Workday AI

Product Summary

July 24, 2026

Contents

Agents

Agent System of Record

Agent Management

Setup Considerations: Agent System of Record

You can use this topic to help make decisions when planning your configuration and use of Agent System of Record. It explains:

- Why to set it up.
- How it fits into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What It Is

The Workday Agent System of Record (ASOR) is a centralized platform that enables you to manage your organization's digital agentic workforce by providing a single solution that you can use to:

- Discover, add, register, configure, monitor and manage your diverse range of AI agents securely at scale across various systems.
- Leverage a single control center for governance, security and auditing your agents, thereby reducing administrative overhead and mitigating security risks.
- View data insights into agent observability, usage and performance, enabling you to analyze and demonstrate the value and impact of your agents.

You can manage these agent types through the **Agent Management Hub**, regardless of where they’re developed and run:

- Workday-built agents (1P)
- Partner-built agents
- Self-built agents (3P)

In ASOR, the **Agent Management Hub** is the central location where you can register, configure, monitor, and manage your AI agents. An agent is a system that uses a Large Language Model (LLM) to reason and take action.

Every agent in ASOR has an agent definition. This definition provides a concrete manifestation of agent code, providing an administrator transparency of what an agent is and what it can do. Each agent definition in ASOR in Workday contains:

- **Agent Name:** The name of the agent.
- **Agent Description:** Brief description of the agent.

- **Skills:** The tasks or activities the agent can execute.
    - **Execution Modes:** We support 2 execution modes for agent skills:
        - Ambient Mode: The agent performs tasks as itself and security is evaluated using its own permissions.
        - Delegate Mode: The agent performs tasks on behalf of a human and, in doing so, security is evaluated using the worker's permissions.
    - **Tools:** The resources the agent may use when executing the skill. For agents that interact with Workday, tools will be Workday APIs.
    - **Resources:** Type of API that a tool uses. Examples: REST, SOAP, Graph, WQL.

Business Benefits

- **Enhanced Administrative Efficiency:** Provides a single control center for governance and auditing, ensuring agents are deployed securely at scale.
- **Operational Transparency:** Offers insights into agent activity, usage, and performance to help analyze the value and impact of your AI workforce.
- **System Stability:** Protects system performance - while ensuring that agents run securely with standardized authentication and auditing.
- **Agentic Interoperability:** Provides the ability for agents to interact across systems to get work done.

Use Cases Throughout the Agent Lifecycle

You can use ASOR and Agent Management Hub to manage your agents throughout the agent lifecycle, which consists of these 5 phases:

- **Define:** You can view the agent definition for an agent on its agent profile page in **Agent Management Hub**. For external agents, you provide a definition for your agent via API.
- **Register:** To start using an agent, you must first register it in **Agent Management Hub** to prepare it for configuration and activation. In order to register in Production Workday-built agents you must meet the following requirements:
    - uMSA
    - Workday product entitlements
- **Configure:** As you configure an agent, you can specify which skills it will use and who can access it.
- **Activate:** Once you register and configure your agent, you can then activate it - which enables users to interact with it based on the security permissions you configured.
- **Deactivate:** When you no longer need an agent, you can deactivate it. This hides the agent from users, but keeps it accessible in **Agent Management Hub** - where you can reactivate it in the future as needed.

Recommendations

- **Review the View Security for Agent Skill report when configuring agents:** Use this report to surface the domain and business process security policy configurations the Workday APIs and resources your agent may use. Upon runtime, Workday first evaluates the security groups that have access to the agent (Available To), then the security groups that have access to the tools (domain or BP policies for the APIs and resources).
- **Audit Trail Review:** Regularly examine the audit log for agent actions. The log clearly distinguishes between an ambient agent operating alone and a delegate agent acting on behalf of a specific user.

Requirements

To access ASOR, you don't require additional SKUs.

To register and use agents in the Agent System of Record fully in your production tenants, your Workday account team needs to opt-in to the Universal Main Service Agreement (UMSA).

Note: UMSA is required for non-production and production tenants for Workday-built agents. UMSA will not be required for non-production tenants for self-built agents.

Limitations

- **Agent Proxy and Delegation:** Workday agent interactions can't be proxied or delegated.
- **Key Management:** While ASOR handles the creation and secure storage of the client credentials (private key) in the Credential Store, you must ensure your security environment supports the OAuth 2.0 token-exchange process that utilizes this key pair.
- **Usage Analytics in Sandbox Tenants:** For agent usage analytics on the overview page, the sandbox refresh will not wipe out usage activities from previous weeks.

ASOR Security

Domains	Considerations
Agent Compliance	Provides access to reports and data required for agent compliance.
Agent Management Hub	Provides access to the Agent Management Hub - the centralized hub for viewing and managing all agents.
Manage: Agents	Provides access to tasks for managing agents including configuration, activation and deactivation in ASOR.
Reports: Agent Reporting	Provides access to view agent analytics and report data sources and filters for agent level reporting.
Reports: AI Agent Security	Provides access to reports about agent security information. Example: the **View AI Agent User Audit Trail** report.
Setup: Agents	Provides access to setup tasks and activities for agents in ASOR.

Agent Security

As you configure your agents, you can specify who has access to interact with the agent by providing security groups on the **Available To** column for each delegate execution mode skill. Example: You can specify *Employee as Self* to make a skill available to an employee who interacts with the agent. As long as a user is part of one of the security groups on one of the skills, they will have access to interact with the agent.

Note: Agent interaction security permissions are separate from tool execution permissions. Consider evaluating alignment between the security groups in the **Available To** prompt and the security groups that have permissions for the **Tools** the agent may execute using the **View Security for Agent Skill** report. This report shows you detailed information about the Agent's Tools APIs and the respective domain or business process security policies and permissions. The agent interaction security groups do not have to be a 1:1 match with the security groups on API policies. In order for the tool execution to succeed, a user must be a member of a security group on the agent skill and one that's on the API security policies. Upon agent runtime, Workday evaluates both user access to the agent and the user access to the APIs the agent is executing as tools.

Example:

Agent	Available To Security Group	Domain Security Policy Security Group Configuration	Successful Tool Execution
Self-Service Agent	Employee as Self	Employee as Self	Yes
Self-Service Agent	Employee as Self	Managers	No

Note: Ambient execution mode skills do not require interaction access because they take action without human user interaction, usually on a schedule or set trigger.

You can use the Set Up AI Administrator Security Permissions task to configure the security for ASOR, PCC and Sana all at once.

You can access the **All AI Agent Accounts** report secured to the *Domains: Workday Accounts* domain in the System functional area to view all agent accounts in your tenant. On the report, you can click the **Workday Account** related actions to view audit trails.

Agent System User (ASU) accounts enable you to secure and manage your agents in Workday. Workday automatically generates an ASU for your agent after you complete the **Configure Agent** task. You can view your ASU accounts for your agents using the **All AI Agent Accounts** task (secured to the Workday Accounts domain in the System functional area). You can also view AI agent accounts using the **All Workday Accounts** task.

Agent developers can leverage ASUs to interact with Workday data through Agent Gateway.

Reporting

The **Overview** section of the hub provides access to these reports (secured to the *Reports: Agent Reporting* domain) and tasks (secured to the *Manage: Agents* domain):

- **Active Agents** report
- **Activate Agents** task
- **Configure Agent** task
- **Deactivate Agent** task
- **Total Agent Sessions Over Time** report (only available for Workday-built agents)
- **Total Agent Sessions** report (only available for Workday-built agents)
- **Total Unique Users** report (only available for Workday-built agents)

The **Agent Registry** section displays your registered agents, along with their status and when an administrator user in Workday last made updates to their configuration.

You can click the name of an agent to view the agent's profile, the available skills for the agent, and these agent analytics reports (secured to the *Reports: Agent Reporting* domain and only available for Workday-built agents):

- **Agent Sessions**
- **Skill Interactions**
- **Total Skill Interactions Over Time**
- **Total Unique Users for the Agent**
- **Total Unique Users for the Skills**

The **Unregistered Workday Agents** section displays the **Find Unregistered Workday Agents** report (secured to the *Agent Management Hub* domain), where you can discover the Workday-built agents you're eligible to register.

You can access these reports for agent security, compliance, and auditing:

- **Agent Input and Output Request Details** (secured to the *Agent Compliance* domain and only available for Workday-built agents)
- **All AI Agent Accounts** (secured to the *Workday Accounts* domain)

- **Generate Agent Input and Output Report** (secured to the *Agent Compliance* domain and only available for Workday-built agents)
- **Input and Output Report For Registered Agents** (secured to the *Agent Compliance* domain and only available for Workday-built agents)
- **View AI Agent User Audit Trail** (secured to the *Reports: AI Agent Security* domain)
- **View Security for Agent Skill** (secured to the *Security Administration* domain and the *Manage: Agents* domain)

For additional agent reporting, you can access these data sources:

- **All Agent Definitions** (secured to the *Reports: Agent Reporting* domain) that provides fields for reporting on all registered and unregistered agent definitions.
- **All Agent Registrations** data source (secured to the *Reports: Agent Reporting* domain) that you can use in custom reports to analyze agent registrations.
- **Agent Input and Output Details** data source (secured to the *Agent Compliance* domain) that you can use to view your agent input and output interactions for the past 30 days. Workday can take up to 20 minutes to display the latest information.

You can also leverage these data sources (secured to the *Reports: Agent Reporting* domain) that provide usage analytics data for the past 30 days:

- **Agent Sessions by Day**
- **Agent Skill Interactions**
- **Agent Skill Interactions by Day**
- **Agent Unique Users by Skills**

Connections and Touchpoints

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Set Up Agent System of Record

Prerequisites

Security: *Security Configuration* domain in the System functional area. Required to configure the ASOR security domains.

Context

You can manage your organization's digital workforce using Agent System of Record (ASOR). To set up ASOR in your tenant, you must:

- Enable the ASOR functional area.
- Configure domain security policies for ASOR tasks and reports.

You must set up and configure ASOR in each of your tenants as there's no current method to migrate configurations.

Steps

1. Access the **Maintain Functional Areas** task.

   Select the **Enabled** check box for the Agent System of Record functional area.

   Click **OK** and then **Done**.
2. Access the **Activate Pending Security Policy Changes** task.

   Enter a comment and click **OK**.

   Select the **Confirm** check box and click **OK**.

3. Access the **Domain Security Policies for Functional Area** report.

   From the **Functional Area** prompt, select *Agent System of Record*.

   Select **Domain Security Policy > Enable** from the related actions menu for these domains:

   - *Agent Compliance*
   - *Agent Management Hub*
   - *Manage: Agents*
   - *Reports: Agent Reporting*
   - *Setup: Agents*

   Repeat this step for the *Reports: AI Agent Security* domain in the System functional area.
4. Access the **Maintain Permissions for Security Group** task.

   Select the *Maintain* operation.

   From the **Source Security Group** prompt, select the security group that you want to grant ASOR agent management access to.

   Note: Currently, you can only configure unconstrained groups on ASOR security policies.

   On the **Domain Security Policy Permissions** tab, provide *View and Modify* permissions for these domain security policies:

   - *Agent Compliance*: Access to reports and data required for agent compliance.
   - *Agent Management Hub*: Access to the **Agent Management Hub -** the centralized hub for viewing and managing all agents.
   - *Manage Agents*: Access to tasks for managing agents including configuration, activation and deactivation in ASOR.
   - *Reports: Agent Reporting*: Access to view agent analytics and report data sources and filters for agent level reporting.
   - *Reports: AI Agent Security*: Access to reports about AI agent security information. Example: the **View AI Agent User Audit Trail** report.
   - *Setup: Agents*: Access to setup tasks and activities for agents in ASOR.
5. Access the **Activate Pending Security Policy Changes** task.

   Enter a comment and click **OK**.

   Select the **Confirm** check box and click **OK**.

Register and Configure Workday-Built Agents

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

Set Up Agent System of Record.

Security: These domains in the Agent System of Record functional area:

- *Agent Compliance*
- *Agent Management Hub*
- *Manage: Agents*
- *Reports: Agent Reporting*
- *Setup: Agents*

Security: *Reports: AI Agent Security* domain in the System functional area.

Context

You can register, configure, activate, and deactivate Workday agents using the **Agent Management Hub**. You can edit previous configurations at any time.

Steps

1. Access the **Agent Management Hub** report.
2. Select the **Unregistered Workday Agent** tab.
3. Click **Register** the agent you want to register.

   You can only register agents in the SKUs obtained by your organization.
4. Select the **Confirm** check box, and then click **OK** to complete the registration.

   Workday moves the agent to the **Agent Registry** tab.
5. Select the **Agent Registry** tab and then click on the agent name to configure the agent.
6. From the agent's profile view, click **Configure Agent**.
7. In the **Status** column, make each relevant skill available by enabling the toggle slider.
8. For each enabled **Skill**, populate the **Available To** prompt with the security groups that you want to provide access to for that specific skill. The security groups added to the **Available To** prompt for an agent establish the agent's interaction policy.

   Note:

   Workday evaluates both user access to the agent and the user access to the APIs the agent is executing as tools at runtime. Workday recommends that you evaluate alignment between the security groups in the **Available To** prompt and the security groups that have permissions for the tools the agent might execute. See the Self-Service Agent FAQ on Workday Community for security troubleshooting information.
9. Click **Activate**.

Result

Employees that have access to the security groups you specified for each skill and the domain or business process security policy associated with the APIs that make up each skill can use the agent. When you activate an agent, the Agent System User (ASU) for the agent also activates automatically.

Sample ASOR API Agent Definition

The first section of this API defines basic information about your agent:

```
{
```

```
 "name": "Change Business Title Agent",
 "description": "A Workday agent for changing a business title with Agent
Gateway",
 "provider": {
   "id": "Provider=SELF-BUILT"
 },
 "url": "https://changetitleagent.com",
 "platform": {
     "id" : "Platform=GOOGLE_AGENTSPACE"
  },
 "skills": [
   {
     "description": "This skill gets worker information and changes a
business title.",
     "id": "changeTitle_1",
     "inputModes": [
       {
         "type": "application/json"
       }
     ],
     "name": "Change Title",
     "outputModes": [
       {
         "type": "application/json"
       }
     ]
   }
 ],
 "workdayConfig": [
   {
     "workdayResources": [
       {
         "description": "Change Business Title",
         "tool_name": "changeBusinessTitle",
         "agent_resource": {
           "id": "c2ffb30053964fbfa7a46dcfa577adb1"
         }
       },
       {
         "description": "Get Workers",
         "tool_name": "getWorkers",
         "agent_resource": {
           "id": "94a39e71541b468fa895955508287acd"
         }
       },
       {
         "description": "Internal Auth Check",
         "tool_name": "internalAuthCheck",
         "agent_resource": {
           "id": "6bbfa713d3851000081920672a0f0009"
         }
       }
     ],
     "executionMode": {
       "id": "Mode=Delegate"
     },
     "skillId": "changeTitle_1"
   }
 ],
 "capabilities": {
   "stateTransitionHistory": false,
   "streaming": false,
   "pushNotifications": false
 },
```



```
  "supportsAuthenticatedExtendedCard": false,
  "version": "v1"
}
```


The second section of this API is optional. It includes Workday-specific information including which APIs will be invoked as part of this agent:


```
 {
      "workdayResources": [
        {
          "description": "Change Business Title",
          "tool_name": "changeBusinessTitle",
          "agent_resource": {
            "id": "c2ffb30053964fbfa7a46dcfa577adb1"
          }
        },
        {
          "description": "Get Workers",
          "tool_name": "getWorkers",
          "agent_resource": {
            "id": "94a39e71541b468fa895955508287acd"
          }
        },
        {
          "description": "Internal Auth Check",
          "tool_name": "internalAuthCheck",
          "agent_resource": {
            "id": "6bbfa713d3851000081920672a0f0009"
          }
        }
      ],
      "executionMode": {
        "id": "Mode=Delegate"
      },
      "skillId": "changeTitle_1"
    }
```


Each skill can have multiple tools. Each tool points to an individual Workday resources in which you can specify using the Workday ID (WID) of the resource.

Sample Response

After you successfully register an agent through the API, you should receive a JSON response:


```
{
  "version": "v1",
  "provider": {
    "descriptor": "Self-Built",
    "id": "9030a823ae1a10002d624e2d637e0000"
  },
  "skills": [
    {
      "inputModes": [
        {
          "type": "application/json"
        }
      ],
```

```
      "id": "changeTitle_1",
      "description": "This skill gets worker information and changes a
 business title.",
      "name": "Change Title",
      "outputModes": [
        {
          "type": "application/json"
        }
      ]
    }
  ],
  "url": "https://changetitleagent.com",
  "description": "A Workday agent for changing a business title with Agent
 Gateway",
  "capabilities": {
    "pushNotifications": false,
    "stateTransitionHistory": false,
    "streaming": false
  },
  "workdayConfig": [
    {
      "executionMode": {
        "descriptor": "Delegate",
        "id": "d785eba56e9c100035d336a043ff0000"
      },
      "skillId": "changeTitle_1",
      "workdayResources": [
        {
          "description": "Internal Auth Check",
          "tool_name": "internalAuthCheck",
          "agent_resource": {
            "id": "6bbfa713d3851000081920672a0f0009",
            "descriptor": "trident/userAuth/checkAuth (GET) (v1 -  )"
          }
        },
        {
          "agent_resource": {
            "id": "c2ffb30053964fbfa7a46dcfa577adb1",
            "descriptor": "api/workers/businessTitleChanges/create (POST)
 (v1 -  )"
          },
          "tool_name": "changeBusinessTitle",
          "description": "Change Business Title"
        },
        {
          "tool_name": "getWorkers",
          "agent_resource": {
            "id": "94a39e71541b468fa895955508287acd",
            "descriptor": "api/workers/view (GET) (v1 -  )"
          },
          "description": "Get Workers"
        }
      ]
    }
  ],
  "platform": {
    "id": "b49b32cfdbef10002184b61535490000",
    "descriptor": "Google Agentspace",
    "reference_id": "GOOGLE_AGENTSPACE"
  },
  "name": "Change Business Title Agent",
  "supportsAuthenticatedExtendedCard": false
}
```

The response contains an ID at the top, which is your reference Workday ID if you need to GET the agent definition using the agentDefinition API.

External Agents

Register External Agents

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

Set Up Agent System of Record.

Security:

- *Agent Management Hub* domain in the Agent System of Record functional area. Required for validating that the agent is registered in Workday.
- *Manage Agents* domain in the Agent System of Record functional area. Required for activation and skill configuration.
- *Set Up: Tenant Setup - Security* domain in the System functional area. Required for registration.

Context

Currently, you can only register and define external agents in Workday by using the ASOR API. External agents are defined and registered simultaneously using the API, they are not two separate steps. You can use any API client of your preference to invoke the API.

Refer to ASOR v1.2 API documentation on Github and ASOR JSON Swagger documentation sample for troubleshooting.

Registration endpoints:

- **REST API Endpoint:** https://us.agent.workday.com/asor/v1/agentDefinition.
- **Token Endpoint:** https://us.agent.workday.com/auth/oauth2/<Tenant_Name>/token
- **Authorize Endpoint:** https://us.agent.workday.com/auth/authorize/<Tenant_Name>?response_type=code&client_id=<client_id>&state=test3pagent1&redirect_uri=<redirect_uri>

For information related to other regional availability outside of the U.S, see the Agent Gateway documentation: Reference: Regional Availability of Agent Gateway.

Authentication Options:

To register external agents, you need an access token in your ASOR API invocation. Below are the different options to obtain a token to invoke the ASOR API call.

Option 1: Manually Authenticate an API Client

1. Access the **Register API Client** task.
    - **Client Name:** Enter a unique identifiable name for your agent. We recommend that you use a separate client for each agent so that they are easier to manage.
    - **Client Grant Type:** *Authorization Code Grant*.
    - **Access Token Type:** *Bearer*.
    - **Redirection URI:** Enter a URL to redirect users to after authorization.
    - **Scope (Functional Areas):** *Agent System of Record*.
    - **Include Workday Owned Scope:** Select this check box.
2. Copy and save the **Client ID** and **Client Secret** values. You can use these to get an access token to call the Definition API.
3. Paste this URL into a new window. It should redirect you to google.com with an appended code which you can use to call the API:

    https://us.agent.workday.com/auth/authorize/<Tenant_Name>?response_type=code&client_id=<client_id>&state=test3pagent1&redirect_uri=<redirect_uri>
4. Create a new request using an external API Client (Example: Bruno): *https://<tenantHost>/ccx/oauth2/<tenantName>/token*
    - Body: *grant_type=authorization_code&code=<authorizationCode>&client_id=<clientID>&client_secret=<ClientSecret>*
    - Auth: Username = *<ClientID>*, Password = *<ClientSecret>*.
    - This generates an access token and refresh token that you can use to call the ASOR Agent Definition API.
    - As you complete this step, consider: Concept: External Agent ASU Considerations .

Note: The user registering the agent must have access to the Setup: Agents domain in the Agent System of Record functional area to register an agent using the ASOR API.

Option 2: Authenticate Using Extend

If you're a Workday Extend or Workday Orchestrate user, you can retrieve an access token through Workday's developer site.

1. Access developer.workday.com and sign in.
2. On the top-right, click the user menu. The menu should display your current company name.
3. Click **Tenant** > **Sign In to Tenant**.
4. Select your environment and tenant and click **Connect to Tenant**.
5. Sign in to the tenant. You must sign in with an account that has access to the *Setup: Agents* domain in the Agent System of Record functional area to register an agent using the ASOR API.

Register an External Agent Using the ASOR API

Prerequisites:

- An access token for an account that has access to the *Setup: Agents* domain in the Agent System of Record functional area.
- An API Client of your choice.
- Security: These domains in the System functional area:
    - *Custom Report Creation*
    - *Manage: All Custom Reports*
    - *Report Tag Management*

Context:

To register an external agent, you must:

- Find the Workday Identifiers (WIDs) of the relevant Workday APIs (SOAP and REST) you intend to include in your agent's Tools Definition by creating a custom report.
- Find the Agent Provider using the **View Agent Provider** task.
- Call the ASOR REST API

Finding SOAP and REST-based WIDs for Agent Tools Definition

1. Access the **Create Custom Report** task.
2. As you create the report, consider:

Option	Description
Report Type	Select *Advanced*.
Optimized for Performance	Unselect this check box.
Data Source	Select *Public Web Services* for SOAP APIs and *All Public Service Operations* for REST APIs.

3. For SOAP APIs: On the **Edit Custom Report** page, on the **Columns** tab of the report definition, add these rows:

Business Object	Field
Web Service	Web Service
Web Service Operation	Web Service Operation Name
Web Service Operation	Workday ID

4. For REST APIs: On the **Edit Custom Report** page, on the **Columns** tab of the report definition, add these rows:

Business Object	Field
Service Operation	Service
Service Operation	Name
Service Operation	Workday ID

5. Save and run the report.

Note: As you retrieve WIDs for your APIs, you can also cross-reference these lists:

- REST API WIDs
- REST APIs Not Available for Ambient Agents
- Graph API WIDs

Find the Agent Provider

Agent providers refer to who has built the agent and are displayed in the **Built By** field on the agent's profile.

1. Access the **View Agent Provider** task, secured to the *Setup: Agents* domain in the Agent System of Record functional area.
2. Use the Provider ID in your agent registration API call.

Find the Agent Platform

Agent platforms refer to the external platform or system the agent is developed and run on and are displayed in the **Built On** field on the agent's profile.

1. Access the **View Agent Platforms** task, secured to the Setup Agents domain in the Agent System of Record functional area.
2. Use the Platform ID in your agent registration API call.

Call the ASOR REST API

Create a new request to register your agent using an external API Client, Example: Bruno.

As you create the request, consider:

- **Endpoint:** https://us.agent.workday.com/asor/v1/agentDefinition
- **Operation:** POST
- **Body:** Refer to ASOR v1.2 API documentation on Github and ASOR JSON Swagger documentation sample.
- **Headers:**
  - Authorization: Bearer <token>
  - wd-agent-tenant-alias:<your tenant name>

Agent Management Hub

After you successfully load your agent definition into Workday, you can verify that it is registered by viewing it in the **Agent Management Hub**.

1. Access the **Agent Management Hub** report.
2. Click **Agent Registry** to display a list of your agents.
3. Click an agent to display overview information for it.

Next Steps

Configure your agent in Workday.

Related Information
Reference
Sample ASOR API Agent Definition

Configure External Agents

Prerequisites

Set Up Agent System of Record

Security: These domains in the Agent System of Record functional area:

- *Agent Compliance*
- *Agent Management Hub*
- *Manage: Agents*
- *Reports: Agent Reporting*
- *Setup: Agents*

Security: *Reports: AI Agent Security* in the System functional area.

For Ambient-mode agents only:

- ../../../../authentication-and-security/security-for-integrations/access-to-external-endpoints/hzp1471450668309.dita. Security: The *Security Administration* domain in the System functional area.

Context

You can configure external agents using the **Agent Management Hub**.

Steps

1. Access the **Agent Management Hub** report.
2. Select the **Agent Registry** tab and then click on the agent name to configure the agent.
3. From the agent's profile view, click **Configure Agent**.
4. In the **Status** column, make each relevant skill available by enabling the toggle slider.
5. For each available delegate execution mode skill, populate the **Available To** prompt and determine the security groups that you want to add for that specific skill for the agent.

   Note: The security groups you select in the **Available To** prompt must also have permissions to the domain or business process security policies that secure the agents' tools. You can use the **View Security for Agent Skill** report to assist with your agent security configurations. This report shows you detailed information about the agent's Tools APIs and the respective domain or business process security policies and permissions. At agent runtime, Workday evaluates both user access to the agent and the user access to the APIs the agent is executing as tools.
6. Click the **Confirm** check box, and then click **OK**.
   a) For delegate skills, you must provide a **Redirect URI** as the callback endpoint for your agent. Your agent development partner can provide this information.
   b) For ambient skills, you must provide an x509 public key from your agent development platform. Your agent development partner can provide this information. Select a unique key that's not in use by another agent. See also: ../../../../authentication-and-security/security-for-integrations/access-to-external-endpoints/hzp1471450668309.dita. Security: The *Security Administration* domain in the System functional area.
7. Click **OK**.
8. When you configure the agent for the first time, we display the OAuth client details for the agent.

   Note: Copy and save the Client ID and Client Secret values. This page won't display again and you won't be able to access this information again.
9. Enter the OAuth client details and endpoint URLs back into the agent development platform code for the agent to enable access during runtime. The OAuth client and endpoint URLs details that we display include:
   - Authorize Endpoint URL
   - Token Endpoint URL
   - Endpoint URL
   - OAuth 2.0 Client ID
   - OAuth 2.0 Client Secret (Delegate only)
   - Username for Agent System Account (Ambient only)
10. Select **Agent Registry**, and click the agent you want to activate.
11. From the agent's profile view, click **Activate Agent**. On the **Activate Agent** window, select the **Confirm** check box, and then **OK** to complete the activation.

Result

Workday automatically creates an Agent System User (ASU) and assigns an Agent Security Group (ASG) for the agent - which you can find through the **All AI Agent Accounts** report, secured to the *Workday Accounts* domain in the System functional area. You can use these as you configure the security policies and permissions for your agent.

Next Steps

Configure Security Policies for Agent Skills .

Concept: External Agent ASU Considerations

We recommend you leverage these considerations while creating external agents.

Delegate ASUs

The ASU client credentials that are provided after agent configuration should be used for OAuth 2.0 Authorization Code Grant Flow to enable your agent to get access during agent runtime.

When manually testing the authorization code grant flow of an external agent, use the client details and endpoint URLs provided during agent configuration as inputs for these steps:

1. Retrieve the authorization code by pasting this URL into a new window: *https://<providedAuthorizeEndpoint>?response_type=code&client_id=<clientID>&state=<agentName>&redirect_uri=<redirectionURI>*.

   The URL redirects you to a login page where you must manually provide your user credentials that the agent will be acting on behalf of.

   After successfully logging in, you're redirected to an **Allow/Deny** page where you grant the agent access to your Workday account. Select **Allow** to be redirected to your provided Redirection URI with an appended code which you can use to call the next API.
2. Retrieve the ASU token by creating a new request using an external API client using the authorization code provided in the previous API call.

   Example: Bruno:

   - *POST https://<providedTokenURL>*
   - *Body:grant_type=authorization_code&code=<authorizationCode>&client_id=<clientID>&client_secret=<ClientSe*

     This generates an access token and a refresh token that you can use to test calls your agent makes to Workday services.

In the body of the response back from the token endpoint, the *expires_in* parameter is expected to be returned as type Integer. In different test environments, this parameter type can differ between Integer and String, so Workday recommends that the external client is able to handle both string and int types.

When you need to update an agent definition, you can supply the same agent name, version, and provider to the POST AgentDefinition API, and it will update. If there isn't a match, Workday creates a new agent registration.

When your agent sends the request to the token endpoint using AuthCode and client credentials, both the access token and refresh tokens are created and sent back.

The access token expiry time is 3600 sec (60 min). The refresh token expiry time is 24 hr.

When an access token expires, the refresh token creates a new one.

Typical OAuth clients should only need:

- **Client Secret** and **Client ID**: Obtained during the agent configuration process.
- **Authorize Endpoint**: *https://us.agent.workday.com/auth/authorize/ <Tenant Alias>*
- **Token Endpoint**: *https://us.agent.workday.com/auth/oauth2/<Tenant_Alias>/token*
- **Redirect URL**: Provided by the agent developer during the agent configuration process.

Ambient ASUs

The ASU Client ID and username that are provided after agent configuration should be used to perform JWT assertion and token generation.

- Issuer must be the Client ID.
- Subject must be the ASU username.

The x509 corresponding keypair that is required during ambient skill registration is used during agent runtime to perform JWT assertion.

Update your agent’s code so that during agent runtime, when a request is submitted to the agent, the agent checks if it has a valid access token cached. If it doesn't, or if the token is expired, we:

- Create a new JWT assertion
- Fetch a JWT Bearer token
- Cache token for Workday API requests

Agent Security and Compliance

Setup Considerations: Agent Security

You can use this topic to help make decisions when planning your agent security configuration. It explains:

- Why to set them up.
- How they fit into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements.
- Questions and limitations to consider before implementation.

What It Is

The Agent Security framework governs the identity, authentication, and authorization of AI agents within your tenant. Unlike standard chatbots, agents can execute significant tasks in enterprise systems, such as requesting time off or retrieving paycheck information. The framework ensures agents operate under the principle of least privilege, with robust controls for both autonomous and user-driven interactions.

Business Benefits

- Enhanced Governance: Ensures that agents, like workers, have unique identities and auditable activity logs.
- Granular Control: Enables you to restrict agent capabilities based on the execution mode, ensuring agents only access data they are explicitly authorized to handle.
- Transparent Auditing: Provides clear audit trails that distinguish when an agent acts autonomously versus when it acts on behalf of a user.

Use Cases

- Interactive Assistance on delegate mode: Interactive Assistance on delegate mode: A user asks an agent to request the next Monday off. The agent executes the request on behalf of the user. Security is evaluated based on the intersection of the user's permissions and the agent's allowed skills.
- Background Processing on the ambient mode: An agent automatically aggregates data pools or evaluates datasets based on a schedule. The agent acts as itself, using its own security permissions without user intervention.

Questions to Consider

Question	Consideration
Which execution mode does your agent require?	There are 2 distinct agent execution modes: • Delegate Mode: Use when the agent acts on behalf of a user. Security checks the user's access to the skills. • Ambient Mode: Use for background tasks where the agent acts as itself. Security checks the agent's access to data and tasks.
Who is permitted to interact with and invoke a specific delegate agent skill?	You must define an Agent Interaction Policy that specifies which user security groups can interact with the agent's skills. The invoking user must

Question	Consideration
	be in the allowed security groups for the skill to successfully trigger it.
How will you manage agent identities?	Agents require unique Agent System User (ASU) accounts. An agent can have up to 2 ASUs: 1 for delegate mode and one 1 ambient mode.
What specific data domains or business process actions does an ambient agent need to access?	An ambient agent's permissions are evaluated solely against its own Agent System User (ASU) permissions. You must assign the unique Ambient Agent Security Group to the required domain or business process security policies.
Which authentication components must the integrating application like Agent Forge support?	For delegate Mode, the system uses an OAuth 2.0 *On-Behalf-Of* flow that involves exchanging the User Alpaca Token for a Delegated Access Token. You must ensure the application can handle the necessary token types and header requirements.
Can I configure ASUs to work with proxy accounts?	No, ASUs don't support proxy accounts.

Recommendations

- Abide by the principle of least privilege. Only grant agents the minimum necessary access to domains and business processes required for their specific skills.
- Use separate ASUs for each mode. Ensure that each agent has distinct accounts for delegate and ambient execution to prevent confusion in authorization and auditing.
- Review the Security Analysis Report. Use this report to surface the domain and business process security policy configurations for your agent skills.
- Audit Trail Review: Regularly examine the audit log for agent actions. The log clearly distinguishes between an ambient agent operating alone and a delegate agent acting on behalf of a specific user.

Requirements

- Define the security policies and enable the agent's skills in the Agent System of Record (ASOR) to generate an Agent System User (ASU) and its credentials.
- The generated ASU and its associated OAuth client are disabled by default. You must activate an agent to enable the agent for use.
- For delegate agent mode, the user making the requests must have security access to the underlying agent tools and tasks.

Limitations

- Dual Identity Requirement: An agent that needs to operate in both delegate and ambient modes must have separate ASU accounts and credentials configured for each execution mode.
- Key Management: While ASOR handles the creation and secure storage of the client credentials (private key) in the Credential Store, you must ensure your security environment supports the OAuth 2.0 token-exchange process that utilizes this key pair.

Tenant Setup

NA

Security

Security groups managing agents require *View* and *Modify* access to Report/Task permissions to view and execute agent tasks, and *Put* access to Integration permissions to transfer agent configuration data.

Domains	Considerations
Manage: Agents	Provides access to setup tasks and activities for the Agent System of Record (ASOR).
Setup: Agents	Provides access to tasks for configuration, activation, and deactivation of agents.
Agent Management Hub	Provides access to the centralized hub for viewing and managing all agents.
Reports: AI Agent Security	Provides access to the new **View AI Agent User Audit Trail** report.

Reporting

- **View Security for Agent Skill**: Displays the domain and business process security policy configuration for agent skills. You can access this report from the related actions menu of an agent skill.
- **View AI Agent User Audit Trail**: Displays user activity, distinguishing between By User and On Behalf Of User. You can access this from the related actions of an agent and as a standalone task.

Connections and Touchpoints

The Agent Security framework touches the following key areas of Workday:

Features	Considerations
Workday Configurable Security	Agent permissions rely entirely on domain and business process security policies and security groups, which control who can access secured items.
Agent System of Record (ASOR)	ASOR manages the definition and configuration of agents and acts as the system of record for agent security policies and credential reference IDs.
OAuth 2.0 Authentication	The agent authentication flow uses OAuth for the On-Behalf-Of token exchange in delegate Mode. First-party (1P) agents: The access token is valid for up to 60 minutes when you use the Authorization Code grant. Third-party (3P) agents: The access token is valid for 4 hours. You can't customize access token expiry for third-party agents currently.
Workday REST APIs	Agent access to Workday data is carried out through REST API endpoints, which are secured to specific domains or business process security policies.

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Configure Security Policies for Agent Skills

Prerequisites

- Unique Ambient Agent Security Group is generated for ambient agents.
- Security: *Security Configuration* domain in the System functional area.

Context

Workday evaluates security for:

- Delegate agents, by using the security access of the invoking user.
- Ambient agents, based on the agent's permissions. When you activate a skill, Agent System of Record (ASOR) generates a unique Ambient Agent Security Group (ASG). You must assign this ASG to the relevant domain or business process security policies to grant access to secured items, such as tools and APIs.

Steps

1. Access the **View Security for Agent Skill** report.
2. From the related actions menu of each **Security Policy**, select **Domain Security Policy** > **Edit Permissions**.
    a) Complete the task:

Option	Description
Delegate Agent	From the **Security Groups** prompt, select the security groups that include the invoking users who require access.
Ambient Agent	From the **Security Groups** prompt, select the Ambient Agent Security Group.

    b) Select the **View** or **Modify** check boxes to grant the security group access to securable items.
    c) If a tool in the **View Security for Agent Skill** report requires Get/Put access, select the **Get** or **Put** check boxes to grant security groups access to integrations.
3. Activate Pending Security Policy Changes

Concept: Agent Security

Agent Security ensures that AI agents operate securely within your enterprise by assigning them unique identities, robust authentication, and granular authorization controls. Agent security governs how agents interact with data and perform tasks, abiding by the principle of least privilege.

Workday secures AI agents using the same robust framework used for workers. To ensure a trusted environment, the system applies the principle of least privilege through two distinct layers of protection:

- Governance: By treating agents as non-human identities, Workday prevents agent sprawl and ensures every machine action is tied to a specific, manageable account.
- Transparency: Every action performed by an agent is fully auditable, providing the same level of visibility into agent actions as you have for employees.

While you manage the lifecycle and definition of your agents in the Agent System of Record (ASOR), Agent Security dictates their runtime behavior.

The Agent Security framework supports 2 distinct agent execution modes:

- Delegate Mode: Acting on behalf of a user. Example: A user delegates to the agent the task of requesting a day off for a specific date.

- Ambient Mode: Acting autonomously based on an event trigger or schedule. Though an agent isn't fully autonomous, the agent operates independently to perform background tasks, such as aggregating data pools or responding to event triggers.

Agent Identity: Agent System User (ASU)

Similar to an Integration System User (ISU), Agents use Agent System User accounts (ASUs). To guarantee that there is unambiguous control over what the agent can access and to provide transparency for auditing, each agent has a unique identity, or user account.

- Unique Identity: Each agent has a unique ASU account.
- Mode-Specific: An agent can have up to 2 ASUs; 1 each for delegate execution and ambient execution. Each ASU will have a specific OAuth 2.0 client.
- Management: The system automatically generates and manages ASUs when you configure skills in the Agent System of Record. Example: Activating an ambient skill triggers the creation of the necessary ambient ASU.

ASU Creation and Registration

The ASU creation process occurs in tandem with the agent's configuration and skill enablement in ASOR.

- ASU Generation: When an administrator enables skills for an agent, ASOR automatically creates a dedicated Delegated ASU or Ambient ASU for that agent in a disabled state. When the agent is activated, the associated ASUs are automatically enabled.
- OAuth Client and Key Pair: An OAuth client is generated and attached to an ASU. A private key pair is created, and the public key is registered with the Workday authorization server. The ASU is then granted the ability to authenticate and perform tasks defined in its skills.
- Credential Storage: ASOR securely stores the client credentials, including the private key, in the Credential Store. A unique reference ID is then stored in ASOR as a pointer to these key-pair credentials, which are used to generate ASU tokens that are exchanged along with the user token for a delegated ASU, rather than for OAuth 2.0 client credentials.

Comparison of Security Modes

Feature	Delegate Mode	Ambient Mode
Primary Use Case	Interactive tasks. Example: Request time off for yourself.	Background tasks. Example: Data aggregation.
Identity Used	Combination of user and agent ASU.	Agent ASU only.
Authentication	The agent uses the OAuth 2.0 in the On-Behalf-Of flow. First-party (1P) agents: The access token is valid for up to 60 minutes when you use the Authorization Code grant. Third-party (3P) agents: The access token is valid for 4 hours. You can't customize access token expiry for third-party agents currently.	The agent authenticates as an ambient ASU, with no user involvement.
Authorization Logic	The system evaluates security based on the intersection of	The system evaluates security solely against the agent's permissions.

Feature	Delegate Mode	Ambient Mode
	the user's permissions and the agent's allowed skills.	
Configuration	Agent Interaction Policy: Defines who can interact with the specific agent skills.	Domain Security Policy: Defines what the agent can access.
Security Groups	The user must be in the allowed security groups for the skill to invoke it.	When an ambient skill is activated, a unique Ambient Agent Security Group is generated and must be assigned to the relevant domain or business process security policies.
Audit Log	Records the transaction as performed by the agent as *By User* and the user as *On Behalf Of User*.	The audit log shows the agent ASU as the *By User*.

Implementation Considerations

Workday provides a Security Analysis report for the domain and business process security policy configurations for agent skills. This report helps you identify what security configurations are necessary for your agents.

Concept: Agent Interaction Policy

The Agent Interaction Policy is a security configuration within the Agent System of Record (ASOR) that explicitly defines which users are authorized to converse with or invoke specific agent skills.

How It Works

The policy functions as an opt-in mechanism for an agent's delegate mode skills. If a user isn't in the security group for an agent skill, the user can't use that skill even if the user has access to the domain or business process security policies for the tools in that skill. When a user attempts to interact with an agent, the Workday Agent Security framework performs a two-step security evaluation:

1. Agent Interaction Check: The system checks whether the user belongs to a security Group included in the agent's Agent Interaction Policy, which is configured in the **Available To** list. If the user isn't a member of any of these groups, the agent interaction is denied, even if the user has the necessary security permissions to perform the tasks defined in the skill's **Tools** section.
2. Domain & Business Process Check: If the user passes the interaction check, the system then verifies their standard permissions including domain and business process security policies, to ensure they are authorized to see the data or perform the action requested. Domains are checked not only for the tools, but also at the field level when the agent's skill is executed, which is consistent with how domain security works without agents..

Applicability

Workday allows you to configure the Agent Interaction Policy only for agents and skills that operate in the delegate mode.

- Delegate Mode: Requires an Agent Interaction Policy. You must explicitly opt-in security groups to allow them to use these skills.
- Ambient Mode: Doesn't use Agent Interaction Policy. As ambient agents act as themselves in the background based on triggers or schedules, they don't interact directly with a user and therefore don't require a policy defining which user can interact with them.

Configuration

You can define Agent Interaction Policy in the **Agent Management Hub** or during agent registration by configuring the **Available To** settings for a specific skill.

Example: For a Recruiting agent with a Job Requisition Creation skill, you can add the Recruiters security group to the **Available To** list. Only users in the Recruiters security group can request the agent to create a requisition. A user in the Employee As Self security group can't use this skill, even if they had domain access to create requisitions.

FAQ: Agent Security

Where are OAuth tokens and token validity stored?	Workday stores OAuth tokens and token validity settings in the Workday Object Management System (OMS).
How does Workday mitigate risk if OAuth or session tokens are compromised?	Workday provides preventive controls to help protect against replay attacks from OAuth clients. If session or access tokens are compromised, an attacker could replay requests within the token's lifetime. Workday can't detect compromised credentials on your behalf. If you suspect compromise, disable the affected OAuth 2.0 client to protect against further use of those credentials. You enforce this control on the customer side.
Can I customize access token expiry for agents?	For first-party (1P) agents, you can customize how long access tokens remain valid when you configure OAuth Client and OAuth Client for Integrations settings. For third-party (3P) agents, access token expiry customization isn't available yet. Workday will add this capability in a future release. For more on how token-related activity is recorded, see Concept: User Activity Logging.
Are access token and refresh token expiry configurable?	Yes. For integration clients, access token and refresh token settings, including expiry, are fully configurable today. For third-party (3P) agents, access token expiry customization is coming in a future release.
How are Agent System Users (ASUs) managed and stored? Do they use the same Workday accounts as Integration System Users (ISUs)?	Workday stores and manages ASUs in the Workday Object Management System (OMS). Similar to an Integration System User (ISU), each agent uses Agent System User (ASU) accounts. Each agent has a unique identity, or user account, so you have unambiguous control over what the agent can access and clear transparency for auditing. • Unique identity: Each agent has a unique ASU account. • Mode-specific accounts: An agent can have up to 2 ASUs—1 for delegate execution and

	1 for ambient execution. Each ASU has a dedicated OAuth 2.0 client. • Management: When you configure skills in the Agent System of Record (ASOR), Workday automatically generates and manages the required ASUs. For example, activating an ambient skill triggers creation of the necessary ambient ASU.
What are the key differences between ASUs and Integration System Users (ISUs)?	ASUs and ISUs both provide dedicated system user accounts in Workday. ASUs are tied to the tools and skills that you configure, manage, and audit in ASOR. ISUs support integration use cases and aren't scoped to agent skills in ASOR. For more information, see Concept: Agent Security.
How are agent skills populated, controlled, and configured by Workday and/or the customer?	You configure agent skills in ASOR under your organization's security administrator. Workday and your organization enable skills based on your agent design and security requirements. Map high-risk or sensitive transactions in your tenant to the skills that Workday and your organization have enabled. You can monitor and audit AI agent transactions and activity using the **View AI Agent Users Audit Trail** report.

Agent Gateway

Authenticate Agents to Agent Gateway

Prerequisites

- Register and activate your agent with Agent System of Record (ASOR) using the agent registration API. See Register External Agents. Note these values:
  - Client ID.
  - Client Secret.
  - Redirect URI for delegate agents.
  - x509 Public Key for ambient agents.
- Configure External Agents.

Context

All agents must use Agent Gateway to interact with Workday. For the Agent Gateway to route requests to the correct Workday data center, it must know the alias of your tenant. You must provide your tenant alias with all agent API requests, including requests for authentication. Your tenant alias is typically the name of your tenant, and can be found in the URL of your Workday instance: https://wd8.myworkday.com/<tenantalias>/d/home.html.

To direct all relevant API calls to your assigned Agent Gateway endpoint, you must modify your agent's code or configuration.

For more details on authentication, see Configure External Agents.

Steps

1. To request an authorization code, send an HTTPS GET request to the authorization endpoint in Agent Gateway.

   Send this request in your browser and sign in if requested:

   ```
   https://us.agent.workday.com/auth/authorize/<Tenant Alias>?
   client_id=<OAuth_Client_ID>&response_type=code
   ```

   Substitute endpoints based on your region.

   The Agent Gateway will send this request to the Auth Gateway in the data center where your tenant is located, using the Tenant Alias in the request. The Auth Gateway will then redirect you to a Workday login pop-up, to authenticate. After a successful login and consent for the agent to access Workday data, your agent will receive an authorization code.
2. Copy the authorization code value from the response.
3. To request an access token, send a POST request to the token endpoint in Agent Gateway.

   Fill in the Client ID and Client Secret you noted from ASOR, your tenant alias, and the authorization code.

   Substitute endpoints based on your region.

   ```
   POST  https://us.agent.workday.com/auth/oauth2/<Tenant_Alias>/token

   grant_type=authorization_code
   code=<authorization_code>
   client_id=<OAuth_Client_ID>
   client_secret=<OAuth_Client_Secret>
   ```

Result

Your agent receives an access token and is now authorized to interact with Workday through Agent Gateway.

Concept: Workday Agent Gateway

You can use Workday's Agent Gateway to connect your AI agents with Workday's Agent System of Record (ASOR) more easily. It enables your agents to collaborate and communicate information with Workday, providing real-time support and automation within your existing workflow.

Agent Gateway provides a single, unified regional endpoint to centralize and streamline how third-party agents interact with Workday. Agent Gateway provides access to the Workday APIs, including Graph, for all agentic partners, along with access to the Agent Definition Registry API. .

The Agent Gateway includes:

- All Public REST operations
- All Public SOAP operations
- Workday Graph API
- Workday Query Language (WQL)
- Workday RaaS

- Agent Gateway enables you to:

- Use your agent to work efficiently with future Workday platform updates and security protocols.
- Ensure your agent interacts with Workday in a stable, high-performance environment through built-in rate limiting and performance guardrails.
- Ensure all API calls are authenticated and authorized through Workday's security layer.
- Use a single entry point for all your agent's Workday API interactions.
- Clearly track your agent's API consumption for accurate billing and cost management.

API Requests Through Agent Gateway

All third-party agents interacting with Workday APIs must route their API traffic through Agent Gateway using Agent System User (ASU) security. For more information, see Concept: Agent Security.

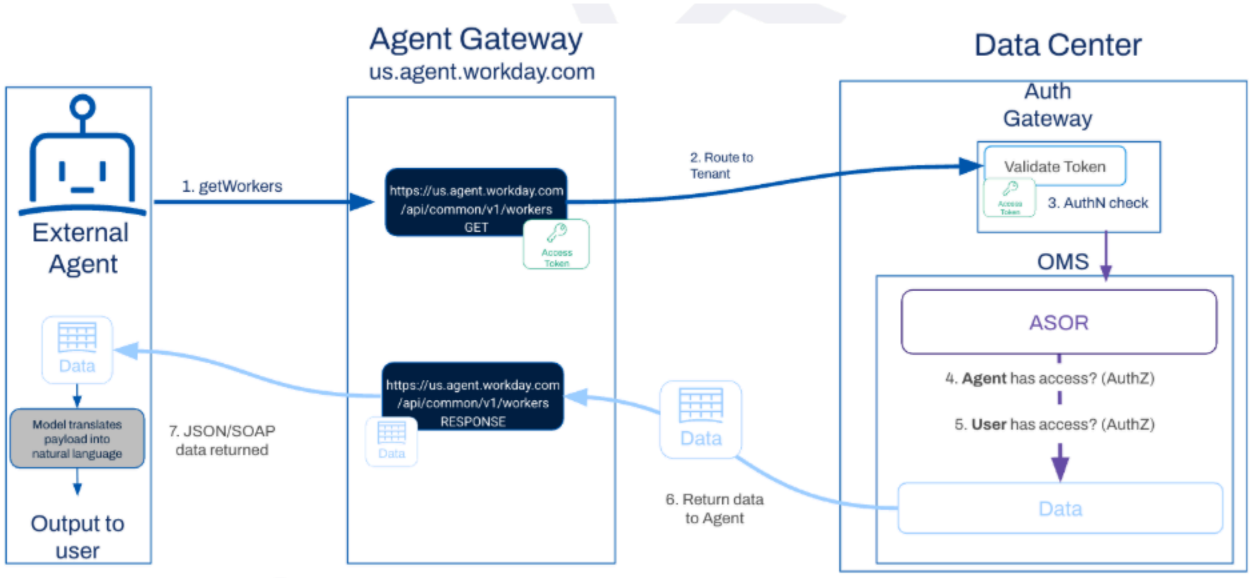

Figure 1: API Requests through Agent Gateway

To route your API traffic through Agent Gateway, you must register your external agents in Workday through Agent System of Record (ASOR) and configure authentication. See Configure External Agents in Workday.

API Call Requirements

Your agent's API calls must include:

- Gateway Endpoint: us.agent.workday.com. Substitute endpoints based on your region.
- Tenant Alias HTTP header: Provide wd-agent-tenant-alias as an HTTP header in the request. The value must be unique.
- SOAP calls: The correct endpoint for SOAP calls is

  ```
  https://us.agent.workday.com/soap/{version}/{serviceName}
  ```

  Substitute endpoints based on your region.

Sample API request for US region:

```
GET https://us.agent.workday.com/api/common/v1/workers
```

Sample HTTP Header:

```
wd-agent-tenant-alias: stark-industries
```

OAuth 2.0 Authentication

If your agent platform supports the OAuth 2.0 standard, it should support the standard OAuth 2.0 Authorization Code Grant authentication flow.

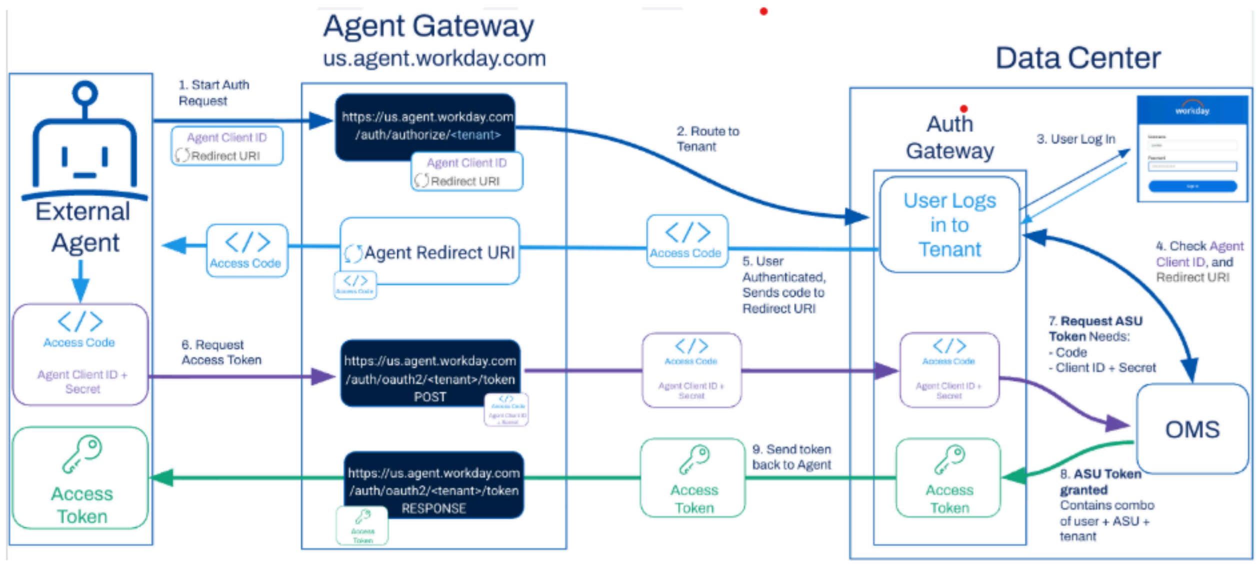

Figure 2: OAuth 2.0 Authentication

Regional Availability of Agent Gateway

Agent Gateway is available in multiple regions. Use these endpoints based on the Workday data center region that hosts your tenant:

Region	Public Regional Endpoint
US	https://us.agent.workday.com
EU	https://eu.agent.workday.com
UK	https://uk.agent.workday.com
CAN	https://ca.agent.workday.com
AU	https://au.agent.workday.com
SIN	https://sg.agent.workday.com
IND	https://in.agent.workday.com
JPN	https://jp.agent.workday.com

Note: Changing regions resets your agent analytics data in **Agent Management Hub**. To preserve your agent analytics data in **Agent Management Hub**, we recommend that you avoid changing regions when possible.

Agent Marketplace

Concept: Agent Marketplace

The Workday Marketplace is the Digital Hub of the Workday economy. It is a single destination for customers to discover, try, and buy trusted solutions from software and services partners. It consolidates the Workday solution ecosystem to support the evaluation of best-practice solutions that integrate with Workday.

Workday provides the Agent Marketplace within the Workday Marketplace for customers to discover AI agents. As part of the Workday ecosystem, the Agent Marketplace provides agent solutions designed to address business challenges and extend Workday functionality.

The Agent Marketplace features a catalog of AI agents from Workday and Workday partners. Partners in the Built on Workday (BoW) or Connect/Platinum partner programs can build and distribute certified agents.

The Agent Marketplace enables you to find targeted solutions. Access the Agent Marketplace at:https://marketplace.workday.com/en-US/pages/agents.

You can register, configure, monitor, and manage AI agents securely at scale using the Agent System of Record (ASOR).

Agent Marketplace for Different User Types

Workday has designed Agent Marketplace for these user types:

- Customers
    - Centralized Discovery: A single location to discover and learn about available Workday and Workday Partner agents.
    - Informed Decision-Making: Access to information on agent features, benefits, and responsible AI practices to help in selecting the right solutions.
    - Direct Connection: The **Contact Us** button allows customers to connect directly with Workday or Workday partners for more details.
- Workday Partners
    - Increased Visibility: An opportunity to showcase the agent-based solutions to a wide range of Workday customers.
    - Lead Generation: The **Contact Us** button serves as a direct channel for customer inquiries and potential leads.
- Implementers: Search and select agents to meet business requirements.
- Developers: Upload new agents or skills.

Concept: Agent Listing in Workday Marketplace

To introduce agent listings, Workday makes these changes to Workday Marketplace:

- Agents solution type: A new **Agents** solution type filter.
- Agent cards and listings: Each agent has a dedicated page with features, benefits, and descriptions of the roles and skills it provides.
- Categorization: Agents are categorized based on Workday’s high-level business groupings so they align with product strategy and support a consistent search and discovery experience across Workday experiences..
- Agent link: A link under the AI Solutions section that directs users to agent listings.
- Responsible AI badging: Workday agents that have completed the **Responsible AI** attestation process are badged accordingly.

Workday-Built Agents

BP Optimize Agent

Set Up BP Optimize Agent

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

You must register and activate the BP Optimize Agent in production before you can use it in your sandbox tenant. After you activate the agent in your production tenant, allow up to 24 hours for the system to process the changes before you try to activate the agent in your sandbox.

- Set Up Agent System of Record.
- Security: These domains in the System functional area:
  - *Reports: AI Agent Security*
  - *Business Process Administrator*
  - *BP Optimize Agent*

  The *BP Optimize Agent* domain inherits security from the *Business Process Administrator* domain. To customize access for your organization, you can override the inheritance and use the *BP Optimize Agent* domain.
- (Optional) The BP Optimize Agent includes an optional ML Data Contribution feature, labeled **BP Optimize Agent**, for UMSA customers. This feature grants Workday access to agent traces, which are generated based on user prompts within the Workday agent chat. It's enabled by default for organizations with UMSA enabled. However, you can manually opt out.

Context

You can register, configure, and activate the BP Optimize agent in Workday using the **Agent Management Hub**.

Review these current requirements and limitations before you set up the BP Optimize Agent:

- Eligibility: To use the agent, your tenant must be in the US, EU, or limited UK-based tenants that generate 2 million or fewer transactions per month. The BP Optimize Agent is not available to customers with UK-based tenants that are subject to strict data processing requirements that prevent Workday from processing customer data outside of the UK.
- Supported Environments: You can use the agent in production and sandbox tenants. To use the agent in a sandbox tenant, you must first activate it in production, which requires Flex Credits.
- Configuration and Cost: During setup, you must configure the agent by selecting your product lines and a lookback period. Currently, you can’t change the lookback period after you submit. Note that these settings dictate your analysis scope and affect your Flex Credit usage, which can incur additional costs.

- Product Line Considerations: When selecting product lines, note these system behaviors:
    - Model Business Processes: These are included in the **Platform and Product Extensions** product line.
    - Shared Business Processes: When a business process spans multiple product lines, you only need to select one of those associated product lines to bring that business process into the agent's scope. You don't need to select all of them.
    - Configuration Updates: When Workday adds a new business process type to an existing product line, or when a product line's associations change, the BP Optimize Agent doesn't automatically apply these changes to your existing configuration.
    - Lookback Period: Carefully consider your lookback period selection. After you submit your initial configuration, you can modify your product lines using the **Reconfigure BP Optimize Agent** task, but you currently can't change your lookback period.
- Language Support: Currently, the BP Optimize Agent only supports English. If a user's language is set to French, for example, the agent will default to English.
- Excluded steps: The agent excludes any step configured after the *Completion* step. It considers a business process complete even if the workflow progresses beyond this step.

Steps

1. Access the **Agent Management Hub** report.
2. Select the **Unregistered Workday Agent** tab.
3. For the **BP Optimize Agent**, click **Register**.
4. Select the **Confirm** check box, and then click **OK** to complete the registration.

   Workday moves the **BP Optimize Agent** to the **Agent Registry** tab.
5. Select the **Agent Registry** tab and then click the *BP Optimize Agent* name to configure the agent.
6. From the agent's profile view, click **Configure Agent**.
7. From the **Additional Configuration** column, click the Configure BP Optimize Agent link to configure your analysis scope and select a **Lookback Period** and **Product Lines**

   Note: As you make your selections, the configuration summary page displays dynamic **Estimated Initial Flex Credits** and **Estimated Flex Credits for Subsequent Months** to help you budget. Carefully review your lookback period selection because you currently can’t change it after you submit.
8. From the **Status** column, make the **Process Improvement** skill available by sliding the toggle.
9. From the **Available To** prompt on the **Process Improvement** skill row, in the System functional area, select either:
    - The *Business Process Administrator* domain.
    - The *BP Optimize Agent* domain if you have customized it.

   The security groups that you select in the **Available To** prompt must also have permissions to the domain or business process security policies that secure the agents. You can use the **View Security for Agent Skill** report to assist with your agent configurations.
10. Click **OK**.
11. From the **Agent Registry** tab, click the **BP Optimize Agent** and click **Activate Agent**.
12. Select the **Confirm** check box and then click **OK**.

Result

After data ingestion completes, which can take up to 48 hours, workers in the *Business Process Administrator* security group can access the BP Optimize Agent from the dashboard and from the Workday agent chat bubble icon to:

- Analyze and visualize business process performance metrics and execution trends.

- Compare your company's performance against peer benchmarks for industry, region, and company size.
- Identify bottlenecks, anomalous execution patterns, and their root causes.
- Get tailored, actionable recommendations to optimize your business processes.

Note:

- Always review and verify the accuracy of AI-generated insights and recommendations before making configuration changes to your business processes.
- When you have more than 1 agent configured, you might need to access the agent chat and select the BP Optimize Agent from the agent menu.
- After your initial onboarding, data ingestion occurs automatically on the first day of each month. The agent processes the previous month's historical event data so those new insights and recommendations become available. This ongoing monthly processing consumes Flex Credits.

Next Steps

To update your product lines after your initial setup, you can use the **Reconfigure BP Optimize Agent** task in the Agent System of Record (ASOR). Note these system behaviors when reconfiguring the agent:

- Lookback Period: You currently can't change your lookback period after your initial activation.
- Timing and Effective Date: Product line updates take effect on the first day of the next month. To ensure that Workday successfully registers your changes in time for the new month, we recommend submitting your updates at least one day before the last calendar day of the current month.
- Historical Data for New Product Lines: When you add new product lines, the agent only analyzes data from the immediately prior month. It doesn't apply the historical lookback period you selected during your initial activation.
- Flex Credit Estimates: The configuration summary page dynamically displays an **Estimated Monthly Difference** to help you budget. If you reduce your product line selections, this estimate can be a negative number, which indicates a decrease in your expected ongoing monthly usage. Workday rounds the Estimated Monthly Difference up to the nearest 100.

If you no longer want to use the BP Optimize Agent, you can deactivate the Process Improvement skill from the Agent Management Hub. When you deactivate the agent or skill, Workday initiates these actions:

- Automatic Data Purge: Workday automatically deletes your tenanted data, including agent configurations in ASOR and business process recommendations, 21 days after deactivation. We do not purge your billing data.
- Reactivation Within 21 Days: When you reactivate the agent before the 21-day threshold, Workday restores your previous settings and insights. We automatically analyze your data for any missed periods during the deactivation. This analysis might consume Flex Credits if it includes new data generated while the agent was inactive.
- Reactivation After 21 Days: When you reactivate the agent after the 21-day threshold, your previous data is permanently deleted. You must configure the agent again as a new setup, which consumes Flex Credits.

Note:

- To avoid consuming additional Flex Credits to reconfigure the agent and reanalyze data that your organization previously processed, we recommend adjusting your product line scope to keep the agent active instead of deactivating it.
- To prevent Flex Credit consumption for the upcoming month, we recommend deactivating the agent at least 3 days before the last day of the current month. When the agent remains active on the first day of the new month, automatic data ingestion begins and consumes Flex Credits for that month.

Concept: BP Optimize Agent

The BP Optimize Agent is an AI-powered assistant that helps you improve the efficiency, effectiveness, and overall performance of your business processes within Workday. The agent analyzes your current processes, identifies areas for improvement, and provides actionable recommendations with step-by-step guidance.

The BP Optimize Agent uses:

- The execution details of configured business processes and their corresponding steps to analyze execution times and identify anomalous patterns.
- Tenant-specific execution data to generate aggregated averages for benchmarking.
- Proprietary system data to determine benchmark groups and data.

Note: To avoid skewing metrics, the BP Optimize Agent excludes data from:

- EIBs
- Web services
- Integration loads
- Transactions that immediately completed (duration = 0)

The agent considers only actual business process transactions that occur within the Workday application.

Process Improvement Skill

The BP Optimize Agent provides the Process Improvement skill, which enables Workday administrators to:

- Gain deep insights into business processes, locate bottlenecks, and identify root causes.
- Compare business process performance against benchmarks across industries, regions, and company sizes.
- Get tailored and actionable optimization recommendations specific to their unique business process usage and configuration.

For details, see Concept: BP Optimize Process Improvement Skill.

Security Considerations

BP Optimize Agent users must have **Modify** permissions on the *Business Process Administration* or *BP Optimize Agent* security domains in the System functional area.

The BP Optimize Agent displays Personally Identifiable Information (PII) data only when displaying the **Created By** and **Last Modified By** users. This information is visible from the **BP Optimize Agent** dashboard and the **Overview** section of the **Trends and Anomalies** page when you:

- Click a business process on the bar chart or line chart view.
- Click **Inspect** on the business process modal view.

Each company's individual benchmarking data can't be identified by other Workday customers. Workday only generates benchmark data when a minimum number of customers meet the defined criteria, specifically to prevent the identification of any single customer.

Agent Deactivation and Data Purge

To help you manage your data securely, Workday handles your data during deactivation and reactivation based on these rules:

- Automatic Data Purge: If you deactivate the agent or the Process Improvement skill, Workday automatically deletes your tenanted data, agent configurations, and recommendations 21 days after deactivation.
- Reactivation Within 21 Days: When you reactivate the agent before the 21-day threshold, Workday restores your previous settings and automatically analyzes data for any missed periods. This analysis might consume Flex Credits if it includes new data generated while the agent was inactive.
- Reactivation After 21 Days: When you reactivate the agent after the 21-day threshold, your previous data is permanently deleted. You must configure the agent again as a new setup, which consumes Flex Credits.

To avoid consuming additional Flex Credits to reconfigure the agent and reanalyze data that your organization previously processed, we recommend adjusting your product line scope to keep the agent active instead of deactivating it.

Limitations

- Trend insights: Limit insights to events that initiate and complete within the selected time period. The agent excludes events that start in one period but complete in a subsequent period.
- Benchmarking insights: Generate only when the minimum required industry peer cohort has enough transactions for that business process in the same time period.
- Event statuses: Consider only completed events with a status of Successfully Completed, Rescinded, Canceled, or Process Terminated. The agent excludes in-progress events.
- Tenant eligibility: Requires your tenant to be in the US, EU or limited UK-based regions and average fewer than 2 million transactions per month. The agent is not available to customers with UK-based tenants that are subject to strict data processing requirements that prevent Workday from processing customer data outside of the UK.
- Language support: Currently limited to English.

Concept: BP Optimize Process Improvement Skill

Overview

The Process Improvement skill of the BP Optimize Agent enables you to:

- Analyze business process data.
- Visualize metrics data.
- Compare with benchmark data.
- Review Benchmarking Insights.
- Observe anomalous trends.
- Identify anomalies and root causes.
- Generate optimization recommendations.
- Implement optimization recommendations.
- Ask questions about business process optimization.

How to Access

You can access the Process Improvement skill on the **BP Optimize Agent** report to:

- Analyze the performance of a specific business process, select it on the chart and click **Inspect**.
- Adjust benchmark data by clicking the filter icon and scrolling down to the **Industry Benchmarking** section of the filter panel.
- Ask questions using natural language by clicking the Workday agent chat bubble icon and selecting the **BP Optimize Agent**.

Analyze Business Process Data

The Process Improvement skill uses the execution details of configured business processes and their corresponding steps. By default, the dashboard displays business processes by:

- Functional Group: The **BP Optimize Agent** dashboard displays a tab for each of your company's licensed product areas (example: Extend, Spend, Talent, Workforce). The default tab is **Workforce**.
- Time Period: The default time period is the last completed quarter of the standard calendar year. Example: In April 2026, the last completed quarter is Q1 2026, which is January to March of 2026.

  You can modify the *Time Period* filter, either by month or by quarter.

  Note: The agent uses calendar months to determine quarters, not the fiscal year.

- Business Process and Business Process Definition: The *Business Process* filter preselects the business process types associated with the top 5 business process definitions that took the longest to complete in the specified time period.

  The *Business Process Definition* filter lists the active business process definitions for the selected business process types.

  Adjust the filter to focus on the business processes you want to analyze.
- Metrics: By default, the graph displays the Time to Completion (Hours), which is the average number of hours it took the business processes to complete. You can select **Send Back**, which shows the percentage of events that are sent back.

Visualize Metrics Data

The Process Improvement skill enables you to view business process performance data for successfully completed, rescinded, cancelled, and terminated events in these formats:

- Bar Chart: This default view displays the average completion time of business process definitions that meet the filter criteria. Click a bar to inspect the business process execution details.

  Note: If benchmark data is available, a line across the bar chart represents the benchmark data. See Compare with Benchmark Data.
- Table: The table displays execution metrics, including average completion time and send backs. The metrics include baseline (tenant values) and benchmark values, if any. You can sort the columns by clicking the funnel to display these types of metrics:
  - **Average**: The average value of a metric.
  - **Maximum**: The maximum value of a metric.
  - **Minimum**: The minimum value of a metric.
  - **p50**: The p50, or median, is the value below which 50 percent of the observed metric values lie for the tenant or the benchmark in the selected time period. Example: 50 percent of events are completed in 20 hours, while the other 50 percent take longer.
  - **p95**: The p95 is the value below which 95 percent of the observed metric values lie for the tenant or the benchmark in the selected time period. Example: 95 percent of events are completed in 37 hours, while the remaining 5 percent take longer.
- Line Chart: This view displays the trend of business process performance over a specified period. You can click each point to see more business process execution details.

To export bar charts and line charts as PDF or image files:

1. On a bar chart or line chart, click **Related Actions**.
2. Select **Download as PDF** or **Download as PNG**.

For easy reference and data analysis, you can also export tables to CSV and Excel formats. The exports include all the available values. (Example: Average, Maximum, p95.)

Compare with Benchmark Data

If benchmark data is available, the bar chart displays a benchmark line across the business process bars. When there is only 1 business process definition, the benchmark data is displayed as a black dot, instead of a horizontal line. The benchmark lines enable you to compare your company's business process performance with other companies in the same industry, region, and company size. The **Table** view also includes benchmark metrics.

The BP Optimize Agent generates benchmark data by:

- Averaging execution data across customers that share these criteria: industry, region, and enterprise size.
- Determining a tenant's benchmark group by referencing the tenant's details within Workday records.

The BP Optimize Agent doesn't display benchmark data when there aren't enough customers in the tenant's benchmarking peer cohort to meet the minimum configured threshold.

Review Benchmarking Insights

When you inspect a business process, you can view deeper comparative insights that identify exactly how your business processes perform compared to your peer cohort.

The **Benchmarking** section:

- Highlights areas where your business process performance falls behind or exceeds your industry, region, and company size benchmarks.
- Analyzes step-level executions to identify up to 5 specific steps with the highest duration for your tenant.
- Compares configuration differences between your tenant and your best-performing peers at both at the definition level and across those 5 steps to generate actionable optimization recommendations. The agent doesn't display comparison data when your benchmarking peer cohort lacks sufficient customers.
- Evaluates only the quarter that you selected.
- Includes events with a status of *Successfully Completed*, *Rescinded*, *Canceled*, or *Process Terminated*.
- Excludes any step configured after the *Completion* step. The agent considers a business process complete even if the workflow progresses beyond this step.

Observe Anomalous Trends

When you select a business process on a chart or table and click **Inspect**, the inspect page opens in a separate tab where you can view deeper trend insights that help you identify anomalies, patterns, or changes in business process performance over time.

The **Trends** section:

- Displays how a specific business process performed in the selected time period compared to the preceding time period. Example: When Q1 2025 is the selected time period, the agent compares the business process performance in the tenant between Q1 2026 and Q4 2025.
- Includes only events that are initiated and complete within the selected time period. The agent excludes events that start in one period but complete in a subsequent period. Example: When Q1 2026 is the selected time period, the agent compares only events initiated and completed in Q1 2026 with events initiated and completed in Q4 2025. It excludes events started in Q1 2026 but completed in Q2 2026.
- Includes events with a status of *Successfully Completed* , *Rescinded*, *Canceled*, or *Process Terminated*.
- Excludes any step configured after the *Completion* step. The agent considers a business process complete even when the workflow progresses beyond this step.
- Displays optimization recommendations when business process performance trends slower. It does not display recommendations when a business process trends faster than in the previous time period.
- Identifies root causes for the trend.

  The agent identifies significant changes in step-level executions between the two time periods and determines which steps had the greatest impact on the business process performance change. It also calculates the percentage contribution of each identified step to indicate its relative impact.

Identify Anomalies and Root Causes

When you inspect a business process, you can view anomalous execution patterns, which identify problematic business processes that need to be resolved or optimized.

The **Anomalies** section:

- Highlights any unusual business process executions, and describes how a specific business process performed within the specified time period.
- Includes events with a status of *Successfully Completed*, *Rescinded*, *Canceled*, or *Process Terminated*.
- Includes events that complete within the selected time period, even when the events started prior to the selected time period. Example: When Q1 2026 is the selected time period, the agent identifies anomalies on business processes completed in Q1 2026, including completed events that started before Q1 2026.
- Excludes any step configured after the *Completion* step. The agent considers a business process complete even when the workflow progresses beyond this step.
- Lists the top root causes and key contributing steps for the anomalous transactions.

  The agent analyzes events identified as anomalous in the selected time period and identifies the steps that had the greatest negative impact on the business process performance.

  The agent displays:

  - The metric measured for the root cause, such as duration, send backs, or reassignment.
  - Specific steps that contribute to the anomaly, including the count of events in which that step is detected as anomalous, the average time taken by that step in those events, and the total occurrences of that anomaly (such as sent backs or reassignment).

Generate Optimization Recommendations

The BP Optimize Agent provides optimization recommendations for trend insights and anomalous execution patterns. Note that the agent displays the **Trends** section only when a business process trends slower than in the previous time period.

When you review the insights in the **Trends and Anomalies** sections, the agent:

- Dynamically generates tailored recommendations in real time instead of relying on pre-computed data. This generation process can take up to 1 minute.
- Formulates actionable advice to assist you in resolving and optimizing problematic business process steps. The BP Optimize Agent language model uses the Workday Administrator Guide, Workday Community, and other expert Workday knowledge sources.
- Provides reference links under **Learn More**, when available.

If recommendations fail to generate and you get an error message, try to generate the recommendations again.

Implement Optimization Recommendations

Although the BP Optimize Agent tailors the recommendations according to the reported anomalies, always carefully review the generated optimization recommendations and determine how they fit your organization and specific business processes. There might be optimization opportunities beyond the provided recommendations.

After you implement a recommendation or make a configuration change to a business process, you can:

-
- View the line chart on the **BP Optimize Agent** dashboard. The line chart enables you to analyze the business process performance and identify any performance changes.
- Use the BP Optimize Agent to review the latest trends, anomaly insights and benchmarks. By iteratively using the agent, you can identify further optimization opportunities and recommendations.

Concept: BP Optimize Agent Flex Credit Estimator

The BP Optimize Agent provides immediate, data-driven Flex Credit estimates to help you manage your budget before you activate or reconfigure the agent.

Workday calculates these Flex Credit projections using a 12-month average of your tenant's actual historical event volumes for your selected product lines. We multiply that average by your selected lookback period and round up to the nearest 100 to provide these estimates:

- Estimated Initial Flex Credits: The immediate, one-time consumption for your initial activation (or a new setup following a deactivation purge). This covers the cost of analyzing your historical data based on your selected lookback period and product lines. Note that this estimate displays as 0 if a waiver applies to your first-time activation.
- Estimated Flex Credits for Subsequent Months (Recurring): The expected ongoing monthly consumption following your activation. On the first of each month, the BP Optimize Agent brings in your previous month's business process events to analyze and generate new insights.
- Estimated Monthly Difference: The change in expected monthly usage when you update your product lines during a reconfiguration.

Viewing Flex Credit Estimates

Before you can access these estimates, you must initiate the setup or reconfiguration of the agent. See Set Up BP Optimize Agent .

As you configure your analysis scope, the configuration summary page dynamically displays your estimates.

Note: The configuration summary page displays these estimates when you configure the agent in a sandbox tenant, but you aren't charged Flex Credits in that environment.

Limitations

- The Flex Credit estimator is intended strictly for budgeting purposes.
- These estimates are provided for informational purposes only, and Workday is not responsible for their accuracy.
- Actual Flex Credit usage might vary from the initial projections based on real-time event volumes and changes in your tenant environment.

Reference: BP Optimize Agent Sample Prompts

When you click the Workday agent chat bubble icon, you can enter specific prompts about business process optimization. When you have more than 1 agent configured, you might need to access the agent chat and select the **BP Optimize Agent** from the agent menu.

Refer to these examples to help you structure your prompts effectively.

Use Case	Sample Prompts
Analyzing Business Processes	• Show me the 3 best performing business processes by duration in Q1 2026. • What are the 3 worst-performing Change Job business processes? • What are the 5 worst send-back counts in December 2025?
Trend Insights	• Can you share trend insights on Request Time Off for Collab Delegation? • How can I improve slow performance? • How are Change Job BPs trending in 2026?
Benchmark Data	• What are the possible regions I can compare my data to? • What are the benchmarks for Request Time Off for Financial Services?

Use Case	Sample Prompts
	• What’s the benchmark for job applications in the Europe region for Q1 2026?

Anomaly Insights	• Which BP has the highest anomaly rate in Q4 of 2025?
	• What's the root cause of anomalies on Change Job BPs in Q1 2026?
	• What are recommendations to remove anomalies on Job Application for Web marketing in 2025?
	  ◦ Can you suggest additional recommendations for the initiation step for the Job Application for Web Marketing?
	  ◦ Can you provide step-by-step instructions on your first recommendation?

Financial Audit Agent

Set Up Financial Audit Agent

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

- Set Up Agent System of Record.
- Security: These domains in the Agent System of Record functional area:
  - *Agent Compliance*
  - *Agent Management Hub*
  - *Manage: Agents*
  - *Reports: Agent Reporting*
  - *Setup: Agents*
- *Reports: AI Agent Security* in the System functional area.

Context

You can set up the financial audit agent so that it can identify and retrieve audit samples for audit requests.

Steps

1. Access the **Agent Management Hub**.
2. In the **Unregistered Workday Agents** section of the **Agent Management Hub**, click **Register** for the **Financial Audit Agent**.
3. Click **Confirm**.
4. Workday moves the **Financial Audit Agent** to the **Agent Registry** section.
5. In the **Agent Registry** section of the **Agent Management Hub**, click on the *Financial Audit Agent* name to configure the agent.
6. From the agent's profile view, click **Configure Agent**.
7. For each enabled Skill, populate the Available To prompt with the security groups that you want to provide access to for that specific skill. The security groups added to the Available To prompt for an agent establish the agent’s interaction policy.

   Note: Workday evaluates both user access to the agent and the user access to the APIs the agent is executing as tools at runtime. Workday recommends that you evaluate alignment between the security groups in the **Available To** prompt and the security groups that have permissions for the tools the agent might execute. Access the **View Security for Agent Skill** report to view which security policies must be configured for the tool to function.
8. Click **Activate**.

Next Steps

When you finish using the Financial Audit Agent, you can click **Deactivate** to turn it off. You can activate, deactivate and reactivate the Financial Audit Agent at any time in the **Agent Management Hub**.

Concept: Financial Audit Agent

Overview

The Financial Audit agent provides accountants an efficient, automated, and accurate way to provide auditors with high volumes of audit sample requests within the procure-to-pay lifecycle.

The Financial Audit Agent includes these skills:

- Audit Samples and Supporting Documents
- Generate Compilation Package

These skills of the Financial Audit Agent enable you to:

- Quickly and accurately retrieve all relevant documents, such as supplier invoice, purchase order, receipt, invoice operational journal entry, supplier payment support, supplier contract, supplier invoice adjustments, or prepaid spend amortization schedule.
- Compile supported documents into an organized package for review and delivery, facilitating prompt audit information request response.

Security Considerations

Financial Audit agent users must have view and modify permissions on the *Audit: Audit Requests* domain in the Common Financial Management functional area.

Additionally, agent users must have permissions to supplier invoice data through at least 1 of these domains:

- *Process: Supplier Invoice - Reporting* in the Supplier Invoice functional area.
- *Reports: Financial Compliance* in the Common Financial Management functional area.

- *Reports: Supplier Accounts* in the Supplier Invoice functional area.

The agent operates on-behalf of the initiator and:

- Retrieves objects that the initiator has access to.
- Retrieves all applicable supporting documents requested, without evaluation of the initiator's security. However, the initiator's security applies for viewing the supporting documents from the audit request results.
- Has read-only access to the financial dataset.

Agent users can view:

- All audit requests submitted by all users.
- All audit request results but the results that display are determined by the user's security access.

Limitations

The Financial Audit agent currently only supports financial data in the accounts payable, procure-to-pay workflow, which includes supplier invoices and related documents. The agent doesn't have access to Human Capital Management data.

Reference: Financial Audit Agent Sample Prompts

Refer to these examples to help you structure your prompts effectively.

Prompting Tip	Example Prompts
Specify sample context and include details such as document types and invoice numbers for precise responses.	N12: SURL Sample Support. Please provide the support requested for our SURL sample selections. For each sample selection, please provide (1) invoice, (2) payment support vouched to the bank statement, and (3) if not included within the invoice, evidence of the delivery date (e.g. contract). Selected supplier invoices: 10043, 10042, 6685.
Clearly define and use conversational language and keywords as filters. You can use words like quarter, vendor, invoices, and between to add granularity.	Provide supporting documentation for invoices paid in Q4 2024 to the vendor Flower Power.
Specify the parameters for more targeted responses.	Retrieve invoices for the company GMS recorded after 1st January 2026 which exceed $100,000.
Specify a time period of less than or equal to 12 months for faster responses.	Retrieve all supporting documents for supplier invoices over $100,000 for GMS from Jan - Mar 2026.

Example: Create a Compilation Package Using Financial Audit Agent

This example illustrates how to create an audit request package with the Generate Compilation Package skill of the Financial Audit Agent.

Context

You are an accounting professional who has just received a sampling request from your external auditor. You must gather all supporting documentation for a few specific invoices.

Note: The compilation package only includes invoice attachments with these file types: PDF, CSV, JPEG, PNG, TXT, XLS, and XLSX.

Prerequisites

- Set up the financial audit agent.
- Security: *Audit: Audit Requests* domain in the Common Financial Management functional area.

Steps

1. Access the **Create Audit Request** task.
2. In the **Request Name** field, enter *Ap Cutoff Sample Selection*.
3. In the **Request Details** field, enter:

   Please provide the support request for our AP Cutoff sample selections. For each sample selection, please provide (1) invoice, (2) payment support vouched to the bank statement, and (3) evidence of the delivery date/ date of service, including a contract, if applicable. Selected supplier invoice: INV-2025-09-081.
4. Click **Start Request**.
5. Ensure the **Document Types** the agent selects match this list by clicking **Add Document Type** or the trash can icon:
   - *Supplier Invoice*
   - *Supplier Payment*
   - *Bank Reconciliation*
   - *Supplier Contract*
   - *Receipt*
6. Select **Confirm Types**.
7. Review the **Sourced Documents** the agent selects.
8. Select **Complete Review**.
9. For an invoice, select **Download Package**.
10. Enter *INV 2025-09-081*in the **PDF File Name** field.
11. Click **Next**.
12. Select **Download Package**.
13. Click **Complete Request**.

Result

You’ve downloaded a compiled audit request sample PDF package that contains all supporting documents for the audit.

Next Steps

Send the PDF package to the external auditor.

Payroll Agent

Set Up Payroll Agent

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.

3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

- Set Up Agent System of Record

Context

You can set up the Payroll agent to enable your payroll practitioners to access and use its skills. The Payroll agent provides task assistance, information retrieval, and data summarization through conversational AI.

Steps

1. Access the **Agent Management Hub** report.
2. Select the **Unregistered Workday Agent** tab.
3. For the **Payroll Agent**, click **Register**.
4. Select the **Confirm** check box, and then click **OK** to complete the registration.

   Workday moves the **Payroll Agent** to the **Agent Registry** tab.
5. Select the **Agent Registry** tab and then click on the *Payroll Agent* name to configure the agent.
6. From the agent's profile view, click **Configure Agent**.
7. In the **Status** column, make each relevant skill available by enabling the toggle slider.
8. For each enabled **Skill**, populate the **Available To** prompt with the security groups that you want to provide access to for that specific skill. The security groups added to the **Available To** prompt for an agent establish the agent’s interaction policy.

   Note: The security groups you select in the **Available To** prompt must also have permissions to the domain or business process security policies that secure the Payroll agent's tools. You can use the **View Security for Agent Skill** report to assist with your agent security configurations. This report shows you detailed information about the Payroll agent’s Tools APIs and the respective domain or business process security policies and permissions. At agent runtime, Workday evaluates both user access to the agent and the user access to the APIs the agent is executing as tools.
9. Click **Activate**. You can also optionally save and return to this configuration.

   Agent configuration can be updated at any time. When you activate the Payroll agent, the ASU for the agent also activates automatically.

Result

You can access Workday Chat to use the Payroll agent.

Next Steps

(Optional) Set up the additional configuration for the:

- Notifications to workers missing payment elections for the Identify Missing Data and Configuration skill.
- Minimum Wage Analysis skill.

(Optional) When you are done with the Payroll agent, you can click **Deactivate** to turn it off. You can activate, deactivate and reactivate the Payroll agent at any time in the **Agent Management Hub**. When you deactivate an agent, the ASU for the agent also deactivates automatically.

Related Information
Examples
Payroll Agent Factsheet

Concept: Payroll Agent

Overview

The Payroll agent is an AI-powered conversational assistant designed to improve the payroll practitioner experience within Workday.

Payroll agent skills include:

- Core Payroll Data Retrieval: Enables the agent to retrieve basic information about workers, pay groups, companies, and more.

  Note: This skill is required for the operation of other skills.
- Payroll Data Insights: Provides access to payroll knowledge and performs actions for users, involving human intervention when necessary.
- Identify Missing Data and Configuration: Monitors system to to find missing or outdated critical payroll data that requires intervening action from a payroll practitioner.
- Minimum Wage Analysis: Analyzes the impacts of minimum wage rate changes for states in the U.S. and provinces in Canada.

Note: We recommend that you establish best practices for reviewing, editing, and verifying the accuracy of AI-generated content before use.

The Payroll agent is available to all Workday Payroll countries:

- Payroll for Australia
- Payroll for Canada
- Payroll for France
- Payroll for Ireland
- Payroll for the UK
- Payroll for the U.S.

Limitations

The Payroll agent:

- Uses conversational AI, an evolving technology. Although built and tested for high accuracy, it can occasionally misinterpret questions or present unexpected results. Always review the output, including numbers and commentary. Before acting on the results, verify them against the source of truth.
- Only supports U.S. English.
- Only remembers 20 interactions in a sequence.

Proxy sessions exclude the Payroll agent's functionality.

Some functionalities for the agent's skills are only applicable to specific countries. Example: You can only use the Identify Missing Data and Configuration skill to find and update expiring FLSA worker period calendars for Payroll for the U.S.

You may:

- Experience a momentary delay in the agent's response.
- Receive responses from the agent for questions unrelated to the Payroll agent's skills.

Set Up Identify Missing Data and Configuration Notifications for Workers Missing Payment Elections

Prerequisites

Security:*Worker Data: Payroll (Payment Elections)* domain in the Core Payroll functional area.

Context

When you set up the Payroll agent, you can immediately use the Identify Missing Data and Configuration skill in Workday Chat.

By default, workers missing payment elections receive a notification based on the parent notification type settings configured on the **Payroll** tab of the **Edit Tenant Setup - Notifications** task. See Reference: Edit Tenant Setup - Notifications.

Workday automatically sends an inbox notification to workers missing payment elections when you initiate the Find Workers Missing Payment Elections job using the Identify Missing Data and Configuration skill.

You can also:

- Configure a delivery override for Workday to additionally deliver email notifications to workers missing payment elections.
- Customize the content of the email notifications that workers receive.

If you want to notify workers with email notifications, you must configure the delivery override before you use the Identify Missing Data and Configuration skill.

Steps

1. Configure a delivery override for emails notifications to workers missing payment elections.
    a) Access the **Edit Tenant Setup - Notifications** task.
    b) In the **Notification Delivery Settings** section, select the **Payroll** tab.
    c) In the **Notification Type** column, select *Missing Payment Elections*.
    d) Select the **Override Parent Notification Type Settings** check box.
    e) From the **Rule** prompt, select *Create Notification Routing Rule*.
    f) Complete the **Create Notification Routing Rule** section:

Option	Description
Notification Type Usage	Select *Missing Payment Elections*.
Channel Frequencies	Click **Add**.
Channel	Select *Email*.
Default Frequency	Select *Immediately*.

    g) Click **OK**.

    Security: *Set Up: Tenant Setup - BP and Notifications* domain in the System functional area.

2. View the default email template for notifications sent to workers missing payment elections to verify if you want to make any changes.
    a) Access the **Email Template Behaviors** report.
    b) Select the **Email Template Behavior** column title.
    c) From the **Value** prompt, select *Missing Payment Elections Email* .
    d) Click **Filter**.
    e) Select the *Missing Payment Elections Email* **Email Template Behavior** to view email template behavior.
3. Edit the default email template for notifications sent to workers missing payment elections.
    a) Access the **Create Email Template** task.
    b) Complete the **Create Email Template** section:

Option	Description
Email Template Behavior	Select *Missing Payment Elections Email*.

    c) Click **OK**.
    d) Click the **Add row** icon to add these rows to the grid:

Order	Description
1	1. Select **Static Content**. 2. From the **Static Content** prompt, select *Create Static Email Text*. 3. In the **Text** field, enter the content you want to display as the header of the notification.
2	1. Select **Static Content**. 2. From the **Static Content** prompt, select *Create Static Email Text*. 3. In the **Text** field, enter the content you want to display as the body of the notification.
3	1. Select **Dynamic Content**. 2. From the **Dynamic Static Content** prompt, select *Actionable Link*.

    e) Click **OK** and **Done**.

    Security: *Set Up: System* in the System functional area.
4. Verify that the custom email template you created is now active.
    a) Access the **Maintain Email Templates** task.
    b) In the **Missing Payment Elections Email** row, confirm the **Active** check box is selected for your custom email template.
    c) Click **OK**.

    Security: *Set Up: System* in the System functional area.

Result

After you configure your email notifications:

- Workers missing payment elections receive both notifications in their Workday Inbox and email inbox if they set up their email address in Workday.

- The notifications that workers receive contain your customized content.

Set Up Minimum Wage Analysis Skill

Prerequisites

Security:

- *Set Up: Minimum Wage Agent* domain in these functional areas:
  - CAN Payroll
  - USA Payroll
- *Set Up: Payroll (Minimum Wages View) - CAN* domain in the CAN Payroll functional area.
- *Set Up: Payroll (Minimum Wages View) - USA* domain in the USA Payroll functional area.
- *Set Up: Payroll (Taxes View)* domain in the Core Payroll functional area.

Context

You can use the Payroll agent to analyze new minimum wage rates in American states and Canadian provinces. To use the Minimum Wage Analysis skill, you must configure your tenant according to these steps so payroll administrators have the necessary permissions to access relevant payroll data.

We recommend that you establish best practices for reviewing, editing, and verifying the accuracy of AI-generated content before use.

Steps

1. Enable the *Set Up: Minimum Wage Agent* domain.
   a) Access the **View Domain** report.
   b) From the **Domain** prompt, select *Set Up: Minimum Wage Agent*.
   c) Next to **Domain Security Policy**, click the magnifying glass icon.
   d) In the **Report/Task Permissions**, verify that the security groups have *View* and *Modify* access.
   e) (Optional) Click **Edit Permissions**.

      Edit security groups and select the *View* and *Modify* check boxes as needed.
   f) Click **OK** and **Done**.
   g) (Optional) Activate Pending Security Policy Changes.

   Security: *Security Configuration* domain in the System functional area.
2. Enable the Minimum Wage Background Scheduler.
   a) Access the **Edit Tenant Setup - Payroll** task.
   b) In the **Tax Elections/Taxes** section, select the **Minimum Wage Background Scheduler** check box.
   c) Click **OK** and **Done**.

   When you enable the Minimum Wage Background Scheduler:

   - The Payroll agent only displays the estimated employer costs of changed minimum wage rates for payroll administrators to view in Workday Chat after 01:00 Pacific Standard Time (PST) the next day.
   - The calculations for the estimated employer costs only include impacted workers who have an hourly plan assignment that enforces minimum wage.

   Security: *Set Up: Tenant Setup - Payroll* domain in the System functional area.

Result

In Workday Chat:

- You can enter a query in related to new minimum wage rates.
- The Payroll agent generates analysis on how new minimum wage rates impact employer costs.

Concept: Identify Missing Data and Configuration Skill

Overview

The Identify Missing Data and Configuration skill of the Payroll agent helps you:

- Streamline payroll processing by finding what data and configurations require your attention.
- Take action to proactively resolve potential issues.

This skill enables you to:

- Monitor and identify outdated or missing data and configurations that are critical for payroll.
- Take actions to resolve data and configuration issues such as sending notifications and making updates.

You can use this skill to find and:

- Notify workers who are missing payment elections for pay types using the Payroll Rule on the **Maintain Payment Election Rules** task. This functionality is applicable for all Workday Payroll countries.
- Update FLSA calendars that are set to expire within 90 days of the current date. This functionality is only applicable for Payroll in the U.S.

How to Access

Before accessing the Payroll agent in your tenant, you must have:

- Payment elections for workers. See Steps: Set Up Payment Elections.
- FLSA work period calendars. See Create FLSA Work Period Calendars (USA).

You also must have access to specific security domains to use different functionalities of the skill:

Domain	Functionality
Worker Data: Payroll (Payment Elections) domain in the Core Payroll functional area	Find and notify workers missing payment elections
Set Up: Payroll (FLSA) - USA domain in the USA Payroll functional area	Find and update expiring FLSA work period calendars

To use the Identify Missing Data and Configuration skill:

1. Once you've set up the Payroll agent and you're in the assigned security group, you can then click the speech bubble from the top navigation bar to launch Workday Chat.
2. Enter a query related to finding and:
    - Notifying workers missing payment elections.
    - Updating expiring FLSA calendars.

Notifications for Workers Missing Payment Elections

You can initiate the Find Workers Missing Payment Elections job using the Identify Missing Data and Configuration skill.

To configure how Workday notifies workers about missing payment elections, see Set Up Identify Missing Data and Configuration Notifications for Workers Missing Payment Elections .

When you find workers missing payment elections using the Payroll agent, Workday automatically notifies you with a notification on the bell icon once the process is complete.

The notification that you receive includes details such as:

- The related pay group of the workers.
- The workers who are missing payment elections.
- Whether or not Workday notified the workers identified by the Payroll agent.

Notifications for Expiring FLSA Calendars

You can initiate the Schedule FLSA Work Period Calendar Update job using the Identify Missing Data and Configuration skill.

When you update an expiring FLSA calendar using the Payroll agent, Workday automatically notifies you with a notification on the bell icon once the process is complete.

The notification that you receive includes details such as the:

- Name of the updated FLSA work period calendar.
- Number of work periods that you requested to be added.

Example Queries for Identify Missing Data and Configuration

- I need to find and take action on missing data and set ups related to payroll. What can you help me with?
- Identify and update expiring FLSA work calendars.
- Find and notify workers missing payment elections.

Concept: Minimum Wage Analysis Skill

Overview

The Minimum Wage Analysis skill of the Payroll agent helps provide you with contextual data analysis and insights related to minimum wage rates and costs.

When you query the Payroll agent, Workday uses AI to generate analysis on the estimated employer costs and number of impacted employees from new minimum wage rates in the U.S. and Canada.

This skill enables you to review and analyze the impact of minimum wage rates changed within the past 6 months or up to 6 months in the future. Your query results are the latest minimum wage changes for a given tax authority, effective 6 months before or after today's date.

For tax authorities with more than 1 minimum wage compliance update in that time frame, you receive the latest compliance update information in your results. Example: California has two minimum wage updates, effective 02/01/2026 and 04/01/2026. The 04/01/2026 minimum wage update is the latest update so is used when calculating employer costs.

This skill is only applicable for:

- Payroll for the U.S.
- Payroll for Canada

How to Access

Before you can access this skill, you must configure the necessary data and permissions. See Set Up Minimum Wage Analysis Skill .

Access Workday Chat from your homepage and enter a query related to minimum wage rates.

Limitations

You can only use the Minimum Wage Analysis skill to analyze new minimum wage rates for American states and Canadian provinces.

Example Queries

- What is the minimum wage for this state or province?
- What is the minimum wage rate for this state or province on this date?
- How many workers are affected by the minimum wage change?
- Show me how this minimum wage rate will affect my overall employer costs.

Concept: Payroll Data Insights Skill

Overview

The Payroll Data Insights skill of the Payroll agent enables you to access payroll knowledge to answer your questions. You can ask questions and receive answers on the data that you need in a simple conversational manner. This reduces your manual effort and the time you spend on generating reports, potentially eliminating the need for creating some custom reports by providing you with the data directly.

Example: For an audit, a payroll administrator needs a specific data point. Instead of running multiple reports, they can ask a question in natural language, such as, " *Show me every pay group in the system that’s on a weekly or bi-weekly basis*." They can also ask follow-up questions such as “ *Show me every worker in [returned in weekly pay group1] that made more than $4000 gross for the last completed pay period*." The agent then provides the data on screen. It includes insights and analysis in natural language, along with displaying the data in an intuitive manner.

How To Access

Once you’ve set up the Payroll agent and you're in the assigned security group, you can then click the speech bubble from the top navigation bar to launch Workday Chat.

Limitations

Currently, the Payroll Data Insights skill can answer these type of questions:

Question Types	Examples
Averages	What was the average gross pay for workers in [pay group] over the last 3 periods?
Basic Worker Pay	What was [worker names] [gross or net pay] last period?
Basic Pay Group Pay	Show me every worker in [pay group] that made more than [amount] in [month]?
Basic Pay Group Information	Which pay groups are paid on a monthly schedule?
Earning or Deduction Inclusion	List all the earnings and deductions with current values.
Earning or Deduction Exclusion	Which workers in [pay group] did not have [some earning/deduction] in their last period?
Period Comparison	Compare the gross pay of [pay group name] last Q1 2025 vs Q1 2026.

FAQ: Payroll Agent

Does the Payroll agent respect security?	Yes, the Payroll agent respects existing security for payroll.
Why can't I see the Agent Management Hub?	You must verify that the:

	• Agent System of Record functional area is set up and enabled. • Appropriate users are in the correct security domain to access the Agent Management Hub.
What kinds of questions can the Payroll agent answer?	See these topics for further information on which questions the Payroll agent can help you with, depending on the skill you want to use: • Concept: Payroll Data Insights Skill • Concept: Identify Missing Data and Configuration Skill • Concept: Minimum Wage Analysis Skill
The Payroll agent seems to get hung up on something from earlier in the chat. What can I do?	You can try asking the question in a different way or starting a new thread.
Why is the Payroll agent not answering questions related compensation plans, cost centers, or specific payroll calculations like overtime?	The Payroll agent currently can only review and answer questions related to: • Payroll results • Result lines • Basic worker information • Pay group information

Sana Self-Service Agent

Set Up Self-Service Agent

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

Note: We recommend that you opt in to the **People Experience** > **Help** service on the **Innovation Services And Data Selection Opt-In** report before you sign the UMSA or change your data hosting region. This prevents a 14 day waiting period limitation for Self-Service Agent to ingest your policy documents.

Set Up Agent System of Record.

Context

You can register, configure, and activate the Self-Service Agent using the **Agent Management Hub**.

The Self-Service Agent is a conversational AI agent that retrieves and summarizes broad self-service data and takes action on common interactions. Those actions, called skills, are common tasks that employees perform, such as submitting support requests and viewing absence information. You can specify which Self-Service Agent skills are available and to which security groups, enabling you to provide the appropriate level of actions to the right employees.

Note: While you can override the default skill configurations, you must keep the **Guide** skill as always active because this is the core skill the agent is required to run on.

Steps

1. Access the **Agent Management Hub** report.
2. Select the **Unregistered Workday Agent** tab.
3. For the **Self-Service Agent**, click **Register**.
4. Select the **Confirm** check box, and then click **OK** to complete the registration.

   Workday moves the **Self-Service Agent** to the **Agent Registry** tab.
5. Select the **Agent Registry** tab and then click on the *Self-Service Agent* name to configure the agent.
6. From the agent's profile view, click **Configure Agent**.
7. From the **Status** column, make each relevant skill available by enabling the toggle slider.
8. For each available **Skill**, populate the **Available To** prompt with the security groups that you want to provide access to for that specific skill.

   Example: For the **ESS - Human Capital Management - Base** skill, you might want to keep the default *Employee As Self* security group selected to provide all employees access to this skill while for the **MSS - Human Capital Management - Base** skill, you might select the *Manager* and *Management Chain* security groups to only provide managers in a management chain access to the skill.

   Note:

   Workday evaluates both user access to the agent and the user access to the APIs the agent is executing as tools at runtime. Access the **View Security for Agent Skill** report to view which security policies must be configured for a given security group for a tool to function.
9. Click **Activate**.

Result

- Workday displays the Workday Chat icon in the global navigation for you and your employees.
- Employees that have access to the security groups you specified for each skill and the domain or business process security policy associated with the tools that make up each skill can use the Self-Service Agent.
- Workday hides the Workday Assistant chat bubble to reduce duplication.

Related Information
Examples
Workday Community: Self-Service Agent AI Fact Sheet

Configure a Custom Fallback Message for Self-Service Agent

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

Note: We recommend that you opt in to the **People Experience** > **Help** service on the **Innovation Services And Data Selection Opt-In** report before you sign the UMSA or change your data hosting region. This prevents a 14 day waiting period limitation for Self-Service Agent to ingest your policy documents.

Set Up Agent System of Record.

Context

As you configure the Self-Service Agent, you can set a custom message that displays for users when they encounter an issue with their self-service request. Although you configure the message on the Guide skill, the message applies to all skills across the entire agent.

Steps

1. Access the **Agent Management Hub** report.
2. Select the **Unregistered Workday Agent** tab.
3. For the **Self-Service Agent**, click **Register**.
4. Select the **Confirm** check box, and then click **OK** to complete the registration.

   Workday moves the **Self-Service Agent** to the **Agent Registry** tab.
5. Select the **Agent Registry** tab and then click on the *Self-Service Agent* name to configure the agent.
6. From the agent's profile view, click **Configure Agent**.
7. On the Guide skill, click **Create Fallback Message**. As you configure the custom fallback message, consider:

Option	Description
Fallback Message	Enter the message that you want to display for users when they encounter an issue.

Option	Description
Link Text	If you want to include a link with the fallback message, specify the link text here.
Link URL	If you want to include a link with the fallback message, specify the link URL here.

Note: Although you configure the message on the Guide skill, the message applies to all skills across the entire agent.

8. Click **OK** to save the message.

   Click **Save** to finish configuring the Self-Service Agent.

Result

The custom fallback message will display for users if they encounter an issue with their self-service request.

About Self-Service Agent

The Self-Service Agent is a conversational AI agent that retrieves and summarizes broad self-service data and takes action on common interactions, such as:

- Updating personal information and requesting time off.
- Managing organizational goals and viewing team learning statuses.
- Viewing organization policy information from knowledge articles stored in Workday.

When you activate the Self-Service Agent and enable at least 1 skill, Workday displays the Workday Chat bubble at the top of your tenant and hides the Workday Assistant chat bubble to reduce duplication. When you activate another agent, such as the Payroll Agent, but not Self-Service Agent, you might see 2 chat bubble icons (Workday Assistant and Workday Chat) in your Workday tenant.

Skills and Tools

Workday uses the term *skill* to refer to specific actions or tasks that an agent can take. Each skill is further made up of *tools*, which agents use when executing skills. Tools are an abstraction layer (facade) over Workday APIs that the agent calls to perform tasks.

The Self-Service Agent skills span varying levels of complexity and intended audiences. Workday makes this distinction in the skill name itself by including these prefixes and suffixes:

- ESS (employee self-service). Skills specifically designed for all employee types.
- MSS (manager self-service). Skills specifically designed for managers.
- Advanced. Complex action skills.
- Base. Simple action skills.

While most Self-Service Agent skills are specifically designed for ESS or MSS roles, you have the ability to make any skill available to any security group, so long as you ensure that the security group has the appropriate access to the underlying APIs that power the tools within a skill.

Example: When you want to make the **MSS - Payroll - Advanced** skill available to the **Management Chain** security group, you must ensure the the **Management Chain** security group has access to the domains that the request_payroll_input tool is secured to.

Use the:

- **Agent Management Hub** to view the descriptions of each Self-Service Agent skill and which tools are associated with each skill.
- **View Security for Agent Skill** report to view the required and recommended security policies that must be configured for each tool.

Limitations

Self-Service Agent currently doesn't support:

- File uploads.
- Contingent workers.
- The ability to hide or require fields using the Configure Optional Fields task.
- Custom labels (tokenization).
- Additional jobs (multi-position).
- Usage with implementer and proxy accounts.
- User preferences indicated in profiles, such as locale.
- Delegated actions. While actions initiated by a delegate through Self-Service Agent might initially appear successful in the chat window, they won't create actual events or requests in the system. When you perform an action in Self-Service Agent and specify that you're acting on behalf of someone else, the agent explicitly states that the action can't be performed.
- Data extractions from articles in Sandbox. We recommend using IMPL tenants instead for test cases related to this.
- Reading document attachments on help articles.

Self-Service agent uses a non-deterministic LLM model which might produce slight grammatical and syntactical variations in responses. Additionally, Self-Service agent's reasoning and responses are updated continuously over time, which might results in slightly differing interactions as the agent improves week over week.

If a skill or tool involves tenant access restrictions, such as multi-factor authentication (MFA), ensure that any security groups that you assign to that skill or tool on the Available To column of the **Configure Agent** task are also set up for those same tenant access restrictions so that they are enforced appropriately.

We recommend that you opt in to the **People Experience** > **Help** service on the **Innovation Services And Data Selection Opt-In** report before you sign the UMSA or change your data hosting region. This prevents a 14 day waiting period limitation for Self-Service Agent to ingest your policy documents.

Language Support

The Self-Service Agent is optimized and validated for:

- English
- French
- French-Canadian
- German
- Japanese

While the underlying LLM can communicate in over 30 additional languages and thus, you might interact with the Agent in these languages, Workday doesn't support the same level of verified accuracy or stylistic consistency (such as formal vs. casual phrasing) provided for its officially supported languages.

Note:

Currently, the Policy Intelligence skill only supports English and French-Canadian. We plan to support additional languages for the Policy Intelligence skill in the future.

Workforce & Frontline Management Skills

Overview and Purpose

Frontline workers and managers often use manual processes to manage worker time and payments. These workflows can be time-consuming and open to user error, requiring repetitive actions for tasks such as approving worker time. The Workforce & Frontline Management skills of the Self-Service Agent enable users to manage these tasks more efficiently through natural conversational language.

MSS - Workforce & Frontline Management Skills

MSS - Workforce & Frontline Management skills enable managers and time approvers to access information by worker:

- Location.
- Name.
- Supervisory organization.

MSS - Workforce & Frontline Management Skills - Base

The MSS - Workforce & Frontline Management - Base skill enables managers and time approvers to view details about their direct reports using AI. They can retrieve information about:

- Entered and submitted time.
- Time off events.
- Totals.
- Validations.

MSS - Workforce & Frontline Management Skills - Advanced

The MSS - Workforce & Frontline Management - Advanced skill enables managers and time approvers to approve, send back, or deny time in bulk or individually for their direct reports using AI.

ESS - Workforce & Frontline Management Skills - Base

The ESS - Workforce & Frontline Management - Base skill enables workers to view information about their:

- Company holidays.
- Entered and submitted time.
- Time off balances and events.

ESS - Workforce & Frontline Management Skills - Advanced

The ESS - Workforce & Frontline Management - Advanced skill enables workers to:

- Check in and out of shifts.
- Enter and submit time.
- Submit time off requests.

Asking Questions

In Workday Chat, managers and timekeepers can use prompts such as:

- Check all timesheets that are ready for approval.
- How many hours did Ben Adams work on Friday?
- Send back to Abby with a comment asking her to verify she worked on New Year's.
- Show me the details of time worked by Todd this week.
- What time blocks does Peter have from 12/01-12/04?

Workers can use prompts such as:

- How many days of time off will I have by the end of this year?
- How many hours did I work last week?
- How many sick days do I have left?
- Submit a time off request for the week of Labor Day.
- What are the dates of company holidays for this year?

The accuracy and relevance of the response depends on the quality of the prompts. Clear and straightforward prompts give better results.

Providing Feedback

Currently these skills don't leverage feedback other than by telling the agent to retry if it's inaccurate or to check its work or assumptions. Example: It mistakes today for Monday when today is actually Tuesday.

To provide feedback on the quality of your interactions, click the thumbs up or thumbs down icon. If you click thumbs down, you must provide details. You can either:

- Select from options we provide or select **Something else** to type in your own feedback. When done, click **Submit**.
- Cancel out at any point by clicking the X. We'll still capture your thumbs down selection.

You only see the options for additional feedback on the last response in the chat. If you scroll back up and click thumbs down then you don't get these options.

Limitations

- These skills can misinterpret questions or present unexpected results. Always review the output to ensure the quality of the content.
- When you navigate to a different location or the session ends, we start a new conversation. You can revisit the prior thread from the chat history.
- For specific limitations of the tools that make up these skills, see Self-Service Agent Tools .

Self-Service Agent Skills

A Self-Service Agent skill refers to specific actions or tasks that an agent can take. You can specify which actions or tasks you want the Self-Service Agent to be able to perform by setting each skill as either active or inactive.

Note: The **Guide** skill must be set as active for the Self-Service Agent to run.

This topic contains Self-Service Agent skill names and general descriptions. You can also view this information directly in Workday when you configure an agent in the **Agent Management Hub**.

Skill and tool configuration changes can take up to 10 minutes to take effect for Self-Service agent due to caching.

Skill	Description
ESS - Help - Advanced Skill	Facilitates the action of submitting support requests, enabling employees to move beyond information gathering to active assistance.
ESS - Human Capital Management - Advanced	Enables employees to use Self-Service Agent to take actions related to their workforce lifecycle by updating personal data and requesting reference letters.
ESS - Human Capital Management - Base	Enables the Self-Service Agent to process requests from employees related to retrieving personal information for core HCM functions including worker profiles, compensation and benefits details, and team information.
ESS - Payroll - Base	Enables the Self-Service Agent to process requests from employees related to compensation, payment, and tax forms.
ESS - Talent Management - Advanced	Enables employees to use Self-Service Agent to take actions related to complex workforce tasks, such as submitting performance reviews and creating referrals.

Skill	Description
ESS - Talent Management - Base	Provides the Self-Service Agent with the ability to retrieve information related to employee professional development, including goals, feedback history, and internal job listings.
ESS - Workforce & Frontline Management - Advanced	Enables employees to use Self-Service Agent to take actions related to complex workforce tasks, such as submitting time-off requests, checking in/out of shifts, entering time blocks and submitting time.
ESS - Workforce & Frontline Management - Base	Provides the Self-Service Agent with the ability to retrieve their time tracking, scheduling, and absence information. This skill handles inquiries such as checking time-off balances and viewing Workday Scheduling schedules.
Guide	Provides intelligent navigational direction, ensuring task completion by directing users to the specific Workday report or task required.
MSS - Human Capital Management - Base	Enables the Self-Service Agent to process requests from managers related to retrieving essential team information, including team structures, work history, and direct report information.
MSS - Payroll - Advanced	Enables the Self-Service Agent to process requests from managers related to initiating financial actions, such as requesting payroll inputs. The skill: • Calls the existing Request Payroll Inputs business process. • Uses your existing payroll and security configuration. • Respects the pay component security segment and domain security that you configure on the Self-Service Agent. The skill focuses on Workday Payroll workers and enforces these key rules: • Creates payroll inputs only for workers on Workday Payroll. When the worker's primary position is in an external pay group, or the worker has no pay group, the skill blocks the request and returns a message that the worker isn't available for payroll input requests. • For multi-job workers, when a manager requests a position-based input without specifying a position, the skill defaults the input to the worker's primary position effective on the input start date.

Skill	Description
MSS - Talent Management - Advanced	Enables the Self-Service Agent to support managers in driving the performance cycle and take actions such as conducting reviews, changing talent data, and executing team development transactions.
MSS - Talent Management - Base	Enables the Self-Service Agent to support managers in overseeing the development of their team by retrieving goal progress, viewing learning statuses and reviewing team feedback.
MSS - Workforce & Frontline Management - Advanced	Enables the Self-Service Agent to process requests from managers related to approving, sending back, or denying submitted time entries.
MSS - Workforce & Frontline Management - Base	Enables the Self-Service Agent to process requests from managers related to retrieving information on team operations, including direct reports' time-off requests, time blocks, and submitted time entries.
Policy Intelligence	Provides the Self-Service Agent with capabilities related to resolving questions about company rules by searching authorized documentation. The skill retrieves specific details from policy documents and procedural guides to ensure responses are compliant and up-to-date. Note: Currently, the Policy Intelligence skill only supports English and French-Canadian. We plan to support additional languages for the Policy Intelligence skill in the future.

Self-Service Agent Tools

Each Self-Service Agent skill is made up of different actions a user can take, called tools. Tools are an abstraction layer (facade) over Workday APIs that the agent calls to perform tasks.

This topic contains Self-Service Agent tool names, descriptions, and limitations, grouped by the skill they're associated. You can also view this information - along with security requirements for each tool - directly in Workday by accessing the **View Security for Agent Skill** report.

Skill and tool configuration changes can take up to 10 minutes to take effect for Self-Service agent due to caching.

ESS - Help - Advanced

Tool	Description	Limitations
create_a_case	Enables users to initiate and submit formal support requests to ensure complex issues are documented and routed correctly for resolution.	

ESS - Human Capital Management - Advanced

Tool	Description	Limitations
change_home_contact_info	Enables users to update their home address and personal phone number(s) in Workday. Supports custom validations.	Doesn't support file uploads. Managers can't update home contact info on behalf of direct reports.
change_marital_status	Guides a user through updating their marital status in three sequential steps: initiation, draft creation, and submission. Supports custom validations.	This tool is for status changes, not read-only profile questions. Doesn't support removing or clearing a marital status. The change might enter an approval workflow and return a pending status until fully effective.
change_name	Enables a user to update their legal name and/or preferred name in Workday only. Supports custom validations.	Other name components, such as social name and former name, aren't supported. Doesn't support file uploads such as legal name change certificates. Doesn't support the effective date of a legal name.
request_reference_letter	Initiates a request for a standard employment verification or reference letter for the current user based on data on file in Workday.	Managers can't initiate reference letter requests for direct reports. Doesn't support custom language, non-standard fields, client-specific formatting, or custom validations.

ESS - Human Capital Management - Base

Tool	Description	Limitations
view_bonus_history	Retrieves historical data for bonuses and one-time payments, such as spot bonuses and gift cards, for the user. Provides payment amounts, currency, effective or scheduled dates, plan names, bonus percentages, and the formal reason for the payment. Supports queries for the most recent payment, a specific calendar year’s history, or a summary of the three most recent events. Automatically retrieves all records if multiple	Doesn’t display clawbacks, non-bonus plan types, or future/ projected payments.

Tool	Description	Limitations
	payments occur on the same date.	
view_coworker_info	Searches for a coworker by name and/or worker ID to retrieve professional information such as title, manager, location, and, where permitted by the user's security access, personal contact fields such as home email and home phone. Retrieves 1 profile for each call.	The fields that the agent returns depend on the session user's security access. For example, **Home Email** and **Home Phone** fields are returned only when the user has access to those fields. Doesn't return sensitive personal fields, such as home addresses. Ambiguous names with multiple matches requires user clarification. Doesn't support bulk or list lookups.
view_dependents	Retrieves a list of all active dependents for the user, including the dependent's name, relationship type, date of birth, age, gender, and tobacco status.	
view_healthcare_elections	Displays active healthcare enrollment offerings and elections information for the user and their dependents, such as plan name, provider, coverage target, costs per frequency, available level options, and external provider URLs.	Only retrieves Healthcare and Retirement Benefits, not additional benefits such as insurance benefits.
view_my_team	Retrieves the list of users on the current session user's my-team list, including display names and headcount. This tool retrieves peers under the same manager, not the user's direct reports.	Detailed profile information such as title or contact details is not included; use view_coworker_info for individual details. Displays an empty team list when the manager has no other direct reports .
view_org_info	Retrieves organization records for organizations the user belongs to or from a specific name search. Results include organization identifiers, status, and location fields.	Retrieves org-level metadata rather than a member roster; use view_my_team or view_direct_reports for people-level queries. Location and address fields are retrieved as stored in Workday

Tool	Description	Limitations
		with no locale transformation applied.
view_personal_info	Retrieves personal information details from the session user's personal and employment profile. Not all profile fields are supported even if they exist. This tool retrieves data for the authenticated session user only; use view_coworker_info for other workers. It uses a read-only GraphQL API with no write capabilities.	Doesn't retrieve fields such as emergency contacts or custom profile. Date formats and field labels are retrieved as stored in Workday with no locale-based transformation applied.
view_retirement_savings	Retrieves the user's active retirement savings plan details, including plan name, coverage type, and frequency. Retrieves contribution rates for both employees and employers, including minimums and maximums, as well as beneficiary allocations such as names and percentages.	
view_total_compensation	Retrieves the user's total base pay, total compensation, pay frequency, and compensation grade, pay range details, and a summary of all stock grants grouped by type and the associated vesting schedule.	Doesn't predict future stock vesting dates or format step progression details beyond the provided string.

ESS - Payroll - Base

Tool	Description	Limitations
model_my_pay	Enables hourly workers to model and plan for possible pay change scenarios. Example prompts: • *What if I made x an hour?* • *What is my gross pay if I made x an hour?* • *What is my net pay if I made x an hour?* • *What are my taxes if I made x an hour?* • *What are my pre-tax deductions if I make x an hour?* Retrieves hourly payroll result lines if the pay component	You must configure pay modeling in your tenant. See Set Up Pay Modeling. Workers must have at least 1 completed pay period with hourly pay to prompt the agent successfully.

Tool	Description	Limitations
	includes *rate* and *hour* pay component related calculations.	
view_direct_deposit	Retrieves user's bank accounts and direct deposit information used in payment elections, including the default country and currency.	Doesn't provide information about payment elections that aren't associated with a bank account.
view_next_paydate	Retrieves the next payroll payment date for on-cycle payments for a user's primary pay group.	Available only for Australia, Canada, France, Ireland, UK, and USA. Additional configuration is required for workers assigned to a Payroll Interface pay group.
view_payslips	Retrieves either the user's latest payslip or payslips filtered by dates. Includes information such as payment date, period dates, gross, net, and YTD aggregated values. Available for Australia, Canada, France, Ireland, UK, and USA, as well as external payslips.	Doesn't support custom labels, line-item details, such as 401K, or net-zero payslips. Doesn't acknowledge the **Disable Payslip Viewing (Online Version)** check box election on the **Edit Tenant Setup – Payroll** task. External payslips only provides gross and net data.
view_w2	Enables a user to view information about their most recent US Wage and Tax Statement (Form W-2). Information is limited to the most recent year and the most recently generated company W-2.	Doesn't retrieve individual W-2 box information.
view_w4	Enables a user to view the details of their US federal tax withholding election (Form W-4) for a specified date. When no date is specified, the tool returns details about the most recent election that has an associated Effective Date.	

ESS - Talent Management - Advanced

Tool	Description	Limitations
create_referral	Enables users to submit a referral for an external candidate to 1 or more job requisitions using job requisition IDs such as candidate's name, country, contact details, optional	Doesn't support resume or file uploads. Doesn't display referral status after submission.

Tool	Description	Limitations
	address, and notes. The specified job requisition ID must be for an active, non-confidential job requisition posted externally.	Doesn't support custom validations. Submission might fail when referral consent for certain candidate countries is missing.
distribute_journey	Enables employees to distribute journeys themselves.	
start_performance_review_self	Initiates a self-performance review by resolving the appropriate category and template and prompting the user for a choice when necessary. Supports custom validations.	Once the review is initiated and inputs are validated, any further interactions must be completed through the Workday UI.
request_feedback_self	Enables users to request feedback from other users by selecting specific feedback templates and determine whether the responses should be private to them or visible to others.	

ESS - Talent Management - Base

Tool	Description	Limitations
find_jobs	Enables users to search approved internal job postings using structured filters such as location, skills, manager, or job requisition ID.	Does not support free-form keyword search or infer a coworker’s role to find similar jobs. Results are retrieved in pages with a limited count per response.
find_journeys	Enables users to search, filter, and retrieve available journeys. This tool displays details for self-service and distributed journeys, and provides specific journeys details when prompted.	
view_feedback	Displays feedback the user has received (both unsolicited anytime and requested) along with the status of pending requests. Includes the date, the provider, and the feedback content with options to filter by date or person. Managers can also view a summary count of feedback requests for their direct reports.	

Tool	Description	Limitations
view_my_goals	Retrieves personal goals including status, due date, and organization alignment.	Doesn't support date range filtering or fields such as Target Amount, Milestones, and Cascaded Goals.
view_org_goals	Retrieves an organization's goals for a specified date range, defaulting to the current user's primary-job supervisory organization. Provides goal names, descriptions, completion percentages (0–100), and parent goal references.	Limited to active supervisory organizations. Doesn't support searching by name or description.
view_performance_review	Retrieves the user's completed or in-progress performance reviews. Only retrieves overall ratings for managers and employees for each section. Users can filter the list by status.	Doesn't display the manager or employee's overall comments. Only retrieves overall ratings for managers and employees for each section.
view_talent_profile_details	Retrieves specific talent profile sections, such as job history, skills, and education for the current user or another worker by their name or ID.	

ESS - Workforce & Frontline Management - Advanced

Tool	Description	Limitations
cancel_time_off	Initiates the *Correct Time Off* business process to cancel or delete an approved time off entry. Also supports the cancelation of in-progress time off request and correction events.	
edit_time_off	Initiates the *Correct Time Off* business process to edit an approved time off entry. Supports modifications to quantity, start and end times, and reasons for both standard time off and absence tables. Supports custom validations.	Doesn't support corrections to the time off type, position, or worktags, and it doesn't display system warnings.
enter_time_block	Enables a user to create time entries for 1 or more days using quantity-based entries (# of hours) or in/out time-based entries (specific times of day).	Doesn't support worktag entry or project-based time entry codes. Doesn't support time blocks requiring worktag selection,

Tool	Description	Limitations
		such as cost center, location, or division.
request_time_off	Initiates a time off request, such as vacation and sick leave, using the *Request Time Off* business process. Supports custom validations.	Doesn't support requests with worktags configured, system warnings or start/end times.
shift_check_in	Enables a user to clock in at the beginning of their shift to start recording worked time. The tool automaticallt resolves available time entry codes and positions.	Doesn't support worktag entry or project-based time entry codes; users requiring worktags can't complete check-in through this tool.
shift_check_out	Enables a user to clock out of their shift, either for a break or for the end of their shift, to stop recording their worked time.	
submit_time	Submits a user's timesheet for review and approval for a single date. Includes all time entries for the full time period the date falls within. For example, any date within a weekly pay period will submit the entire week.	Doesn't support custom validations.
update_time_block_comment	Adds or updates a comment associated with a specific time block.	Doesn't support editing any other fields on the time block, such as time type or quantity.

ESS - Workforce & Frontline Management - Base

Tool	Description	Limitations
my_time_off_events	Retrieves the user's time off events with a status of Approved, Submitted, Not Submitted, or Sent Back for a specified date range. When an approved entry has been corrected, the tool retrieves the latest corrected entry only.	Doesn't retrieve Cancelled or Denied time off entries.
time_off_balance	Retrieves and displays the user's time off balances as of an effective date.	Doesn't return time off carryover, expiring accrual balances, or expiration details.
time_off_types	Displays all the types of time off the user is eligible for. Supports custom validations.	Excludes time off types that can't be entered through the standard process, such as those enabled only for time tracking, forfeiture adjustments, or selling.

Tool	Description	Limitations
view_holiday_calendar	Retrieves the user’s company holiday calendar events for a specified date range.	While the tool identifies the holidays, it doesn't return the specific duration of the holiday calendar event.
view_time_blocks	Displays all recorded time blocks for a specified date range for the user.	Results are limited to the first 20 time blocks per request.

Guide

Tool	Description	Limitations
navigation_deeplink	Provides a direct navigational link to the correct task or report within the Workday system when the agent can't answer a question directly.	

MSS - Human Capital Management - Base

Tool	Description	Limitations
recommend_change_job_template	Recommends a predefined template for a Change Job request based on the user's context. Template recommendations are driven by the user's current job profile, location and organization.	Only surfaces the recommendation; doesn't initiate or submit the actual job change workflow.
view_direct_reports_info	Retrieves professional profile information, such as anniversary dates, birthdays, promotion history, and tenure, for a manager's direct reports or a specific worker	Provides data for direct reports only, not skip-level reports. Managers with large teams might experience higher response volume. Depending on an individual's employment record, some fields might not populate.
view_direct_reports	Retrieves the names and IDs of the workers who report directly to the manager user.	Only provides data for direct reports, not skip-level reports. For broader organization hierarchy context, use view_org_info instead or consider asking your question in another way. For richer profile data on direct reports, use view_direct_reports_info or view_coworker_info instead.

Tool	Description	Limitations
view_worker_history	Retrieves employment-related details for events such as hire, job change, and compensation for the user or a named worker within a specified date range. Each invocation retrieves a single event category.	When a name is provided, the worker must be part of the manager's reporting structure. When multiple or zero matches are found for a name, the tool returns an error rather than a list.

MSS - Payroll - Advanced

Tool	Description	Limitations
request_payroll_input	Guides authorized users in creating payroll input requests for earnings or deductions by identifying eligible pay components and retrieving the next available payroll start date for accurate scheduling.	Doesn't support custom validations.

MSS - Talent Management - Advanced

Tool	Description	Limitations
start_performance_review_worker	Starts a new *Employee Review* business process for a manager's single direct report or for their entire team.	While you must select a template and period dates, you can only use 1 template when starting reviews for all direct reports simultaneously. Doesn't support custom validations.
request_feedback_worker	Enables a manager to request feedback about a worker from other users. Users can select specific feedback templates and determine if the responses should be confidential or visible to others.	

MSS - Talent Management - Base

Tool	Description	Limitations
find_job_requisition	Displays up to 10 open or in-progress job requisitions for supervisory organizations where the manager holds a leadership role.	Excludes evergreen requisitions and internal apply postings.
view_candidate_status	Retrieves application information, such as skills, experience, and links for managers, recruiters, and	Doesn't retrieve information for candidates without My Candidates.

Tool	Description	Limitations
	candidates that have My Candidates access.	Links and formatting in chat might be inconsistent, such as the inability to click links in some scenarios.
view_team_goals	Aggregates and retrieves up to 100 goals for a manager's direct reports, grouped by worker and completion status. Supports filters for status, keywords, and due dates.	Doesn't support filters for milestones, categories, or specific target and actual currency fields.
view_team_learning_status	Retrieves learning records such as completion, grade, and expiration for a manager's direct team.	Only provides data on learning activities in which the team has already formally enrolled; assigned but not-yet-enrolled training is excluded. Doesn't support filtering by due dates or individual learners.
view_team_performance_review	Retrieves high-level review metadata and overall ratings for the supervisory organization the manager leads.	When a manager leads multiple organizations, only the first supervisory organization is retrieved. Doesn't support non-overall section ratings or comments.

MSS - Workforce & Frontline Management - Advanced

Tool	Description	Limitations
approve_time_entries	Enables a user to approve time entries for multiple workers.	Displays a maximum of 60 records, with 20 records per page.
create_time_blocks_workers	Enables a user to create time blocks for multiple workers.	For a maximum of: • 20 workers. • 100 time blocks. • Date range of 1 week. Doesn't support projects or worktags.
deny_time_entries	Enables a user to deny time entries for multiple workers.	Displays a maximum of 60 records, with 20 records per page.
send_back_time_entries	Enables a user to send back time entries for multiple workers.	Displays a maximum of 60 records, with 20 records per page.

MSS - Workforce & Frontline Management - Base

Tool	Description	Limitations
view_direct_reports_time_off	Retrieves time off events (Approved, Submitted, Not Submitted, or Sent Back) for a manager's direct reports within a specified date range. When an approved time off entry is corrected, the tool retrieves only the latest version.	Doesn't reference your specific team absence configuration or retrieve cancelled and denied entries.
view_time_blocks_workers	Retrieves time blocks for multiple workers.	Displays up to 100 time blocks for a maximum of 20 workers for a maximum date range of 1 month. Doesn't display project time entry details.
view_submitted_time_entries_workers	Retrieves submitted time entries for multiple workers.	Displays a maximum of 60 records, with 20 records per page.

Policy Intelligence

Tool	Description	Limitations
search_policy_documents	Retrieves company policy and procedural information from Help Knowledge Base articles to ensure responses are accurate and based on official documentation.	• We recommend that you opt in to the **People Experience** > **Help** service on the **Innovation Services And Data Selection Opt-In** report before you sign the UMSA or change your data hosting region. This prevents a 14 day waiting period for Self-Service Agent to ingest your policy documents. • Doesn't extract data from articles in Sandbox enviroments. We recommend using IMPL tenants instead for test cases related to this. • Doesn't read document attachments or linked documents in help articles. Only reads the text of the article itself. • Currently only supports English and French-Canadian. We plan

Tool	Description	Limitations
		to support additional languages in the future.

Related Information

Examples

2026R1 Feature Release Note: Journeys and Onboarding Plans for the Self-Service Agent Experience

Planning Agent

Register Planning Agent in Agent System of Record

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

- Configure SSO with user sync and map user profiles between Workday and Adaptive Planning. See Steps: Configure Adaptive Planning for HCM and Financials.

  Note: If your Adaptive Planning instance is *not* Workday-enabled, then you don't need SSO and user sync. You only require the correct permissions assigned. See Concept: Planning Agent.
- Set Up Agent System of Record .

Context

You can register and configure the Planning Agent in Workday’s Agent System of Record (ASOR). The ASOR provides a central management framework, for securely managing and governing all your agents. By registering agents in this system, you can:

- Reduce administrative overhead
- Gain data insights into agent performance and business impact.

The Planning agent is an intelligent, conversational AI assistant that integrates directly into Adaptive Planning using Ask Workday for Adaptive Planning (Ask Workday). Acting as an on-demand digital analyst, it empowers FP&A professionals, CFOs, and operational managers to interact with complex multi-dimensional models using natural language.

Using agents in a sandbox Adaptive Planning instance doesn’t consume flex credits.

The Analyst role of the Planning agent includes the Data Exploration skill. See Concept: Planning Agent: Data Exploration.

Steps

1. Register and Configure Workday-Built Agents .

   Register the **Planning Agent** and then configure the agent to enable the **Data Exploration** skill. Select the security groups that include the invoking users who require access. See Configure Security Policies for Agent Skills .
2. Optional. Write effective prompts to explore the planning data. See Reference: Data Exploration: Prompt Examples.
3. Optional. Use specifications to get clear results from your prompts. See Reference: Data Exploration: Suggested Questions.
4. Optional. Use best practices to structure your queries for data look-ups or complex variance breakdowns. See Reference: Data Exploration: Best Practices for AI Prompts.

Result

Example

Next Steps

Deployment Agent in Implementation Environments

Set Up Deployment Agent in Implementation Environments

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA.

- Set Up Agent System of Record.
- Security: *Reports: AI Agent Security* domain in the System functional area.

Context

To use the Deployment Agent, you must configure it separately for each tenant (Implementation, Preview, or Sandbox). Setting up the agent in one tenant does not enable it in others. The primary setup steps require you to:

- Configure security for the **Deployment Agent** task.

- Activate the Deployment Agent in the Agent System of Record (ASOR).

Workday makes the domain for the Deployment Agent available when ASOR functionality is activated in the tenant. After you register and configure the agent, you can activate it in the **Agent Management Hub**.

To avoid manually reconfiguring the agent in your Sandbox tenants after each tenant refresh, we recommend also setting it up in your Production tenant. While the Deployment Agent is not accessible for use in Production environments, establishing the configuration there ensures it persists and propagates to your Sandbox tenants during standard refresh cycles. However, while your configuration persists, your chat history does not. A Sandbox tenant refresh permanently deletes all Deployment Agent chat history data.

Steps

1. Sign in to the tenant you want to configure.
    - For Implementation or Preview tenants: Sign in directly to the specific tenant.
    - For Sandbox tenants: Sign in to your Production tenant to ensure the configuration persists across future tenant refreshes.

      If you need to use the agent in your Sandbox before the next refresh, complete this setup in Production and then also repeat it in your Sandbox tenant to cover the gap.
2. Create the domain security policy for the Deployment Agent.

   If a policy already exists, skip this step. To verify if a policy exists:
    a) Access the **Create Security Policy for Domain** task.
    b) Select the **For Domain** prompt and enter: *Deployment Agent*.
        - If it doesn’t display, the policy exists. Skip this step.
        - If it does display, select it and click **OK** to create the policy.
3. Edit the security policy and assign security groups.
    a) Search for **View Domain** and enter the domain name: Deployment Agent Users.
    b) From the related actions menu of the domain, select **Domain** > **Edit Security Policy Permissions**.
    c) In the **Report/Task Permissions** or **Integration Permissions** grid, add a new row.
    d) In the new row, select the security groups to which you want to grant access. Example: Implementers.
    e) Select View permissions.
    f) Click **OK**.

       The ASOR agent requires these security groups when you configure the Deployment Agent in the Agent Management hub.
4. (Optional) Assign users to security groups.

   If you haven't already done so, assign users to security policies by adding them to security groups included in the policy.
    - To assign multiple users to a single user-based security group: Access the **Assign Users to User-Based Security Group** task.
    - To assign a single user to 1 or more user-based security groups: Access the **Assign User-Based Security Groups for Person** task.

   You can combine multiple user-based security groups into an aggregation security group.
5. Activate security policy changes.
    a) Access the **Activate Pending Security Policy Changes** task
    b) Enter a comment describing your changes.
    c) Review the pending changes and select the **Confirm** check box.
    d) Click **OK** to activate the changes.

6. Register the Deployment Agent.

   You must register the Deployment Agent in the tenant before you can configure it.

   a) Access the **Agent Management Hub** report.
   b) Select the **Unregistered Workday Agent** tab.
   c) For the Deployment Agent, click **Register**.
   d) Select the **Confirm** check box, and then click **OK** to complete the registration.

      Workday moves the Deployment Agent to the **Agent Registry** tab.
7. Configure the Deployment Agent.

   After you register the Deployment Agent, configure it in the tenant.

   a) On the **Agent Registry** tab, click the *Deployment Agent* name to configure it.
   b) From the profile view of the agent, click **Configure Agent**.
   c) In the **Status** column, use the toggle slide to enable the **Configuration Intelligence Q&A** skill.
   d) If available, enable any other relevant skills you want.
   e) For each enabled skill, populate the **Available To** prompt with the security groups that you want to provide access to for that specific skill.

      The security groups added to the **Available To** prompt for an agent establish the interaction policy of the agent.

      Note: Ensure the security group you add also belongs to the *Deployment Agent Users* domain security policy. Workday displays an error validation when the security group you add here isn't also part of the *Deployment Agent Users* security domain policy. Users in the security group won't have access to the Deployment agent in the tenant.
8. Activate the Deployment Agent.

   When you complete agent configuration, you can activate the Deployment Agent in the tenant.

   a) Click **Activate**.
   b) If prompted, confirm activation.

   Once activated, the Deployment Agent becomes available for use by the members of the security groups you assigned to its skills. You can deactivate and reactivate agents at any time from the **Agent Management Hub**.

Result

You can now access the Deployment Agent and view chat histories in your configured tenant. Each tenant isolates its own chat histories. You can't view a chat history from one tenant (such as Sandbox) in another tenant (such as Preview).

Note: A Sandbox tenant refresh permanently deletes all Deployment Agent chat history data. While your agent configuration persists if you set it up in Production, you can't recover chat history data after a refresh.

Related Information

Tasks

Set Up Agent System of Record

Reference

Reference: Deployment Agent Skills and Capabilities in Implementation Environments

Concept: Deployment Agent in Implementation Environments

Overview and Purpose

The Workday Deployment Agent is an AI-powered conversational assistant that you can access by entering *Deployment Agent* on the global navigation bar. It leverages Google Gemini Large Language Models (LLMs) and a retrieval-augmented generation (RAG) framework to provide instant guidance.

The primary purpose of the agent is to equip Workday implementers and customer administrators with configuration intelligence while working in Implementation environments. Implementation environments include:

- Implementation tenants.
- Preview tenants.
- Sandbox tenants.

Note: The Deployment Agent isn't available as a conversation assistant in Production tenants.

The Deployment Agent acts as a specialized technical architect that doesn't just search for keywords, but understands the logic, dependencies, and structural requirements of the Workday platform. It functions as a knowledge assistant that draws from and synthesizes a repository of curated information, including:

- Workday Administrator and User Guides, to provide step-by-step how-to instructions and functional definitions.
- Community articles and Q&A, to leverage accepted, real-world peer solutions and troubleshooting tips.
- Implementer-only documentation, to offer technical guidance previously restricted to service partners.
- Web service descriptions (WSDLs), to interpret SOAP or integration errors and identify missing data fields or security permissions.

Business Benefits

- Provides immediate answers to how-to questions, reducing the time spent searching external sites.
- Helps identify the root causes of web service errors, like SOAP errors, or business process logic failures.
- Offers an environment for users to quickly get up to speed on unfamiliar functional areas.
- Maintains system stability and security by routing implementation tenant AI traffic through the Agent Gateway, ensuring all interactions are authenticated and audited.

Sandbox Tenant Refreshes

When you refresh a Sandbox tenant, Workday permanently deletes all Deployment Agent chat history data. You cannot recover this data after a refresh.

To avoid manually reconfiguring the agent in your Sandbox tenant after each refresh, we recommend setting up the agent in your Production tenant. You can't use the Deployment Agent in the Production tenant. However, establishing the configuration there ensures it persists and propagates to your Sandbox tenant during standard refresh cycles. If you do not configure the agent in Production, you must manually reconfigure it in your Sandbox tenant after every refresh to continue using it.

Limitations

The agent:

- Might occasionally produce inaccurate or incomplete information. Users must validate all suggestions against official documentation.
- Can’t access your specific data or live tenant configurations. It also can’t detect your current security policies or existing instances.
- Has a limit of 60 questions per conversation You may continue to ask questions in the conversation but the Deployment agent can access and use only the most recent 60 questions (and associated answers). This is to maintain system stability and performance during peak usage. Once you reach this limit, you can continue to ask questions by starting a new chat conversation.
- Is designed to assist, not replace, human expertise.

Related Information

Examples

Example: Create a Calculated Field with the Deployment Agent in Implementation Environments

Example: Troubleshoot a SOAP Error with the Deployment Agent in Implementation Environments

Workday AI Fact Sheet: Deployment Agent

Reference: Deployment Agent Skills and Capabilities in Implementation Environments

Capability	Skill	Description
Configuration Intelligence	Q&A	Provides the primary chat logic for the Deployment agent. Note: In implementation environments, enabling this skill automatically enables all other skills for the Deployment Agent.
Configuration Intelligence	Step-by-Step instructions	Provides detailed setup steps for tasks like creating calculated fields or linking compensation grades.
Configuration Intelligence	Configuration Catalog support	Offers smart package suggestions and assists with automatic setup of the Configuration Catalog.
Technical troubleshooting	Error interpretation	Analyzes web service or SOAP errors and suggests likely resolutions.
Technical troubleshooting	Logic analysis	Helps identify why a business process isn't behaving as expected or why a rule isn't initiating.
Knowledge discovery	Conceptual summaries	Summarizes complex Workday concepts into layperson's terms. Example: Top of Stack.
Knowledge discovery	Source referencing	Provides links and citations to Community and Administrator Guide sources to verify information.

Related Information

Tasks

Set Up Deployment Agent in Implementation Environments

Reference: Deployment Agent Sample Prompts for Implementation Environments

CRAFT Method for Building Prompts

To ensure more accurate results, use these CRAFT elements to build your prompts: Context

- Role
- Action
- Format

- Tone

Prompt Element	Prompting Tip	Example Prompts
Context	Specify the relevant Workday functional area, module, or project phase.	I am working on Financials in a Phase X implementation.
Role	Specify your persona to get context-appropriate advice. Omit the role when the persona is obvious, or you have already established the role earlier in the chat.	I am a Workday administrator... As a configuration specialist,...
Action	Clearly define the task you need to perform (the how, why, or what).	...how do I load project budgets in bulk?
Format	Request a specific output format for the information.	Omit format if you're comfortable with the default paragraph or step-by-step instructions for how-to questions. Provide the answer in a numbered list of steps.
Tone	Specify the level of technical detail or the intended audience. Omit tone when you are performing standard technical tasks where the default Workday professional voice suffices.	Give me a layperson's terms explanation of the concept, 'Top of Stack.'

Sample Deployment Agent Prompts

Use Case	Sample Prompt
New configuration	*I am an implementer working on Financials. Provide step-by-step instructions on how to create a calculated field that counts Scheduled Weekly Days.*
Troubleshooting errors	*I am getting a SOAP error while using Object Transporter to migrate Payroll data. What are the common causes for this error and how do I fix them?*
Learning or refresher	*As a Workday administrator, give me a layman's terms explanation of the 'Top of Stack' concept. Provide the answer in bullet points.*
Optimization	*Suggest best practices for linking Compensation Grades to Job Requisitions to ensure data integrity during a high-volume hiring phase.*

Related Information

Concepts

Concept: Deployment Agent in Implementation Environments

Example: Troubleshoot a SOAP Error with the Deployment Agent in Implementation Environments

This example illustrates how an integration consultant uses the CRAFT method to get assistance from the Deployment agent in resolving a SOAP web service error encountered during a migration or integration task.

Context

You are working as an integration consultant to finalize an automated expense-clearing integration. You attempt to use the Submit_Expense_Report web service to migrate data from a legacy travel system into Workday. However, every time your middleware makes a call, Workday returns this SOAP error:

`Validation error occurred. The field Expense_Report_Data is required.`

You have already confirmed that the field, **Expense_Report_Data**, is present in your XML. You suspect the error is a false positive, an occasional behavior in Workday SOAP services in which the service triggers a generic error for a parent element when the real issue is a missing child element or a specific security requirement. Have access to Customer Central with the Deployment agent available on the global navigation bar and the sidebar.

Prerequisites

- Have access to the Implementation, Preview, or Sandbox tenant with the Deployment agent available in the global navigation bar.

  See Set Up Deployment Agent in Implementation Environments .
- Have the specific error message or code ready to paste. Example: An error message from a web service.

Steps

1. Sign in to the Implementation, Preview, or Sandbox tenant
2. Access the Deployment agent entry from the global navigation bar or sidebar.
3. Enter your prompt using the CRAFT method to provide a clear prompt that includes your role and the context of your request.

   Your prompt:

   I am an integration consultant working on a Financials implementation. I am calling the Submit_Expense_Report web service and receiving a 'Validation error occurred' message regarding a missing field.
4. Continue by describing the technical issue:

   Paste the exact error message and provide details on what you have already verified.

   The error says: ‘The field Expense_Report_Data is required.’ I have confirmed this field is in my XML. What are the most common hidden missing fields or security issues that cause this specific SOAP fault for this service?
5. (Optional) If the initial answer is broad, refine the request.

   Ask the agent to drill down in to security or business process requirements. Your prompt:

   List the specific functional area and security domain permissions my Integration System User (ISU) needs to initiate this specific web service.

Result

The Deployment agent provides a list of potential root causes and specific configuration areas to check. It often points you toward the exact field or security permission that is likely causing the failure, saving hours of manual research.

Next Steps

Once the Deployment agent provides the steps, run the **Create Calculated Field** task to implement the logic. After building the field, use the **Thumbs Up** or **Thumbs Down** icon to rate the accuracy of the logic provided.

Related Information
Reference
Reference: Deployment Agent Sample Prompts for Implementation Environments

Example: Create a Calculated Field with the Deployment Agent in Implementation Environments

This example shows how a Deployment agent user uses a CRAFT prompt to generate logic for a Conditional Management Level calculated field.

Context

You are a Workday administrator and configuration specialist. You want to use a calculated field to categorize workers into 2 specific groups, Manager or Individual Contributor, based on your existing management level hierarchy. You need to categorize workers as Manager or Individual Contributor so that you can:

- Enhance custom reporting and dashboards: Use this field to group data in summary reports, enabling executives to see high-level workforce distributions without getting bogged down in dozens of specific job grades.
- Streamline outbound integrations: When you send data to external systems (like an LMS or benefits provider) that only recognize simple management statuses, use this field to map your complex internal hierarchy to the simplified values they require.
- Drive business process condition rules: Use this this field to initiate specific workflow steps. For example, you might create a rule that requires an additional approval level only if the worker's status is *Manager*.
- Automate security group assignments: Use the results of this field to define the scope of constrained security groups or to help automate membership in integration system security groups.
- Perform data audits: Use this field to identify data discrepancies, such as finding individual contributors who are incorrectly assigned as managers of a Supervisory Organization.

Steps

1. Sign in to the Implementation, Preview, or Sandbox tenant.
2. Access the Deployment Agent entry in the global navigation bar.
3. Use the CRAFT method to provide a clear prompt that defines your role and the context of your request, including the conditional logic you need.

   Your prompt:

   I am a Workday administrator. I need to create a calculated field on the Worker business object. The logic should be: if a worker's 'Management Level' is 'Manager' or any level above that (like Director or VP), return the text 'Manager'. Otherwise, return 'Individual Contributor'. Can you provide the step-by-step [Format] configuration and the specific calculation type I should use?
4. Review the logic.

   The agent analyzes the request and typically suggests an Evaluate Expression function. It provides the configuration parameters you need to enter in the Create Calculated Field task in Workday:

   - **Business Object**: Worker.
   - **Function Type**: Evaluate Expression.
   - **Default Value**: Individual Contributor.
   - **Condition**: Management Level (using an *In Selection List* operator).
   - **Return Value if True**: Manager.

5. (Optional) If your organization uses unique naming conventions, you can ask a follow-up question. Your prompt:

   My tenant uses 'Lead' instead of 'Manager'. How should I update the condition to include 'Lead' and everything above it?
6. Review the suggested logic against the specific management level hierarchy of your tenant to ensure all levels are captured correctly.

Result

The Deployment agent provides you with the structural logic and specific functions needed for the field. This eliminates the need for you to manually browse the Administrator Guide to determine which calculation type best supports if/then/else text strings.

Next Steps

Once the Deployment agent provides the steps, run the **Create Calculated Field** task to implement the logic. After building the field, use the **Thumbs Up** or **Thumbs Down** icon in the Deployment agent window to rate the accuracy of the logic provided.

Related Information

Reference

Reference: Deployment Agent Sample Prompts for Implementation Environments

Sana for Workday

Concept: Sana Workspace

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

To use this functionality, you must:

- Sign the Universal Main Subscription Agreement (UMSA).

  Note: When you sign the agreement, Workday provides your organization with complimentary Flex Credits that you can use towards Sana Core for Workday. Once you reach the allotted complimentary Flex Credit consumption, you must sign the Workday Flex Credits and Platform Entitlement Policy to continue to use Sana Core for Workday.

- Purchase the Core Human Capital Management or Core Financials SKU. This only applies to Sana Core.
- Sign the Workday Flex Credits and Platform Entitlement Policy. This only applies to Sana Enterprise.
- Purchase the Sana Enterprise SKU. This only applies to Sana Enterprise.

Sana Core provides conversational, agentic AI for HCM and Financials, both within Workday and the Sana Workspace, enabling workers to ask questions and take action within Workday.

Sana Enterprise expands on Sana Core to include third-party connectors and orchestrations, enabling workers to complete work both within Workday and across other third-party applications.

To help you get started, see the:

- Frequently Asked Questions for Sana Core and Enterprise on Workday Community.
- Sana Help Center.

Capabilities	Sana Core	Sana Enterprise
Access to the Sana Workspace, including file upload (research and analysis) and LLM chat (web only).	Yes	Yes
Read and write actions in Workday through Workday Self-Service Agent (WSAA).	Yes	Yes
Agentic chat with user history and citations.	Yes	Yes
Single sign-on shared with your Workday tenant.	Yes	Yes
Role and permission mirroring so access and actions respect Workday security configuration.	Yes	Yes
Administrators can enable and manage supported third-party connectors used by Sana Enterprise. Available connectors can read and write across external applications. Administrators have granular connector controls to limit user access.	No	Yes
Support custom Model Context Protocol (MCP) connectors. Administrators can integrate internal or long-tail systems securely using OAuth.	No	Yes
Users with appropriate permissions can request and perform actions in connected	No	Yes

Capabilities	Sana Core	Sana Enterprise
systems directly from Sana Enterprise chat.		
Prompts users to review and confirm actions that require human-in-the-loop approval before proceeding. All cross-system actions are logged and available for audit.	No	Yes
Provides data analysis and visualization through secure backend code execution, supporting structured data such as spreadsheets and generating charts. Sana writes and runs code behind the scenes.	No	Yes
Deliver chat responses containing rich, interactive elements instead of only plain text.	No	Yes
Use agent builder to create custom agents. Describe what you want using natural language. Users can trigger agents manually, on a schedule, or through third-party events.	No	Yes
A central location to view completed agent outputs and manage pending approvals in the Sana Inbox.	No	Yes
Individual agent pages that enable users to navigate back to each agent to view the history and configuration.	No	Yes
A Meeting Agent can join Google Meet, Microsoft Teams, and Zoom meetings automatically as a notetaker. The agent records, creates searchable summaries, and extracts decisions and action items. Indexes meeting transcripts. Transcripts become searchable and become available to agents to consume.	No	Yes
A navigational search-as-you-type in the main chat drop down that surfaces links to Workday people, reports, and tasks.	No	Yes

Capabilities	Sana Core	Sana Enterprise
Users can jump straight to the right place.		
An in-chat conversational search to refine queries naturally, providing users with a flexible, conversational way to find things. Users can ask Sana for a specific person, task, or report and get deep-linked, clickable results right in the conversation.	No	Yes

Sana Workspace

You can access the Sana Workspace from your Workday tenant when you:

- Click the **Sana** card on the **Workday Home** page.
- Click the **Explore Sana** button on the Workday search results page.
- Click **Sana** in the Global Navigation Bar.

Note: To enable the **Sana** card on the **Home** page and the **Explore Sana** button on search, you must enable the **Sana** card within the **Work Tools** section of the **Home Cards Workspace**.

Related Information
Examples
Sana Help Center
Sana Features Page
Getting Started for Admins
Connector Guides
Workday Community: Getting Started with Sana
2025R2 Feature Release Note: Sana Core for Workday
2025R2 Feature Release Note: Sana Enterprise for Workday

Steps: Set Up Sana for Workday

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

To use this functionality, you must:

- Sign the Universal Main Subscription Agreement (UMSA).

  Note: When you sign the agreement, Workday provides your organization with complimentary Flex Credits that you can use towards Sana Core for Workday. Once you reach the allotted complimentary Flex Credit consumption, you must sign the Workday Flex Credits and Platform Entitlement Policy to continue to use Sana Core for Workday.
- Purchase the Core Human Capital Management or Core Financials SKU. This only applies to Sana Core.
- Sign the Workday Flex Credits and Platform Entitlement Policy. This only applies to Sana Enterprise.
- Purchase the Sana Enterprise SKU. This only applies to Sana Enterprise.

Security: These domains in the System functional area:

- *Sana Agent User Provisioning*
- *Sana Enterprise*
- *Security Activation*
- *Security Configuration*

Context

To ensure security setup for Sana and the related AI agents is complete, Workday sends notifications to administrators. We notify:

- Workday security administrators to complete the **Set Up AI Admin Security Permissions** task.
- Agent System of Record administrators to configure and activate the **Self-Service Agent**.
- Sana administrators to optionally configure or modify default settings in the **Sana Workspace**.
- User provisioning administrators to provision employees to **Sana**.

Steps

1. Set Up AI Administrator Security Permissions.
2. Set Up Agent System of Record.
3. Edit Domain Security Policies.

   Configure the *Sana Enterprise* domain in the System functional area.

   Note: This step is required if your organization purchased the Sana Enterprise SKU. This domain configuration determines who can use cross-system connections and Sana Enterprise features.
4. (Optional) Access the **Set Up Security Groups for User Provisioning** task. If you only want particular security groups to be available for Sana provisioning, add rows to the grid and select the groups to enable on the **Security Groups** prompt.

   Security: *Set Up: User Provisioning* domain in the System and User Provisioning functional areas.

5. Provision users to Sana Workspace.

   We notify user provisioning administrators to provision users to the Sana Workspace.

   a. In Workday, open the **Action Required: Provision Users to Sana Workspace** notification from the bell icon.
   b. Click the link in the notification to open the **User Provisioning Workspace**.
   c. On the **Products** page, click **Configure** in the **Sana** tile.
   d. In the **Provision Users** section, click **Edit Provisioning Group**.
   e. In the **Using Workday Security Groups** prompt, select either:
      - *All* to provision all users for Sana.
      - Individual security groups to provision. You can only select individual security groups if you set them up for user provisioning on the **Set Up Security Groups for User Provisioning** task.
   f. Click **Update Provisioning Group**.
   g. Click **Preview and Enable Sync**.
   h. Review the users who will be provisioned, select the confirmation check box, and click **Enable Sync**.

   After sync is enabled, users in the selected security groups are automatically provisioned and can sign in to the Sana Workspace.
6. Enable access to the Sana Workspace from Workday.

   To make it easy for users to find and access the Sana Workspace from your Workday tenant, enable the **Sana** card on the Home page:

   a. On the Home Cards Workspace, click **Home**.
   b. Click **Cards**.
   c. Click **Edit Work Tools**.
   d. In the **Edit Work Tools** pop up, add a row to the grid.
   e. In the **Name** field, enter *Sana*.
   f. Click **OK**.
7. (Optional) Configure the Sana Workspace.

   a. From the Sana Workspace, click the arrow next to the workspace name in the navigation menu.
   b. Click **Workspace Settings**.
   c. (Optional) Configure optional settings. You can:

   - Disable web search.
   - Disable intercom support chat.
   - Disable specific third-party connectors. (Sana Enterprise only.)
   - Restrict agentic actions to approved email domains. (Sana Enterprise only.)

Result

Users can immediately access Sana from Workday and use Sana capabilities.

Related Information
Examples

Sana Help Center

Workday Community: Getting Started with Sana

2025R2 Feature Release Note: Sana Core for Workday

2025R2 Feature Release Note: Sana Enterprise for Workday

Set Up AI Administrator Security Permissions

Prerequisites

Note: You might need to take additional steps to enable this feature based on your organization's subscription service agreement. Your organization is either on the Main Service Agreement (MSA) or the Universal Main Service Agreement (UMSA). To determine your organization's subscription service agreement:

1. Select your profile avatar on Workday Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job title.
4. View your **Subscription Service Agreement** value.

If the value is:

- *UMSA*, the feature is automatically available. Keep data contributions enabled to ensure full agent functionality. For more information on Machine Learning data contributions, see Concept: Workday AI for Universal Main Subscription Agreement Customers.
- *MSA*, your organization must opt in to UMSA and enable this feature through Innovation Services.

UMSA is required for non-production and production tenants for Workday-Built agents. UMSA is not required for non-production tenants for self-built agents.

For information about how using agents impacts your Flex Credits, see: Workday Flex Credits Community page.

To use Sana Core and Sana Enterprise, you must:

- Purchase the Sana Enterprise SKU. This only applies to Sana Enterprise.
- Purchase the Core Human Capital Management or Core Financials SKU. This only applies to Sana Core.
- Sign the Universal Main Subscription Agreement (UMSA).

  Note: When you sign the agreement, Workday provides your organization with complimentary Flex Credits that you can use towards Sana Core for Workday. Once you reach the allotted complimentary Flex Credit consumption, you must sign the Workday Flex Credits and Platform Entitlement Policy to continue to use Sana Core for Workday.
- Sign the Workday Flex Credits and Platform Entitlement Policy. This only applies to Sana Enterprise.

Security: You have security permission on these domains in the System functional area:

- *Security Activation*
- *Security Configuration*

Context

The **Set Up AI Admin Security Permissions** task bundles all the necessary security configuration steps into a single task which when complete, initiates backend processing to get your organization set up to use Workday AI features.

This is a one-time task for each tenant. The task simplifies granting security access for:

- Agent System of Record: Assign users access to manage and configure AI agent behavior and integrations in a central location.
- User Provisioning Workspace for Sana: Assign administrators to provision users to Sana.
- Platform Consumption Console: Assign users access to monitor and manage infrastructure resources that your agents use.
- Sana: Assign users as Sana administrators to configure Sana features in the Sana Workspace.

Workday sends a notification to security administrators in all your tenants (Production, Sandbox, Sandbox Preview, Implementation, and Implementation Preview) to access and complete the **Set Up AI Admin Security Permissions** task.

Note: The security configuration notification expires in 30 days.

While you can configure areas of the **Set Up AI Admin Security Permissions** task separately, Workday recommends using the task to ensure all critical dependencies for your AI experience are met.

Security administrators must complete all sections. Once you submit the task, you can’t edit it. You can manually update the configuration through the standard Workday security settings.

Note: If multiple administrators are configuring this task, Workday processes the first configuration that's submitted.

Steps

1. Access the **Action Required: Review and Configure the Security for Sana and Workday Agents** notification from the bell icon in Workday.

   Note: If administrators never received this notification or it expired and was removed after 30 days, you can access the **Notify Users to Configure Sana Agent Security** task to resend the security configuration notification. The user must have **Modify** permissions on the *Security Configuration* domain to receive the notification. The **Notify Users to Configure Sana Agent Security** task is only available in the tenant when you sign the UMSA. We don’t resend the notification if an administrator has already completed the **Set Up AI Admin Security Permissions** task.
2. In the notification, click **Start Configuration**.
3. As you complete the **Configure Security Policies** section on the **Configuration** tab, consider:

   You only need to configure grids with an ***Incomplete*** status. We display a:

   - ***Completed*** status when domain security policies are configured. We hide the **Security Group** and **View or Add Users to Security Group** columns in the grid.
   - **Completed with Exceptions** status when at least 1 of the domain security policies in the **Domain Security Policies** column isn't currently active or it has pending changes.

   In the **View or Add Users to Security Group** column:

   - You can add members only when you create a new security group or select a group that's not used in other policies and doesn't have members.
   - You can't add or remove members in the column when you select a security group that's currently used in other policies or it has existing members.

   In the **Details** column, you can drill into each domain security policy configuration by clicking **Details**. When you click the link, we display a **View Domain Details** pop-up box where you can view the configuration.

Option	Description
Agent System of Record	This section enables you to configure access to the Agent System of Record workspace. The **Domain Security Policies** column displays all domain security policies you need to configure. In the **Security Group** column, select an existing user-based security group or create a new one. We display the members in the **View or Add Users to Security Group** column. Workday adds users in those groups to the domain

Option	Description
	security policies listed in the **Domain Security Policies** column with **View** and **Modify** permissions.
Platform Consumption Console	This section enables you to configure access to the Platform Consumption Console. The **Domain Security Policies** column displays all domain security policies you need to configure. In the **Security Group** column, select an existing user-based security group or create a new one. We only require a security group with **View Only** permission on the *Management Dashboard: Platform Consumption Console* domain security policy. You can only add a security group to the *Management Dashboard: Platform Consumption Console* domain using this task if there are no existing security groups with **View Only** or **View** and **Modify** permissions configured on the domain security policy. Note: Workday displays a **Completed** status on the **Platform Consumption Console** grid when these security configuration criteria are met. We display the members in the **View or Add Users to Security Group** column. Workday adds users in those groups to the domain security policies listed in the **Domain Security Policies** column with **View Only** permission.
User Provisioning Workspace	This section enables you to configure access to the User Provisioning workspace for Sana. The **Domain Security Policies** column displays all domain security policies you need to configure. In the **Security Group** column, select an existing user-based security group or create a new one. We display the members in the **View or Add Users to Security Group** column. Workday adds users in those groups to the domain security policies listed in the **Domain Security**

Option	Description
	Policies column with **View** and **Modify** permissions.

When a domain is disabled and you access the **Set Up AI Admin Security Permissions** task:

- You can add security groups to the domain. Once you submit the changes on the task, this activates the domain.
- We display a ***Completed*** status if the domain has existing security groups.

4. As you complete the **Set Up Sana Administrators** section on the **Configuration** tab, consider:

Option	Description
Set Up Sana Administrators	This section enables you to define which users are Sana administrators. Workday automatically provisions these users into Sana upon activation. In the **Security Group** column, select an existing user-based security group or create a new one. Users with Sana administrator privileges can access and configure the Sana Workspace.

5. Select the **Activate Pending Security Policy Changes** tab.

   To activate security policy changes in your tenant, you must have permission on the *Security Activation* domain.
6. As you complete the **Activate Pending Security Policy Changes** tab, consider:

Option	Description
Security Policy grids	Review the security changes in the grids.
Confirm check box	Select the check box to submit all security policy changes. Workday activates all security policy changes in the grids including the security settings on the **Configuration** tab.

7. Click **OK** and then click **Done**.

Result

Workday automatically activates pending security policy changes and makes applicable tasks available. Workday might notify members of included security groups of additional tasks and actions they can take.

If assigning Sana administrator access to members in the security groups fails, we display a **Resubmit** button in the **Set Up Sana Administration** section of the **Configuration** tab. You can retry the provisioning by clicking the button. Workday attempts to assign the users with Sana administrator privileges.

Next Steps

(Optional) If you need to update the configuration on this task, access the standard Workday security settings to manually make the changes.

Related Information

Examples

Sana Help Center

Workday Community: Getting Started with Sana
2025R2 Feature Release Note: Sana Core for Workday
2025R2 Feature Release Note: Sana Enterprise for Workday

Platform Consumption Console

Set Up Security for Platform Consumption Console

Prerequisites
To complete these steps, you must be an implementer or security administrator.

Context

Note: The solutions described in this section are not part of the Workday Service. See Legal Notice for details.

Note: The data displayed in the **Platform Consumption Console** dashboard is usage data and is not considered customer content.

Universal Main Subscription Agreement (UMSA) or Main Service Agreement (MSA) subscribers can use the **Platform Consumption Console** dashboard to review their document storage data, which helps you monitor your storage levels. See Workday Community: Simplified Platform Access: Faster, More Predictable Workday AI Adoption.

UMSA subscribers can also use the **Platform Consumption Console** dashboard to visualize their company's use of complimentary and purchased Workday Flex Credits based on their usage of Workday offers.

Steps

1. Access the *Management Dashboard: Platform Consumption Console* domain in the System functional area.
2. From the related actions menu of the domain, select **Domain > Create Security Policy**.
3. Select the **Confirm** check box and click **OK**.
4. In the **Report/Task Permissions** grid, add security groups relevant to your organization.
5. Select the **View** check box and click **OK**.
6. Activate Pending Security Policy Changes.

Result

Selected security groups can now access the **Platform Consumption Console** dashboard.

Related Information
Examples
The Next Level: Platform Consumption Console (PCC) Overview
Workday Community: Flex Credits FAQ
Workday Community: Flex Credits Overview
Workday Community: Workday Flex Credits

Concept: Platform Consumption Console

The **Platform Consumption Console** dashboard enables Universal Main Subscription Agreement (UMSA) subscribers to monitor their usage of Workday offers and associated Flex Credit balances.

Main Service Agreement (MSA) subscribers can also use the dashboard to review document storage data and monitor storage levels. See Workday Community: Simplified Platform Access: Faster, More Predictable Workday AI Adoption.

Flex Credits Access and Policy Requirements

UMSA subscribers can use the **Platform Consumption Console** dashboard to visualize their company's use of Flex Credits based on their usage of Workday offers included in the Workday Flex Credits Rate Card.

Flex Credits are only available to UMSA customers. UMSA customers are provided Flex Credits subject to either the Complimentary Flex Credits Policy incorporated in the UMSA Product Terms or the Flex Credits and Platform Entitlement Policy incorporated into an Order Form.

If you are subject to the Complimentary Flex Credits Policy, you must sign the Workday Flex Credits and Platform Entitlement Policy to continue using Workday AI agents once you have exhausted your complimentary Flex Credits.

Credit Balance and Entitlement

The **Credit Balance** page displays your daily Flex Credit activity. The **Credit Entitlement** page displays your Flex Credit package purchase history, organized by these statuses:

Status	Definition
Active	Credits available for consumption.
Expired	Credits that have expired.
Inactive	Purchased credits that are available for consumption at a future date.

All Flex Credits are fungible and you can apply them universally across the Workday offers in the Rate Card to which you are entitled.

Rate Card

The **Rate Card** page is the definitive resource for the monetary value of your entitlements in terms of credit usage. Workday uses these variables to calculate usage:

Column	Definition
In Blocks of (Units)	The number of units included in a chargeable block.
Credit Rate per Block	The rate charged for that block of units.

Understanding and Tracking Usage

Workday updates your usage daily to reflect the previous day's usage. Usage is based on the specific capabilities defined in the **Rate Card** page and the policy version associated with your agreement. Workday uses multiple components to determine your usage:

Component	Definition
Agents	Usage of agent skills and activities.
API Requests	Number of API requests. Note: This data is only available to customers who have signed the Workday Flex Credits and Platform Entitlement Policy.
Document Storage	Gigabytes (GB) of data stored. Note: Usage of document storage does not result in Flex Credit consumption but is subject to service limits. See Reference: Document, File Size, and Printing Limits.

Your policy provides a baseline usage allowance or embedded entitlement. After this embedded entitlement is used, Workday charges your usage against your available credit entitlements, prioritizing the credits that will expire first.

You can track your usage against this threshold in the Embedded Entitlement Overview visualization on the **Overview** page. For more detailed metrics, you can use the **Consumption Usage** page to drill down and view a breakdown of consumption by service.

Note: If your organization has signed a version of the Workday Flex Credits and Platform Entitlement Policy that does not include platform components or entitlements, you won't see those entitlements or usage on the **Platform Consumption Console** dashboard.

Credit Entitlement Notifications

Workday notifies you as you consume your active credit entitlement. When your credit entitlement usage reaches 80%, 90%, and 100%, users with access to the *Management Dashboard: Platform Consumption Console* domain receive notifications, and Workday displays a banner on the **Platform Consumption Console** dashboard. To configure your notification delivery settings, see Concept: Notifications.

Workday doesn't deactivate offers on the **Platform Consumption Console** dashboard when you exceed your credit entitlement. To deactivate an agent, see Register and Configure Workday-Built Agents.

Non-Production Tenants

Workday enables the **Platform Consumption Console** dashboard in your Production and non-Production tenants. For most offers, use in non-Production tenants doesn't affect your Workday Flex Credit balance. While non-Production tenants track your consumption and display an informational Workday Flex Credit balance, for most offers Workday only applies usage from your Production tenant against your organization's Flex Credit balance.

Workday sends daily aggregate data across all of your non-Production tenants to the **Platform Consumption Console** dashboard. Example: When you use the **Platform Consumption Console** dashboard in your Sandbox tenant, the dashboard displays combined activity from all of your non-Production environments.

Related Information
Examples

The Next Level: Platform Consumption Console (PCC) Overview

Workday Community: Flex Credits FAQ

Workday Community: Flex Credits Overview

Workday Community: Workday Flex Credits

AI Data Contributions

Steps: Set Up Notifications for AI Feature Data Contributions

Context

Universal Main Subscription Agreement (UMSA) customers can configure the *AI Features and Third Party Notification* domain to receive these notifications.

Notification Type	Delivery Timing	Purpose
AI Feature Availability	On the day of feature release.	Confirms the AI feature is available in your Production tenant and starts a 14-day period for you to manage your data contributions before data extraction begins.
Description or Technical Updates	Weekly, as triggered by changes.	Reports updates to feature descriptions and changes to data fields used by the AI feature.
Upcoming AI Features	30 days before release.	Provides a notice of upcoming AI features applicable to your purchased SKUs.

Note: To determine your company's subscription agreement type:

1. Access your Community profile.
2. Beneath your name, click the **name of your company**.

In the **Subscription Service Agreement** field:

- **MSA** indicates the Main Service Agreement type.
- **UMSA** indicates the Universal Main Subscription Agreement type.

Steps

1. Edit Domain Security Policies.

   Add the relevant security groups to the *AI Features and Third Party Notification* domain in the Innovation Services functional area.
2. Activate Pending Security Policy Changes.
3. Access the **Edit Tenant Setup - Notifications** task.

   On the **System** tab of the **Notification Delivery Settings** section, verify the routing rule for the **Parent Notification Type** includes email notifications.

   If not, from the **Ascend Notifications** row, select the **Override Parent Notification Type Settings** check box, and select a routing rule that includes email notifications. See Create Notification Routing Rules.

   Security: *Set Up: Tenant Setup - BP and Notifications* domain in the System functional area.

Result

Security group members will receive notifications about upcoming changes to AI features.

Enable Innovation Services Feature and AI Data Contributions for MSA Customers

Context

You can use Innovation Services to access features that provide functionality beyond Workday's core products. When your organization subscribes to the Main Service Agreement (MSA), you can only access these features through Innovation Services. You must sign the Innovation Services Addendum (ISA) before you can enable Innovation Services features using these steps.

We use artificial intelligence (AI) in some Innovation Services features as part of their functionality. For these features, you must also enable data contribution, which Workday uses to provide better in-feature AI results.

Contact your Customer Success Manager, or have your Named Support Contact Administrator open a Customer Success request on Workday Community, to acquire and sign the order form to subscribe to Innovation Services.

Steps

1. Enable the Innovation Services functional area.

   See: Steps: Enable Functional Areas and Security Policies.
2. Edit Domain Security Policies.

   Configure the *Manage: Innovation Services* domain in the Innovation Services functional area.
3. Access the **Innovation Services and Data Selection Opt-In** report.
4. On the **Innovation Services Opt-In** task, select the check box for the feature you want to enable from the **Available Services** tab.
5. Click **Next**.
6. (Optional) On the **Maintain Innovation Services Data Selection Opt-In** task, select the check boxes for the data you want to contribute for AI.

   See: Reference: Workday AI Data Contributions to view which data contributions the feature requires.

Next Steps

AI features that require data contributions don't function accurately in your Sandbox tenant. To test AI features that require data contributions before deploying them to your Production tenant, use your Implementation tenant.

You can use these tasks to test your configuration in your Implementation tenant:

Task	Description
Maintain Weekly Data Contribution Activation for Implementation Tenant	Manages future weekly data extracts.
Run On-Demand Data Contribution Activation for Implementation Tenant	Extracts data and subscribes the tenant to future weekly extracts.

To ensure accurate testing, Workday recommends you refresh your Sandbox Preview or Implementation tenant before running these tasks. AI features require a certain amount of data, so it can take up to 2 weeks for Workday to provide recommendations.

Related Information

Examples

Workday Community: Workday AI Gateway

Workday Community: Workday Innovation Services

Workday Community: Workday Innovation Services - Frequently Asked Questions

Manage Workday AI Data Contributions for Universal Main Subscription Agreement Customers

Prerequisites

- Your organization must be on the Universal Main Subscription Agreement.

  Note: To determine your company's subscription agreement type:

  1. Access your Community profile.
  2. Beneath your name, click the **name of your company**.

  In the **Subscription Service Agreement** field:

  - **MSA** indicates the Main Service Agreement type.
  - **UMSA** indicates the Universal Main Subscription Agreement type.
- Security: These domains in the Innovation Services functional area:
  - *Manage: Data for ML Features*
  - *View: Data for ML Features*

Context

When you subscribe to the UMSA, you automatically enable data contributions for AI features.

You can manage data contributions for AI features by product line or AI feature.

For more information on feature-level contributions, see Reference: Workday AI Data Contributions .

Steps

1. Access the **Data Contribution for Workday AI** report.
2. Complete the task:

Field	Description
Disallow Data Contribution	When you select this check box, Workday: • Disables data contribution for the associated product line or AI feature. • Deletes your past data contributions within 30 days.
Data Details	Click **View Data Collected** to view definitions for the types of data contributed to Workday.
View Upcoming Contribution Changes	Click **Contribution Changes** to view upcoming changes to the feature's required data contributions.
Countries Excluded from Data Collection by End User Location	At the AI feature level, select countries that you would like to exclude from data contributions.

3. Click **OK**.

Result

When you disable data contributions, Workday stops collecting new data and deletes your past contributions within 30 days.

Note:

When you disable data contributions, you might impact the performance of certain AI features, including a degraded experience to the feature not functioning at all.

To understand how disabling contributions may affect a feature, see the feature's Workday AI Fact Sheet.

Next Steps

Note: You can manage data contributions for Enhanced Features by Product Line or AI feature through the **Data Contribution for Workday AI** report. For any Enhanced Feature that is not included in the **Data Contribution for Workday AI** report, customers can opt out of data contribution for training and improvement by initiating a Workday support request.

Related Information
Concepts
Concept: Workday AI for Universal Main Subscription Agreement Customers

Concept: Workday AI for Universal Main Subscription Agreement Customers

Note: To determine your company's subscription agreement type:

1. Access your Community profile.
2. Beneath your name, click the **name of your company**.

In the **Subscription Service Agreement** field:

- **MSA** indicates the Main Service Agreement type.
- **UMSA** indicates the Universal Main Subscription Agreement type.

Workday often relies on data contributions to deliver artificial intelligence (AI) features. For customers who are subject to the UMSA, Workday automatically enables data contributions for AI features in your purchased SKUs. Workday may use this data to train or enhance the associated AI feature.

Note: Workday activates AI features for UMSA customers in stages:

- Workday enables AI features in the next service update, such as the weekly maintenance window.
- We populate data contributions in the **Data Contributions for Workday AI** task within 24 hours.
- We provide AI recommendations in your tenant within 14 days.

Data Contributions

UMSA customers can manage their data contributions using the **Data Contribution for Workday AI** task, secured to the *Manage: Data for ML Features* and *View: Data for ML Features* domains in the Innovation Services functional area. See Manage Workday AI Data Contributions for Universal Main Subscription Agreement Customers .

Workday groups data contributions by the AI feature that uses the data, so you only share the specific data needed for each feature. You can manage contributions for each feature individually or at the product line level.

To view the data categories needed for each AI feature, see Reference: Workday AI Data Contributions .

When you disable data contributions for an AI feature or a product line, you no longer contribute data and Workday deletes your past data contributions within 30 days.

Note:

Disabling data contributions can impact the performance of certain AI features. The impact of disabling data contributions will vary by feature, from a degraded experience to the feature not functioning at all.

To understand how disabling contributions may affect a feature, see the feature's Workday AI Fact Sheet.

Note: You can manage data contributions for Enhanced Features by Product Line or AI feature through the **Data Contribution for Workday AI** report. For any Enhanced Feature that is not included in the **Data Contribution for Workday AI** report, customers can opt out of data contribution for training and improvement by initiating a Workday support request.

These reports can also help you view contribution details:

- **AI Features Data Details**, which is secured to the *View: Data for ML Features* domain and displays the data contributions associated with all AI features available across Workday, filtered by product line.
- **Intelligent Features Report**, which is secured to the *Manage: Data for ML Features* and *View: Data for ML Features* domains and displays AI features for all SKUs and AI features for your purchased SKUs.

AI Feature Notifications

You can enable notifications about upcoming changes to AI features by configuring the *AI Features and Third Party Notification* domain in the Innovation Services functional area. See Steps: Set Up Notifications for AI Feature Data Contributions .

Members of security groups with access to the *AI Features and Third Party Notification* domain receive these notifications.

Notification Type	Delivery Timing	Purpose
AI Feature Availability	On the day of feature release.	Confirms the AI feature is available in your Production tenant and starts a 14-day period for you to manage your data contributions before data extraction begins.
Description or Technical Updates	Weekly, as initiated by changes.	Reports updates to feature descriptions and changes to data fields used by the AI feature.
Upcoming AI Features	30 days before release.	Provides a notice of upcoming AI features applicable to your purchased SKUs.

Workday doesn't extract data for the new AI feature until 14 days after the Workday release. You can disable data contributions the day of the AI feature release.

Testing AI Features

AI features that require data contributions don't function accurately in your Sandbox tenant. To test AI features that require data contributions before deploying them to your Production tenant, use your Implementation tenant.

You can use these tasks to test your configuration in your Sandbox Preview or Implementation tenants.

Task	Description
Maintain Weekly Data Contribution Activation for Implementation Tenant	Manages future weekly data extracts. After you select the **Activate for Implementation Tenant** check box to enable a feature in your Implementation tenant, we automatically run the report on Mondays to refresh data.
Run On-Demand Data Contribution Activation for Implementation Tenant	Extracts data and subscribes the tenant to future weekly extracts.

To ensure accurate testing, Workday recommends you refresh your Sandbox Preview or Implementation tenant before running these tasks. Because AI features require a certain amount of data, we might take up to 2 weeks to provide recommendations.

Related Information

Examples

Workday Community: Streamlining Feature Adoption and the Workday AI Home Page

Workday Community: Workday AI Gateway

Reference: Workday AI Data Contributions

Based on your organization's subscription service agreement, these features require you to contribute your tenant data to maximize the benefits of artificial intelligence (AI) and machine learning (ML).

- Cross Application Services: Intelligent Core Generally Available Features
- Reference: Workday AI Data Contributions
- Financials: Receipt Scanning for Expenses
- HCM: HCM Machine Learning GA Features
- HCM: Workforce Management Machine Learning Services
- Payroll: Payroll Machine Learning GA Features
- People Experience: User Experience Machine Learning
- Spend Management: Spend Management Machine Learning GA Features

Cross Application Services: Intelligent Core Generally Available Features

ML Feature	Opt-In Data Category	Considerations
Machine Learning Recommendations for Change Job	**Custom Organization Data** **Supervisory Organization Data** **Staffing Event Data** **Worker Profile Data**	Country exclusion is unavailable for the **Supervisory Organization Data** and **Custom Organization Data** categories.

Financials: Financial Management Generally Available Machine Learning Features and Third Party Services

Data Category	Consideration
Customer Payment Data	To enable Intelligent Customer Payment Matching, you must have customer payment transaction data in the past 30 days.

Data Category	Consideration
	This functionality provides beneficial recommendations only when you're processing customer payments in Workday.
Expenses Data	To use the Expense Protect feature, you need at least 10,000 expense report lines in your tenant. When users submit expenses, Expense Protect automatically evaluates them to provide risk levels, recommendations, and insights.
Journal Line Data	Before you can use the Journal Insights feature, you need at least 12 months of existing historical data.
Supplier Invoice Data	You can enable ML suggestions for your top 5 most commonly used selections for these worktags on supplier invoice lines: • Cost center • Location • Region • Spend category Note: After you opt in to the Innovation Service, you must enable worktag recommendations on supplier invoice documents in the **Supplier Accounts Options** section on the **Edit Tenant Setup – Financials** task.
Accounts Receivable Data	To enable customer overpayment reason and worktag recommendations, you need a minimum of 3,000 historical customer overpayments. To enable recommendations for customer invoice lines, you need a minimum of 3,000 customer invoices with the revenue category and sales item fields.

Financials: Receipt Scanning for Expenses

Data Category	Consideration
Receipt Scanning for Expenses	You can scan receipts in PDF, JPG, TIFF, and PNG file formats.

HCM: HCM ML Features and Third Party Connectors GA

To enable ML for these features, you must enable the **HCM ML Features and Third Party Connectors GA** service and enable data contribution for each feature.

ML Feature	ML Categories for Feature	Opt-In Data Category	Considerations
ML for Worker Profile and Skills	• **Skills Cloud** • **Skills Suggestions and Verification**	• **Job Requisition Data** • **Talent Profile Data**	• Workday recommends enabling Skills Cloud to

ML Feature	ML Categories for Feature	Opt-In Data Category	Considerations
		• **Worker Profile Data**	maintain the skills data of your workers. • Country exclusion is unavailable for the Talent Profile Data and Job Requisition Data categories. • While not required, Workday recommends you opt in to contributing data for the Skills Cloud and Skills Suggestions and Verification categories.
ML for Recruiting	• **Suggested Jobs for External Candidates** • **Suggested Skills for External Candidates** • **Suggested Skills for Job Requisitions**	**Job Requisition Data**	Country exclusion is unavailable for the Job Requisition Data category.
ML for Learning Core	• **Learning Skills Tagging** • **Machine Learning Recommended For You** • **Related Content Recommendations** • **Based on Your Skills to Develop**	**Learning Data**	• Use the **Edit Tenant Setup - HCM** task to configure the **Related Content Recommendations** worklet. • Use the **Maintain Learner Experience** task to configure the **Based on Your Skills to Develop** and **Machine Learning Recommended For You** worklets.

ML Feature	ML Categories for Feature	Opt-In Data Category	Considerations
			• You must opt into the Learning Data category to use the **Based on Your Skills to Develop** worklet. Workday provides a non-ML version of recommendations if you don't opt into it. • You must opt into the Learning Data category to use the **Related Content Recommendations** worklet. • You must opt into the Learning Data and Worker Profile Data categories to use the **Machine Learning Recommended For You** worklet. • Workday updates ML data every 24 hours, Monday through Friday.
ML for Talent Marketplace	**Talent Marketplace**	• **Demographics Data** • **Job Requisition Data** • **Learning Data** • **Projects Data** • **Skills Data** • **Talent Opportunity Marketplace Data** • **Worker Profile Data**	• Country exclusion is unavailable for the Job Requisition Data and Talent Opportunity Marketplace Data categories. • Talent Opportunity Marketplace Data and Worker Profile Data are required. For details about which features depend on these

ML Feature	ML Categories for Feature	Opt-In Data Category	Considerations
			data categories, see Steps: Set Up Talent Marketplace.
ML for Career Hub	**Career Hub**	• **Job Requisition Data** • **Learning Data** • **Talent Opportunity Marketplace Data** • **Talent Profile Data** • **Worker Profile Data** • **Skills Data**	• You must be a Career Hub customer and meet certain requirements to use this feature. Contact your Customer Success Manager for information on Career Hub. • Country exclusion is unavailable for the Job Requisition Data, Talent Opportunity Marketplace Data, and Talent Profile Data categories. • Talent Profile Data and Worker Profile Data are required. For details about which features depend on these data categories, see Steps: Set Up Career Hub.
ML for Manager Insights Hub	**Manager Insights Hub**	• **Learning Data** • **Talent Opportunity Marketplace Data** • **Worker Profile Data**	• Country exclusion is unavailable for the Talent Opportunity Marketplace Data category. • The Suggested Opportunities section of Manager Insights Hub uses ML to make personalized suggestions.

ML Feature	ML Categories for Feature	Opt-In Data Category	Considerations
			To access this functionality, opt in to the HCM Machine Learning GA Features service and relevant data categories, and enable Skills Cloud and Interests.

Note: If you enabled Skills Cloud through the Workday Graph innovation service, your data selection and Skills Cloud configuration remain valid.

You can access the **Innovation Service Data Details** report to drill into the fields tied to the HCM ML Features and Third Party Connectors GA service.

HCM: Workforce Management Machine Learning Services

Data Category	Consideration
Time Configuration Data	• You must contribute data from this category to use the Workday Time Anomaly feature. • Workday updates the data used to train the ML model weekly with all time entry template, work schedule calendar, and time calculation data.
Worker Data	• You must contribute data from this category to use the Workday Time Anomaly feature. • Workday updates the data used to train the ML model weekly with limited worker organization and job data for workers who have entered time.
Historical Schedule Block Data	• You must contribute data from this category to use the Workday Time Anomaly feature. • Workday updates the data used to train the ML model weekly with historical schedule blocks for workers.
Worker Time and Absence Data	• You must contribute data from this category to use the Workday Time Anomaly feature. • Workday updates the data used to train the ML model weekly with all workers' time block, time block history, time off entry, and time review event data.
User Feature Delivery Data	• You can contribute data in your tenant from the User Feature Delivery Data category to help Workday detect time anomalies. • To see which data from this category you're contributing, run the **Innovation**

Data Category	Consideration
	Service Data Details report for Workforce Management Machine Learning Services. • Country exclusion is unavailable for this category.

Payroll: Payroll Machine Learning GA Features

Select **Payroll: Payroll Machine Learning GA Features** from the **Innovation Services Valid for Maintain Data Opt-In** field. Select the **Opt In** check box for these categories:

Data Category	Consideration
Anomalous Payroll Results	You must contribute data from this category to use the Workday Pay Anomalies feature.
Payroll Data	• You must contribute data from this category to use the Workday Pay Anomalies feature. • We recommend that your tenant has at least 6 pay periods or more of historical payroll data before opting into this feature. This ensures there's enough training data for the ML model.
Payroll Data (Historical)	• You must contribute data from this category to use the Workday Pay Anomalies feature. • We recommend that your tenant has at least 6 pay periods or more of historical payroll data before opting into this feature. This ensures there's enough training data for the ML model.
Pay Anomalies Validations	You must contribute data from this category to use the Workday Pay Anomalies feature.
Previous States of Payroll Results (Historical)	• You must contribute data from this category to use the Workday Pay Anomalies feature. • We recommend that your tenant has at least 6 pay periods or more of historical payroll data before opting into this feature. This ensures there's enough training data for the ML model.
Worker Data	You must contribute data from this category to use the Workday Pay Anomalies feature.
P45 Tax Form Scanning	You must select this category to use the Workday P45 Tax Form Scanning feature.

Note: To enable Pay Anomalies functionality and build tenanted models, you must opt in to these categories:

- Anomalous Payroll Results
- Payroll Data
- Payroll Data (Historical)
- Pay Anomalies Validations
- Previous States of Payroll Results (Historical)
- Worker Data

Not selecting these data categories will result in the ML model failing to build and deploy as designed. The Pay Anomalies feature won't be fully functional without these models.

Workday recommends that you don't opt out of the innovation service once you run the Pay Anomalies report to view predictions. Opting out disables the feature and causes data synchronization issues.

People Experience: User Experience Machine Learning

Data Category	Consideration
Workday-Generated User Information	Workday displays the 3 recommended tasks in the **Quick Tasks** section on the home page based on: • The trends occurring across tenants. • User activity in your production tenant.
Knowledge Management Articles	You can contribute data in your tenant from the Knowledge Management Articles category, enabling Workday to recommend relevant articles to users.
Search Query	You can contribute data in your tenant from the Search Query category to provide more relevant and personalized search results when using Workday Search.

Spend Management: Spend Management Machine Learning GA Features

Data Category	Consideration
Spend Transaction Data	• If you opted in before Workday added support for purchase orders, Workday displays an **Opt In to Additional Data** check box. Select this check box to contribute data for purchase order recommendations. • When you opt out of the data contribution, Workday purges your data within 2 weeks.

Adaptive Planning: Planning GA Features

ML Feature	Data Category	Consideration
Planning Agent	Operational Telemetry and Agent Traces	Workday collects operational telemetry and agent execution traces to: • Monitor system behavior and performance. • Improve the product experience, guide manual improvements, and ensure system reliability over time. Workday doesn't use the data to retrain or fine-tune the pre-trained foundation model .

		You can disable the collection of this trace data at any time by selecting **Administration** > **General Setup** > **Disallow Data Contribution** in Adaptive Planning. Disabling the option can impact our ability to troubleshoot any unexpected behavior with agent responses.

Related Information

Examples

Workday Community: Workday Innovation Services

FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)

- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)
- FAQ: Transitioning from Innovation Services Addendum (ISA) to the Universal Main Subscription Agreement (UMSA)

Why can I no longer access Innovation Services reports and security domains?	When you sign the Universal Main Subscription Agreement (UMSA), Workday replaces the reports, tasks, and security domains for managing Innovation Services with those for managing Workday AI (artificial intelligence) features on the UMSA. See Concept: Workday AI for Universal Main Subscription Agreement Customers Example: Rather than using the **Innovation Services and Data Selection Opt-In** report (secured to the *Manage: Innovation Services* domain)

	to manage Workday AI features, you'll use the **Data Contribution for Workday AI** report (secured to the *Manage: Data for ML Features* and *View: Data for ML Features* domains). UMSA customers can disregard all information regarding Innovation Services.
Do I need to opt in to Workday AI features on the UMSA, as I did on the Innovation Services Addendum (ISA)?	Most AI and third-party integration features are automatically available under the UMSA. To manage these features, see Manage Workday AI Data Contributions for Universal Main Subscription Agreement Customers .
How do I validate that features I enabled under the ISA remain enabled under the UMSA?	Access the **Data Contribution for Workday AI** report (secured to the *Manage: Data for ML Features* and *View: Data for ML Features* domains) to review Workday AI features enabled under the UMSA and ensure that default settings meet your organization's needs. For instructions on managing feature enablement, see Manage Workday AI Data Contributions for Universal Main Subscription Agreement Customers . For considerations on the impact of managing your features, see Reference: Workday AI Data Contributions .
How do I validate that third-party integrations enabled under the ISA are enabled under the UMSA?	To validate integrations that used Innovation Services, access the **All Integration Systems** report (secured to the *Integration Reports* domain) to confirm their status.
Is data contribution for Intelligent Application features enabled by default under UMSA?	Workday enables data contribution for Intelligent Application features by default.
How can I opt out of data contribution for Workday AI features?	If you want to disable data contribution, you can use the **Data Contribution for Workday AI** report (secured to the *Manage: Data for ML Features* and *View: Data for ML Features* domains) to opt out of specific product lines or individual features. Note: If an Intelligent Application doesn't require data contributions, there's nothing to disable. Note: You can manage data contributions for Enhanced Features by Product Line or AI feature through the **Data Contribution for Workday AI** report. For any Enhanced Feature that is not included in the **Data Contribution for Workday AI** report, customers can opt out of data contribution for training and improvement by initiating a Workday support request.
How has security configuration changed for AI features under UMSA?	Workday updated the security domains. You must ensure you have enabled the relevant security

	groups and added them to the *Manage: Data for ML Features* and *View: Data for ML Features* domains. These domains replace the previous *Manage: Innovation Services* domain.
How can I see the specific data Workday uses for AI features?	Click **View Data Collected** on the **Data Contribution for Workday AI** report (secured to the *Manage: Data for ML Features* and *View: Data for ML Features* domains) to access these details.
How does Workday notify me about new or updated AI features?	If you have enabled notifications about upcoming changes to AI features, Workday sends a 30-day notification before delivering new or updated AI features to your preview and production tenants. See Steps: Set Up Notifications for AI Feature Data Contributions .
What happened to the Media Cloud Addendum? Does my existing content (like SCORM/AICC files) still work?	Yes, your existing packaged content will continue to operate. The legal and contractual terms have shifted from the old addendum to the relevant terms within the Platform and Product Extensions Product Terms under your UMSA.
What configurations do I need to review for Workday Learning?	If you use third-party content, you must verify your **Learner Name** configuration to ensure content launches correctly. After transitioning to UMSA, access the **Edit Tenant Setup - HCM** task and select the **Send Learner Name to Third-Party Content Provider** check box. See Steps: Set Up Packaged Content for Learning.
How do I submit support requests for subscription management (such as new licenses)?	In Workday Community, route subscription management requests, like new licenses, as a Customer Success Request.