oak site.

Client Configuration Requirements (Entra ID SAML Setup)

To allow users to authenticate via SAML single sign-on (SSO), your SAML application definition in Entra ID must include Oak's metadata endpoints alongside existing production URLs.

Required Entra ID SAML Settings:

- **Identifier (Entity ID):** https://sts-uk1.oak.com/sso/saml/metadata
- **Reply URL (Assertion Consumer Service URL):** https://sts-uk1.oak.com/sso/saml/acs

Critical Note: Append these URLs to the existing SAML app definition. **Do not overwrite or remove** existing production URLs, or standard Oak web logins will fail.

Copilot Studio Integration Configuration

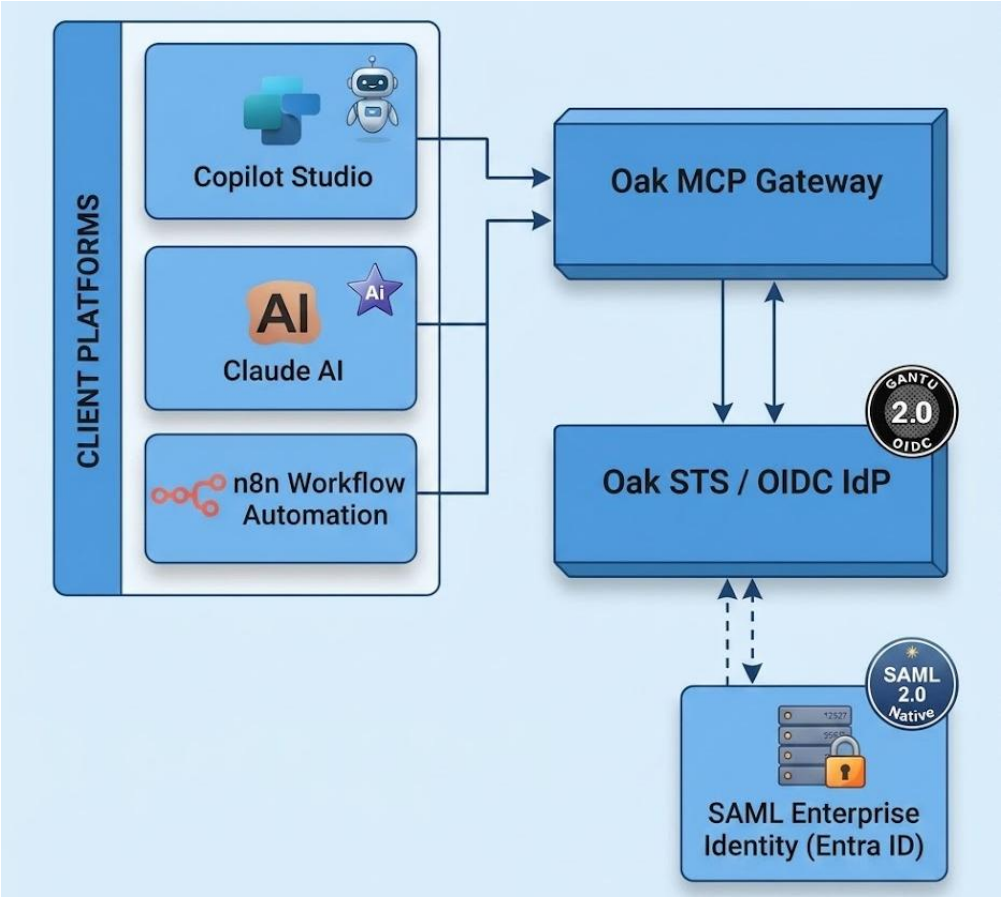
Parameter	Value	Notes
Host	https://mcp-uk1.oak.com	MCP service domain
Base URL	/	Base route
Identity Provider	Generic OAuth 2	Custom OIDC integration

© Oak Engage | Employee Engagement Solutions 2026 All rights reserved.

Client ID	<client-id> (shared separately)	Tenant-specific platform key
Client Secret	<client-secret> (shared separately)	Keep secure; store in safe vault
Authorization URL	https://sts-uk1.oak.com/oidc/authorize	Authorisation Code + PKCE endpoint
Token URL	https://sts-uk1.oak.com/oidc/token	Exchange code for tokens
Refresh URL	https://sts-uk1.oak.com/oidc/token	Obtain new access tokens
Scope	.default	Standard client requested scope

High-Level Architecture

The MCP system acts as a secure middleware layer between Client Platforms (Copilot, Claude, n8n) and underlying Oak resources, delegating user identity verification to the Oak Security Token Service (STS) and upstream Enterprise IdPs like Entra ID.



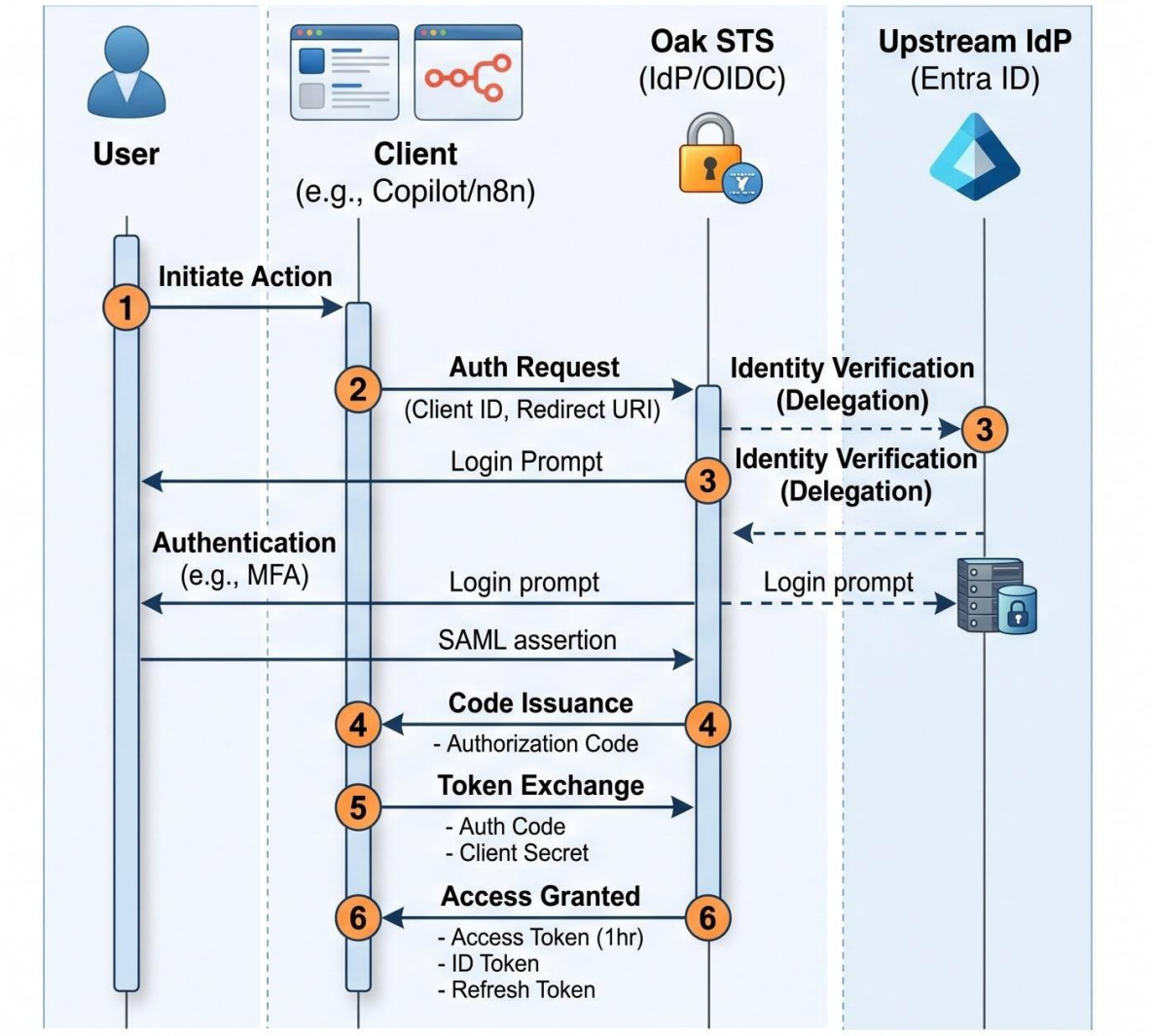
© Oak Engage | Employee Engagement Solutions 2026 All rights reserved.

Authentication & Authorisation Process

Authentication follows the **OAuth 2.0 / OIDC Authorisation Code Flow** (with optional PKCE support).

Key Architectural Rules

- **Client Credentials:** Grant software permission to act as an OAuth client for a tenant. They **do not** grant resource permissions or contain user identities.
- **User Credentials:** User passwords and tokens are processed strictly within Oak STS / Entra ID and are **never exposed to the client application**.
- Token Lifespan: Access tokens expire after 1 hour. Clients must use the **Refresh Token** endpoint to fetch active tokens without requiring user re-authentication.



1. **Initiation:** The user requests an action in the Client Application.
2. **Authorisation Request:** Client redirects the user to https://sts-uk1.oak.com/oidc/authorize with its registered **Client ID**.

© Oak Engage | Employee Engagement Solutions 2026 All rights reserved.

3. **Identity Verification:** Oak STS delegates authentication to your Entra ID via SAML 2.0 (or native Oak authentication).
4. **Code Issuance:** Upon successful login, Oak STS redirects back to the client with a temporary Authorisation Code.
5. **Token Exchange:** The client sends the Authorisation Code alongside its confidential ***Client Secret*** directly to https://sts-uk1.oak.com/oidc/token.
6. **Access Granted:** Oak STS validates credentials and returns an Access Token (1-hour lifespan), ID Token, and Refresh Token.

Security Guardrails

- **Secret Isolation:** Client secrets must **never** be checked into version control or embedded in client-side code exposed to end-users. Store secrets exclusively in server-side configuration systems or secret managers.
- **Credential Loss & Rotation:**
    - Oak does not store readable client secrets. If a client secret is lost, a replacement must be requested/generated via Oak operations.
    - In the event of a secret leak or compromise, notify Oak immediately. Oak will rotate the credentials; the **Client ID** will remain unchanged.
- **Platform Isolation:** Client registrations are tenant-specific and non-transferable across platforms. Copilot, Claude, and n8n must run on distinct client IDs.
- **Scope Minimisation:** Client credentials only permit authorisation delegation; they convey no elevated API privileges or access on their own.

Support RACI Matrix

Task / Responsibility	**Client**	**Oak**
SAML Entity ID & ACS URL Configuration in EntraID	R / A	C
Creation of Application Client Registrations	C	R / A
Client Secret Vaulting & Management	R / A	I
Secret Re-issuance on Loss or Compromise	C	R / A
MCP Gateway Service Availability & Uptime	I	R / A
End-User Access Control & Enterprise IdP Lifecycle	R / A	I
Client Platform Setup (Copilot Studio, Claude, etc.)	R / A	C

R: Responsible, A: Accountable, C: Consulted, I: Informed

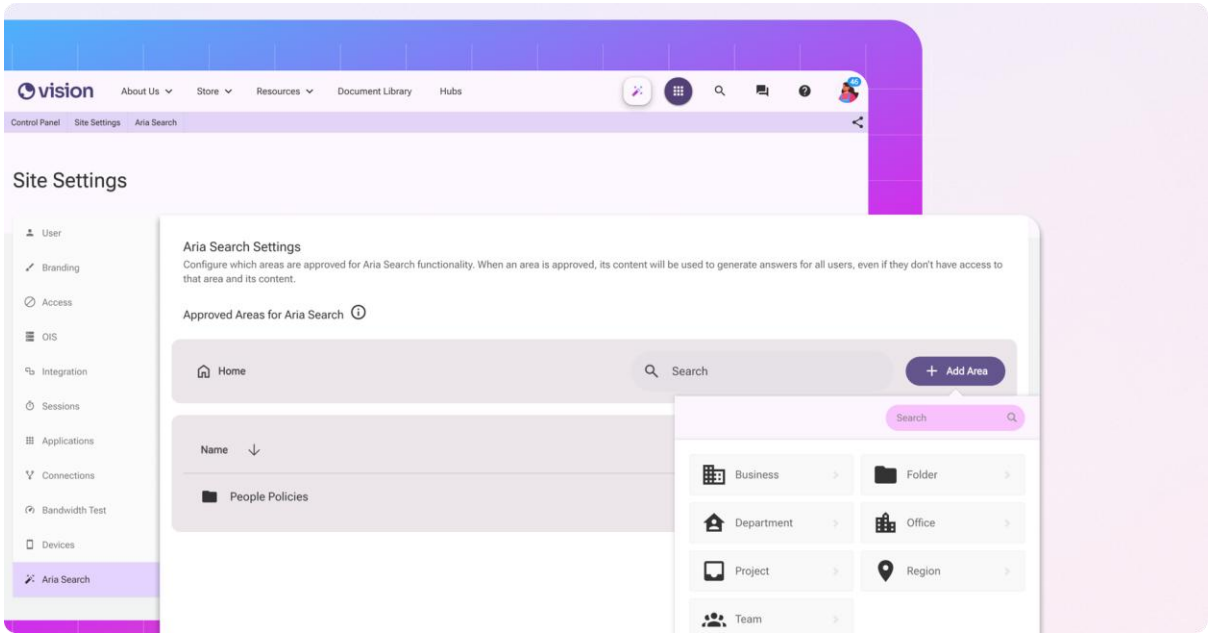
© Oak Engage | Employee Engagement Solutions 2026 All rights reserved.

Aria Search Tool

The Aria Search MCP tool requires the application to be enabled and configured within your Oak site. Aria Search can be enabled from the Site Settings page allowing administrators to access the Aria Search Settings page.
Please note that access to the Aria Search features is limited to users within the Aria Search role found in your top-level business permissions page. This means Aria Search can be enabled for use with the MCP server without any users being able to access the feature directly within Oak.

How to Add Content to Aria Search

Aria Search only uses content you explicitly approve. This gives admins full control over what information is used to generate answers. To get started, head to Site Settings and open the new Aria Search section.



From here, you can choose which areas are approved for Aria Search.

Supported content types

Aria Search currently uses the following content types when generating answers:

- Blank pages
- News articles
- Word documents
- PDFs
- Policies
- Blog posts
- Other content types will come in future updates.

© Oak Engage | Employee Engagement Solutions 2026 All rights reserved.

Managing approved areas

You can remove an area from Aria Search at any time. Removing an area does not delete it or affect the content itself. It simply means that the content in that area will no longer be used by Aria Search when answering questions. This makes it easy to adjust what Aria Search can reference as your content evolves, or if certain information should no longer be surfaced through AI.

AI, Security, and Trust

We know that introducing AI into your intranet raises important questions around security, privacy, and accuracy. Here are some of the most common ones we hear.

Is our data secure?

Yes. Aria Search is powered by Microsoft Azure OpenAI and runs in a secure, enterprise grade environment, within the same geographical region as your Oak data.
Your data is not used to train public AI models, and it is not shared outside of your organisation. Content is processed only to generate responses for your users, and remains within Oak's trusted infrastructure and Microsoft's controlled AI services.

Is our content used to train the AI?

No. Your internal content is not used to train or improve any underlying AI models.
Each query is handled in isolation and responses are generated only from the content you have explicitly approved for Aria Search.

Can Aria Search make things up?

Aria Search is designed to reduce hallucinations by grounding responses entirely in your approved internal content only.
If an answer cannot be confidently generated from that content, Aria will not invent information or pull from external sources. This helps ensure employees receive accurate, trustworthy answers they can rely on.

Who can control what Aria Search uses?

Admins stay in full control.
You decide which areas are approved for Aria Search, and you can remove areas at any time. Removing an area simply stops that content from being used by AI. It does not delete anything or change how the content is managed elsewhere in Oak.

© Oak Engage | Employee Engagement Solutions 2026 All rights reserved.

Is this compliant with enterprise and regulated environments?

Aria Search is built with enterprise use in mind. Using Microsoft Azure OpenAI provides strong foundations for security, data handling, and responsible AI practices, making it suitable for information heavy and regulated organisations.

© Oak Engage | Employee Engagement Solutions 2026 All rights reserved.