aws

Guide de l’utilisateur

Amazon One

Amazon One: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon One Enterprise ? 1
Appareil Amazon One 1
Console Amazon One Enterprise 2
Achat d'appareils Amazon One 3
Tarification d'Amazon One Enterprise 3
Comment fonctionne Amazon One 4
Flux de travail Amazon One 4
Termes clés d'Amazon One 5
Configuration de la console Amazon One 6
S'inscrire à un compte AWS 6
Création d'un utilisateur doté d'un accès administratif 7
Sécurisation de votre compte AWS 7
Création d'un utilisateur doté d'un accès administratif 7
Se connecter en tant qu'administrateur 8
Attribuer l'accès à des utilisateurs supplémentaires 8
Ajouter des utilisateurs d'Amazon One 9
Création d'un site 11
Création d'instances d'appareils 12
Création d'un modèle de configuration 13
Configuration d'une instance de terminal pour l'activation 14
Installation et activation d'Amazon One 16
Comprendre les exigences 16
Normes prises en charge 16
Exigences relatives au réseau 17
Exigence de puissance 17
Comprendre les concepts d'installation 17
Installation d'Amazon One Pedestal 18
Installation de l'appareil Amazon One à montage mural 20
Installation du hub d'E/S pour appareils Amazon One pour un accès sécurisé 31
Activation de l'appareil Amazon One 42
Inscription et saisie d'utilisateurs 44
Création d'une politique de point de terminaison 44
Authentification pour la saisie 44
Gestion des utilisateurs 46

Afficher les utilisateurs inscrits 46
Supprimer les utilisateurs inscrits et leurs données biométriques 46
Gestion des appareils Amazon One 48
Entretien et nettoyage des appareils Amazon One 48
Pour nettoyer l'appareil Amazon One 49
Gestion du site 49
Modification du nom du site 50
Mettre à jour l'adresse du site 50
Gestion des instances de périphériques 50
Affichage de l'état de l'instance du terminal 51
Redémarrage d'un appareil Amazon One 51
Mettre à jour les configurations des appareils Amazon One 52
Mise à jour des identifiants Wi-Fi 52
Désactivation des instances de terminal 53
Sécurité 54
Protection des données 54
Pour utiliser le chiffrement par défaut des données au repos 56
Chiffrement des données en transit 56
Gestion des identités et des accès 56
Public ciblé 57
Authentification par des identités 57
Gestion des accès à l'aide de politiques 61
Comment Amazon One Enterprise fonctionne avec IAM 64
Exemples de politiques basées sur l'identité 72
AWS politiques gérées 81
Actions, ressources et clés de condition 84
Actions 85
Types de ressources 89
Clés de condition 90
Validation de conformité 91
Surveillance 93
Surveillance des événements 93
Abonnez-vous aux événements Amazon One Enterprise 93
Types d'événements de modification de l'état de l'appareil 95
Types d'événements du profil utilisateur 96
Exemples d'événements 98

L'état de santé de l'appareil est passé à sain 98
L'état de santé de l'appareil est passé à critique 99
La connectivité de l'appareil est passée en ligne 99
La connectivité de l'appareil est passée en mode hors ligne 100
CloudTrail journaux 101
Informations sur Amazon One Enterprise dans CloudTrail 101
Comprendre les entrées du fichier journal Amazon One Enterprise 102
Résolution des problèmes 105
Résolution des problèmes d'identité et d'accès avec 105
Je ne suis pas autorisé à effectuer une action dans Amazon One 105
Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources Amazon One 106
Résolution des problèmes liés à la console Amazon One 106
Je ne parviens pas à créer un site 107
Je ne parviens pas à créer une instance de périphérique 107
Je ne parviens pas à créer un modèle de configuration 107
Je ne parviens pas à créer un code QR d'activation 107
Résolution des problèmes liés à l'appareil Amazon One 107
écran blanc 108
Je ne parviens pas à me connecter au Wi-Fi ou au réseau 109
Redémarrer un appareil avec des alertes actives 109
Erreur du système 109
Le code QR n'est pas reconnu 110
Impossible de lire le code QR 110
Plusieurs codes QR détectés 110
L'instance de périphérique n'existe pas 110
Site non trouvé 111
Le code postal ne correspond pas 111
Le délai de la passerelle a expiré 111
Je ne parviens pas à configurer l'appareil 111
L'appareil a redémarré avec un message d'erreur et un code d'erreur 112
Logo Amazon sur l'écran de l'appareil sans autre activité 112
Temporairement indisponible 112
Quelque chose s'est mal passé de notre côté 112
Temporairement hors service 113
L'appareil Amazon One présente des dommages physiques 113

Impossible de lire la paume 113
Palm non reconnue 113
Appareil verrouillé en raison d'une inactivité prolongée 114
Appareil verrouillé en raison d'un acte d'altération 114
Historique de la documentation 116
..... cxviii

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
- Console Amazon One Enterprise
- Achat d'appareils Amazon One
- Tarification d'Amazon One Enterprise

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 5 GHz), Ethernet, 2 ports USB de type A, 1 port 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, entrée 110/220 VAC, adaptateur AC/DC 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

Amazon One est un service biométrique basé sur le cloud qui utilise un appareil Amazon One pour authentifier un utilisateur à l'aide de la biométrie palmaire. Vous pouvez commander des appareils Amazon One en nous contactant.

Après avoir installé l'appareil Amazon One, vous pouvez activer et enregistrer vos appareils avec votre compte AWS sur la console Amazon One et dans l'application d'authentification. Vous pouvez consulter les profils biométriques des utilisateurs inscrits. Si nécessaire, vous pouvez annuler leur inscription et supprimer leurs données biométriques.

La console Amazon One sert de plateforme centralisée pour la gestion des activités opérationnelles, telles que le suivi des appareils et l'affichage des factures mensuelles. Les utilisateurs peuvent s'inscrire en scannant leurs paumes dans les stations d'inscription supervisées sur place. Une fois inscrits, les utilisateurs peuvent facilement entrer ou sortir des emplacements sécurisés en passant leur paume sur un appareil compatible Amazon One.

Rubriques

- Flux de travail Amazon One
- Termes clés d'Amazon One

Flux de travail Amazon One

Ce qui suit décrit le flux de travail de base d'Amazon One :

1. Achetez et installez les appareils Amazon One en nous contactant.
2. Après avoir installé l'appareil, activez Amazon One.
3. Connectez-vous à votre compte Amazon One.
4. Configurez les dispositifs d'inscription et de saisie des utilisateurs.
5. Inscrivez les paumes des employés.
6. Utilisez les fonctionnalités de gestion et de surveillance pour garantir l'intégrité des appareils, maintenir les configurations à jour et suivre les inscriptions des utilisateurs pour une surveillance complète.

Termes clés d'Amazon One

Voici les principaux termes relatifs à Amazon One :

- Site : le client gérait les bâtiments physiques dans lesquels il installe les appareils Amazon One. Un site doit répondre aux exigences d'installation, de réseau et d'alimentation de vos appareils Amazon One.
- Appareil : appareil biométrique Amazon One à scanner la paume de la main pour l'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.

Configuration de la console Amazon One

Ce chapitre explique les étapes de base pour démarrer avec la console Amazon One.

Configuration d'un site, d'instances d'appareils et de modèles de configuration : suivez ces étapes pour créer une structure permettant d'ajouter un emplacement physique pour héberger vos appareils Amazon One, puis pour les configurer et les gérer à l'aide de la console Amazon One Enterprise. Vous n'utiliserez ce processus qu'occasionnellement, voire une seule fois, en fonction du nombre de sites, d'instances d'appareils et de vos modèles de configuration.

Rubriques

- S'inscrire à un compte AWS
- Création d'un utilisateur doté d'un accès administratif
- Ajouter des utilisateurs d'Amazon One
- Création d'un site
- Création d'instances d'appareils
- Création d'un modèle de configuration
- Configuration d'une instance de terminal pour l'activation

S'inscrire à un compte AWS

Si vous n'avez pas de compte AWS, complétez les étapes suivantes pour en créer un.

Pour s'inscrire à un compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
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 pour un compte AWS, un utilisateur root du compte AWS est créé. L'utilisateur root a accès à tous les services et ressources AWS du compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root

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

Création d’un utilisateur doté d’un accès administratif

Après avoir créé un compte AWS, sécurisez l'utilisateur root de votre compte AWS, activez AWS IAM Identity Center et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Rubriques

- Sécurisation de votre compte AWS
- Création d'un utilisateur doté d'un accès administratif
- Se connecter en tant qu'administrateur
- Attribuer l'accès à des utilisateurs supplémentaires

Sécurisation de votre compte AWS

Maintenant que vous êtes connecté à votre compte Amazon One, sécurisez votre compte.

Pour sécuriser l'utilisateur root de votre compte AWS

1. Connectez-vous à l'AWS Management Console en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant l'adresse e-mail de votre compte AWS.
2. 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 Se connecter en tant qu'utilisateur root dans le guide de l'utilisateur AWS Sign-In.
3. Activez l’authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activation d'un dispositif MFA virtuel pour l'utilisateur root de votre compte AWS (console) dans le Guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

Maintenant que vous avez sécurisé votre compte Amazon One, créez un utilisateur doté d'un accès administratif.

Pour créer un utilisateur doté d’un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez la section Activation d'AWS IAM Identity Center dans le guide de l'utilisateur d'AWS IAM Identity Center.

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du répertoire IAM Identity Center comme source d'identité, consultez Configurer l'accès utilisateur avec le répertoire IAM Identity Center par défaut dans le guide de l'utilisateur d'AWS IAM Identity Center.

Se connecter en tant qu'administrateur

Maintenant que vous avez créé un utilisateur doté d'un accès administratif, connectez-vous en tant qu'administrateur.

Pour vous connecter en tant qu'utilisateur disposant d'un accès administratif

- Connectez-vous avec votre utilisateur IAM Identity Center, en utilisant l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

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

Attribuer l'accès à des utilisateurs supplémentaires

Maintenant que vous êtes connecté en tant qu'administrateur, vous pouvez attribuer l'accès à d'autres utilisateurs.

Pour attribuer l'accès à des utilisateurs supplémentaires

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

  Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de l'utilisateur d'AWS IAM Identity Center.

Ajouter des utilisateurs d'Amazon One

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 uniquement pour récupérer les codes QR d'activation des appareils Amazon One.

Pour ajouter un utilisateur Amazon One

1. Suivez la procédure de connexion adaptée à votre type d'utilisateur, comme décrit dans la section Comment se connecter AWS dans le guide de l'Connexion à AWS 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 son nom de connexion pour AWS.

   > **Note**
   >
   > Le nombre et la taille des ressources IAM dans un Compte AWS sont limités. Pour plus d'informations, consultez les rubriques Quotas IAM et AWS STS. 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 TESTUSER et testuser. Lorsqu'un nom d'utilisateur est utilisé dans une politique ou dans le cadre d'un ARN, il est sensible à la casse. 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 utilisateur IAM.
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 — Le mot de passe que vous entrez dans le champ est attribué à l'utilisateur.

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 une politique AWS gérée nommée `IAMUserChangePassword` aux 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 de balises dans IAM, consultez Balisage des ressources IAM.
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
    - URL de 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.

Création d'un site

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

> **Important**
>
> Amazon One 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 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.

Création d'instances d'appareils

Maintenant que vous avez créé un site dans l'AWS Management Console, vous pouvez utiliser la console Amazon One pour créer des instances d'appareils.

Pour créer une instance de terminal

1. Ouvrez la console Amazon One à l'adresse https://console.aws.amazon.com/one-enterprise.
2. Dans le volet de navigation, sélectionnez les instances de l'appareil. 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.

Création d'un modèle de configuration

Maintenant que vous avez créé des instances d'appareils, vous pouvez utiliser la console Amazon One pour créer un modèle de configuration.

Pour créer un modèle de configuration

1. Ouvrez la console Amazon One 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 pour un accès sécurisé.

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 (voirCréation 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 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, voirCréation 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 pour un accès sécurisé.

Installation et activation d'Amazon One

Après avoir correctement configuré votre console Amazon One, les étapes suivantes consistent à installer les appareils Amazon One sur votre site et à vous assurer qu'ils sont correctement activés. Ce processus consiste à placer physiquement les appareils dans des zones désignées, à les connecter à votre réseau et à terminer le processus d'activation pour permettre une identification fluide des utilisateurs et des fonctionnalités de transaction. Une fois activés, vos appareils Amazon One seront prêts à offrir une expérience sécurisée et sans contact à vos clients ou à vos employés.

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

Rubriques

- Comprendre les exigences
- Comprendre les concepts d'installation
- Installation d'Amazon One Pedestal
- Installation de l'appareil Amazon One à montage mural
- Installation du hub d'E/S pour appareils Amazon One pour un accès sécurisé
- Activation de l'appareil Amazon One

Comprendre les exigences

Un appareil Amazon One peut être installé dans n'importe quel lieu d'entreprise ou d'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.

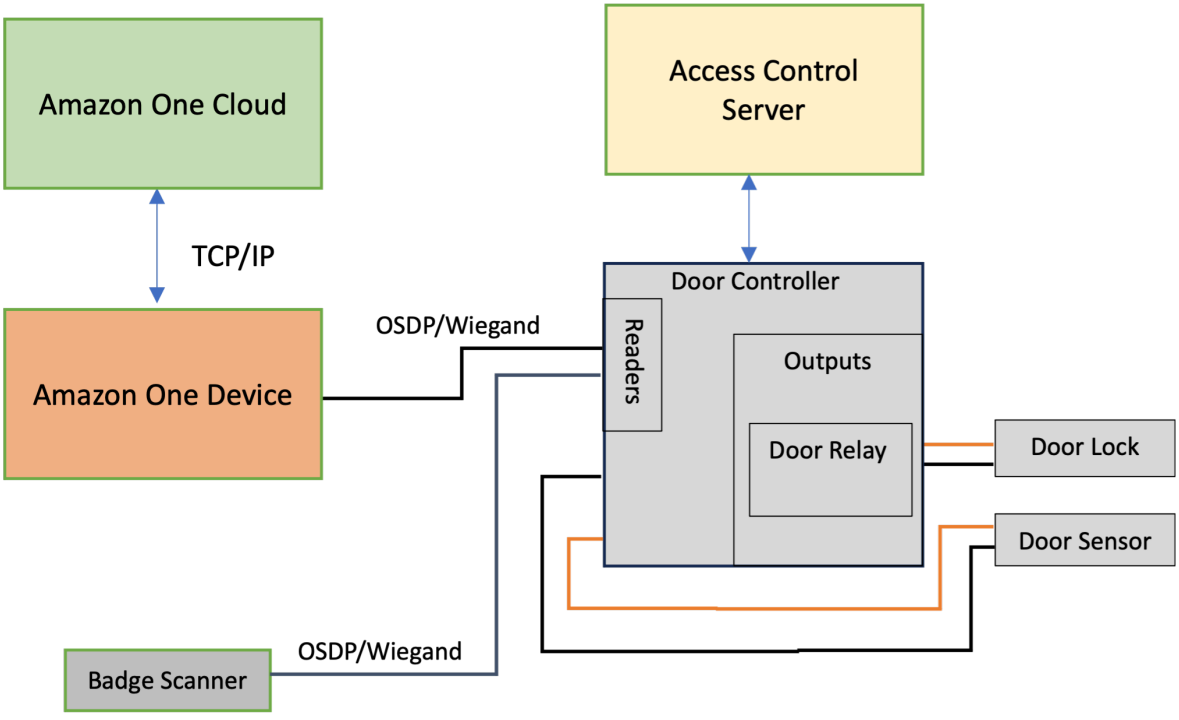
Exigence de puissance

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 au bâtiment, Amazon One 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 enregistrés 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 du contrôleur de porte via une interface OSDP.
  - Si une interface Wiegand est nécessaire, un OSDP-to-Wiegand convertisseur COTS peut être utilisé.
  - Une fois l'authentification réussie, l'appareil Amazon One envoie l'identifiant du badge de l'utilisateur au contrôleur de porte.
  - 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 des badges RFID et envoyer le numéro du badge au serveur de contrôle d'accès. Avec Amazon One, un scanner de badges se connecte à l'appareil Amazon One, permettant aux utilisateurs de scanner leurs badges, ce qui les associe à leur profil Palm.

Installation d'Amazon One Pedestal

Le socle Amazon One est un élément clé du système d'identification et de transaction Amazon One, conçu pour offrir une expérience fluide et sans contact aux utilisateurs. Cet appareil est doté d'une authentification biométrique sécurisée. Vous pouvez l'intégrer à différents sites pour fournir un accès ou des solutions de paiement fluides.

Cette section fournit les exigences en matière de localisation et step-by-step les instructions d'installation d'Amazon One Pedestal. Une préparation et une installation appropriées sont essentielles pour garantir que le système fonctionne de manière sûre et efficace, offrant aux utilisateurs une expérience fluide et fiable.

Conditions préalables et préparation à l'installation de l'Amazon One Pedestal

Avant de commencer l'installation, assurez-vous que les conditions suivantes sont remplies pour une configuration sûre, sécurisée et efficace :

- Exigences en matière d'alimentation : si vous utilisez le POE+ (Power over Ethernet) pour alimenter le périphérique, vérifiez que le câblage Cat6 est déjà installé et qu'un injecteur ou un commutateur POE+ est disponible pour utilisation. Sinon, si une alimentation en courant alternatif (120 V) est utilisée, assurez-vous qu'une prise secteur accessible est située à moins de 20 pieds du socle.
- Configuration physique : Le sol doit être plat, propre et exempt de tout débris pour garantir une installation stable et sûre du socle.

- Emplacement du piédestal : installez le socle dans un endroit où il ne bloquera pas les portes, les voies ou les points d'accès, ce qui permettra de vous déplacer facilement dans la zone.
- Gestion des câbles : acheminez et fixez tous les câbles excédentaires à l'intérieur du socle pour éviter tout encombrement et tout dommage potentiel lors d'une utilisation normale.

Une fois ces prérequis confirmés, vous pouvez poursuivre le processus d'installation.

Pour installer Amazon One Pedestal

1. Retirez le socle Amazon One de son emballage.
2. Retirez la porte en dévissant les deux vis inviolables M4.
3. Branchez le câble d'alimentation.
4. Faites passer le câble dans le trou de la plaque de base du socle.
5. Enroulez tout câble d'alimentation excédentaire à l'intérieur du socle.
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.

Après avoir installé votre appareil Amazon One, vous êtes prêt à l'activer.

Installation de l'appareil Amazon One à montage mural

L'appareil mural Amazon One est un système d'identification biométrique compact et polyvalent conçu pour offrir une expérience fluide et sans contact aux utilisateurs dans divers environnements. Il utilise une technologie avancée de reconnaissance des paumes pour un accès ou un paiement sécurisés, ce qui le rend idéal pour les lieux très fréquentés tels que les espaces commerciaux, les entrées de bureaux, etc.

Cette section décrit les exigences de localisation nécessaires et les étapes détaillées pour installer l'appareil Amazon One à montage mural afin de garantir des performances et une sécurité optimales.

Conditions préalables et préparation à l'installation de l'appareil Amazon One à montage mural

Avant de commencer l'installation, assurez-vous que les conditions suivantes sont remplies pour garantir que l'appareil fonctionne efficacement et qu'il est correctement configuré dans votre espace :

- Utilisation en intérieur uniquement : l'appareil mural Amazon One est destiné à une utilisation en intérieur uniquement. Assurez-vous donc qu'il est installé dans un environnement approprié.
- Exigences relatives au mur : le mur doit être plat pour garantir le bon alignement et le bon fonctionnement de l'appareil.
- Hauteur de montage : le haut du support mural ne doit pas être placé à plus de 44 à 46 pouces du sol après l'installation, afin de garantir un accès facile aux utilisateurs.
- Gestion des câbles : assurez-vous que tous les câbles excédentaires sont acheminés derrière le support mural et solidement fixés pour éviter de les endommager ou de les encombrer.
- Power Over Ethernet (PoE++) : Si vous utilisez Power Over Ethernet (PoE++), vérifiez qu'un commutateur PoE++ IEEE 802.3bt (type 3) classe 6 (extrémité) ou un injecteur (envergure intermédiaire) est disponible. La source PoE++ doit être répertoriée ou certifiée et conforme aux normes IEC 62368-1. Il est important de noter que la source PoE++ doit être située dans le même bâtiment que l'appareil. Utilisez uniquement une source PoE++ approuvée avec l'appareil AOE.
- Entrée d'alimentation 15 V DC : Si vous utilisez une entrée d'alimentation 15 V DC, assurez-vous que seule une alimentation NEC de classe 2 ou une alimentation approuvée à puissance limitée est utilisée. L'alimentation doit être répertoriée ou certifiée pour des raisons de sécurité et de compatibilité.

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

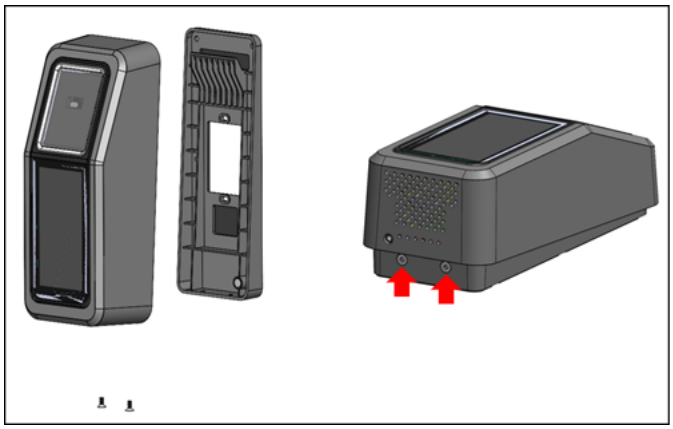
Inclus avec l'appareil Amazon One à montage mural

- 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

Une fois ces conditions préalables confirmées, vous pouvez procéder aux étapes d'installation pour monter et configurer en toute sécurité l'appareil Amazon One à montage mural.

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

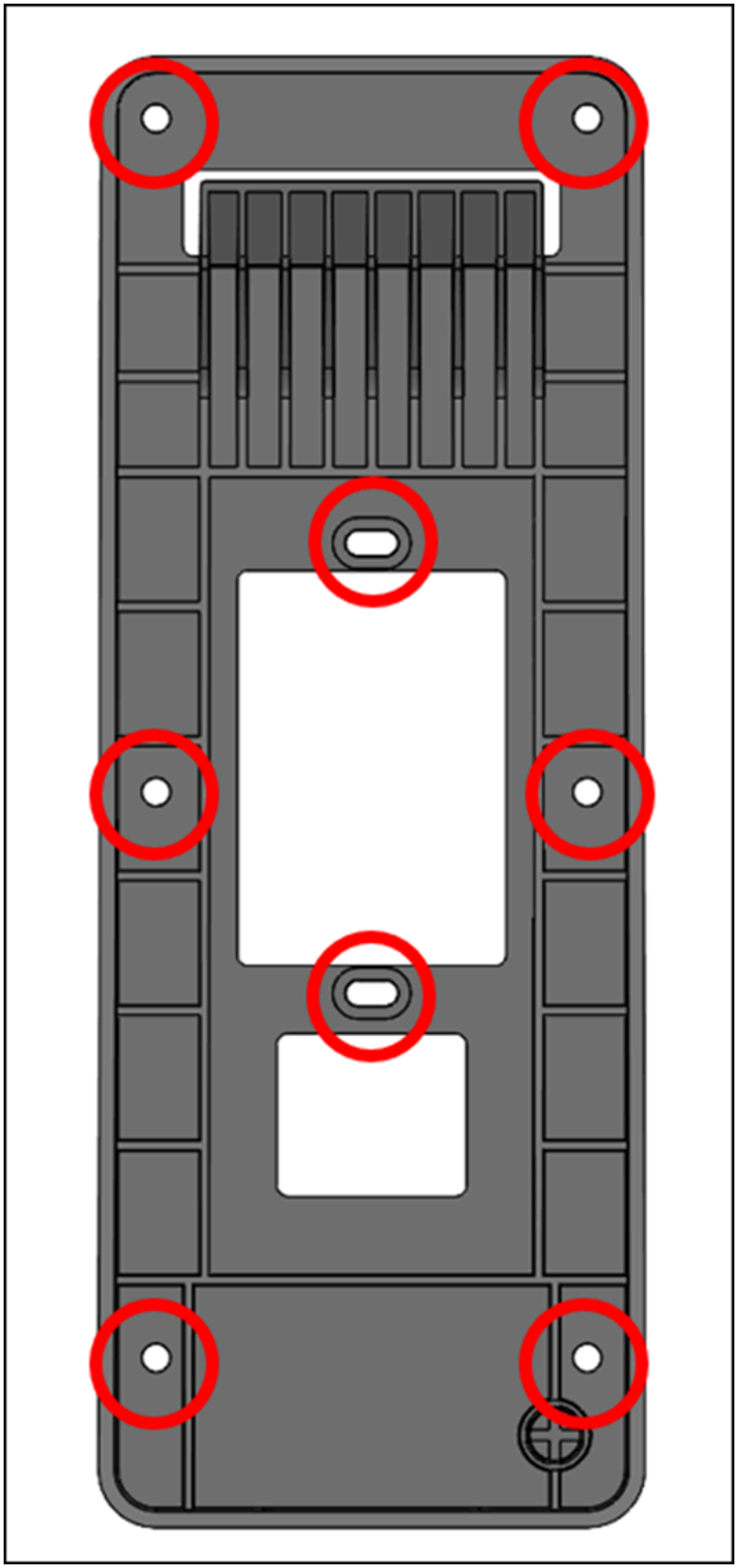
1. Retirez votre appareil Amazon One de son emballage.
2. Séparez la plaque de montage de votre appareil Amazon One en retirant les deux vis de sécurité Torx inférieures.



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.

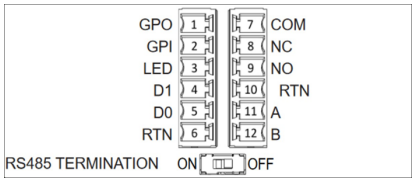
Pour connecter votre appareil Amazon One à montage mural

Vous pouvez configurer un appareil Amazon One avec les protocoles de contrôle d'accès OSDP et 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	

Connecteur	Connexion	Description	Utiliser
2	GPI	Saisie à usage général	Signal d'entrée numérique — Facultatif
3	LED	LED Wiegand	LED Wiegand — en option
4	D1	Wiegand D1	Wiegand data 1 — Fil blanc
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 normaleme nt fermé — fil orange
9	NO	Relais normalement ouvert	Relais de contact normalement ouvert — fil jaune
10	RTN	Retour du signal	Retour OSDP — Fil noir

Connecteur	Connexion	Description	Utiliser	
11	A	RS485_A/D1/ Horloge	OSDP D1 — Fil blanc	
12	B	RS485_B/D0/ Données	OSDP D0 — Fil vert	

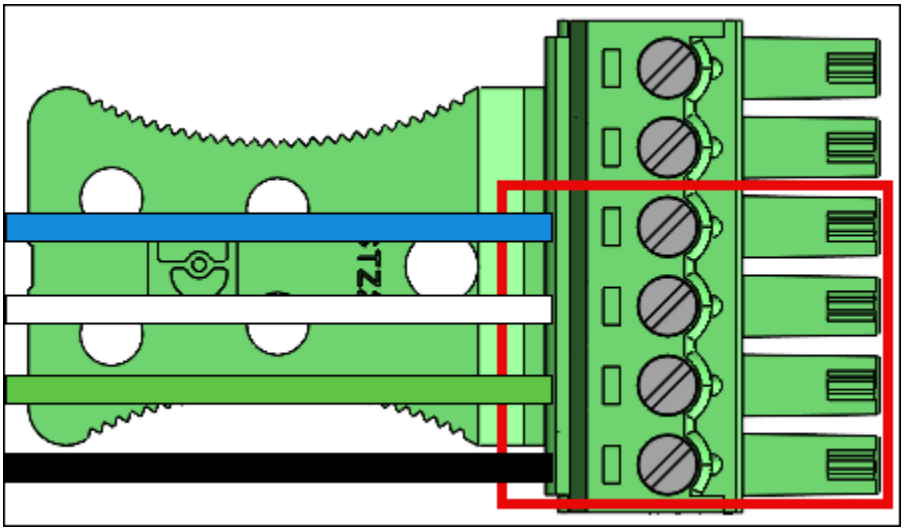
2. Lorsque vous installez un fil, dénudez 3 mm à 5 mm de l'extrémité du fil.
3. Insérez l'extrémité dénudée du fil dans la position terminale souhaitée.
4. À l'aide d'un tournevis à tête plate, tournez la vis de fixation du terminal dans le sens des aiguilles d'une montre pour fixer le fil jusqu'à ce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



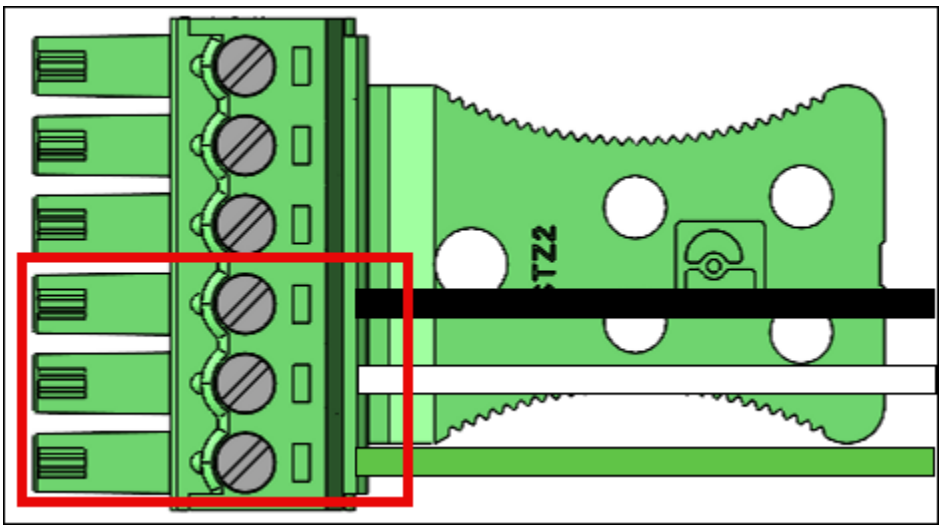
Câblage de sortie Wiegand

Connecteur	Connexion	Description	Utiliser	
3	LED	LED Wiegand	Entrée LED Wiegand — en option (5 V TTL)	
4	D1	Wiegand D1	Sortie Wiegand D1 (5 V TTL)	
5	D0	Wiegand D0	Sortie Wiegand D0 (5V 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.

RS485 connexions

- 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).

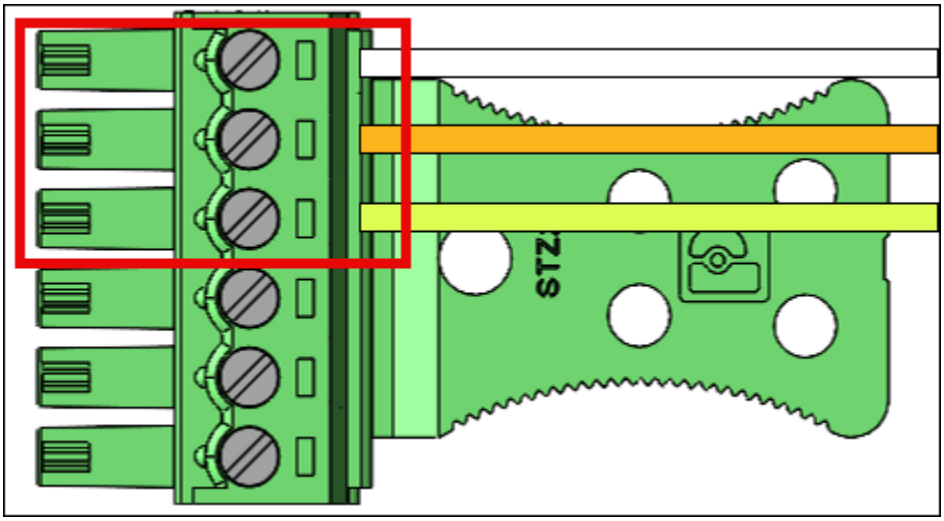


RS485 câblage

Connecteur	Connexion	Description	Utiliser
10	RTN	Retour du signal	Ground (Sol)
11	A	RS485_A/D1/ Horloge	RS485 signal non inverseur
12	B	RS485_B/D0/ Données	RS485 signal inverseur

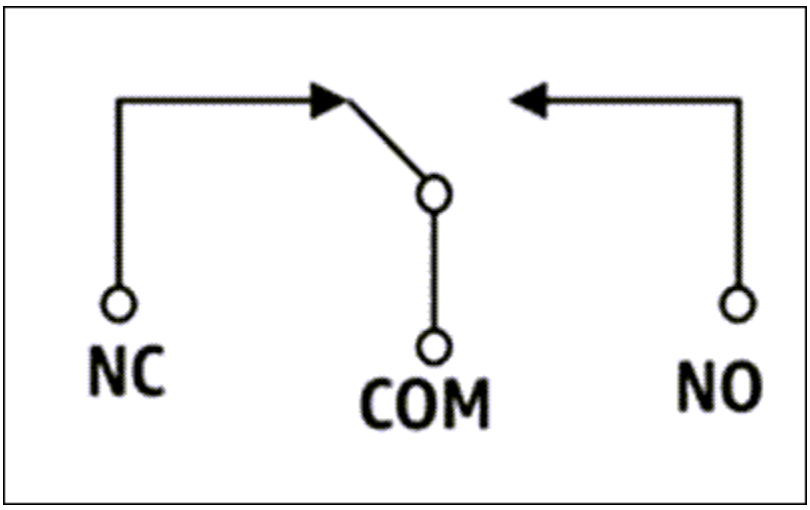
Connexions par relais

- 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

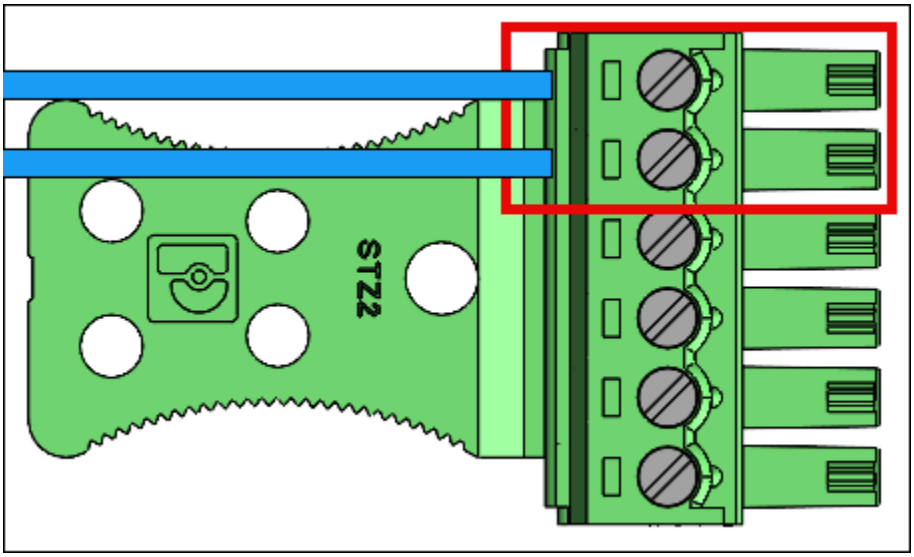
Connecteur	Connexion	Description	Utiliser	
7	COM	Relais commun	Relais de contact commun — fil blanc	
8	NC	Relais normalement fermé	Relais de contact normaleme nt fermé — fil orange	
9	NO	Relais normalement ouvert	Relais de contact normalement ouvert — fil jaune	



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

Connexions d'entrée/sortie numériques

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



Câblage d'entrée/sortie numérique

Connecteur	Connexion	Description	Utiliser	
1	GPO	Sortie à usage général	Signal de sortie numérique (5 V)	

Connecteur	Connexion	Description	Utiliser	
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.

Après avoir installé votre appareil Amazon One, vous êtes prêt à l'activer.

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

L'appareil Amazon One avec hub d'E/S fait partie intégrante du système Amazon One Enterprise, conçu pour améliorer la sécurité et rationaliser le contrôle d'accès pour divers environnements. L'appareil utilise la reconnaissance biométrique de la paume de la main pour fournir une authentification sécurisée et sans contact aux utilisateurs, ce qui le rend idéal pour une utilisation dans des zones hautement sécurisées telles que les immeubles de bureaux, les points d'entrée restreints ou les installations nécessitant une gestion fluide des accès. Le hub d'E/S agit comme un pont entre l'appareil et votre infrastructure de sécurité existante, permettant la communication avec les serrures de porte, les alarmes et les autres systèmes de contrôle d'accès.

Cette section fournit les exigences de localisation et step-by-step les instructions relatives à l'installation de l'appareil Amazon One avec un hub d'E/S. Une préparation et une installation appropriées sont essentielles pour garantir que le système fonctionne de manière sûre et efficace, offrant aux utilisateurs une expérience fluide et fiable.

Conditions préalables et préparation à l'installation de l'appareil Amazon One avec hub d'E/S

Avant de commencer l'installation, assurez-vous que les conditions suivantes sont remplies pour garantir une configuration sûre, sécurisée et efficace :

- Utilisation en intérieur uniquement : l'appareil Amazon One avec hub d'E/S est conçu pour une utilisation en intérieur uniquement. Assurez-vous qu'il est installé dans un environnement approprié.
- Power Over Ethernet (PoE++) : Si vous utilisez Power Over Ethernet (PoE++), vérifiez qu'un commutateur PoE++ IEEE 802.3bt (type 3) classe 6 (extrémité) ou un injecteur (envergure

intermédiaire) est disponible. La source PoE++ doit être répertoriée ou certifiée et conforme aux normes IEC 62368-1. Il est important de noter que la source PoE++ doit être située dans le même bâtiment que l'appareil. Utilisez uniquement une source PoE++ approuvée avec l'appareil AOE.

- Entrée d'alimentation 15 V DC : Si vous utilisez une entrée d'alimentation 15 V DC, assurez-vous que seule une alimentation approuvée NEC de classe 2 ou à puissance limitée est utilisée. L'alimentation doit être répertoriée ou certifiée pour des raisons de sécurité. Pour plus de détails, 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

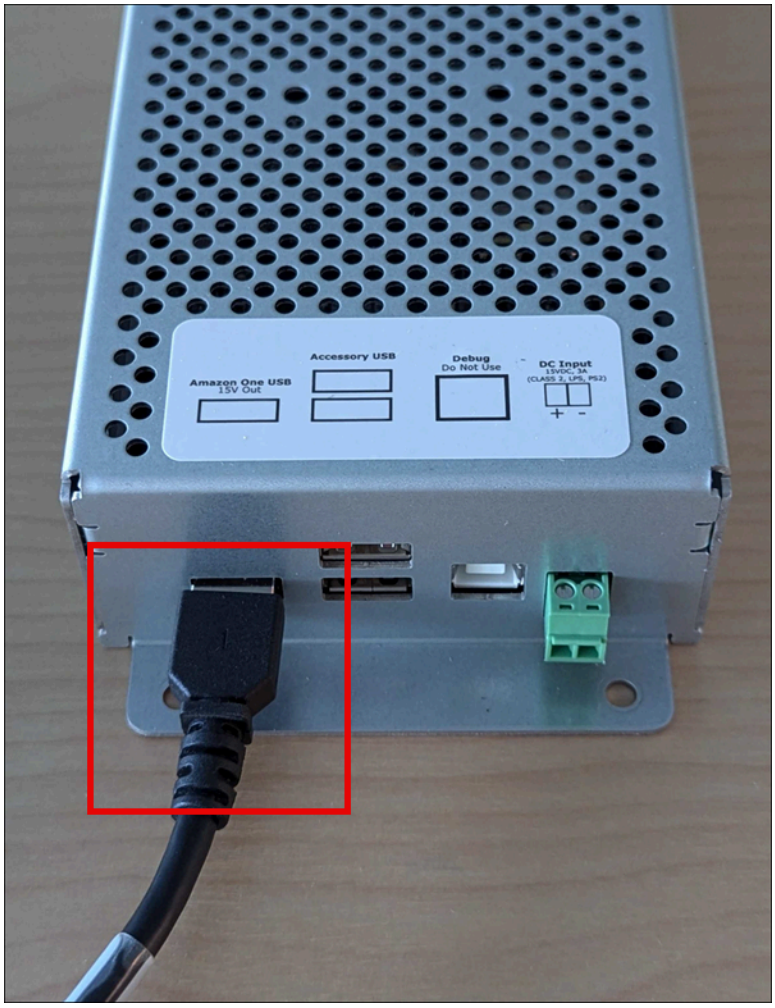
Inclus avec l'appareil Amazon One avec hub d'E/S

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

Une fois ces conditions préalables confirmées, vous pouvez poursuivre le processus d'installation afin de garantir une configuration sûre et efficace de votre appareil Amazon One avec I/O Hub. Une préparation adéquate permettra de garantir que l'appareil fonctionne comme prévu et qu'il s'intègre parfaitement à votre système d'accès sécurisé.

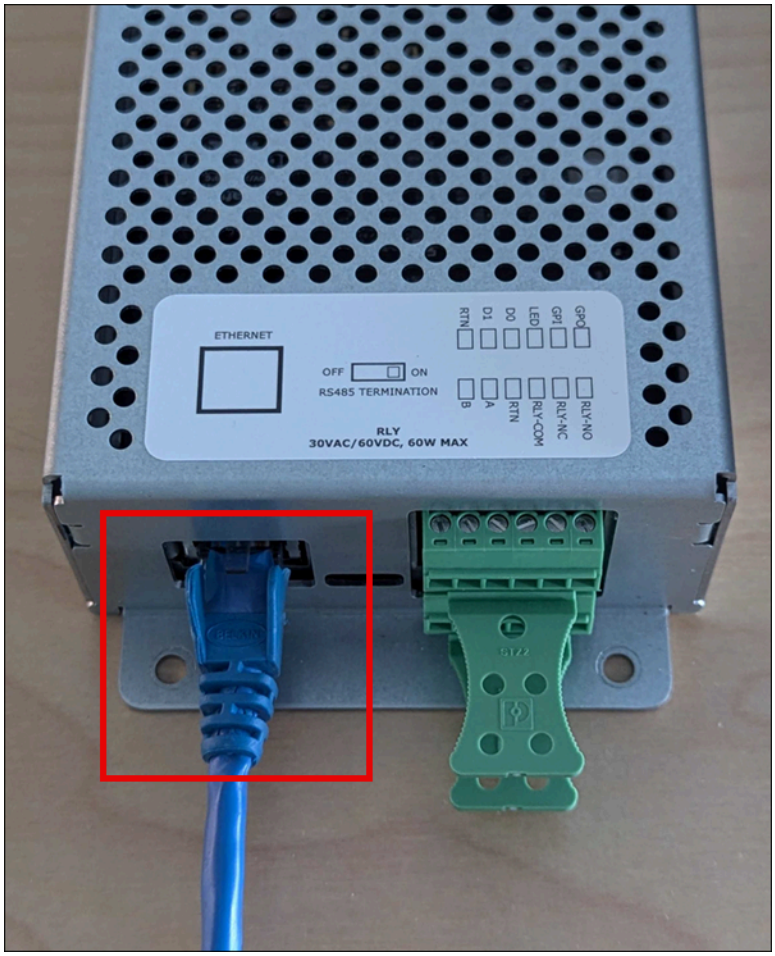
Pour installer le hub d'E/S sur votre appareil Amazon One

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 câble USB Amazon One sur le port du hub d'E/S.



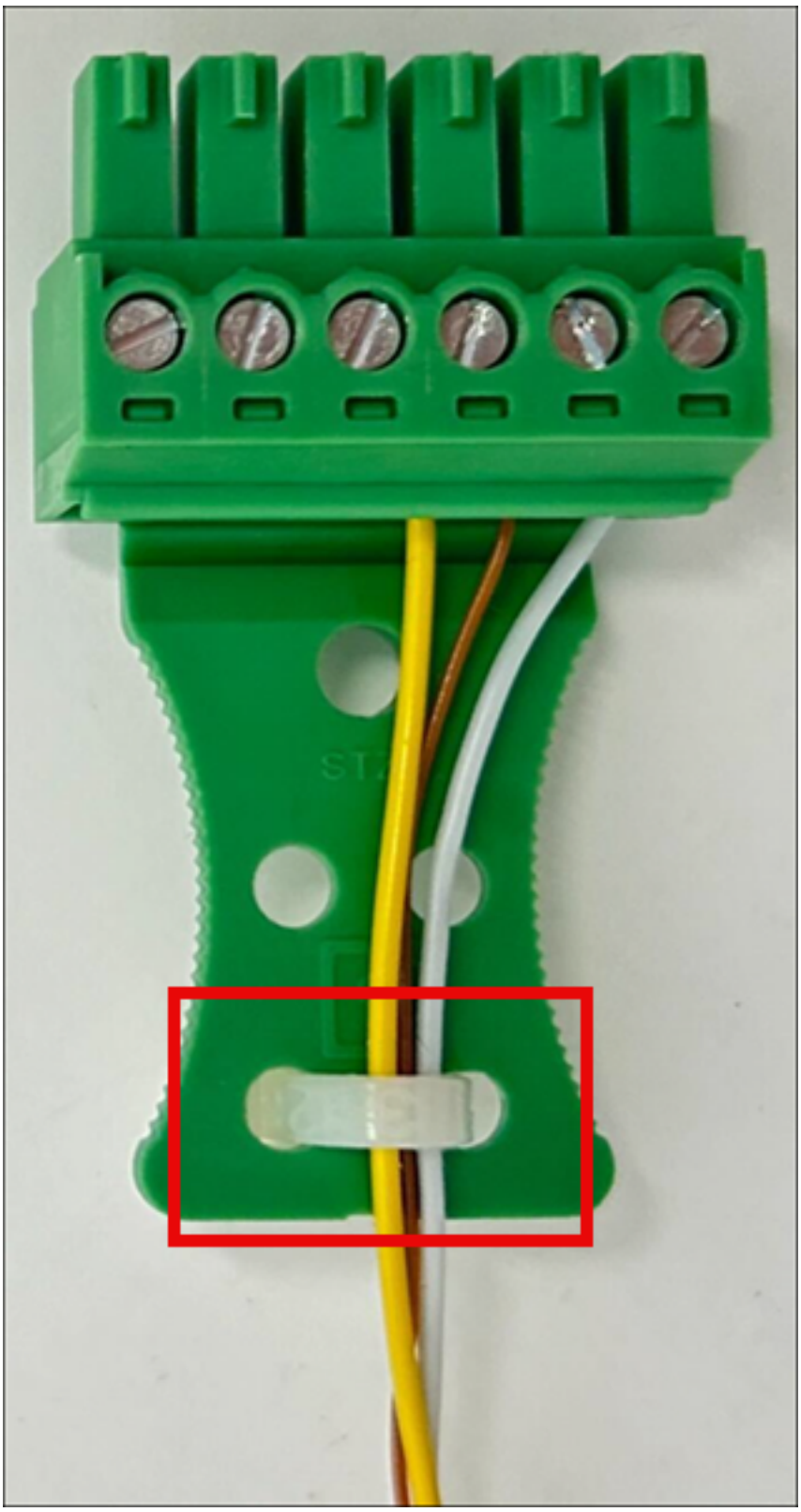
4. Pour l'alimentation POE++, branchez le câble Ethernet reliant la source POE++ au port du hub d'E/S.

   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

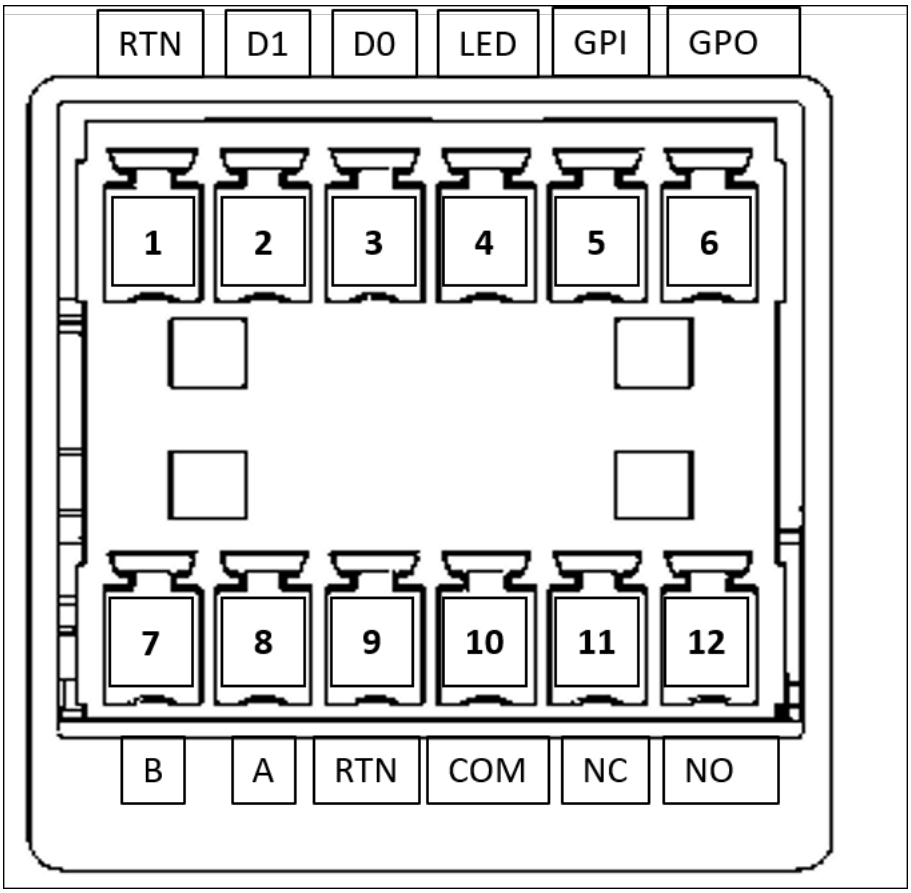
- Installez une boucle anti-goutte pour éviter que des liquides ne s'écoulent accidentellement le long du cordon et ne pénètrent dans le hub d'E/S.
- Fixez une pince antitraction pour protéger les fils contre les dommages ou le stress, comme indiqué dans l'image suivante.



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

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

Connexions



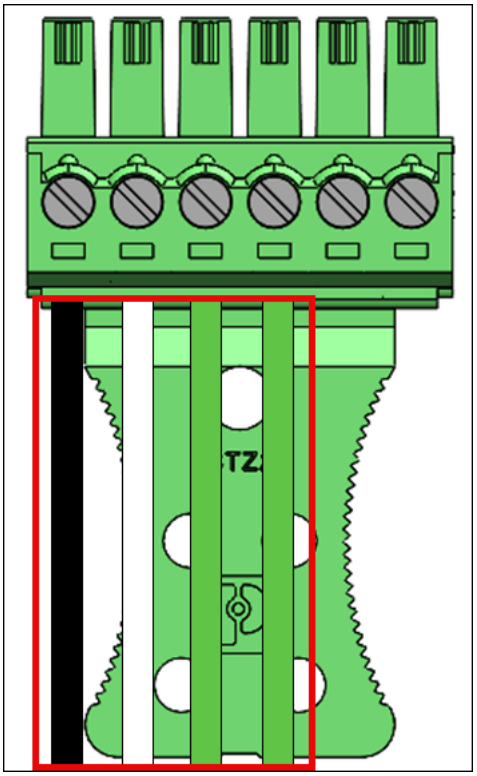
Connecteur	Connexion	Description	Utiliser
1	RTN	Retour du signal	Wiegand Ground — Fil noir
2	D1	Wiegand D1	Wiegand Data 1 — Fil blanc
3	D0	Wiegand D0	Wiegand data 0 — Câble vert
4	LED	LED Wiegand	LED Wiegand — en option

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	OSDP D0 — Fil vert	
8	A	RS485_A/D1/ Horloge	OSDP D1 — Fil blanc	
9	RTN	Retour du signal	Retour OSDP — 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 par 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).

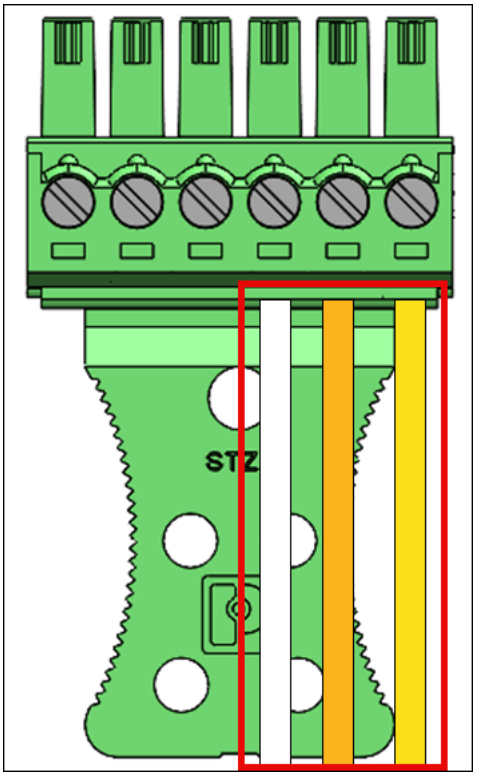
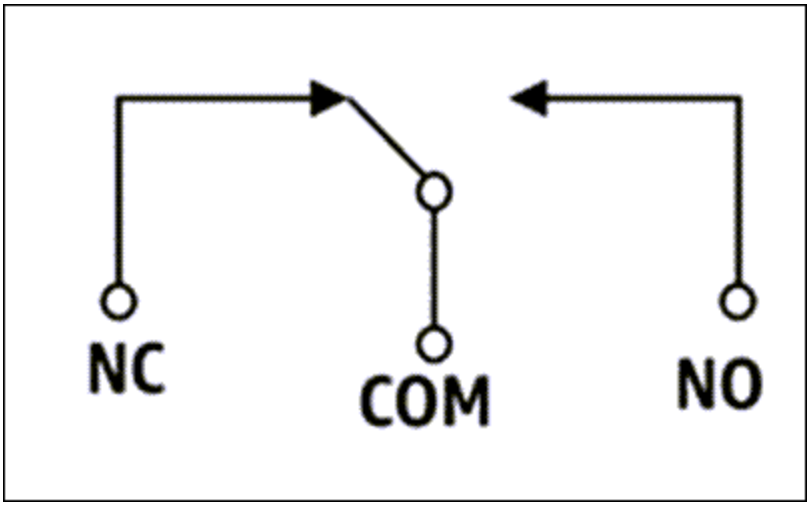


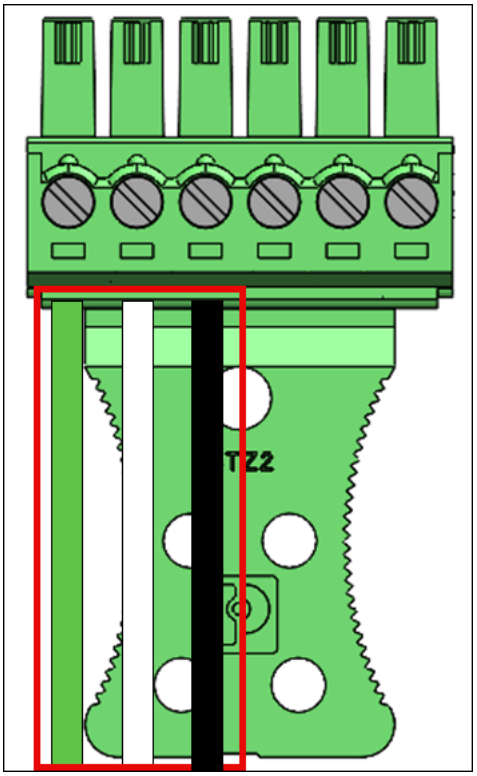
Schéma du relais



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

RS485 connexions

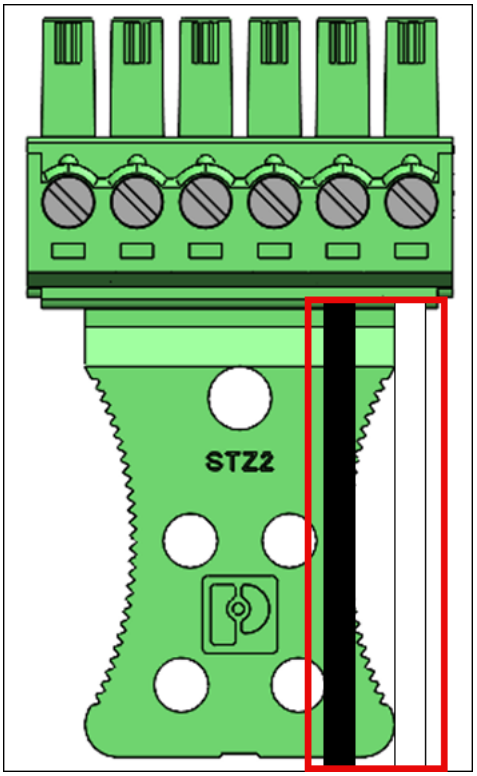
- Insérez le fil vert dans la broche 7 (B).
- Insérez le fil blanc dans la broche 8 (A).
- Insérez le fil noir dans la broche 9 (RTN).



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

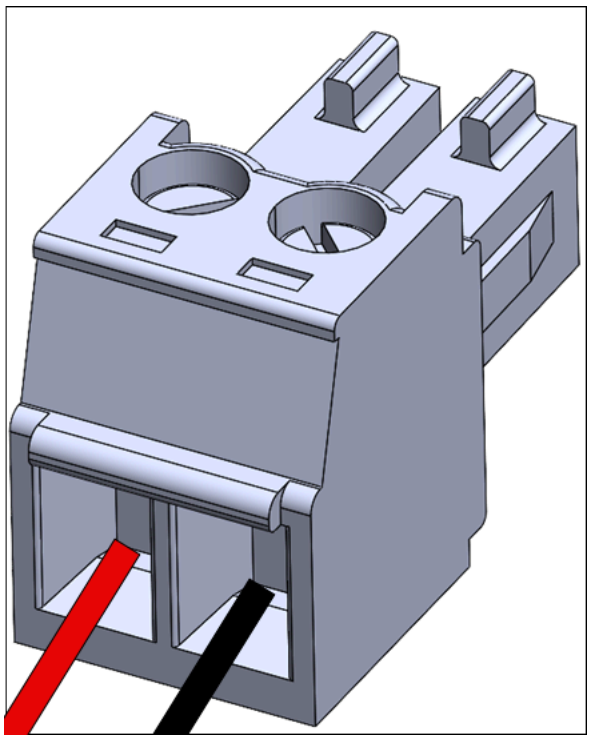
- Insérez le fil noir dans la broche 5 (GPI).
- Insérez le fil blanc dans la broche 6 (GPO).



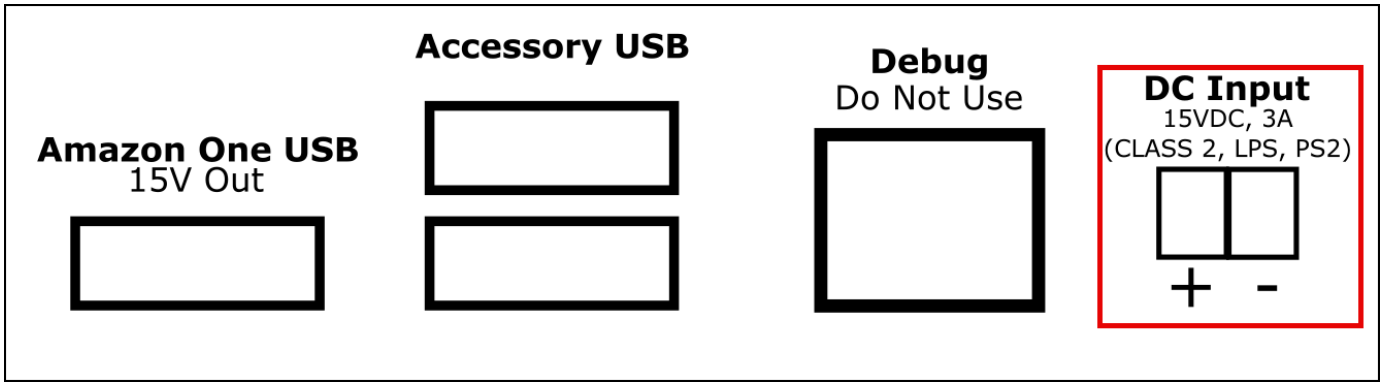
- Les connexions d'entrée/sortie numériques doivent être utilisées comme indiqué.

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.



Après avoir installé votre appareil Amazon One, vous êtes prêt à l'activer.

Activation de l'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 Ajouter des utilisateurs d'Amazon One.
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. Notez que le code QR est actualisé régulièrement pour des raisons de sécurité, vous ne pouvez utiliser un code QR qu'une seule fois.
11. Entrez le code postal du site, puis sélectionnez Confirmer les paramètres après avoir vérifié que le bon site est affiché.
12. Lorsque l'écran de l'appareil Amazon One indique que l'activation est terminée ! , l'appareil est prêt à être utilisé.

Inscription et saisie d'utilisateurs

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

- Création d'une politique de point de terminaison
- Authentification pour la saisie

Création d'une politique de point de terminaison

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.

Authentification pour la saisie

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

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.

Rubriques

- Afficher les utilisateurs inscrits
- Supprimer les utilisateurs inscrits et leurs données biométriques

Afficher les utilisateurs inscrits

La procédure suivante explique comment inscrire des utilisateurs.

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 badge RFID 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.

Supprimer les utilisateurs inscrits et leurs données biométriques

La procédure suivante explique comment supprimer les utilisateurs inscrits et leurs données biométriques.

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 Amazon One

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

- Entretien et nettoyage des appareils Amazon One
- Gestion du site
- Gestion des instances de périphériques

Entretien et nettoyage des appareils Amazon One

La maintenance de votre appareil Amazon One permet de bénéficier d'un environnement d'exploitation et d'une expérience optimaux.

Avant de nettoyer l'appareil Amazon One, assurez-vous de ce qui suit :

- Bien que vous n'ayez pas à activer ou désactiver Amazon One, assurez-vous que les appareils sont connectés à une source d'alimentation, qu'ils disposent d'une connectivité réseau et que tous les périphériques et accessoires (le cas échéant) sont connectés.
- Signalez les problèmes à votre administrateur si la connectivité réseau n'est pas disponible (un écran d'erreur sera visible sur l'appareil Amazon One dans ce cas), un écran d'erreur sera visible sur l'appareil Amazon One ou un problème de connexion de l'appareil sera visible sur la console.
- Sécurisez physiquement les appareils afin que des personnes non autorisées ne puissent pas les manipuler.
- Inspectez visuellement les appareils Amazon One tous les jours, en vérifiant toute connexion non autorisée à un appareil Amazon One.
- Inspectez tous les côtés de l'appareil pour détecter tout signe d'altération, y compris les vis visibles de l'appareil et du boîtier, afin de vous assurer qu'aucun espace ou ouverture n'expose les composants/circuits internes de l'appareil Amazon One.
- En cas d'erreur ou de panne, suivez les instructions affichées sur l'écran de l'appareil Amazon One ou consultez le guide de dépannage pour résoudre les problèmes.

Pour nettoyer l'appareil Amazon One

Le nettoyage régulier de votre appareil Amazon One permet d'éliminer les taches ou les marques telles que les empreintes digitales et les empreintes de mains.

> **Note**
>
> N'utilisez aucun autre produit de nettoyage en dehors de ceux listés dans ce guide. Le programme de nettoyage recommandé est d'une ou deux fois par semaine, ou chaque fois que de la saleté, de la poussière ou des taches sont visibles sur l'appareil, mais jamais plus d'une fois par jour.

1. Nettoyez l'appareil Amazon One avec des lingettes à base d'alcool isopropylique (IPA). Nettoyez uniquement la surface tactile de l'appareil. Ne touchez pas la vitre optique et n'utilisez aucun autre produit de nettoyage sauf indication contraire d'Amazon One.
2. Essuyez les traces avec un chiffon en microfibre sec.
3. Dépoussiérez légèrement (n'essuyez pas) les saletés ou débris visibles sur la fenêtre optique. Limitez le nettoyage de la fenêtre optique à une seule fois par jourand/or when the window is visually dirty (e.g., finger/hand prints/smudges). Cette partie de l'appareil n'est pas destinée à être touchée, mais de nouveaux clients pourraient la toucher par inadvertance.
4. Utilisez un nettoyeur de cartes à puce KIC pour nettoyer l'intérieur d'un lecteur de carte, le cas échéant.
5. Nettoyez l'appareil une ou deux fois par semaine, ou chaque fois que de la saleté, de la poussière ou des taches sont visibles sur l'appareil.

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.

Rubriques

- Modification du nom du site
- Mettre à jour l'adresse du site

Modification du nom du site

La procédure suivante explique comment modifier le nom du site pour votre appareil.

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.

Mettre à jour l'adresse du site

La procédure suivante explique comment mettre à jour l'adresse du site pour votre appareil.

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
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.

Rubriques

- Affichage de l'état de l'instance du terminal
- Redémarrage d'un appareil Amazon One
- Mettre à jour les configurations des appareils Amazon One
- Mise à jour des identifiants Wi-Fi
- Désactivation des instances de terminal

Affichage de l'état de l'instance du terminal

La procédure suivante explique comment afficher l'état de votre instance de terminal.

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.

Redémarrage d'un appareil Amazon One

La procédure suivante explique comment redémarrer votre appareil Amazon One.

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.

Mettre à jour les configurations des appareils Amazon One

La procédure suivante explique comment mettre à jour les configurations des appareils 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 (voirConfiguration d'une instance de terminal pour l'activation). Ensuite, vous pouvez suivre le processus d'activation de l'appareil (voirActivation de l'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.

Mise à jour des identifiants Wi-Fi

La procédure suivante explique comment mettre à jour les informations d'identification Wi-Fi.

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.

Désactivation des instances de terminal

La procédure suivante explique comment désactiver les instances de terminal.

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

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
- Gestion des identités et des accès pour Amazon One Enterprise
- Actions, ressources et clés de condition pour Amazon One Enterprise
- Validation de conformité pour Amazon One Enterprise

Protection des données dans Amazon One Enterprise

Le modèle de responsabilité AWS partagée de 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. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou 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) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent 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 modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 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 Nom. Cela inclut lorsque vous travaillez avec Amazon One Enterprise ou une autre entreprise Services AWS à l'aide de la console AWS CLI, de l'API 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 une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas

inclure d’informations d’identification dans l’adresse URL permettant de valider votre demande adressée à 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 des clés de chiffrement AWS.

Clés détenues par AWS : Amazon One Enterprise utilise ces clés par défaut pour chiffrer automatiquement les données sensibles des utilisateurs finaux. Vous ne pouvez pas consulter, gérer ou utiliser les clés détenues par AWS, 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 les clés détenues par AWS dans le guide du développeur d'AWS Key Management Service.

Chiffrement des données en transit

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

Gestion des identités et des accès pour Amazon One Enterprise

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

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l’aide de politiques
- Comment Amazon One Enterprise fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour Amazon One Enterprise
- AWS politiques gérées pour Amazon One Enterprise

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie 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 pouvez pas accéder à une fonctionnalité d'Amazon One Enterprise, consultezRésolution des problèmes d'identité et d'accès à Amazon One.

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 soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser l'IAM avec Amazon One Enterprise, consultezComment Amazon One Enterprise fonctionne avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, 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 Amazon One Enterprise que vous pouvez utiliser dans IAM, 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 l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS 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 (IAM Identity 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 avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

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

Si vous y accédez AWS par programmation, 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 d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

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

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS 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 vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

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 à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, 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 toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

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

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. 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 les ressources IAM.

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 plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- 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 obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent 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 direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains

services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'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 de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé 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 AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON 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 octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter 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 à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

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 au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des 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 les politiques AWS gérées par IAM dans 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. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, 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.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). 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 Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. 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. Le SCP limite les autorisations pour les entités

figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations 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 Politiques de session dans le Guide de l'utilisateur IAM.

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 déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon One Enterprise fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon One Enterprise, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Amazon One Enterprise.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon One Enterprise

Fonctionnalité IAM	Assistance Amazon One Enterprise
Politiques basées sur l'identité	Oui

Fonctionnalité IAM	Assistance Amazon One Enterprise
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (étiquettes 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 les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

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 des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et 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 découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

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 de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des 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 permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte 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 administrateur IAM 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, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour Amazon One Enterprise

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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 `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. 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 les politiques AWS JSON 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 de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de 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 ARNs caractéristiques, et pour savoir quelles actions vous pouvez utiliser pour spécifier l'ARN de chaque ressource, 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

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 les politiques AWS JSON 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 éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` 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 accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

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

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

ACLs dans 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. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Amazon One Enterprise

Prise en charge d'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas 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'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

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

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS 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 Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y 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 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 utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Amazon One Enterprise

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'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 endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS 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 de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

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

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Amazon One Enterprise
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accès en lecture seule à Amazon One Enterprise
- Accès complet à Amazon One Enterprise
- Autorisations prises en charge au niveau des ressources pour les actions d'API Amazon One Enterprise Rule
- Informations supplémentaires

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 frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS 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 des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

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 présentes dans votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

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

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

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

```
{
    "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 une politique AWS 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'élément `Resource` répertorie les ressources AWS 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 autorise toutes les actions Amazon One Enterprise, mais pas les actions relatives AWS aux autres services.
- `"Action": ["*"]`

  Cela permet toutes les AWS actions. Cette autorisation convient à un utilisateur qui agit en tant qu' 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 prises en charge au niveau des ressources pour les actions d'API Amazon One Enterprise Rule

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 l'API des règles 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 actions de l'API de 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 un ARN, 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 action d'API 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.

Action d'API	Ressources
CreateDeviceInstance	Instance de périphérique arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
GetDeviceInstance	Instance de périphérique arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
UpdateDeviceInstance	Instance de périphérique arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteDeviceInstance	Instance de périphérique arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceActivationQrCode	Instance de périphérique arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteAssociatedDevice	Instance de périphérique arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
RebootDevice	Instance de périphérique arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceInstanceConfiguration	Configuration de l'instance de l'appareil

Action d'API	Ressources
	arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*
GetDeviceInstanceConfiguration	Configuration de l'instance de l'appareil arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*
CreateSite	Site arn:aws:one ::site/ *region:accountID siteId*
DeleteSite	Site arn:aws:one ::site/ *region:accountID siteId*
GetSiteAddress	Site arn:aws:one ::site/ *region:accountID siteId*
UpdateSite	Site arn:aws:one ::site/ *region:accountID siteId*
UpdateSiteAddress	Site arn:aws:one ::site/ *region:accountID 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*

Action d'API	Ressources
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 les actions de lecture des AWS Config 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 l'API de règles Amazon One Enterprise.

Informations supplémentaires

Pour en savoir plus sur la création d'utilisateurs IAM, de groupes, de politiques et d'autorisations, consultez Création de votre premier groupe d'utilisateurs et d'administrateurs IAM et Gestion de l'accès dans le Guide de l'utilisateur IAM.

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 lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

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

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 flux RSS sur la page d'historique des documents Amazon One Enterprise.

Modification	Description	Date
Amazon One Enterprise a été ajouté AmazonOneMetricPublishAccess	La politique d'autorisation de rôle nommée AmazonOneMetricPublishAccess permet à Amazon One Enterprise d'effectuer CloudWatch : PutMetricData sur CloudWatch Namespace AmazonOneAWS/.	6 février 2025
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

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 propres au service suivantes à utiliser dans les politiques d'autorisation IAM.

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 indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. 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'opération d'API ou à la commande CLI 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 indiquer un ARN de ce type dans une déclaration avec 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 dans une politique IAM, vous devez inclure un ARN ou un modèle 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 une instance de terminal	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	Écrire	instance de dispositif*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	l'appareil et l'instance du périphérique				
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 une instance de terminal	Écrire	sites*		
GetSite	Accorder l'autorisation d'obtenir des informations sur le site	Lecture	sites*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSites	Accorder l'autorisation de répertorier des sites	Lecture			
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	Autoriser la suppression du 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

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. 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 que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. 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 :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- 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 décrivent 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, telles que la norme PCI DSS, 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.

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 les appels d'API et les événements associés 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 AWS CloudTrail Guide de l’utilisateur .

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. Connectez-vous à votre console AWS à l'adresse https://console.aws.amazon.com/events/.
2. Ouvrez la EventBridge console à l'adresse https://console.aws.amazon.com/events/.
3. Dans le volet de navigation, sous Bus, sélectionnez Rules.
4. Choisissez Créer une règle.
5. Sur la page de détail de la règle par défaut, attribuez un nom à la règle.
6. Sélectionnez Rule with an event pattern (Règle avec un modèle d'événement), puis sélectionnez Next (Suivant).
7. 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.
8. Sous Exemple de type d'événement, sélectionnez AWS Events.
9. Pour Méthode de création, choisissez Motif personnalisé.
10. Dans la section Modèle d'événement, ajoutez un JSON avec la source de l'événement comme `aws:one` et le type de détail requis :

```
"
source": ["aws.one"],
"detail-type": ["New Successful Enrollment",
"New Successful Un-enrollment",
"Unsuccessful Enrollment",
"Unsuccessful Un-enrollment",
"Successful Recognition",
"Unsuccessful Recognition"]
}
```

    Vous pouvez choisir le type de détail requis dans la liste ci-dessus et supprimer les informations inutiles.
11. Choisissez Suivant.
12. Sur la page Sélectionner une ou plusieurs cibles, sélectionnez une cible de votre choix, qui inclut une fonction Lambda, une file d'attente SQS ou un sujet SNS. Pour plus d'informations sur la configuration des cibles, consultez la section Amazon EventBridge Targets.

    Par exemple, pour savoir quand quelqu'un se connecte, choisissez « Reconnaissance réussie ». Regardez ensuite le détail de l'événement (donné en annexe) pour voir qui s'est inscrit.

Pour terminer votre flux de travail, vous pouvez exécuter une API externe ou une autre cible.

13. Vous pouvez éventuellement configurer des balises.
14. 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 au format JSON. Pour chaque type d'événement, un blob JSON 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.

L'état de santé de l'appareil est passé à 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 à la connectivité en ligne

L'appareil est connecté à Internet.

resources

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

métadonnées

Nom du site

- Nom du site sur lequel le DeviceInstance est présent.

Site Earn

- Arn pour le site où le DeviceInstance est présent.

data

Connectivité actuelle

- Indique si la DeviceInstance est connectée ou déconnectée d'Internet.
- Valeurs possibles : CONNECTED, DISCONNECTED

Connectivité précédente

- Indique si la DeviceInstance était connectée ou déconnectée d'Internet avant l'événement.
- Valeurs possibles : CONNECTED, DISCONNECTED

currentHealthStatus

- Indique si l'instance DeviceInstance a passé avec succès tous les tests de santé.
- Valeurs possibles : SAIN, CRITIQUE

previousHealthStatus

- Indique si l'instance DeviceInstance a réussi tous les tests de santé lors de sa dernière vérification.
- Valeurs possibles : SAIN, CRITIQUE

assetTagId

- Le assetTagId de l'appareil associé à la DeviceInstance.

deviceInstanceName

- Nom de l'instance DeviceInstance pour laquelle 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.

Source de la demande

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

Horodatage créé

- Heure de création de l'événement.

État de l'utilisateur

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

ID associé

- 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 est passé à critique
- La connectivité de l'appareil est passée en ligne
- La connectivité de l'appareil est passée en mode hors ligne

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 de santé CRITIQUE à SAIN.


```
{
    "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 passé à critique

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

```
{
  "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 de l'appareil est passée en ligne

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

```
{
  "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 de CONNECTED à DISCONNECTED.

```
{
  "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"
    }
  }
}
```

Journalisation des appels d'API 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 appels d'API 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 vers les opérations de l'API 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 à l'aide de 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 notifications Amazon SNS 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 de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

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 appels d'API 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"
}
```

Résolution des problèmes liés à Amazon One

Si vous rencontrez des problèmes avec l'application Amazon One ou l'un de vos appareils Amazon One, suivez ces suggestions pour résoudre le problème. Ensuite, si le problème persiste, contactez AWS Support.

Rubriques

- Résolution des problèmes d'identité et d'accès à Amazon One
- Résolution des problèmes liés à la console Amazon One
- Résolution des problèmes liés à l'appareil Amazon One

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

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 et IAM.

Rubriques

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

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

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 quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `one:`*`GetWidget`* 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 Compte AWS à moi à accéder à mes ressources Amazon One

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 plus d'informations, consultez les éléments suivants :

- Pour savoir si Amazon One Enterprise prend en charge ces fonctionnalités, consultezComment Amazon One Enterprise fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Résolution des problèmes liés à la console Amazon One

Si vous rencontrez des problèmes avec l'application Amazon One ou l'un de vos appareils Amazon One, suivez ces suggestions pour résoudre le problème. Ensuite, si le problème persiste, contactez AWS Support.

Rubriques

- Je ne parviens pas à créer un site
- Je ne parviens pas à créer une instance de périphérique
- Je ne parviens pas à créer un modèle de configuration
- Je ne parviens pas à créer un code QR d'activation

Je ne parviens pas à créer un site

- Contactez l'administrateur de votre console Amazon One pour qu'il vous donne accès.
- Si le problème persiste, contactez AWS Support.

Je ne parviens pas à créer une instance de périphérique

- Contactez l'administrateur de votre console Amazon One pour qu'il vous donne accès.
- Si le problème persiste, contactez AWS Support.

Je ne parviens pas à créer un modèle de configuration

- Contactez l'administrateur de votre console Amazon One pour qu'il vous donne accès.
- Si le problème persiste, contactez AWS Support.

Je ne parviens pas à créer un code QR d'activation

- Contactez l'administrateur de votre console Amazon One pour qu'il vous donne accès.
- Si le problème persiste, contactez AWS Support.

Résolution des problèmes liés à l'appareil Amazon One

Si vous rencontrez des problèmes avec la console Amazon One ou l'un de vos appareils Amazon One, suivez ces suggestions pour résoudre le problème. Ensuite, si le problème persiste, contactez AWS Support.

Rubriques

- écran blanc

- Je ne parviens pas à me connecter au Wi-Fi ou au réseau
- Redémarrer un appareil avec des alertes actives
- Erreur du système
- Le code QR n'est pas reconnu
- Impossible de lire le code QR
- Plusieurs codes QR détectés
- L'instance de périphérique n'existe pas
- Site non trouvé
- Le code postal ne correspond pas
- Le délai de la passerelle a expiré
- Je ne parviens pas à configurer l'appareil
- L'appareil a redémarré avec un message d'erreur et un code d'erreur
- Logo Amazon sur l'écran de l'appareil sans autre activité
- Temporairement indisponible
- Quelque chose s'est mal passé de notre côté
- Temporairement hors service
- L'appareil Amazon One présente des dommages physiques
- Impossible de lire la paume
- Palm non reconnue
- Appareil verrouillé en raison d'une inactivité prolongée
- Appareil verrouillé en raison d'un acte d'altération

écran blanc

Cela se produit lorsque le périphérique n'est pas alimenté ou qu'il est bloqué lors du redémarrage.

Procédez comme suit pour résoudre ce problème :

- Patientez quelques instants (moins de 30 secondes) au cas où l'appareil redémarrerait.
- Si l'anneau lumineux clignote alors que l'appareil est vide, attendez jusqu'à 30 secondes.
- Vérifiez si le cordon d'alimentation est branché à la fois sur la prise secteur et bien branché à l'arrière de l'appareil Amazon One. Vérifiez également que le cordon n'est pas endommagé.

- Vérifiez la source d'alimentation.
- Vérifiez que tous les câbles sont correctement connectés à Amazon One et au hub USB.
- Redémarrez l'appareil depuis la console.
- Si le redémarrage de l'appareil ne résout pas le problème, débranchez le hub USB Amazon One de l'alimentation, puis rebranchez-le.
- Si le problème persiste, contactez AWS Support.

Je ne parviens pas à me connecter au Wi-Fi ou au réseau

Cela se produit lorsque l'appareil perd sa connectivité.

Procédez comme suit pour résoudre ce problème :

- Si vous êtes connecté au Wi-Fi, utilisez un autre appareil pour vérifier si le Wi-Fi apparaît sur les réseaux disponibles.
- Vérifiez si le routeur Wi-Fi est allumé et s'il est à portée.
- L'appareil se reconnectera une fois le réseau rétabli.
- Si le problème persiste, contactez le support AWS.

Redémarrer un appareil avec des alertes actives

Lorsqu'un redémarrage est demandé depuis la console, l'opération attend jusqu'à 15 minutes pour que l'appareil reçoive la commande et tente de redémarrer, même s'il est hors ligne ou s'il rencontre des problèmes de réseau.

Procédez comme suit pour résoudre ce problème :

- Attendez que le redémarrage soit terminé.
- Si le problème persiste, contactez le support AWS.

Erreur du système

Cela est dû à une erreur interne.

Procédez comme suit pour résoudre ce problème :

- Choisissez Redémarrer à l'écran pour redémarrer l'application.
- Après 2 tentatives, si le problème n'est pas résolu, contactez AWS Support.

Le code QR n'est pas reconnu

Cela est dû à un code QR non autorisé ou à un code QR expiré.

Procédez comme suit pour résoudre ce problème :

- Choisissez Réessayer pour revenir à l'écran du code QR.
- Créez un nouveau code QR sur la console AWS, puis scannez le code QR valide.

Impossible de lire le code QR

Cela se produit lorsque l'application ne parvient pas à lire le code QR.

Procédez comme suit pour résoudre ce problème :

- Choisissez Réessayer pour revenir à l'écran du code QR.
- Si le problème persiste, annulez le flux de travail d'activation et redémarrez.

Plusieurs codes QR détectés

Cela se produit lorsque plusieurs codes QR sont scannés.

Procédez comme suit pour résoudre ce problème :

- Choisissez Réessayer pour revenir à l'écran du code QR.
- Scannez un seul code QR valide à la fois.

L'instance de périphérique n'existe pas

Cela se produit lorsque l'instance de l'appareil est supprimée ou n'existe pas dans la console AWS.

Procédez comme suit pour résoudre ce problème :

- Choisissez Réessayer pour revenir à l'écran du code QR.

- Vérifiez la console AWS pour trouver la bonne instance d'appareil. Si l'instance de l'appareil est manquante, contactez votre administrateur.
- Créez un nouveau code QR pour cette instance d'appareil, puis scannez le nouveau code QR.

Site non trouvé

Cela se produit lorsque le site est supprimé ou n'existe pas dans la console AWS.

Procédez comme suit pour résoudre ce problème :

- Consultez la console AWS pour obtenir des informations sur le site. Si le site n'existe pas, contactez votre administrateur.

Le code postal ne correspond pas

Cela se produit lors de la saisie d'un code postal différent de celui configuré pour l'appareil.

Procédez comme suit pour résoudre ce problème :

- Choisissez Réessayer pour revenir à l'écran du code postal.
- Vérifiez si vous avez le bon code postal du site.
- Si le problème persiste, contactez votre administrateur pour vérifier le code postal du site sur la console AWS.

Le délai de la passerelle a expiré

Cela se produit lorsqu'il n'y a aucune réponse de la passerelle dans un délai spécifié.

Procédez comme suit pour résoudre ce problème :

- Choisissez Redémarrer pour redémarrer l'application.
- Après deux tentatives, si le problème n'est pas résolu, contactez AWS Support.

Je ne parviens pas à configurer l'appareil

Cela se produit lorsque l'opération n'a pas réussi à enregistrer la configuration sur le disque de l'appareil.

Procédez comme suit pour résoudre ce problème :

- Choisissez Redémarrer pour redémarrer l'application.
- Après deux tentatives, si le problème n'est pas résolu, contactez AWS Support.

L'appareil a redémarré avec un message d'erreur et un code d'erreur

Procédez comme suit pour résoudre ce problème :

- Choisissez Redémarrer et laissez l'appareil récupérer.
- Si l'appareil ne se rétablit pas, débranchez le hub USB de l'alimentation et reconnectez-le.
- Si le problème persiste, contactez AWS Support.

Logo Amazon sur l'écran de l'appareil sans autre activité

Procédez comme suit pour résoudre ce problème :

- Patientez quelques instants (moins de 30 secondes) au cas où l'appareil redémarrerait.
- Débranchez le hub USB de l'alimentation et rebranchez-le.
- Si le problème persiste, contactez AWS Support.

Temporairement indisponible

Procédez comme suit pour résoudre ce problème :

- Assurez-vous que les connexions USB avec le périphérique ou le système hôte sont sécurisées.
- Déconnectez puis reconnectez tous les câbles qui entrent dans le hub USB.
- Si le problème persiste, contactez AWS Support.

Quelque chose s'est mal passé de notre côté

Cela se produit en cas d'erreur interne.

Procédez comme suit pour résoudre ce problème :

1. Éteignez l'appareil.

2. Débranchez-le de son alimentation.
3. Patientez 30 secondes.
4. Rebranchez l'appareil sur sa source d'alimentation.
5. Allumez l'appareil.
6. Si le problème persiste, contactez AWS Support.

Temporairement hors service

Cela se produit lorsque l'appareil a été mis hors service par Amazon One.

Procédez comme suit pour résoudre ce problème :

- Contactez AWS Support.

L'appareil Amazon One présente des dommages physiques

Procédez comme suit pour résoudre ce problème :

- Contactez AWS Support pour connaître les étapes suivantes et fournissez autant de détails que possible, tels que ce qui s'est passé, quand et pourquoi cela s'est produit.

Impossible de lire la paume

Procédez comme suit pour résoudre ce problème :

- Vérifiez que l'appareil Amazon One ne présente pas de traces ni de taches.
- Assurez-vous que la paume du client est exempte d'occlusions telles que des bandages, des manches et d'importantes saletés/huiles.
- Si le problème persiste et que l'appareil ne lit aucune paume, contactez le support AWS.

Palm non reconnue

Procédez comme suit pour résoudre ce problème :

- Demandez au client d'essayer d'utiliser l'autre paume de sa main.

- Assurez-vous que le client est déjà inscrit. Sinon, demandez-leur de s'inscrire en ligne ou sur l'appareil.
- Si le problème persiste et que l'appareil ne lit aucun contact avec la paume de la main, contactez le support AWS.

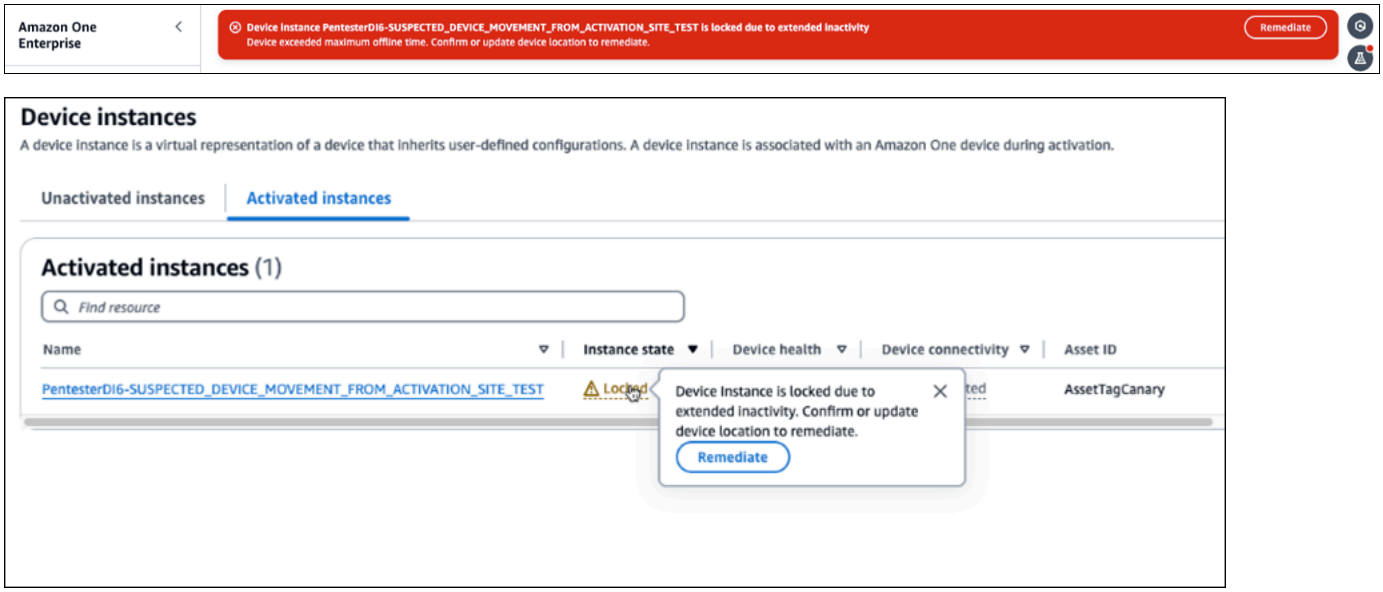
Appareil verrouillé en raison d'une inactivité prolongée

Lorsque l'appareil soupçonne qu'il a été déplacé du site d'activation, il verrouille les utilisateurs. Cela se produit lorsque l'appareil dépasse le maximum de 120 heures de temps hors ligne.

Procédez comme suit pour déverrouiller l'appareil :

1. Connectez-vous à votre console AWS et choisissez l'instance de l'appareil.
2. Dans le bandeau d'erreur en haut de la page, sélectionnez Corriger.

   Facultatif : dans Instances activées, sélectionnez Verrouillé, puis Corriger.



3. Si l'appareil se trouve toujours sur le site d'activation d'origine, choisissez Oui, l'appareil se trouve sur ce site.
4. Si l'appareil se trouve sur un autre site, choisissez Non, l'appareil se trouve sur un autre site. Choisir Non désactive l'appareil. Activez l'appareil sur le nouveau site.

Appareil verrouillé en raison d'un acte d'altération

Pour des raisons de sécurité, l'appareil Amazon One sera verrouillé en cas de falsification.

Procédez comme suit pour résoudre ce problème :

- Contactez AWS Support.

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	Ajout d'une section sur les rôles liés aux services	4 février 2025
Mettre à jour	Ajouté : contenu basé sur des scénarios	10 octobre 2024
Mettre à jour	Sujet ajouté : Résolution des problèmes liés à la console Amazon One Enterprise	10 octobre 2024
Mettre à jour	Sujet ajouté : Résolution des problèmes liés à l'appareil Amazon One Enterprise	10 octobre 2024
Mettre à jour	Chapitre ajouté : Configuration d'Amazon One Enterprise	10 octobre 2024
Mettre à jour	Sujet ajouté : Maintenance et nettoyage des appareils Amazon One Enterprise	10 octobre 2024
Mettre à jour	Contenu réorganisé	10 octobre 2024
Mettre à jour	Sujet ajouté : Installation du hub d'E/S pour appareils Amazon One Enterprise pour un accès sécurisé	14 août 2024
Mettre à jour	Sujet ajouté : Installation d'un appareil Amazon One Enterprise à montage mural	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.