

IA Workday

Product Summary

August 17, 2026



Contents

Agents.....	3
Agent Système d'enregistrement.....	3
Gestion des agents.....	3
Agents externes.....	14
Sécurité et conformité des agents.....	20
Agent Gateway.....	27
Agent Marketplace.....	30
Concept : Agent Marketplace.....	30
Concept : liste des agents dans Workday Marketplace.....	31
Agents prédéfinis par Workday.....	32
Agent Optimisation des processus de gestion.....	32
Agent Paie.....	41
Agent Libre-Service Sana.....	50
 Sana pour Workday.....	 92
Concept : espace de travail Sana.....	92
Étapes : définir Sana pour Workday.....	93
Définir les autorisations de sécurité de l'administrateur de l'IA.....	96
 Console de consommation de la plateforme.....	 100
Définir la sécurité pour la console de consommation de la plateforme.....	100
Concept : console de consommation de la plateforme.....	100
 Contributions de données d'IA.....	 102
Étapes : définir les notifications pour les contributions de données de la fonctionnalité d'IA.....	102
Activer la fonctionnalité Innovation Services et les contributions de données IA pour les clients MSA...	103
Gérer les contributions de données Workday AI pour les clients de l'accord d'abonnement principal universel.....	105
Concept : Workday AI pour les clients d'un contrat d'abonnement principal universel.....	106
Référence : contributions de données Workday AI.....	108
FAQ : Transition de l'addendum Innovation Services (ISA) à l'Accord principal universel d'abonnement (UMSA).....	117

Agents

Agent Système d'enregistrement

Gestion des agents

Éléments de définition : agent Système d'enregistrement

Cette thème peut vous aider à prendre les bonnes décisions lors de la planification de la configuration et de l'utilisation de l'agent Système d'enregistrement. Elle explique :

- Pourquoi effectuer cette configuration.
- Comment cette configuration s'intègre dans Workday.
- Les impacts en aval, ainsi que les interactions entre produits.
- Les conditions requises en matière de sécurité et les configurations du processus de gestion.
- Les questions à se poser et les limites à prendre en compte avant l'implémentation.

Reportez-vous aux instructions détaillées des tâches pour avoir une vision exhaustive de la configuration.

Présentation

L'agent Système d'enregistrement Workday (ASOR) est une plateforme centralisée qui vous permet de gérer le personnel agentique numérique de votre organisation en fournissant une seule solution que vous pouvez utiliser pour :

- Découvrez, ajoutez, enregistrez, configurez, contrôlez et gérez votre plage d'agents IA en toute sécurité à grande échelle sur différents systèmes.
- Bénéficiez d'un centre de contrôle unique pour la gouvernance, la sécurité et l'audit de vos agents, et ainsi réduire les coûts indirects (rate) administratifs et atténuer les risques liés à la sécurité.
- Afficher des analyses de données sur la visibilité, l'utilisation et les performances des agents, ce qui vous permet d'analyser et de démontrer la valeur et l'impact de vos agents.

Vous pouvez gérer les types d'agent suivants via le **hub Gestion des agents** , quel que soit l'endroit où ils sont développés et exécutés :

- Agents prédéfinis par Workday (1P)
- Agents créés avec des partenaires
- Agents auto-configurés (3P)

Dans ASOR, le **Hub Gestion des agents** constitue le site centralisé où vous pouvez enregistrer, configurer, contrôler et gérer vos agents IA. Un agent est un système qui utilise un grand modèle de langage (LLM) pour raisonner et effectuer une action.

Chaque agent dans ASOR a une définition d'agent. Cette définition fournit une représentation concrète du code de l'agent, offrant aux administrateurs une transparence sur ce qu'est un agent et sur ce qu'il peut faire. Chaque définition d'agent dans ASOR de Workday contient :

- **Nom de l'agent** : nom de l'agent.
- **Description de l'agent** : description abrégée de l'agent.

- **Aptitudes** : tâches ou activités que l'agent peut exécuter.
 - **Modes d'exécution** : nous prenons en charge deux modes d'exécution pour les aptitudes de l'agent :
 - Mode ambigu : l'agent effectue des tâches pour lui-même et la sécurité est évaluée à l'aide de ses propres autorisations.
 - Mode délégataire : l'agent effectue des tâches pour le compte d'un être humain. Pour cela, la sécurité est évaluée en utilisant les autorisations de l'employé.
 - **Outils** : ressources que l'agent peut utiliser lors de l'exécution de l'aptitude. Pour les agents qui interagissent avec Workday, les outils seront des API Workday.
 - **Ressources** : type d'API utilisé par un outil. Exemples : REST, SOAP, Graph, WQL.

Avantages pour l'entreprise

- **Une efficacité administrative accrue** : fournit un centre de contrôle unique pour la gouvernance et l'audit, ce qui garantit le déploiement sécurisé des agents à grande échelle.
- **Transparence opérationnelle** : offre des analyses sur l'activité, l'utilisation et la performance des agents afin de vous aider à analyser la valeur et l'impact de votre personnel IA.
- **Stabilité du système** : protège les performances du système, tout en garantissant la sécurité des agents avec une authentification et un audit standardisés.
- **Interopérabilité des agents** : aptitude aux agents d'interagir avec l'ensemble des systèmes pour terminé le travail.

Cas d'utilisation au cours du cycle de vie de l'agent

Vous pouvez utiliser l'ASOR et le hub Gestion des agents pour gérer vos agents tout au long du cycle de vie des agents, qui comprend les 5 phases suivantes :

- **Définir** : vous pouvez afficher la définition d'agent d'un agent sur la page de son profil d'agent dans **le hub Gestion des agents**. Pour les agents externes, vous fournissez une définition de votre agent via API.
- **Enregistrer** : pour commencer à utiliser un agent, vous devez d'abord l'enregistrer dans **le hub Gestion des agents** afin de le préparer à la configuration et à l'activation. Pour pouvoir vous enregistrer dans les agents prédéfinis par Workday en production, vous devez satisfaire aux conditions suivantes :
 - uMSA
 - [Politique relative aux crédits variables et aux droits à la plateforme Workday](#)
 - Droits d'utilisation des produits Workday
- **Configurer** : lorsque vous configurez un agent, vous pouvez spécifier les aptitudes qu'il utilisera et les personnes autorisées à y accéder.
- **Activer** : une fois que vous avez enregistré et configuré votre agent, vous pouvez l'activer, ce qui permet aux utilisateurs d'interagir avec lui en fonction des autorisations de sécurité que vous avez configurées.
- **Désactiver** : lorsque vous n'avez plus besoin d'un agent, vous pouvez le désactiver. Ainsi, l'agent est masqué pour les utilisateurs, mais il reste accessible dans **le hub Gestion des agents**, où vous pouvez le réactiver ultérieurement si nécessaire.

Recommandations

- **Consultez le rapport View Security for Agent Skill lors de la configuration des agents** : utilisez ce rapport pour mettre en évidence les configurations de règle de sécurité de domaine et de règle de sécurité du processus de gestion que les API et ressources Workday peuvent utiliser. Lors de l'exécution, Workday évalue d'abord les groupes de sécurité ayant accès à l'agent (Disponible pour), puis les groupes de sécurité ayant accès aux outils (règles de domaine ou de processus de gestion pour les API et les ressources).

- **Révision de la piste d'audit** : examine régulièrement le journal d'audit pour connaître les actions de l'agent. Le journal fait la distinction entre un agent environnement client agissant en lui-même et un agent déléguer agissant pour le compte d'un utilisateur spécifique.

Actions requises

Pour accéder à ASOR, vous n'avez pas besoin de SKU supplémentaires.

Pour enregistrer et utiliser entièrement des agents dans Agent System of Record dans vos environnements clients de production, votre équipe de compte Workday doit :

- Activez l' [UMSA \(UMSA\)](#) .
- Activez la [politique de crédits variables et de droits à la plateforme de Workday](#) .

Remarque : Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser d'agents en production tant que vous n'avez pas accepté ces contrats. L'UMSA est obligatoire pour les environnements clients hors production et de production pour les agents prédéfinis par Workday. L'UMSA n'est pas obligatoire pour les environnements clients hors production pour les agents auto-configurés.

Limites

- **Agent Proxy et Délégation** : les interactions de l'agent Workday ne peuvent être ni proxy ni déléguées.
- **Gestion de clé** : pendant qu'ASOR gère la création et le stockage sécurisé des identifiants clients (clé privée) dans le magasin d'identifiants, vous devez vous assurer que votre environnement de sécurité contribue à le processus OAuth 2.0 token-exchange qui utilise cette paire de clés.
- **Analyses d'utilisation dans les environnements clients sandbox** : pour les analyses d'utilisation de l'agent sur la page d'aperçu, l' actualiser de l'environnement sandbox n'efface pas les activités d'utilisation des semaines précédentes.

Sécurité ASOR

Domaines	Éléments à prendre en compte
Conformité de l'agent	Donne accès aux rapports et données obligatoire pour garantir la conformité de l'agent.
Hub Gestion des agents	Donne accès au Hub Gestion des agents, le hub centralisé pour afficher et gérer tous les agents.
Manage: Agents	Ce domaine permet d'accéder aux tâches de gestion des agents, notamment la configuration des, l'activation et la désactivation dans ASOR.
Reports: Agent Reporting	Ce domaine permet d'afficher des analyses sur les agents ainsi que des sources de données et des filtres de rapport pour les rapports au niveau de l'agent.
Reports: AI Agent Security	Donne accès aux rapports sur les informations de sécurité des agents. Exemple : rapport View AI Agent User Audit Trail .
Setup: Agents	Donne accès aux tâches et activités de définition des agents dans ASOR.

Sécurité de l'agent

Lorsque vous configurez vos agents, vous pouvez spécifier qui a accès pour interagir avec l'agent en fournissant des groupes de sécurité dans la colonne **Disponible** pour pour chaque aptitude en mode d'exécution délégué. Exemple : vous pouvez spécifier *Salarié (pour lui-même)* afin de mettre une aptitude à disposition d'un salarié qui interagit avec l'agent. Tant qu'un utilisateur fait partie de l'un des groupes de sécurité pour l'une des aptitudes, il aura le droit d'interagir avec l'agent.

Remarque : Les autorisations de sécurité interaction l'agent sont distinctes des autorisations d'exécution de l'outil. Réfléchissez à l'évaluation de l'alignement entre les groupes de sécurité dans l'invite **Disponible pour** et les groupes de sécurité disposant des autorisations pour les **outils** que l'agent peut exécuter à l'aide du rapport **Afficher la sécurité des aptitudes de l'agent**. Ce rapport affiche des informations détaillées sur les API Outils de l'agent, ainsi que les règles de sécurité et les autorisations respectives du domaine ou du processus de gestion. Les groupes de sécurité interaction l'agent ne doivent pas nécessairement être une correspondance 1:1 avec les groupes de sécurité dans les règles API. Pour que l'exécution de l'outil réussisse, un utilisateur doit être membre d'un groupe de sécurité sur l'aptitude de l'agent et d'un autre sur les règles de sécurité de API. Au moment de l'exécution de l'agent, Workday évalue à la fois l'accès utilisateur à l'agent et l'accès utilisateur aux API qu'il exécute en tant qu'outils.

Exemple :

Agent	Disponible pour le groupe de sécurité	Configuration de groupe de sécurité de règle de sécurité de domaine	Exécution de l'outil réussie
Agent Libre-service	Salarié (pour lui-même)	Salarié (pour lui-même)	Oui
Agent Libre-service	Salarié (pour lui-même)	Responsables	Non

Remarque : Les aptitudes en mode d'exécution ambigus ne nécessitent pas d'accès interaction, car elles effectuent des actions sans interaction manuelle, généralement sur un calendrier ou un déclencheur défini.

Vous pouvez accéder au rapport **Tous les comptes d'agents IA** sécurisé via le domaine *Domains: Workday Accounts* dans le domaine domaine fonctionnel System pour afficher tous les comptes d'agent dans votre environnement client. Dans le rapport, vous pouvez cliquer sur les actions associées **du Compte Workday** pour afficher les pistes d'audit.

Les comptes Utilisateur système d'agent (ASU) vous permettent de sécuriser et de gérer vos agents dans Workday. Workday génère automatiquement un ASU pour votre agent une fois que vous avez terminé la tâche **Configurer l'agent**. Vous pouvez afficher vos comptes ASU de vos agents à l'aide de la tâche **Tous les comptes d'agents IA** (sécurisé via le domaine Workday Accounts dans le domaine fonctionnel System). Vous pouvez également afficher les comptes d'agents IA à l'aide de la tâche **Tous les comptes Workday**.

Les développeurs d'agents peuvent utiliser les ASU pour interagir avec les données Workday via Agent Gateway.

Reporting

La section **Aperçu** du hub permet d'accéder aux rapports (sécurisé via le domaine *Reports: Agent Reporting*) et aux tâches (sécurisé via le domaine *Manage: Agents*) suivants :

- Rapport **Agents actifs**
- tâche **Activer les agents**
- **Configurer** la tâche de l'agent
- Désactiver la tâche **Désactiver l'agent**
- Rapport **Nombre total de sessions de l'agent au fil du temps** (disponible uniquement pour les agents Workday)
- Rapport **Total des sessions de l'agent** (disponible uniquement pour les agents Workday)

- Rapport **Nombre total d'utilisateurs uniques** (disponible uniquement pour les agents Workday)

La section **Registre de l'agent** affiche vos agents enregistrés, ainsi que leur statut et la date à laquelle un administrateur de Workday a effectué des mises à jour pour la dernière fois à leur configuration.

Vous pouvez cliquer sur le nom d'un agent pour afficher le profil de l'agent, les aptitudes disponibles pour l'agent et les rapports d'analyse de l'agent suivants (sécurisé via le domaine *Reports: Agent Reporting* et uniquement disponibles pour les agents prédéfinis par Workday) :

- **Sessions de l'agent**
- **Interactions d'aptitudes**
- **Total des interactions d'aptitude au fil du temps**
- **Nombre total d'utilisateurs uniques pour l'agent**
- **Nombre total d'utilisateurs uniques pour les aptitudes**

La section **Agents Workday non enregistrés** affiche le rapport **Rechercher des agents Workday non enregistrés** (sécurisé via le domaine *Agent Management Hub*), dans lequel vous pouvez découvrir les agents prédéfinis par Workday que vous êtes éligible à enregistrer.

Vous pouvez accéder aux rapports suivants pour la sécurité, la conformité et l'audit des agents :

- **Détail de la demande d'entrées/sorties de l'agent** (sécurisé via le domaine *Conformité de l'agent* et uniquement disponible pour les agents prédéfinis par Workday)
- **Tous les comptes d'agents IA** (sécurisé via le domaine *Workday Accounts*)
- **Générer un rapport des entrées et des sorties de l'agent** (sécurisé via le domaine *Conformité de l'agent* et uniquement disponible pour les agents prédéfinis par Workday)
- **Input and Output Report For Registered Agents** (sécurisé via le domaine *Agent Compliance* et uniquement disponible pour les agents prédéfinis par Workday)
- **Afficher la piste d'audit des utilisateurs de l'agent IA** (sécurisé via le domaine *Reports: AI Agent Security*)
- **Afficher la sécurité des aptitudes de l'agent** (sécurisé via le domaine *Security Administration* et le domaine *Manage: Agents*)

Pour les rapports avec des agents supplémentaires, vous pouvez accéder aux sources de données suivantes :

- **Toutes les définitions d'agent** (sécurisé via le domaine *Reports: Agent Reporting*) qui fournissent des champs pour la génération de rapports sur toutes les définitions d'agents enregistrées et non enregistrées.
- source de données **Tous les enregistrements d'agent** (sécurisé via le domaine *Reports: Agent Reporting*) que vous pouvez utiliser dans les rapports personnalisés pour analyser les enregistrements d'agent.
- source de données **Agent Input and Output Details** (sécurisé via le domaine *Agent Compliance*) que vous pouvez utiliser pour afficher les interactions des entrées et sorties de votre agent au cours des 30 derniers jours.

Vous pouvez également utiliser les sources de données suivantes (sécurisé via le domaine *Reports: Agent Reporting*) qui fournissent des données d'analyses d'utilisation pour les 30 derniers jours :

- **Sessions de l'agent par jour**
- **Interactions avec les aptitudes de l'agent**
- **Interactions avec les aptitudes de l'agent par jour**
- **Agent Utilisateurs uniques par aptitudes**

Relations et interactions

Workday propose un kit appelé Touchpoints Kit, qui rassemble plusieurs ressources pour vous aider à mieux comprendre les relations de configuration dans votre environnement client. Pour en savoir plus sur ce kit, visitez notre page [Workday Touchpoints Kit](#) sur le site Workday Community.

Définir l'agent Système d'enregistrement

Prerequisites

Sécurité : domaine *Security Configuration* dans le domaine fonctionnel System. Requis pour configurer les domaines de sécurité ASOR.

Context

Vous pouvez gérer le personnel numérique de votre organisation à l'aide de l'agent Système d'enregistrement (ASOR). Pour définir la règle ASOR dans votre environnement client, vous devez :

- Activez le domaine fonctionnel ASOR.
- Configurez les règles de sécurité des domaine pour les tâches et rapports ASOR.

Vous devez définir et configurer ASOR dans chacun de vos environnements clients, car il n'existe aucune méthode actuelle pour migrer les configurations.

Steps

1. Accédez à la tâche **Maintain Functional Areas**.
Cochez la case à cocher **Activé** pour le domaine fonctionnel Agent System of Record.
Cliquez sur **OK**, puis sur **Terminé**.
2. Accédez à la tâche **Activate Pending Security Policy Changes**.
Saisissez un commentaire et cliquez sur **OK**.
Cochez la case **Confirmer**, puis cliquez sur **OK**.
3. Accédez au rapport **Règles de sécurité des domaines par domaine fonctionnel**.
Dans l'invite **Domaine fonctionnel**, sélectionnez *Agent System of Record*.
Sélectionnez **Règle de sécurité de domaine > Activer** dans le menu des actions associées des domaines suivants :
 - *Conformité de l'agent*
 - *Hub Gestion des agents*
 - *Manage: Agents*
 - *Reports: Agent Reporting*
 - *Setup: Agents*

Répétez cette étape pour le domaine *Reports: AI Agent Security* dans le domaine fonctionnel System.

4. Accédez à la tâche **Maintain Permissions for Security Group** .

Sélectionnez l'opération *Mettre à jour* .

Dans l'invite **Groupe de sécurité source** , sélectionnez le groupe de sécurité auquel vous souhaitez subvention l'accès à la gestion de l'agent ASOR.

Note: Actuellement, vous pouvez uniquement configurer des groupes non limités dans les règles de sécurité ASOR.

Dans l'onglet **Autorisations de règle de sécurité de domaine** , fournissez les autorisations *Afficher et Modifier* pour les règles de sécurité des domaine suivants :

- *Conformité de l'agent* : accès aux rapports et aux données obligatoire pour la conformité de l'agent.
- *Hub Gestion des agents* : accès au **Hub Gestion des agents** , le hub centralisé pour afficher et gérer tous les agents.
- *Gérer les agents* : accéder aux tâches relatives à la gestion des agents, notamment la configuration, l'activation et la désactivation dans ASOR.
- *Reports: Agent Reporting* : permet d'afficher des analyses sur les agents, ainsi que des sources de données et des filtres de rapport pour les rapports au niveau de l'agent.
- *Reports: AI Agent Security* : permet d'accéder aux rapports sur les informations de sécurité de l'agent IA. Exemple : rapport **View AI Agent User Audit Trail** .
- *Setup: Agents* : accès aux tâches et activités de définition des agents dans ASOR.

5. Accédez à la tâche **Activate Pending Security Policy Changes**.

Saisissez un commentaire et cliquez sur **OK**.

Cochez la case **Confirmer**, puis cliquez sur **OK**.

Enregistrer et configurer des agents prédéfinis par Workday

Prerequisites

Note: Des étapes supplémentaires peuvent être nécessaires pour enregistrer et utiliser des agents dans les environnements clients de production en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services (MSA), soit sur le Contrat-cadre de services universel (UMSA). Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().
4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- *UMSA* , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- *MSA* , votre organisation doit activer le système UMSA.

Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser d'agents en production tant que vous n'avez pas accepté ces contrats. L'UMSA est obligatoire pour les environnements clients hors production et de production pour les agents Workday-Built. L'UMSA n'est pas obligatoire pour les environnements clients hors production pour les agents auto-configurés.

- Activez la [politique de crédits variables et de droits à la plateforme de Workday](#) . obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production.
- Définissez l'agent [Système d'enregistrement](#) .

Sécurité : les domaines suivants dans le domaine fonctionnel Agent System of Record :

- *Conformité de l'agent*
- *Hub Gestion des agents*
- *Manage: Agents*
- *Reports: Agent Reporting*
- *Setup: Agents*

Sécurité : domaine *Reports: AI Agent Security* dans le domaine fonctionnel System.

Context

Vous pouvez enregistrer, configurer, activer et désactiver des agents Workday à l'aide du **Hub Gestion des agents** .

Steps

1. Accédez au rapport **Hub Gestion des agents** .
2. Sélectionnez l'onglet **Agent Workday non enregistré** .
3. Cliquez sur **Enregistrer** l'agent que vous souhaitez enregistrer.
Vous pouvez uniquement enregistrer des agents dans les SKU obtenus par votre organisation.
4. Cochez la case à cocher **Confirmer** , puis cliquez sur **OK** pour finaliser l'enregistrement.
Workday déplace l'agent vers l'onglet **Agent Register** .
5. Sélectionnez l'onglet **Registre de l'agent** , puis cliquez sur le nom de l'agent pour configurer l'agent.
6. Dans la vue du profil de l'agent, cliquez sur **Configurer l'agent** .
7. Dans la colonne **Statut** , rendez chaque aptitude pertinente disponible en activant le carrousel à bascule .
8. Pour chaque **aptitude** activée , renseignez l'invite **Disponible pour** avec les groupes de sécurité auxquels vous voulez autoriser l'accès pour cette aptitude spécifique. Les groupes de sécurité ajoutés à l'invite **Disponible pour** d'un agent établissent la règle interaction de l'agent.

Note: Les groupes de sécurité que vous sélectionnez dans l'invite **Disponible pour** doivent également disposer d'autorisations sur les règles de sécurité du domaine ou du processus de gestion qui sécurisent les outils des agents. Vous pouvez utiliser le rapport **Afficher la sécurité des aptitudes de l'agent** pour vous aider à configurer vos agents. Ce rapport affiche des informations détaillées sur les API Outils de l'agent et les règles de sécurité et autorisations respectives du domaine ou du processus de gestion . Au moment de l'exécution de l'agent, Workday évalue à la fois l'accès utilisateur à l'agent et l'accès utilisateur aux API qu'il exécute en tant qu'outils.
9. Cliquez sur **Activer** . Vous pouvez également enregistrer et revenir à cette configuration.
La configuration de l'agent peut être mise à jour à tout moment. Lorsque vous activez un agent, l'ASU de l'agent s'active également automatiquement.
10. (Facultatif) Lorsque vous avez terminé avec votre agent, vous pouvez cliquer sur **Désactiver** pour le désactiver.
Vous pouvez activer, désactiver et réactiver vos agents à tout moment dans le **Hub Gestion des agents** . Lorsque vous désactivez un agent, l'ASU de l'agent est également désactivé automatiquement.

Référence : exemple de définition de l'agent API ASOR

La première section de cette API définit les informations de base sur votre 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_AGENTSPEACE"
},
"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": "c2fffb30053964fbfa7a46dcfa577adb1"
        }
      },
      {
        "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"
}

```

La deuxième section de cette API est facultative. Il inclut des informations spécifiques de Workday, notamment les API qui seront appelées dans le cadre de cet 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"
}
```

Chaque aptitude peut avoir plusieurs outils. Chaque outil pointe sur une ressource Workday spécifique, que vous pouvez spécifier à l'aide de l'identifiant Workday (identifiant Workday) de la ressource.

Sample Response

Une fois que vous avez enregistré un agent via l' API, vous devez recevoir une réponse JSON :

```
{
  "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_AGENTSPEACE"
  },
  "name": "Change Business Title Agent",
  "supportsAuthenticatedExtendedCard": false
}

```

La réponse contient un identifiant en haut, qui est votre identifiant Workday de référence si vous devez extraire la définition de l'agent à l'aide de l' API agent Definition .

Agents externes

Inscrire des agents externes

Conditions préalables

Note: Des étapes supplémentaires peuvent être nécessaires pour activer cette fonctionnalité en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services (MSA), soit sur le Contrat-cadre de services universel (UMSA). Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().
4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- *UMSA* , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- *MSA* , votre organisation doit activer le système UMSA.

Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser d'agents en production tant que vous n'avez pas accepté ces contrats. L'UMSA est obligatoire pour les environnements clients hors production et de production pour les agents Workday-Built. L'UMSA n'est pas obligatoire pour les environnements clients hors production pour les agents auto-configurés.

[Définissez l'agent Système d'enregistrement](#) .

Sécurité :

- domaine *Agent Management Hub* dans le domaine fonctionnel Agent System of Record. Obligatoire pour vérifier que l'agent est enregistré dans Workday.
- domaine *Manage Agents* dans le domaine fonctionnel Agent System of Record. Obligatoire pour l'activation et la configuration des aptitudes .
- Domaine *Set Up: Tenant Setup - Security* dans le domaine fonctionnel System. Obligatoire pour l'inscription.

Contexte

Actuellement, vous pouvez uniquement enregistrer et définir des agents externes dans Workday à l'aide de l' API ASOR. Les agents externes sont définis et enregistrés simultanément à l'aide de l' API. Il ne s'agit pas de deux étapes distinctes. Vous pouvez utiliser n'importe quel client API de votre choix pour appeler l' API.

Reportez-vous à [la documentation sur API ASOR v1.2 sur Github](#) et [l'exemple de documentation ASOR JSON](#) Pour la résolution des problèmes.

Points de terminaison d'enregistrement :

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

Pour plus d'informations sur la disponibilité en dehors des États-Unis, reportez-vous à la documentation Agent Gateway : [Référence : disponibilité de Agent Gateway dans certaines régions](#) .

Options d'authentification :

Pour enregistrer des agents externes, vous avez besoin d'un jeton d'accès dans votre invocation de API ASOR. Vous trouverez ci-dessous les différentes options permettant d'obtenir un jeton pour appeler l'appel API ASOR.

Option 1 : authentifier manuellement un client API

1. Accédez à la tâche **Register API Client** .

- **Nom du client** : saisissez un nom unique pour identifier votre agent. Nous vous recommandons d'utiliser un client distinct pour chaque agent afin de faciliter leur gestion.
- **Client Grant Type:** *Authorization Code Grant* .
- **Access Token Type:** *Career* .
- **Redirection URI** : saisissez une URL vers laquelle rediriger les utilisateurs après autorisation.
- **Périmètre (domaines fonctionnels)** : *Agent Système d'enregistrement* .
- **Inclure un périmètre prédéfini par Workday** : cochez cette case à cocher.

2. Copiez et enregistrez les valeurs **Identifiant client** et **Clé secrète client** . Vous pouvez les utiliser pour obtenir un jeton d'accès afin d'appeler l' API de définition .

3. Collez cette URL dans une nouvelle fenêtre. Cela devrait vous rediriger vers google.com avec un code ajouté que vous pouvez utiliser pour appeler l' API:

`https://us.agent.workday.com/auth/authorize/<Tenant_Name>?response_type=code&client_id=<client_id>&state=test3pagent1&redirect_uri=<redirect_uri>`

4. Créer une nouvelle demande à l'aide d'un client API externe (par exemple, Duo) : `https://<tenantHost>/ccx/oauth2/<tenantName>/jeton`

- Corps :
`Grant_type=authorization_code&code=<authorizationCode>&client_id=<clientID>&client_secret=<ClientSecret>`
- Authentification : nom d'utilisateur = `<ClientID>` , mot de passe = `<ClientSecret>` .
- Cela génère un jeton d'accès et un jeton actualiser que vous pouvez utiliser pour appeler l' API de définition de l'agent ASOR.
- Pour cette étape, tenez compte des éléments suivants : [Concept : éléments à prendre en compte avec l'agent ASU externe](#) .

Note: L'utilisateur enregistrement l'agent doit avoir accès au domaine *Setup: Agents* dans le domaine domaine fonctionnel Agent System of Record pour enregistrer un agent à l'aide de l' API ASOR.

Option 2 : s'authentifier avec Extend

Si vous êtes un utilisateur Workday Extend ou Workday Orchestrate, vous pouvez récupérer un jeton d'accès via le site de développement de Workday.

1. Accédez à development.workday.com et connectez-vous.
2. En haut à droite, cliquez sur le menu utilisateur. Le menu doit afficher le nom actuel de votre unité légale .
3. Cliquez sur **Environnement client > Connexion à l'environnement client**.
4. Sélectionnez votre environnement et environnement client , puis cliquez sur **Se connecter à l'environnement client** .
5. Connectez-vous à l' environnement client. Vous devez vous connecter avec un compte ayant accès au *domaine Setup: Agents* dans le domaine domaine fonctionnel Agent System of Record pour enregistrer un agent à l'aide de l' API ASOR.

Enregistrer un agent externe à l'aide de l' API ASOR

Prérequis :

- jeton d'accès pour un compte ayant accès au domaine *Setup: Agents* dans le domaine fonctionnel Agent System of Record.
- Un client API de votre choix.

- Sécurité : domaines suivants dans le domaine fonctionnel System :
 - *Custom Report Creation*
 - *Manage: All Custom Reports*
 - *Report Tag Management*

Contexte :

Pour enregistrer un agent externe, vous devez :

- Recherchez les identifiants Workday des API Workday (SOAP et REST) pertinentes que vous prévoyez d'inclure dans la définition des outils de votre agent en créant un rapport personnalisé.
- Recherchez le fournisseur d'agents à l'aide de la tâche **Afficher un fournisseur d'agents**.
- Appelez l' API REST ASOR

Recherche d'identifiants Workday SOAP et REST pour la définition d'outils de l'agent

1. Accédez à la tâche **Créer un rapport personnalisé**.
2. Pour créer le rapport, tenez compte des éléments suivants :

Option	Description
Type de rapport	Sélectionnez <i>Avancé</i> .
Optimisé pour les performances	Désélectionnez la case à cocher.
Source de données	Sélectionnez <i>Public Web Services for SOAP</i> et <i>All Public Service Operations</i> pour les API REST.

3. Pour les API SOAP : sur la page **Modifier un rapport personnalisé**, dans l'onglet **Colonnes** de la définition du rapport, ajoutez les lignes suivantes :

Objet de gestion	Champ
<i>Service web</i>	Service web
<i>Opération du service web</i>	Nom de l'opération du service web
<i>Opération du service web</i>	Identifiant Workday

4. Pour les API REST : sur la page **Modifier un rapport personnalisé**, dans l'onglet **Colonnes** de la définition du rapport, ajoutez les lignes suivantes :

Objet de gestion	Champ
<i>Opération de service</i>	Service
<i>Opération de service</i>	Nom
<i>Opération de service</i>	Identifiant Workday

5. Enregistrez et exécutez le rapport.

Note: Lorsque vous récupérez les identifiants Workday pour vos API, vous pouvez également faire référence aux listes suivantes :

- [Identifiant Workday de API REST](#)
- [API REST non disponibles pour les agents ambigus](#)
- [Identifiant Workday de API Graph](#)

Rechercher le fournisseur d'agents

Les fournisseurs d'agents font référence à la personne qui a conçu l'agent et qui sont affichés dans le champ **Création par** du profil de l'agent.

1. Accédez à la tâche **View Agent Provider** , sécurisé via le domaine *Setup: Agents* dans le domaine fonctionnel Agent System of Record .
2. Utilisez le code de l'organisme dans votre appel API d'enregistrement de l'agent.

Rechercher la plateforme de l'agent

Les plateformes d'agents font référence à la plateforme ou au système externe sur lequel l'agent est développé et exécuté et qui sont affichées dans le champ **Création** sur le profil de l'agent.

1. Accédez à la tâche **View Agent Platforms** , sécurisé via le domaine *Setup Agents* dans le domaine fonctionnel Agent System of Record.
2. Utilisez l'identifiant de la plateforme dans l'appel API d'enregistrement de l'agent.

Appelez l' API REST ASOR

Créez une nouvelle demande pour enregistrer votre agent à l'aide d'un client API externe, Exemple : Carlos.

Pour créer la demande, tenez compte des éléments suivants :

- **Endpoint:** <https://us.agent.workday.com/asor/v1/agentDefinition>
- **Opération :** POST
- **Corps du message :** Reportez-vous à [la documentation API ASOR v1.2 sur Github](#) et à [l'exemple de documentation ASOR JSON SREE](#) .
- **En-têtes :**
 - Autorisation : porteur < jeton >
 - wd-agent-tenant-alias:<votre nom de l'environnement client>

Hub Gestion des agents

Une fois que vous avez chargé votre définition d'agent dans Workday, vous pouvez vérifier qu'elle est enregistrée en l'affichant dans le **hub Gestion des agents** .

1. Accédez au rapport **Hub Gestion des agents** .
2. Cliquez sur **Registre de l'agent** pour afficher la liste de vos agents.
3. Cliquez sur un agent pour afficher ses informations d'aperçu.

Étapes suivantes

Configurez votre agent dans Workday.

Related Information

Reference

Référence : [exemple de définition de l'agent API ASOR](#)

Configurer des agents externes

Prerequisites

[Définir l'agent Système d'enregistrement](#)

Sécurité : les domaines suivants dans le domaine fonctionnel Agent System of Record :

- *Conformité de l'agent*
- *Hub Gestion des agents*
- *Manage: Agents*
- *Reports: Agent Reporting*
- *Setup: Agents*

Sécurité : domaine *Reports: AI Agent Security* dans le domaine fonctionnel System.

Pour les agents en mode ambigu suivants uniquement :

- [../././././authentication-and-security/security-for-integrations/access-to-external-endpoints/hzp1471450668309.dita](https://hwp1471450668309.dita). Sécurité : domaine *Security Administration* dans le domaine fonctionnel System.

Context

Vous pouvez configurer des agents externes à l'aide du **hub Gestion des agents** .

Steps

1. Accédez au rapport **Hub Gestion des agents** .
2. Sélectionnez l'onglet **Registre de l'agent** , puis cliquez sur le nom de l'agent pour configurer l'agent.
3. Dans la vue du profil de l'agent, cliquez sur **Configurer l'agent** .
4. Dans la colonne **Statut** , rendez chaque aptitude pertinente disponible en activant le carrousel à bascule .
5. Pour chaque aptitude en mode d'exécution de déléguer disponible, renseignez l' invite **Disponible pour** et déterminez les groupes de sécurité que vous souhaitez ajouter pour cette aptitude spécifique pour l'agent.

Note: Les groupes de sécurité que vous sélectionnez dans l' invite **Disponible pour** doivent également disposer d'autorisations sur les règles de sécurité du domaine ou du processus de gestion qui sécurisent les outils des agents. Vous pouvez utiliser le rapport **Afficher la sécurité des aptitudes de l'agent** pour vous aider à configurer vos agents. Ce rapport affiche des informations détaillées sur les API Outils de l'agent et les règles de sécurité et autorisations respectives du domaine ou du processus de gestion . Au moment de l'exécution de l'agent, Workday évalue à la fois l'accès utilisateur à l'agent et l'accès utilisateur aux API qu'il exécute en tant qu'outils.

6. Cochez la case à cocher **Confirmer** , puis cliquez sur **OK** .
 - a) Pour les aptitudes déléguer , vous devez fournir un **URI de redirection** comme point de terminaison de rappel pour votre agent. Votre partenaire de développement d'agent peut fournir ces informations.
 - b) Pour les aptitudes autonomes, vous devez fournir une clé publique x509 depuis votre plateforme de développement d'agents. Votre partenaire de développement d'agent peut fournir ces informations. Sélectionnez une clé unique qui n'est pas utilisée par un autre agent. Voir aussi : [../././././authentication-and-security/security-for-integrations/access-to-external-endpoints/hzp1471450668309.dita](https://hwp1471450668309.dita) . Sécurité : domaine *Security Administration* dans le domaine fonctionnel System.
7. Cliquez sur **OK**.
8. Lorsque vous configurez l'agent pour la première fois, nous affichons le détail du client OAuth pour l'agent.

Note: Copiez et enregistrez les valeurs Identifiant client et Clé secrète client. Cette page ne s'affichera plus et vous ne pourrez plus accéder à ces informations.
9. Saisissez le détail du client OAuth et les URL de point de terminaison dans le code de la plateforme de développement de l'agent pour autoriser l'accès lors de l'exécution. Le détail des URL de client et de point de terminaison OAuth que nous affichons inclut les éléments suivants :
 - URL du point de terminaison autorisé
 - URL du point de terminaison du jeton
 - URL du point de terminaison
 - OAuth 2.0 Client ID
 - OAuth 2.0 Client Secret (délégataire uniquement)
 - Nom d'utilisateur pour le compte système de l'agent (son environnement client uniquement)
10. Sélectionnez **Registre de l'agent** et cliquez sur l'agent que vous souhaitez activer.

11. Dans la vue du profil de l'agent, cliquez sur **Activer l'agent** . Dans la fenêtre **Activer l'agent** , cochez la case à cocher **Confirmer** , puis **cliquez sur OK** pour finaliser l'activation.

Result

Workday crée automatiquement un utilisateur système d'agent (ASU) et affecte un groupe de sécurité d'agent (ASG) pour l'agent, que vous pouvez rechercher via le rapport **Tous les comptes d'agents IA** , sécurisé via le domaine *Workday Accounts* dans le domaine fonctionnel System. Vous pouvez les utiliser lorsque vous configurez les règles de sécurité et les autorisations pour votre agent.

Next Steps

[Configurer les règles de sécurité pour les agents](#) .

Concept : éléments à prendre en compte avec l'agent ASU externe

Nous vous recommandons de tenir compte de ces éléments lorsque vous créez des agents externes.

Déléataires ASU

Les identifiants du client ASU fournis après la configuration de l'agent doivent être utilisés pour [le flux de subvention OAuth 2.0](#) pour permettre à votre agent d'obtenir un accès pendant son exécution.

Lorsque vous testez manuellement le flux de subvention des codes d'autorisation d'un agent externe, utilisez le détail du client et les URL de point de terminaison fournis lors de la configuration de l'agent comme entrées pour les étapes suivantes :

1. Récupérez le code d'autorisation en collant l'URL suivante dans une nouvelle fenêtre : `https://<providedAuthorizeEndpoint>?response_type=code&client_id=<clientID>&state=<agentName>&redirect_uri=<redirectionURI>` .
L'URL vous redirige vers une page de connexion où vous devez fournir manuellement vos identifiants d'utilisateur pour le compte desquels l'agent agira.
Une fois connecté, vous êtes redirigé vers une page **Autoriser/Refuser** sur laquelle vous subvention à l'agent l'accès à votre compte Workday. **Autorisez** la redirection vers l'URI de redirection fourni avec un code ajouté que vous pouvez utiliser pour appeler l' API suivante .
2. Récupérez le jeton ASU en créant une nouvelle demande à l'aide d'un client API externe en utilisant le code d'autorisation fourni dans l'appel API précédent.

Par exemple, Carlos :

- *POST https://<providedTokenURL>*
- *Corps :octroi_type=Auteur*

Cela génère un jeton d'accès et un jeton actualiser que vous pouvez utiliser pour tester les appels de test que votre agent envoie aux services Workday .

Dans le corps de la réponse depuis le point de terminaison du jeton , le paramètre *expires_in* doit être renvoyé sous la forme d'un entier. Dans différents environnements de test, ce type de paramètre peut différer entre les types Entier et Chaîne. C'est pourquoi Workday recommande que le client externe puisse gérer à la fois les types Chaîne et Intent.

Lorsque vous devez mettre à jour une définition d'agent, vous pouvez indiquer le même nom d'agent, la même version et le même fournisseur à l' API POST Agent Definition et celle-ci sera mise à jour. En l'absence de correspondance, Workday crée un nouvel enregistrement de l'agent.

Lorsque votre agent envoie la demande au point de terminaison du jeton à l'aide d'AuthCode et identifiants client , le jeton d'accès et les jetons actualiser sont créés et renvoyés.

Le délai d'expiration du jeton d'accès est de 3 600 secondes (60 mins). Le délai d'expiration du jeton actualiser est de 24 heures.

Lorsqu'un jeton d'accès expire, le jeton actualiser en crée un nouveau.

Les clients OAuth types doivent seulement avoir besoin de :

- **Clé secrète client et Identifiant client** : obtenu lors du processus de configuration de l'agent.
- **Authorize Endpoint** : <https://us.agent.workday.com/auth/authorize/> <Tenant Alias>
- **Point de terminaison du jeton** : https://us.agent.workday.com/auth/oauth2/<Tenant_Alias>/jeton
- **URL de redirection** : fournie par le développeur de l'agent lors du processus de configuration de l'agent.

ASU ambigus

L'identifiant client et le nom d'utilisateur ASU fournis après la configuration de l'agent doivent être utilisés pour effectuer l'assertion JWT et la génération de jeton .

- L'émetteur doit être l'identifiant client.
- Le sujet doit être le nom d'utilisateur ASU.

La paire de clés x509 correspondante qui est obligatoire lors de l'enregistrement d'une aptitude en environnement de travail est utilisée lors de l'exécution de l'agent pour effectuer l'assertion JWT.

Mettez à jour le code de votre agent de sorte que, lors de l'exécution de l'agent, lorsqu'une demande est soumise à l'agent, celui-ci vérifie s'il dispose d'un jeton d'accès valide mis en cache. Si ce n'est pas le cas, ou si le jeton a expiré, nous :

- Créer une nouvelle assertion JWT
- Récupérer un jeton de porteur JWT
- jeton de mise en cache pour les demandes API Workday

Sécurité et conformité des agents

Éléments de définition : sécurité des agents

Cette thème peut vous aider à prendre les bonnes décisions lors de la planification de la configuration de la sécurité des agents. Elle explique :

- Pourquoi effectuer cette configuration.
- Comment cette configuration s'intègre dans Workday.
- Les impacts en aval, ainsi que les interactions entre produits.
- Les exigences de sécurité.
- Les questions à se poser et les limites à prendre en compte avant l'implémentation.

Présentation

La structure de sécurité des agents régit l'identité, authentification et l'autorisation des agents IA au sein de votre environnement client. Contrairement aux chatbots standard, les agents peuvent exécuter des tâches importantes dans les systèmes d'entreprise, comme demander des absences ou récupérer des informations sur des chèques de paie. La structure garantit que les agents opèrent selon le principe du minimum, avec des contrôles robustes pour les interactions autonomes et orientées utilisateur.

Avantages pour l'entreprise

- **Gouvernance améliorée** : garantit que les agents, comme les employés, ont des identités uniques et des journaux d'activité pouvant être audités.
- **Contrôle granulaire** : vous permet de limiter les fonctionnalités des agents en fonction du mode d'exécution, afin que les agents accèdent uniquement aux données qu'ils sont explicitement autorisés à traiter.
- **Audits transparents** : fournit des pistes d'audit claires qui distinguent lorsqu'un agent agit de manière autonome ou pour le compte d'un utilisateur.

Cas d'utilisation

- Assistant interactif en mode déléguer : Assistant interactif en mode déléguer : un utilisateur demande à un agent de demander le lundi suivant. L'agent exécute la demande pour le compte de l'utilisateur. La sécurité est évaluée en fonction de l'intersection des autorisations de l'utilisateur et des aptitudes autorisées de l'agent.
- Traitement en arrière-plan en mode environnement client : un agent agrège automatiquement les viviers de données ou évalue les jeux de données en fonction d'un planning. L'agent assure lui-même, en utilisant ses propres autorisations de sécurité sans intervention de l'utilisateur.

Questions à se poser

Question	Élément à prendre en compte
Quel mode d'exécution est requis par votre agent ?	Il existe deux modes d'exécution des agents distincts : • Mode délégataire : à utiliser lorsque l'agent agit pour le compte d'un utilisateur. La sécurité vérifie l'accès de l'utilisateur aux aptitudes. • Mode ambigu : à utiliser pour les tâches en arrière-plan pour lesquelles l'agent fait office lui-même. La sécurité vérifie l'accès de l'agent aux données et aux tâches.
Avec qui est autorisé à interagir et à appeler une aptitude spécifique d'un agent déléguer ?	Vous devez définir une règle d'interaction avec l'agent qui indique les groupes de sécurité utilisateur pouvant interagir avec les aptitudes de l'agent. L'utilisateur demandeur doit faire partie des groupes de sécurité autorisés pour que l'aptitude puisse être déclencheur avec succès.
Comment allez-vous gérer les identités des agents ?	Les agents nécessitent un compte utilisateur système d'agent unique. Un agent peut avoir jusqu'à 2 ASU : 1 pour le mode déléguer et un pour le mode Brut.
À quels domaines de données ou actions de processus de gestion spécifiques un agent doit-il accéder ?	Les autorisations d'un agent environnement client sont uniquement évaluées par rapport à ses propres autorisations Utilisateur système de l'agent (ASU). Vous devez affecter le groupe de sécurité d'agent ambigu dans les règles de sécurité du domaine ou du processus de gestion obligatoire .
Quels composants d'authentification doivent être pris en charge par l'application d'intégration, comme l'agent Forge ?	Pour le mode déléguer , le système utilise un flux OAuth 2.0 <i>On-Behalf-O</i> qui implique l'échange du jeton User Alpaca pour un jeton d'accès délégué. Vous devez vous assurer que l'application peut prendre en charge les types de jeton et les exigences d'en-tête nécessaires.
Est-il possible de configurer des ASU pour qu'ils fonctionnent avec des comptes proxy ?	Non, les ASU ne prennent pas en charge les comptes proxy.

Recommandations

- Respecter le principe du minimum de privilège. subvention aux agents l'accès minimum nécessaire aux domaines et aux processus de gestion obligatoire pour leurs aptitudes spécifiques.
- Utilisez des avis préalables d'expédition distincts pour chaque mode. Assurez-vous que chaque agent dispose de comptes distincts pour l'exécution déléguer et l'exécution d'environnement client afin d'éviter toute confusion au niveau des autorisations et des audits.
- Consultez le rapport Analyse de sécurité. Utilisez ce rapport pour mettre en évidence les configurations des domaine et des règle de sécurité du processus de gestion pour vos aptitudes d'agent.
- Révision de la piste d'audit : examine régulièrement le journal d'audit pour connaître les actions de l'agent. Le journal fait la distinction entre un agent environnement client agissant en lui-même et un agent déléguer agissant pour le compte d'un utilisateur spécifique.

Actions requises

- Définissez les règles de sécurité et activez les aptitudes de l'agent dans l'agent Système d'enregistrement (ASOR) pour générer un utilisateur système agent (ASU) et ses identifiants.
- L'ASU généré et son client OAuth associé sont désactivés par défaut. Vous devez activer un agent pour permettre son utilisation.
- Pour le mode Agent déléguer , l'utilisateur à l'origine des demandes doit disposer d'un accès de sécurité aux outils et tâches de l'agent sous-jacents.

Limites

- Critère de double identité : un agent qui doit fonctionner à la fois en mode déléguer et en mode environnement client doit avoir des comptes ASU et des identifiants distincts configurés pour chaque mode d'exécution.
- Gestion de clé : pendant qu'ASOR gère la création et le stockage sécurisé des identifiants clients (clé privée) dans le magasin d'identifiants, vous devez vous assurer que votre environnement de sécurité contribue à le processus OAuth 2.0 token-exchange qui utilise cette paire de clés.

Définition de l'environnement client

N/A

Sécurité

Les groupes de sécurité gérant les agents requièrent les droits d'accès *Afficher* et *Modifier* aux autorisations de rapport/tâche pour afficher et exécuter les tâches de l'agent, et l' accès Insérer à l'intégration pour transfert / mutation les données de configuration de l'agent.

Domaines	Éléments à prendre en compte
<i>Manage: Agents</i>	Donne accès aux tâches et activités de définition de l'agent Système d'enregistrement (ASOR).
<i>Setup: Agents</i>	Donne accès aux tâches de configuration, d'activation et de désactivation des agents.
<i>Hub Gestion des agents</i>	Donne accès au hub centralisé pour afficher et gérer tous les agents.
<i>Reports: AI Agent Security</i>	Donne accès au nouveau rapport View AI Agent User Audit Trail .

Reporting

- **Afficher la sécurité des aptitudes de l'agent** : affiche la configuration de la règle de sécurité du domaine et du règle de sécurité du processus de gestion pour les aptitudes de l'agent. Vous pouvez accéder à ce rapport à partir du menu des actions associées d'une aptitude de l'agent.
- **View AI Agent User Audit Trail** : affiche l'activité de l'utilisateur, en distinguant les données Par utilisateur et Pour le compte de l'utilisateur. Vous pouvez y accéder à partir du menu des actions associées d'un agent et en tant que tâche autonome .

Relations et interactions

La structure de sécurité des agents touche les domaines clés suivants de Workday:

Fonctionnalités	Éléments à prendre en compte
Sécurité configurable Workday	Les autorisations des agents dépendent entièrement des règles de sécurité et des groupes de sécurité des domaine et des processus de gestion , qui contrôlent l'accès aux éléments sécurisé .
Agent Système d'enregistrement (ASOR)	ASOR gère la définition et la configuration des agents et fait office de système d'enregistrement pour les règles de sécurité des agents et les codes de référence des identifiants.
Authentification OAuth 2.0	Le flux authentification de l'agent utilise OAuth pour l'échange de jeton Pour le compte d'une autre unité légale en mode déléguer .
API REST Workday	L'accès des agents aux données de Workday s'effectue via des points de terminaison de API REST qui sont sécurisé via des domaines ou des règles de sécurité de processus de gestion spécifiques.

Workday propose un kit appelé Touchpoints Kit, qui rassemble plusieurs ressources pour vous aider à mieux comprendre les relations de configuration dans votre environnement client. Pour en savoir plus sur ce kit, visitez notre [page Workday Touchpoints Kit](#) sur le site Workday Community.

Configurer les règles de sécurité pour les agents

Prerequisites

- Un groupe de sécurité d'agent ambigu est généré pour les agents agents générateurs.
- Sécurité : domaine *Security Configuration* dans le domaine fonctionnel System.

Context

Workday évalue la sécurité différemment en fonction du type d'agent :

- **Agents déléataires** : Workday utilise les droits d'accès de l'utilisateur à l'origine de la transaction. Si l'utilisateur demandeur dispose déjà des autorisations de domaine et de processus de gestion obligatoire pour les outils sous-jacents, aucune mise à jour n'est nécessaire. N'utilisez cette procédure que si l'utilisateur à l'origine de la transaction a besoin d'un accès supplémentaire aux domaines sécurisant les outils de l'agent.
- **Agents ambigus** : Workday évalue la sécurité uniquement par rapport aux autorisations de l'agent. Lorsque vous activez une aptitude, ASOR génère un groupe de sécurité d'agent (ASOR) unique. Vous devez explicitement affecter ce groupe de sécurité du système aux règles de sécurité du

domaine ou du processus de gestion pour subvention l'accès aux éléments sécurisé , tels que les outils et les API.

Steps

1. Accédez au rapport **Afficher la sécurité des aptitudes de l'agent** dans le menu des actions associées d'une aptitude de l'agent.
2. Identifiez les domaines qui sécurisent les outils dans l'aptitude.
3. Recherchez et sélectionnez la règle de sécurité du domaine pour le point de terminaison de l' API REST ou les données auxquelles l'agent doit accéder.
4. Dans le menu des actions associées de la règle de sécurité de domaine , sélectionnez **Règle de sécurité > Modifier la règle de sécurité de domaine** .
5. Exécutez la tâche :

Option	Description
Agent Déléataire	Dans l' invite Groupes de sécurité , sélectionnez les groupes de sécurité qui incluent les utilisateurs à l'origine de la requête et qui ont besoin d'un accès.
Agent Ame saisie	Dans l' invite Groupes de sécurité , sélectionnez l'agent Am saisir un groupe de sécurité.

6. Cochez les cases **Afficher** ou **Modifier** pour subvention au groupe de sécurité l'accès aux éléments sécurisables.
7. Si un outil du rapport **Afficher la sécurité des aptitudes de l'agent** requiert un accès Extraire/ Insérer, cochez la case **Extraire** ou **Insérer** pour subvention aux groupes de sécurité l'accès aux intégrations.
8. [Activez les modifications des règles de sécurité en attente.](#)

Result

L'agent peut désormais effectuer les actions obligatoire sur le domaine sécurisé . Pour les agents déléguer , les utilisateurs appelant spécifiques que vous avez mis à jour disposent désormais des autorisations obligatoire pour utiliser les outils de l'agent.

Concept : sécurité des agents

Agent Security garantit que les agents IA opèrent en toute sécurité au sein de votre entreprise en leur affectant des identités uniques, une authentification robuste et des contrôles d'autorisation précis. La sécurité des agents régit la façon dont les agents interagissent avec les données et effectuent des tâches, en respectant le principe du minimum de privilège.

Lorsque vous gérez le cycle de vie et la définition de vos agents dans l'agent Système d'enregistrement (ASOR), Agent Security détermine leur comportement au moment de l'exécution.

La structure de sécurité des agents contribue à deux modes d'exécution des agents distincts :

- Mode déléataire : agit pour le compte d'un utilisateur. Exemple : un utilisateur délègue à l'agent la tâche de demander un jour d'absence pour une date spécifique.
- Mode ambigu : agit de manière autonome en fonction d'un déclencheur ou d'un calendrier événement . Bien qu'un agent ne soit pas entièrement autonome, il fonctionne de manière indépendante pour effectuer des tâches en arrière-plan, telles que l'agrégation de viviers de données ou la réponse à des déclencheurs événement .

Identité de l'agent : utilisateur système (ASU)

À l'instar des utilisateurs du système d'intégration (ISU), les agents utilisent des comptes Utilisateur système agent (ASU). Pour garantir un contrôle impartial sur ce à quoi l'agent peut accéder et pour assurer la transparence des audits, chaque agent a une identité unique ou un compte utilisateur.

- Identité unique : chaque agent dispose d'un compte ASU unique.
- Spécifique du mode : un agent peut avoir jusqu'à 2 ASU ; 1 pour l'exécution délégué et l'exécution d'environnement client. Chaque ASU aura un client OAuth 2.0 spécifique.
- Management : le système génère et gère automatiquement les ASU lorsque vous configurez les aptitudes dans l'Agent Système d'enregistrement. Exemple : l'activation d'une aptitude d'environnement client déclenche la création de l'ASU requise.

Création et enregistrement d'un ASU

Le processus de création de l'ASU s'effectue en parallèle avec la configuration de l'agent et l'activation des aptitudes dans ASOR.

- Génération ASU : lorsqu'un administrateur active des aptitudes pour un agent, ASOR crée automatiquement un ASU dédié ou un ASU ambigu pour cet agent en cas de désactivation. Lorsque l'agent est activé, les ASU associés sont automatiquement activés.
- Client OAuth et paire de clés : un client OAuth est généré et joint à un ASU. Une paire de clé privée est créée et la clé publique est enregistrée avec le serveur d'autorisation Workday . L'ASU se voit alors attribuer la aptitude de s'authentifier et d'effectuer les tâches définies dans ses aptitudes.
- Stockage d'identifiants : ASOR stocke en toute sécurité les identifiants clients , y compris la clé privée, dans le magasin d'identifiants. Un code de référence unique est ensuite stocké dans ASOR en tant que pointeur vers ces identifiants de paire de clés, qui sont utilisés pour générer des jetons ASU échangés avec le jeton utilisateur pour un ASU délégué, plutôt que pour les identifiants client OAuth 2.0.

Comparaison des modes de sécurité

Fonctionnalité	Mode délégataire	Mode ambigu
Cas d'utilisation principal	Tâches interactives. Exemple : demander une absence pour vous-même.	Tâches en arrière-plan. Exemple : agrégation de données.
Identité utilisée	Combinaison entre l'utilisateur et l'agent ASU.	Agent ASU uniquement.
Authentification	L'agent utilise l'OAuth 2.0 pour le flux Pour le compte d'une autre unité légale.	L'agent s'authentifie en tant qu'ASU existantes, sans intervention de l'utilisateur.
Logique d'autorisation	Le système évalue la sécurité en fonction de l'intersection des autorisations de l'utilisateur et des aptitudes autorisées de l'agent.	Le système évalue la sécurité uniquement en fonction des autorisations de l'agent.
Configuration	Règle d'interaction avec l'agent : définit qui peut interagir avec les aptitudes spécifiques de l'agent.	Règle de sécurité de domaine : définit ce à quoi l'agent peut accéder.
Groupes de sécurité	L'utilisateur doit faire partie des groupes de sécurité autorisés pour l'aptitude pour pouvoir l'appeler.	Lorsqu'une aptitude est activée, un groupe de sécurité d'agent ambigu est généré et doit être affecté aux règles de sécurité

Fonctionnalité	Mode délégataire	Mode ambigu
		du domaine ou du processus de gestion appropriées.
Journal d'audit	Enregistre la transaction comme étant effectuée par l'agent en tant qu'utilisateur et l'utilisateur en tant que <i>Pour le compte de l'utilisateur</i> .	Le journal d'audit indique l'agent ASU comme étant l' <i>utilisateur</i> .

Éléments à prendre en compte lors de l'implémentation

Workday fournit un rapport Analyse de la sécurité pour les configurations des règles de sécurité des domaine et des règle de sécurité du processus de gestion pour les aptitudes de l'agent. Ce rapport vous aide à identifier les configurations de sécurité nécessaires pour vos agents.

Concept : règle d'interaction avec l'agent

La règle d'interaction avec l'agent est une configuration de sécurité au sein de l'agent Système d'enregistrement (ASOR) qui définit explicitement les utilisateurs autorisés à communiquer avec ou à invoquer des aptitudes spécifiques de l'agent.

Fonctionnement

La règle fonctionne comme un mécanisme d'activation des aptitudes en mode déléguer d'un agent. Si un utilisateur n'appartient pas au groupe de sécurité pour une aptitude d'agent, l'utilisateur ne peut pas utiliser cette aptitude même s'il a accès au domaine ou aux règles de sécurité des processus de gestion pour les outils de cette aptitude. Lorsqu'un utilisateur tente d'interagir avec un agent, la structure Workday Agent Security effectue une évaluation de la sécurité en deux étapes :

1. Vérification des interactions de l'agent : le système vérifie si l'utilisateur appartient à un groupe de sécurité inclus dans la règle d'interaction avec l'agent de l'agent, qui est configurée dans la liste **Disponible pour**. Si l'utilisateur n'est membre d'aucun de ces groupes, l'interaction avec l'agent est refusée, même si l'utilisateur dispose des autorisations de sécurité nécessaires pour effectuer les tâches définies dans la section **Outils** de l'aptitude.
2. Vérification des domaines et des processus de gestion : si l'utilisateur réussit la vérification interaction, le système vérifie ses autorisations standard, y compris les domaine et les règles de sécurité des processus de gestion, pour s'assurer qu'il est autorisé à consulter les données ou à effectuer l'action demandée. Les domaines sont vérifiés non seulement pour les outils, mais aussi au niveau du champ lorsque l'aptitude de l'agent est exécutée, ce qui est cohérent avec le fonctionnement de la sécurité de domaine sans agent.

Assujettissement

Workday vous permet de configurer la règle d'interaction avec l'agent uniquement pour les agents et les aptitudes qui opèrent en mode déléguer.

- Mode délégataire : nécessite une règle d'interaction avec l'agent. Vous devez activer explicitement les groupes de sécurité pour leur permettre d'utiliser ces aptitudes.
- Mode ambigu : n'utilise pas la règle d'interaction avec l'agent. Lorsque les agents environnement peuvent agir eux-mêmes en arrière-plan sur la base de déclencheurs ou de plannings, ils n'interagissent pas directement avec un utilisateur et n'ont donc pas besoin de définir une règle définissant quel utilisateur peut interagir avec eux.

Configuration

Vous pouvez définir une règle d'interaction avec les agents dans le **hub Gestion des agents** ou lors de l'enregistrement de l'agent en configurant les paramètres **Disponible pour** pour une aptitude spécifique.

Exemple : pour un agent Recrutement disposant d'une aptitude Création de demande de poste, vous pouvez ajouter le groupe de sécurité Recruteurs à la liste **Disponible pour** . Seuls les utilisateurs du groupe de sécurité Recruteurs peuvent demander à l'agent de créer une demande d'achat. Un utilisateur du groupe de sécurité Salarié (pour lui-même) ne peut pas utiliser cette aptitude, même s'il avait accès au domaine pour créer des demandes d'achat.

Agent Gateway

Authentification via Agent Gateway

Prerequisites

- Enregistrez votre agent avec l'agent Système d'enregistrement (ASOR) via la nouvelle API d'enregistrement de l'agent . Pour plus d'informations sur enregistrement de votre agent avec ASOR, voir [Enregistrer et définir votre agent via une API](#) .
- Identifiant client : obtenu à partir de l'étape de configuration dans ASOR.
- Clé secrète client : obtenue à partir de l'étape de configuration dans ASOR.
- Point de terminaison d'autorisation : `https://us.agent.workday.com/auth/authorize/<Tenant_Alias>`
- Point de terminaison du jeton : `https://us.agent.workday.com/auth/oauth2/<Tenant_Alias>/jeton`
- Rediriger l'URI : le développeur de l'agent fournit ce dans ASOR lors de l'étape Configuration de votre agent.
- Votre agent est actif dans ASOR.

Context

Pour que la passerelle d'agent achemine les demandes vers le centre de données Workday approprié, elle doit connaître l' alias de votre environnement client. Cet alias doit être fourni avec toutes les demandes API de l'agent, y compris les demandes d' authentification. Votre alias environnement client est généralement le nom de votre environnement client . Il se trouve dans l'URL de votre instance Workday : `https://wd8.myworkday.com/stark-secteurs/d/home.html`.

Pour diriger tous les appels API pertinents vers le point de terminaison Agent Gateway, vous devez modifier le code ou la configuration de votre agent.

L'image suivante illustre un flux authentification OAuth 2.0 Code d'autorisation standard. Il s'agit d'étapes détaillées du flux lui-même ; si votre plateforme d'agents externe contribue à la norme OAuth 2.0, elle doit déjà prendre en charge ce processus.

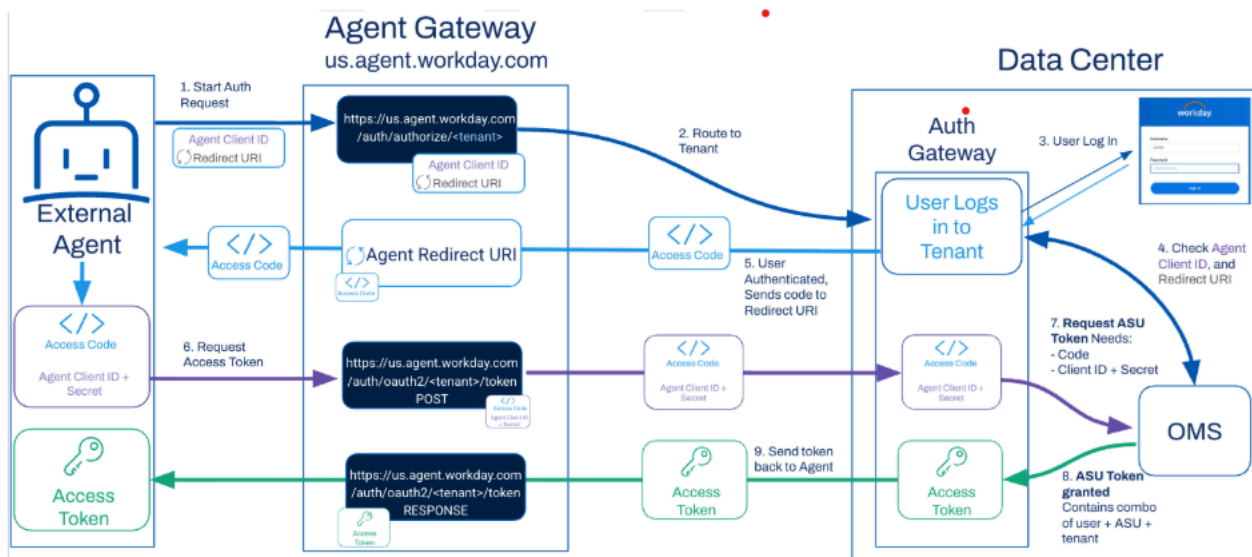


Figure 1: Authentification OAuth 2.0

Note: Les étapes décrivent le flux OAuth 2.0 standard, que vous n'avez pas besoin d'implémenter manuellement. Un client OAuth classique requiert uniquement les valeurs de configuration indiquées dans la section Conditions préalables . Pour plus d'informations sur authentification, voir [Configurer des agents externes dans Workday](#) .

Steps

1. Pour demander un code d'autorisation, envoyez une requête HTTPS GET au point de terminaison de l'autorisation dans la passerelle Agent.

Envoyez cette demande dans votre navigateur et connectez-vous si vous le souhaitez :

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

La passerelle de l'agent enverra cette demande à la passerelle d'authentification dans le centre de données où se trouve votre environnement client , en utilisant l'alias de l'environnement client dans la demande. La passerelle d'authentification vous redirige ensuite vers une fenêtre contextuelle de connexion Workday pour vous authentifier. Une fois que l'agent a été connecté et qu'il a accepté les données Workday , ce dernier recevoir un code d'autorisation.

2. Copiez la valeur du code d'autorisation de la réponse.
3. Pour demander un jeton d'accès, envoyez une demande POST au point de terminaison du jeton dans la passerelle Agent.

```
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>
```

La passerelle d'agent achemine la demande à la passerelle d'authentification au centre de données de l'environnement client. Après avoir validé les identifiants indiqués , la passerelle d'authentification demandera le jeton d'accès depuis l'OMS. Votre agent recevoir alors le jeton d'accès.

Concept : demandes API via Agent Gateway

Vos agents enverront les demandes API via Agent Gateway, y compris l'alias de l'environnement client en tant qu'en-tête HTTP. L'alias de l'environnement client figurant dans l'en-tête permettra à Agent Gateway d'acheminer la demande vers le centre de données approprié pour votre environnement client.

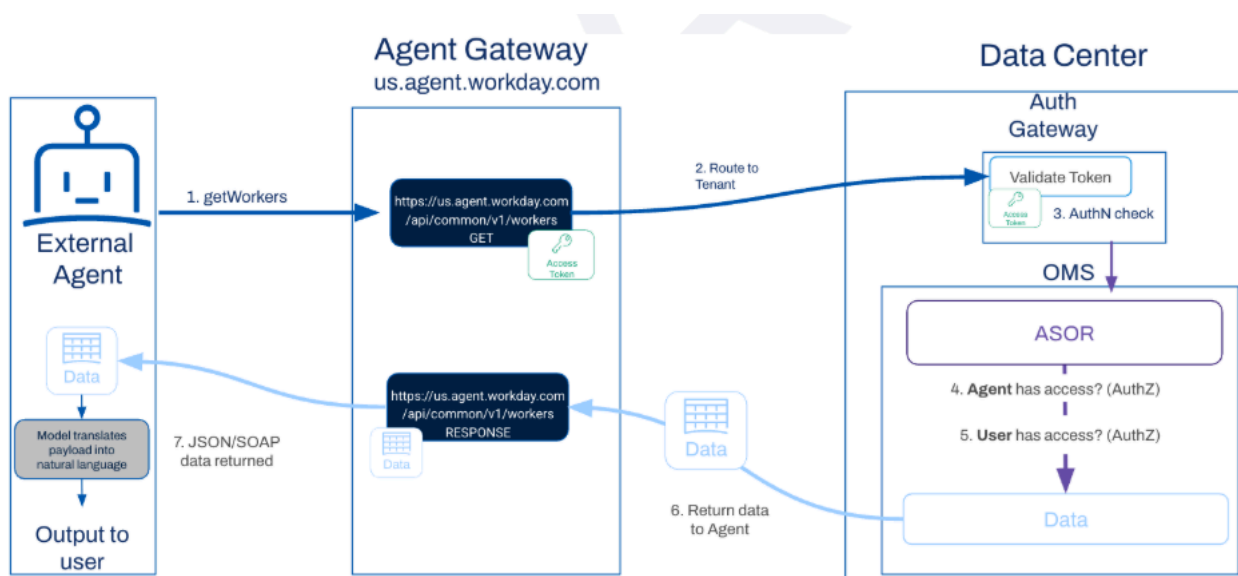


Figure 2: Demandes API via Agent Gateway

Exemple de demande API :

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

Exemple d'en-tête HTTP :

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

Les appels API de votre agent doivent inclure :

- Point de terminaison de passerelle : us.agent.workday.com .
- En-tête HTTP de l'alias de l'environnement client : fournissez wd-agent-tenant-alias comme en-tête HTTP dans la demande. La valeur doit être unique.
- Appels SOAP : le point de terminaison approprié pour les appels SOAP est

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

Concept : Workday Agent Gateway pour les agents partenaires

Ce document fournit les instructions obligatoire pour garantir une implémentation transparente de la passerelle d'agent, afin que vos agents puissent tirer parti des avantages de la passerelle tout en respectant les normes de la plateforme d'agents Workday .

La fonctionnalité Agent Gateway de Workday vous permet de connecter plus facilement vos agents IA à l'Agent Système d'enregistrement de Workday (ASOR). Il permet à vos agents de collaborer et de communiquer des informations avec l'écosystème Workday , ce qui vous permet d'assurer un support et une automatisation en temps réel au sein de votre workflow existant.

Agent Gateway fonctionne comme un proxy inverse sécurisé et intelligent en fournissant un point de terminaison régional unique et unifié pour centraliser et rationaliser la manière dont les agents tiers s'interfaçent avec Workday. La passerelle d'agent donne accès aux API Workday , y compris Graph, à tous les partenaires agentiques, ainsi qu'à l' API Registre des définitions d'agent.

La passerelle d'agent comprend :

- [Toutes les opérations REST publiques](#)
- [Toutes les opérations SOAP publiques](#)
- API Workday Graph

- Workday Query Language (WQL)
- Workday RaaS

Agent Gateway est votre point de départ pour créer de puissantes expériences agentiques intégrées avec Workday, avec la sécurité, l'évolutivité et les outils opérationnels dont vous avez besoin. La passerelle d'agent offre les avantages suivants :

- Visibilité complète : permet de surveiller la performance et l'intégrité des agents à l'aide d'enregistrements et de métriques détaillés.
- Sécurité future : prépare votre agent à travailler efficacement avec les futures mises à jour de la plateforme Workday et les protocoles de sécurité.
- Performance et stabilité prévisibles : garantit que votre agent interagit avec Workday dans un environnement stable et performant via des limites de taux et des garde-fous de performance intégrés.
- Sécurité et confiance robustes : garantit que tous les appels API sont authentifiés et autorisés via la couche de sécurité robuste de Workday, fournissant un modèle d'interaction sûr et conforme.
- Accès simplifié aux API Workday : fournit un point d'entrée géré et cohérent pour toutes les interactions API Workday de votre agent.
- Suivi d'utilisation transparent : assure un suivi clair de la consommation de API par votre agent, fournissant les données nécessaires pour une facturation et une gestion des coûts précises.

Tous les agents tiers qui interagissent avec les API de Workday obligatoire acheminer leur trafic API via Agent Gateway en utilisant la sécurité ASU (Agent System User) comme obligatoire. Pour plus d'informations sur la sécurité des agents, voir [Concept : sécurité des agents](#) .

Pour acheminer votre trafic API via Agent Gateway, vous devez enregistrer vos agents externes dans Workday via l'Agent Système d'enregistrement (ASOR) et configurer leur mode d'authentification. Pour plus d'informations sur l'enregistrement d'agents externes dans ASOR et la configuration de l'authentification, voir [Configurer des agents externes dans Workday](#) .

Référence : disponibilité de Agent Gateway dans certaines régions

Agent Gateway est disponible dans plusieurs régions pour répondre à vos besoins. Utilisez les points de terminaison suivants en fonction de votre région :

Région	Point de terminaison régional public
États-Unis	https://us.agent.workday.com
EU	https://eu.agent.workday.com
Royaume-Uni	https://uk.agent.workday.com
SIN	https://sg.agent.workday.com
ININD	https://in.agent.workday.com
JPN	https://jp.agent.workday.com

Agent Marketplace

Concept : Agent Marketplace

Workday Marketplace est le hub numérique de l'économie Workday . Les clients peuvent découvrir, tester et acheter des solutions fiables auprès de partenaires logiciels et services depuis un seul et même endroit. Il consolide l'écosystème de solutions Workday pour prendre en charge l'évaluation des solutions de bonnes pratiques qui s'intègrent à Workday.

Workday fournit Agent Marketplace dans Workday Marketplace pour permettre aux clients de découvrir des agents IA. Au sein de l'écosystème Workday, Agent Marketplace fournit des solutions d'agents conçues pour répondre aux défis professionnels et étendre les fonctionnalités de Workday.

Agent Marketplace propose un catalogue d'agents IA de Workday et de Workday partenaires. Les partenaires des programmes de partenaires construites dans Workday (BoW) ou Connect/Platinum peuvent build et distribuer des agents certifiés.

Agent Marketplace vous permet de rechercher des solutions ciblées. Accédez à Agent Marketplace à l'adresse : <https://marketplace.workday.com/en-US/pages/agents>.

Vous pouvez enregistrer, configurer, surveiller et gérer les agents IA à grande échelle en toute sécurité à l'aide de l'agent Système d'enregistrement (ASOR).

Agent Marketplace pour différents types d'utilisateur

Workday a conçu Agent Marketplace pour les types d'utilisateur suivants :

- Clients
 - Découverte centralisée : un site unique pour découvrir et se familiariser avec les agents Workday et les partenaires Workday disponibles.
 - Prise de décision éclairée : accédez à des informations sur les fonctionnalités des agents, les avantages sociaux et les pratiques d'IA responsable pour vous aider à choisir les solutions adaptées.
 - Connexion directe : le bouton **Nous contacter** permet aux clients de se connecter directement avec Workday ou avec des partenaires Workday pour plus d'informations.
- Workday Partners
 - Une visibilité accrue : l'occasion de présenter les solutions basées sur des agents à une large plage de clients Workday.
 - Génération de prospects : le bouton **Nous contacter** sert de canal direct pour les demandes des clients et les prospects potentiels.
- Chargés d'implémentation : recherchez et sélectionnez des agents en fonction des besoins de votre activité.
- Développeurs : télécharger de nouveaux agents ou aptitudes.

Concept : liste des agents dans Workday Marketplace

Pour introduire les listes d'agents, Workday apporte les modifications suivantes à Workday Marketplace :

- Type de solution d'agents : un nouveau filtre de type de solution **Agents**.
- Fiches des agents et listes : chaque agent a une page dédiée avec des fonctionnalités, des avantages sociaux et des descriptions des rôles et des aptitudes qu'il fournit.
- Catégorisation : les agents sont classés en fonction des regroupements généraux de Workday afin qu'ils s'alignent sur la stratégie produit et offrent une expérience de recherche et de découverte cohérente dans toutes les expériences Workday.
- Associer de l'agent : associer sous la section Solutions d'IA qui redirige les utilisateurs vers les listes d'agents.
- Identification par l'IA responsable : les agents Workday qui ont terminé le processus d'attestation de **l'IA responsable** reçoivent le badge en conséquence.

Agents prédéfinis par Workday

Agent Optimisation des processus de gestion

Définir l'agent Optimisation des processus de gestion

Prerequisites

Note: Votre organisation doit accepter l'UMSA (Universal Main Service Agreement) pour utiliser l'agent Optimisation des processus de gestion. des étapes supplémentaires peuvent être nécessaires pour activer cette fonctionnalité en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services principal (MSA), soit sur l'UMSA. Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().
4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- *UMSA* , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- *MSA* , votre organisation doit accepter l'UMSA.

Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser des agents en production tant que vous n'aurez pas accepté ces contrats. L'UMSA est obligatoire pour les environnements clients hors production et de production pour les agents Workday-Built. Vous devez enregistrer et activer l'agent Optimisation des processus de gestion en production avant de pouvoir l'utiliser dans votre environnement environnement client de production . Une fois que vous avez activé l'agent dans votre instance de production , comptez jusqu'à 24 heures pour que le système traite les modifications avant que vous ne tentiez d'activer l'agent dans votre environnement sandbox.

- Activer la [politique de crédits variables et de droits à la plateforme de Workday](#) . obligatoire uniquement pour une utilisation dans les environnements clients de production.
- [Définissez l'agent Système d'enregistrement](#) .
- Sécurité : les domaines suivants dans le domaine fonctionnel Agent System of Record :
 - *Conformité de l'agent*
 - *Hub Gestion des agents*
 - *Manage: Agents*
 - *Reports: Agent Reporting*
 - *Reports: AI Agent Security*
 - *Setup: Agents*
- Sécurité : domaines suivants dans le domaine fonctionnel System :
 - *Business Process Administrator*
 - *Agent Optimisation des processus de gestion*

Le domaine *Business Process Agent* hérite de la sécurité du domaine *Business Process Administrator* . Pour personnaliser l'accès à votre organisation, vous pouvez remplacer l'héritage et utiliser le domaine *BP Optimize Agent* .

- (Facultatif) L'agent Optimisation de processus de gestion inclut une fonctionnalité facultative de contribution des données de Machine Learning, appelée **Agent Optimisation des processus de**

gestion , pour les clients UMSA. Cette fonction permet à Workday d'accéder aux pistes de l'agent, qui sont générées à partir d'invites utilisateur dans le tchat de l'agent Workday . Cette option est activée par défaut pour les clients UMSA ; Toutefois, les clients conservent la aptitude de refuser manuellement la fonctionnalité .

Context

Vous pouvez enregistrer, configurer et activer l'agent Optimisation des processus de gestion dans Workday à l'aide du **hub Gestion des agents** .

Tenez compte des exigences et limites actuelles avant de configurer l'agent Optimisation des processus de gestion :

- **Éligibilité** : pour utiliser l'agent, votre environnement client doit se trouver dans les régions des États-Unis ou de l'UE et avoir moins de 2 millions de transactions par mois en moyenne.
- **Environnements pris en charge** : vous pouvez uniquement enregistrer et utiliser l'agent dans une instance sandbox de production ou de production.
- **Configuration et Coût** : lors de la configuration, vous devez configurer l'agent en sélectionnant vos lignes de produit et une période rétrospective. Actuellement, une fois que vous les avez soumises, vous ne pouvez plus les modifier/changer . Notez que ces paramètres déterminent votre périmètre d'analyse et affectent votre utilisation des crédits variables, ce qui peut entraîner des coûts supplémentaires.
- **Langue prise en charge** : actuellement, l'agent Optimisation des processus de gestion prend uniquement en compte l'anglais. Si la langue d'un utilisateur est le français, par exemple, l'agent utilisera par défaut l'anglais.
- **Étapes exclues** : l'agent exclut toutes les étapes configurées après l'étape *Finalisation* . Il considère qu'un processus de gestion est terminé même si le workflow dépasse cette étape.

Steps

1. Accédez au rapport **Hub Gestion des agents** .
2. Sélectionnez l'onglet **Agent Workday non enregistré** .
3. Pour l' **agent Optimisation des processus de gestion** , cliquez sur **Enregistrer** .
4. Cochez la case à cocher **Confirmer** , puis cliquez sur **OK** pour finaliser l'enregistrement. Workday déplace l' **agent Optimisation des processus de gestion** dans l'onglet **Registre de l'agent** .
5. Sélectionnez l'onglet **Registre de l'agent** , puis cliquez sur le nom de l'agent *BP Optimize* pour configurer l'agent.
6. Dans la vue du profil de l'agent, cliquez sur **Configurer l'agent** .
7. Dans la colonne **Configuration supplémentaire** , cliquez sur le bouton Configurer l'agent Optimisation des processus de gestion et sélectionnez une **Période rétrospective et des Lignes de produit** .

Note: Vos sélections affectent votre périmètre d'analyse et l'utilisation des crédits variables. Examinez attentivement les lignes de produit, les types de processus de gestion et la période rétrospective avant de soumettre. Actuellement, vous ne pouvez pas modifier/changer ces paramètres une fois que vous avez soumis votre .

8. Dans la colonne **Statut** , rendez disponible l'aptitude **Amélioration des processus** en faisant glisser la bascule.

9. Dans l'invite **Disponible pour** de la ligne **Amélioration des aptitudes** , dans le domaine fonctionnel System, sélectionnez l'une des options suivantes :

- domaine *Business Process Administrator* .
- Le domaine *BP Optimize Agent* si vous l'avez personnalisé.

Les groupes de sécurité que vous sélectionnez dans l'invite **Disponible pour** doivent également disposer d'autorisations sur les règles de sécurité du domaine ou du processus de gestion qui sécurisent les agents. Vous pouvez utiliser le rapport **View Security for Agent Skill** pour vous aider à configurer vos agents.

10. Cliquez sur **OK**.

11. Dans l'onglet **Registre de l'agent** , cliquez sur l' **agent Optimisation des processus de gestion** , puis sur **Activer l'agent** .

12. Cochez la case à cocher **Confirmer** , puis cliquez sur **OK** .

Result

Une fois ingestion des données terminée, ce qui peut prendre jusqu'à 48 heures, les employés du groupe de sécurité *Business Process Administrator* peuvent accéder à l'agent Optimisation des processus de gestion depuis le tableau de bord et depuis l'icône en bulles de tchat de l'agent Workday pour :

- Analyser et visualiser les indicateurs de performance des processus de gestion et les tendances d'exécution.
- Comparez la performance de votre unité légale aux benchmarks de pair pour le secteur d'activité, la région et la taille de unité légale .
- Identifier les goulets d'étranglement, les modèles d'exécution anormaux et leurs causes premières.
- Obtenir des recommandations personnalisées et exploitables pour optimiser vos processus de gestion.

Note:

- Révissez et vérifiez toujours l'exactitude des analyses et des recommandations générées par l'IA avant d'apporter des modifications à la configuration de vos processus de gestion.
- Lorsque plusieurs agents sont configurés, vous devrez peut-être accéder au chat de l'agent et sélectionner l'agent Optimisation des processus de gestion dans le menu de l'agent.

Concept : agent Optimisation des processus de gestion

L'agent Optimisation des processus de gestion est un assistant basé sur l'IA qui vous aide à améliorer l'efficacité et la performance globale de vos processus de gestion dans Workday. L'agent analyse vos processus actuels, identifie les points à améliorer et fournit des recommandations concrètes avec des instructions étape par étape.

L'agent Optimisation des processus de gestion utilise les éléments suivants :

- Détail de l'exécution des processus de gestion configurés et des étapes correspondantes pour analyser les temps d'exécution et identifier les modèles anormaux.
- Données d'exécution spécifiques à l'environnement client pour générer des moyennes agrégées pour le benchmarking.
- Des données système propriétaires pour déterminer les données et les groupes de référence.

Note: Pour éviter les métriques biaisées, l'agent Optimisation des processus de gestion exclut les données des éléments suivants :

- Générateurs EIB
- Services web
- Chargements d'intégration
- Transactions immédiatement terminées (durée = 0)

L'agent prend uniquement en compte les transactions de processus de gestion réelles effectuées dans l'application Workday .

Aptitude d'amélioration des processus

L'agent Optimisation des processus de gestion fournit l'aptitude Amélioration des processus qui permet aux administrateurs Workday de :

- Obtenir des analyses détaillées sur les processus de gestion, localiser les goulets d'étranglement et identifier les causes premières.
- Comparer les performances des processus de gestion par rapport à des benchmarks entre secteurs d'activité, régions et tailles unité légale .
- Obtenir des recommandations d'optimisation personnalisées et exploitables spécifiques à l'utilisation et à la configuration des processus de gestion spécifiques aux .

Pour plus d'informations, voir [Concept : aptitude d'amélioration du processus d'optimisation des processus de gestion](#) .

Éléments de sécurité à prendre en compte

Les utilisateurs de l'agent Optimisation de processus de gestion doivent disposer de l'autorisation **Modifier** dans le domaine de sécurité *Business Process Administration* ou *BP Optimize Agent* dans le domaine fonctionnel System .

L'agent Optimisation des processus de gestion affiche les données d'identification personnelle (PII) uniquement lorsqu'il affiche les utilisateurs **Création par** et **Dernière modification par** . Ces informations sont visibles depuis le tableau de bord **Agent Optimisation des processus de gestion** et la section **Aperçu** de la page **Tendances et anomalies** lorsque vous :

- Cliquez sur un processus de gestion dans le graphique à barres ou le graphique linéaire .
- Cliquez sur **Inspecter** dans la vue modale du processus de gestion .

Les données de benchmarking de chaque unité légale ne peuvent pas être identifiées par d'autres clients Workday . Workday ne génère des données de référence que lorsqu'un nombre minimum de clients répond aux critères définis, notamment pour empêcher l'identification de tout client.

Limites

- analyses des tendances : limitez les analyses aux événements qui lancent et se terminent au cours de la période sélectionnée. L'agent exclut les événements qui commencent dans une période mais qui se terminent dans une période suivante.
- analyses de benchmarking : générer uniquement lorsque la cohorte de pair minimale obligatoire par secteur contient suffisamment de transactions pour ce processus de gestion au cours de la même période.
- Statuts des événements : ne tenez compte que des événements terminés dont le statut est Terminé avec succès, Retiré, Annulé ou Processus terminé. L'agent exclut les événements en cours.
- Éligibilité de l'environnement client : exige que votre environnement client se trouve dans les régions des États-Unis ou de l'UE et qu'il effectue une moyenne de moins de 2 millions de transactions par mois.
- Langue prise en charge : actuellement limité à l'anglais.

Concept : aptitude d'amélioration du processus d'optimisation des processus de gestion

Aperçu

L'aptitude Amélioration des processus de l'agent Optimisation des processus de gestion vous permet de :

- [Analyser les données des processus de gestion](#) .
- [Visualiser les données des métriques](#).

- Comparer avec les données de référence.
- Réviser les analyses sur le benchmarking.
- Respecter les tendances anormales.
- Identifier les anomalies et les causes premières.
- Générer des recommandations d'optimisation.
- Implémenter des recommandations d'optimisation.
- Poser des questions sur l'optimisation des processus de gestion .

Comment y accéder ?

Vous pouvez accéder à l'aptitude Amélioration des processus dans le rapport **Agent Optimisation des processus de gestion** pour :

- Analysez la performance d'un processus de gestion spécifique, sélectionnez-le dans le graphique et cliquez sur **Inspecter** .
- Ajustez les données de référence en cliquant sur l' icône de filtre et en faisant défiler l'écran jusqu'à la section **Benchmarking sectoriel** du panneau de filtre .
- Poser des questions à l'aide du langage naturel en cliquant sur icône en bulles de tchat de l'agent Workday et en sélectionnant l' **agent Optimisation des processus de gestion** .

Analyser les données des processus de gestion

L'aptitude Amélioration des processus utilise le détail d'exécution des processus de gestion configurés et les étapes correspondantes. Par défaut, le tableau de bord affiche les processus de gestion par :

- Groupe fonctionnel : le tableau de bord **de l'agent Optimisation des processus de gestion** affiche un onglet pour chacun des domaines de produit sous licence de votre unité légale (exemple : Extend, Spend, Talent, Workforce). L'onglet par défaut est **Personnel** .
- Période : la période par défaut correspond au dernier trimestre terminé de l' année civile standard . Exemple : en avril 2026, le dernier trimestre terminé est le premier trimestre 2026, qui court de janvier à mars 2026.

Vous pouvez modifier le filtre de *période* , soit par mois, soit par trimestre.

Note: L'agent utilise les mois calendrier pour déterminer les trimestres, et non l' exercice.

- Processus de gestion et définition de processus de gestion : le filtre *Processus de gestion* présélectionne les types de processus de gestion associés aux cinq définitions de processus de gestion dont l'exécution a pris le plus de temps au cours de la période spécifiée .

Le filtre *Définition de processus de gestion* répertorie les définitions de processus de gestion actives pour les types de processus de gestion sélectionnés.

Ajustez le filtre pour vous concentrer sur les processus de gestion que vous souhaitez analyser.

- Indicateurs : par défaut, le graphique affiche le Délai d'achèvement (heures), qui correspond au nombre moyen d'heures qu'il a fallu aux processus de gestion pour s'exécuter. Vous pouvez sélectionner **Renvoyer** , qui affiche le pourcentage d'événements renvoyés.

Visualiser des données d'indicateur/de métrique

L'aptitude Amélioration des processus vous permet d'afficher des données sur la performance des processus de gestion pour les événements terminés avec succès, retirés, annulés et terminés avec succès dans les formats suivants :

- Graphique à barres : cette vue par défaut affiche le délai moyen d'exécution des définitions de processus de gestion correspondant aux critères de filtre . Cliquez sur une barre pour Inspecter le détail de l'exécution du processus de gestion .

Note: Si des données de référence sont disponibles, une ligne sur le graphique à barres représente les données de référence. Voir [Comparer avec les données de référence](#) .

- **Tableau** : le tableau affiche les métriques d'exécution, y compris le délai moyen d'exécution et les renvois. Les indicateurs incluent les valeurs de référence (valeurs de environnement client) et de référence, le cas échéant. Vous pouvez trier les colonnes en cliquant sur le cheminement pour afficher les types d'indicateur/de métrique suivants :
 - **Moyenne** : valeur moyenne d'un indicateur/une métrique.
 - **Maximum** : valeur maximum d'un indicateur/une métrique.
 - **Minimum** : valeur minimum d'un indicateur/une métrique.
 - **p50** : la valeur p50, ou médiane, est la valeur en dessous de laquelle 50 % des valeurs d'indicateur/de métrique constatées concernent l'environnement client ou le benchmark au cours de la période sélectionnée . Exemple : 50 % des événements sont terminés en 20 heures, tandis que les 50 % restants prennent plus de temps.
 - **p95** : le p95 est la valeur en dessous de laquelle 95 % des valeurs d'indicateur/de métrique constatées se trouvent pour l'environnement client ou le benchmark dans la période sélectionnée . Exemple : 95 % des événements sont terminés en 37 heures, tandis que les 5 % restants prennent plus de temps.
- **Graphique linéaire** : cette vue affiche la tendance des performances des processus de gestion sur une période donnée. Vous pouvez cliquer sur chaque point pour afficher plus d'informations sur l'exécution du processus de gestion .

Pour exporter des graphiques à barres et des graphiques linéaires au PDF ou linéaire :

1. Sur un graphique à barres ou un graphique linéaire, cliquez sur **Actions associées** .
2. Sélectionnez **Télécharger au PDF** ou **Télécharger au format PNG** .

Pour faciliter l'analyse des données et des références, vous pouvez également exporter des tableaux aux formats CSV et Excel. Les exportations incluent toutes les valeurs disponibles. (Exemple : moyen, maximum, p95.)

Comparer avec les données de référence

Si des données de référence sont disponibles, le graphique à barres affiche une ligne de référence sur les barres du processus de gestion . Lorsqu'il n'existe qu'une seule définition du processus de gestion, les données de référence s'affichent sous la forme d'un point noir au lieu d'une ligne horizontale. Les lignes de référence vous permettent de comparer les performances des processus de gestion de votre unité légale avec celles d'autres unités légales du même secteur, de la même région et de la même taille unité légale . La vue **Table** inclut également des indicateurs de référence.

L'agent Optimisation des processus de gestion génère des données de référence en :

- Moyenne des données d'exécution pour les clients qui partagent/partager les critères suivants : secteur d'activité, région et taille de l'entreprise.
- Déterminer le groupe de référence d'un environnement client en référençant les données de l'environnement client dans les enregistrements Workday .

L'agent Optimisation des processus de gestion n'affiche pas les données de référence lorsqu'il n'y a pas suffisamment de clients dans la cohorte de pair de benchmarking de l'environnement client pour atteindre le seuil minimum configuré.

Réviser des analyses sur le benchmarking

Lorsque vous inspectez un processus de gestion, vous pouvez bénéficier analyses comparatives plus approfondies qui identifient précisément les performances de vos processus de gestion par rapport à ceux de votre cohorte de pair .

La section **Benchmarking** :

- Met en évidence les domaines dans lesquels la performance de votre processus de gestion est en retard ou la dépasse par rapport à vos benchmarks liés au secteur, à la région et à unité légale .

- Analyse les exécutions au niveau des étapes pour identifier jusqu'à 5 étapes spécifiques avec la durée la plus élevée pour votre environnement client.
- Compare les différences de configuration entre votre environnement client et vos pairs les plus performants, à la fois au niveau de la définition et sur l'ensemble de ces cinq étapes, afin de générer des recommandations d'optimisation exploitables. L'agent n'affiche pas les données de comparaison lorsque votre cohorte de pair benchmarking n'a pas suffisamment de clients.
- Évalue uniquement le trimestre que vous avez sélectionné.
- Inclut les événements dont le statut est *Terminé avec succès*, *Retiré*, *Annulé* ou *Processus terminé*.
- Exclut toutes les étapes configurées après l'étape *Finalisation*. L'agent considère qu'un processus de gestion est terminé même si le workflow dépasse cette étape.

Respecter les tendances anormales

Lorsque vous sélectionnez un processus de gestion dans un graphique ou une table et que vous cliquez sur **Inspecter**, la page Inspecter s'ouvre dans un onglet distinct qui vous permet d'afficher des analyses plus approfondies sur les tendances afin de vous aider à identifier les anomalies, les modèles ou les modifications apportées à la performance des processus de gestion au performance moyenne dans la durée.

La section **Tendances** :

- Affiche le comportement d'un processus de gestion spécifique dans la période sélectionnée par rapport à la période précédente. Exemple : lorsque T1 2025 est la période sélectionnée, l'agent compare la performance du processus de gestion dans l'environnement client entre le T1 2026 et le T4 2025.
- Inclut uniquement les événements lancés et terminés au cours de la période sélectionnée. L'agent exclut les événements qui commencent dans une période mais qui se terminent dans une période suivante. Exemple : lorsque T1 2026 est la période sélectionnée, l'agent compare uniquement les événements lancés et terminés en T1 2026 à des événements lancés et terminés au T4 2025. Cela exclut les événements commencé au premier trimestre 2026 mais terminés au deuxième trimestre 2026.
- Inclut les événements dont le statut est *Terminé avec succès*, *Retiré*, *Annulé* ou *Processus terminé*.
- Exclut toutes les étapes configurées après l'étape *Finalisation*. L'agent considère qu'un processus de gestion est terminé même lorsque le workflow dépasse cette étape.
- Affiche les recommandations d'optimisation lorsque les tendances des processus de gestion diminuent. Il n'affiche pas de recommandations lorsque la tendance d'un processus de gestion est plus rapide que dans la période précédente.
- Identifie les causes profondes de la tendance.

L'agent identifie les changements significatifs dans les exécutions au niveau des étapes entre les deux périodes et détermine les étapes qui ont le plus d'impact sur l' modifier/changer des performances des processus de gestion. Elle calcule également le pourcentage de contribution de chaque étape identifiée pour indiquer son impact parent.

Identifier les anomalies et les causes premières

Lorsque vous inspectez un processus de gestion, vous pouvez voir des modèles d'exécution anormaux, qui identifient les processus de gestion problématiques devant être résolus ou optimisés.

La section **Anomalies** :

- Met en évidence les exécutions de processus de gestion inhabituelles et décrit le mode de fonctionnement d'un processus de gestion spécifique au cours de la période spécifiée.
- Inclut les événements dont le statut est *Terminé avec succès*, *Retiré*, *Annulé* ou *Processus terminé*.
- Inclut les événements qui se terminent au cours de la période sélectionnée, même lorsque les événements ont commencé avant la période sélectionnée. Exemple : lorsque T1 2026 est la période sélectionnée, l'agent identifie les anomalies dans les processus de gestion terminés au 1er trimestre 2026, y compris les événements terminés qui ont commencé avant le 1er trimestre 2026.

- Exclut toutes les étapes configurées après l'étape *Finalisation* . L'agent considère qu'un processus de gestion est terminé même lorsque le workflow dépasse cette étape.
- Répertorie les causes profondes principales et les principales étapes contributives aux transactions anormales.

L'agent analyse les événements identifiés comme anormaux dans la période sélectionnée et identifie les étapes qui ont le plus grand impact négatif sur la performance du processus de gestion .

L'agent affiche les éléments suivants :

- Indicateur calculé pour la cause initiale, tel que la durée, les renvois ou la réaffectation.
- Étapes spécifiques qui contribuent à l'anomalie, notamment le nombre d'événements dans lesquels cette étape est détectée comme anormale, le temps moyen écoulé par cette étape dans ces événements et le nombre total d'occurrences de cette anomalie (par exemple, renvois ou réaffectation).

Générer des recommandations d'optimisation

L'agent Optimisation des processus de gestion fournit des recommandations d'optimisation pour analyses les tendances et les modèles d'exécution anormaux. Notez que l'agent affiche la section **Tendances** uniquement lorsque les tendances d'un processus de gestion sont plus lentes que dans la période précédente .

Lorsque vous révisez les analyses des sections **Tendances et anomalies** , l'agent :

- Génère de manière dynamique des recommandations personnalisées en temps réel au lieu de s'appuyer sur des données précalculées. Ce processus de génération peut prendre jusqu'à une minute.
- Formule des conseils décisionnels pour vous aider à résoudre et à optimiser les étapes des processus de gestion problématiques. Le modèle de langage de l'agent Optimisation des processus de gestion utilise le Guide de l'administrateur Workday , le Workday Community et d'autres sources de connaissances approfondies de Workday .
- Fournit des liens de référence sous **En savoir plus** , lorsqu'ils sont disponibles.

Si la génération des recommandations échoue et que vous recevez un message erreur , réessayez de générer les recommandations.

Recommandations liées à l'optimisation implémentée

Bien que l'agent Optimisation des processus de gestion personnalise les recommandations en fonction des anomalies signalées, examinez toujours attentivement les recommandations d'optimisation générées et déterminez comment elles s'adaptent à votre organisation et à des processus de gestion spécifiques. Il peut exister des opportunités d'optimisation au-delà des recommandations fournies.

Après avoir implémenté une recommandation ou apporté une modifier/changer de configuration à un processus de gestion, vous pouvez :

-
- Afficher le graphique linéaire dans le tableau de bord de **l'agent Optimisation des processus de gestion** . Le graphique linéaire vous permet d'analyser la performance du processus de gestion et d'identifier les modifications de performance éventuelles.
- Utiliser l'agent Optimisation des processus de gestion pour consulter les dernières tendances, la analyses des anomalies et les benchmarks. En utilisant l'agent de manière itérative, vous pouvez identifier d'autres recommandations et opportunités d'optimisation.

Référence : exemples d'invites de l'agent Optimisation des processus de gestion

Lorsque vous cliquez sur l' icône en bulles de tchat de l'agent Workday , vous pouvez saisir des invites spécifiques sur l'optimisation des processus de gestion . Lorsque plusieurs agents sont configurés, vous

devrez peut-être accéder au chat de l'agent et sélectionner l' **agent Optimisation des processus de gestion** dans le menu de l'agent.

Consultez ces exemples pour vous aider à structurer efficacement vos invites.

Cas d'utilisation	Exemples d'invite
Analyse des processus de gestion	- Affiche les 3 processus de gestion les plus performants par durée au 1er 2026. - Quels sont les trois processus de gestion Changer d'emploi les plus performants ? - Quels sont les cinq plus faibles nombres de renvois en décembre 2025 ?
Analyses des tendances	- Pouvez-vous partage/partager des analyses sur les tendances sur Demander une absence pour une délégation de collaboration ? - Comment améliorer les performances dégradées ? - Quelle est la tendances des processus de gestion Changement d'emploi en 2026 ?
Données de référence	- À quelles régions puis-je comparer mes données ? - Quels sont les benchmarks pour les demandes d'absence pour les services financiers ? - Quel est le benchmark des candidatures dans la région Europe pour le premier trimestre 2026 ?
Analyse des anomalies	- Quel processus de gestion a le taux d'anomalies le plus élevé au 4e trimestre 2025 ? - Quelle est la cause première des anomalies sur les processus de gestion Changement d'emploi au premier trimestre 2026 ? - Quelles sont les recommandations pour supprimer les anomalies des candidatures pour le marketing Web en 2025 ? - Pouvez-vous suggérer d'autres recommandations pour l' étape de lancement de la Candidature pour le marketing Web ? - Pouvez-vous fournir des instructions détaillées pour votre première recommandation ?

Agent Paie

Définir l'agent Paie

Prerequisites

Note: Des étapes supplémentaires peuvent être nécessaires pour activer cette fonctionnalité en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services (MSA), soit sur le Contrat-cadre de services universel (UMSA). Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().
4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- *UMSA* , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- *MSA* , votre organisation doit activer l'UMSA.
- Activez la [politique de crédits variables et de droits à la plateforme de Workday](#) dans les environnements clients de production.
- [Définir l'agent Système d'enregistrement](#)
- Sécurité :
 - Domaines suivants dans le domaine fonctionnel Agent System of Record :
 - *Conformité de l'agent*
 - *Hub Gestion des agents*
 - *Manage: Agents*
 - *Reports: Agent Reporting*
 - *Setup: Agents*
 - *Reports: AI Agent Security* dans le domaine fonctionnel System.

Context

Vous pouvez définir l'agent Paie pour permettre à vos professionnels de la paie d'accéder et d'utiliser ses aptitudes. L'agent Paie assure l'assistance dans les tâche , la récupération d'informations et la synthèse des données via une IA conversationnelle.

Steps

1. Accédez au rapport **Hub Gestion des agents** .
2. Sélectionnez l'onglet **Agent Workday non enregistré** .
3. Pour l' **agent Paie** , cliquez sur **Enregistrer** .
4. Cochez la case à cocher **Confirmer** , puis cliquez sur **OK** pour finaliser l'enregistrement.
Workday transfère l' **agent Paie** vers l'onglet **Registre de l'agent** .
5. Sélectionnez l'onglet **Registre de l'agent** , puis cliquez sur le nom *de l'agent Paie* pour configurer l'agent.
6. Dans la vue du profil de l'agent, cliquez sur **Configurer l'agent** .
7. Dans la colonne **Statut** , rendez chaque aptitude pertinente disponible en activant le carrousel à bascule .

8. Pour chaque **aptitude** activée, renseignez l'invite **Disponible pour** avec les groupes de sécurité auxquels vous voulez autoriser l'accès pour cette aptitude spécifique. Les groupes de sécurité ajoutés à l'invite **Disponible** pour d'un agent établissent la règle d'interaction de l'agent.

Note: Les groupes de sécurité que vous sélectionnez dans l'invite **Disponible pour** doivent également disposer d'autorisations sur les règles de sécurité du domaine ou du processus de gestion qui sécurisent les outils de l'agent Paie. Vous pouvez utiliser le rapport **Afficher la sécurité des aptitudes de l'agent** pour vous aider à configurer vos agents. Ce rapport affiche des informations détaillées sur les API Outils de l'agent Paie et les règles de sécurité et autorisations relatives au domaine ou au processus de gestion. Au moment de l'exécution de l'agent, Workday évalue à la fois l'accès utilisateur à l'agent et l'accès utilisateur aux API qu'il exécute en tant qu'outils.

9. Cliquez sur **Activer**. Vous pouvez également enregistrer et revenir à cette configuration. La configuration de l'agent peut être mise à jour à tout moment. Lorsque vous activez l'agent Paie, l'ASU de l'agent s'active également automatiquement.

Result

Vous pouvez accéder au chat de Workday pour utiliser l'agent Paie.

Next Steps

(Facultatif) Définissez la configuration supplémentaire pour :

- Notifications aux employés pour lesquelles des options de paiement sont manquantes pour l'aptitude Identifier les données manquantes et Configuration.
- Aptitude Analyse du salaire minimum.

(Facultatif) Lorsque vous avez terminé avec l'agent Paie, vous pouvez cliquer sur **Désactiver** pour le désactiver. Vous pouvez activer, désactiver et réactiver l'agent Paie à tout moment dans le **hub Gestion des agents**. Lorsque vous désactivez un agent, l'ASU de l'agent est également désactivé automatiquement.

Concept : agent Paie

Aperçu

L'agent Paie est un assistant conversationnel basé sur l'IA conçu pour améliorer l'expérience des professionnels de la paie dans Workday.

Les aptitudes de l'agent Paie sont les suivantes :

- Récupération des données de paie de base : permet à l'agent de récupérer des informations de base sur les salariés, les lots de paie, les unités légales et plus encore.

Note: Cette aptitude est obligatoire pour le fonctionnement d'autres aptitudes.

- Analyses des données de la paie : Donne accès aux connaissances en matière de paie et effectue des actions pour les utilisateurs, en impliquant une intervention manuelle si nécessaire.
- Identification des données manquantes et configuration : permet de surveiller le système pour rechercher les données de paie critiques manquantes ou obsolètes nécessitant l'intervention d'un professionnel de la paie.
- Analyse du salaire minimum : permet d'analyser l'impact des modifications du taux de salaire minimum pour des États des États-Unis et des provinces du Canada.

Note: Nous vous recommandons d'établir de bonnes pratiques en matière de consultation, modification et vérification de l'exactitude du contenu généré par l'IA avant de l'utiliser.

L'agent Paie est disponible dans tous les pays de Workday Payroll :

- Workday Payroll for Australia

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

Limites

L'agent Paie :

- Utilise l'IA conversationnelle, une technologie en constante évolution. Bien que conçu et testé pour une haute précision, il peut parfois interpréter des questions erronées ou présenter des résultats inattendus. Réviser toujours la sortie, y compris les nombres et les commentaires. Avant d'agir sur les résultats, vérifiez-les par rapport à la source de données.
- contribue à uniquement l'anglais américain.
- Mémoire seulement 20 interactions dans une séquence.

Les sessions proxy excluent la fonctionnalité de l'agent Paie.

Certaines fonctionnalités de l'agent ne s'appliquent qu'à des pays spécifiques. Exemple : vous pouvez uniquement utiliser l'aptitude Identifier les données manquantes et Configuration pour rechercher et mettre à jour les calendriers de périodes des employés FLSA arrivant à expiration pour Workday Payroll for the US.

Vous pouvez :

- Présentez un délai temporaire dans la réponse de l'agent ().
- Recevoir des réponses de l'agent pour les questions non liées aux aptitudes de l'agent Paie.

Définir l'identification des données manquantes et des notifications de configuration pour les employés sans options de paiement

Prérequis

Sécurité : domaine *Worker Data: Payroll (Payment Elections)* dans le domaine fonctionnel Core Payroll.

Contexte

Lorsque vous définissez l'agent Paie, vous pouvez immédiatement utiliser l'aptitude Identifier les données manquantes et Configuration dans le chat Workday .

Par défaut, les employés sans options de paiement recevoir une notification en fonction des paramètres du type de notification parent configurés dans l'onglet **Paie** de la tâche **Modifier la définition de l'environnement client - notifications** . Voir [Référence : modifier la définition de l'environnement client - notifications](#) .

Workday envoie automatiquement une notification dans la boîte de réception des employés pour lesquels des options de paiement sont manquantes lorsque vous lancer la tâche Rechercher les employés manquant dans les options de paiement à l'aide de l'aptitude Identifier les données manquantes et Configuration.

Vous pouvez également :

- Configurez un remplacement d'envoi afin que Workday envoie des notifications par e-mail supplémentaires aux employés pour lesquels des options de paiement sont manquantes.
- Personnalisez le contenu des notifications par e-mail que les employés recevoir.

Si vous souhaitez envoyer des notifications par e-mail aux employés, vous devez configurer le remplacement des envois avant d'utiliser l'aptitude Identifier les données manquantes et Configuration.

Steps

1. Configurez un remplacement de remise pour les notifications par e-mail envoyées aux employés pour lesquels des options de paiement sont manquantes.
 - a) Accédez à la tâche **Modifier la définition de l'environnement client - notifications**.
 - b) Dans la section **Paramètres de remise des notifications**, sélectionnez l'onglet **Paie**.
 - c) Dans la colonne **Type de notification**, sélectionnez *Options de paiement manquantes*.
 - d) Cochez la case à cocher **les paramètres du type de notification parent**.
 - e) Dans l'invite **Règle**, sélectionnez *Créer une règle de routage de notification*.
 - f) Renseignez la section **Créer une règle de routage de notification**:

Option	Description
Utilisation du type de notification	Sélectionnez <i>Options de paiement manquantes</i> .
Fréquences de canal	Cliquez sur Ajouter .
Canal	Sélectionnez <i>E-mail</i> .
Fréquence par défaut	Sélectionnez <i>Immédiatement</i> .

- g) Cliquez sur **OK**.

Sécurité : domaine *Set Up: Tenant Set Up - BP and Notifications* dans le domaine fonctionnel System.

2. Affichez le modèle d'e-mail par défaut pour les notifications envoyées aux employés sans options de paiement afin de vérifier si vous souhaitez apporter des modifications.
 - a) Accédez au rapport **Comportements de modèle d'e-mail**.
 - b) Sélectionnez le titre de la colonne **Comportement de modèle d'e-mail**.
 - c) Dans l'invite **Valeur**, sélectionnez *E-mail des options de paiement manquantes*.
 - d) Cliquez sur **Filtrer**.
 - e) Sélectionnez l'option **Comportement du modèle d'e-mail** *relatif aux options de paiement manquantes* pour afficher le comportement du modèle d'e-mail.
3. Modifiez le modèle d'e-mail par défaut pour les notifications envoyées aux employés pour lesquels des options de paiement sont manquantes.
 - a) Accédez à la tâche **Créer un modèle d'e-mail**.
 - b) Renseignez la section **Créer un modèle d'e-mail**:

Option	Description
Comportement de modèle d'e-mail	Sélectionnez <i>E-mail concernant les options de paiement manquantes</i> .

- c) Cliquez sur **OK**.
- d) Cliquez sur l'icône **Ajouter une ligne** pour ajouter les lignes suivantes dans la grille:

Ordre	Description
1	1. Sélectionnez Contenu statique. 2. Dans l'invite Contenu statique, sélectionnez <i>Créer un texte d'e-mail statique</i>. 3. Dans le champ Texte, saisissez le contenu que vous souhaitez afficher comme en-tête de la notification.
2	1. Sélectionnez Contenu statique.

Ordre	Description
	2. Dans l'invite Contenu statique , sélectionnez <i>Créer un texte d'e-mail statique</i> . 3. Dans le champ Texte , saisissez le contenu que vous souhaitez afficher comme corps de la notification.
3	1. Sélectionnez Contenu dynamique . 2. Dans l'invite Contenu statique dynamique , sélectionnez <i>Lien interactif</i> .

e) Cliquez sur **OK**, puis sur **Terminé**.

Sécurité : domaine *Set Up: System* dans le domaine fonctionnel System.

4. Vérifiez que le modèle d'e-mail personnalisé que vous avez créé est désormais actif.

- Accédez à la tâche **Mettre à jour les modèles d'e-mail**.
- Dans la ligne **E-mail des options de paiement manquantes** , vérifiez que la case à cocher **Actif** est cochée pour votre modèle d'e-mail personnalisé .
- Cliquez sur **OK**.

Sécurité : domaine *Set Up: System* dans le domaine fonctionnel System.

Result

Après avoir configuré vos notifications par e-mail :

- Les employés sans options de paiement recevoir les deux notifications dans leur boîte de réception Workday et par e-mail s'ils configurent leur adresse e-mail dans Workday.
- Les notifications que les employés recevoir contiennent votre contenu personnalisé.

Définir une aptitude d'analyse du salaire minimum

Prerequisites

Sécurité :

- Domaine *Set Up: Minimum Wage Agent* dans les domaines fonctionnels suivants :
 - Paie CAN
 - Paie USA
- Domaine *Set Up: Payroll (minimum Wages View)* - CAN dans le domaine fonctionnel CAN Payroll.
- Domaine *Set Up: Payroll (Maximum Wages View)* - USA dans le domaine fonctionnel USA Payroll.
- Domaine *Set Up: Payroll (Taxes View)* dans le domaine fonctionnel Core Payroll.

Context

Vous pouvez utiliser l'agent Paie pour analyser les nouveaux taux de salaire minimum dans les États américains et les province canadiennes. Pour utiliser l'aptitude Analyse du salaire minimum, vous devez configurer votre environnement client en fonction des étapes ci-dessous afin que les administrateurs de la paie disposent des autorisations nécessaires pour accéder aux données de paie pertinentes.

Nous vous recommandons d'établir de bonnes pratiques pour la révision, la modification et la vérification de l'exactitude du contenu généré par l'IA avant utilisation.

Steps

1. Activez le domaine *Set Up: Minimum Wage Agent* .
 - a) Accédez au rapport **Afficher un domaine** .
 - b) Dans l'invite **Domaine** , sélectionnez *Set Up: Minimum Wage Agent* .
 - c) En regard de **Règle de sécurité de domaine** , cliquez sur l'icône de la loupe.
 - d) Dans les **Autorisations de rapport/tâche** , vérifiez que les groupes de sécurité disposent des droits d'accès *Afficher et Modifier* .
 - e) (Facultatif) Cliquez sur **Modifier les autorisations** .
Modifiez les groupes de sécurité et cochez les cases *Afficher* et *Modifier* selon vos besoins.
 - f) Cliquez sur **OK** , puis sur **Terminé** .
 - g) (Facultatif) [Activez les modifications de règle de sécurité en attente](#) .

Sécurité : domaine *Security Configuration* dans le domaine fonctionnel System.

2. Activez le planificateur en arrière-plan du salaire minimum.
 - a) Accédez à la tâche **Modifier la définition de l'environnement client - paie** .
 - b) Dans la section **Options de cotisations/Taxes** , cochez la case **Planificateur en arrière-plan du salaire minimum** .
 - c) Cliquez sur **OK** , puis sur **Terminé** .

Lorsque vous activez le planificateur en arrière-plan Salaire minimum :

- L'agent de la paie affiche uniquement les coûts estimés pour l'employeur en fonction des taux de salaire minimum modifiés que les administrateurs de la paie peuvent afficher dans le tchat de Workday après 01h00 (PST) le lendemain.
- Les calculs des coûts estimés pour l'employeur incluent uniquement les employés concernés dont l'affectation de régime horaire applique un salaire minimum.

Sécurité : domaine *Set Up: Tenant Setup - Payroll* dans le domaine fonctionnel System.

Result

Dans le tchat de Workday :

- Vous pouvez saisir une requête dans liée aux nouveaux taux de salaire minimum.
- L'agent Paie génère une analyse de la façon dont les nouveaux taux de salaire minimum affectent les coûts pour l'employeur.

Concept : identification des données manquantes et aptitudes de configuration

Aperçu

L'aptitude Identifier les données manquantes et Configuration de l'agent Paie vous aide à :

- Rationaliser le traitement de la paie en identifiant les données et les configurations qui requièrent votre attention.
- Prendre des mesures pour résoudre de manière proactive les problèmes potentiel .

Cette aptitude vous permet de :

- Surveillez et identifiez les données obsolètes ou manquantes et les configurations critiques pour la paie.
- Prenez des mesures pour résoudre les problèmes de données et de configuration , notamment l'envoi de notifications et la réalisation de mises à jour.

Vous pouvez utiliser cette aptitude pour rechercher et :

- Avertissez les employés pour lesquels des options de paiement sont manquantes pour un type de paie à l'aide de la Règle de la paie, dans la tâche **Mettre à jour les règles d'option de paiement** . Cette fonctionnalité s'applique à tous les pays de Workday Payroll.

- Mettez à jour les calendriers FLSA configurés pour expirer dans les 90 jours suivant la date du jour. Cette fonctionnalité s'applique uniquement à Workday Payroll aux États-Unis.

Comment y accéder ?

Avant d'accéder à l'agent Paie dans votre environnement client, vous devez avoir :

- Options de paiement des employés. Voir [Étapes : définir les options de paiement](#) .
- Calendriers de périodes de travail FLSA. Voir [Créer des calendriers de périodes de travail FLSA \(USA\)](#) .

Vous devez également avoir accès à des domaines de sécurité spécifiques pour utiliser les différentes fonctionnalités de l'aptitude :

Domaine	Fonctionnalités
domaine <i>Worker Data: Payroll (Payment Elections)</i> dans le domaine fonctionnel Core Payroll	Rechercher et notifier les employés pour lesquels des options de paiement sont manquantes
domaine <i>Set Up: Payroll (FLSA) - USA</i> dans le domaine fonctionnel USA Payroll	Rechercher et mettre à jour les calendriers de périodes de travail FLSA arrivant à expiration

Pour utiliser l'aptitude Identification des données manquantes et configuration :

1. Une fois que vous avez configuré l'agent Paie et que vous êtes dans le groupe de sécurité affecté , vous pouvez cliquer sur la bulle dans la barre de navigation supérieure pour lancer Workday Chat.
2. Saisissez une requête liée à la recherche et :
 - Notifier les employés pour lesquels les options de paiement sont manquantes.
 - Mettant à jour les calendriers FLSA arrivant à expiration.

Notifications pour les employés sans options de paiement

Vous pouvez lancer la tâche Rechercher les employés sans options de paiement à l'aide de l'aptitude Identifier les données manquantes et Configuration.

Pour configurer la façon dont Workday envoie une notification aux employés lorsqu'il manque des options de paiement, voir [Définir l'identification des données manquantes et des notifications de configuration pour les employés sans options de paiement](#) .

Lorsque vous recherchez des employés sans options de paiement à l'aide de l'agent Paie, Workday vous envoie automatiquement une notification en cliquant sur l' icône en forme de anneau, une fois le traitement terminé.

La notification que vous recevez inclut des informations telles que :

- Le lot de paie associé des employés.
- Les employés sans options de paiement.
- Si Workday a notifié ou non les employés identifiés par l'agent Paie.

Notifications pour les calendriers FLSA arrivant à expiration

Vous pouvez lancer la tâche Planifier la mise à jour du calendrier de périodes de travail FLSA à l'aide de l'aptitude Identifier les données manquantes et Configuration.

Lorsque vous mettez à jour un calendrier FLSA arrivant à expiration à l'aide de l'agent Paie, Workday vous envoie automatiquement une notification avec une notification en cliquant sur l' icône en forme de con demander dès que le traitement est terminé.

La notification que vous recevez inclut des informations telles que :

- Nom du calendrier de périodes de travail FLSA mis à jour .

- Nombre de périodes de travail dont vous avez demandé l'ajout.

Exemples de requêtes pour identifier les données et la configuration manquantes

- Je dois rechercher et intervenir sur les données manquantes et les paramètres liés à la paie. Que puis-je faire d'aide ?
- Identifier et mettre à jour les calendriers de travail FLSA arrivant à expiration.
- Rechercher et notifier les employés pour lesquels des options de paiement sont manquantes.

Concept : aptitude d'analyse du salaire minimum

Aperçu

L'aptitude Analyse du salaire minimum de l'agent Paie vous permet de fournir une analyse des données contextuelles et des analyses sur les taux et les coûts de salaire minimum .

Cette aptitude vous permet de réviser et d'analyser l'impact des taux de salaire minimum au cours des 6 derniers mois ou jusqu'à 6 mois à venir. Lorsque vous interrogez l'agent Paie, Workday utilise l'IA pour générer une analyse sur les coûts estimés pour l'employeur et le nombre de salariés concernés par les nouveaux taux de salaire minimum aux États-Unis et au Canada.

Cette aptitude n'est applicable que pour :

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

Comment y accéder ?

Avant de pouvoir accéder à cette aptitude, vous devez configurer les données et les autorisations nécessaires. Consulter [Définir une aptitude d'analyse du salaire minimum](#) .

Accédez au Chat dans Workday depuis votre page d'accueil et saisissez une requête relative aux taux de salaire minimum .

Limites

Vous pouvez uniquement utiliser l'aptitude Analyse du salaire minimum pour analyser les nouveaux taux de salaire minimum pour des États américains et des provinces du Canada.

Exemples de requête

- Quel est le salaire minimum pour cet état ou cette province ?
- Quel est le taux de salaire minimum pour cet état ou cette province à cette date ?
- Combien d'employés sont concernés par la modifier/changer du salaire minimum ?
- Montre-moi comment ce taux de salaire minimum affectera les coûts globaux pour l'employeur.

Concept : aptitude Analyses des données de la paie

Aperçu

L'aptitude Analyses des données de la paie de l'agent Paie vous permet d'accéder aux connaissances en matière de paie pour répondre à vos questions. Vous pouvez poser des questions et recevoir des réponses sur les données dont vous avez besoin de manière conversationnelle simple. Cela réduit les tâches manuelles et le temps consacré à la génération de rapports, ce qui peut éviter de devoir créer certains rapports personnalisés grâce à la mise à disposition directe des données.

Exemple : pour un audit, un administrateur de la paie a besoin d'un point de données spécifique . Au lieu d'exécuter plusieurs rapports, ils peuvent poser une question en langage naturel, par exemple : « *Afficher tous les lot de paie dans le système sur une base hebdomadaire ou toutes les deux semaines* ». Ils peuvent également poser des questions de suivi, telles que « *Afficher* » "mois" chaque employé dans [retourné dans

le lot de paie hebdomadaire1] ayant fait plus de 4 000 USD de brut pour la dernière période de paie terminée ." L'agent fournit ensuite les données à présélection/présélectionner. Il inclut des analyses et des analyses en langage naturel, ainsi qu'un affichage des données de manière intuitive.

Comment accéder à

Une fois que vous avez configuré l'agent Paie et que vous êtes dans le groupe de sécurité affecté , vous pouvez cliquer sur la bulle dans la barre de navigation supérieure pour lancer Workday Chat.

Limites

Actuellement, l'aptitude Analyses des données de la paie peut répondre aux types de question suivants :

Types de question	Exemples
Moyennes	Quel était le salaire brut moyen des employés dans [lot de paie] sur les trois dernières périodes ?
Salaire de base de l'employé	Quel était le montant de [noms employé] [soit le salaire brut ou le net à payer] lors de la dernière période ?
Salaire de base	Peux-tu afficher tous les employé de [lot de paie] ayant créé plus de [montant] en [mois] ?
Informations de base sur le lot de paie	Quels lots de paie sont payés sur une base mensuelle ?
Inclusion de gains ou de déductions	Répertorier tous les gains et déductions avec des valeurs actuelles.
Exclusion de gains ou de déductions	Quels employés de [lot de paie] n'ont pas eu [quelque gains (HCM)/ déduction] au cours de leur dernière période ?
Comparaison de périodes	Comparez le salaire brut de [nom du lot de paie] du dernier trimestre 2025 au premier trimestre 2026.

FAQ : Agent Paie

L'agent Paie respecte-t-il la sécurité ?	Oui, l'agent Paie respecte la sécurité existante pour la paie.
Pourquoi est-ce que je n'arrive pas à afficher le hub Gestion des agents ?	Vous devez vérifier que : - Le domaine fonctionnel Agent System of Record est défini et activé. - Les utilisateurs appropriés se trouvent dans le domaine de sécurité approprié pour accéder au hub Gestion des agents.
À quels types de question l'agent Paie peut-il répondre ?	Pour plus d'informations sur les questions auxquelles l'agent Paie peut vous aider, en fonction de l'aptitude que vous souhaitez utiliser, consultez les rubriques suivantes : Concept : aptitude Analyses des données de la paie

	• Concept : identification des données manquantes et aptitudes de configuration • Concept : aptitude d'analyse du salaire minimum
L'agent Paie pour s' retrouver un problème avec ce problème plus tôt dans le tchat. Que puis-je faire ?	Vous pouvez essayer de poser la question d'une autre manière ou de démarrer un nouveau fil.
Pourquoi l'agent Paie ne répond-il pas aux questions liées aux plans de rémunération , aux centres de coûts ou à des calculs de paie spécifiques, comme les heures supplémentaires?	Actuellement, l'agent Paie peut uniquement réviser et répondre aux questions liées aux éléments suivants : • Résultats de paie • Lignes de résultat • Informations de base sur employé • Informations sur le lot de paie

Agent Libre-Service Sana

Définir l'agent Libre-service

Prerequisites

Note: Des étapes supplémentaires peuvent être nécessaires pour activer cette fonctionnalité en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services (MSA), soit sur le Contrat-cadre de services universel (UMSA). Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().
4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- [UMSA](#) , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- [MSA](#) , votre organisation doit activer le système UMSA.

Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser des agents en production tant que vous n'aurez pas accepté ces contrats. Le système UMSA est obligatoire pour les environnements clients autres que de production et de production pour les agents Workday-Built. L'UMSA n'est pas obligatoire pour les environnements clients autres que de production pour les agents auto-configurés.

- Activer [la politique de crédits variables et de droits à la plateforme de Workday](#) . obligatoire uniquement pour une utilisation dans les environnements clients de production.
- [Définissez l'agent Système d'enregistrement](#) .
- Sécurité : les domaines suivants dans le domaine fonctionnel Agent System of Record :
 - *Conformité de l'agent*
 - *Hub Gestion des agents*
 - *Manage: Agents*
 - *Reports: Agent Reporting*
 - *Setup: Agents*

- Sécurité : domaines suivants dans le domaine fonctionnel System :
 - *Reports: AI Agent Security*
 - *Applications Workday Graph API* . autorisation Afficher et modifier (rapport/tâche et intégration). Pensez à affecter ces autorisations au groupe de sécurité *Tous les salariés* ou *Tous les utilisateurs* pour garantir l'accès de tous les salariés/utilisateurs.

Context

Vous pouvez enregistrer, configurer et activer l'agent Libre-service dans Workday à l'aide du **hub Gestion des agents** .

Steps

1. Accédez au rapport **Hub Gestion des agents** .
2. Sélectionnez l'onglet **Agent Workday non enregistré** .
3. Pour l' **agent Libre-service** , cliquez sur **Enregistrer** .
4. Cochez la case à cocher **Confirmer** , puis cliquez sur **OK** pour finaliser l'enregistrement. Workday transfère l' **agent Libre-service** dans l'onglet **Registre de l'agent** .
5. Sélectionnez l'onglet **Registre de l'agent** , puis cliquez sur le nom de l'*agent Libre-service* pour configurer l'agent.
6. Dans la vue du profil de l'agent, cliquez sur **Configurer l'agent** .
7. Dans la colonne **Statut** , rendez chaque aptitude pertinente disponible en activant le carrousel à bascule .
8. Pour chaque **aptitude** disponible , renseignez l' invite **Disponible pour** avec les groupes de sécurité auxquels vous voulez autoriser l'accès pour cette aptitude spécifique.

Exemple : pour l'aptitude **de base ESS - Gestion du capital humain - de base** , sélectionnez le groupe de sécurité *Salarié (pour lui-même)* pour autoriser les salariés à accéder à cette aptitude et pour l'aptitude **de base MSS - Gestion du capital humain - Base** , sélectionnez les groupes de sécurité *Responsable* et *Chaîne hiérarchique* à l'autoriser uniquement. les responsables d'une chaîne hiérarchique qui ont accès à l'aptitude.

Note:

Workday évalue à la fois l'accès utilisateur à l'agent et l'accès utilisateur aux API que l'agent exécute en tant qu'outils au moment de l'exécution. C'est pourquoi Workday vous recommande d'évaluer l'alignement entre les groupes de sécurité dans l' invite **Disponible pour** et les groupes de sécurité disposant des autorisations pour les **outils**. que l'agent peut exécuter. Dans ce cadre, nous vous recommandons également de consulter la [FAQ sur les agents en libre-service](#) pour davantage de résolution de problèmes de sécurité.

Workday définit automatiquement les aptitudes ESS comme actives avec *Salarié (pour lui-même)* comme groupe de sécurité **Disponible** pour par défaut.

Bien que vous puissiez remplacer ces valeurs par défaut, vous devez conserver l'aptitude **Guide** en permanence, car il s'agit de l'aptitude principale sur laquelle l'agent obligatoire s'exécute.

9. Cliquez sur **Activer** .

Result

Workday affiche l' icône en bulles de tchat Workday dans la navigation globale pour vous et vos salariés. Les salariés ayant accès aux groupes de sécurité que vous avez indiqués pour chaque aptitude et à la règle de sécurité du domaine ou du règle de sécurité du processus de gestion associée aux API qui composent chaque aptitude peuvent utiliser l'agent Libre-service.

Concept : agent Libre-service

À propos de l'agent Libre-service

L'agent Libre-service est un agent d'IA conversationnel qui permet aux salariés et aux responsables d'effectuer des actions en libre-service dans Workday et Sana, telles que :

- Récupérer des informations interactives sur leurs données Workday , comme l'affichage des bulletins de paie récents, la mise à jour de leurs données personnelles et la demande d'absence.
- Gérer les objectifs de l'organisation et afficher les statuts de formation des équipes .
- Afficher des informations sur les politiques de leur organisation à partir d'articles de la base de connaissances stockés dans Workday.

Aptitudes : ESS et MSS

L'agent Libre-service contribue à les aptitudes pour les tâches en libre-service salarié et en libre-service responsable . Certaines aptitudes sont conçues spécifiquement pour les salariés ou les responsables et sont donc marquées du préfixe ESS ou MSS.

Note:

Workday définit automatiquement les aptitudes ESS comme actives avec *Salarié (pour lui-même)* comme groupe de sécurité **Disponible** pour par défaut.

Bien que vous puissiez remplacer ces valeurs par défaut, vous devez conserver l'aptitude **Guide en permanence**, car il s'agit de l'aptitude principale sur laquelle l'agent obligatoire s'exécute.

Aptitudes - de base et avancées

L'agent Libre-service contribue à les aptitudes de base et les aptitudes avancées. Les aptitudes de base prennent en charge des actions simples, tandis que les aptitudes avancées prennent en charge des actions plus complexes. Vous pouvez voir ce que chaque aptitude couvre dans la description de l'aptitude lorsque vous configurez les aptitudes dans l'agent.

Note: Workday évalue à la fois l'accès utilisateur à l'agent et l'accès utilisateur aux API que l'agent exécute en tant qu'outils au moment de l'exécution. C'est pourquoi Workday vous recommande d'évaluer l'alignement entre les groupes de sécurité dans l'invite **Disponible pour** et les groupes de sécurité disposant des autorisations pour les **outils** que l'agent peut exécuter. Dans ce cadre, nous vous recommandons également de consulter la [FAQ sur les agents en libre-service](#) pour davantage de résolution de problèmes de sécurité.

Comptes agents

Vous pouvez utiliser le rapport **Tous les comptes d'agents IA** sécurisé via le *domaine Domains: Workday Accounts* dans le domaine fonctionnel System pour afficher tous les comptes d'agent dans votre environnement client. Dans le rapport, cliquez sur les actions associées **du Compte Workday** en regard de la loupe pour **View Audit Trail** .

Éléments à prendre en compte supplémentaires pour l'agent Libre-service

L'agent Libre-service ne prend actuellement pas en charge l'utilisation avec des comptes chargé d'implémentation et proxy.

Si vous activez l'agent Libre-service et activez au moins une aptitude, nous masquer la bulle de chat de Workday Assistant afin de réduire la création de doublons dans l'interface utilisateur. Si vous activez un autre agent, par exemple l'agent Paie, mais pas l'agent Libre-service, vous pourrez voir deux icônes de chat en bulles (Workday Assistant et Workday Chat) dans l'interface utilisateur.

L'agent Libre-service ne prend actuellement pas en charge les actions déléguées, car la structure de l'agent système (ASU) ne prend pas encore en charge un modèle de sécurité de délégation . Par résultat, les actions initiées par un déléguer via l'agent Libre-service peuvent initialement s'afficher avec succès

dans la fenêtre de tchat, mais ne créent pas de demandes ou d'événements réels dans le système. Nous travaillons activement à la résoudre de ce problème.

Exemple : gérer vos absences à l'aide de l'agent Libre-service

Prerequisites

- Activer [la politique de crédits variables et de droits à la plateforme de Workday](#) . obligatoire uniquement pour une utilisation dans les environnements clients de production.
 - Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser des agents en production tant que vous n'aurez pas accepté ces contrats. Le système UMSA est obligatoire pour les environnements clients autres que de production et de production pour les agents Workday-Built. L'UMSA n'est pas obligatoire pour les environnements clients autres que de production pour les agents auto-configurés.
- [Définir l'agent Système d'enregistrement](#)
- [Définir l'agent Libre-service](#)
- API REST Demander une absence - obligatoire comme action de lancement du processus de gestion Demander une absence.
- Sécurité : domaine *Request Time Off* dans le domaine fonctionnel Time Off and Leave.

Context

Cet exemple décrit comment journal et gérer vos absences à l'aide de l'agent Libre-service dans Workday.

Scénario :

Vous voulez savoir comment utiliser efficacement vos absences cette année sur la base des jours fériés de unité légale et des absences rémunérées. Au lieu de comparer les rapports et les politiques de unité légale , vous souhaitez demander, en texte brut, le meilleur moyen d'optimiser et de planifier vos absences.

Steps

1. Accédez à l'agent Libre-service en cliquant sur l' icône de chat Workday dans la barre de navigation globale.
2. Saisissez une invite demandant à l'agent Libre-service des informations sur votre solde d'absences. Exemple : *Je souhaite prendre une absence de ce trimestre. Combien de jours dois-je prendre ? Inclure les jours fériés de unité légale et les congés sabbatiques.*
L'agent peut vous invite à apporter des informations supplémentaires, telles que :

- Indiquent le type absence .
- Indiquez la durée que vous souhaitez effectuer.

3. Répondez à l'agent et confirmez votre demande.
4. Répétez ce processus en posant cette question à l'agent Libre-service pour chaque trimestre à venir. Exemple : *Qu'en est-il du trimestre suivant ? Combien de jours puis-je prendre ?*

Result

L'agent affiche le détail de votre demande.

Next Steps

Réviser les informations et confirmez-les.

Référence : aptitudes de l'agent Libre-service

Niveau d'aptitude	Description
ESS - Aide - Aptitude avancée	Facilite l'envoi des demandes de support, permettant ainsi aux collaborateurs de passer au-delà de la collecte d'informations pour passer à une assistance active.
ESS - Gestion des talents - avancé	Permet aux salariés d'utiliser l'agent Libre-service pour effectuer des actions liées au cycle de vie de leur personnel en mettant à jour données personnelles et en demandant des attestations d'employeur.
ESS - Gestion du capital humain - Base	Permet à l'agent Libre-service de traiter les demandes des salariés liées à la récupération de données personnelles pour les fonctions principales HCM, notamment les profils des employé , le détail de la rémunération et des avantages sociaux, ainsi que les informations sur équipe .
ESS - Paie - Base	Permet à l'agent Libre-service de traiter les demandes des salariés liées à la rémunération, au paiement et aux formulaires fiscaux.
ESS - Gestion des talents - avancé	Permet aux salariés d'utiliser l'agent Libre-service pour effectuer des actions liées à des tâches complexes personnel , comme la soumission d'évaluations de la performance, la création de recommandations et la création d'objectifs.
ESS - Gestion des talents - base	Permet à l'agent Libre-service de aptitude des informations liées au développement professionnel des salarié , notamment les objectifs de performance, l'historique du feedback et les listes d'emplois internes.
ESS - Gestion du personnel - Avancé	Permet aux salariés d'utiliser l'agent Libre-service pour effectuer des actions liées à des personnel complexes, comme la soumission de demandes d'absence, le pointage d'arrivée/de sortie d'une période de travail, la saisie de tranches horaires et la soumission des heures.
ESS - Gestion du personnel - Base	Permet à l'agent Libre-service de aptitude des informations sur leur gestion des temps, leur planification et absence . Cette aptitude permet de traiter des demandes comme la vérification des soldes d'absences ou l'affichage des calendriers de travail.
Guide	Fournit une direction de navigation intelligente, garantissant l'exécution des tâche en guidant les utilisateurs vers le rapport ou la tâche Workday spécifique obligatoire. Note: Cette aptitude est obligatoire pour que l'agent Libre-service fonction.

Niveau d'aptitude	Description
MSS - Gestion du capital humain - Base	Permet à l'agent Libre-service de traiter les demandes des responsables visant à récupérer des informations essentielles sur équipe , notamment les structures de équipe , l'historique professionnel et les informations sur les subordonné direct .
MSS - Paie - Avancé	Permet à l'agent Libre-service de traiter les demandes des responsables liées au lancement d'actions financières, comme les demandes de saisies d'élément de paie. L'aptitude • Appelle le processus de gestion Demander des saisies d'élément de paie existant . • Utilise votre configuration de sécurité et de paie existante . • Respecte le segment de sécurité et la sécurité du domaine de élément de paie que vous configurez dans l'agent Libre-service. L'aptitude se concentre sur les employés de Workday Payroll et applique les règles clés suivantes : • Crée des saisies d'élément de paie uniquement pour les employés dans Workday Payroll. Lorsque le poste principal de l'employé se trouve dans un lot de paie externe , ou si l' employé n'est associé à aucun lot de paie, l'aptitude bloque la demande et renvoie un message indiquant que l' employé n'est pas disponible pour les demandes de saisie d'élément de paie . • Pour les employés ayant plusieurs emplois, lorsqu'un responsable demande une saisie d'élément de poste sans indiquer de poste, l'aptitude utilise par défaut la saisie correspondant au poste principal de l'employé à compter de la date de début de la saisie d'élément de paie.
MSS - Gestion des talents - avancé	Permet à l'agent Libre-service d'aider les responsables à piloter le cycle de performance et à effectuer des actions, comme la conduite d'évaluations, la modification des données des talents et l'exécution des transactions de développement équipe .
MSS - Gestion des talents - base	Permet à l'agent Libre-service d'aider les responsables à superviser le développement de leur équipe en récupérant la progression des objectif , en affichant les statuts de formation et en examinant le feedback de équipe .

Niveau d'aptitude	Description
MSS - Gestion du personnel - Base	Permet à l'agent Libre-service de traiter les demandes des responsables liées à la récupération d'informations sur les opérations de équipe , notamment les soldes d'absences des subordonnés directs et les calendriers actuels.
Intelligence politique	Donne à l'agent Libre-service des fonctionnalités permettant de résoudre les questions relatives aux règles de unité légale en recherchant la documentation autorisée. L'aptitude récupère des données spécifiques dans les documents relatifs aux politiques et aux guides de procédure pour garantir que les réponses sont conformes et à jour.

Référence : conditions requises pour la sécurité des outils de l'agent Libre-service

Cette thème décrit les critères de sécurité pour les outils populaires dans chaque aptitude dans l'agent Libre-service.

Note:

Chaque domaine doit être répertorié, sauf s'il est séparé par le mot *ou* le , dans ce cas , vous n'en avez besoin qu'un seul.

ESS - Aide

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
create_case	- domaine <i>Self Service: Help Case Management</i> dans le domaine fonctionnel Help . - domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher		
create_case	domaine <i>Self Service: Help Case Management</i> dans le domaine fonctionnel Help .	Modifier		

ESS - Gestion du capital humain

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
change_home_contact	domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Modification des coordonnées personnelles	Modifier les coordonnées personnelles (service REST)
change_home_contact_info	- domaine <i>Self-Service: Home Address</i> dans le domaine fonctionnel Contact Information. - domaine <i>Self-Service: Home Email</i> dans le domaine fonctionnel Contact Information. <i>Self-Service: Home Phone</i> dans le domaine fonctionnel Contact Information.	Modifier	Modification des coordonnées personnelles	Modifier les coordonnées personnelles (service REST)
change_marital_status	- domaine <i>Self-Service: Marital Status</i> dans le domaine fonctionnel Personal Data. - domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Modification des données personnelles	Modifier les données personnelles (service REST)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
change_marital_status	domaine <i>Self-Service: Marital Status</i> dans le domaine fonctionnel Personal Data.	Modifier	Modification des données personnelles	Modifier les données personnelles (service REST)
change_legal_name	• domaine <i>Self-Service: Legal Name</i> dans le domaine fonctionnel Personal Data. • domaine <i>Self-Service: Current Staffing Information</i> ou <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Changement du nom légal	Modifier le nom légal (service REST)
change_preferred_name	• domaine <i>Self-Service: Preferred Name</i> dans le domaine fonctionnel Personal Data. • domaine <i>Self-Service: Current Staffing Information</i> ou <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Changement du nom d'usage	Modifier le nom d'usage (service REST)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
request_reference_letter	Demande d'attestation de l'employeur / attestation d'employeur pour vous-même • Domaine <i>Search: Find Worker</i> dans le domaine fonctionnel Worker Profile and Skills. • domaine <i>Self-Service: Current Staffing Information</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. Demander une attestation de l'employeur / attestation d'employeur pour une autre personne • domaine <i>Set Up: Reference Letter Security Segments</i> dans le domaine	Afficher	Demander une attestation d'employeur	Créer une attestation d'employeur pour un employé (API Graph)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Staffing. • domaine <i>Worker Data: Active Employees</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Business Title on Worker Profile</i> ou <i>Worker Data: Current Staffing Information</i> ou <i>Worker Data: Management Chain</i> dans le domaine fonctionnel Staffing.			
view_bonus_history	domaine <i>Self-Service: Compensation</i> dans le domaine fonctionnel Core Compensation.	Afficher		
view_coworker_info	• Domaine <i>Search: Find Worker</i> dans le domaine fonctionnel	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	Worker Profile and Skills. • domaine <i>Person</i> <i>Data: Home Email</i> ou <i>Self-Service: Home Email</i> dans le domaine fonctionnel Contact Information ou domaine <i>Worker</i> <i>Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Person</i> <i>Data: Work Email</i> ou <i>Self-Service: Work Email</i> dans le domaine fonctionnel Contact Information ou domaine <i>Worker</i> <i>Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Person</i> <i>Data: Home Phone</i> ou <i>Self-Service: Home Phone</i> dans le domaine			

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Contact Information ou <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Person Data: Home Address</i> ou <i>Self-Service: Home Address</i> dans le domaine fonctionnel Contact Information. • domaine <i>Self-Service: Current Staffing Information</i> ou <i>Worker Data: Business Title on Worker Profile</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Current Staffing Information</i> ou <i>Worker Data: Management Chain</i> dans le domaine fonctionnel Staffing.			

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
view_dependents	• domaine <i>Self-Service: Dependent Identifiable Data</i> dans le domaine fonctionnel Benefits. • domaine <i>Self-Service: Dependent Identifiable Data blocks Use</i> dans le domaine fonctionnel Benefits. • domaine <i>Self-Service: Dependents</i> dans le domaine fonctionnel Benefits.	Afficher		
view_healthcare_elections	• domaine <i>Self-Service: Benefits Elections</i> dans le domaine fonctionnel Benefits. • domaine <i>Self-Service: Retirement Savings</i> dans le domaine fonctionnel Benefits.	Afficher		
view_my_team	• <i>Domaine Reports: Manager</i> dans le domaine fonctionnel Staffing ou <i>Domaine Reports: Matrix</i>	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	<i>Manager</i> dans le domaine fonctionnel Staffing ou <i>Domaine Search: Find Worker</i> dans le domaine fonctionnel Worker Profile and Skills ou <i>Domaine Worker Data: Compensation for Managers</i> dans le domaine fonctionnel Core Compensation ou <i>Worker Data: Current Staffing Information</i> dans le domaine fonctionnel Staffing. • <i>domaine Self-Service: Current Staffing Information</i> ou <i>Worker Data: Business Title on Worker Profile</i> dans le domaine fonctionnel Staffing.			
view_org_info	domaine <i>Reports: Organization</i>	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	dans le domaine fonctionnel Organizations and Roles.			
view_personal_info	• domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Self-Service: Current Staffing Information</i> dans le domaine fonctionnel Staffing. • domaine <i>Self-Service: Service Dates</i> dans le domaine fonctionnel Staffing. • domaine <i>Self-Service: Date of Birth</i> dans le domaine fonctionnel Personal Data. • domaine <i>Self-Service: Home Email</i> dans le domaine fonctionnel Contact Information. • domaine <i>Self-Service: Work Email</i> dans le domaine	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Contact Information. • <i>Self-Service:</i> <i>Home Phone</i> dans le domaine domaine fonctionnel Contact Information. • <i>Self-Service:</i> <i>Work Phone</i> dans le domaine domaine fonctionnel Contact Information. • domaine <i>Worker</i> <i>Data:</i> <i>Succession</i> dans le domaine fonctionnel Talent Pipeline. • domaine <i>Worker</i> <i>Data:</i> <i>Succession</i> dans le domaine fonctionnel Talent Pipeline. • domaine <i>Worker</i> <i>Data:</i> <i>Current</i> <i>Staffing</i> <i>Information</i> ou <i>Worker</i> <i>Data:</i> <i>Management</i> <i>Chain</i> dans le domaine fonctionnel Staffing.			

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	• domaine <i>Worker Data: Annivers travail/ anniversaire de travail</i> ou <i>Worker Data: Current Staffing Information</i> dans le domaine fonctionnel <i>Staffing</i>.			
view_retirement_savings	• domaine <i>Self-Service: Benefits Elections</i> dans le domaine fonctionnel <i>Benefits</i>. • domaine <i>Self-Service: Retirement Savings</i> dans le domaine fonctionnel <i>Benefits</i>.	Afficher		
view_total_compensation	• domaine <i>Self-Service: Compensation</i> dans le domaine fonctionnel <i>Core Compensation</i>. • domaine <i>Self-Service: Compensation Salary Grade</i> dans le domaine fonctionnel <i>Core Compensation</i>.	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	• domaine <i>Self-Service: Compensation Basis</i> dans le domaine fonctionnel Core Compensation. • domaine <i>Self-Service: Compensation Management</i> dans le domaine fonctionnel Advanced Compensation. • domaine <i>Self-Service: Total Base Pay Range</i> dans le domaine fonctionnel Core Compensation.			

ESS - Paie

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
view_direct_deposit	• domaine <i>Self-Service: Payment Election</i> dans le domaine fonctionnel Expenses. • domaine <i>Self-Service: Payroll (My Payment Elections)</i> dans le domaine fonctionnel	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	Core Payroll. • domaine <i>Self-Service: interface de la paie (Payment Elections)</i> dans le domaine fonctionnel interface de la paie . • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.			
view_next_paydate	• domaine <i>Self-Service: Payment Election</i> dans le domaine fonctionnel Expenses. • domaine <i>Self-Service: Payroll (My Payment Elections)</i> dans le domaine fonctionnel Core Payroll. • domaine <i>Self-Service: interface de la paie (Payment Elections)</i> dans le domaine fonctionnel	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	interface de la paie . • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.			
view_next_paydate	• domaine <i>Self-Service: Payroll (My Payslips)</i> dans le domaine fonctionnel Core Payroll. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher		
view_payslips	domaine <i>Self-Service: Payroll (My Payslips)</i> dans le domaine fonctionnel Core Payroll.	Afficher		
view_w2	• domaine <i>Self-Service: Payroll (My Tax Documents) - USA</i> dans le domaine fonctionnel USA Payroll. • domaine <i>Worker Data: Public Worker</i>	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	<i>Reports</i> dans le domaine fonctionnel Staffing.			
view_w4	• domaine <i>Self-Service: Payroll (My Withholding Elections)</i> - USA dans le domaine fonctionnel USA Payroll. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher		

ESS - Gestion des talents

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
create_referral	• domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Internal Careers</i> ou <i>Recruiting Agency Careers</i> dans le domaine	Afficher	Recommander un candidat	Recommander un candidat (Graph API)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Recruiting.			
find_job_requisition	• domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Organizations</i> dans le domaine fonctionnel Staffing. • domaine <i>Job Requisition Data</i> dans le domaine fonctionnel Pre-Hire Process. • <i>Job Requisitions for Recruiting</i> dans le domaine domaine fonctionnel Recruiting.	Afficher		
find_jobs	domaine <i>Internal Careers</i> dans le domaine fonctionnel Recruiting.	Afficher		
start_my_performance	domaine <i>Self-Service: Performance Reviews</i> dans le domaine fonctionnel Performance Enablement.	Afficher	Démarrer l'évaluation de la performance	Démarrer l'évaluation de la performance (service REST)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
view_feedback	Afficher du feedback sur vous-même • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • Domaine <i>Search: Find Worker</i> dans le domaine fonctionnel Worker Profile and Skills. • Domaine <i>Worker Data: Current Staffing Information</i> dans le domaine fonctionnel Staffing. • domaine <i>Self-Service: Anytime Feedback</i> dans le domaine fonctionnel Performance Enablement. • domaine <i>Self-Service: Current Staffing Information</i> dans le domaine fonctionnel Staffing.	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	• domaine <i>Self-Service: Role Requested Feedback</i> ou <i>Self-Service: Self Requested Feedback</i> dans le domaine fonctionnel <i>Performance Enablement</i>. Afficher le feedback concernant une autre personne • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel <i>Staffing</i>. • domaine <i>Worker Data: Anytime Feedback</i> dans le domaine fonctionnel <i>Performance Enablement</i>. • domaine <i>Search: Find Worker</i> dans le domaine fonctionnel <i>Worker Profile and Skills</i> ou domaine <i>Worker Data: Active Employees</i>			

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	dans le domaine fonctionnel Staffing . • domaine Reports: Manager ou Reports: Matrix Manager ou Worker Data: Current Staffing Information dans le domaine fonctionnel Staffing. • domaine Worker Data: Role Requested Feedback ou Worker Data: Self Requested Feedback dans le domaine fonctionnel Performance Enablement. • domaine Worker Data: Business Title on Worker Profile ou Worker Data: Current Staffing Information ou Worker Data: Management Chain dans le domaine			

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Staffing.			
view_org_goals	• domaine <i>Reports: Organization</i> dans le domaine fonctionnel <i>Organizations and Roles</i>. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Organization Goals</i> ou <i>Self-Service: Organization Goals</i> dans le domaine fonctionnel <i>Performance Enablement</i>.	Afficher		
view_performance_reviews	domaine <i>Worker Data: Employee Reviews</i> ou <i>Self-Service: Employee Reviews</i> dans le domaine fonctionnel <i>Performance Enablement</i> .	Afficher		
create_goal_self	domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Gérer les objectifs	Gérer les objectifs (service REST)
create_goal_self	<i>Self-Service: Employee Goals</i> ou <i>Worker Data:</i>	Modifier	Gérer les objectifs	Gérer les objectifs (service REST)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	<i>Employee Goals</i> dans le domaine fonctionnel Performance Enablement.			
view_talent_profile_detail	Afficher vos propres données de talents • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Self-Service: Education</i> dans le domaine fonctionnel Worker Profile and Skills. • domaine <i>Self-Service: Skills</i> dans le domaine fonctionnel Worker Profile and Skills. • domaine <i>Self-Service: Job History</i> dans le domaine fonctionnel Worker Profile and Skills. Afficher les données des talents des collègues • domaine <i>Worker</i>			

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	<i>Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Self-Service: Education</i> dans le domaine fonctionnel Worker Profile and Skills. • domaine <i>Self-Service: Skills</i> dans le domaine fonctionnel Worker Profile and Skills. • domaine <i>Self-Service: Job History</i> dans le domaine fonctionnel Worker Profile and Skills.			

ESS - Gestion du personnel

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
delete_time_off	domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Corriger les absences	Corriger une saisie d'absence (service REST)
edit_time_off	domaine <i>Worker Data: Public Worker Reports</i>	Afficher	Corriger les absences	Corriger une saisie d'absence (service REST)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	dans le domaine fonctionnel Staffing.			
enter_time_block	• domaine <i>Process: Time Block REST</i> dans le domaine fonctionnel Time Tracking. • domaine <i>Process: Time Clock Event REST APIs</i> dans le domaine fonctionnel Time Tracking. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher		
enter_time_block	domaine <i>Process: Time Block REST</i> dans le domaine fonctionnel Time Tracking.	Modifier		
my_time_off_events	• domaine <i>Self-Service: Time Off</i> dans le domaine fonctionnel Time Off and Leave. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Staffing.			
request_time_off	domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Demander une absence	Demander une saisie d'absence (service REST)
shift_check_in	• domaine <i>Process: Time Clock Event REST APIs</i> dans le domaine fonctionnel Time Tracking. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher		
shift_check_in	domaine <i>Process: Time Clock Event REST APIs</i> dans le domaine fonctionnel Time Tracking.	Modifier		
shift_check_out	• domaine <i>Process: Time Clock Event REST APIs</i> dans le domaine fonctionnel Time Tracking. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Staffing.			
shift_check_out	domaine <i>Process: Time Clock Event REST APIs</i> dans le domaine fonctionnel Time Tracking.	Modifier		
submit_time	• domaine <i>Process: Time Block REST</i> dans le domaine fonctionnel Time Tracking. • domaine <i>Process: Time Tracking Configuration Objects REST APIs</i> dans le domaine fonctionnel Time Tracking. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Saisir les temps	Soumission des temps (service REST)
time_off_balance	• domaine <i>Self-Service: Time Off Balances</i> dans le domaine fonctionnel Time Tracking. • domaine <i>Worker Data: Public</i>	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	<i>Worker Reports</i> dans le domaine fonctionnel Staffing.			
time_off_types	- Action autorisée <i>Demander une absence pour soi-même</i> pour lancer le processus de gestion <i>Demander une absence</i> . - domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher	Demander une absence	Demander une absence (service REST)
update_time_block_column	domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing.	Afficher		
update_time_block_column	domaine <i>Process: Time Block REST</i> dans le domaine fonctionnel Time Tracking.	Modifier		
view_holiday_calendar	- domaine <i>Self-Service: Leave of Absence</i> dans le domaine fonctionnel Time Off and Leave. - domaine <i>Self-Service:</i>	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	<i>Time Off</i> dans le domaine fonctionnel <i>Time Off and Leave</i> . • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel <i>Staffing</i>.			
view_time_blocks	• domaine <i>Process: Time Block REST</i> dans le domaine fonctionnel <i>Time Tracking</i>. • domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel <i>Staffing</i>.	Afficher		
view_time_entry_codes	• domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel <i>Staffing</i>. • domaine <i>Process: Time Block REST APIs</i> ou <i>Process: Time Clock Event REST APIs</i> dans le domaine	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Time Tracking.			
view_time_entry_projects	• domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Process: Time Block REST APIs</i> ou <i>Process: Time Clock Event REST APIs</i> dans le domaine fonctionnel Time Tracking.	Afficher		

MSS - Gestion du capital humain

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
recommend_change_job_templates	• domaine <i>Jobs and Positions: Change Job Templates GraphAPI Results</i> dans le domaine fonctionnel Jobs and Positions.	Afficher	Changer d'emploi	Changer d'emploi (GraphQL)
view_direct_reports	• domaine <i>Reports: Manager ou Reports: Matrix Manager ou Worker Data: Current Staffing Information</i> dans le domaine fonctionnel Staffing.	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
view_direct_reports	info • domaine <i>Reports: Manager</i> ou <i>Reports: Matrix Manager</i> ou <i>Worker Data: Current Staffing Information</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Succession</i> dans le domaine fonctionnel Talent Pipeline. • domaine <i>Worker Data: Birthdays Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Time in Position</i> dans le domaine fonctionnel Staffing. • domaine <i>Public Profile Preferences: processus anniversaire</i> dans le domaine	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	fonctionnel Staffing.			
view_team_learning_status	domaine Worker Data: Public Worker Reports dans le domaine fonctionnel Staffing. • Reports: Learning Record ou Person Data: Learning dans le domaine fonctionnel Learning Core.	Afficher		
view_worker_history	• domaine Worker Data: Public Worker Reports dans le domaine fonctionnel Staffing. • domaine Worker Data: Active Employees dans le domaine fonctionnel Staffing ou Domaine Search: Find Worker dans le domaine fonctionnel Worker Profile and Skills. • Worker Data:	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	Historical Staffing Information dans le domaine fonctionnel Staffing.			

MSS - Gestion des talents

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
start_performance_review_tool	Domaine Worker Data: Public Worker Reports dans le domaine fonctionnel Staffing. Reports: Manager dans le domaine domaine fonctionnel Staffing ou Reports: Matrix Manager dans le domaine fonctionnel Staffing ou Domaine Worker Data: Market Position Details dans le domaine domaine fonctionnel Core Compensation ou domaine Worker	Afficher	Démarrer l'évaluation de la performance	startPerformanceReview (Graph API v1)

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	<i>Data:</i> <i>Current Staffing</i> <i>Information</i> dans le domaine fonctionnel Staffing.			
view_candidate_status	• <i>Candidates for My Jobs</i> dans le domaine fonctionnel Recruiting. • domaine <i>Internal Careers</i> dans le domaine fonctionnel Recruiting. • domaine <i>Candidate Data: Personal Information</i> dans le domaine fonctionnel Recruiting ou <i>Candidate Data: Job Application</i> dans le domaine fonctionnel Recruiting ou <i>Candidate Data: Global Search</i> dans le domaine fonctionnel Recruiting ou <i>Prospects</i> dans le domaine fonctionnel	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	Talent Pipeline.			
view_team_goals	• domaine <i>Worker Data: Public Worker Reports</i> dans le domaine fonctionnel Staffing. • domaine <i>Worker Data: Employee Goals</i> dans le domaine fonctionnel Performance Enablement. • domaine <i>Reporting: Performance and Goals</i> dans le domaine fonctionnel Performance Enablement. • domaine <i>Worker Data: Organization Goals</i> dans le domaine fonctionnel Performance Enablement. • <i>Rechercher un employé ou Reports: Manager ou Reports: Matrix Manager ou Worker Data: Current Staffing Information</i>	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	dans le domaine domaine fonctionnel Staffing.			
view_team_performance	• domaine Worker Data: Public Worker Reports dans le domaine fonctionnel Staffing. • domaine Worker Data: Employee Reviews dans le domaine fonctionnel Performance Enablement.	Afficher		

MSS - Gestion du personnel

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
view_direct_reports	• Domaine Reports: Manager dans le domaine fonctionnel Staffing ou Domaine Reports: Matrix Manager dans le domaine fonctionnel Staffing ou domaine Self-Service: My Team	Afficher		

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
	dans le domaine fonctionnel Staffing ou <i>domaine Worker Data: Time Off (Time Off Manager View)</i> dans le domaine Time Off dans le domaine fonctionnel Time Off and Leave ou <i>Worker Data: Time Off (Time Off Manager View)</i> dans le domaine fonctionnel Time Off and Leave.			

MSS - Paie

Outil	Domaines obligatoires	Autorisations requises	Processus de gestion obligatoire	Action de lancement de processus de gestion requise
request_payroll_input	• <i>Domaine Reports: Manager</i> dans le domaine fonctionnel Staffing. • <i>domaine Manager Pay Component Visibility</i> dans le domaine fonctionnel Core Payroll.	Afficher	Demander des saisies d'élément de paie	Demander des saisies d'élément de paie (service REST)

Sana pour Workday

Concept : espace de travail Sana

Note: Des étapes supplémentaires peuvent être nécessaires pour activer cette fonctionnalité en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services (MSA), soit sur le Contrat-cadre de services universel (UMSA). Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().
4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- *USA* , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- *MSA* , votre organisation doit activer le système UMSA.

Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser des agents en production tant que vous n'aurez pas accepté ces contrats. Le système UMSA est obligatoire pour les environnements clients autres que de production et de production pour les agents Workday-Built. L'UMSA n'est pas obligatoire pour les environnements clients autres que de production pour les agents auto-configurés.

Pour utiliser cette fonctionnalité, vous devez :

- Signez l'accord principal universel d'abonnement (UMSA).
- Signez la [politique de crédits variables et de droits à la plateforme de Workday](#) .
- Achat du SKU Sana Enterprise Cela s'applique uniquement à Sana Enterprise.

Sana Core et Sana Enterprise offrent une expérience native d'IA pour les RH et la Finance sur Sana et Workday. Ils vous permettent d'interagir avec Workday de manière conversationnelle.

Caractéristiques	Sana Core	Sana Enterprise
Accès à l'espace de travail Sana, y compris le télécharger de fichiers (recherche et analyse) et le chat LLM (Web uniquement).	Oui	Oui
Lire et écrire des actions dans Workday via l'agent Libre-service Workday (WSAA).	Oui	Oui
Chat agentique avec l'historique de l'utilisateur et les citations.	Oui	Oui
Des workflows automatisés qui orchestrent les processus HCM et financiers à plusieurs étapes.	Oui	Oui

Caractéristiques	Sana Core	Sana Enterprise
Authentification unique partagée avec votre environnement client Workday .	Oui	Oui
Le rôle et autorisation sont reflétés pour que l'accès et les actions respectent la configuration de sécurité de Workday .	Oui	Oui
Les administrateurs peuvent activer et gérer les connecteurs tiers pris en charge utilisés par Sana Enterprise.	Non	Oui
Les utilisateurs disposant des autorisations appropriées peuvent demander et effectuer des actions dans les systèmes connectés directement depuis la discussion Sana Enterprise.	Non	Oui
Invite les utilisateurs à réviser et à confirmer les actions qui nécessitent une approbation manuelle avant de poursuivre. Toutes les actions entre les systèmes sont consignées et disponibles pour audit.	Non	Oui

Espace de travail Sana

Vous pouvez accéder à l'espace de travail Sana depuis votre environnement client Workday lorsque vous :

- Cliquez sur la vignette **Sana** sur la page **d'accueil Workday** .
- Cliquez sur le bouton **Explorer Sana** sur la page des résultats de recherche Workday .
- Cliquez sur **Sana** dans la barre de navigation globale.

Note: Pour activer la vignette **Sana** sur la page **d'accueil** et le bouton **Explorer Sana** dans les résultats de la recherche, vous devez activer la vignette **Sana** dans la section **Outils de travail** de l' **espace de travail Vignettes d'accueil** .

Étapes : définir Sana pour Workday

Prerequisites

Note: Des étapes supplémentaires peuvent être nécessaires pour activer cette fonctionnalité en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services (MSA), soit sur le Contrat-cadre de services universel (UMSA). Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().

4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- *UMSA* , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- *MSA* , votre organisation doit activer le système UMSA.

Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser des agents en production tant que vous n'aurez pas accepté ces contrats. Le système UMSA est obligatoire pour les environnements clients autres que de production et de production pour les agents Workday-Built. L'UMSA n'est pas obligatoire pour les environnements clients autres que de production pour les agents auto-configurés.

Pour utiliser cette fonctionnalité, vous devez :

- Signez l'accord principal universel d'abonnement (UMSA).
- Signez la [politique de crédits variables et de droits à la plateforme de Workday](#) .
- Achat du SKU Sana Enterprise Cela s'applique uniquement à Sana Enterprise.

Sécurité : domaines suivants dans le domaine fonctionnel System :

- *Attribution de comptes aux utilisateurs de l'agent Sana*
- *Sana Enterprise*
- *Security Activation*
- *Security Configuration*

Context

Pour vérifier que la configuration de la sécurité de Sana et des agents IA associés est terminée, Workday envoie des notifications aux administrateurs. Nous notifions :

- Aux administrateurs de la sécurité Workday d'effectuer la tâche **Définir les autorisations de sécurité de l'administrateur de l'IA** .
- Les administrateurs système d'enregistrement pour configurer et activer l' **agent Libre-service** .
- Aux administrateurs Sana de configurer ou de modifier éventuellement les paramètres par défaut dans l' **espace de travail Sana** .
- Aux administrateurs allocation de ressources aux utilisateurs pour attribuer des salariés à **Sana** .

Steps

1. [Définissez les autorisations de sécurité de l'administrateur IA](#) .
2. [Définissez l'agent Système d'enregistrement](#) .
3. [Modifiez les règles de sécurité des domaines](#) .

Configurez le domaine *Sana Enterprise* dans le domaine fonctionnel System.

Note: Cette étape est obligatoire si votre organisation a acheté Sana Enterprise SKU. Cette domaine détermine qui peut utiliser des connexions intersystèmes et des fonctionnalités configuration Enterprise.

4. (Facultatif) Accédez à la tâche **Définir des groupes de sécurité pour l'attribution d'utilisateurs** . Si vous souhaitez que certains groupes de sécurité soient disponibles pour allocation de ressources Sana, ajoutez des lignes dans la grille et sélectionnez les groupes à activer dans l' invite **Groupes de sécurité** .

Sécurité : domaine *Set Up: User Provisioning* dans les domaines fonctionnels System et User Provisioning.

5. Attribuer des utilisateurs à l'espace de travail Sana.

Nous informons les administrateurs allocation de ressources aux utilisateurs d'attribuer des comptes aux utilisateurs à l'espace de travail Sana.

- a. Dans Workday, ouvrez la notification **Action requise : attribuer des comptes utilisateurs pour accéder à l'espace de travail Sana** à partir de l'icône en forme de bulles.
- b. Cliquez sur le bouton **Associer** dans la notification pour ouvrir l' **espace de travail d'attribution de comptes aux utilisateurs** .
- c. Sur la page **Produits** , cliquez sur **Configurer** dans la vignette **Sana** .
- d. Dans la section **Attribution de comptes aux utilisateurs** , cliquez sur **Modifier le groupe d'attribution de comptes** .
- e. Dans l'invite **Utiliser les groupes de sécurité Workday** , sélectionnez l'une des options suivantes :
 - *All* pour attribuer tous les utilisateurs de Sana.
 - Groupes de sécurité individuels à attribuer. Vous pouvez uniquement sélectionner des groupes de sécurité individuels si vous les avez définis pour allocation de ressources aux utilisateurs dans la tâche **Définir des groupes de sécurité pour l'attribution d'utilisateurs** .
- f. Cliquez sur **Mettre à jour un groupe d'attribution de comptes** .
- g. Cliquez sur **Aperçu et activez la synchronisation** .
- h. Réviser les utilisateurs qui seront provisionnés, cochez la case à cocher **Confirmer** et cliquez sur **Activer la synchronisation** .

Une fois la synchronisation activée, les utilisateurs des groupes de sécurité sélectionnés sont automatiquement provisionnés et peuvent se connecter à l'espace de travail Sana.

6. Autorisez l'accès à l'espace de travail Sana depuis Workday.

Pour faciliter la recherche et l'accès des utilisateurs à l'espace de travail Sana depuis votre environnement client Workday , activez la vignette **Sana** sur la page d'accueil :

- a. Dans l'espace de travail des vignettes d'accueil, cliquez sur **Accueil** .
- b. Cliquez sur **Vignettes** .
- c. Cliquez sur **Modifier les outils de travail** .
- d. Dans la fenêtre contextuelle **Modifier les outils de travail** , ajoutez une ligne à la grille.
- e. Dans le champ **Nom** , saisissez *Sana* .
- f. Cliquez sur **OK**.

7. (Facultatif) Configurez l'espace de travail Sana.

- a. Depuis l'espace de travail Sana, cliquez sur la flèche en regard du nom de l'espace de travail dans le menu de navigation.
- b. Cliquez sur **Paramètres de l'espace de travail** .
- c. (Facultatif) Configurez les paramètres facultatifs. Vous pouvez :
 - Désactiver la recherche sur le web.
 - Désactiver le chat pris en charge par intercompagnies.
 - Désactiver certains connecteurs tiers. (Sana Enterprise uniquement.)
 - Limiter les actions d'agent aux domaines d'e-mail approuvés. (Sana Enterprise uniquement.)

Result

Les utilisateurs peuvent accéder immédiatement à Sana depuis Workday et utiliser les fonctionnalités de Sana.

Définir les autorisations de sécurité de l'administrateur de l'IA

Prerequisites

Note: Des étapes supplémentaires peuvent être nécessaires pour activer cette fonctionnalité en fonction du contrat service' abonnement de votre organisation. Votre organisation figure soit sur le Contrat-cadre de services (MSA), soit sur le Contrat-cadre de services universel (UMSA). Pour déterminer le contrat de service d'abonnement de votre organisation :

1. Sélectionnez l'avatar de votre profil dans [Workday Community](#) .
2. Sélectionnez **Profil** .
3. Sur la page de votre profil, sélectionnez le nom de votre organisation, qui est sous votre nom et à côté de la désignation de l'emploi ().
4. Affichez la valeur de votre **accord d'abonnement** .

Si sa valeur est égale à :

- *UMSA* , la fonctionnalité est automatiquement disponible. Pour plus d'informations sur les contributions de données de Machine Learning, voir [Concept : Workday AI for Universal Subscription Agreement Customers](#) .
- *MSA* , votre organisation doit activer le système UMSA.

Des crédits variables sont obligatoire uniquement pour enregistrement et utiliser des agents dans vos environnements clients de production. Vous ne pourrez pas enregistrer et utiliser des agents en production tant que vous n'aurez pas accepté ces contrats. Le système UMSA est obligatoire pour les environnements clients autres que de production et de production pour les agents Workday-Built. L'UMSA n'est pas obligatoire pour les environnements clients autres que de production pour les agents auto-configurés.

Pour utiliser Sana Core et Sana Enterprise, vous devez :

- Achat du SKU Sana Enterprise Cela s'applique uniquement à Sana Enterprise.
- Signez l'accord principal universel d'abonnement (UMSA).
- Signez la [politique de crédits variables et de droits à la plateforme de Workday](#) .

Sécurité : vous disposez des autorisation' accès aux domaines suivants dans le domaine fonctionnel System :

- *Security Activation*
- *Security Configuration*

Context

La tâche **Définir les autorisations de sécurité de l'administrateur de l'IA** regroupe toutes les étapes nécessaires à la configuration de la sécurité dans une seule tâche qui, une fois terminée, lance un traitement back-end pour permettre à votre organisation d'utiliser les fonctionnalités d'IA de Workday .

Il s'agit d'une tâche ponctuelle pour chaque environnement client. La tâche simplifie l'octroi des droits d'accès pour :

- Agent Système d'enregistrement : accordez aux utilisateurs l'accès pour gérer et configurer le comportement et les intégrations de l'agent IA depuis un site centralisé.
- Espace de travail d'attribution de comptes aux utilisateurs pour Sana : affectez des administrateurs pour attribuer des utilisateurs à Sana.
- Console de consommation de la plateforme : accordez aux utilisateurs l'accès pour surveiller et gérer les ressources d'infrastructure utilisées par vos agents.
- Sana : affectez des utilisateurs en tant qu'administrateurs Sana pour configurer les fonctions Sana dans l'espace de travail Sana.

Workday envoie une notification aux administrateurs de la sécurité dans tous vos environnements clients (Production, Sandbox, Sandbox Preview, Implementation et Implementation Preview) pour accéder et finaliser la tâche **Définir les autorisations de sécurité pour les administrateurs de l'IA**.

Bien que vous puissiez configurer certains domaines de la tâche **Définir les autorisations de sécurité de l'administrateur de l'IA**, Workday vous recommande d'utiliser cette tâche pour garantir que toutes les dépendances critiques de votre expérience d'IA sont satisfaites.

Les administrateurs de la sécurité doivent renseigner toutes les sections. Une fois que vous avez soumis la tâche, vous ne pouvez plus la modifier. Vous pouvez mettre à jour manuellement la configuration via les paramètres de sécurité standard de Workday.

Note: Si plusieurs administrateurs configurent cette tâche, Workday traite la première configuration qui a été soumise.

Steps

1. Accédez à la notification **Action requise : réviser et configurer la sécurité des agents Sana et Workday** à partir de l'icône en forme de bulles dans Workday.
2. Dans la notification, cliquez sur **Démarrer la configuration**.
3. Pour la section **Configure Security Policies** dans l'onglet **Configuration**, tenez compte des éléments suivants :

Vous devez uniquement configurer les grilles dont le statut **est Incomplet**. Nous affichons une :

- Statut **Terminé** lorsque les règles de sécurité des domaine sont configurées. Les colonnes **Groupe de sécurité** et **Afficher ou ajouter des utilisateurs à un groupe de sécurité** sont masquer dans la grille.
- **Terminé avec le statut Exceptions** lorsqu'au moins une des règles de sécurité des domaine figurant dans la colonne **Règles de sécurité des domaines** n'est pas active actuellement ou fait l'objet de modifications en attente.

Dans la colonne **View or Add Users to Security Group** :

- Vous pouvez ajouter des membres uniquement lorsque vous créez un nouveau groupe de sécurité ou que vous sélectionnez un groupe qui n'est pas utilisé dans d'autres règles et qui ne contient pas de membres.
- Vous ne pouvez pas ajouter ni supprimer de membres dans la colonne lorsque vous sélectionnez un groupe de sécurité qui est actuellement utilisé dans d'autres règles ou qu'il a des membres.

Dans la colonne **Détail**, vous pouvez explorer chaque configuration de règle de sécurité de domaine en cliquant sur **Détail**. Lorsque vous cliquez sur le associer, une fenêtre contextuelle **Afficher le détail du domaine** s'affiche dans laquelle vous pouvez afficher la configuration.

Option	Description
Agent Système d'enregistrement	Cette section vous permet de configurer l'accès à l'espace de travail Agent Système d'enregistrement. La colonne Règles de sécurité des domaines affiche toutes les règles de sécurité des domaine que vous devez configurer. Dans la colonne Groupe de sécurité, sélectionnez un groupe de sécurité par utilisateur existant ou créez-en un nouveau. Nous affichons les membres dans la colonne View or Add Users to Security Group. Workday ajoute les utilisateurs de ces

Option	Description
	groupes aux règles de sécurité des domaine répertoriées dans la colonne Règles de sécurité des domaines avec les autorisations Afficher et Modifier .
Console de consommation de la plateforme	Cette section vous permet de configurer l'accès à la console de consommation de la plateforme. La colonne Règles de sécurité des domaines affiche toutes les règles de sécurité des domaine que vous devez configurer. Dans la colonne Groupe de sécurité , sélectionnez un groupe de sécurité par utilisateur existant ou créez-en un nouveau. Nous avons uniquement besoin d'un groupe de sécurité disposant de autorisation Afficher uniquement dans la règle de sécurité du domaine <i>Management Dashboard: Platform Consumption Console</i> . Vous ne pouvez ajouter un groupe de sécurité au domaine <i>Management Dashboard: Platform Consumption Console</i> à l'aide de cette tâche s'il n'existe aucun groupe de sécurité disposant des autorisations Afficher uniquement ou Afficher et modifier configurées dans la règle de sécurité du domaine . Note: Workday affiche le statut Terminé dans la grille Console de consommation de la plateforme lorsque ces critères de configuration de la sécurité sont remplis. Nous affichons les membres dans la colonne View or Add Users to Security Group . Workday ajoute les utilisateurs de ces groupes aux règles de sécurité des domaine répertoriées dans la colonne Règles de sécurité des domaines avec l' autorisation Affichage seul .
Espace de travail d'attribution de comptes aux utilisateurs	Cette section vous permet de configurer l'accès à l'espace de travail Attribution de comptes aux utilisateurs pour Sana. La colonne Règles de sécurité des domaines affiche toutes les règles de sécurité des domaine que vous devez configurer. Dans la colonne Groupe de sécurité , sélectionnez un groupe de sécurité par utilisateur existant ou créez-en un nouveau. Nous affichons les membres dans la colonne View or Add Users to Security Group . Workday ajoute les utilisateurs de ces groupes aux règles de sécurité des domaine

Option	Description
	répertoriées dans la colonne Règles de sécurité des domaines avec les autorisations Afficher et Modifier .

Lorsqu'un domaine est désactivé et que vous accédez à la tâche **Set Up AI Admin Security Permissions** :

- Vous pouvez ajouter des groupes de sécurité au domaine. Une fois que vous avez soumis les modifications dans la tâche, le domaine est activé.
 - Le statut **Terminé** s'affiche si le domaine a des groupes de sécurité existants.
4. Pour la section **Définir les administrateurs Sana** de l'onglet **Configuration** , tenez compte des éléments suivants :

Option	Description
Définir les administrateurs Sana	Cette section vous permet de définir les utilisateurs qui sont administrateurs Sana. Workday attribue automatiquement ces utilisateurs au système Sana lors de l'activation. Dans la colonne Groupe de sécurité , sélectionnez un groupe de sécurité par utilisateur existant ou créez-en un nouveau. Les utilisateurs disposant des droits d'administration Sana peuvent accéder à l'espace de travail Sana et le configurer.

5. Accédez à l'onglet **Activate Pending Security Policy Changes** .

Pour activer les modifications de règle de sécurité dans votre environnement client, vous devez disposer des autorisation sur le domaine *Security Activation* .

6. Pour l'onglet **Activate Pending Security Policy Changes** , tenez compte des éléments suivants :

Option	Description
Grilles de règle de sécurité	Réviser les modifications de sécurité dans les grilles.
Confirmer la case à cocher	Cochez la case à cocher pour soumettre toutes les modifications de règle de sécurité . Workday active toutes les modifications de règle de sécurité dans les grilles, y compris les paramètres de sécurité de l'onglet Configuration .

7. Cliquez sur **OK**, puis sur **Terminé**.

Result

Workday active automatiquement les modifications de règle de sécurité en attente et rend les tâches applicables disponibles. Workday peut informer les membres des groupes de sécurité inclus des tâches et actions supplémentaires qu'ils peuvent effectuer.

Si l'accès de l'administrateur Sana échoue aux membres des groupes de sécurité, un bouton **Soumettre à nouveau** s'affiche dans la section **Définir l'administration Sana** de l'onglet **Configuration** . Vous pouvez relancer l' allocation de ressources en cliquant sur le bouton. Workday tente d'affecter aux utilisateurs des droits d'administration Sana.

Next Steps

(Facultatif) Si vous devez mettre à jour la configuration de la tâche, accédez aux paramètres de sécurité standard de Workday pour effectuer manuellement les modifications.

Console de consommation de la plateforme

Définir la sécurité pour la console de consommation de la plateforme

Context

Note: Les solutions décrites dans cette section ne font pas partie des services Workday. Pour plus d'informations, voir [les Mentions légales](#).

Pour les abonnements à l'UMSA (UMSA), aux crédits variables Workday et à la politique de droits à la plateforme, vous pouvez utiliser le tableau de bord **Console de consommation de la plateforme** pour visualiser la consommation des crédits variables par votre unité légale en fonction de votre utilisation des offres Workday.

Steps

1. Accédez au domaine *Management Dashboard: Platform Consumption Console* dans le domaine fonctionnel System.
2. Dans le menu des actions associées du domaine, sélectionnez **Create Security Policy**.
3. Cochez la case **Confirmer**, puis cliquez sur **OK**.
4. Dans la grille **Autorisations de rapport/tâche**, ajoutez des groupes de sécurité pertinents pour votre organisation.
5. Cochez la case à cocher **Afficher** et cliquez sur **OK**.
6. [Activez les modifications des règles de sécurité en attente](#).

Result

Les groupes de sécurité sélectionnés peuvent désormais accéder au tableau de bord **Console de consommation de la plateforme**.

Concept : console de consommation de la plateforme

Vous pouvez utiliser le tableau de bord **Console de consommation de la plateforme** pour visualiser la consommation des crédits variables dans votre unité légale en fonction de votre utilisation des offres Workday incluses dans la vignette de taux des crédits variables Workday. Le tableau de bord **Console de consommation de la plateforme** vous permet de surveiller votre consommation et votre solde de Crédits variables.

Note: Les agents Workday AI nécessitent l'utilisation de crédits variables Workday. Pour plus d'informations, voir cet [article de Community](#).

Les crédits variables et le tableau de bord **Console de consommation de la plateforme** sont uniquement disponibles pour les abonnés au contrat de souscription principal universel (UMSA) et aux abonnements à la politique de droits à la plateforme et aux crédits variables Workday. Si vous êtes abonné à l'UMSA, mais que vous n'avez pas avec signe la politique de crédits variables et de droits à la plateforme de Workday, vous pouvez configurer la sécurité pour le tableau de bord **Console de consommation de la plateforme**, mais vous ne verrez pas les données de consommation tant que la politique n'a pas été avec signe.

Solde de crédit et droits aux absences

La page **Solde de crédit** affiche votre activité quotidienne de crédits variables. La page **Droits au crédit** affiche l'historique d'achat de votre package de crédits variables.

Statut	Définition
Actif	Crédits disponibles à la consommation.
Expiré	Des crédits qui ont expiré.
Inactif	Crédits achetés pouvant être consommés à une date ultérieure.

Tous les crédits variables sont facturables et peuvent être appliqués de manière générique à l'ensemble des offres Workday dans la vignette de taux à laquelle vous avez droit d'accéder.

Vignette de taux

La page **Vignette de taux** est la ressource définitive qui définit la valeur monétaire de vos droits en termes de consommation de crédit.

Colonne	Définition
En blocs de (unités)	Nombre d'unités incluses dans un bloc facturable.
Taux de crédit par bloc	Le taux facturé pour ce bloc d'unités.

Comprendre et suivre la consommation

Workday met quotidiennement à jour votre utilisation de consommation pour refléter l'utilisation du jour précédent. La consommation est fondée sur les fonctionnalités spécifiques définies dans la page **Vignette de taux** et la version de politique associée à votre contrat. Workday détermine votre consommation à l'aide de plusieurs composants.

Composant	Définition
Agents	Utilisation des aptitudes et des activités de l'agent.
Demandes API	Nombre de demandes API .
Stockage de documents	Gigaoctets (Go) de données stockées.
Événements d'intégrations	Nombre d'événements intégration traités.

Votre politique fournit une indemnités' utilisation de référence ou des droits intégrés. Une fois ces droits intégrés utilisés, Workday impute votre consommation à vos droits de crédit disponibles, en donnant la priorité aux crédits qui expirent en premier.

Vous pouvez suivre votre utilisation par rapport à ce seuil dans la visualisation de l'aperçu des droits intégrés sur la page **Aperçu** . Pour des métriques plus détaillées, vous pouvez utiliser la page **Utilisation de la consommation** pour explorer (en détail) et voir une détail de la consommation par service.

Workday effectue le suivi de la consommation à partir du 13/02/2026 pour les clients actuels avec Crédits variables et à partir de la date d'effet du contrat pour les nouveaux clients.

Note: Si votre organisation a avec signe une version de la politique des crédits variables et des droits à la plateforme de Workday qui n'inclut pas de composants ou de droits à la plateforme, ces droits ou cette utilisation ne s'affichent pas dans le tableau de bord **Console de consommation de la plateforme** .

Notifications de droits aux crédits

Workday vous envoie une notification lorsque vous utilisez vos droits aux crédits actifs. Lorsque l'utilisation de vos droits aux crédits atteint 80 %, 90 % et 100 %, les utilisateurs ayant accès au domaine *Management Dashboard: Platform Consommation Console* reçoivent des notifications et voient une bannière dans le tableau de bord **Console de consommation de la plateforme**. Pour configurer vos paramètres de remise des notification, voir [Concept : notifications](#).

Le tableau de bord **Console de consommation de la plateforme** ne désactive pas les offres Workday si vous dépassez vos droits de crédit. Pour désactiver un agent, voir [Register and Configure Workday-Built Agents](#).

Environnements hors production

Le tableau de bord **Console de consommation de la plateforme** est activé dans vos environnements clients de production et hors production. La consommation dans les environnements clients autres que de production n'affecte pas votre solde de crédits variables Workday. Alors que les environnements clients hors production suivent votre consommation et affichent un solde de crédits variables Workday à titre d'information, Workday applique uniquement la consommation de l'environnement client de production au solde des crédits variables de votre organisation.

Le tableau de bord **Console de consommation de la plateforme** reçoit des données agrégées quotidiennes pour tous vos environnements clients hors production. Exemple : lorsque vous utilisez le tableau de bord **Console de consommation de la plateforme** dans votre environnement client Sandbox, le tableau de bord affiche l'activité combinée de tous vos environnements hors production.

Related Information

Exemples

[Workday Community: Workday Flex Credits](#)

Contributions de données d'IA

Étapes : définir les notifications pour les contributions de données de la fonctionnalité d'IA

Contexte

Les clients de l'accord d'abonnement principal universel (UMSA) peuvent configurer le domaine *AI Features and Third Party Notification* pour recevoir ces notifications.

Type de notification	Synchronisation de la livraison	Objet
Disponibilité de la fonctionnalité d'IA	Le jour de la mise en production de la fonctionnalité.	Confirme que la fonctionnalité IA est disponible dans votre environnement client de production et démarre une période de 14 jours pour vous permettre de gérer vos contributions de données avant le début de l'extraction de données.
Description ou mises à jour techniques	Hebdomadaire, déclenché par les modifications.	Signale les mises à jour des descriptions de fonctionnalité et les modifications des champs

Type de notification	Synchronisation de la livraison	Objet
		de données utilisés par la fonctionnalité d'IA.
Fonctionnalités d'IA à venir	30 jours avant la publication.	Met à jour les fonctionnalités d'IA à venir applicables aux SKU que vous avez achetées.

Note: Pour déterminer le type de contrat d'abonnement de votre unité légale :

1. Accédez à votre [profil Community](#) .
2. Sous votre nom, cliquez sur le **nom de votre unité légale** .

Dans le champ **Contrat de services d'abonnement** :

- **MSA** indique le type d'accord de services principaux (MSA).
- **UMSA** indique le type d'accord d'abonnement principal universel (UMSA).

Steps

1. [Modifier les règles de sécurité des domaines](#) .

Ajoutez les groupes de sécurité appropriés au domaine *AI Features and Third Party Notification* dans le domaine fonctionnel Innovation Services.

2. [Activez les modifications de règles de sécurité en attente.](#)

3. Accédez à la tâche **Modifier la définition de l'environnement client - notifications** .

Dans l'onglet **Système** de la section **Paramètres de remise des notifications** , vérifiez que la règle de routage pour le **Type de notification parent** inclut les notifications par e-mail.

Si ce n'est pas le cas, sur la ligne **Ascend Notifications** , cochez la case Remplacer **les paramètres du type de notification parent** , puis sélectionnez une règle de routage qui inclut des notifications par e-mail. Voir [Créer des règles de routage de la notification](#) .

Sécurité : domaine *Set Up: Tenant Set Up - BP and Notifications* dans le domaine fonctionnel System.

Result

Les membres du groupe de sécurité recevront des notifications relatives aux modifications à venir des fonctionnalités d'IA.

Activer la fonctionnalité Innovation Services et les contributions de données IA pour les clients MSA

Context

Innovation Services propose des fonctionnalités qui vont au-delà des produits de base de Workday. Lorsque l'accord d'abonnement de service de votre organisation est un accord de service principal (MSA), vous pouvez uniquement accéder à ces fonctionnalités via Innovation Services. Pour accéder à Innovation Services, vous devez signer l'accord Innovation Services Addendum (ISA). Vous pouvez ensuite activer les fonctionnalités Innovation Services en procédant comme suit.

Certaines fonctionnalités d'Innovation Services utilisent l'intelligence artificielle (IA) dans le cadre de leur fonctionnalité. Pour ces fonctionnalités, vous devez également activer la contribution de données, que Workday utilise pour fournir de meilleurs résultats d'IA en fonctionnalité.

Contactez votre CSM ou demandez à votre administrateur de contact support désigné d'ouvrir une demande de réussite client via [Workday Community](#) pour acquérir et signer le formulaire de commande d'abonnement à Innovation Services.

Steps

1. Activez le domaine fonctionnel Innovation Services.
Voir [Étapes : activer les domaines fonctionnels et les règles de sécurité associées](#) .
2. [Modifier les règles de sécurité des domaines](#) .
Configurez le domaine *Manage: Innovation Services* dans le domaine fonctionnel Innovation Services.
3. Accédez au rapport **Innovation Services and Data Selection Opt-In** .
4. Dans la tâche **Activation d'Innovation Services** , cochez la case de la fonctionnalité que vous souhaitez activer dans l'onglet **Available Services** .
5. (Facultatif) Dans la tâche **Maintain Innovation Services Data Selection Opt-In** , cochez les cases des données que vous voulez fournir pour l'IA.
Voir : [Référence : contributions de données de Machine Learning](#) pour voir les contributions de données requises par la fonctionnalité.

Next Steps

Les fonctionnalités d'IA qui nécessitent des contributions de données ne fonctionneront pas de manière précise dans votre environnement client Sandbox. Pour tester les fonctionnalités d'IA avant de les déployer dans votre environnement client de production, utilisez vos environnements clients Sandbox Preview ou Implementation.

Vous pouvez utiliser ces tâches pour tester votre configuration dans votre environnement client d'implémentation.

Tâche	Description
Mettre à jour l'activation de la contribution de données hebdomadaire pour l'environnement client d'implémentation	Gère les extractions de données hebdomadaires futures.
Exécuter l'activation de la contribution de données à la demande pour l'environnement client d'implémentation	Extrait les données et abonnement l'environnement client à de futures extractions hebdomadaires.

Pour garantir l'exactitude des tests, Workday vous recommande d'actualiser votre environnement Sandbox Preview ou Implementation avant d'exécuter ces tâches. Comme les fonctionnalités d'IA requièrent une certaine quantité de données, les recommandations peuvent ne pas apparaître jusqu'à deux semaines.

Related Information

Examples

[Workday Community: Workday AI Gateway](#)

[Workday Community: Workday Innovation Services](#)

[Workday Community: Workday Innovation Services - Questions fréquemment posées](#)

Gérer les contributions de données Workday AI pour les clients de l'accord d'abonnement principal universel

Prerequisites

- Votre organisation doit figurer sur le contrat d'abonnement principal universel.

Note: Pour déterminer le type de contrat d'abonnement de votre unité légale :

1. Accédez à votre [profil Community](#) .
2. Sous votre nom, cliquez sur le **nom de votre unité légale** .

Dans le champ **Contrat de services d'abonnement** :

- **MSA** indique le type d'accord de services principaux (MSA).
- **UMSA** indique le type d'accord d'abonnement principal universel (UMSA).
- Sécurité : les domaines suivants dans le domaine fonctionnel Innovation Services :
 - *Manage: Data for ML Features*
 - *Afficher : Données pour les fonctionnalités de Machine Learning*

Context

Lorsque vous passez à l'UMSA, vous activez automatiquement les contributions de données pour les fonctionnalités d'IA.

Vous pouvez gérer les contributions de données des fonctionnalités d'IA par ligne de produit ou fonctionnalité d'IA.

Pour plus d'informations sur les contributions au niveau des fonctionnalités, voir [Référence : contributions des données de Machine Learning](#) .

Steps

1. Accédez au rapport **Contribution de données pour Workday AI** .
2. Exécutez la tâche :

Champ	Description
Ne pas autoriser la contribution de données	Lorsque vous cochez cette case, Workday : • Désactive la contribution de données pour la ligne de produit ou la fonctionnalité d'IA associée. • Supprime vos contributions de données passées dans un délai de 30 jours.
Détail des données	Cliquez sur View Data Collected pour afficher les définitions des types de données fournies à Workday.
Afficher les modifications de cotisations à venir	Cliquez sur Modifications de la contribution pour afficher les modifications à venir concernant les contributions de données obligatoires de la fonctionnalité.
Pays exclus de la collecte de données par site de l'utilisateur final	Au niveau de la fonctionnalité de l'IA, sélectionnez les pays que vous souhaitez exclure des contributions de données.

3. Cliquez sur **OK** .

Result

Lorsque vous désactivez les contributions de données, Workday arrête de collecter les nouvelles données et supprime vos contributions précédentes dans un délai de 30 jours.

Note:

La désactivation des contributions de données peut affecter les performances de certaines fonctionnalités d'IA. L'impact de la désactivation des contributions de données variera selon la fonctionnalité, depuis une expérience paiement jusqu'à une fonctionnalité qui ne fonctionne pas du tout.

Pour comprendre comment la désactivation des contributions peut affecter une fonctionnalité, consultez la [fiche d'informations Workday AI](#) de la fonctionnalité .

Related Information

Concepts

[Concept : Workday AI pour les clients d'un contrat d'abonnement principal universel](#)

Concept : Workday AI pour les clients d'un contrat d'abonnement principal universel

Note: Pour déterminer le type de contrat d'abonnement de votre unité légale :

1. Accédez à votre [profil Community](#) .
2. Sous votre nom, cliquez sur le **nom de votre unité légale** .

Dans le champ **Contrat de services d'abonnement** :

- **MSA** indique le type d'accord de services principaux (MSA).
- **UMSA** indique le type d'accord d'abonnement principal universel (UMSA).

Workday s'appuie souvent sur des contributions de données pour proposer des fonctionnalités d'intelligence artificielle (IA). Pour les clients soumis à l'URSSA, Workday active automatiquement les contributions de données pour les fonctions d'IA dans les SKU que vous avez achetées. Workday peut utiliser ces données pour entraîner ou améliorer la fonctionnalité d'IA associée.

Note: Workday active les fonctionnalités d'IA pour les clients UMSA dans les phases suivantes :

- Workday active les fonctionnalités d'IA lors de la prochaine mise à jour de service, par exemple dans la fenêtre de maintenance hebdomadaire.
- Les contributions de données sont renseignées dans la tâche **Contributions de données pour Workday AI** dans un délai de 24 heures.
- Les recommandations d'IA apparaissent dans votre environnement client dans un délai de 14 jours.

Contributions de données

Les clients UMSA peuvent gérer leurs contributions de données à l'aide de la tâche **Data Contribution for Workday AI** , sécurisée via les *domaines Manage: Data for ML Features* et *View: Data for ML Features* dans le domaine fonctionnel Innovation Services. Voir [Gérer les contributions de données Workday AI pour les clients de l'accord d'abonnement principal universel](#) .

Workday regroupe les contributions de données en fonction de la fonctionnalité d'IA qui utilise les données. Ainsi, vous ne partagez que les données spécifiques nécessaires pour chaque fonctionnalité. Vous pouvez gérer les contributions de chaque fonctionnalité individuellement ou au niveau de la ligne de produit.

Pour afficher les catégories de données requises pour chaque fonctionnalité d'IA, voir [Référence : contributions des données de Machine Learning](#) .

Lorsque vous désactivez les contributions de données pour une fonctionnalité d'IA ou une ligne de produit, vous ne fournissez plus de données et Workday supprime vos contributions de données passées dans un délai de 30 jours.

Note:

La désactivation des contributions de données peut affecter les performances de certaines fonctionnalités d'IA. L'impact de la désactivation des contributions de données variera selon la fonctionnalité, depuis une expérience paiement jusqu'à une fonctionnalité qui ne fonctionne pas du tout.

Pour comprendre comment la désactivation des contributions peut affecter une fonctionnalité, consultez la [fiche d'informations Workday AI](#) de la fonctionnalité .

Les rapports suivants peuvent également vous aider à afficher le détail des cotisations :

- Le rapport **Détail des données des fonctionnalités d'IA** , sécurisé via le domaine *View: Data for ML Features* , affiche les contributions de données associées à toutes les fonctions d'IA disponibles dans Workday, filtrées par ligne de produits.
- Le rapport **sur les fonctionnalités intelligentes** , sécurisé via les domaines *Manage: Data for ML Features* et *View: Data for ML Features* , affiche les fonctionnalités d'IA pour tous les SKU et les fonctionnalités d'IA pour les SKU achetés.

Notifications de fonctionnalités d'IA

Vous pouvez activer les notifications relatives aux modifications à venir des fonctions d'IA en configurant le domaine *AI Features and Third Party Notification* dans le domaine fonctionnel Innovation Services. Voir [Étapes : définir les notifications pour les contributions de données de la fonctionnalité d'IA](#) .

Les membres des groupes de sécurité ayant accès au domaine *AI Features and Third Party Notification* reçoivent ces notifications.

Type de notification	Synchronisation de la livraison	Objet
Disponibilité de la fonctionnalité d'IA	Le jour de la mise en production de la fonctionnalité.	Confirme que la fonctionnalité IA est disponible dans votre environnement client de production et démarre une période de 14 jours pour vous permettre de gérer vos contributions de données avant le début de l'extraction de données.
Description ou mises à jour techniques	Hebdomadaire, déclenché par les modifications.	Signale les mises à jour des descriptions de fonctionnalité et les modifications des champs de données utilisés par la fonctionnalité d'IA.
Fonctionnalités d'IA à venir	30 jours avant la publication.	Met à jour les fonctionnalités d'IA à venir applicables aux SKU que vous avez achetées.

Workday n'extrait pas les données pour la nouvelle fonctionnalité d'IA avant 14 jours après la sortie de Workday. Vous pouvez désactiver les contributions de données le jour de la mise en production de la fonctionnalité d'IA.

Test des fonctionnalités d'IA

Les fonctionnalités d'IA qui nécessitent des contributions de données ne fonctionneront pas de manière précise dans votre environnement client Sandbox. Pour tester les fonctionnalités d'IA avant de les déployer dans votre environnement client de production, utilisez vos environnements clients Sandbox Preview ou Implementation.

Vous pouvez utiliser ces tâches pour tester votre configuration dans vos environnements clients Sandbox Preview ou Implementation.

Tâche	Description
Mettre à jour l'activation de la contribution de données hebdomadaire pour l'environnement client d'implémentation	Gère les extractions de données hebdomadaires futures. Après avoir sélectionné Activer pour l'environnement client d'implémentation pour activer une fonctionnalité dans votre environnement client d'implémentation, le rapport s'exécute automatiquement le lundi pour actualiser les données.
Exécuter l'activation de la contribution de données à la demande pour l'environnement client d'implémentation	Extrait les données et abonnement l'environnement client à de futures extractions hebdomadaires.

Pour garantir l'exactitude des tests, Workday vous recommande d'actualiser votre environnement Sandbox Preview ou Implementation avant d'exécuter ces tâches. Comme les fonctionnalités d'IA requièrent une certaine quantité de données, les recommandations peuvent ne pas apparaître jusqu'à deux semaines.

Related Information

Examples

[Workday Community: StreamStreaming Feature Adoption et la page d'accueil Workday AI](#)

[Workday Community: Workday AI Gateway](#)

Référence : contributions de données Workday AI

En fonction du contrat d'abonnement de votre organisation, ces fonctionnalités vous obligent à fournir des données à votre environnement client pour tirer le meilleur parti de l'intelligence artificielle (IA) et du Machine Learning (ML).

- [Services inter-applications : fonctionnalités de base intelligentes disponibles pour la mise à jour](#)
- [Finances : fonctionnalités Financial Management Machine Learning GA](#)
- [Gestion financière : scan des justificatifs de frais](#)
- [HCM: HCM Machine Learning GA Features](#)
- [HCM: Workforce Management Machine Learning Services](#)
- [Paie : fonctionnalités du Machine Learning GA](#)
- [People Experience: User Experience Machine Learning](#)
- [Gestion des dépenses : fonctionnalités de Machine Learning GA pour Gestion des dépenses](#)

Services inter-applications : fonctionnalités de base intelligentes disponibles pour la mise à jour

Fonctionnalité de machine learning	Catégorie de données à activer	Éléments à prendre en compte
Recommandations de Machine Learning pour le processus de gestion Changer d'emploi	Données de l'organisation personnalisée Données de l'organisation hiérarchique Données d'événements d'affectation de personnel Données de profil d'employé	L'exclusion de pays n'est pas disponible pour les catégories Données d'organisations hiérarchiques et Données d'organisations personnalisées .

Finances : fonctionnalités Financial Management Machine Learning GA

Catégorie de données	Élément à prendre en compte
Données de règlement client	Pour activer le rapprochement intelligent des règlements clients, vous devez disposer de données de transactions de règlements clients pour les 30 derniers jours. Cette fonctionnalité fournit des recommandations utiles uniquement lorsque vous traitez des règlements clients dans Workday.
Données de frais	Pour utiliser la fonctionnalité Expense Protect, votre environnement client doit contenir au moins 10 000 lignes de note de frais. Lorsque les utilisateurs soumettent des notes de frais, Expense Protect les évalue automatiquement de manière à fournir des niveaux de risque, des recommandations et des analyses.
Données de lignes d'écritures	Avant de pouvoir utiliser la fonctionnalité Détection des anomalies d'écriture, vous devez disposer d'un historique de données d'un minimum de 12 mois.
Données des factures fournisseurs	Vous pouvez activer les suggestions par ML pour vos 5 sélections les plus couramment utilisées pour les worktags suivants sur les lignes de facture fournisseur : • Centre de coûts • Site • Région • Catégorie de dépense Note: Après avoir activé le service d'innovation, vous devez activer les recommandations de worktags sur les factures fournisseurs dans la section Options des comptes fournisseurs de la tâche Modifier la définition de l'environnement client - Finances .
Données des comptes clients	Pour activer le motif du trop-perçu client et les recommandations de worktags, vous avez besoin d'un minimum de 3 000 trop-perçus clients historiques. Pour activer les recommandations pour les lignes de facture client, vous avez besoin d'un minimum de 3 000 factures clients avec des champs de catégorie de produit et d'article de vente.

Gestion financière : scan des justificatifs de frais

Catégorie de données	Élément à prendre en compte
Scan des justificatifs de frais	Vous pouvez scanner les justificatifs aux formats PDF, JPG, TIFF et PNG.

HCM: HCM ML Features et Third Party Connectors GA

Pour activer ML pour ces fonctionnalités, vous devez activer le service **HCM ML Features and Third Party Connectors GA** et activer la contribution de données pour chaque fonctionnalité.

Fonctionnalité de machine learning	Catégories de machine learning pour la fonctionnalité	Catégorie de données à activer	Éléments à prendre en compte
ML pour Worker Profile and Skills	• Workday Skills Cloud • Suggestions d'aptitudes et vérification	• Données de demande de poste • Données de profil de talent • Données de profil d'employé	• Workday recommande d'activer Skills Cloud pour mettre à jour les données d'aptitude de vos employés. • L'exclusion de pays n'est pas disponible pour les catégories Talent Profile Data et Job Requisition Data. • Bien que cela ne soit pas obligatoire, Workday vous recommande d'activer la contribution de données pour les catégories Skills Cloud et Skills Suggestions and Verification.
ML pour Recruiting	• Emplois suggérés pour les candidats externes • Aptitudes suggérées pour les candidats externes • Aptitudes suggérées pour les demandes de poste	Données de demande de poste	L'exclusion de pays n'est pas disponible pour la catégorie Job Requisition Data.

Fonctionnalité de machine learning	Catégories de machine learning pour la fonctionnalité	Catégorie de données à activer	Éléments à prendre en compte
ML pour Learning Core	• Identification des aptitudes de formation • Machine Learning recommandé pour vous • Recommandations de contenu associées • En fonction de vos aptitudes à développer	Données de formation	• Utilisez la tâche Modifier la définition de l'environnement client - HCM pour configurer le worklet Recommandations de contenu associé. • Utilisez la tâche Mettre à jour l'expérience d'apprenant pour configurer les worklets En fonction de vos aptitudes à développer et Machine Learning recommandé pour vous. • Vous devez activer la catégorie Learning Data pour utiliser le worklet En fonction de vos aptitudes à développer. Workday fournit une version non-ML des recommandations si vous ne l'activez pas. • Vous devez activer la catégorie Learning Data pour utiliser le worklet Recommandations de contenu associé. • Vous devez activer les catégories Learning Data et Worker

Fonctionnalité de machine learning	Catégories de machine learning pour la fonctionnalité	Catégorie de données à activer	Éléments à prendre en compte
			Profile Data pour utiliser le worklet Machine Learning Recommandé pour vous. Workday met à jour les données ML toutes les 24 heures, du lundi au vendredi.
ML pour Talent Marketplace	Talent Marketplace	Données démographiques Données de demande de poste Données de formation Données de projets Données d'aptitudes Données du marché des opportunités Données de profil d'employé	- L'exclusion de pays n'est pas disponible pour les catégories Job Requisition Data et Talent Opportunity Marketplace Data. - Les données Talent Opportunity Marketplace et Worker Profile Data sont obligatoires. Pour en savoir plus sur les fonctionnalités qui dépendent de ces catégories de données, voir Étapes : définir Talent Marketplace.
ML pour le hub Carrière	Hub Carrière	Données de demande de poste Données de formation Données du marché des opportunités Données de profil de talent Données de profil d'employé	Vous devez être client du hub Carrière et satisfaire à certaines conditions pour utiliser cette fonctionnalité. Contactez votre CSM pour en savoir plus sur le Hub Carrière.

Fonctionnalité de machine learning	Catégories de machine learning pour la fonctionnalité	Catégorie de données à activer	Éléments à prendre en compte
		• Données d'aptitudes	• L'exclusion de pays n'est pas disponible pour les catégories Job Requisition Data, Talent Opportunity Marketplace Data et Talent Profile Data. • Les données de profil de talent et de profil d'employé sont obligatoires. Pour en savoir plus sur les fonctionnalités qui dépendent de ces catégories de données, voir Étapes : définir le hub Carrière.
ML pour le hub Management	Hub Management	• Données de formation • Données du marché des opportunités • Données de profil d'employé	• L'exclusion de pays n'est pas disponible pour la catégorie Talent Opportunity Marketplace Data. • La section Opportunités suggérées du hub Management utilise le Machine Learning pour proposer des suggestions personnalisées. Pour accéder à cette fonctionnalité, activez le service HCM Machine Learning GA Features et les catégories de données pertinentes,

Fonctionnalité de machine learning	Catégories de machine learning pour la fonctionnalité	Catégorie de données à activer	Éléments à prendre en compte
			puis activez Skills Cloud et Interests.

Note: Si vous avez activé Skills Cloud via le service d'innovation Workday Graph, votre sélection de données et la configuration de Skills Cloud restent valides.

Vous pouvez accéder au rapport **Innovation Service Data Details** pour accéder au détail des champs associés au service HCM ML Features et Third Party Connectors GA.

HCM: Workforce Management Machine Learning Services

Catégorie de données	Élément à prendre en compte
Données de configuration des temps	- Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalie de temps de Workday. - Workday met à jour les données utilisées pour entraîner le modèle de Machine Learning toutes les semaines avec l'ensemble des modèles de saisie des temps, du calendrier de travail et des données de calcul des temps.
Recherche de données	- Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalie de temps de Workday. - Workday met à jour les données utilisées pour entraîner le modèle de Machine Learning chaque semaine avec des données d'organisation et emploi limitées pour les employés qui ont saisi des temps.
Données historiques de tranches de planning	- Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalie de temps de Workday. - Workday met à jour les données utilisées pour entraîner le modèle de machine learning chaque semaine avec des tranches de planning historiques pour les employés.
Données de temps et d'absence des employés	- Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalie de temps de Workday. - Workday met à jour les données utilisées pour entraîner le modèle de Machine Learning toutes les semaines avec toutes les données des tranches horaires, de l'historique des tranches horaires, des saisies d'absences et des événements de révision des temps des employés.

Catégorie de données	Élément à prendre en compte
Données de livraison de fonctionnalité d'utilisateur	- Vous pouvez fournir des données dans votre environnement client à partir de la catégorie User Feature Delivery Data pour aider Workday à détecter les anomalies de temps. - Pour voir les données de cette catégorie auxquelles vous contribuez, exécutez le rapport Innovation Service Data Details pour les services de Machine Learning de Workforce Management. - L'exclusion de pays n'est pas disponible pour cette catégorie.

Paie : fonctionnalités du Machine Learning GA

Sélectionnez **Payroll: Payroll Machine Learning GA Features** dans le champ **Innovation Services Valid for Maintain Data Opt-In** . Cochez la case **Activer** pour les catégories suivantes :

Catégorie de données	Élément à prendre en compte
Résultats de paie anormaux	Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Workday Pay Anomalies.
Données de paie	- Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalies de la paie Workday. - Nous vous recommandons de définir au moins 6 périodes de paie ou plus d'historique de données de paie avant d'activer cette fonctionnalité. Cela garantit qu'il y a suffisamment de données de formation pour le modèle de machine learning.
Données de paie (historiques)	- Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalies de la paie Workday. - Nous vous recommandons de définir au moins 6 périodes de paie ou plus d'historique de données de paie avant d'activer cette fonctionnalité. Cela garantit qu'il y a suffisamment de données de formation pour le modèle de machine learning.
Validations des anomalies de paie	Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalies de la paie Workday.
États précédents des résultats de paie (historiques)	- Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalies de la paie Workday. - Nous vous recommandons de définir au moins 6 périodes de paie ou plus d'historique de données de paie avant

Catégorie de données	Élément à prendre en compte
	d'activer cette fonctionnalité. Cela garantit qu'il y a suffisamment de données de formation pour le modèle de machine learning.
Recherche de données	Vous devez fournir des données de cette catégorie pour utiliser la fonctionnalité Anomalies de la paie Workday.
Scan du formulaire P45	Vous devez sélectionner cette catégorie pour utiliser la fonctionnalité Workday P45 Tax Form Scanning.

Note: Pour activer la fonctionnalité Anomalies de paie et créer des modèles définis dans l'environnement client, vous devez activer les catégories suivantes :

- Résultats de paie anormaux
- Données de paie
- Données de paie (historiques)
- Validations des anomalies de paie
- États précédents des résultats de paie (historiques)
- Recherche de données

Si vous ne sélectionnez pas ces catégories de données, le modèle de machine learning ne sera pas créé et déployé comme prévu. La fonctionnalité Anomalies de paie ne sera pas entièrement fonctionnelle sans ces modèles.

Workday vous recommande de ne pas désactiver le service d'innovation une fois que vous avez exécuté le rapport Anomalies de paie pour afficher les prédictions. La désactivation désactive la fonctionnalité et entraîne des problèmes de synchronisation des données.

People Experience: User Experience Machine Learning

Catégorie de données	Élément à prendre en compte
Informations sur l'utilisateur générées par Workday	Workday affiche les 3 tâches recommandées dans la section Tâches rapides de la page d'accueil en fonction des éléments suivants : • Les tendances qui se produisent dans l'ensemble des environnements clients. • L'activité des utilisateurs dans votre environnement client de production.
Articles sur la gestion des connaissances	Vous pouvez fournir des données dans votre environnement client à partir de la catégorie Articles de la gestion des connaissances, ce qui permet à Workday de recommander des articles pertinents aux utilisateurs.
Requête de recherche	Vous pouvez fournir des données dans votre environnement client à partir de la catégorie Requête de recherche afin de fournir des résultats de recherche plus pertinents et personnalisés lorsque vous utilisez la recherche Workday.

Gestion des dépenses : fonctionnalités de Machine Learning GA pour Gestion des dépenses

Catégorie de données	Élément à prendre en compte
Données de transaction de dépense	- Si vous l'avez activé avant que Workday n'ajoute la prise en charge des bons de commande, Workday affiche la case à cocher Opt in to Additional Data . Cochez cette case pour alimenter en données les recommandations de bons de commande. - Lorsque vous désactivez la contribution des données, Workday purge vos données dans les deux semaines.

Related Information

Examples

[Workday Community: Workday Innovation Services](#)

FAQ : Transition de l'addendum Innovation Services (ISA) à l'Accord principal universel d'abonnement (UMSA)

- Pourquoi ne puis-je plus accéder aux rapports Innovation Services et aux domaines de sécurité associés ?
- Dois-je accepter les fonctionnalités d'IA de Workday dans l'UMSA, comme je l'ai fait pour l'ISA ?
- Comment vérifier que les fonctions activées dans le cadre de l'ISA restent activées dans le cadre de l'UMSA ?
- Comment vérifier que les intégrations tierces activées dans le cadre de l'ISA sont activées dans le cadre de l'UMSA ?
- La contribution de données pour les fonctionnalités d'application intelligente est-elle activée par défaut dans UMSA ?
- Comment refuser la contribution de données pour les fonctionnalités Workday AI ?
- Comment la configuration de la sécurité a-t-elle changé pour les fonctionnalités d'IA sous UMSA ?
- Comment voir les données spécifiques utilisées par Workday pour les fonctionnalités d'IA ?
- Comment Workday m'envoie-t-il une notification en cas de nouvelles fonctionnalités d'IA ou de mises à jour ?
- Que s'est-il passé avec Workday Media Cloud ? Mon contenu existant (comme les fichiers SCORM/ AICC) fonctionne-t-il toujours ?
- Quelles configurations faut-il réviser pour Workday Learning?
- Comment soumettre les demandes de support pour la gestion des abonnements (comme les nouvelles licences) ?

Pourquoi ne puis-je plus accéder aux rapports Innovation Services et aux domaines de sécurité associés ?	Lorsque vous signez l'UMSA, Workday remplace les rapports, tâches et domaines de sécurité permettant de gérer Innovation Services par ceux permettant de gérer les fonctionnalités d'IA (intelligence artificielle) de Workday dans l'UMSA. Consulter Concept : Workday AI pour les clients d'un contrat d'abonnement principal universel Exemple : plutôt que d'utiliser le rapport Innovation Services and Data Selection Opt-In (sécurisé via le domaine <i>Manage: Innovation Services</i>) pour gérer les fonctionnalités de Workday AI, vous utilisez le rapport Data Contribution for Workday
--	---

	AI (sécurisé via le domaine <i>Manage: Data for ML Features</i> et View: <i>Data for ML Features</i>). Les clients UMSA peuvent ignorer toutes les informations concernant Innovation Services.
Dois-je accepter les fonctionnalités d'IA de Workday pour l'UMSA, comme je l'ai fait pour l'addendum Innovation Services (ISA) ?	La plupart des fonctionnalités d'IA et intégration tierces sont automatiquement disponibles sous l'UMSA. Pour gérer ces fonctionnalités, voir Gérer les contributions de données Workday AI pour les clients de l'accord d'abonnement principal universel .
Comment vérifier que les fonctions activées dans le cadre de l'ISA restent activées dans le cadre de l'UMSA ?	Accédez au rapport Contribution de données pour l'IA de Workday (sécurisé via les domaines <i>Manage: Data for ML Features</i> et View: <i>Data for ML Features</i>) pour passer en revue les fonctionnalités d'IA de Workday activées dans l'UMSA et vérifier que les paramètres par défaut répondent aux besoins de votre organisation. Pour obtenir des instructions sur la gestion de l'activation des fonctionnalités, voir Gérer les contributions de données Workday AI pour les clients de l'accord d'abonnement principal universel . Pour prendre en compte l'impact de la gestion de vos fonctionnalités, voir Référence : contributions de données Workday AI .
Comment vérifier que les intégrations tierces activées dans le cadre de l'ISA sont activées dans le cadre de l'UMSA ?	Pour valider les intégrations qui ont utilisé Innovation Services, accédez au rapport All Integration Systems (sécurisé via le domaine <i>Integration Reports</i>) pour vérifier leur statut.
La contribution de données pour les fonctionnalités d'application intelligente est-elle activée par défaut dans UMSA ?	Par défaut, Workday active la contribution de données pour les fonctionnalités d'application intelligente.
Comment refuser la contribution de données pour les fonctionnalités Workday AI ?	Si vous souhaitez désactiver la contribution de données, vous pouvez utiliser le rapport Data Contribution for Workday AI (sécurisé via les domaines <i>Manage: Data for ML Features</i> et View: <i>Data for ML Features</i>) pour refuser des lignes de produit spécifiques ou des fonctionnalités individuelles. Note: • Si une application intelligente ne nécessite pas de contributions de données, il n'y a rien à désactiver. • Certains produits (tels que Peakon et HiredScore) peuvent ne pas offrir de

	désactiver la contribution de données à ce niveau.
Comment la configuration de la sécurité a-t-elle changé pour les fonctionnalités d'IA sous UMSA ?	Workday a mis à jour les domaines de sécurité. Vous devez vous assurer que vous avez activé les groupes de sécurité appropriés et les avez ajoutés aux domaines <i>Manage: Data for ML Features</i> et <i>View: Data for ML Features</i> . Ces domaines remplacent le précédent domaine <i>Manage: Innovation Services</i> .
Comment voir les données spécifiques utilisées par Workday pour les fonctionnalités d'IA ?	Cliquez sur View Data Collected dans le rapport Data Contribution for Workday AI (sécurisé via les domaines <i>Manage: Data for ML Features</i> et <i>View: Data for ML Features</i>) pour accéder à ces informations.
Comment Workday m'envoie-t-il une notification en cas de nouvelles fonctionnalités d'IA ou de mises à jour ?	Si vous avez activé les notifications relatives aux modifications à venir des fonctionnalités d'IA, Workday envoie une notification dans les 30 jours avant d'intégrer des fonctionnalités d'IA nouvelles ou mises à jour dans vos environnements clients de production ou Preview. Consulter Étapes : définir les notifications pour les contributions de données de la fonctionnalité d'IA .
Que s'est-il passé avec Workday Media Cloud ? Mon contenu existant (comme les fichiers SCORM/AICC) fonctionne-t-il toujours ?	Oui, votre contenu packagé existant continuera de fonctionner. Les conditions légales et contractuelles sont passées de l'ancien addenda aux conditions pertinentes dans les conditions de produit de la plateforme et des extensions de produit dans le cadre de votre UMSA.
Quelles configurations faut-il réviser pour Workday Learning?	Si vous utilisez du contenu tiers, vous devez vérifier votre configuration Nom de l'apprenant pour que le contenu soit correctement lancé. Après être passé à UMSA, accédez à la tâche Modifier la définition de l'environnement client - HCM et cochez la case à cocher Envoyer le nom de l'apprenant au fournisseur de contenu tiers . Voir Étapes : définir le contenu packagé pour la formation .
Comment soumettre les demandes de support pour la gestion des abonnements (comme les nouvelles licences) ?	Dans Workday Community, acheminez les demandes de gestion des abonnements, comme les nouvelles licences, en tant que Customer Success Request.