M365 Agentic API Developer Guide (v2.0)

1. Overview

The M365 Agentic API allows developers to build "autonomous agents" that can perform actions within the Microsoft 365 ecosystem (Teams, Outlook, SharePoint). Unlike standard chatbots that simply answer questions, these Agents use a **"Reasoning Engine"** to create plans and execute multi-step workflows on behalf of the user.

2. Architecture Components

• **The Copilot Orchestrator:** This is the central brain. It receives the user's prompt and determines if it needs to fetch data or perform an action.

• **The Semantic Index:** A vector database that connects all user data (Emails, Chats, Files). The Agent queries this index to understand the 'context' before acting.

• **Microsoft Graph API:** The bridge used to perform actual operations (e.g., POST /sendMail, GET /events).

3. The 'Planner' Workflow

When an API request is received, the system follows a 4-step loop known as **'Grounding'**:

1. **Receive:** The User says 'Schedule a meeting with the design team based on the email from Sarah.'

2. **Retrieve:** The Agent searches the Semantic Index for 'Email from Sarah' and 'Design Team availability.'

3. **Plan:** The LLM generates a JSON plan: *{ 'action': 'calendar.create', 'attendees': ['sarah@m365.com'] }*.

4. **Execute:** The Agent calls the Graph API endpoint to book the slot.

4. API Endpoints

Endpoint	Method	Description
/v1/agent/invoke	POST	Triggers the agent with a prompt.
/v1/memory/context	GET	Retrieves the last 5 conversation turns.
/v1/actions/approve	PUT	User confirmation for high-risk actions.

5. Rate Limits & Quotas

• **Standard Tier:** 50 requests per minute (RPM).

• **Enterprise Tier:** 200 requests per minute (RPM).

• **Context Window:** The Agent can process up to **32,000 tokens** of context per interaction.

6. Security & Compliance

• **Just-In-Time (JIT) Access:** The Agent only has permission to access files relevant to the specific query.

• **Data Residency:** All data processing occurs within the user's home region (e.g., US-East or EU-West).

• **Audit Logs:** Every action taken by the Agent is logged in the Microsoft Purview compliance portal.