ORACLE

Delegated Authority for Agents in Oracle AI Agent Studio

The Know-Your-Agent Framework

October 2026, Version 1.0
Copyright © 2026, Oracle and/or its affiliates
Public

Executive summary

Know Your Agent (KYA) establishes the identity, ownership, authority, and accountability of an AI agent before and while it acts on behalf of a person or organization. For enterprise applications, knowing which agent is acting is only the starting point. The enterprise must also know who is responsible for it, whose authority it is acting under, the limits of that authority, and how its actions are accounted for.

This paper focuses on delegated authority within KYA. It defines a framework for AI agents operating in Oracle Fusion Cloud Applications, including how an enterprise distinguishes the authority of the person or organization from the narrower authority delegated to an agent and how that authority remains enforceable as agents move from assistance to execution. It is intended for enterprise architects, security leaders, application leaders, and product teams responsible for deploying AI agents that can access enterprise data and take business actions.

An agent is an AI-powered software actor that can reason, access enterprise information, invoke capabilities, and take actions on behalf of a user or organization. Its deployed version is the specific version of that agent running when the action occurs. The acting-for identity is the authenticated user or approved automation identity whose underlying business authority applies.

KYA asks four questions:

1. **Who is acting?** Agent name and deployed version
2. **On whose behalf?** Acting-for identity
3. **Within what limits?** Delegation
4. **With what accountability?** Evidence of decision and execution

User authority is the ceiling. Agent delegation can only further constrain it. It cannot expand it.

From identity to authority

Enterprise AI began primarily by helping people find information, summarize data, answer questions, and recommend what to do next. Increasingly, agents can take actions and perform work on behalf of people and organizations.

Across Oracle Fusion AI, agents can be created in AI Agent Studio, delivered as part of Fusion Agentic Applications, and used for more complex or long-running work through Fusion Claw. The nature and duration of the work may differ, but the security question is consistent: what authority has the enterprise delegated to the agent performing the work?

Knowing which agent is acting is necessary, but it is not sufficient. Traditional Fusion security starts with the acting-for identity. It establishes what that identity can access and what business actions it may perform. Agentic execution adds another software actor between intent and execution. That actor may need access to only part of the user's data, only certain operations, or only a limited form of an otherwise authorized transaction.

The result is a simple but important principle: User authority is the ceiling. Agent delegation can only further constrain it. It cannot expand it. Greater autonomy therefore does not require transferring all of a user's authority to an agent. It requires defining the portion of that authority appropriate for the work being delegated.

Copyright © 2026, Oracle and/or its affiliates / Public

Access, capability, and delegated authority

Three concepts need to remain separate: access, capability, and delegation.

- **Access.** Fusion identity, roles, privileges, and data security determine what the acting-for identity may access and do. If an HR specialist can access 5,000 worker records, that defines the user's data access. An agent resolving a specific HR case may need only the worker record associated with that case. KYA can constrain the agent to that narrower scope. The agent does not gain access to records that the acting-for identity cannot access.
- **Capability.** A capability is a bounded Fusion operation authorized at runtime. It might retrieve a manufacturing cost, search for a work order, update permitted employee information subject to applicable controls, or create a purchase. Capabilities make specific operations available to agents without turning the entire application into an unrestricted tool surface. Fusion authorization still applies when the capability executes. A skill is guidance, not a gate. A skill is business guidance that helps the model determine when and how to use capabilities. It can provide business semantics, required context, sequencing guidance, expected outputs, and boundaries. A skill is not an authorization boundary.
- **Delegation.** A delegation is the configured set of limits on what a particular agent may do with a capability. Those limits can apply to records, amounts, categories, suppliers, destinations, business units, task context, or other conditions. Access to data and possession of a capability are not the same as delegated authority to use them.

SAME USER, DIFFERENT AUTHORITY: A PROCUREMENT EXAMPLE	
A procurement user may be authorized to make purchases up to $10,000. A routine purchasing agent may legitimately have the capability to create purchases, while its delegation limits it to $100, designated categories, approved suppliers, and authorized business units.	
$75 purchase allowed Satisfies the $100 limit, designated categories, approved suppliers, and authorized business units.	**$500 purchase denied** The user is authorized to make it; the agent is not under its delegation.

How delegated authority is evaluated

KYA is enforced at runtime using trusted platform context. The model does not determine its own authority.

A prompt that tells an agent to access only one worker or spend no more than $100 can guide its reasoning, but that instruction is not the authorization decision. Agent identity, acting-for identity, records, amounts, business context, and other information needed to evaluate authority must come from trusted context rather than from the model's assertion that an action is permitted.

The evaluation can be understood as four distinct gates:

1. **Fusion authority.** Fusion identity, roles, privileges, and data security determine what the acting-for identity may access or do.
2. **Capability allow-list.** Determines which bounded operations this agent may invoke.
3. **KYA delegation.** Applies the narrower limits for this agent, deployed version, and task, such as permitted records, amounts, categories, suppliers, destinations, business units, and conditions.
4. **Business controls.** Deterministic validations, workflows, and approvals determine whether the transaction itself is allowed under applicable business rules.

Copyright © 2026, Oracle and/or its affiliates / Public

A failure at any gate stops the action or causes it to follow the applicable escalation or approval path. Guidance contained in a skill or prompt cannot override any of these gates.

KYA and deterministic business controls can both touch the same field, such as amount, and still do different jobs. KYA decides whether this agent, version, and task may attempt the action within its delegated limits. Validations, workflows, and approvals decide whether the transaction itself is valid. A delegation limit does not replace a business validation, and a business validation does not replace a delegation limit. Existing Fusion security, validations, workflows, and approvals remain authoritative.

KYA across Fusion AI

KYA provides the same authority model across AI Agent Studio, Fusion Agentic Applications, and Fusion Claw, while the way agents are created and the work they perform can differ.

SURFACE	WHO AUTHORS THE AGENT	WHAT WORK IT PERFORMS	WHO OWNS THE DELEGATION
AI Agent Studio	A customer or partner may author the agent.	Agent work is created in AI Agent Studio.	The customer or partner establishes the appropriate delegation for it.
Fusion Agentic Applications	Oracle, the customer, or the partner delivers the agent.	Agent work is delivered as part of a Fusion Agentic Application.	The enterprise owns and can narrow or withdraw the delegation in its Fusion environment.
Fusion Claw	An agent is authored in AI Agent Studio or delivered in a Fusion Agentic Application.	The agent performs complex or long-running work rather than a single bounded action.	The same delegation remains in force for the life of that work rather than being re-derived by the agent.

Greater execution capability does not confer greater authority.

KYA therefore provides a consistent way to reason about authority even when the execution pattern changes.

Governed execution

An agent can reason about a business objective and request a bounded Fusion operation. Execution still passes through the gates defined above. Only after the applicable controls permit the action does Fusion execute against authoritative enterprise data and state. The model can determine what it believes should happen next. It cannot turn that conclusion into permission.

AI reasons. Enterprise controls authorize. Fusion executes.

Accountability and evidence

Delegated authority must also be accountable.

- **Agent + version:** which agent and deployed version acted
- **Acting-for identity:** on whose behalf the agent acted
- **Capability:** which capability the agent invoked
- **Delegation:** which delegation limits were evaluated
- **Decision:** what authorization decision was made

Copyright © 2026, Oracle and/or its affiliates / Public

- **Execution:** what Fusion executed
- **Result:** what result was produced

Authorization evidence and execution evidence serve related but different purposes. The authorization decision establishes whether the requested action fell within the applicable authority. An Outcome Receipt is evidence of what was executed and the result. It should not be treated as the authorization mechanism itself. This distinction matters when an agent performs more than a single action. The enterprise needs to be able to connect the software actor and its delegated authority to the work that Fusion performed.

Accountability also means that delegation can be changed or withdrawn. The organization should not have to change the user's underlying business authority simply because it wants to change what a particular agent is permitted to do. KYA therefore makes the agent, its version, its acting-for identity, its delegation, and the resulting execution visible as distinct parts of the same enterprise action.

Increasing autonomy without losing control

Enterprise AI will continue moving toward greater autonomy. The objective is neither unrestricted agent access nor mandatory human approval for every action. It is controlled delegation.

An agent's authority can start narrow. The enterprise can then use execution evidence and evaluation to understand how the agent is performing. If the organization decides that broader autonomy is appropriate, it can make an explicit configuration change to broaden the agent's delegation. If less autonomy is appropriate, it can narrow or withdraw that delegation. The enterprise owns that decision.

The agent cannot widen its own delegation, and improved model capability does not automatically change its authority. A more capable model, a richer skill, additional capabilities, or a longer-running execution does not alter what the agent has been authorized to do.

That separation allows AI capability and enterprise authority to evolve independently. Agents can become better at reasoning and execution while the enterprise continues to decide how much authority each agent should receive for a particular job.

Know Your Agent provides a consistent framework for making that decision explicit and enforceable. It establishes the agent, the identity on whose behalf it acts, the limits of its delegation, and the evidence required for accountability. As AI moves from assistance to execution, the principle remains simple:

> **User authority is the ceiling. Agent delegation can only further constrain it. It cannot expand it.**

Greater autonomy can therefore coexist with enterprise control, because the agent's ability to perform work and its authority to perform that work remain separate.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

Copyright © 2026, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.