AI Engine

Business Guide: Data Access, Security & Agent Capabilities

For Administrators & Business Decision Makers | v1.33

---

1. What Can the AI Agent Do?

The AI Agent is a read-only assistant. It helps users understand their Salesforce data by answering questions in natural language. Here is a precise breakdown of what the agent can and cannot do:

Action	Can Agent Do It?	Details
Read records (SELECT)	✅ Yes	Agent reads records based on user's question
Create records (INSERT)	🚫 Never	Agent cannot create any records
Edit records (UPDATE)	🚫 Never — except one case	See scoring note below
Delete records (DELETE)	🚫 Never	Fully blocked in code
Send emails	✅ Yes — user-initiated only	User clicks Send, agent drafts the email
Create Tasks	✅ Yes — user-initiated only	User clicks 'Create Task' button
Update AI Score fields	✅ Yes — automated	AI_Score__c, AI_Score_Label__c on Lead/Opportunity only
Access other objects	✅ Only admin-configured	Admin controls which objects agent can query

⚠️ The only automatic data write: AI Scoring

When AI Scoring is enabled, the agent automatically updates three fields on Lead and Opportunity records:

AI_Score__c (number), AI_Score_Label__c (Hot/Warm/Cold), AI_Score_Reason__c (text explanation).

These are package-owned fields added by AI Engine. No standard or custom business fields are ever modified automatically.

---

2. Which Records Does the Agent Show?

The agent respects Salesforce's standard security model. Users see exactly the same records through the agent as they would see directly in Salesforce. The agent does not grant access to any additional data.

Salesforce Sharing Rules — Fully Respected

- If a user can only see their own Leads in Salesforce — they will only see their own Leads when asking the agent
- If sharing rules restrict visibility to a team or territory — the agent respects those same restrictions
- If a user cannot see a field due to Field Level Security — that field will never appear in agent results
- Organization-wide defaults, sharing rules, manual shares, and role hierarchy all apply

How It Works Technically

The agent generates a SOQL query and executes it as the current user. After execution, AI Engine applies Security.stripInaccessible() — a Salesforce security API that automatically removes any fields the user cannot access, even if the AI accidentally included them in the query. This provides a double layer of protection.

✅ Summary: The agent cannot show a user any data they couldn't already see in Salesforce.
There is no elevated access. There is no admin bypass for regular users.
A sales rep sees their own pipeline. A manager sees what their sharing rules allow.

---

3. Which Fields Does the Agent Access?

Fields the Agent Can Read

The agent only queries fields that are explicitly configured by the Salesforce administrator in the AI Agent Config object. The admin sets up which objects and which fields are available for each object.

Object	Fields Available	Who Configures It
Lead	Admin-selected fields (e.g. Name, Status, Rating, Company)	Salesforce Admin
Opportunity	Admin-selected fields (e.g. Name, Stage, Amount, Close Date)	Salesforce Admin
Account	Admin-selected fields	Salesforce Admin
Contact	Admin-selected fields	Salesforce Admin
Custom Objects	Admin-selected fields	Salesforce Admin
Task / Event	Available for context queries	Built-in
User	Name, Email (for owner lookups only)	Built-in

PII (Personal Identifiable Information)

The administrator controls whether PII fields (Email, Phone, MobilePhone) are included when data is sent to the AI provider for analysis. This is controlled by the AI Allow PII setting in the AI Engine Profile.

Setting	Behavior
AI Allow PII = OFF (default)	Email, Phone, MobilePhone are never sent to AI provider
AI Allow PII = ON	Admin explicitly enables PII fields for AI analysis

---

4. What Data Leaves Salesforce?

When a user asks a question, the following data is sent to the configured AI provider (OpenAI, Anthropic Claude, or Azure OpenAI):

Data Sent to AI Provider

- The user's question (natural language text)
- Record context — field values from the current record (admin-configured fields only)
- Query results — data returned by the SOQL query (fields visible to the user, FLS-filtered)
- Conversation history — previous messages in the current chat session
- Organization playbook — admin-configured system prompt (company description, guidelines)

Data NOT Sent to AI Provider

- Salesforce credentials or session tokens
- API keys (stored securely in Named Credentials, never passed through code)
- PII fields — unless AI Allow PII is explicitly enabled by admin
- Other users' data (sharing rules prevent this at query level)
- Any data outside the admin-configured field list

All AI provider connections use Salesforce Named Credentials.

API keys are stored encrypted by Salesforce — they never appear in code or logs.

Connections use HTTPS/TLS encryption in transit.

AI Engine does not store prompts or AI responses — only metadata (token count, duration, success/fail).

---

5. Who Can Use the Agent?

Access is controlled by two Salesforce Permission Sets included with AI Engine:

Permission Set	Custom Permission	What They Can Do
AI_Engine_User	AI_Engine_User	Use the chat agent, view AI scores, analyze records
AI_Engine_Admin	AI_Engine_Admin + AI_Engine_User	Everything above + configure AI settings, manage templates, view usage logs

Users without these Permission Sets cannot invoke any AI Engine functionality, even if they can see the Lightning component on a page. All Apex methods check the Custom Permission before executing.

---

6. Explicit Limitations — What the Agent Will Never Do

🚫 The agent CANNOT:

- Create, edit, or delete business records (Leads, Opportunities, Accounts, Contacts, Cases, etc.)
- Access objects not configured by the administrator
- Access fields the user cannot see in Salesforce (FLS enforced)
- Access records the user cannot see in Salesforce (sharing rules enforced)
- Execute any SOQL with subqueries, semicolons, or DML keywords (blocked by code)
- Store or cache customer data outside of Salesforce
- Access Salesforce configuration, metadata, or system settings
- Send emails without explicit user action (clicking Send button)
- Create tasks without explicit user action (clicking Create Task button)
- Operate outside the current user's permission context

---

7. What Is Logged?

AI Engine logs activity metadata to the AI Activity Log object (AI_Activity_Log__c) for usage monitoring and billing purposes. Here is exactly what is and is not logged:

Data	Logged?	Where
Action type (Chat, Summary, Scoring)	✅ Yes	AI_Activity_Log__c
Model used (e.g. gpt-4.1)	✅ Yes	AI_Activity_Log__c
Token count (input/output)	✅ Yes	AI_Activity_Log__c
Duration (milliseconds)	✅ Yes	AI_Activity_Log__c

Data	Logged?	Where
Success / failure status	✅ Yes	AI_Activity_Log__c
Record type and ID (context)	✅ Yes	AI_Activity_Log__c
User who made the request	✅ Yes	AI_Activity_Log__c
The user's question/prompt	🚫 Never	Not stored anywhere
The AI's response	🚫 Never	Not stored anywhere
Record field values	🚫 Never	Not stored anywhere
PII data	🚫 Never	Not stored anywhere

Summary for Business Stakeholders

✅ READ ONLY — The agent reads Salesforce data. It does not modify business records.

✅ RESPECTS ALL SECURITY — Sharing rules, FLS, profiles, and permission sets all apply. Users see exactly what they would see in Salesforce directly.

✅ ADMIN-CONTROLLED — Administrators decide which objects and fields the agent can access. Nothing is accessible by default — everything must be explicitly configured.

✅ PERMISSION-GATED — Only users with the AI_Engine_User Permission Set can use the agent.

✅ SECURE INTEGRATIONS — AI provider connections use encrypted Named Credentials. No API keys in code. No sensitive data in logs.

✅ ONE AUTOMATIC WRITE — AI Scoring updates three package-owned score fields on Lead and Opportunity. No standard or custom business fields are ever auto-modified.