aws

Guide de l’utilisateur

Amazon One Enterprise

Amazon One Enterprise: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon One Enterprise ?

Amazon One Enterprise est un nouveau service d'authentification basé sur Palm qui fournit aux employés un accès sécurisé aux bâtiments et aux actifs de l'entreprise, sans avoir à utiliser de badges ou de codes PINs d'accès.

Rubriques

Appareil Amazon One

L'appareil Amazon One est conçu pour Amazon One Enterprise, un service d'identité sécurisé basé sur Palm pour le contrôle d'accès des entreprises. Notez les caractéristiques techniques suivantes de l'appareil :

- Entrées utilisateur — Palm Biometrics, correspondance par code QR
- Interface hôte : Wi-Fi (2.4 GHz et 5GHz), Ethernet, 2 ports de USB type A, 1 USB de type B
- Commentaires des utilisateurs — écran tactile de 5,5 pouces, anneau lumineux, haut-parleur, casque
- Protocole de contrôle d'accès physique — OSDP et Wiegand
- Alimentation — POE adaptateur AC/DC VAC d'entrée 110/220 fourni, 30 W à 15 V
- Sécurité — Interrupteurs antialtération
- Dimensions (HxWxD mm) — 86 x 85 x 256

Console Amazon One Enterprise

Amazon One Enterprise inclut une console, qui peut être utilisée de différentes manières :

- Un responsable informatique ou un responsable des installations utilise Amazon One Enterprise pour créer et gérer un site. Le site ressemble à un emplacement physique pour les tâches effectuées par l'équipe lors de la surveillance et de la gestion des appareils et des profils utilisateur Amazon One Enterprise. Les tâches du responsable informatique ou du responsable des installations incluent :
  - Création d'un site contenant toutes les instances d'appareils Amazon One dans un emplacement physique
  - Ajout d'un utilisateur administrateur pour gérer le site et d'un utilisateur installateur pour accéder aux codes QR d'activation

- Un administrateur utilise Amazon One Enterprise pour créer des instances d'appareils et pour gérer les appareils Amazon One. Les tâches d'administration incluent :
  - Création d'une instance d'appareil sous un site
  - Création d'un modèle de configuration à appliquer à une instance de périphérique
  - Surveillance de l'état de santé des appareils et mise à jour de leur configuration
  - Annulation des inscriptions d'utilisateurs
- Un installateur utilise Amazon One Enterprise pour accéder aux codes QR d'activation afin d'activer des appareils. Les tâches de l'installateur incluent :
  - Accès à un code QR d'activation sur la console
  - Sélection d'un code QR correspondant à l'instance de l'appareil à activer
  - Scanner le code QR sélectionné avec l'appareil Amazon One installé

Achat d'appareils Amazon One

Contactez-nous pour en savoir plus sur Amazon One Enterprise, et un membre de l'équipe de développement commercial vous contactera pour partager plus de détails sur notre offre, y compris les prix, et répondre à toutes vos questions.

Tarification d'Amazon One Enterprise

Contactez-nous pour en savoir plus sur les tarifs d'Amazon One Enterprise.

Comment fonctionne Amazon One Enterprise

Amazon One Enterprise est un service biométrique basé sur le cloud qui utilise un appareil Amazon One pour authentifier un utilisateur à l'aide de la biométrie de la paume de sa main. Vous pouvez commander des appareils Amazon One en nous contactant, et vous pouvez vous inscrire au service d'accès sécurisé Amazon One Enterprise en utilisant le AWS Management Console.

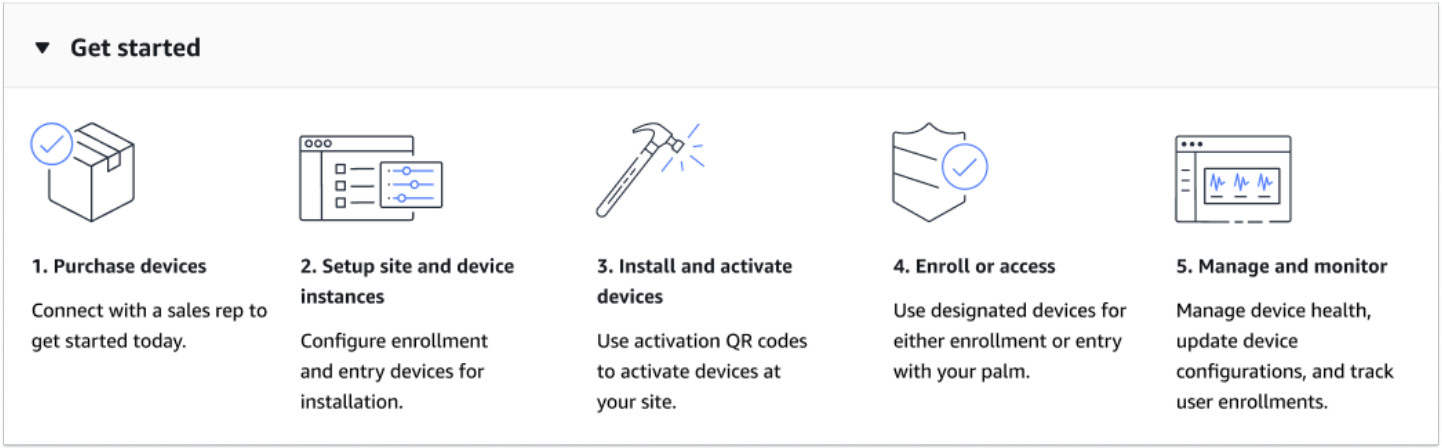
Une fois Amazon One Enterprise installé, vous pouvez activer les appareils et les enregistrer auprès de vous Compte AWS sur la console Amazon One Enterprise, et vous pouvez utiliser l'application d'authentification. Vous pouvez également consulter le profil biométrique d'un employé inscrit et annuler son inscription. Lorsque des employés quittent votre entreprise ou perdent leur badge, vous pouvez facilement supprimer leurs données biométriques. L'Amazon One Enterprise Console agit également comme un emplacement centralisé pour gérer les activités opérationnelles, telles que le suivi des appareils installés et la consultation des factures mensuelles.

Les employés peuvent s'inscrire en scannant leurs badges et leurs paumes dans les postes d'inscription supervisés sur place. Une fois que les employés sont inscrits, ils peuvent simplement passer leur paume sur un appareil Amazon One pour entrer ou sortir d'un lieu sécurisé.

Rubriques

Flux de travail Amazon One Enterprise

Le schéma suivant montre le flux de travail de base d'Amazon One Enterprise.



1. Achetez un appareil Amazon One en nous contactant.
2. Créez des sites et des instances d'appareils, en configurant les appareils d'inscription et d'entrée pour l'installation.
3. Après l'installation, activez les appareils Amazon One en scannant un code QR sécurisé spécifique à l'instance de l'appareil.
4. Demandez aux employés d'inscrire leurs paumes, puis de s'authentifier avec leurs paumes pour y accéder.
5. Utilisez les fonctionnalités de gestion et de surveillance : assurez-vous de l'intégrité des appareils, maintenez les configurations à jour et suivez les inscriptions des utilisateurs pour une surveillance complète.

Termes clés d'Amazon One Enterprise

Voici les principaux termes relatifs à Amazon One Enterprise :

- Site : le client gérait les bâtiments physiques dans lesquels il installe les appareils Amazon One Enterprise. Un site doit répondre aux exigences d'installation, de réseau et d'alimentation de vos appareils Amazon One Enterprise.
- Appareil : appareil biométrique Amazon One Enterprise à scanner la paume de la main à des fins d'authentification.
- Instance de périphérique : représentation logique d'un périphérique avec des configurations. L'utilisation d'instances d'appareils permet d'échanger des appareils Amazon One tout en héritant automatiquement des configurations et des noms définis précédemment. Une instance de périphérique possède un nom défini par l'utilisateur (convention de dénomination partagée avec votre logiciel de contrôle d'accès) et un ensemble de configurations de communication. Les instances de l'appareil ont trois états principaux :
  - Configuration des besoins
  - Prêt pour l'activation
  - Actif
- Modèle de configuration : ensemble complet de configurations appliquées à une instance de terminal.

Mise en route

Ce chapitre explique les étapes de base pour démarrer avec Amazon One Enterprise :

1. Configuration d'un site, d'instances d'appareils et de modèles de configuration : suivez ces étapes pour créer un cadre permettant d'ajouter un emplacement physique pour héberger vos appareils Amazon One, puis pour les configurer et les gérer. Les étapes utilisent la console Amazon One Enterprise. Vous n'utiliserez ce processus qu'occasionnellement, voire une seule fois, selon le nombre de sites, d'instances d'appareils et de modèles de configuration que vous choisissez d'avoir.
2. Installation et activation des appareils : suivez ces étapes au début de votre configuration. L'activation de l'appareil nécessite que les installateurs accèdent à la console Amazon One Enterprise via un téléphone portable pour récupérer les codes QR d'activation.
3. Gestion des appareils et des utilisateurs : suivez ces étapes pour une utilisation quotidienne de la console Amazon One Enterprise. Vous pouvez utiliser ces étapes pour surveiller l'état de santé des appareils, comprendre les indicateurs d'engagement des utilisateurs et configurer les appareils.

Pour en savoir plus sur Amazon One Enterprise, vous pouvez consulter la page détaillée du produit Amazon One Enterprise.

Rubriques

Configuration d'Amazon One Enterprise

La première étape de l'utilisation d'Amazon One Enterprise consiste à configurer votre site, vos instances d'appareils et vos modèles de configuration à l'aide de la console Amazon One Enterprise.

Rubriques

Étape 1 : Création d'un compte et d'un utilisateur administrateur

Inscrivez-vous pour un Compte AWS

Si vous n'avez pas de Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, une Utilisateur racine d'un compte AWSest créé. L'utilisateur root a accès à tous Services AWS et les ressources du compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après avoir souscrit à un Compte AWS, sécurisez votre Utilisateur racine d'un compte AWS, activer AWS IAM Identity Center, et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous au AWS Management Consoleen tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre Compte AWS adresse e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter à l'aide de l'utilisateur root, consultez la section Connexion en tant qu'utilisateur root dans le Connexion à AWS Guide de l'utilisateur.
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, voir Activer un MFA appareil virtuel pour votre Compte AWS utilisateur root (console) dans le guide de IAM l'utilisateur.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, voir Activation AWS IAM Identity Center dans le .AWS IAM Identity Center Guide de l'utilisateur.
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur avec la valeur par défaut Répertoire IAM Identity Center dans le .AWS IAM Identity Center Guide de l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URLidentifiant envoyé à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter à l'aide d'un utilisateur d'IAMIdentity Center, consultez la section Connexion au AWS portail d'accès dans le Connexion à AWS Guide de l'utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme à la meilleure pratique consistant à appliquer les autorisations du moindre privilège.

Pour obtenir des instructions, voir Créer un ensemble d'autorisations dans AWS IAM Identity Center Guide de l'utilisateur.

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans AWS IAM Identity Center Guide de l'utilisateur.

Étape 2 : ajouter des utilisateurs d'Amazon One Enterprise

Outre les utilisateurs administrateurs, vous pouvez également ajouter des utilisateurs qui n'ont pas les autorisations d'administrateur. Par exemple, ces utilisateurs peuvent être des installateurs qui accèdent à la console Amazon One Enterprise uniquement pour récupérer les codes QR d'activation des appareils Amazon One.

Pour ajouter un utilisateur Amazon One Enterprise

1. Suivez la procédure de connexion adaptée à votre type d'utilisateur, comme décrit dans Comment se connecter à AWS dans le Connexion à AWS Guide de l'utilisateur.
2. Dans le volet de navigation, sélectionnez Utilisateurs, puis sélectionnez Ajouter des utilisateurs.
3. Sur la page Spécifier les détails de l'utilisateur, sous Détails de l'utilisateur, dans Nom d'utilisateur, entrez le nom du nouvel utilisateur. Il s'agit de leur nom de connexion pour AWS.

> **Note**
>
> Le nombre et la taille des IAM ressources d'un Compte AWS sont limités. Pour plus d'informations, consultez la section IAMet AWS STS quotas. Les noms d'utilisateur peuvent être une combinaison de 64 lettres, chiffres et des caractères suivants : plus (+), égal (=), virgule (,), point (.), signe arobase (@), trait de soulignement (_) et tiret (-). Les noms doivent être uniques dans un compte. Ils ne sont pas sensibles à la casse. Par exemple, vous ne pouvez pas créer deux utilisateurs nommés TESTUSERet testuser. Lorsqu'un nom d'utilisateur est utilisé dans une politique ou dans le cadre d'une politiqueARN, le nom distingue les majuscules et minuscules. Lorsqu'un nom d'utilisateur apparaît aux clients dans la console, par exemple lors du processus de connexion, il n'est pas sensible à la casse.

4. Il vous est demandé si vous accordez l'accès à la console à un utilisateur. Sélectionnez Fournir un accès utilisateur au — AWS Management Console facultatif.
5. Sélectionnez Je souhaite créer un IAM utilisateur.
6. Pour Mot de passe de la console, sélectionnez l'une des options suivantes :

   - Mot de passe généré automatiquement — L'utilisateur reçoit un mot de passe généré de manière aléatoire conformément à la politique de mot de passe du compte. Vous pouvez afficher ou télécharger le mot de passe lorsque vous accédez à la page Récupérer le mot de passe.
   - Mot de passe personnalisé — L'utilisateur reçoit le mot de passe que vous entrez dans le champ.

7. (Facultatif) Par défaut, les utilisateurs doivent créer un nouveau mot de passe lors de leur prochaine connexion (cette option est recommandée) afin de garantir que l'utilisateur soit tenu de modifier son mot de passe la première fois qu'il se connecte.

   > **Note**
   >
   > Si un administrateur a activé le paramètre de politique de mot de passe de compte (Autoriser les utilisateurs à modifier leur propre mot de passe), cette case à cocher ne sert à rien. Dans le cas contraire, il attache automatiquement un AWS politique gérée nommée `IAMUserChangePassword`pour les nouveaux utilisateurs. La politique leur accorde l'autorisation de modifier leurs propres mots de passe.

8. Sélectionnez Suivant.
9. Sur la page Définir les autorisations, choisissez Joindre directement les politiques.
10. Sélectionnez les politiques que vous souhaitez associer à l'utilisateur.

    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

    > **Note**
    >
    > AmazonOneEnterpriseInstallerAccess la politique gérée permettra aux utilisateurs d'accéder aux codes QR d'activation uniquement dans la console Amazon One

Enterprise. Cette politique est idéale pour les entreprises qui font appel à un tiers pour installer des appareils Amazon One.

11. Sélectionnez Suivant.
12. (Facultatif) Sur la page Vérifier et créer, sous Balises, sélectionnez Ajouter une nouvelle balise pour ajouter des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour plus d'informations sur l'utilisation des balisesIAM, consultez la section IAMRessources de balisage.
13. Passez en revue tous les choix que vous avez faits jusqu'à présent. Une fois que vous êtes prêt à continuer, sélectionnez Créer un utilisateur.
14. Sur la page Récupérer le mot de passe, récupérez le mot de passe attribué à l'utilisateur :
    - Sélectionnez Afficher à côté du mot de passe pour afficher le mot de passe de l'utilisateur et l'enregistrer manuellement.
    - Sélectionnez Télécharger le fichier .csv pour télécharger les informations de connexion de l'utilisateur sous forme de fichier .csv que vous pouvez enregistrer en lieu sûr.
15. Sélectionnez Instructions de connexion par e-mail. Votre client de messagerie local s'ouvre avec un modèle que vous pouvez personnaliser et envoyer à l'utilisateur. Le modèle d'e-mail inclut les informations suivantes pour chaque utilisateur :
    - Nom utilisateur
    - URLsur la page de connexion au compte. Utilisez l'exemple suivant, en remplaçant l'ID et l'alias de compte comme approprié :

```
https://AWS-account-ID or alias.signin.aws.amazon.com/console
```

> **Important**
>
> Le mot de passe de l'utilisateur n'est pas inclus dans l'e-mail généré. Vous devez fournir le mot de passe à l'utilisateur d'une manière conforme aux normes de sécurité de votre organisation.

Étape 3 : créer un site

Maintenant que vous êtes connecté au AWS Management Console, vous pouvez utiliser la console Amazon One Enterprise pour créer votre site.

> **Important**
>
> Amazon One Enterprise est uniquement disponible dans la région de l'est des États-Unis (Virginie du Nord).

Pour créer un site

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Choisissez Accéder à la vue d'ensemble.
3. Dans le panneau de navigation, choisissez Sites.
4. Choisissez Créer des sites.
5. Sous Informations sur le site, dans Nom du site, entrez un nom pour le site.
6. Sous Adresse physique, entrez l'adresse du site sur lequel vos appareils Amazon One seront installés.
7. (Facultatif) Pour ajouter une balise au site, entrez une paire clé-valeur sous Balises, puis choisissez Ajouter une nouvelle balise. Pour supprimer cette balise avant de créer le site, choisissez Supprimer.
8. Choisissez Create site pour créer le site.

Étape 4 : créer des instances d'appareils

Pour créer une instance de terminal

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez Device instances. Assurez-vous que vous êtes sur l'onglet Instances non activées.
3. Sous Détails de l'instance, choisissez un site dans la liste déroulante Site ou créez un nouveau site en cliquant sur le bouton Créer un site.

4. Entrez manuellement le nom de chaque instance de périphérique individuelle.
5. (Facultatif) Pour ajouter une balise à l'instance de l'appareil, entrez une paire clé-valeur sous Balises, puis choisissez Ajouter une nouvelle balise. Pour supprimer cette balise avant de créer l'instance de l'appareil, choisissez Supprimer.
6. Choisissez Create instances pour créer les instances de l'appareil.

> **Note**
>
> Remarque : les instances du périphérique doivent être configurées avant que l'installation puisse avoir lieu.

Étape 5 : Création d'un modèle de configuration

Pour créer un modèle de configuration

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez Modèles de configuration.
3. Sélectionnez Create template (Créer un modèle).
4. Sous Informations sur le modèle, dans Nom du modèle, entrez le nom du modèle de configuration.
5. Sous Configurations de l'appareil, sélectionnez un mode de fonctionnement.

   To configure Enrollment operating mode

   1. (Facultatif) Dans Configuration Wi-Fi, entrez vos informations d'identification Wi-Fi.
   2. (Facultatif) Pour ajouter une balise au site, entrez une paire clé-valeur sous Balises, puis choisissez Ajouter une nouvelle balise. Pour supprimer cette balise avant de créer le site, choisissez Supprimer.
   3. Choisissez Configurer.

To configure Entry operating mode

1. Sous Paramètres du panneau de configuration, indiquez les paramètres de communication permettant aux appareils Amazon One de communiquer avec votre panneau de commande.
2. Sous Paramètres du format du badge, indiquez les paramètres de configuration qui spécifient la mise en page du format du badge de votre entreprise.
3. (Facultatif) Dans Configuration Wi-Fi, entrez vos informations d'identification Wi-Fi.
4. (Facultatif) Pour ajouter une balise au site, entrez une paire clé-valeur sous Balises, puis choisissez Ajouter une nouvelle balise. Pour supprimer cette balise avant de créer le site, choisissez Supprimer.
5. Choisissez Configurer.

> **Important**
>
> Vous devez configurer au moins un appareil d'inscription et un appareil d'entrée pour activer toutes les fonctionnalités d'Amazon One Enterprise en matière d'accès sécurisé.

Étape 6 : Configuration d'une instance de terminal pour l'activation

Une fois qu'une instance de périphérique est créée, vous la configurez à l'aide d'un modèle de configuration créé précédemment (voirÉtape 5 : Création d'un modèle de configuration), ou vous pouvez ajouter des configurations manuellement.

Pour configurer une instance de terminal en vue de son activation

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez Device instances. Assurez-vous que vous êtes sur l'onglet Instances non activées.
3. Sélectionnez une ou plusieurs instances à configurer.
4. Choisissez Configurer.
5. Sous Configurations des appareils, sélectionnez l'une des deux méthodes de saisie :

a. Pour l'option Utiliser un modèle, choisissez un modèle dans le menu déroulant. Vérifiez ou modifiez ces informations de configuration importées.

   Pour l'option Créer un modèle, voirÉtape 5 : Création d'un modèle de configuration.

b. Pour l'option de saisie manuelle, sélectionnez un mode de fonctionnement.

   To configure Enrollment operating mode

   a. (Facultatif) Dans Configuration Wi-Fi, fournissez un identifiant Wifi.
   b. (Facultatif) Pour ajouter une balise au site, entrez une paire clé-valeur sous Balises, puis choisissez Ajouter une nouvelle balise. Pour supprimer cette balise avant de créer le site, choisissez Supprimer.
   c. Choisissez Configurer.

   To configure Entry operating mode

   a. Sous Paramètres du panneau de configuration, indiquez les paramètres de communication permettant aux appareils Amazon One de communiquer avec votre panneau de commande.
   b. Sous Paramètres du format du badge, indiquez les paramètres de configuration qui spécifient la mise en page du format du badge de votre entreprise.
   c. (Facultatif) Dans Configuration Wi-Fi, fournissez un identifiant Wifi.
   d. (Facultatif) Pour ajouter une balise au site, entrez une paire clé-valeur sous Balises, puis choisissez Ajouter une nouvelle balise. Pour supprimer cette balise avant de créer le site, choisissez Supprimer.
   e. Choisissez Configurer.

6. Dans le tableau Instances non activées, l'état de l'instance doit s'afficher 

7. Vérifiez que les codes QR d'activation sont disponibles pour l'activation. Dans le volet de navigation, sélectionnez Activation QR Code.
8. Dans la liste déroulante Sélectionnez un site, sélectionnez un site.
9. Sous Informations sur le site, validez l'adresse du site.

10. Sous Codes QR d'activation, chaque instance de terminal possède un code QR correspondant. Choisissez Obtenir le code QR pour afficher les codes QR d'activation.

> **Important**
>
> Vous devez configurer au moins un appareil d'inscription et un appareil d'entrée pour activer toutes les fonctionnalités d'Amazon One Enterprise en matière d'accès sécurisé.

Installation et activation d'Amazon One

Une fois votre console Amazon One Enterprise configurée, les étapes suivantes consistent à installer les appareils Amazon One Enterprise sur votre site, puis à les activer.

> **Note**
>
> Cette section se concentre sur l'installation et utilise un navigateur mobile pour accéder AWS Management Console pour obtenir les codes QR d'activation de l'appareil.

Rubriques

Comprendre les exigences

Un appareil Amazon One peut être installé dans n'importe quelle entreprise ou entreprise dont les portes peuvent être contrôlées électriquement.

Exigence du panneau de commande

Les appareils Amazon One peuvent se connecter à la plupart des panneaux de contrôle d'accès standard en tant que lecteur. Les appareils Amazon One prennent en charge les protocoles suivants :

- OSDP(v1 et v2)
- Wiegand

Exigences relatives au réseau

Les appareils Amazon One doivent toujours être connectés à Internet pour un fonctionnement normal. La connectivité Internet peut être fournie par Ethernet filaire ou Wi-Fi. La bande passante minimale requise est de 10 Mbits/s.

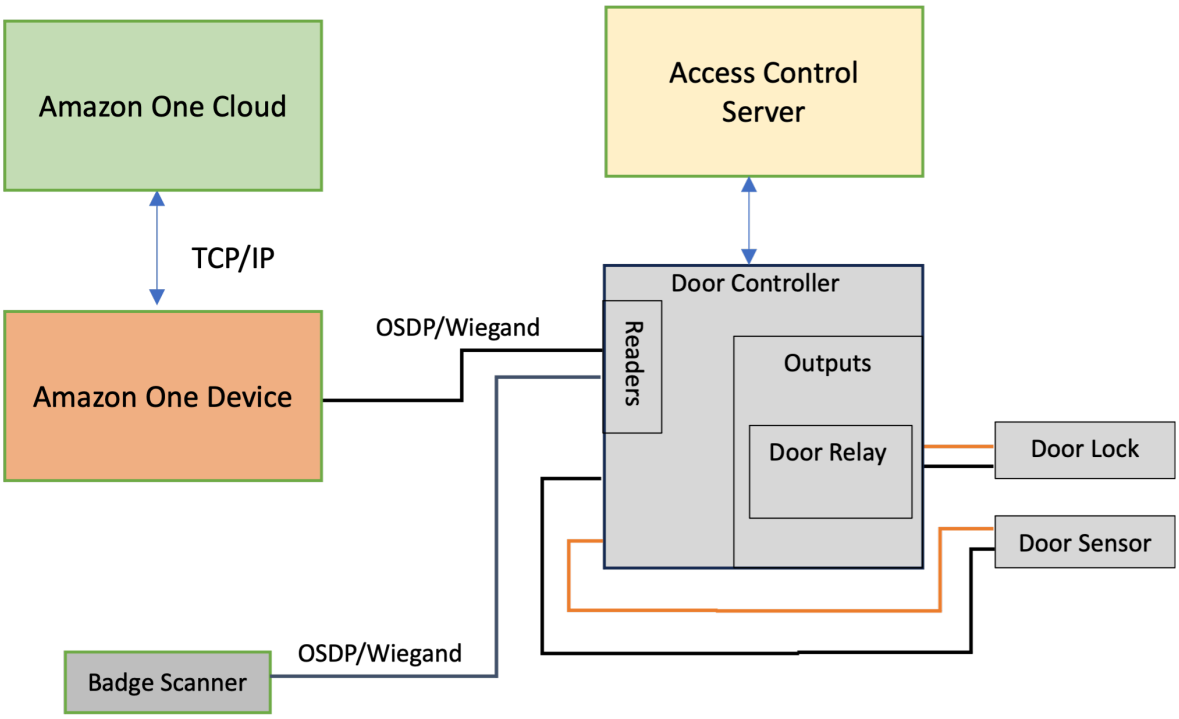
Exigence de puissance

Les appareils Amazon One peuvent être alimentés de deux manières différentes :

- En utilisant l'adaptateur secteur 120 V fourni dans la boîte.
- En utilisant un appareil compatible PoE+.

Comprendre les concepts d'installation

Pour sécuriser correctement l'accès aux bâtiments, Amazon One Enterprise vous recommande d'installer l'appareil dans le cadre d'un environnement de contrôle d'accès classique, comme décrit dans le schéma fonctionnel suivant.



Un environnement de contrôle d'accès comprend généralement les composants suivants :

- Appareil Amazon One : il s'agit du dispositif de reconnaissance de la paume qui effectuera une authentification biométrique pour identifier la personne qui tente d'accéder à une zone sécurisée du bâtiment.
- Serveur de contrôle d'accès : ce composant contrôle généralement les droits d'accès des utilisateurs à la zone sécurisée. Les badges IDs des personnes ayant accès à la zone sont généralement stockés sur ce serveur. Ce serveur met en cache les informations pertinentes IDs pour les contrôleurs de porte appropriés.
- Contrôleur de porte :
  - Un appareil Amazon One se connecte au serveur Door Controller via une OSDP interface.
  - Si une interface Wiegand est nécessaire, un COTS OSDP convertisseur vers Wiegand peut être utilisé.
  - Une fois l'authentification réussie, l'appareil Amazon One envoie l'identifiant du badge de l'utilisateur au Door Controller.
  - Le contrôleur de porte répond par une décision, qui permet ensuite à l'appareil Amazon One d'afficher un message d'accès accordé ou d'accès refusé.
- Scanner de badges : Un scanner de badges est généralement utilisé pour scanner les RFID badges et envoyer le numéro du badge au serveur de contrôle d'accès. Avec Amazon One

Enterprise, un scanner de badges est connecté à l'appareil Amazon One d'inscription pour permettre de scanner les badges des employés et de les associer à leur profil Palm.

Installation du socle Amazon One Enterprise

Cette section décrit les exigences en matière de localisation et les étapes nécessaires à l'installation d'un socle Amazon One Enterprise.

Avant de commencer l'installation, assurez-vous que les conditions préalables suivantes sont remplies :

- Si vous utilisez le signe POE + pour alimenter l'appareil, assurez-vous que le câblage Cat6 est installé et qu'un injecteur ou un commutateur POE + est disponible pour l'utilisation.

- Si une source d'alimentation CA (120 V) est utilisée, une prise secteur doit être disponible à moins de 20 pieds du AOE socle.
- Le sol doit être plat et propre.
- Le piédestal ne doit pas bloquer la porte ou la voie.
- Tout excédent de câble doit être conservé à l'intérieur du socle et fixé.

Pour installer le socle d'un appareil Amazon One

1. Retirez le socle Amazon One Enterprise de son emballage.
2. Retirez la porte en dévissant les deux vis inviolables M4.
3. Branchez le câble d'alimentation. Faites passer le câble dans le trou de la plaque de base du socle.
4. Enroulez tout câble d'alimentation excédentaire à l'intérieur du socle.
5. Faites passer le câble Ethernet (Cat5E ou supérieur) par la plaque inférieure du socle et branchez-le sur le port Ethernet.
6. Faites passer le câble Ethernet (Cat5E ou supérieur) par la plaque inférieure du socle et branchez-le sur le port Ethernet.
7. Installez une boucle en ferrite sur le câble Ethernet à 2 pouces au-dessus de la base du socle.
8. Branchez le câble RS485 série entre le panneau de contrôle d'accès (ou le lecteur de badges) et le socle, avec une longueur excédentaire de 1 pied.
9. Installez une boucle en ferrite sur le RS485 câble à 2 pouces au-dessus de la base du socle.
10. Branchez l'alimentation sur la prise et vérifiez que l'appareil Amazon One est allumé.
11. Refixez la porte au socle et revissez les deux vis antialtération M4 pour la fixer.

Installation d'un appareil Amazon One à montage mural

Cette section détaille les exigences de localisation et les étapes nécessaires pour installer votre appareil Amazon One à montage mural.

Avant de commencer l'installation, vérifiez les points suivants :

- L'appareil Amazon One à montage mural est destiné à une utilisation en intérieur uniquement.
- Le mur est plat.
- Le haut du support mural ne doit pas être à plus de 44 à 46 pouces du sol après le montage.

- Tout le surplus de câble se trouve derrière le support mural et est fixé.
- Pour l'alimentation par Ethernet (PoE++) :

  Assurez-vous qu'un commutateur IEEE 802.3bt (type 3) de classe POE 6++ (extrémité) ou un injecteur (envergure intermédiaire) est disponible pour utilisation, qu'il soit répertorié ou certifié et conforme à la norme 62368-1. IEC

  À utiliser uniquement AOE avec une source PoE++ approuvée.

  La source PoE++ doit être située dans le même bâtiment.

- Pour une alimentation électrique de 15 V DC, vous ne devez utiliser l'appareil Amazon One qu'avec une alimentation approuvée de NEC classe 2 ou à alimentation limitée répertoriée ou certifiée.

Outils nécessaires :

- Mèche de 1/4 po pour cloison sèche ou maçonnerie si des ancrages muraux sont nécessaires
- Pince à dénuder
- Mèche de 7/64 po pour percer des avant-trous
- Tournevis Phillips #2
- Tournevis à tête plate de 0,5 mm x 2 mm
- Pilote Torx sécurisé T12
- Crayon
- Niveau

Inclus avec l'appareil Amazon One à montage mural :

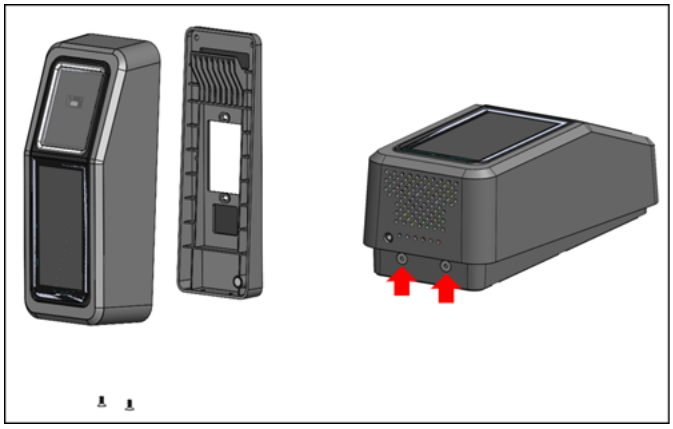
- 6 ancrages pour cloisons sèches #8
- 6 vis #8 -32 de 1 po de long
- 2 vis mécaniques #6 -32 de 1 po
- 2 connecteurs de bornier à 6 positions
- 2 vis à tête plate Torx Security M4x10

Pour installer la plaque de montage mural sur votre appareil Amazon One

<result>

</result>

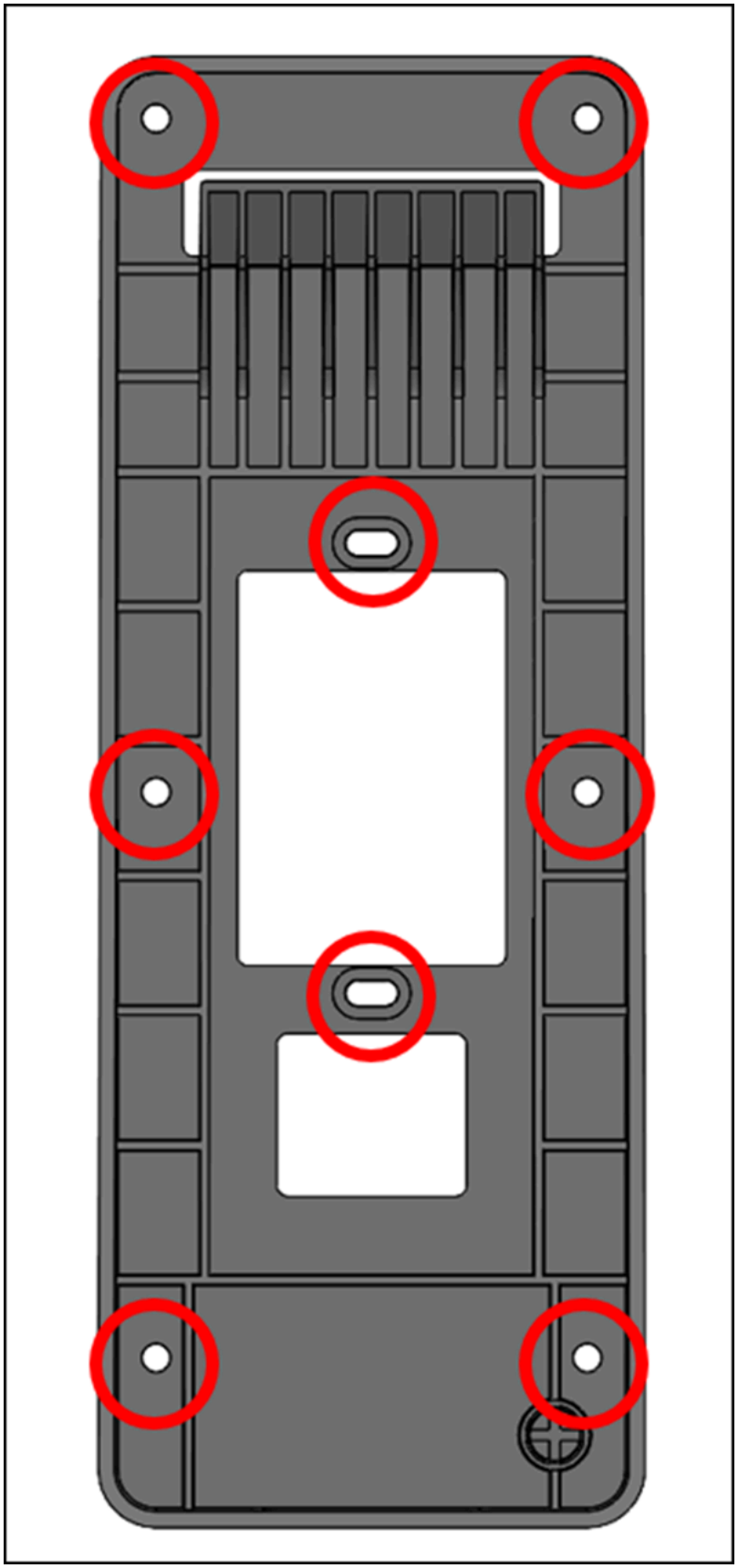
1. Retirez votre appareil Amazon One de son emballage.
2. Séparez la plaque de montage de votre appareil Amazon One en retirant les deux vis de sécurité Torx inférieures.



3. Positionnez la plaque de montage sur le mur à l'endroit souhaité. Utilisez le support comme gabarit pour marquer les six trous de vis extérieurs, comme indiqué dans l'image suivante.

   (Facultatif) Si un boîtier monobloc est disponible en position d'installation, effectuez les opérations suivantes :

   - Fixez la plaque sans serrer sur le boîtier en insérant les vis mécaniques #6 -32 incluses dans les trous oblongs.
   - Assurez-vous que la plaque de montage est à niveau.
   - Utilisez la plaque de montage comme gabarit pour marquer les six positions de vis avec un crayon. Vous pouvez utiliser les trous oblongs et la vis #6 -32 comme support supplémentaire pour la plaque de montage. N'utilisez pas les positions de vis #6 -32 comme principal moyen de montage de la plaque murale.



4. Pour le montage sur des surfaces en stuc, en placoplâtre, en brique ou en béton, percez des trous de 1/4 po à chaque endroit marqué, puis installez les ancrages muraux en les enfonçant dans le trou jusqu'à ce que l'ancrage soit au même niveau que le mur.

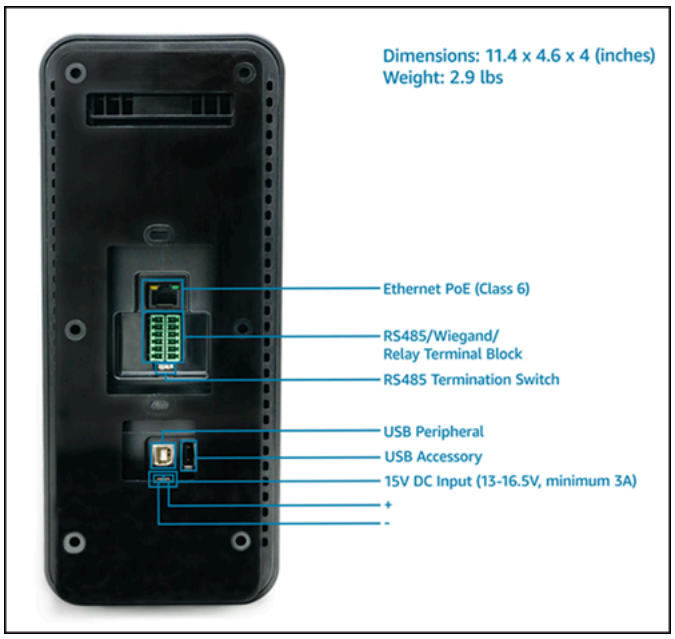
   En cas de montage sur une surface en bois, les ancrages ne sont pas nécessaires et seuls des avant-trous de 7/64 pouces sont nécessaires aux emplacements marqués.
5. Fixez sans serrer la plaque murale au mur à l'aide des vis à bois #8 en position d'ancrage.
6. Une fois que toutes les fixations sont en place, assurez-vous que la plaque de montage est à niveau.
7. Serrez les vis pour fixer la plaque de montage au mur.

Pour connecter votre appareil Amazon One à montage mural

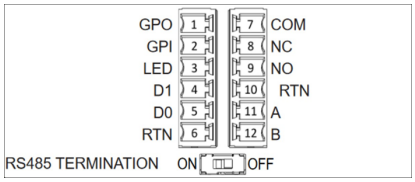
Vous pouvez configurer un appareil Amazon One avec les protocoles OSDP de contrôle d'accès Weigand. Pour simplifier l'installation, l'appareil Amazon One utilise des connecteurs de bornier (Mfg P/N : Phoenix Contact 1767694). Vous avez également la possibilité de configurer un appareil Amazon One pour contrôler directement les appareils externes à l'aide du relais interne ou des connexions d'entrée et de sortie à usage général.

1. Pour déterminer la configuration de câblage appropriée pour votre application, reportez-vous au schéma et au tableau de connexions suivants.

   Pour connaître les caractéristiques électriques détaillées des signaux, reportez-vous aux instructions de câblage.



Connexions



Connecteur	Connexion	Description	Utiliser	
1	GPO	Sortie à usage général	Signal de sortie numérique - Facultatif	
2	GPI	Saisie à usage général	Signal d'entrée numérique — Facultatif	
3	LED	Wiegand LED	Wiegand — Facultatif LED	
4	D1	Wiegand D1	Wiegand data 1 — Fil blanc	

Connecteur	Connexion	Description	Utiliser
5	D0	Wiegand D0	Wiegand data 0 — Câble vert
6	RTN	Retour du signal	Wiegand Ground — Fil noir
7	Com	Relais commun	Relais de contact commun — fil blanc
8	NC	Relais normalement fermé	Relais de contact normalement fermé — fil orange
9	NO	Relais normalement ouvert	Relais de contact normalement ouvert — fil jaune
10	RTN	Retour du signal	OSDPretour — Fil noir
11	A	RS485_A/D1/ Horloge	OSDPD1 — Fil blanc
12	B	RS485_B/D0/ Données	OSDPD0 — Fil vert

2. Lorsque vous installez un fil, dénudez 3 mm à 5 mm de l'extrémité du fil.
3. Insérez l'extrémité dénudée du fil dans la position terminale souhaitée.
4. À l'aide d'un tournevis à tête plate, tournez la vis de fixation du terminal dans le sens des aiguilles d'une montre pour fixer le fil jusqu'à ce qu'il soit bien ajusté. Ne pas trop serrer.

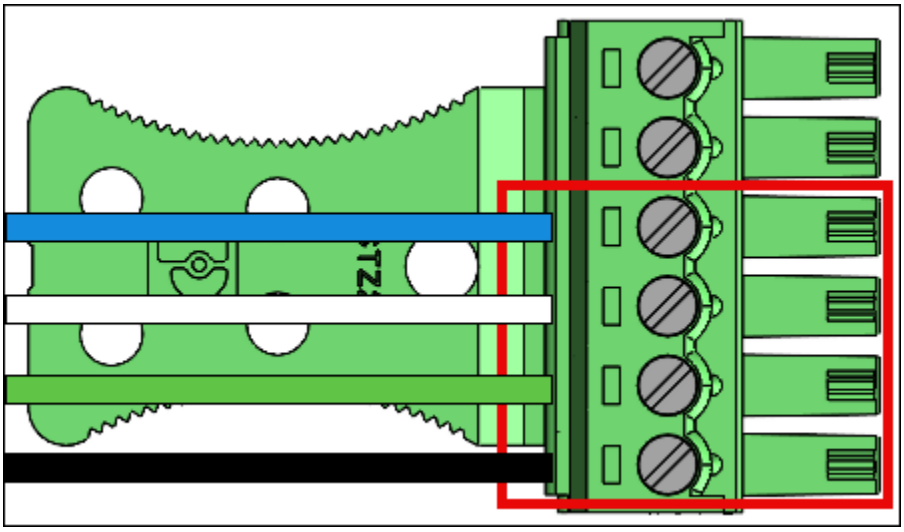
5. Après la fixation, tirez doucement sur le fil pour vous assurer qu'il est bien en place.
6. Après avoir effectué les connexions nécessaires, insérez le connecteur dans le réceptacle correspondant du bornier de votre appareil Amazon One.
7. Insérez le câble Ethernet Cat6 dans la RJ45 prise jack.
8. Positionnez l'appareil Amazon One de manière à ce que le crochet de la plaque murale glisse dans l'ouverture située à l'arrière de l'appareil.
9. Assurez-vous que les câbles ne sont pas coincés entre l'appareil et la plaque de montage, et laissez l'appareil pivoter et le siège en position.
10. Fixez votre appareil Amazon One à la plaque de montage à l'aide de deux vis à tête plate Torx Security M4x10.
11. Serrez les vis à la main. Ne serrez pas trop fort.

Pour câbler votre appareil Amazon One à montage mural

Installez uniquement les fils nécessaires à votre application.

Connexions Wiegand

- Insérez le fil bleu dans la broche 3 (LED).
- Insérez le fil blanc dans la broche 4 (D1).
- Insérez le fil vert dans la broche 5 (D0).
- Insérez le fil noir dans la broche 6 (RTN).



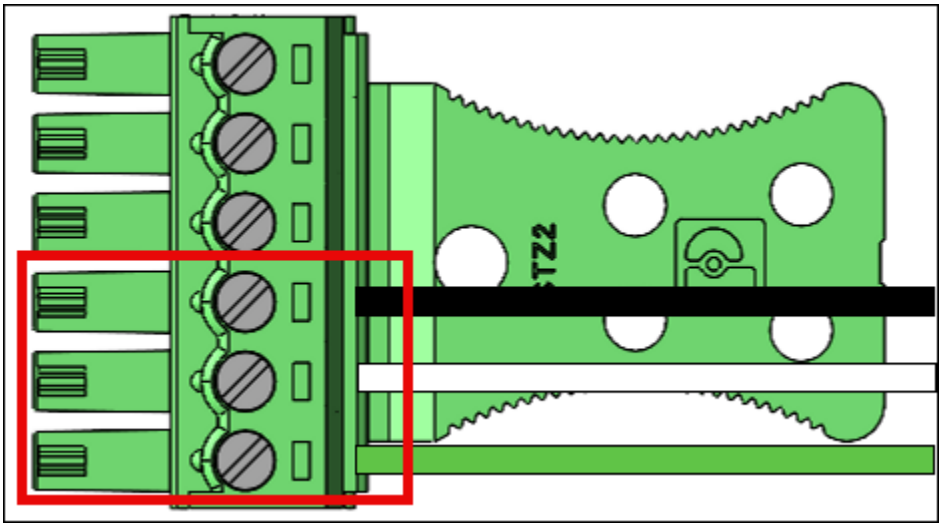
Câblage de sortie Wiegand

Connecteur	Connexion	Description	Utiliser	
3	LED	Wiegand LED	LEDEntrée Wiegand — en option (5 V) TTL	
4	D1	Wiegand D1	Sortie Wiegand D1 (5 V) TTL	
5	D0	Wiegand D0	Sortie Wiegand D0 (5 V) TTL	
6	RTN	Retour du signal	Référence Wiegand GND	

Activez le commutateur de RS485 terminaison sur « ON » si l'appareil est le dernier appareil sur la ligne. Ce commutateur active la terminaison de la résistance de 120 ohms sur la ligne.

RS485connexions

- Insérez le fil noir dans la broche 10 (RTN).
- Insérez le fil blanc dans la broche 11 (A).
- Insérez le fil vert dans la broche 12 (B).

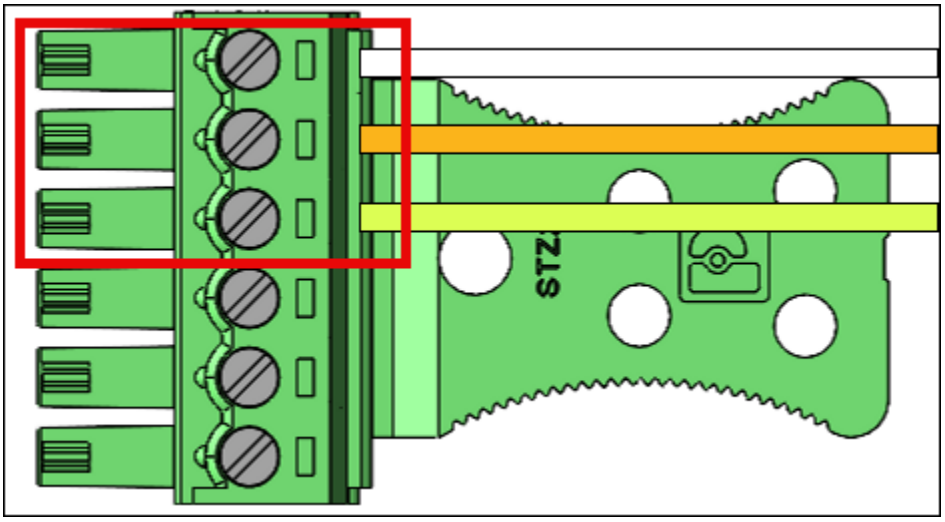


RS485câblage

Connecteur	Connexion	Description	Utiliser	
10	RTN	Retour du signal	Ground (Sol)	
11	A	RS485_A/D1/ Horloge	RS485signal non inverseur	
12	B	RS485_B/D0/ Données	RS485signal inverseur	

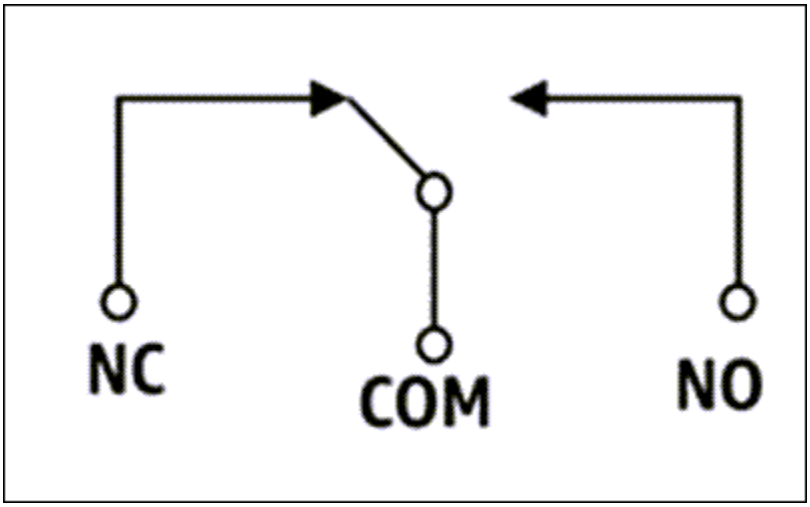
Connexions relais

- Insérez le fil blanc dans la broche 7 (COM).
- Insérez le fil orange dans la broche 8 (NC).
- Insérez le fil jaune dans la broche 9 (NO).



Câblage du relais

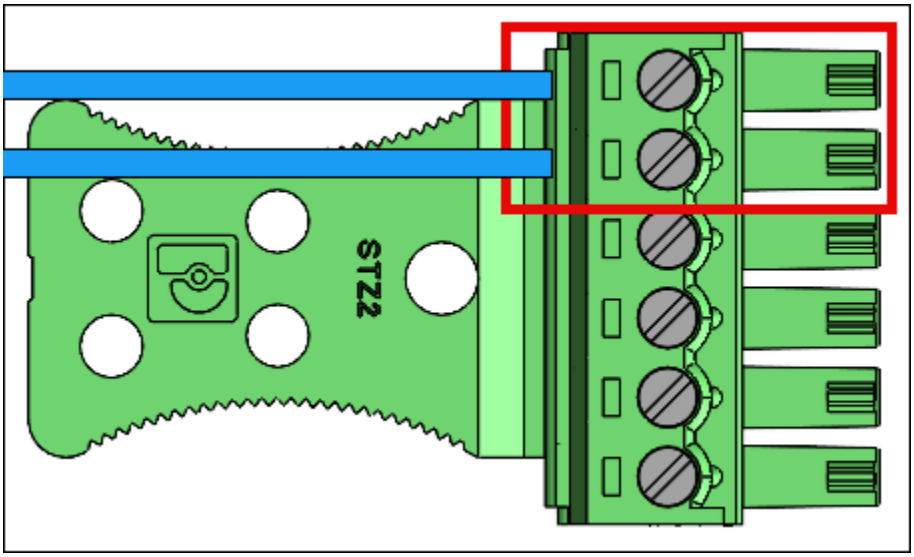
Connecteur	Connexion	Description	Utiliser	
7	COM	Relais commun	Relais de contact commun — fil blanc	
8	NC	Relais normalement fermé	Relais de contact normaleme nt fermé — fil orange	
9	NO	Relais normalement ouvert	Relais de contact normalement ouvert — fil jaune	



Le relais doit être utilisé conformément aux valeurs de sécurité spécifiées 30 VAC /60VDC, 60 W max.

Connexions d'entrée/sortie numériques

- Insérez le fil bleu dans la broche 1 (GPO).
- Insérez le fil bleu dans la broche 2 (GPI).



Connecteur	Connexion	Description	Utiliser	
1	GPO	Sortie à usage général	Signal de sortie numérique (5 V)	
2	GPI	Saisie à usage général	Signal d'entrée numérique (3,6 V — 5 V)	

- Les connexions d'entrée/sortie numériques doivent être utilisées comme indiqué.

Consultez Activation d'un appareil Amazon One la section pour activer votre appareil Amazon One.

Installation du hub d'E/S pour appareils Amazon One pour un accès sécurisé

Cette section détaille les exigences de localisation et les étapes nécessaires pour installer votre appareil Amazon One Enterprise (AOE) avec I/O Hub.

Avant de commencer l'installation, vérifiez les points suivants :

- L'appareil Amazon One avec hub d'E/S est destiné à une utilisation en intérieur uniquement.
- Pour l'alimentation par Ethernet (PoE++) :

Assurez-vous qu'un commutateur IEEE 802.3bt (type 3) de classe POE 6++ (extrémité) ou un injecteur (envergure intermédiaire) est disponible pour utilisation, qu'il soit répertorié ou certifié et conforme à la norme 62368-1. IEC

Utilisez uniquement un appareil Amazon One doté d'une source PoE++ approuvée.

La source PoE++ doit être située dans le même bâtiment.

- Pour une alimentation électrique de 15 V DC, vous ne devez utiliser l'appareil Amazon One qu'avec une alimentation approuvée de NEC classe 2 ou à alimentation limitée répertoriée ou certifiée. Reportez-vous à la section DC optionnelle ci-dessous.

Outils nécessaires :

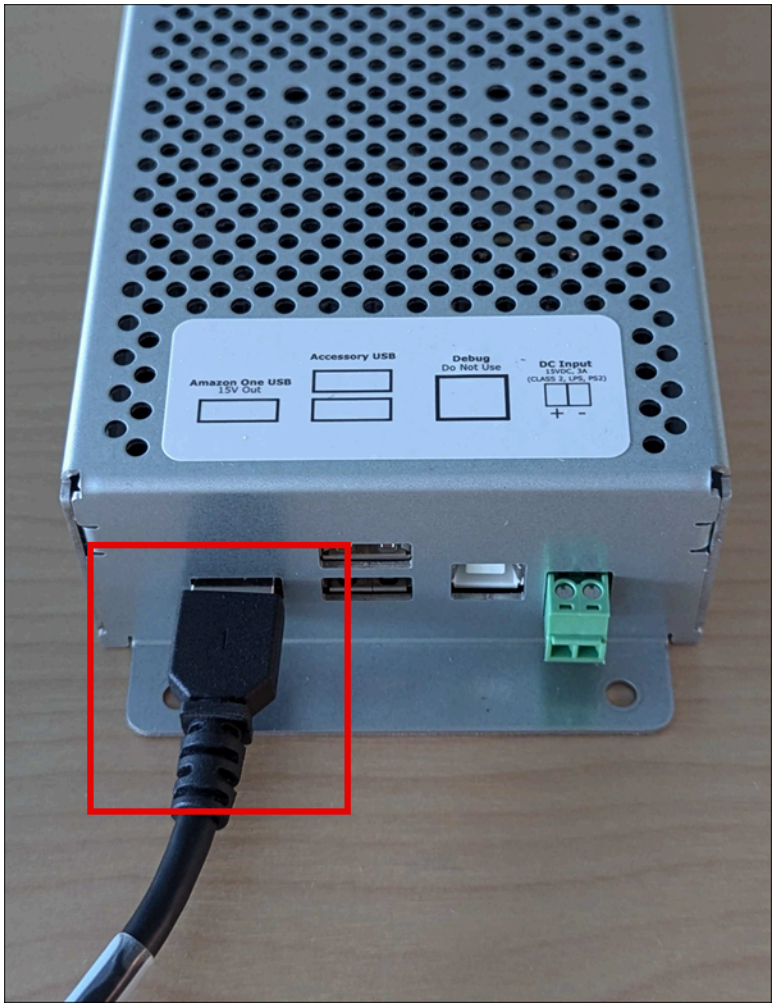
- Pince à dénuder
- Tournevis Phillips #2
- Tournevis à tête plate de 0,5 mm x 2 mm

Inclus avec l'appareil Amazon One avec hub d'E/S :

- 2 connecteurs de bornier à 6 positions
- Connecteur DC
- Câble d'alimentation/de données de 72 pouces

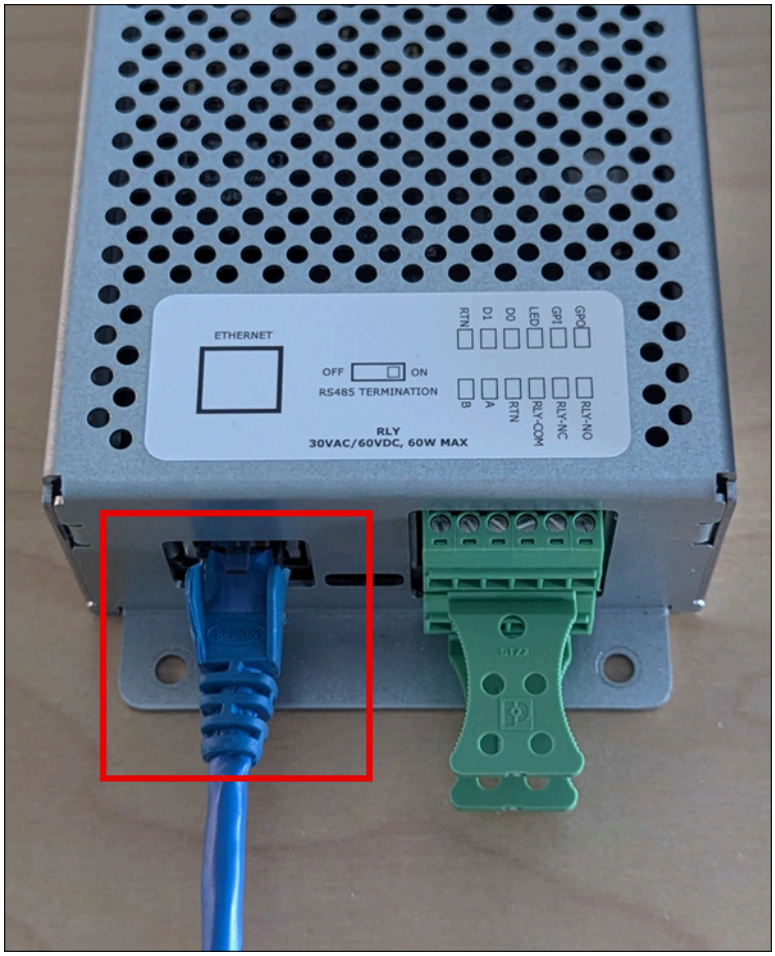
Pour installer le hub d'E/S sur votre appareil Amazon One

1. Retirez votre appareil Amazon One avec I/O Hub de son emballage.
2. Fixez le hub d'E/S à l'emplacement souhaité.
3. Branchez le USB câble Amazon One sur le port du hub d'E/S.



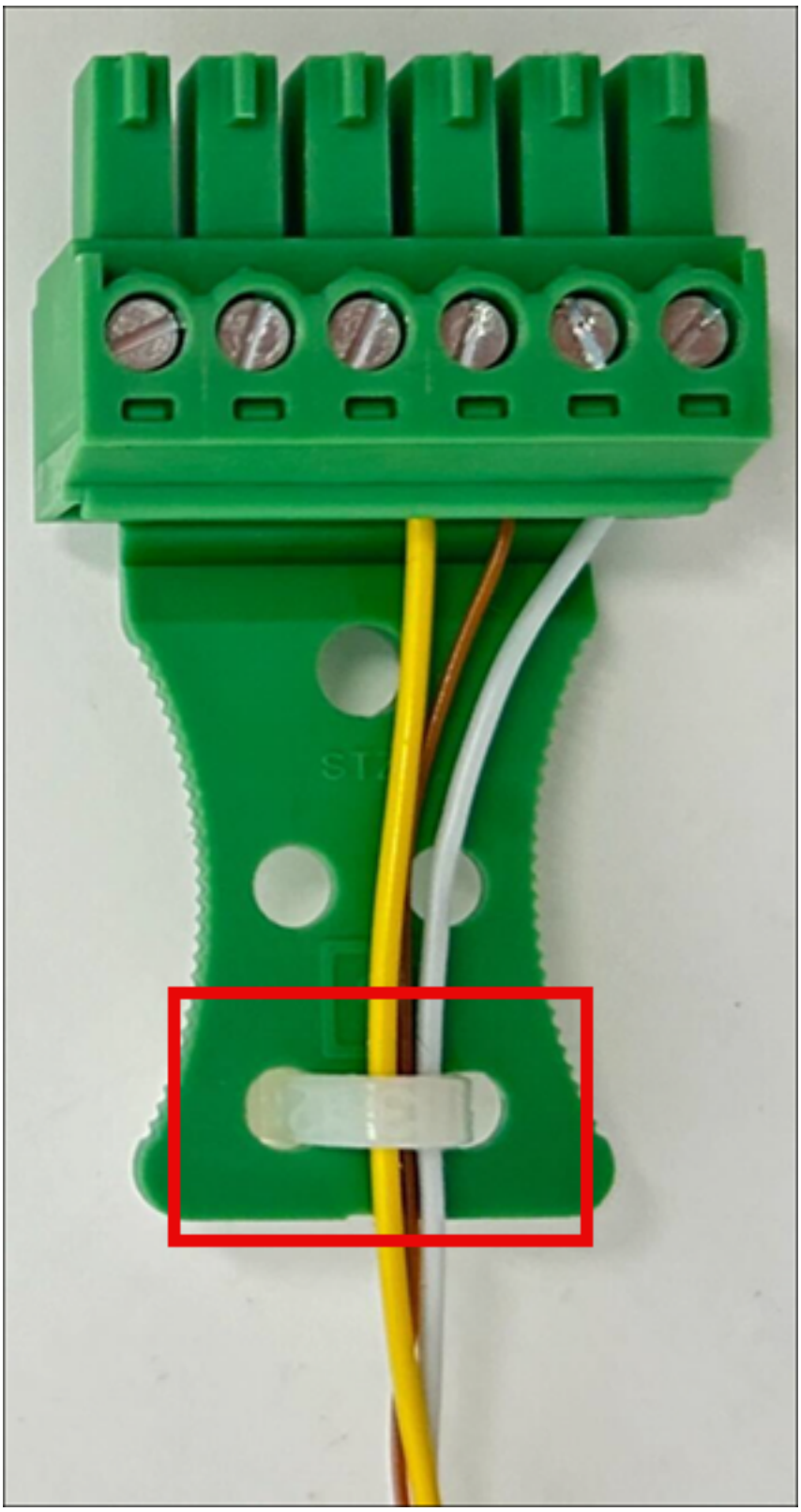
4. Pour une alimentation POE ++, branchez le câble Ethernet reliant la source POE ++ au port du hub d'E/S.

   Facultatif : pour l'alimentation en courant continu, reportez-vous à la section d'installation du câblage en courant continu ci-dessous.



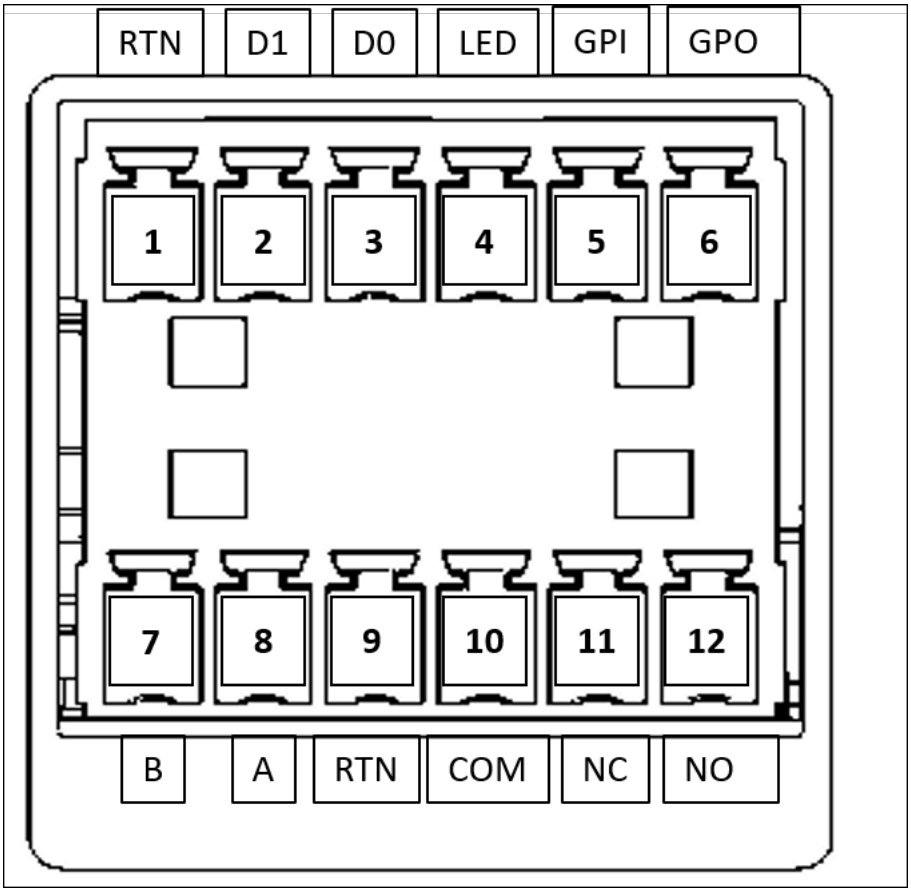
Pour câbler le hub d'E/S de votre appareil Amazon One

- Installez une boucle anti-goutte pour éviter que des liquides ne s'écoulent accidentellement le long du cordon et ne pénètrent dans le hub d'E/S.
- Fixez une pince antitraction pour protéger les fils contre les dommages ou le stress, comme indiqué dans l'image suivante.



1. Insérez uniquement les fils nécessaires à votre application dans les connecteurs du bornier. Reportez-vous au tableau de câblage et aux schémas suivants.

2. Insérez les connecteurs du bornier dans le hub d'E/S.



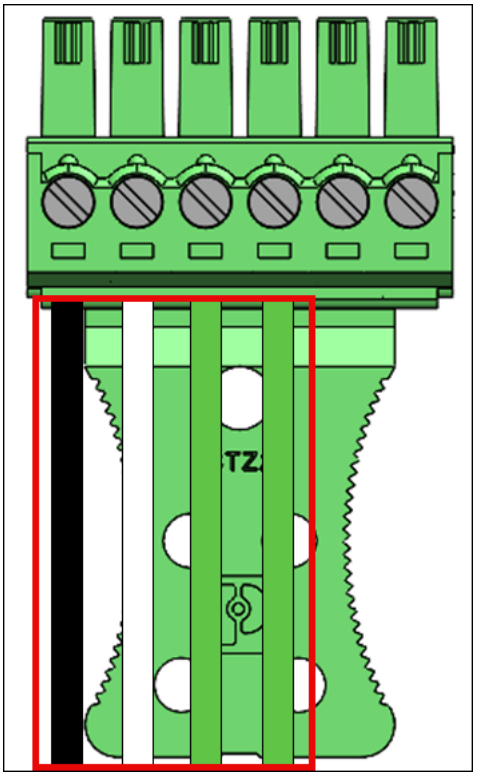
Connecteur	Connexion	Description	Utiliser	
1	RTN	Retour du signal	Wiegand Ground — Fil noir	
2	D1	Wiegand D1	Wiegand Data 1 — Fil blanc	
3	D0	Wiegand D0	Wiegand data 0 — Câble vert	
4	LED	Wiegand LED	Wiegand — Facultatif LED	

Connecteur	Connexion	Description	Utiliser	
5	GPI	Saisie à usage général	Signal d'entrée numérique — Facultatif	
6	GPO	Sortie à usage général	Signal de sortie numérique - Facultatif	
7	B	RS485_B/D0/ Données	OSDPD0 — Fil vert	
8	A	RS485_A/D1/ Horloge	OSDPD1 — Fil blanc	
9	RTN	Retour du signal	OSDPretour — Fil noir	
10	COM	Relais commun	Relais de contact commun — fil blanc	
11	NC	Relais normalement fermé	Relais de contact normaleme nt fermé — fil orange	
12	NO	Relais normalement ouvert	Relais de contact normalement ouvert — fil jaune	

Connexions Wiegand

- Insérez le fil noir dans la broche 1 (RTN).
- Insérez le fil blanc dans la broche 2 (D1).
- Insérez le fil vert dans la broche 3 (D0).

- Facultatif : insérez le fil vert dans la broche 4 (LED).



Connexions relais

- Insérez le fil blanc dans la broche 10 (COM).
- Insérez le fil orange dans la broche 11 (NC).
- Insérez le fil jaune dans la broche 12 (NO).

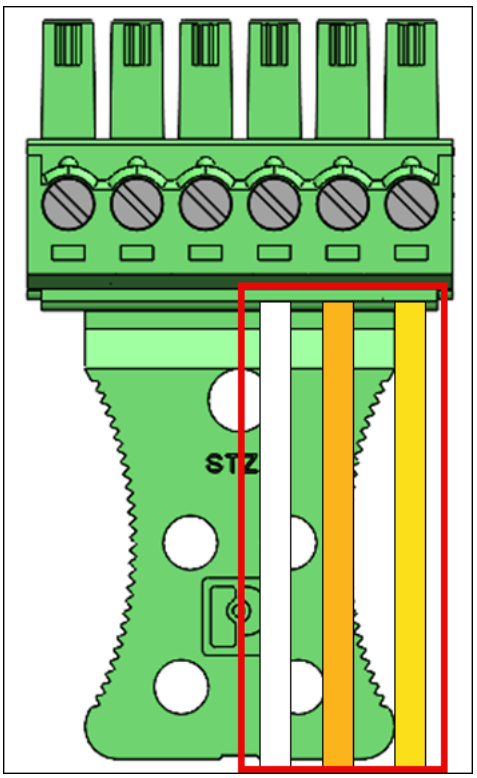
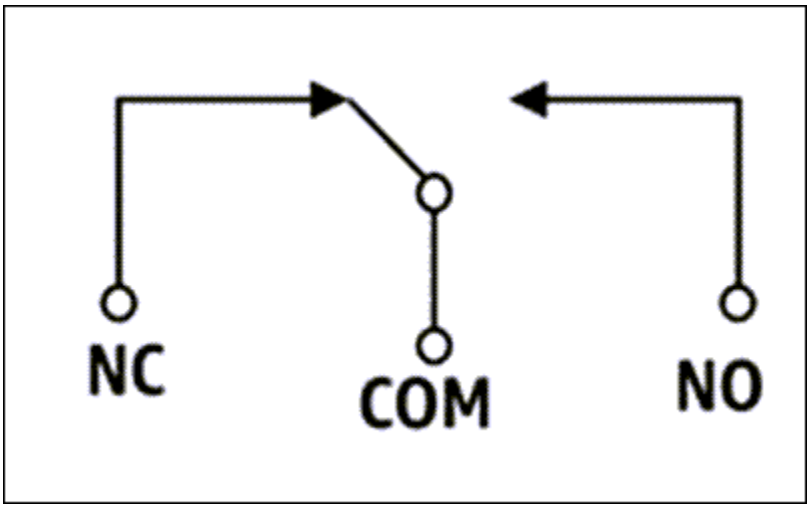


Schéma du relais

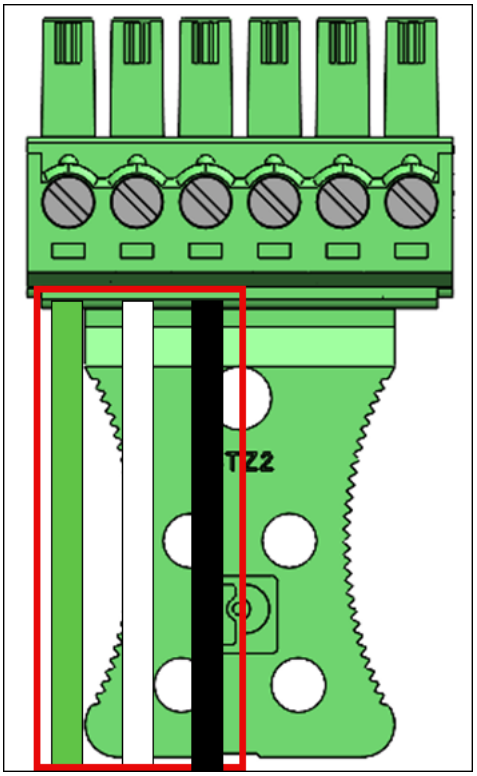


Le relais doit être utilisé conformément aux valeurs de sécurité spécifiées 30 VAC /60VDC, 60 W max.

RS485connexions

- Insérez le fil vert dans la broche 7 (B).
- Insérez le fil blanc dans la broche 8 (A).

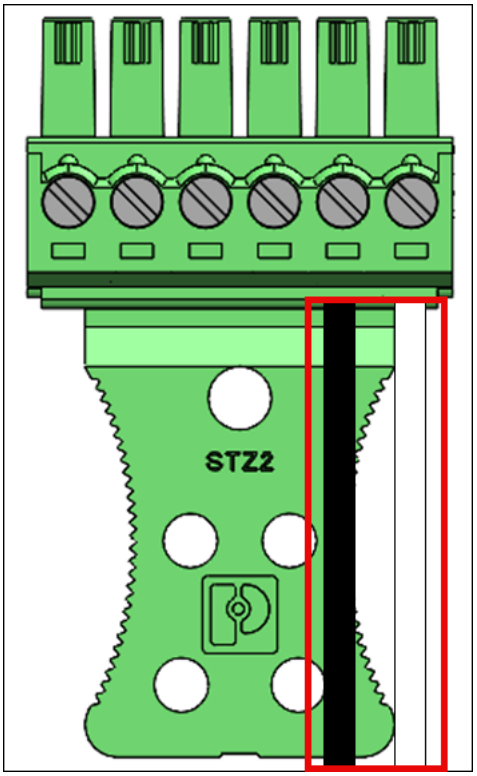
- Insérez le fil noir dans la broche 9 (RTN).



Activez le commutateur de RS485 terminaison sur « ON » si l'appareil est le dernier appareil sur la ligne. Ce commutateur active la terminaison de la résistance de 120 ohms sur la ligne.

Connexions d'entrée/sortie numériques

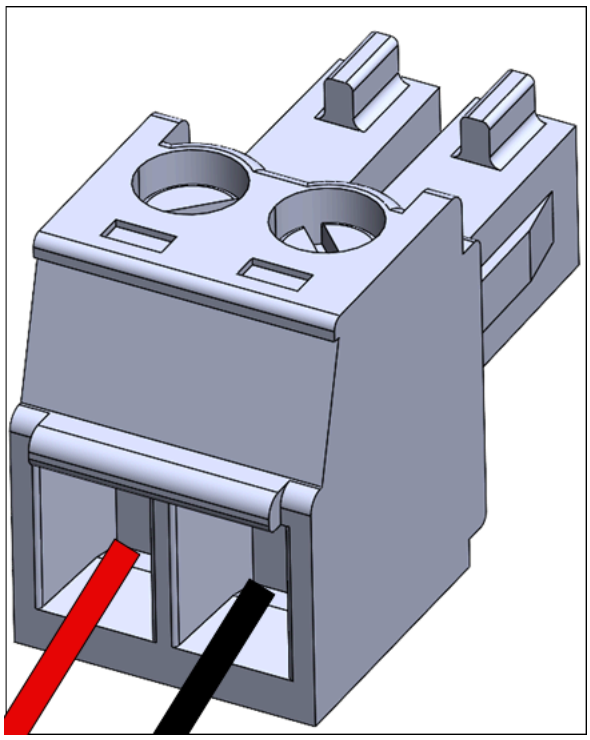
- Insérez le fil noir dans la broche 5 (GPI).
- Insérez le fil blanc dans la broche 6 (GPO).



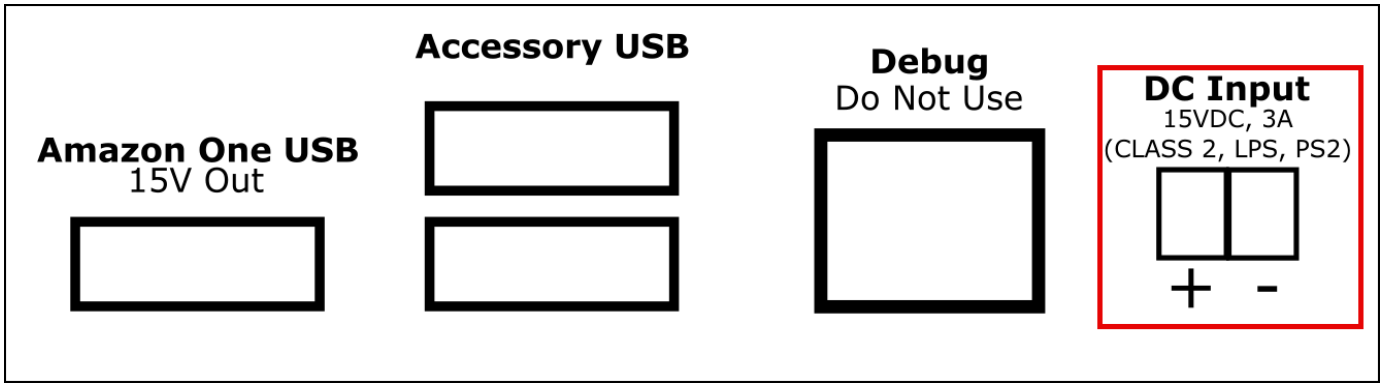
- Les connexions d'entrée/sortie numériques doivent être utilisées comme indiqué.

Facultatif : pour installer un câblage DC

1. Dénudez 3 mm à 5 mm de l'extrémité d'un fil rouge pour le positif (+) et d'un fil noir pour le négatif (-).
2. Insérez l'extrémité dénudée du fil DC dans la prise DC.



3. Vissez le fil en place.
4. Insérez la prise DC filaire dans le port d'entrée DC.



Activation d'un appareil Amazon One

Lorsque votre appareil Amazon One est installé et allumé, vous êtes prêt à l'activer.

Pour activer votre appareil Amazon One

1. Sur l'appareil Amazon One, appuyez sur l'écran pour commencer.
2. Choisissez Ethernet ou Wifi pour vous connecter à Internet.

   Dès que l'appareil est connecté à Internet, il commence à télécharger le dernier progiciel.

3. Lorsque l'écran indique que le téléchargement du logiciel est terminé ! , sélectionnez OK.
4. Sélectionnez le code QR.

   L'écran de l'appareil Amazon One affichera le code Scan QR.
5. Pour récupérer le code QR d'activation, ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.

   > **Note**
   >
   > Nous vous recommandons vivement d'accorder une autorisation limitée à vos installateurs afin qu'ils n'aient accès qu'aux codes QR d'activation de votre console Amazon One Enterprise. Consultez Étape 2 : ajouter des utilisateurs d'Amazon One Enterprise.
6. Dans le volet de navigation, sélectionnez Activation QR codes.
7. Dans la liste déroulante Sélectionnez un site, sélectionnez le site sur lequel l'appareil Amazon One est installé.
8. Sous Informations sur le site, confirmez l'adresse du site.
9. Sous Codes QR d'activation, recherchez le nom de l'instance de l'appareil que vous activez, puis sélectionnez le code Get QR correspondant pour récupérer le code QR.
10. Scannez le code QR avec l'appareil Amazon One.
11. Lorsque l'écran de l'appareil Amazon One indique que l'activation est terminée ! , l'appareil est prêt à être utilisé.

Inscription et entrée

Maintenant que votre appareil Amazon One est activé, vos employés peuvent commencer à inscrire leurs paumes et à authentifier leurs paumes pour y accéder.

Rubriques

- Inscription des utilisateurs
- Authentifiez-vous pour entrer

Inscription des utilisateurs

Avant que les utilisateurs puissent authentifier leurs paumes pour entrer, ils devront suivre le processus d'inscription. Le personnel de sécurité doit toujours vérifier l'identité de l'utilisateur avant de l'autoriser à s'inscrire.

Pour inscrire vos paumes sur un appareil Amazon One

1. Sur l'appareil d'inscription Amazon One Enterprise, appuyez sur Commencer.
2. Scannez un badge d'employé à l'aide du scanner de badges connecté à votre appareil d'inscription Amazon One Enterprise.

   Lorsque le badge est scanné avec succès, l'écran de l'appareil Amazon One affiche le badge scanné.
3. Lisez les conditions d'utilisation, puis appuyez sur OK.
4. Lisez Consentement : informations biométriques de votre paume, puis appuyez sur J'accepte si vous y consentez.
5. Suivez les instructions affichées à l'écran pour terminer le processus d'inscription.

Authentifiez-vous pour entrer

Une fois que vous avez inscrit votre Palm avec succès, vous êtes prêt à vous authentifier avec votre Palm sur votre appareil d'entrée Amazon One Enterprise.

Pour authentifier votre Palm lors de la saisie sur un appareil Amazon One

- Placez votre paume sur le dessus de l'appareil et suivez les instructions à l'écran pour scanner votre paume.

Gestion des utilisateurs inscrits

Vous pouvez utiliser la page de gestion des utilisateurs inscrits pour suivre les utilisateurs inscrits et supprimer leurs données biométriques. Un utilisateur dont les données biométriques associées sont supprimées n'aura plus accès aux appareils Amazon One pour s'authentifier.

Pour afficher les utilisateurs inscrits

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez Gestion des utilisateurs inscrits.
3. Sous Utilisateurs inscrits, vous trouverez tous les utilisateurs inscrits ainsi que les informations suivantes :

   - Identifiant du badge — Informations d'identification du badge capturées par un lecteur de RFID badge au moment de l'inscription.
   - Source d'inscription : détails de l'appareil Amazon One utilisé pour l'inscription.
   - Date d'inscription — Date et heure de l'inscription.

Pour supprimer les utilisateurs inscrits et leurs données biométriques

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez Gestion des utilisateurs inscrits.
3. Sous Utilisateurs inscrits, sélectionnez l'identifiant du badge de l'utilisateur dont vous souhaitez supprimer les données biométriques de la paume de la main.
4. Choisissez Supprimer les données biométriques.
5. Choisissez Supprimer pour confirmer la suppression des données biométriques de l'utilisateur.

> **Important**
>
> Cette action entraîne la suppression définitive de la biométrie palmaire d'un utilisateur d'Amazon One Enterprise. L'utilisateur devra se réinscrire avec un appareil d'inscription Amazon One Enterprise pour pouvoir utiliser Amazon One Enterprise à des fins d'authentification. La suppression des données biométriques d'un utilisateur entraîne également la suppression définitive d'autres attributs de profil, tels que l'identifiant du badge, d'Amazon One Enterprise.

Gestion des appareils

Une fois que votre appareil Amazon One est installé et activé, il commence à signaler l'état de santé de l'appareil sur la console Amazon One Enterprise. Vous pouvez utiliser la console Amazon One Enterprise pour effectuer des tâches de gestion des appareils, telles que le redémarrage des appareils ou la mise à jour des configurations.

Rubriques

Gestion du site

Un site représente un emplacement physique où un ensemble d'instances de périphériques sont installées et fonctionnent. Vous pouvez utiliser des sites pour organiser les appareils Amazon One partageant la même adresse physique.

Pour modifier le nom du site

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez Site.
3. Sous Sites, sélectionnez le site dont vous souhaitez modifier le nom.
4. Choisissez Modifier.
5. Dans Informations sur le site, entrez le nom et la description du site souhaités (facultatif).
6. Choisissez Enregistrer les modifications à mettre à jour.

Pour mettre à jour l'adresse du site

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez Site.
3. Sous Sites, sélectionnez le site dont vous souhaitez mettre à jour l'adresse.
4. Sous Instances de l'appareil, assurez-vous que le nombre d'instances activées est égal à 0.

5. (Facultatif) Si le nombre d'instances activées n'est pas égal à 0, voir Pour désactiver les instances du terminal
6. Choisissez Modifier.
7. Dans Adresse physique, entrez l'adresse physique correcte.
8. Choisissez Enregistrer les modifications à mettre à jour.

Gestion des instances de périphériques

Une instance de périphérique est une représentation logique d'un périphérique avec des configurations. L'utilisation d'instances d'appareils permet d'échanger des appareils Amazon One tout en héritant automatiquement des configurations et des noms définis précédemment. Une instance de périphérique possède un nom défini par l'utilisateur (convention de dénomination partagée avec votre logiciel de contrôle d'accès) et un ensemble de configurations de communication.

Pour afficher l'état de l'instance de l'appareil

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, choisissez Device instance.
3. Sous Instances activées, vous verrez la liste des appareils Amazon One activés.
4. Choisissez le nom d'une instance d'appareil pour afficher les détails de l'instance d'appareil.

Pour redémarrer un appareil Amazon One

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, choisissez Device instance.
3. Sous Instances activées, choisissez le nom de l'instance de l'appareil que vous souhaitez redémarrer.
4. Choisissez Redémarrer pour redémarrer l'appareil Amazon One.

Pour mettre à jour les configurations des appareils Amazon One

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.

2. Dans le volet de navigation, choisissez Device instance.
3. Sous Instances activées, choisissez le nom de l'instance de l'appareil que vous souhaitez mettre à jour.
4. Sous Configurations de l'appareil, choisissez Modifier.

> **Note**
>
> Pour modifier le mode d'appareil Amazon One, vous devez d'abord désactiver l'instance de terminal, puis la configurer avec le mode d'appareil souhaité (voir Étape 6 : Configuration d'une instance de terminal pour l'activation). Ensuite, vous pouvez suivre le processus d'activation de l'appareil (voir Activation d'un appareil Amazon One).

5. Après avoir apporté les modifications souhaitées, choisissez Mettre à jour les configurations de l'appareil pour confirmer la mise à jour.

Pour mettre à jour les informations d'identification Wi-Fi

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, choisissez Device instance.
3. Sous Instances activées, choisissez le nom de l'instance de l'appareil que vous souhaitez mettre à jour.
4. Sous Réseau, choisissez Modifier.
5. Sous Configurations Wi-Fi, apportez les modifications souhaitées.
6. Choisissez Mettre à jour le réseau pour confirmer la mise à jour.

Pour désactiver les instances du terminal

1. Ouvrez la console Amazon One Enterprise à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, choisissez Device instance.
3. Sous Instances activées, sélectionnez le nom de l'instance de terminal que vous souhaitez désactiver.
4. Choisissez Désactiver l'appareil.

5. Pour confirmer la désactivation, tapez « désactiver » dans la boîte de message et choisissez Désactiver l'appareil.

Sécurité dans Amazon One Enterprise

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon One Enterprise, consultez la section AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon One Enterprise. Les rubriques suivantes expliquent comment configurer Amazon One Enterprise pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon One Enterprise.

Rubriques

Protection des données dans Amazon One Enterprise

Le AWS modèle de responsabilité partagée modèle s'applique à la protection des données dans Amazon One Enterprise. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure

mondiale qui gère tous les AWS Cloud. Il vous incombe de garder le contrôle sur votre contenu hébergé sur cette infrastructure. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour Services AWS que tu utilises. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le AWS Modèle de responsabilité partagée et article de GDPR blog sur le AWS Blog sur la sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger Compte AWS informations d'identification et configuration des utilisateurs individuels avec AWS IAM Identity Center or AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et enregistrement de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation CloudTrail des sentiers pour capturer AWS activités, voir Travailler avec les CloudTrail sentiers dans le AWS CloudTrail Guide de l'utilisateur.
- Utiliser AWS solutions de chiffrement, ainsi que tous les contrôles de sécurité par défaut intégrés Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un FIPS point de terminaison. Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon One Enterprise ou un autre Services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Pour utiliser le chiffrement par défaut des données au repos

Amazon One Enterprise fournit un chiffrement par défaut pour protéger les données sensibles au repos à l'aide de clés de AWS chiffrement.

AWSclés détenues : Amazon One Enterprise utilise ces clés par défaut pour chiffrer automatiquement les données sensibles des utilisateurs finaux. Vous ne pouvez pas afficher, gérer ou utiliser les clés que vous AWS possédez, ni auditer leur utilisation. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez la section sur les clés AWS détenues dans le Guide du développeur du service de gestion des AWS clés.

Chiffrement des données en transit

Amazon One Enterprise utilise Transport Layer Security (TLS) pour sécuriser les données et Signature Version 4 pour authentifier toutes les API demandes entrantes adressées aux AWS services. Ce chiffrement est activé par défaut.

Gestion des identités et des accès pour Amazon One Enterprise

AWS Identity and Access Management (IAM) est un Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès à AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon One Enterprise. IAMest un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

Comment utilisez-vous AWS Identity and Access Management (IAM) diffère en fonction du travail que vous effectuez dans Amazon One Enterprise.

Utilisateur du service : si vous utilisez le service Amazon One Enterprise pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'Amazon One Enterprise pour effectuer votre travail, il se peut que vous ayez besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité d'Amazon One Enterprise, consultezRésolution des problèmes d'identité et d'accès à Amazon One Enterprise.

Administrateur du service — Si vous êtes responsable des ressources Amazon One Enterprise au sein de votre entreprise, vous avez probablement un accès complet à Amazon One Enterprise. C'est à vous de déterminer les fonctionnalités et les ressources d'Amazon One Enterprise auxquelles les utilisateurs de vos services doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM Amazon One Enterprise, consultezComment fonctionne Amazon One Enterprise avec IAM.

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Amazon One Enterprise. Pour consulter des exemples de politiques basées sur l'identité d'Amazon One Enterprise que vous pouvez utiliserIAM, consultez. Exemples de politiques basées sur l'identité pour Amazon One Enterprise

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS en utilisant vos informations d'identification. Vous devez être authentifié (connecté) à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant

qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez AWS en utilisant la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au AWS Management Console ou le AWS portail d'accès. Pour plus d'informations sur la connexion à AWS, voir Comment se connecter à votre Compte AWS dans le .Connexion à AWS Guide de l'utilisateur.

Si vous accédez AWS programmatiquement, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas AWS outils, vous devez signer les demandes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, voir Signature AWS APIdemandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez la section Authentification multifactorielle dans le AWS IAM Identity Center Guide de l'utilisateur et utilisation de l'authentification multifactorielle (MFA) dans AWS dans le guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion qui donne un accès complet à tous Services AWS et les ressources du compte. Cette identité s'appelle Compte AWS utilisateur root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, le AWS Directory Service, le répertoire Identity Center ou tout utilisateur accédant Services AWS en utilisant les informations d'identification fournies par le biais d'une source d'identité. Lorsque les identités fédérées accèdent Comptes AWS, ils assument des rôles, et les rôles fournissent des informations d'identification temporaires.

Pour une gestion centralisée des accès, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans tous vos Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le AWS IAM Identity Center Guide de l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans AWS Management Console en changeant de rôle. Vous pouvez assumer un rôle en appelant un AWS CLI or AWS APIopération ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les ensembles d'autorisations, voir Ensembles d'autorisations dans le AWS IAM Identity Center Guide de l'utilisateur.
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Cependant, avec certains Services AWS, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- Accès multiservices — Certains Services AWS utiliser des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) : lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions dans AWS, vous êtes considéré comme un directeur. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un

autre service. FASutilise les autorisations du principal appelant un Service AWS, combiné à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

- Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, voir Création d'un rôle pour déléguer des autorisations à un Service AWS dans le guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle lié à un service Service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui créent AWS CLI or AWS APIdemandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS pour attribuer un rôle à une EC2 instance et le mettre à la disposition de toutes ses applications, vous créez un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès dans AWS en créant des politiques et en les rattachant à AWS identités ou ressources. Une politique est un objet dans AWS qui, lorsqu'elle est associée à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu

des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSONpolitiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console, le AWS CLI, ou le AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent AWS politiques gérées et politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans

laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou Services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser AWS politiques gérées à partir IAM d'une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 AWS WAF, et Amazon VPC sont des exemples de services qui prennent en chargeACLs. Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.
- Politiques de contrôle des services (SCPs) : SCPs sont des JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service de regroupement et de gestion centralisée de plusieurs Comptes AWS que votre entreprise possède. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un

ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités figurant dans les comptes des membres, y compris chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et SCPs consultez les politiques de contrôle des services dans le AWS Organizations Guide de l'utilisateur.

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS détermine s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, voir la logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment fonctionne Amazon One Enterprise avec IAM

Avant de commencer IAM à gérer l'accès à Amazon One Enterprise, découvrez quelles IAM fonctionnalités peuvent être utilisées avec Amazon One Enterprise.

IAMfonctionnalités que vous pouvez utiliser avec Amazon One Enterprise

IAMfonctionnalité	Assistance Amazon One Enterprise
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui

IAMfonctionnalité	Assistance Amazon One Enterprise
ACLs	Non
ABAC(balises dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont Amazon One Enterprise et d'autres AWS les services fonctionnent avec la plupart IAM des fonctionnalités, voir AWS services compatibles avec IAM le Guide de l'IAMutilisateur.

Politiques basées sur l'identité pour Amazon One Enterprise

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour Amazon One Enterprise

Pour consulter des exemples de politiques basées sur l'identité d'Amazon One Enterprise, consultez. Exemples de politiques basées sur l'identité pour Amazon One Enterprise

Politiques basées sur les ressources au sein d'Amazon One Enterprise

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou Services AWS.

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, voir Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions politiques pour Amazon One Enterprise

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSONpolitiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions politiques portent généralement le même nom que les actions associées AWS APIopération. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions Amazon One Enterprise, consultezActions, ressources et clés de condition pour Amazon One Enterprise.

Les actions politiques dans Amazon One Enterprise utilisent le préfixe suivant avant l'action :

```
one
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "one:action1",
      "one:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "one:Describe*"
```

Pour consulter des exemples de politiques basées sur l'identité d'Amazon One Enterprise, consultez. Exemples de politiques basées sur l'identité pour Amazon One Enterprise

Ressources relatives aux politiques pour Amazon One Enterprise

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSONpolitiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Amazon One Enterprise et leurs caractéristiquesARNs, et pour savoir quelles actions vous pouvez utiliser pour spécifier chaque ressource, consultezActions, ressources et clés de condition pour Amazon One Enterprise. ARN

Pour consulter des exemples de politiques basées sur l'identité d'Amazon One Enterprise, consultez. Exemples de politiques basées sur l'identité pour Amazon One Enterprise

Clés de conditions de politique pour Amazon One Enterprise

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser AWS JSONpolitiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs `Condition` éléments dans une instruction ou plusieurs clés dans un seul `Condition` élément, AWS les évalue à l'aide d'une `AND` opération logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour tout voir AWS clés de condition globales, voir AWS clés contextuelles des conditions globales dans le guide de IAM l'utilisateur.

Pour consulter la liste des clés de condition Amazon One Enterprise et pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultezActions, ressources et clés de condition pour Amazon One Enterprise.

Pour consulter des exemples de politiques basées sur l'identité d'Amazon One Enterprise, consultez. Exemples de politiques basées sur l'identité pour Amazon One Enterprise

ACLsdans Amazon One Enterprise

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

ABACavec Amazon One Enterprise

Supports ABAC (balises dans les politiques) : Oui

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Entrée AWS, ces attributs sont appelés balises. Vous pouvez associer des tags à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation d'informations d'identification temporaires avec Amazon One Enterprise

Prend en charge les informations d'identification temporaires : oui

Momentanée Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris lesquelles Services AWS utilisez des informations d'identification temporaires, voir Services AWS qui fonctionnent avec IAM le Guide de l'IAMutilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez au AWS Management Console en utilisant n'importe quelle méthode, à l'exception du nom d'utilisateur et du mot de passe. Par exemple, lorsque vous accédez AWS à l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI or AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Amazon One Enterprise

Prend en charge les sessions d'accès direct (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions dans AWS, vous êtes considéré comme un directeur. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant un Service AWS, combiné à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour Amazon One Enterprise

Supporte les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus

d'informations, voir Création d'un rôle pour déléguer des autorisations à un Service AWS dans le guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités d'Amazon One Enterprise. Modifiez les rôles de service uniquement lorsque Amazon One Enterprise fournit des instructions à cet effet.

Rôles liés à un service pour Amazon One Enterprise

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un Service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service, voir AWS services qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Amazon One Enterprise

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon One Enterprise. Ils ne peuvent pas non plus effectuer de tâches à l'aide du AWS Management Console, AWS Command Line Interface (AWS CLI), ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par Amazon One Enterprise, y compris le format du ARNs pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour Amazon One Enterprise la référence d'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Amazon One Enterprise dans votre compte. Ces actions peuvent entraîner des coûts pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez les directives et recommandations suivantes :

- Commencez avec AWS politiques gérées et évolution vers des autorisations avec le moindre privilège — Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez AWS politiques gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant AWS des politiques gérées par le client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez .AWS politiques gérées ou AWS politiques gérées pour les fonctions professionnelles dans le guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un Service AWS, comme

AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.

- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger une authentification multifactorielle (MFA) — Si vous avez un scénario qui nécessite IAM des utilisateurs ou un utilisateur root dans votre Compte AWS, activez MFA pour plus de sécurité. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console Amazon One Enterprise

Pour accéder à la console Amazon One Enterprise, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon One Enterprise dans votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) dotées de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Amazon One Enterprise, joignez également la console Amazon One Enterprise `ConsoleAccess` ou `ReadOnly` AWS politique gérée pour les entités. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le Guide de IAM l'utilisateur.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès en lecture seule à Amazon One Enterprise

L'exemple suivant montre un AWS politique gérée, `AmazonOneEnterpriseReadOnlyAccess` qui accorde un accès en lecture seule à Amazon One Enterprise.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "one:Get*",
        "one:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Dans les déclarations de politique, l'élément `Effect` spécifie si les actions sont autorisées ou refusées. L'élément `Action` répertorie les actions spécifiques que l'utilisateur est autorisé à effectuer. L'`Resource`élément répertorie les AWS ressources sur lesquelles l'utilisateur est autorisé à effectuer ces actions. Pour les politiques qui contrôlent l'accès aux actions d'Amazon One Enterprise, l'`Resource`élément est toujours défini sur`*`, un caractère générique qui signifie « toutes les ressources ».

Les valeurs de l'`Action`élément correspondent à celles prises APIs en charge par les services. Les actions sont précédées `config:` d'une mention indiquant qu'elles font référence à des actions Amazon One Enterprise. Vous pouvez utiliser le caractère générique `*` dans l'élément `Action`, comme dans les exemples suivants :

- `"Action": ["one:*DeviceInstanceConfiguration"]`

  Cela autorise toutes les actions Amazon One Enterprise qui se terminent par DeviceInstance « » (`GetDeviceInstanceConfiguration`,`CreateDeviceInstanceConfiguration`).
- `"Action": ["one:*"]`

  Cela permet toutes les actions d'Amazon One Enterprise, mais pas les actions pour les autres AWS services.
- `"Action": ["*"]`

Cela permet à tous AWS actions. Cette autorisation convient à un utilisateur qui agit en tant que AWS administrateur de votre compte.

La politique de lecture seule n'accorde pas d'autorisation à l'utilisateur pour des actions telles que `CreateDeviceInstanceUpdateDeviceInstance`, et. `DeleteDeviceInstance` Les utilisateurs soumis à cette politique ne sont pas autorisés à créer une instance d'appareil, à mettre à jour une instance d'appareil ou à supprimer une instance d'appareil. Pour consulter la liste des actions Amazon One Enterprise, consultezActions, ressources et clés de condition pour Amazon One Enterprise.

Accès complet à Amazon One Enterprise

L'exemple suivant montre une politique qui accorde un accès complet à Amazon One Enterprise. Il accorde aux utilisateurs l'autorisation d'effectuer toutes les actions d'Amazon One Enterprise.

> **Important**
>
> Cette politique accorde des autorisations étendues. Avant d'accorder un accès complet, commencez avec un ensemble d'autorisations minimum et accordez-en d'autres si nécessaire. Cette méthode est plus sûre que de commencer avec des autorisations trop permissives et d'essayer de les restreindre plus tard.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "one:*"
            ],
            "Resource": "*"
        },
    ]
}
```

Autorisations au niveau des ressources prises en charge pour les actions de règles Amazon One Enterprise API

Les autorisations au niveau des ressources font référence à la possibilité de spécifier les ressources sur lesquelles les utilisateurs sont autorisés à exécuter des actions. Amazon One Enterprise prend en charge les autorisations au niveau des ressources pour certaines actions de règles API Amazon One Enterprise. Cela signifie que pour certaines actions relatives aux règles Amazon One Enterprise, vous pouvez contrôler les conditions dans lesquelles les utilisateurs sont autorisés à utiliser ces actions. Ces conditions peuvent être des actions qui doivent être réalisées, ou des ressources spécifiques que les utilisateurs sont autorisés à utiliser.

Le tableau suivant décrit les API actions des règles Amazon One Enterprise qui prennent actuellement en charge les autorisations au niveau des ressources. Il décrit également les ressources prises en charge et les ressources correspondantes ARNs pour chaque action. Lorsque vous spécifiez unARN, vous pouvez utiliser le caractère générique * dans vos chemins ; par exemple, lorsque vous ne pouvez pas ou ne voulez pas spécifier la ressource IDs exacte.

> **Important**
>
> Si une API action de règle Amazon One Enterprise n'est pas répertoriée dans ce tableau, cela signifie qu'elle ne prend pas en charge les autorisations au niveau des ressources. Si une action de règle Amazon One Enterprise ne prend pas en charge les autorisations au niveau des ressources, vous pouvez autoriser les utilisateurs à utiliser l'action, mais vous devez spécifier un * pour l'élément ressource de votre déclaration de politique.

APIAction	Ressources
CreateDeviceInstance	Instance de périphérique arn:aws:one :*region:accountID* :instance/*deviceInstanceId*
GetDeviceInstance	Instance de périphérique arn:aws:one :*region:accountID* :instance/*deviceInstanceId*
UpdateDeviceInstance	Instance de périphérique

APIAction	Ressources
	arn:aws:one :*region:accountID* :instance/*deviceInstanceId*
DeleteDeviceInstance	Instance de périphérique arn:aws:one :*region:accountID* :instance/*deviceInstanceId*
CreateDeviceActivationQrCode	Instance de périphérique arn:aws:one :*region:accountID* :instance/*deviceInstanceId*
DeleteAssociatedDevice	Instance de périphérique arn:aws:one :*region:accountID* :instance/*deviceInstanceId*
RebootDevice	Instance de périphérique arn:aws:one :*region:accountID* :instance/*deviceInstanceId*
CreateDeviceInstanceConfiguration	Configuration de l'instance de l'appareil arn:aws:one :*region:accountID* :instance/*deviceInstanceId* /configuration/*version*
GetDeviceInstanceConfiguration	Configuration de l'instance de l'appareil arn:aws:one :*region:accountID* :instance/*deviceInstanceId* /configuration/*version*
CreateSite	Site arn:aws:one :*region:accountID* :site/*siteId*

APIAction	Ressources
DeleteSite	Site arn:aws:one :*region:accountID* :site/*siteId*
GetSiteAddress	Site arn:aws:one :*region:accountID* :site/*siteId*
UpdateSite	Site arn:aws:one :*region:accountID* :site/*siteId*
UpdateSiteAddress	Site arn:aws:one :*region:accountID* :site/*siteId*
CreateDeviceConfigurationTemplate	Modèle de configuration de l'appareil arn:aws:one :*region:accountID* :device-configuration-template/*templateId*
DeleteDeviceConfigurationTemplate	Modèle de configuration de l'appareil arn:aws:one :*region:accountID* :device-configuration-template/*templateId*
GetDeviceConfigurationTemplate	Modèle de configuration de l'appareil arn:aws:one :*region:accountID* :device-configuration-template/*templateId*
UpdateDeviceConfigurationTemplate	Modèle de configuration de l'appareil arn:aws:one :*region:accountID* :device-configuration-template/*templateId*

Par exemple, vous voulez autoriser l'accès en lecture et refuser l'accès en écriture à des règles spécifiques à des utilisateurs spécifiques.

Dans la première politique, vous autorisez AWS Config des actions de lecture de règles, par exemple `GetSite` sur les règles spécifiées.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "one:GetSite",
                    "one:GetSiteAddress"
                ],
                "Resource": [
                    "arn:aws:one:region:accountID:site/siteId"
                ]
            }
        ]
    }
```

Dans la seconde politique, vous refusez les actions d'écriture de règles Amazon One Enterprise sur la règle spécifique.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "one:DeleteSite",
                "one:UpdateSiteAddress"
               ],
            "Resource": "arn:aws:one:region:accountID:site/siteId"
           }
      ]
   }
```

Avec les autorisations au niveau des ressources, vous pouvez autoriser l'accès en lecture et refuser l'accès en écriture pour effectuer des actions spécifiques sur les actions de règles API Amazon One Enterprise.

Informations supplémentaires

Pour en savoir plus sur la création d'IAMutilisateurs, de groupes, de politiques et d'autorisations, consultez les sections Création de votre premier groupe IAM d'utilisateurs et d'administrateurs et gestion des accès dans le guide de IAM l'utilisateur.

AWS politiques gérées pour Amazon One Enterprise

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d’utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou que de nouvelles API opérations sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques AWS gérées dans le Guide de IAM l'utilisateur.

AmazonOneEnterpriseFullAccess

Cette politique accorde des autorisations administratives qui permettent d'accéder à toutes les ressources et opérations d'Amazon One Enterprise.

`one:*`Vous permet d'effectuer toutes les actions d'Amazon One Enterprise.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "FullAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:*"
   ],
   "Resource": "*"
  }
 ]
}
```

AmazonOneEnterpriseReadOnlyAccess

Cette politique accorde des autorisations en lecture seule à toutes les ressources et opérations d'Amazon One Enterprise.

`one:Get*`Obtient les ressources Amazon One Enterprise.

`one:List*`Répertorie les ressources Amazon One Enterprise.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ReadOnlyAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:Get*",
    "one:List*"
   ],
   "Resource": "*"
  }
 ]
```

```
}
```

AmazonOneEnterpriseInstallerAccess

Cette politique accorde des autorisations de lecture et d'écriture limitées qui vous permettent de créer un code QR d'activation pour toute instance d'appareil configurée afin d'activer l'appareil sur n'importe quel site.

`one:CreateDeviceActivationQrCode`Vous permet de créer un code QR pour activer l'appareil.

`one:GetDeviceInstance`Permet de récupérer les informations relatives à une instance d'appareil Amazon One.

`one:GetSite`Permet de récupérer les informations relatives à un site Amazon One Enterprise.

`one:GetSiteAddress`Permet de récupérer l'adresse physique d'un site Amazon One Enterprise.

`one:ListDeviceInstances`Vous permet de répertorier les instances d'appareils Amazon One.

`one:ListSites`Vous permet de répertorier les sites Amazon One Enterprise.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstallerAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:CreateDeviceActivationQrCode",
    "one:GetDeviceInstance",
    "one:GetSite",
    "one:GetSiteAddress",
    "one:ListDeviceInstances",
    "one:ListSites"
   ],
   "Resource": "*"
  }
 ]
}
```

Amazon One Enterprise met à jour les politiques AWS gérées

Consultez les informations relatives aux mises à jour apportées aux politiques AWS gérées pour Amazon One Enterprise depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS flux sur la page d'historique des documents Amazon One Enterprise.

Modification	Description	Date
Amazon One Enterprise a commencé à suivre les modifications	Amazon One Enterprise a commencé à suivre les modifications apportées AWS à ses politiques gérées.	1er décembre 2023

Résolution des problèmes d'identité et d'accès à Amazon One Enterprise

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon One Enterprise etIAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Amazon One Enterprise
- Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes ressources Amazon One Enterprise

Je ne suis pas autorisé à effectuer une action dans Amazon One Enterprise

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit lorsque l'`mateojacksonIAM`utilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `one:`*`GetWidget`* autorisations fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 one:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `one:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes ressources Amazon One Enterprise

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon One Enterprise prend en charge ces fonctionnalités, consultezComment fonctionne Amazon One Enterprise avec IAM.
- Pour savoir comment fournir un accès à vos ressources sur Comptes AWS dont vous êtes le propriétaire, voir Fournir un accès à un IAM utilisateur dans un autre Compte AWS dont vous êtes propriétaire dans le guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, voir Fournir un accès à Comptes AWS appartenant à des tiers dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Actions, ressources et clés de condition pour Amazon One Enterprise

Amazon One Enterprise (préfixe de service :one) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans IAM les politiques d'autorisation.

Rubriques

- Actions définies par Amazon One Enterprise

- Types de ressources définis par Amazon One Enterprise
- Clés de condition pour Amazon One Enterprise

Actions définies par Amazon One Enterprise

Vous pouvez spécifier les actions suivantes dans l'`Action`élément d'une déclaration de IAM politique. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'APIopération ou à la CLI commande portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez spécifier un type ARN de ressource de ce type dans une instruction comportant cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément d'une IAM politique, vous devez inclure un modèle ARN ou pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeviceInstance	Accorder l'autorisation de créer une instance de terminal	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	Accorder l'autorisation d'obtenir des informations sur l'instance de l'appareil	Lecture	instance de dispositif*		
ListDeviceInstances	Accorder l'autorisation de répertorier les instances de l'appareil	Lecture			
UpdateDeviceInstance	Autoriser la mise à jour de l'instance de l'appareil	Écrire	instance de dispositif*		
DeleteDeviceInstance	Accorder l'autorisation de supprimer l'instance de l'appareil	Écrire	instance de dispositif*		
CreateDeviceActivationQrCode	Autoriser la création d'un code QR pour activer un appareil sur une instance de terminal	Écrire	instance de dispositif*		
DeleteAssociatedDevice	Accorder l'autorisation de supprimer l'association entre l'appareil et l'instance du périphérique	Écrire	instance de dispositif*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RebootDevice	Autoriser le redémarrage de l'appareil	Écrire	instance de dispositif*		
CreateDeviceInstanceConfiguration	Accorder l'autorisation de créer une configuration d'instance de périphérique	Écrire			
GetDeviceInstanceConfiguration	Accorder l'autorisation d'obtenir des informations sur la configuration de l'instance de l'appareil	Lecture	configuration*		
CreateSite	Accorder l'autorisation de créer un site	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	Accorder l'autorisation de supprimer l'instance de l'appareil	Écrire	sites*		
GetSite	Accorder l'autorisation d'obtenir des informations sur le site	Lecture	sites*		
ListSites	Accorder l'autorisation de répertorier des sites	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSiteAddress	Accorder l'autorisation d'obtenir des informations sur l'adresse du site	Lecture	sites*		
UpdateSite	Autoriser la mise à jour du site	Écrire	sites*		
UpdateSiteAddress	Autoriser la mise à jour de l'adresse du site	Écrire	sites*		
CreateDeviceConfigurationTemplate	Accorder l'autorisation de créer une instance de terminal	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	Accorder l'autorisation de supprimer le modèle de configuration de l'appareil	Écrire	device-configuration-template*		
GetDeviceConfigurationTemplate	Accorder l'autorisation d'obtenir des informations sur le modèle de configuration de l'appareil	Lecture	device-configuration-template*		
ListDeviceConfigurationTemplates	Accorder l'autorisation de répertorier les modèles de configuration des appareils	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDeviceConfigurationTemplate	Autoriser la mise à jour du modèle de configuration de l'appareil	Écrire	device-configuration-template*		
TagResource	Accorde l'autorisation de baliser une ressource	Identification	instance de périphérique, site, device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	instance de périphérique, site, device-configuration-template	aws:TagKeys	
ListTagForResources	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture			

Types de ressources définis par Amazon One Enterprise

Les types de ressources suivants sont définis par ce service et peuvent être utilisés dans l'`Resource`élément des déclarations de politique d'IAMautorisation. Chaque action du tableau

Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Device Instance	`arn:aws:one: region:accountID :device-instance/ deviceInstanceId`	aws:ResourceTag/${TagKey}
Device Instance Configuration	`arn:aws:one: region:accountID :device-instance/ deviceInstanceId /configuration/ version`	
Site	`arn:aws:one: region:accountID :site/siteId`	aws:ResourceTag/${TagKey}
Device Configuration Template	`arn:aws:one: region:accountID :device-configuration-template/ templateId`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon One Enterprise

Amazon One Enterprise définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une IAM politique. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez Clés de condition globales disponibles.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès par les identifications de la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès par les clés d'identification à partir de la demande	ArrayOfString

Validation de conformité pour Amazon One Enterprise

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne Services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.

- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Journalisation et surveillance d'Amazon One Enterprise

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon One Enterprise et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Amazon One Enterprise, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon EventBridge peut être utilisé pour automatiser vos AWS services et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.
- AWS CloudTrailcapture API les appels et les événements connexes effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Surveillance des événements Amazon One Enterprise sur Amazon EventBridge

Vous pouvez surveiller les événements Amazon One Enterprise dans EventBridge, qui fournit un flux de données en temps réel à partir de vos propres applications, applications software-as-a-service (SaaS) et AWS services. EventBridgeachemine ces données vers des cibles telles qu' AWS Lambda Amazon Simple Notification Service. Ces événements fournissent un flux d'événements système en temps quasi réel qui décrivent les modifications apportées aux AWS ressources.

Abonnez-vous aux événements Amazon One Enterprise

Les événements de modification du statut de l'appareil et du profil utilisateur Amazon One sont publiés à l'aide EventBridge de la EventBridge console et peuvent être activés dans celle-ci en créant une nouvelle règle. Bien que les événements ne soient pas classés, ils ont un horodatage qui vous permet de consommer les données. Les événements sont générés dans la mesure du possible.

Pour vous abonner aux événements Amazon One Enterprise

1. Ouvrez la EventBridge console à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, sous Bus, sélectionnez Rules.
3. Choisissez Créer une règle.
4. Sur la page détaillée de la règle par défaut, attribuez un nom à la règle, choisissez Règle avec un modèle d'événement, puis cliquez sur Suivant.
5. Sur la page Créer un modèle d'événement, sous Source de l'événement, vérifiez que AWS les événements ou les événements EventBridge partenaires sont sélectionnés.
6. Sous Exemple de type d'événement, choisissez Enter my own.
7. Copiez et collez depuis l'un desExemples d'événements.
8. Pour Méthode de création, choisissez Motif personnalisé. Dans la section Modèle d'événement, ajoutez un JSON avec la source de l'événement **`aws:one`** et le type de détail requis, puis choisissez Next.
9. Sur la page Sélectionner une ou plusieurs cibles, sélectionnez une cible de votre choix, qui inclut une fonction Lambda, une SQS file d'attente ou SNS un sujet. Pour plus d'informations sur la configuration des cibles, consultez la section Amazon EventBridge Targets.
10. Vous pouvez éventuellement configurer des balises.
11. Sur la page Vérifier et créer, choisissez Créer une règle. Pour plus d'informations sur la configuration des règles, consultez EventBridgeles règles du Guide de EventBridge l'utilisateur.

Types d'événements de modification de l'état de l'appareil

Les événements de changement d'état de l'appareil sont générés dansJSON. Pour chaque type d'événement, un JSON blob est envoyé à la cible de votre choix, comme configuré dans la règle. Les types de détails suivants sont disponibles :

L'état de santé de l'appareil est passé à Healthy

L'appareil a passé tous les tests de santé.

État de santé de l'appareil devenu critique

L'appareil a échoué à un ou plusieurs tests de santé.

La connectivité de l'appareil est passée en mode hors ligne

L'appareil n'est pas connecté à Internet.

La connectivité des appareils est passée en ligne

L'appareil est connecté à Internet.

resources

Contient la liste des deviceInstance ARN pour lesquels l'événement Device Status Change a été publié.

métadonnées

siteName

- Nom du site où le deviceInstance est présent.

siteArn

- Arn pour le site où le deviceInstance est présent.

data

currentConnectivity

- Indique s'il deviceInstance est connecté ou déconnecté d'Internet.
- Valeurs possibles :CONNECTED, DISCONNECTED

previousConnectivity

- Indique s'il deviceInstance était connecté ou déconnecté d'Internet avant l'événement.
- Valeurs possibles :CONNECTED, DISCONNECTED

currentHealthStatus

- Indique s'il deviceInstance a réussi tous les tests de santé.
- Valeurs possibles :HEALTHY, CRITICAL

previousHealthStatus

- Indique s'ils deviceInstance ont réussi tous les tests de santé lors de leur dernière vérification.
- Valeurs possibles :HEALTHY, CRITICAL

assetTagId

- Le assetTagId de l'appareil associé audeviceInstance.

deviceInstanceName

- Nom du deviceInstance pour lequel l'événement Device Status a été publié.

Types d'événements du profil utilisateur

Les types de détails des événements liés au profil utilisateur sont les suivants :

Nouvelle inscription réussie

Lorsqu'un utilisateur s'est inscrit avec succès.

Nouvelle désinscription réussie

Lorsqu'un utilisateur s'est désinscrit avec succès.

Inscription infructueuse

Lorsqu'un utilisateur ne parvient pas à s'inscrire.

Désinscription infructueuse

Lorsqu'un utilisateur ne parvient pas à se désinscrire.

Reconnaissance réussie

Lorsqu'un utilisateur scanne Palm pour s'authentifier avec succès.

Reconnaissance infructueuse

Lorsque la reconnaissance d'un scan de la paume a échoué.

resources

Contient la liste des ARN de profil utilisateur pour lesquels l'événement de profil utilisateur a été publié.

data

accountId

- Le AWS compte correspondant à l'appareil à l'origine de la demande.

requestSource

- Il s'agit deviceInstanceId de l'appareil à l'origine de la demande.

createdTimestamp

- Heure de création de l'événement.

userStatus

- État actuel de l'utilisateur.
- Valeurs possibles :ACTIVE, DELETED

associatedId

- L'identifiant associé de l'utilisateur, par exemple l'identifiant du badge.

raison

- Cette valeur s'affichera en cas d'échec des événements. Il contient la raison pour laquelle l'événement a échoué.

Exemples d'événements

Les exemples suivants présentent des événements pour Amazon One Enterprise.

Rubriques

L'état de santé de l'appareil est passé à sain

L'état de santé de l'appareil a été rétabli et l'état de santé de l'instance de l'appareil est passé de l'état HEALTHY de CRITICAL santé à l'état de santé.


```
{
    "version": "0",
    "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
```

```
    "detail-type": "Device Health Status Changed To Healthy",
    "source": "aws.one",
    "account": "123456789012",
    "time": "2022-10-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
    "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "HEALTHY",
      "previousHealthStatus": "CRITICAL",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

L'état de santé de l'appareil est devenu critique

L'appareil a échoué à un ou plusieurs tests de santé et l'état de santé de l'instance de l'appareil est passé à CRITICAL deHEALTHY.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Health Status Changed To Critical",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "CRITICAL",
```

```
      "previousHealthStatus": "HEALTHY",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

La connectivité des appareils est passée en ligne

L'appareil est connecté à Internet et l'état de connectivité de l'instance de l'appareil est passé à CONNECTED deDISCONNECTED.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Online",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "CONNECTED",
      "previousConnectivity": "DISCONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

La connectivité de l'appareil est passée en mode hors ligne

L'appareil n'est pas connecté à Internet et l'état de connectivité de l'instance de l'appareil est passé à DISCONNECTED deCONNECTED.

```
{
```

```
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Offline",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "DISCONNECTED",
      "previousConnectivity": "CONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

Nouvelle inscription réussie

Un événement lorsqu'un utilisateur s'est inscrit avec succès.

```
{
    "version": "0",
    "id": "aebc9c86-f20e-75db-caaa-63bf14926f59",
    "detail-type": "New Successful Enrollment",
    "source": "aws.one",
    "account": "679792848029",
    "time": "2023-11-22T02:55:17Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:one:us-east-1:679792848029:user"
    ],
    "detail": {
        "version": "1.0.0",
        "data": {
            "accountId": "679792848029",
            "enrollmentSource": "QfUuUnFqs5accJ",
```

```
            "createdTimestamp": "2023-11-22T02:55:17Z",
            "userStatus": "ACTIVE",
            "associatedIds": "[{\"associatedIdType\":\"badge\",\"associatedIdValue\":
\"1111358294500\"}]",
        }
    }
}
```


Enregistrement des API appels Amazon One Enterprise à l'aide de AWS CloudTrail

Amazon One Enterprise est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon One Enterprise. CloudTrail capture tous les API appels pour Amazon One Enterprise sous forme d'événements. Les appels capturés incluent des appels provenant de la console Amazon One Enterprise et des appels de code destinés aux API opérations d'Amazon One Enterprise. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon One Enterprise. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon One Enterprise, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur Amazon One Enterprise dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité a lieu dans Amazon One Enterprise, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements survenus dans votre environnement Compte AWS, y compris des événements relatifs à Amazon One Enterprise, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal

enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des SNS notifications Amazon pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions d'Amazon One Enterprise sont enregistrées CloudTrail et documentées dans leActions, ressources et clés de condition pour Amazon One Enterprise. Par exemple, les appels au `ListSites` `RebootDevice` et les `DeleteDeviceInstance` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'CloudTrail userIdentityélément.

Comprendre les entrées du fichier journal Amazon One Enterprise

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateSite`action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAKDBGOAT6C2EXAMPLE:J_DOE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_DOE",
        "accountId": "123456789012",
        "accessKeyId": "AKIALAVPULGA71EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAKDBGOAT6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-11T06:28:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-11T07:19:09Z",
    "eventSource": "one.amazonaws.com",
    "eventName": "CreateSite",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "name": "***",
        "description": "***",
        "address": {
            "addressLine1": "***",
            "addressLine2": "***",
            "addressLine3": "***",
            "city": "EXAMPLE_CITY",
            "postalCode": "12345",
            "countryCode": "EXAMPLE_COUNTRY",
            "stateOrRegion": "EXAMPLE_STATE"
        },
        "clientToken": "abc12d34-567e-8910-1112-12fghi0jk13l"
```

```
    },
    "responseElements": {
        "stateOrRegion": "EXAMPLE_STATE",
        "createdAtInMillis": 1697008749263,
        "city": "EXAMPLE_CITY",
        "countryCode": "EXAMPLE_COUNTRY",
        "deviceInstanceCount": 0,
        "postalCode": "12345",
        "name": "***",
        "description": "***",
        "siteId": " abCdefG12hijkL",
        "siteArn": "arn:aws:one:us-east-1:123456789012:site/abCdefG12hijkL",
        "tags": "***"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Historique du document pour le guide de l'utilisateur d'Amazon One Enterprise

Le tableau suivant décrit les versions de documentation pour Amazon One Enterprise.

Modification	Description	Date
Mettre à jour	Nouveau sujet ajouté : Installation du hub d'E/S pour appareils Amazon One pour un accès sécurisé Guide de l'utilisateur Amazon One Enterprise	14 août 2024
Mettre à jour	Nouveau sujet ajouté : Installation d'un appareil Amazon One à montage mural Guide de l'utilisateur Amazon One Enterprise	5 juin 2024
Première version	Publication initiale du guide de l'utilisateur d'Amazon One Enterprise	27 novembre 2023

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.