Outward Intelligence

SECURITY OVERVIEW

MCP connector: authentication and access control

The connector runs on the same single sign-on already in production for the Outward Intelligence platform. Same identity provider, same accounts, no new credentials. This sheet sets out how a user is authenticated and how their access is enforced on every request.

IDENTITY

Your identity provider, not ours
Users authenticate against your corporate IdP over single sign-on (SAML or OIDC). Outward Intelligence never sees, stores or transmits a user's password, and enforces no password policy of its own.

No API keys
Access is delegated by the signed-in user through OAuth 2.1. There is no long-lived shared secret to distribute, rotate, or leak, and nothing for an administrator to hand out.

One user lifecycle
Accounts are the same ones used for the platform. Disabling a user at your IdP ends their access: they can no longer authenticate, and issued tokens are short-lived.

HOW A CONNECTION IS AUTHORISED

1. **Discovery**
   The AI tool reads the connector's published metadata (RFC 9728) to learn which authorization server to use. No credentials are ever entered into the tool itself.

2. **Sign-in**
   The user is redirected to an Outward Intelligence sign-in page, which brokers straight through to your IdP over single sign-on. Authentication happens on your side, under your existing controls.

3. **Explicit consent**
   The user approves the connection before any data can flow. The authorization code is exchanged using PKCE, so an intercepted code cannot be redeemed by anyone else.

4. **Scoped token**
   The tool receives a short-lived access token that is valid only for this connector. The user can withdraw it at any time from within their AI tool.

IDENTITY SOURCE	AUTHORIZATION SERVER	
Your corporate IdP, via SSO	**PropelAuth**	The MCP connector is purely an OAuth 2.1 resource server. Outward Intelligence never authenticates your users or holds their credentials.

ENFORCED ON EVERY REQUEST

The token is re-validated

Every call re-validates the bearer token against the authorization server (RFC 7662). Tokens are opaque: they carry no permissions of their own, so a client cannot forge, inspect or widen one.

The token is bound to this service

Audience binding (RFC 8707) ties a token to this connector alone. A token issued for anything else is rejected here, and a token issued here is useless anywhere else.

Permissions come from our records

What a user may see is resolved per call from the same access-control tables as the web platform, never from a claim inside the token. The connector cannot exceed a user's existing platform access.

DATA HANDLING AND COMPLIANCE

- **SOC 2 Type 2.** Outward Intelligence is SOC 2 Type 2 compliant. The report is available under NDA.
- **Encrypted in transit.** All traffic to the connector is served over TLS.
- **Read-only by design.** The connector exposes survey analysis only. It has no capability to write, modify or delete data.
- **Nothing retained.** The connector is stateless. Results are computed on demand, returned in the response, and no conversation content is stored.
- **Access is granted, not assumed.** Study-level access is assigned per user by an administrator. A new user who authenticates successfully but holds no grants can see nothing.

Security questions, documentation, or compliance requests: **support@outwardintelligence.com**