aws

Guía del usuario

Amazon One Enterprise

Amazon One Enterprise: Guía del usuario

Table of Contents

¿Qué es Amazon One Enterprise?

Amazon One Enterprise es un nuevo servicio de autenticación basado en la palma de la mano que proporciona a los empleados un acceso seguro a edificios y activos empresariales, sin el uso de credenciales o códigos PINs de acceso.

Temas

Dispositivo Amazon One

El dispositivo Amazon One está diseñado para Amazon One Enterprise, un servicio de identidad seguro y basado en la palma de la mano para el control de acceso empresarial. Tenga en cuenta las siguientes especificaciones del dispositivo:

- Entradas de usuario: datos biométricos de Palm, coincidencia de códigos QR
- Interfaz de host: Wi-Fi (2.4 GHz y 5GHz), Ethernet, 2 de tipo A y 1 de USB tipo B USB
- Comentarios de los usuarios: pantalla táctil de 5,5 pulgadas, Lightring, altavoz y auriculares
- Protocolo de control de acceso físico y Wiegand OSDP
- Fuente de alimentación: incluye POE un adaptador de CA a CC de 110/220 VAC entradas, 30 W a 15 V
- Seguridad: interruptores antisabotaje
- Dimensión (HxWxD mm): 86 x 85 x 256

Consola Amazon One Enterprise

Amazon One Enterprise incluye una consola que se puede utilizar de las siguientes maneras:

- Un administrador de TI o de una instalación utiliza Amazon One Enterprise para crear y administrar un sitio. El sitio se asemeja a una ubicación física para las tareas que el equipo realiza mientras supervisa y administra los dispositivos y perfiles de usuario de Amazon One Enterprise. Las tareas del administrador de instalaciones o de TI incluyen:
  - Crear un sitio que contenga todas las instancias de dispositivos de Amazon One en una ubicación física
  - Añadir un usuario administrador para administrar el sitio y un usuario instalador para acceder a los códigos QR de activación

- Un administrador usa Amazon One Enterprise para crear instancias de dispositivos y administrar los dispositivos de Amazon One. Las tareas de administración incluyen:
  - Crear una instancia de dispositivo en un sitio
  - Crear una plantilla de configuración para aplicarla a una instancia de dispositivo
  - Supervisar el estado del dispositivo y actualizar las configuraciones del dispositivo
  - Cancelar las inscripciones de usuarios
- Un instalador utiliza Amazon One Enterprise para acceder a los códigos QR de activación para activar los dispositivos. Las tareas del instalador incluyen:
  - Acceder a un código QR de activación en la consola
  - Seleccionar un código QR que corresponda a la instancia del dispositivo que se va a activar
  - Escanear el código QR seleccionado con el dispositivo Amazon One instalado

Comprar dispositivos Amazon One

Ponte en contacto con nosotros para obtener más información sobre Amazon One Enterprise y un miembro del equipo de desarrollo empresarial se pondrá en contacto contigo para darte más detalles sobre nuestra oferta, incluidos los precios, y responder a cualquier pregunta que tengas.

Precios de Amazon One Enterprise

Ponte en contacto con nosotros para obtener más información sobre los precios de Amazon One Enterprise.

Cómo funciona Amazon One Enterprise

Amazon One Enterprise es un servicio biométrico basado en la nube que utiliza un dispositivo Amazon One para autenticar a un usuario mediante la biometría de la palma de la mano. Puede solicitar dispositivos Amazon One poniéndose en contacto con nosotros y puede suscribirse al servicio de acceso seguro Amazon One Enterprise utilizando el AWS Management Console.

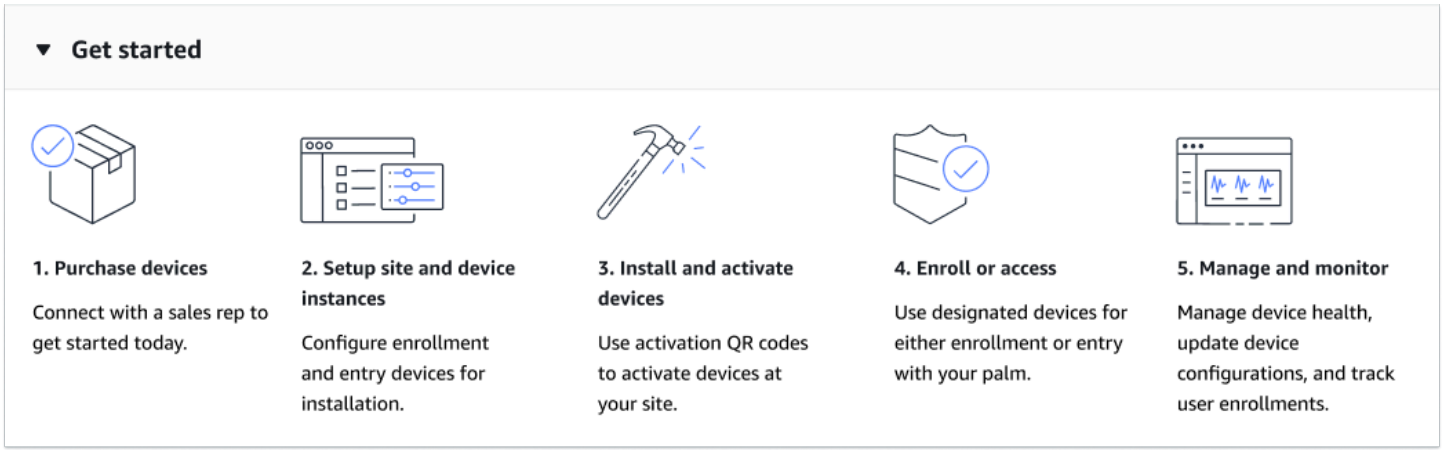
Una vez instalado Amazon One Enterprise, puede activar los dispositivos y registrarlos Cuenta de AWS en la consola Amazon One Enterprise Console, además de utilizar la aplicación de autenticación. También puedes ver el perfil biométrico de un empleado inscrito y cancelar la inscripción de un empleado. Cuando los empleados abandonan tu empresa o pierden su credencial, puedes eliminar fácilmente sus datos biométricos. La consola Amazon One Enterprise también actúa como una ubicación centralizada para administrar las actividades operativas, como el seguimiento de los dispositivos instalados y la visualización de las facturas mensuales.

Los empleados pueden inscribirse escaneando sus tarjetas de identificación y palma de la mano en los puestos de inscripción supervisados del establecimiento. Una vez inscritos, los empleados pueden simplemente colocar la palma de la mano sobre un dispositivo Amazon One para entrar o salir de un lugar seguro.

Temas

Flujo de trabajo de Amazon One Enterprise

El siguiente diagrama muestra el flujo de trabajo básico de Amazon One Enterprise.



1. Para comprar un dispositivo Amazon One, ponte en contacto con nosotros.
2. Cree sitios e instancias de dispositivos, configurando los dispositivos de inscripción y entrada para la instalación.
3. Tras la instalación, activa los dispositivos Amazon One escaneando un código QR seguro específico de la instancia del dispositivo.
4. Pide a los empleados que inscriban sus palmas y que, después, se autentiquen con las palmas de las manos para poder acceder.
5. Utilice las funciones de administración y monitoreo: garantice el estado del dispositivo, mantenga las configuraciones actualizadas y realice un seguimiento de las inscripciones de usuarios para una supervisión integral.

Términos clave de Amazon One Enterprise

Estos son los términos clave de Amazon One Enterprise:

- Sitio: el cliente administraba edificios físicos donde el cliente instala los dispositivos Amazon One Enterprise. Un sitio debe cumplir con los requisitos de instalaciones, redes y alimentación de sus dispositivos Amazon One Enterprise.
- Dispositivo: un dispositivo biométrico de escaneo de la palma de la mano de Amazon One Enterprise para la autenticación.
- Instancia de dispositivo: representación lógica de un dispositivo con configuraciones. El uso de instancias de dispositivos permite intercambiar dispositivos de Amazon One y, al mismo tiempo, heredar automáticamente las configuraciones y los nombres establecidos anteriormente. Una instancia de dispositivo tiene un nombre definido por el usuario (convención de nomenclatura compartida con el software de control de acceso) y un conjunto de configuraciones de comunicación. Las instancias de dispositivo tienen tres estados principales:
  - Necesita configuración
  - Listo para la activación
  - Activo
- Plantilla de configuración: un conjunto completo de configuraciones que se aplica a una instancia de dispositivo.

Introducción

En este capítulo se explican los pasos básicos para empezar a utilizar Amazon One Enterprise:

1. Configuración de un sitio, instancias de dispositivos y plantillas de configuración: sigue estos pasos para crear un marco que te permita añadir una ubicación física en la que alojar tus dispositivos Amazon One y, a continuación, configurarlos y gestionarlos. Los pasos utilizan la consola Amazon One Enterprise. Utilizará este proceso solo de vez en cuando, o incluso solo una vez, según la cantidad de sitios, instancias de dispositivos y plantillas de configuración que elija tener.
2. Instalación y activación de dispositivos: siga estos pasos al principio de la configuración. La activación del dispositivo requiere que los instaladores accedan a la consola de Amazon One Enterprise a través de un teléfono móvil para obtener los códigos QR de activación.
3. Administración de dispositivos y usuarios: siga estos pasos para el uso diario de la consola Amazon One Enterprise. Puede seguir estos pasos para supervisar el estado de los dispositivos, comprender las métricas de participación de los usuarios y configurar los dispositivos.

Para obtener más información sobre Amazon One Enterprise, visita la página de detalles del producto Amazon One Enterprise.

Temas

Configuración de Amazon One Enterprise

El primer paso para usar Amazon One Enterprise es configurar el sitio, las instancias de dispositivos y las plantillas de configuración mediante la consola de Amazon One Enterprise.

Temas

Paso 1: Crea una cuenta y un usuario administrador

Inscríbase para obtener una Cuenta de AWS

Si no tienes un Cuenta de AWS, complete los pasos siguientes para crear uno.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, un Usuario raíz de la cuenta de AWSse crea. El usuario root tiene acceso a todos Servicios de AWS y los recursos de la cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de suscribirse a una Cuenta de AWS, asegure su Usuario raíz de la cuenta de AWS, habilitar AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su Cuenta de AWS dirección de correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con un usuario root, consulte Iniciar sesión como usuario root en AWS Sign-In Guía del usuario.
2. Activa la autenticación multifactorial (MFA) para tu usuario root.

   Para obtener instrucciones, consulte Habilitar un MFA dispositivo virtual para su Cuenta de AWS usuario root (consola) en la Guía IAM del usuario.

Creación de un usuario con acceso administrativo

1. Habilite IAM Identity Center.

   Para obtener instrucciones, consulte Habilitar AWS IAM Identity Center en la AWS IAM Identity Center Guía del usuario.
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre el uso de Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la AWS IAM Identity Center Guía del usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con su usuario de IAM Identity Center, utilice el inicio de sesión URL que se envió a su dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, consulte Iniciar sesión en AWS acceda al portal en el AWS Sign-In Guía del usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos con privilegios mínimos.

Para obtener instrucciones, consulte Crear un conjunto de permisos en AWS IAM Identity Center Guía del usuario.

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para obtener instrucciones, consulte Añadir grupos en AWS IAM Identity Center Guía del usuario.

Paso 2: Añadir usuarios de Amazon One Enterprise

Además de los usuarios administradores, también puede añadir usuarios que carezcan de permisos de administrador. Por ejemplo, estos usuarios pueden ser instaladores que acceden a la consola de Amazon One Enterprise solo para recuperar los códigos QR de activación de dispositivos para activar los dispositivos Amazon One.

Para añadir un usuario de Amazon One Enterprise

1. Siga el procedimiento de inicio de sesión correspondiente a su tipo de usuario, tal y como se describe en Cómo iniciar sesión en AWS en el AWS Sign-In Guía del usuario.
2. En el panel de navegación, selecciona Usuarios y, a continuación, selecciona Agregar usuarios.
3. En la página Especificar detalles del usuario, en Detalles del usuario, en Nombre del usuario, ingrese el nombre del usuario nuevo. Este es su nombre de inicio de sesión para AWS.

> **Note**
>
> La cantidad y el tamaño de los IAM recursos de un Cuenta de AWS son limitados. Para obtener más información, consulte IAMy AWS STS cuotas. Los nombres de usuario pueden ser una combinación de hasta 64 letras, dígitos y los siguientes caracteres: más (+), igual (=), coma (,), punto (.), signo de arroba (@), guión bajo (_) y guión (-). Los nombres deben ser únicos dentro de una cuenta. No distinguen entre mayúsculas y minúsculas. Por ejemplo, no puede crear dos usuarios denominados TESTUSERy testuser. Cuando se usa un nombre de usuario en una política o como parte de unaARN, el nombre distingue entre mayúsculas y minúsculas. Cuando los clientes ven un nombre de usuario en la consola, por ejemplo, durante el proceso de inicio de sesión, el nombre del usuario no distingue entre mayúsculas y minúsculas.

4. Se le pregunta si proporciona acceso a la consola a una persona. Seleccione Proporcionar acceso de usuario a: AWS Management Console opcional.
5. Seleccione Deseo crear un IAM usuario.
6. En Contraseña de la consola, seleccione una de las siguientes opciones:

   - Contraseña generada automáticamente: el usuario recibe una contraseña generada aleatoriamente que cumple con la política de contraseñas de la cuenta. Si ingresa a la página Recuperar contraseña, puede ver o descargar la contraseña.
   - Contraseña personalizada: al usuario se le asigna la contraseña que introduzca en el campo.

7. (Opcional) De forma predeterminada, los usuarios deben crear una contraseña nueva la próxima vez que inicien sesión (se recomienda) está seleccionada para garantizar que el usuario tenga que cambiar su contraseña la primera vez que inicie sesión.

   > **Note**
   >
   > Si un administrador habilita la configuración de política de contraseñas de cuentas Permitir a los usuarios cambiar su contraseña, esta casilla de verificación no hace nada. De lo contrario, adjunta automáticamente una AWS política gestionada con el nombre `IAMUserChangePassword`de los nuevos usuarios. La política les otorga permiso para cambiar sus propias contraseñas.

8. Seleccione Siguiente.
9. En la página Establecer permisos, seleccione Asociar políticas existentes directamente.
10. Seleccione las políticas que desee adjuntar al usuario.

    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

    > **Note**
    >
    > AmazonOneEnterpriseInstallerAccess La política gestionada proporcionará a los usuarios acceso a los códigos QR de activación únicamente en la consola de Amazon One Enterprise. Esta política es ideal para las empresas que contratan a un tercero para instalar los dispositivos Amazon One.

11. Seleccione Siguiente.

12. (Opcional) En la página Revisar y crear, en Etiquetas, seleccione Agregar una etiqueta nueva para agregar metadatos al usuario mediante la asociación de etiquetas como pares de clave-valor. Para obtener más información sobre el uso de etiquetas enIAM, consulta Cómo etiquetar IAM los recursos.
13. Revisa todas las opciones que has hecho hasta ahora. Cuando esté listo para continuar, seleccione Crear usuario.
14. En la página Recuperar contraseña, obtendrá la contraseña que se le asignó al usuario:
    - Seleccione Mostrar junto a la contraseña para ver la contraseña del usuario y poder registrarla de forma manual.
    - Selecciona Descargar .csv para descargar las credenciales de inicio de sesión del usuario en un archivo.csv que puedes guardar en un lugar seguro.
15. Seleccione Instrucciones de inicio de sesión por correo electrónico. Su cliente de correo local se abrirá con un borrador que usted puede personalizar y enviar al usuario. La plantilla de correo electrónico contiene los detalles siguientes de cada usuario:
    - Nombre de usuario
    - URLa la página de inicio de sesión de la cuenta. Utilice el ejemplo siguiente y realice la sustitución con el número de ID o de alias de cuenta correcto:

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

> **Important**
>
> La contraseña del usuario no está incluida en el correo electrónico. Debe proporcionar la contraseña al usuario de una manera que cumpla con las directrices de seguridad de la organización.

Paso 3: Crea un sitio

Ahora que ha iniciado sesión en AWS Management Console, puede usar la consola de Amazon One Enterprise para crear su sitio.

> **Important**
>
> Amazon One Enterprise solo está disponible en la región EE.UU. Este (Norte de Virginia).

Cómo crear un sitio

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. Selecciona Ir a la descripción general.
3. En el panel de navegación, seleccione Sitios.
4. Selecciona Crear sitios.
5. En Información del sitio, en Nombre del sitio, introduzca un nombre para el sitio.
6. En Dirección física, introduce la dirección del sitio en el que se instalarán tus dispositivos Amazon One.
7. (Opcional) Para añadir una etiqueta al sitio, introduce un par clave-valor en Etiquetas y, a continuación, selecciona Añadir nueva etiqueta. Para eliminar esta etiqueta antes de crear el sitio, selecciona Eliminar.
8. Selecciona Crear sitio para crear el sitio.

Paso 4: Crear instancias de dispositivos

Para crear una instancia de dispositivo

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, selecciona Instancias de dispositivos. Asegúrese de estar en la pestaña Instancias no activadas.
3. En Detalles de la instancia, selecciona un sitio en el menú desplegable Sitio o crea un sitio nuevo pulsando el botón Crear sitio.
4. Introduzca manualmente el nombre de cada instancia de dispositivo individual.
5. (Opcional) Para añadir una etiqueta a la instancia del dispositivo, introduce un par clave-valor en Etiquetas y, a continuación, selecciona Añadir nueva etiqueta. Para eliminar esta etiqueta antes de crear la instancia del dispositivo, selecciona Eliminar.
6. Elija Crear instancias para crear las instancias del dispositivo.

> **Note**
>
> Nota: las instancias del dispositivo deben configurarse antes de que se pueda realizar la instalación.

Paso 5: Crear una plantilla de configuración

Para crear una plantilla de configuración

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, elija Plantillas de configuración.
3. Seleccione Crear plantilla.
4. En Información de la plantilla, en Nombre de la plantilla, introduzca un nombre para la plantilla de configuración.
5. En Configuraciones de dispositivos, seleccione un modo de funcionamiento.

   To configure Enrollment operating mode

   1. (Opcional) En la configuración de WiFi, proporciona tus credenciales de WiFi.
   2. (Opcional) Para añadir una etiqueta al sitio, introduce un par clave-valor en Etiquetas y, a continuación, selecciona Añadir nueva etiqueta. Para eliminar esta etiqueta antes de crear el sitio, selecciona Eliminar.
   3. Elija Configurar.

   To configure Entry operating mode

   1. En Configuración del panel de control, proporciona la configuración de comunicación para que los dispositivos Amazon One se comuniquen con tu panel de control.
   2. En Ajustes del formato de los distintivos, proporciona los ajustes de configuración que especifican el diseño del formato de los distintivos de tu empresa.
   3. (Opcional) En la configuración de WiFi, proporciona tus credenciales de WiFi.
   4. (Opcional) Para añadir una etiqueta al sitio, introduce un par clave-valor en Etiquetas y, a continuación, selecciona Añadir nueva etiqueta. Para eliminar esta etiqueta antes de crear el sitio, selecciona Eliminar.
   5. Elija Configurar.

> **Important**
>
> Debe configurar al menos un dispositivo de inscripción y un dispositivo de entrada para habilitar todas las capacidades de Amazon One Enterprise para un acceso seguro.

Paso 6: Configurar una instancia de dispositivo para su activación

Una vez creada una instancia de dispositivo, puede configurarla con una plantilla de configuración creada anteriormente (consultePaso 5: Crear una plantilla de configuración) o puede añadir las configuraciones manualmente.

Para configurar una instancia de dispositivo para su activación

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, selecciona Instancias de dispositivos. Asegúrese de estar en la pestaña Instancias no activadas.
3. Seleccione una o más instancias para configurarlas.
4. Elija Configurar.
5. En Configuraciones de dispositivos, selecciona uno de los dos métodos de entrada:

    a. Para la opción Usar plantilla, elija una plantilla del menú desplegable. Revise o modifique esta información de configuración importada.

    Para ver la opción Crear plantilla, consultePaso 5: Crear una plantilla de configuración.

    b. Para la opción de introducción manual, seleccione un modo de funcionamiento.

    To configure Enrollment operating mode

        a. (Opcional) En la configuración de WiFi, proporciona una credencial de WiFi.
        b. (Opcional) Para añadir una etiqueta al sitio, introduce un par clave-valor en Etiquetas y, a continuación, selecciona Añadir nueva etiqueta. Para eliminar esta etiqueta antes de crear el sitio, selecciona Eliminar.
        c. Elija Configurar.

To configure Entry operating mode

a. En Configuración del panel de control, proporciona la configuración de comunicación para que los dispositivos Amazon One se comuniquen con tu panel de control.

b. En Ajustes del formato de los distintivos, proporciona los ajustes de configuración que especifican el diseño del formato de los distintivos de tu empresa.

c. (Opcional) En la configuración de WiFi, proporciona una credencial de WiFi.

d. (Opcional) Para añadir una etiqueta al sitio, introduce un par clave-valor en Etiquetas y, a continuación, selecciona Añadir nueva etiqueta. Para eliminar esta etiqueta antes de crear el sitio, selecciona Eliminar.

e. Elija Configurar.

6. En la tabla de instancias no activadas, debería

mostrarse el estado de la instancia.

7. Compruebe que los códigos QR de activación estén disponibles para la activación. En el panel de navegación, selecciona Código QR de activación.

8. En la lista desplegable Seleccione un sitio, seleccione un sitio.

9. En Información del sitio, valide la dirección del sitio.

10. En Códigos QR de activación, cada instancia de dispositivo tiene el código QR correspondiente. Selecciona Obtener código QR para mostrar los códigos QR de activación.

> **Important**
>
> Debe configurar al menos un dispositivo de inscripción y un dispositivo de entrada para habilitar todas las capacidades de Amazon One Enterprise para un acceso seguro.

Instalación y activación de Amazon One

Una vez configurada la consola de Amazon One Enterprise, los siguientes pasos son instalar los dispositivos Amazon One Enterprise en su sitio y, a continuación, activarlos.

> **Note**
>
> Esta sección se centra en la instalación y utiliza un navegador móvil para acceder AWS Management Console para obtener los códigos QR de activación del dispositivo.

Temas

Comprensión de los requisitos

Se puede instalar un dispositivo Amazon One en cualquier ubicación corporativa o empresarial que tenga puertas que se puedan controlar eléctricamente.

Requisito del panel de control

Los dispositivos Amazon One se pueden conectar a la mayoría de los paneles de control de acceso estándar como lectores. Los dispositivos Amazon One admiten los siguientes protocolos:

- OSDP(v1 y v2)
- Wiegand

Requisito de red

Los dispositivos Amazon One deben estar siempre conectados a Internet para que funcionen normalmente. La conectividad a Internet se puede proporcionar mediante Ethernet cableado o Wi-Fi. El ancho de banda mínimo requerido es de 10 Mbps.

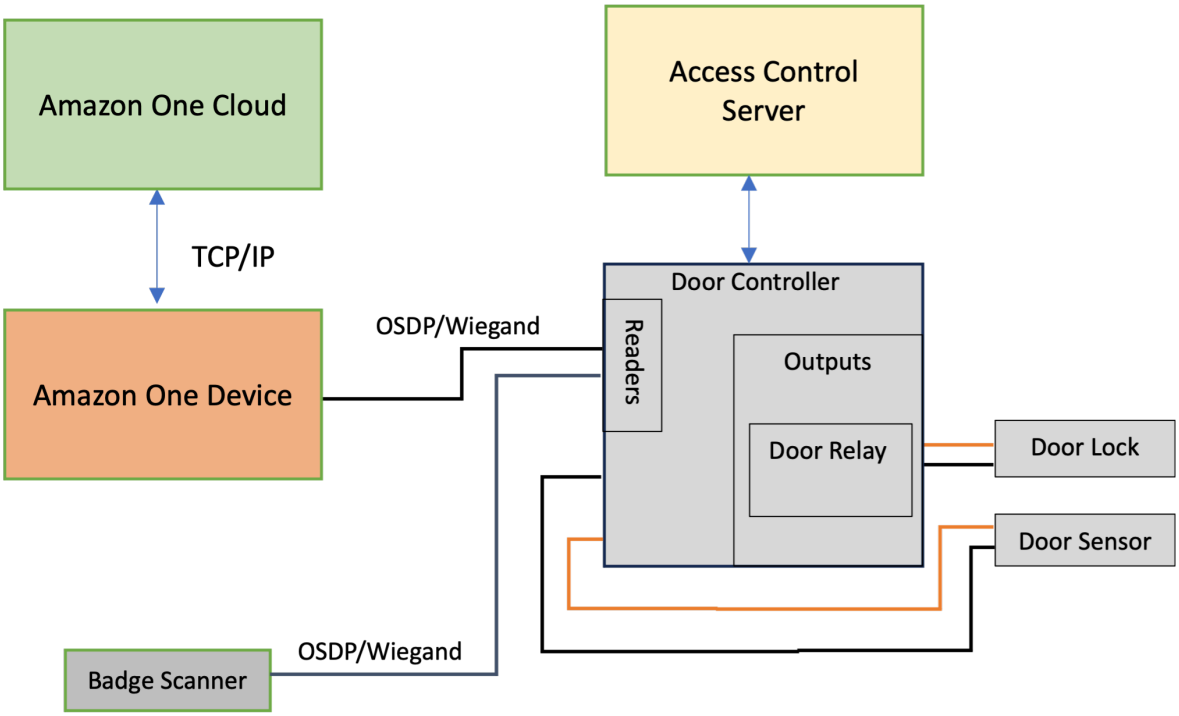
Requisito de alimentación

Los dispositivos Amazon One se pueden alimentar de dos maneras:

- Mediante el adaptador de corriente de 120 V que se incluye en la caja.
- Mediante un dispositivo compatible con PoE+.

Comprensión de los conceptos de instalación

Para proteger adecuadamente el acceso al edificio, Amazon One Enterprise recomienda instalar el dispositivo como parte de un entorno de control de acceso típico, tal y como se describe en el siguiente diagrama de bloques.



Un entorno de control de acceso normalmente consta de los siguientes componentes:

- Dispositivo Amazon One: este es el dispositivo de reconocimiento de la palma de la mano que realizará la autenticación biométrica para identificar a la persona que intenta acceder a un área segura del edificio.
- Servidor de control de acceso: este componente normalmente controla los derechos de acceso de los usuarios al área segura. Las credenciales IDs de las personas que tienen acceso al área generalmente se almacenan en este servidor. Este servidor almacena en caché lo relevante IDs para los controladores de puerta correspondientes.
- Controlador de puerta:
  - Un dispositivo Amazon One se conecta al servidor del controlador de puertas a través de una OSDP interfaz.

- Si se necesita una interfaz Wiegand, se puede utilizar un conversor COTS OSDP a Wiegand.
- Tras la autenticación correcta, el dispositivo Amazon One envía el identificador de identificación del usuario al controlador de la puerta.
- El controlador de puerta responde con una decisión, que luego permite que el dispositivo Amazon One muestre un mensaje de acceso concedido o acceso denegado.

- Escáner de credenciales: normalmente se utiliza un escáner de RFID credenciales para escanear tarjetas y enviar el número de placa al servidor de control de acceso. Con Amazon One Enterprise, se conecta un escáner de credenciales al dispositivo Amazon One de inscripción para poder escanear las insignias de los empleados y asociarlas a los perfiles de sus palmas.

Instalación del pedestal Amazon One Enterprise

En esta sección se describen los requisitos de ubicación y los pasos necesarios para instalar un pedestal Amazon One Enterprise.

Antes de iniciar la instalación, asegúrese de que se cumplen los siguientes requisitos previos:

- Si utiliza POE + para alimentar el dispositivo, asegúrese de que el cableado Cat6 esté dispuesto y de que haya un inyector o interruptor POE + disponible para su uso.
- Si se utiliza una fuente de alimentación de CA (120 V), la toma de CA debe estar disponible a menos de 20 pies del pedestal. AOE
- El suelo debe estar nivelado y limpio.
- El pedestal no debe bloquear la puerta o el carril.
- Todo el cable sobrante debe mantenerse dentro del pedestal y asegurarse.

Para instalar el pedestal de dispositivo Amazon One

1. Retira el pedestal Amazon One Enterprise del embalaje.
2. Retire la puerta desatornillando los dos tornillos M4 a prueba de manipulaciones.
3. Enchufe el cable de alimentación. Pase el cable a través del orificio de la placa base del pedestal.
4. Enrolle cualquier cable de alimentación sobrante dentro del pedestal.
5. Pase el cable Ethernet (Cat5E o mejor) a través de la placa inferior del pedestal y conéctelo al puerto Ethernet.
6. Pase el cable Ethernet (Cat5E o mejor) a través de la placa inferior del pedestal y conéctelo al puerto Ethernet.
7. Instale un lazo de ferrita en el cable Ethernet a 2 pulgadas por encima de la base del pedestal.
8. Introduzca el cable de RS485 serie desde el panel de control de acceso (o el lector de tarjetas) hasta el pedestal, con un exceso de longitud de 1 pie.
9. Instale un lazo de ferrita en el RS485 cable a 2 pulgadas por encima de la base del pedestal.
10. Conecta la alimentación a la toma de corriente y confirma que el dispositivo Amazon One está encendido.
11. Vuelva a colocar la puerta en el pedestal y vuelva a atornillar los dos tornillos M4 resistentes a la manipulación para fijarla.

Instalación de un dispositivo Amazon One que se pueda montar en la pared

En esta sección se detallan los requisitos de ubicación y los pasos necesarios para instalar tu dispositivo Amazon One que se puede montar en la pared.

Antes de iniciar la instalación, asegúrate de lo siguiente:

- El dispositivo Amazon One que se puede montar en la pared es solo para uso en interiores.
- La pared está nivelada.
- La parte superior del soporte de pared no debe estar a más de 44-46 pulgadas del suelo después del montaje.
- El cable sobrante queda colocado detrás del soporte de pared y asegurado.
- Para alimentación a través de Ethernet (PoE++):

Asegúrese de que esté disponible para su uso un conmutador IEEE 802.3bt (tipo 3) de clase 6 POE ++ o un inyector (tramo medio), que esté listado o certificado y cumpla con la norma 62368-1. IEC

Úselo AOE únicamente con una fuente PoE++ aprobada.

La fuente de PoE++ debe estar ubicada en el mismo edificio.

- Para una entrada de alimentación de 15 V DC, solo debes usar el dispositivo Amazon One con una fuente de alimentación aprobada de NEC clase 2 o con límite de energía que esté listada o certificada.

Herramientas necesarias:

- Broca de 1/4» para pared seca o mampostería si se requieren anclajes de pared
- Pelacables
- Broca de 7/64» para taladrar orificios piloto
- Destornillador Phillips #2
- Destornillador de cabeza plana de 0,5 mm x 2 mm
- Controlador Torx T12 Secure
- Lápiz
- Nivel

Incluido con el dispositivo Amazon One de montaje en pared:

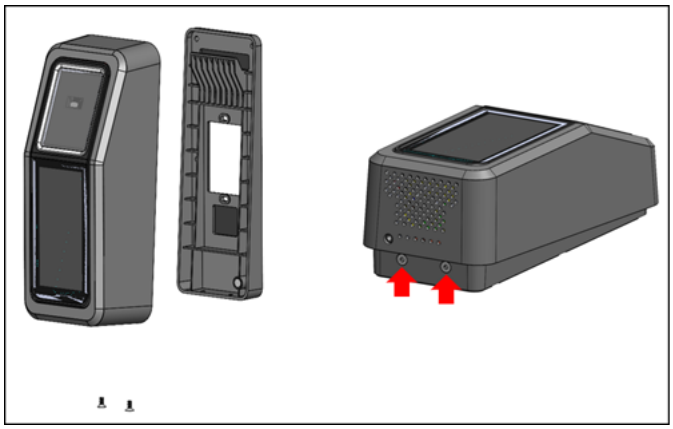
- 6 anclajes #8 para paneles de yeso
- 6 tornillos #8 -32 de 1 pulgada de largo
- 2 tornillos de máquina #6 -32 de 1 pulgada
- 2 conectores de bloque de terminales de 6 posiciones
- 2 tornillos Torx Security M4x10 de cabeza plana

Para instalar la placa de montaje en pared para tu dispositivo Amazon One

<result>

</result>

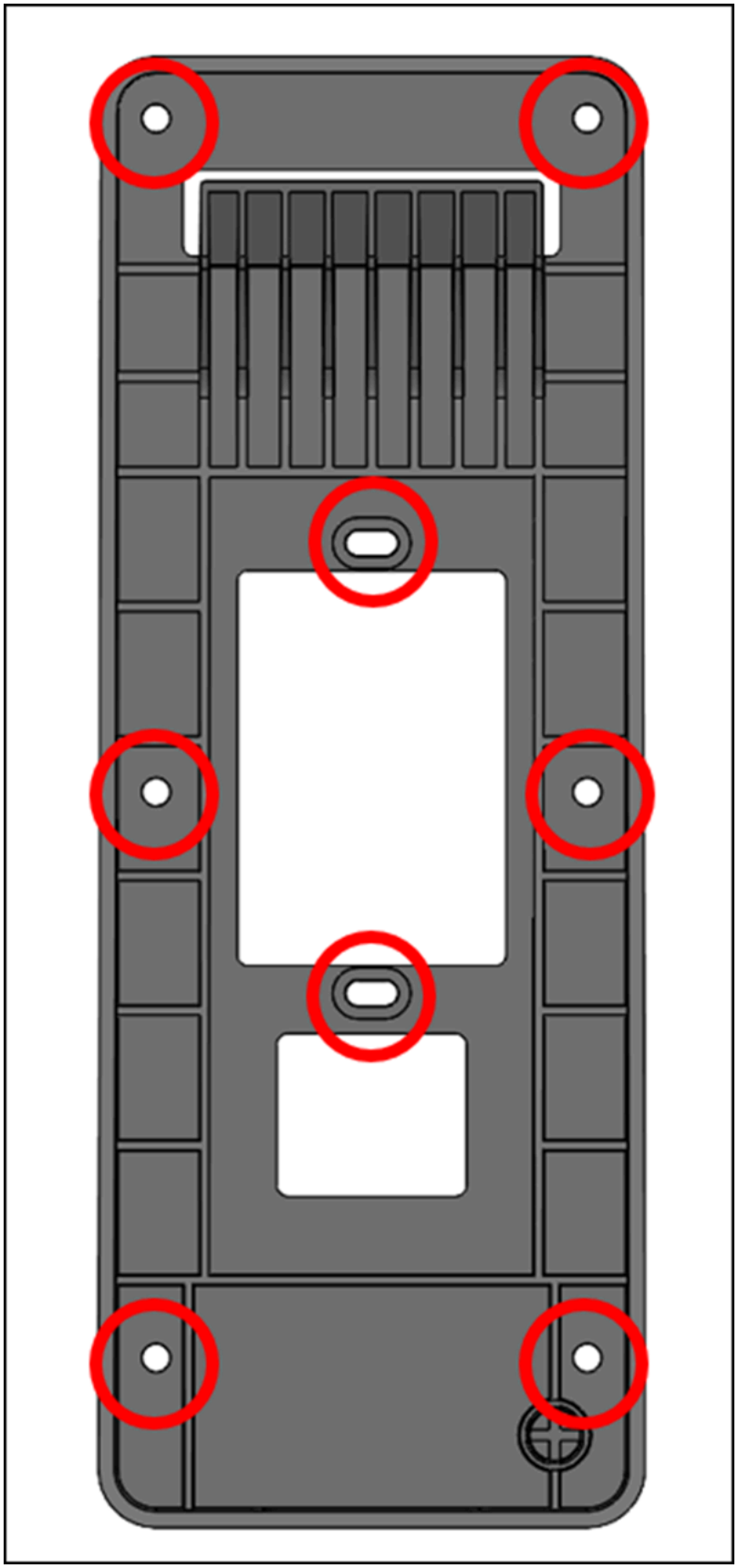
1. Retira tu dispositivo Amazon One del embalaje.
2. Separa la placa de montaje de tu dispositivo Amazon One quitando los dos tornillos de seguridad Torx inferiores.



3. Coloque la placa de montaje en la pared en el lugar deseado. Utilice el soporte como plantilla para marcar los seis orificios exteriores de los tornillos, como se muestra en la siguiente imagen.

   (Opcional) Si hay una caja de un solo conector disponible en la posición de instalación, lleve a cabo lo siguiente:

   - Coloque la placa sin apretar en la caja de montaje insertando los tornillos de máquina #6 -32 incluidos a través de los orificios oblongos.
   - Asegúrese de que la placa de montaje esté nivelada.
   - Utilice la placa de montaje como plantilla para marcar las seis posiciones de los tornillos con un lápiz. Puede utilizar los orificios oblongos y el tornillo #6 -32 como soporte adicional para la placa de montaje. No utilice las posiciones de los tornillos #6 -32 como medio principal para montar la placa de pared.



4. Si lo monta en superficies de estuco, paneles de yeso, ladrillo u hormigón, taladre orificios de 1/4 pulgada en cada lugar marcado y, a continuación, instale los anclajes de pared presionándolos en el orificio hasta que el anclaje quede al ras de la pared.

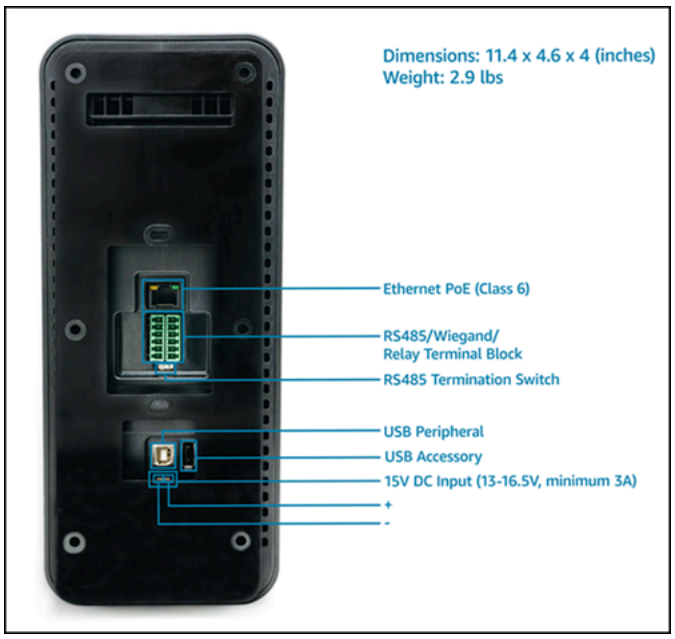
   Si se monta sobre una superficie de madera, no se necesitan anclajes y solo se necesitan orificios guía de 7/64 pulgadas en los lugares marcados.
5. Fije holgadamente la placa de pared a la pared con los tornillos para madera #8 en las posiciones de anclaje.
6. Una vez que todos los sujetadores estén en su lugar, asegúrese de que la placa de montaje esté nivelada.
7. Apriete los tornillos para fijar la placa de montaje a la pared.

Para conectar tu dispositivo Amazon One que se puede montar en la pared

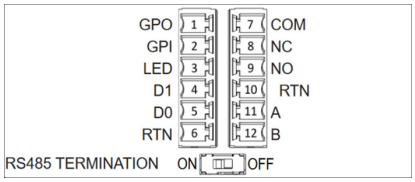
Puede configurar el dispositivo Amazon One con OSDP los protocolos de control de acceso de Weigand. Para simplificar la instalación, el dispositivo Amazon One utiliza conectores de bloque de terminales (fabricante P/N: Phoenix Contact 1767694). También tienes la opción de configurar el dispositivo Amazon One para controlar directamente los dispositivos externos mediante el relé interno o las conexiones de entrada y salida de uso general.

1. Para determinar la configuración de cableado adecuada para su aplicación, consulte el siguiente diagrama y la tabla de conexiones.

   Para obtener información detallada sobre las características eléctricas de las señales, consulte las instrucciones de cableado.



Conexiones



Pin	Connection	Descripción	Uso	
1	GPO	Salida de uso general	Señal de salida digital: opcional	
2	GPI	Entrada de uso general	Señal de entrada digital: opcional	
3	LED	Wiegand LED	Wiegand — Opcional LED	
4	D1	Wiegand D1	Wiegand data 1 — Cable blanco	

Pin	Connection	Descripción	Uso	
5	D0	Wiegand D0	Datos de Wiegand 0 — Cable verde	
6	RTN	Retorno de señal	Wiegand Ground — Cable negro	
7	Com	Relé común	Relé de contacto común: cable blanco	
8	NC	Relé normalmente cerrado	Relé de contacto normalmente cerrado: cable naranja	
9	NO	El relé está normalmente abierto	El relé de contacto está normalmente abierto: cable amarillo	
10	RTN	Retorno de señal	OSDPretorno — Cable negro	
11	A	RS485_A/D1/ Reloj	OSDPD1 — Cable blanco	
12	B	RS485_B/D0/ Datos	OSDPD0 — Cable verde	

2. Al instalar un cable, separe entre 3 mm y 5 mm del extremo del cable.
3. Inserte el extremo pelado del cable en la posición de terminal deseada.

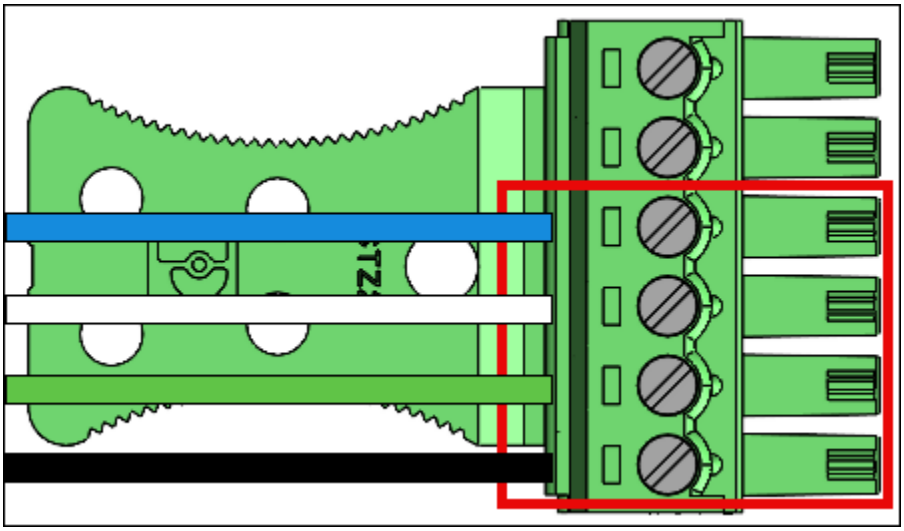
4. Con un destornillador de punta plana, gire el tornillo de retención del terminal en el sentido de las agujas del reloj para sujetar el cable hasta que quede ajustado. No lo apriete demasiado.
5. Después de sujetarlo, tire suavemente del cable para asegurarse de que quede bien asentado.
6. Después de realizar las conexiones necesarias, inserta el enchufe en el receptáculo correspondiente del bloque de terminales de tu dispositivo Amazon One.
7. Inserta el cable Ethernet Cat6 en la toma. RJ45
8. Coloca el dispositivo Amazon One de forma que el gancho de la placa de pared se deslice dentro de la abertura de la parte trasera del dispositivo.
9. Asegúrese de que los cables no queden atrapados entre el dispositivo y la placa de montaje y deje que el dispositivo gire y se asiente en su posición.
10. Fije su dispositivo Amazon One a la placa de montaje con dos tornillos Torx Security M4x10 de cabeza plana.
11. Apriete los tornillos con la mano. No los aprietes demasiado.

Para conectar tu dispositivo Amazon One que se puede montar en la pared

Instale solo los cables necesarios para su aplicación.

Conexiones Wiegand

- Inserte el cable azul en el pin 3 ()LED.
- Inserte el cable blanco en el pin 4 (D1).
- Inserte el cable verde en el pin 5 (D0).
- Inserte el cable negro en el pin 6 (RTN).



Cableado de salida Wiegand

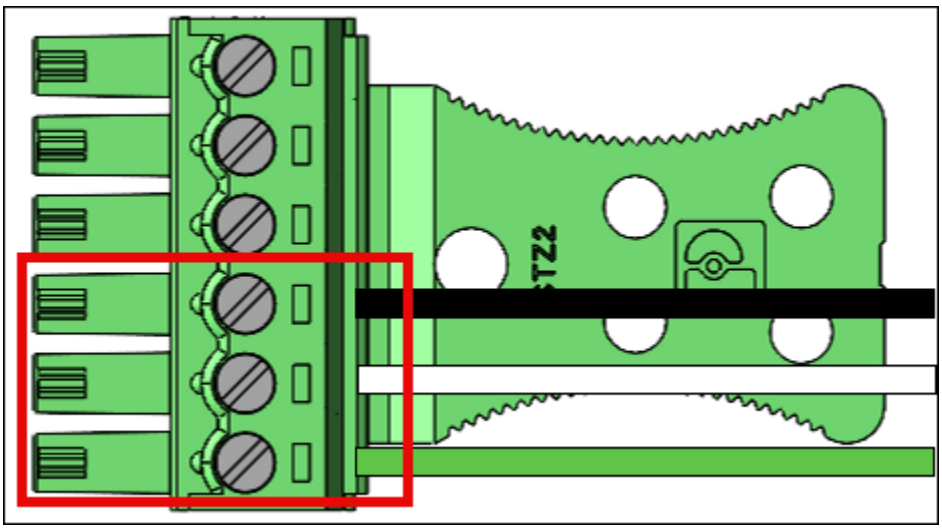
Pin	Connection	Descripción	Uso
3	LED	Wiegand LED	LEDEntrada Wiegand: opcional (5 V) TTL
4	D1	Wiegand D1	Salida Wiegand D1 (5 V) TTL
5	D0	Wiegand D0	Salida Wiegand D0 (5 V) TTL
6	RTN	Retorno de señal	Referencia de Wiegand GND

Gire el interruptor de RS485 terminación a la posición «ON» si el dispositivo es la última unidad de la línea. Este interruptor activa la terminación de una resistencia de 120 ohmios en la línea.

RS485conexiones

- Inserte el cable negro en el pin 10 (RTN).
- Inserte el cable blanco en el pin 11 (A).

- Inserte el cable verde en el pin 12 (B).

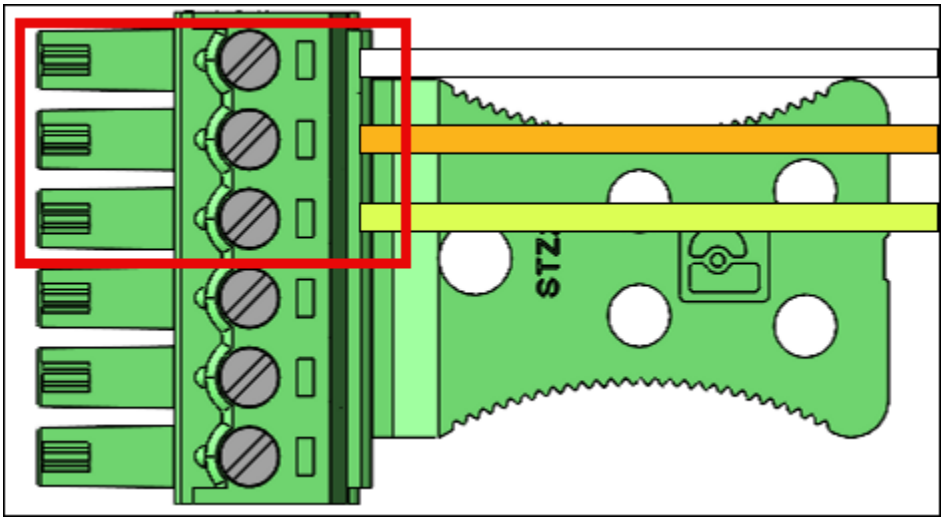


RS485cableado

Pin	Connection	Descripción	Uso
10	RTN	Retorno de señal	Suelo
11	A	RS485_A/D1/ Reloj	RS485señal no inversora
12	B	RS485_B/D0/ Datos	RS485señal inversora

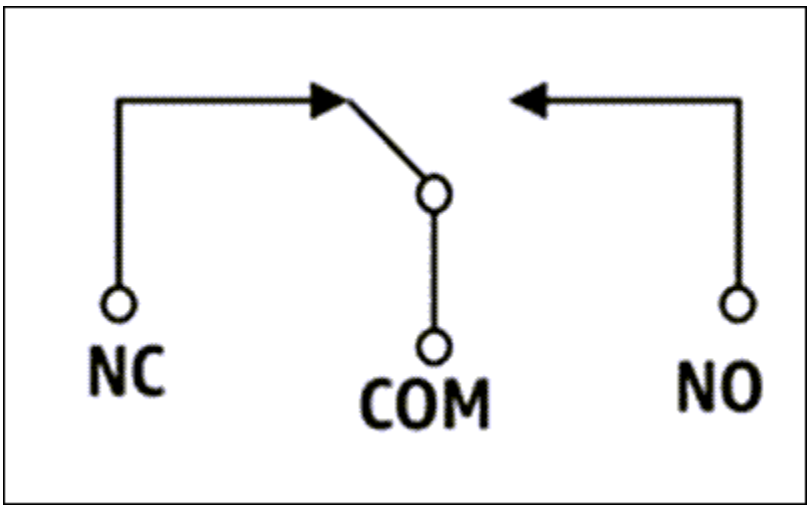
conexiones de relé

- Inserte el cable blanco en el pin 7 (COM).
- Inserte el cable naranja en el pin 8 (NC).
- Inserte el cable amarillo en el pin 9 (NO).



cableado del relé

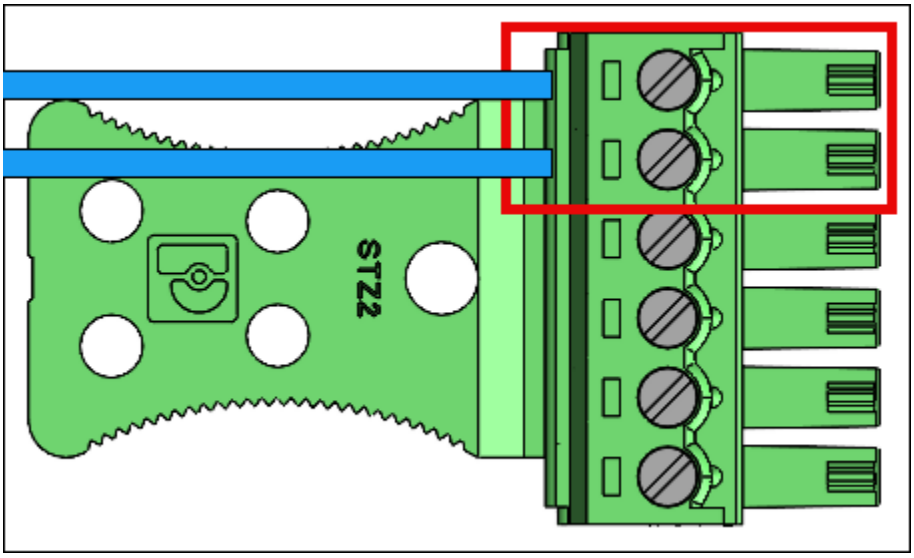
Pin	Connection	Descripción	Uso
7	COM	Relé común	Relé de contacto común: cable blanco
8	NC	Relé normalmente cerrado	Relé de contacto normalmente cerrado: cable naranja
9	NO	El relé está normalmente abierto	El relé de contacto está normalmente abierto: cable amarillo



El relé debe funcionar de acuerdo con las clasificaciones de seguridad especificadas de VAC 30/60VDC, 60 W como máximo.

Conexiones de entrada/salida digitales

- Inserte el cable azul en el pin 1 (). GPO
- Inserte el cable azul en el pin 2 (GPI).



Pin	Connection	Descripción	Uso	
1	GPO	Salida de uso general	Señal de salida digital (5 V)	

Pin	Connection	Descripción	Uso	
2	GPI	Entrada de uso general	Señal de entrada digital (3.6 V — 5 V)	

- Las conexiones de entrada/salida digital deben funcionar como se indica.

Consulta Activación del dispositivo Amazon One para activar tu dispositivo Amazon One.

Instalación del hub de E/S de dispositivos Amazon One para un acceso seguro

En esta sección se detallan los requisitos de ubicación y los pasos necesarios para instalar tu dispositivo Amazon One Enterprise (AOE) con I/O Hub.

Antes de iniciar la instalación, asegúrese de lo siguiente:

- El dispositivo Amazon One con hub de E/S es solo para uso en interiores.
- Para alimentación a través de Ethernet (PoE++):

  Asegúrese de que esté disponible para su uso un conmutador IEEE 802.3bt (tipo 3) de clase 6 POE ++ o un inyector (tramo medio), que esté listado o certificado y cumpla con la norma 62368-1. IEC

  Utiliza únicamente un dispositivo Amazon One con una fuente PoE++ aprobada.

  La fuente PoE++ debe estar ubicada en el mismo edificio.

- Para una entrada de alimentación de 15 V DC, solo debes usar el dispositivo Amazon One con una fuente de alimentación aprobada de NEC clase 2 o con energía limitada que esté listada o certificada. Consulta la sección de corriente continua opcional que aparece a continuación.

Herramientas necesarias:

- Pelacables
- Destornillador Phillips #2

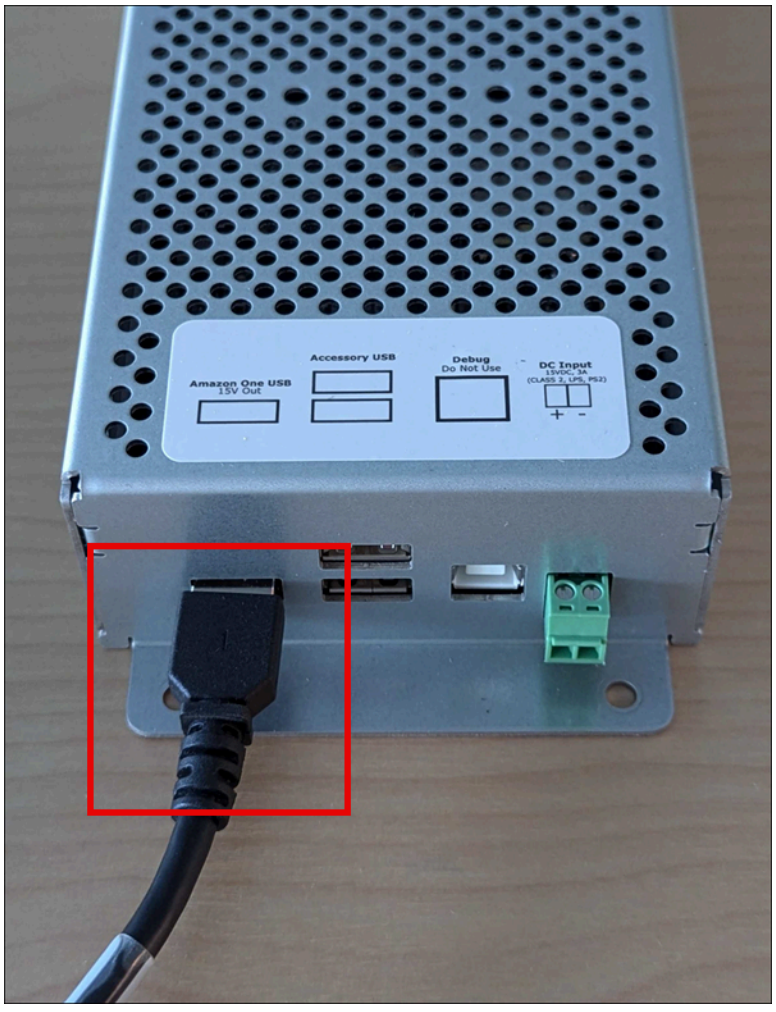
- Destornillador de cabeza plana de 0,5 mm x 2 mm

Incluido con el dispositivo Amazon One con hub de E/S:

- 2 conectores de bloque de terminales de 6 posiciones
- Conector DC
- Cable de alimentación/datos de 72 pulgadas

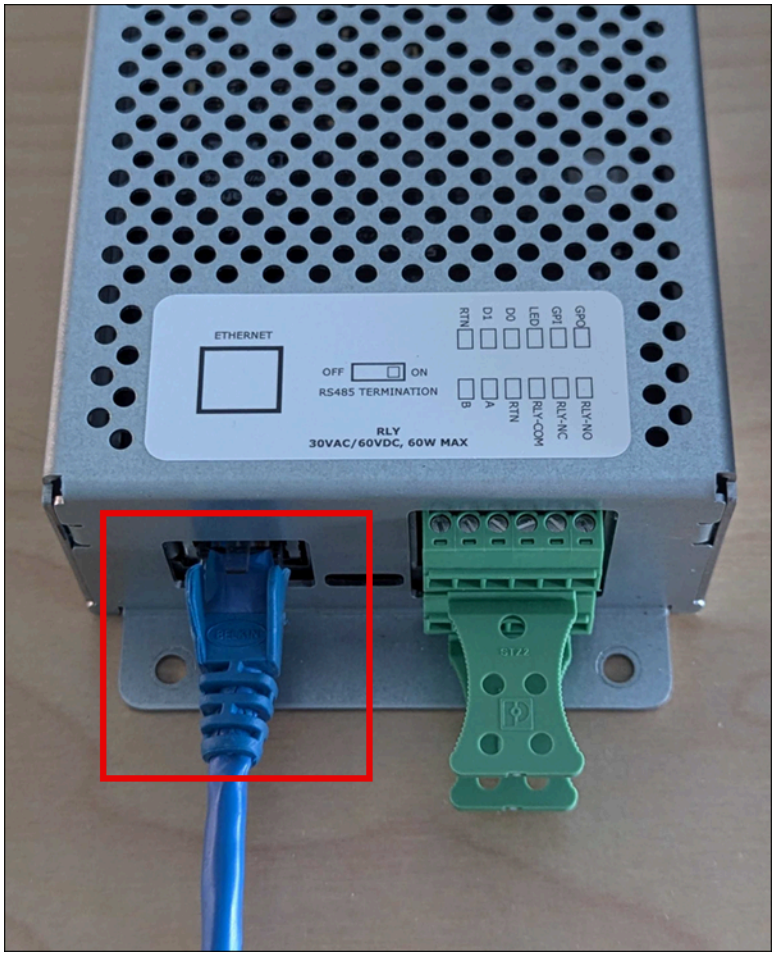
Para instalar el hub de E/S para tu dispositivo Amazon One

1. Saca tu dispositivo Amazon One con I/O Hub del embalaje.
2. Fije el hub de E/S en la ubicación deseada.
3. Conecta el USB cable Amazon One al puerto del hub de E/S.



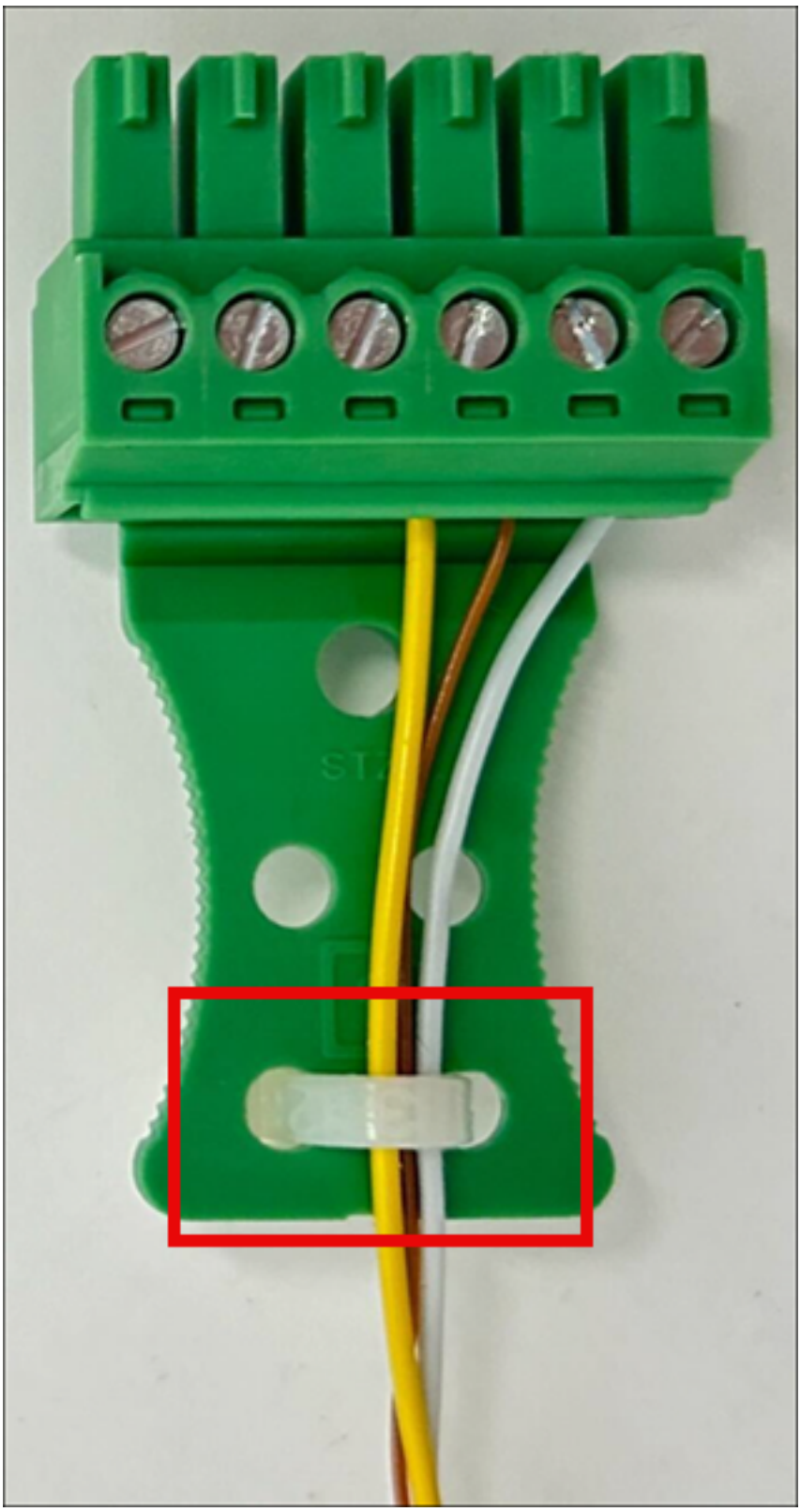
4. Para la alimentación POE ++, conecte el cable Ethernet de la fuente POE ++ al puerto del hub de E/S.

   Opcional: para la alimentación de corriente continua, consulte la sección de instalación del cableado de corriente continua que aparece a continuación.



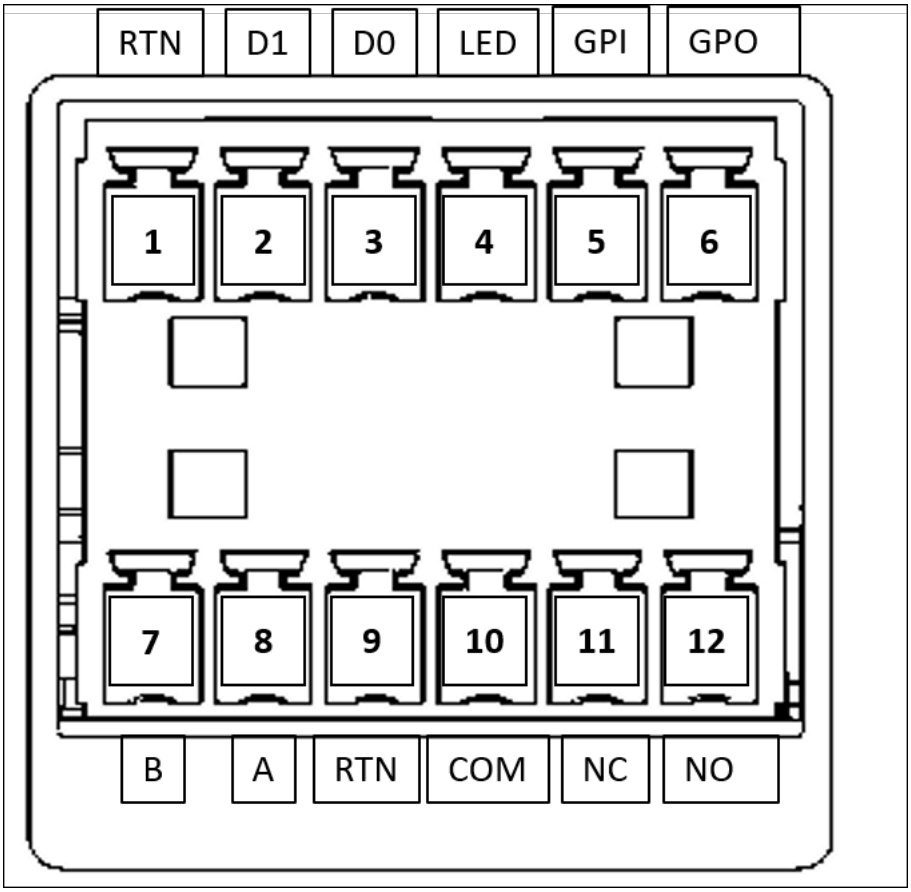
Para conectar el hub de E/S de tu dispositivo Amazon One

- Instale un circuito de goteo para evitar que los líquidos corran accidentalmente por el cable y entren en el hub de E/S.
- Coloque una pinza limitadora de tensión para proteger los cables de daños o tensiones, como se muestra en la siguiente imagen.



1. Inserte solo los cables necesarios para su aplicación a través de los enchufes del bloque de terminales. Consulte la tabla y los diagramas de cableado siguientes.

2. Inserte los enchufes del bloque de terminales en el hub de E/S.

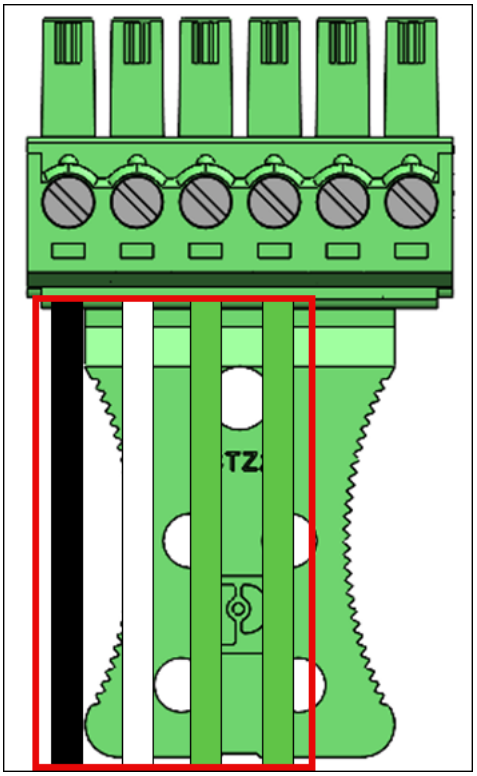


Pin	Connection	Descripción	Uso	
1	RTN	Retorno de señal	Wiegand Ground — Cable negro	
2	D1	Wiegand D1	Wiegand Data 1 — Cable blanco	
3	D0	Wiegand D0	Datos de Wiegand 0 — Cable verde	
4	LED	Wiegand LED	Wiegand — Opcional LED	

Pin	Connection	Descripción	Uso	
5	GPI	Entrada de uso general	Señal de entrada digital: opcional	
6	GPO	Salida de uso general	Señal de salida digital: opcional	
7	B	RS485_B/D0/ Data	OSDPD0 — Cable verde	
8	A	RS485_A/D1/ Reloj	OSDPD1 — Cable blanco	
9	RTN	Retorno de señal	OSDPretorno — Cable negro	
10	COM	Relé común	Relé de contacto común: cable blanco	
11	NC	Relé normalmente cerrado	Relé de contacto normalmente cerrado: cable naranja	
12	NO	El relé está normalmente abierto	El relé de contacto normalmente está abierto: cable amarillo	

Conexiones Wiegand

- Inserte el cable negro en el pin 1 ()RTN.
- Inserte el cable blanco en el pin 2 (D1).
- Inserte el cable verde en el pin 3 (D0).
- Opcional: inserte el cable verde en el pin 4 (LED).



Conexiones de rel

- Inserte el cable blanco en el pin 10 (COM).
- Inserte el cable naranja en el pin 11 (NC).
- Inserte el cable amarillo en el pin 12 (NO).

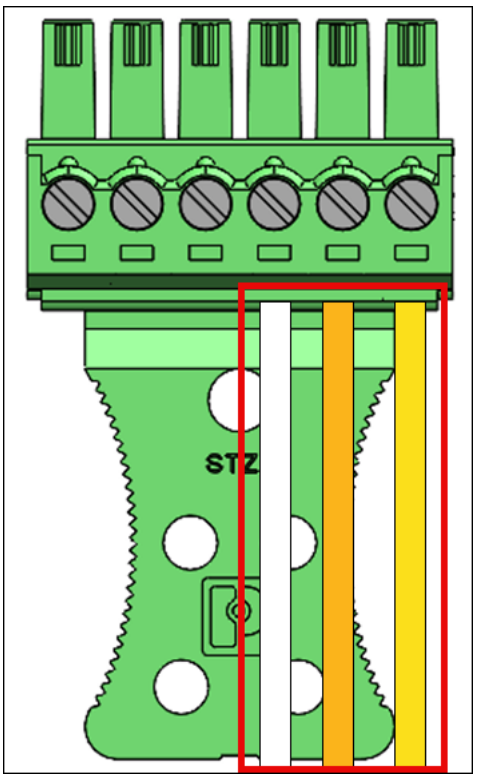
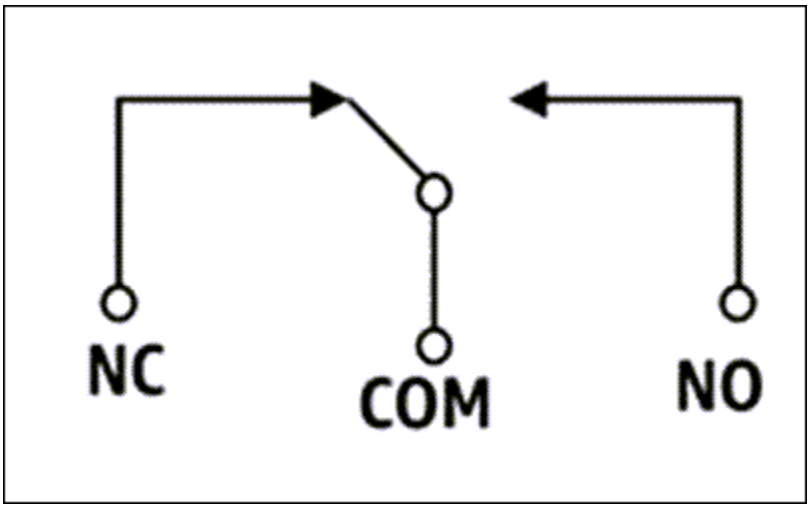


Diagrama de relés

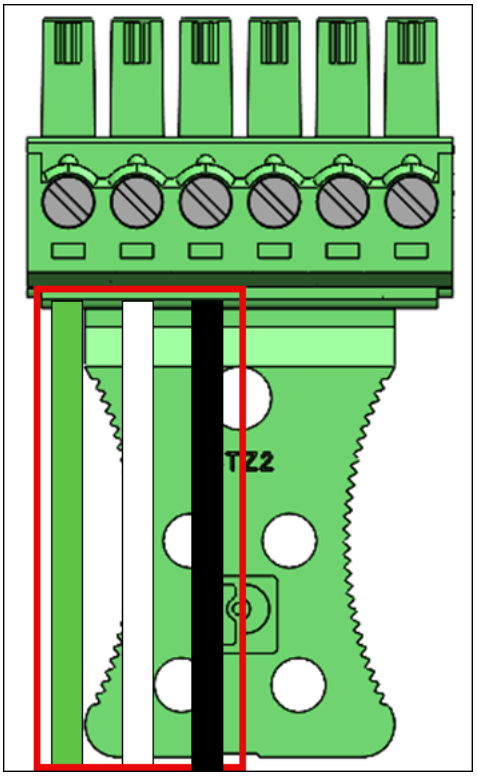


El relé debe funcionar de acuerdo con las clasificaciones de seguridad especificadas de VAC 30/60VDC, 60 W como máximo.

RS485conexiones

- Introduzca el cable verde en el pin 7 (B).
- Inserte el cable blanco en el pin 8 (A).

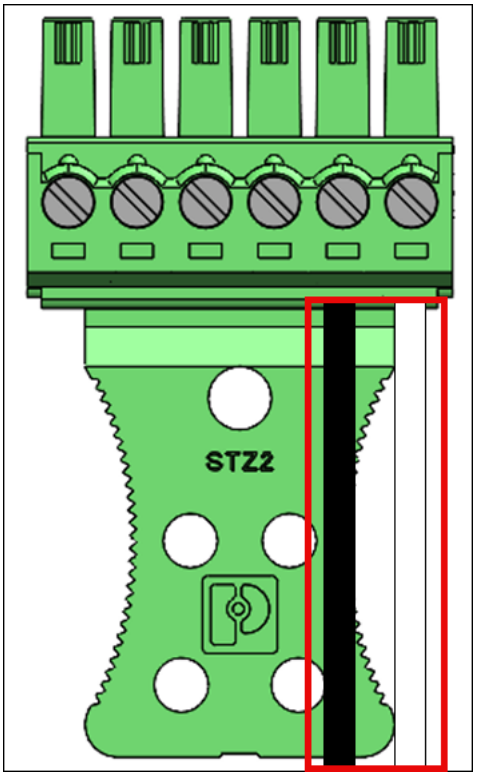
- Inserte el cable negro en el pin 9 (RTN).



Encienda el interruptor de RS485 terminación si el dispositivo es la última unidad de la línea. Este interruptor activa la terminación de una resistencia de 120 ohmios en la línea.

Conexiones de entrada/salida digitales

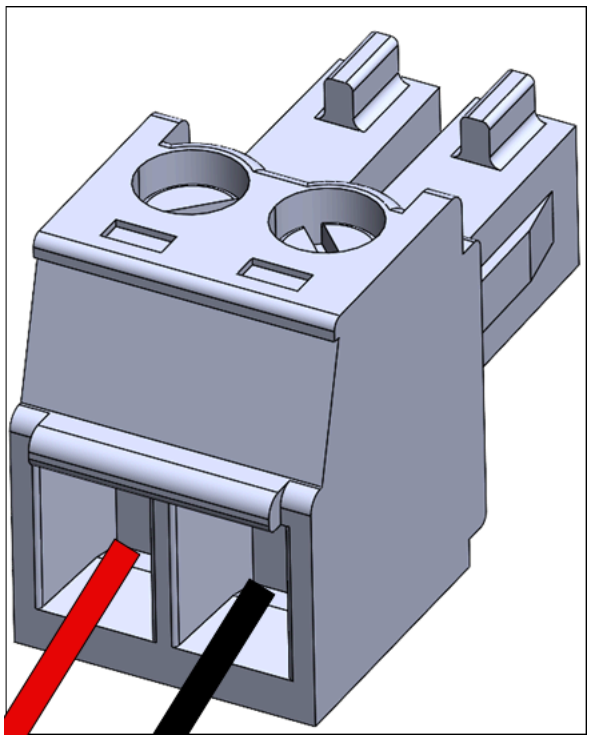
- Inserte el cable negro en el pin 5 (). GPI
- Inserte el cable blanco en el pin 6 (GPO).



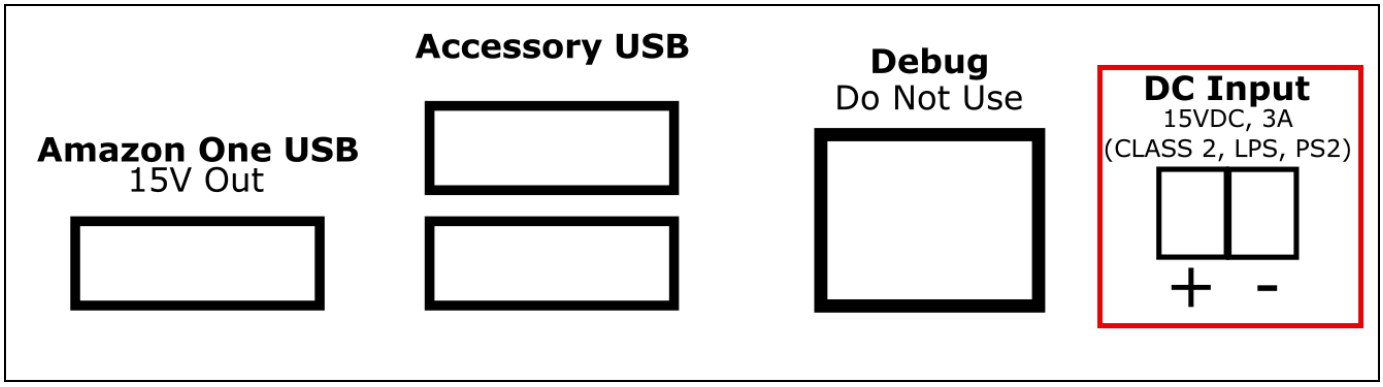
- Las conexiones de entrada/salida digital deben funcionar como se indica.

Opcional: para instalar el cableado de corriente continua

1. Quita 3 mm a 5 mm del extremo de un cable rojo para el positivo (+) y un cable negro para el negativo (-).
2. Inserte el extremo pelado del cable de corriente continua en el conector de corriente continua.



3. Atornille el cable en su posición.
4. Inserte el conector de corriente continua cableado en el puerto de entrada de corriente continua.



Activación del dispositivo Amazon One

Cuando tu dispositivo Amazon One esté instalado y encendido, estarás listo para activarlo.

Para activar tu dispositivo Amazon One

1. En el dispositivo Amazon One, toca la pantalla para empezar.
2. Elige Ethernet o Wifi para conectarte a Internet.

Tan pronto como el dispositivo se conecte a Internet, empezará a descargar el paquete de software más reciente.

3. ¡Cuando la pantalla muestre que se ha completado la descarga del software! , selecciona OK.
4. Selecciona el código QR.

   La pantalla del dispositivo Amazon One mostrará Escanear código QR.
5. Para recuperar el código QR de activación, abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.

   > **Note**
   >
   > Te recomendamos encarecidamente que concedas un permiso limitado a tus instaladores para que solo tengan acceso a los códigos QR de activación en tu consola de Amazon One Enterprise. Consulte Paso 2: Añadir usuarios de Amazon One Enterprise.
6. En el panel de navegación, selecciona Códigos QR de activación.
7. En la lista desplegable Selecciona un sitio, selecciona el sitio en el que está instalado el dispositivo Amazon One.
8. En Información del sitio, confirma la dirección del sitio.
9. En Códigos QR de activación, busca el nombre de la instancia del dispositivo que estás activando y selecciona la opción Obtener código QR correspondiente para recuperar el código QR.
10. Escanea el código QR con el dispositivo Amazon One.
11. Cuando la pantalla del dispositivo Amazon One muestre ¡Activación completa! , el dispositivo está listo para su uso.

Inscripción e ingreso

Ahora que tu dispositivo Amazon One está activado, tus empleados pueden empezar a registrar sus palmas de las manos y autenticarlas para poder acceder.

Temas

- Inscripción de usuarios

Inscripción de usuarios

Antes de que los usuarios puedan autenticar sus manos para poder entrar, deberán pasar por el proceso de inscripción. El personal de seguridad siempre debe comprobar la identidad del usuario antes de permitir que el usuario se inscriba.

Para inscribir tus palmas en un dispositivo Amazon One

1. En el dispositivo de inscripción Amazon One Enterprise, presiona Comenzar.
2. Escanea una credencial de empleado con el escáner de credenciales que está conectado a tu dispositivo de inscripción Amazon One Enterprise.

   Cuando la insignia se escanea correctamente, la pantalla del dispositivo Amazon One muestra la insignia escaneada.
3. Lee las condiciones de uso y, a continuación, pulsa OK.
4. Lee detenidamente Consentimiento: la información biométrica de tu palma y pulsa Acepto si das tu consentimiento.
5. Siga las instrucciones que aparecen en pantalla para completar el proceso de inscripción.

Autenticate para entrar

Una vez que hayas registrado correctamente tus palmas, estarás listo para autenticarte con ellas en tu dispositivo de entrada Amazon One Enterprise.

Para autenticar la palma de la mano para entrar en un dispositivo Amazon One

- Coloca la palma de la mano sobre el dispositivo y sigue las instrucciones que aparecen en pantalla para escanearla.

Administración de usuarios inscritos

Puedes usar la página de administración de usuarios inscritos para realizar un seguimiento de los usuarios inscritos y eliminar los datos biométricos de los usuarios. Un usuario cuyos datos biométricos asociados se eliminen ya no tendrá acceso a los dispositivos Amazon One para su autenticación.

Para ver los usuarios inscritos

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, seleccione Administración de usuarios inscritos.
3. En Usuarios inscritos, encontrará todos los usuarios inscritos y los siguientes detalles:
   - ID de credencial: información sobre el identificador de la RFID credencial capturada por un lector de credenciales en el momento de la inscripción.
   - Fuente de inscripción: detalles del dispositivo Amazon One que se utilizó para la inscripción.
   - Fecha de inscripción: fecha y hora de inscripción.

Para eliminar los usuarios inscritos y sus datos biométricos

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, seleccione Administración de usuarios inscritos.
3. En Usuarios inscritos, seleccione el identificador del usuario cuyos datos biométricos de la palma de la mano desee eliminar.
4. Selecciona Eliminar datos biométricos.
5. Seleccione Eliminar para confirmar la eliminación de los datos biométricos del usuario.

> **Important**
>
> Esta acción tiene como resultado la eliminación permanente de los datos biométricos de la palma de un usuario de Amazon One Enterprise. El usuario tendrá que volver a inscribirse con un dispositivo de inscripción de Amazon One Enterprise para poder utilizar Amazon One Enterprise para la autenticación. Al eliminar los datos biométricos de un usuario, también se eliminarán permanentemente otros atributos del perfil, como el identificador de la insignia, de Amazon One Enterprise.

Administración de dispositivos

Una vez instalado y activado el dispositivo Amazon One, comienza a informar sobre el estado del dispositivo en la consola Amazon One Enterprise. Puede usar la consola Amazon One Enterprise para realizar tareas de administración de dispositivos, como reiniciar dispositivos o actualizar configuraciones.

Temas

Administración del sitio

Un sitio representa una ubicación física en la que se instala y funciona un conjunto de instancias de dispositivos. Puedes usar sitios para organizar los dispositivos de Amazon One que comparten la misma dirección física.

Para cambiar el nombre del sitio

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, selecciona Sitio.
3. En Sitios, seleccione el sitio cuyo nombre desee editar.
4. Elija Editar.
5. En Información del sitio, introduzca el nombre y la descripción del sitio que desee (opcional).
6. Selecciona Guardar cambios para actualizarlos.

Para actualizar la dirección del sitio

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, selecciona Sitio.
3. En Sitios, seleccione el sitio cuya dirección desee actualizar.
4. En Instancias de dispositivos, asegúrese de que el número de instancias activadas sea 0.
5. (Opcional) Si el número de instancias activadas no es 0, consulte Para desactivar las instancias del dispositivo
6. Elija Editar.
7. En Dirección física, introduzca la dirección física correcta.
8. Selecciona Guardar cambios para actualizarlos.

Administración de instancias de dispositivos

Una instancia de dispositivo es una representación lógica de un dispositivo con configuraciones. El uso de instancias de dispositivos permite intercambiar dispositivos de Amazon One y, al mismo tiempo, heredar automáticamente las configuraciones y los nombres establecidos anteriormente. Una instancia de dispositivo tiene un nombre definido por el usuario (convención de nomenclatura compartida con el software de control de acceso) y un conjunto de configuraciones de comunicación.

Para ver el estado de la instancia del dispositivo

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, elija Device instance.
3. En Instancias activadas, verás una lista de dispositivos Amazon One activados.
4. Elige un nombre de instancia de dispositivo para ver los detalles de la instancia de dispositivo.

Para reiniciar un dispositivo Amazon One

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, elija Device instance.
3. En Instancias activadas, elige el nombre de la instancia del dispositivo que quieres reiniciar.
4. Selecciona Reiniciar para reiniciar el dispositivo Amazon One.

Para actualizar las configuraciones de los dispositivos Amazon One

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, elija Device instance.
3. En Instancias activadas, elija el nombre de la instancia del dispositivo que desee actualizar.
4. En Configuraciones de dispositivos, selecciona Editar.

> **Note**
>
> Para cambiar el modo de dispositivo de Amazon One, primero debe desactivar la instancia del dispositivo y, a continuación, configurarla con el modo de dispositivo deseado (consultePaso 6: Configurar una instancia de dispositivo para su activación).

Luego, puede realizar el proceso de activación del dispositivo (consulteActivación del dispositivo Amazon One).

5. Una vez realizados los cambios deseados, selecciona Actualizar las configuraciones del dispositivo para confirmar la actualización.

Para actualizar las credenciales de WiFi

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, elija Device instance.
3. En Instancias activadas, elija el nombre de la instancia del dispositivo que desee actualizar.
4. En Red, selecciona Editar.
5. En Configuraciones de Wi-Fi, realiza los cambios que desees.
6. Selecciona Actualizar red para confirmar la actualización.

Para desactivar las instancias del dispositivo

1. Abra la consola de Amazon One Enterprise en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, elija Device instance.
3. En Instancias activadas, seleccione el nombre de la instancia del dispositivo que desee desactivar.
4. Selecciona Desactivar dispositivo.
5. Para confirmar la desactivación, escribe «desactivar» en el cuadro de mensaje y selecciona Desactivar dispositivo.

Seguridad en Amazon One Enterprise

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon One Enterprise, consulte AWS Servicios incluidos en el ámbito del programa de conformidad AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Amazon One Enterprise. En los temas siguientes se muestra cómo configurar Amazon One Enterprise para cumplir sus objetivos de seguridad y conformidad. También aprenderás a usar otros AWS servicios que te ayudan a monitorear y proteger tus recursos de Amazon One Enterprise.

Temas

Protección de datos en Amazon One Enterprise

La AWS modelo de responsabilidad compartida de se aplica a la protección de datos en Amazon One Enterprise. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable

de mantener el control sobre el contenido que está alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad del Servicios de AWS que utilices. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte la AWS Modelo de responsabilidad compartida y entrada de GDPR blog sobre AWS Blog de seguridad.

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UtiliceSSL/TLSpara comunicarse con AWS recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Trabajar con CloudTrail senderos en la AWS CloudTrail Guía del usuario.
- Uso AWS soluciones de cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder AWS a través de una interfaz de línea de comandos oAPI, utilice un FIPS punto final. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma Federal de Procesamiento de Información (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Amazon One Enterprise u otro Servicios de AWS usando la consolaAPI, AWS CLI, o AWS SDKs. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

Para utilizar el cifrado predeterminado de los datos en reposo

Amazon One Enterprise proporciona cifrado de forma predeterminada para proteger los datos confidenciales en reposo mediante claves de AWS cifrado.

AWSclaves propias: Amazon One Enterprise utiliza estas claves de forma predeterminada para cifrar automáticamente los datos confidenciales de los usuarios finales. No puede ver, administrar ni usar las claves AWS propias, ni auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulte las claves AWS propias en la Guía AWS para desarrolladores del Servicio de administración de claves.

Cifrado de datos en tránsito

Amazon One Enterprise utiliza Transport Layer Security (TLS) para proteger los datos y Signature Version 4 para autenticar todas las API solicitudes entrantes a AWS los servicios. Este cifrado está activado de forma predeterminada.

Administración de identidad y acceso para Amazon One Enterprise

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Amazon One Enterprise. IAMes un Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

Cómo se usa AWS Identity and Access Management (IAM) varía según el trabajo que realices en Amazon One Enterprise.

Usuario del servicio: si utilizas el servicio Amazon One Enterprise para realizar tu trabajo, el administrador te proporcionará las credenciales y los permisos que necesitas. A medida que vaya utilizando más funciones de Amazon One Enterprise para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de Amazon One Enterprise, consulteSolución de problemas de identidad y acceso a Amazon One Enterprise.

Administrador de servicios: si está a cargo de los recursos de Amazon One Enterprise en su empresa, probablemente tenga acceso completo a Amazon One Enterprise. Es su trabajo determinar a qué funciones y recursos de Amazon One Enterprise deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Amazon One Enterprise, consulteCómo funciona Amazon One Enterprise con IAM.

IAMadministrador: si es IAM administrador, puede que desee obtener más información sobre cómo puede redactar políticas para administrar el acceso a Amazon One Enterprise. Para ver ejemplos de políticas basadas en la identidad de Amazon One Enterprise que puede utilizarIAM, consulte. Ejemplos de políticas basadas en identidad para Amazon One Enterprise

Autenticación con identidades

La autenticación es la forma de iniciar sesión en AWS utilizando tus credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como IAM usuario o asumiendo un IAM rol.

Puede iniciar sesión en AWS como identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios de (IAMIdentity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accedes AWS al usar la federación, está asumiendo un rol de manera indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el AWS Management Console o el AWS portal de acceso. Para obtener más información sobre cómo iniciar sesión en AWS, consulta Cómo iniciar sesión en tu Cuenta de AWS en la AWS Sign-In Guía del usuario.

Si accedes AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no usa AWS herramientas, debe firmar las solicitudes usted mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar AWS APIsolicitudes en la Guía IAM del usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo: AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la AWS IAM Identity Center Guía del usuario y Uso de la autenticación multifactorial () MFA en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Al crear un Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todas Servicios de AWS y los recursos de la cuenta. Esta identidad se denomina Cuenta de AWS usuario root y se accede a él iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web, AWS Directory Service, el directorio del Centro de identidades o cualquier usuario que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para la administración centralizada del acceso, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todos sus Cuentas de AWS y aplicaciones. Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en el AWS IAM Identity Center Guía del usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

IAMroles

Un IAMrol es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puede asumir un rol llamando a un AWS CLI o AWS APIoperación o mediante una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información sobre los conjuntos de permisos, consulte los conjuntos de permisos en la AWS IAM Identity Center Guía del usuario.
- Permisos de IAM usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del director que llama a un Servicio de AWS, combinado con la solicitud Servicio de AWS para realizar solicitudes a los servicios intermedios. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completar. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un Servicio de AWS. El servicio puede asumir la función de realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de las funciones vinculadas al servicio.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y se están creando AWS CLI o AWS APIsolicitudes. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS Un rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia que se adjunte a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

Usted controla el acceso en AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto en AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte Descripción general de JSON las políticas en la Guía del IAM usuario.

Los administradores pueden utilizar AWS JSONpolíticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre su función en AWS Management Console, el AWS CLI, o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su Cuenta de AWS. Las políticas gestionadas incluyen AWS las políticas gestionadas y las políticas gestionadas por el cliente. Para saber cómo elegir entre una política gestionada o una política en línea, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAMusuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar AWS políticas gestionadas desde una política basada IAM en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3, AWS WAF, y Amazon VPC son ejemplos de servicios que admitenACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades en la Guía del IAMusuario.
- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada múltiples Cuentas de AWS que es propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar las políticas de control de servicios (SCPs) a cualquiera de tus cuentas o a todas ellas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas todas Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte Políticas de control de servicios en la AWS Organizations Guía del usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determina si se permite una solicitud cuando se

trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

Cómo funciona Amazon One Enterprise con IAM

Antes de utilizar Amazon One Enterprise IAM para gestionar el acceso a Amazon One Enterprise, infórmese sobre las IAM funciones disponibles para su uso con Amazon One Enterprise.

IAMfunciones que puedes usar con Amazon One Enterprise

IAMcaracterística	Soporte para Amazon One Enterprise
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC(etiquetas en las políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general de cómo Amazon One Enterprise y otros AWS los servicios funcionan con la mayoría de IAM las funciones, consulte AWS servicios con los que funcionan IAM en la Guía IAM del usuario.

Políticas basadas en identidad para Amazon One Enterprise

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que puede adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Ejemplos de políticas basadas en identidad para Amazon One Enterprise

Para ver ejemplos de políticas basadas en la identidad de Amazon One Enterprise, consulte. Ejemplos de políticas basadas en identidad para Amazon One Enterprise

Políticas basadas en recursos en Amazon One Enterprise

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador

de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

Acciones políticas para Amazon One Enterprise

Compatibilidad con las acciones de política: sí

Los administradores pueden usar AWS JSONpolíticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que las asociadas AWS APIoperación. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Amazon One Enterprise, consulteAcciones, recursos y claves de condición para Amazon One Enterprise.

Las acciones políticas en Amazon One Enterprise usan el siguiente prefijo antes de la acción:

```
one
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

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

Para ver ejemplos de políticas basadas en la identidad de Amazon One Enterprise, consulte. Ejemplos de políticas basadas en identidad para Amazon One Enterprise

Recursos de políticas para Amazon One Enterprise

Compatibilidad con los recursos de políticas: sí

Los administradores pueden utilizar AWS JSONpolíticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Amazon One Enterprise y sus ARNs respectivos tipos de recursos y saber qué acciones puede utilizar para especificar cada recurso, consulteAcciones, recursos y claves de condición para Amazon One Enterprise. ARN

Para ver ejemplos de políticas basadas en la identidad de Amazon One Enterprise, consulte. Ejemplos de políticas basadas en identidad para Amazon One Enterprise

Claves de condición de la política para Amazon One Enterprise

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar AWS JSONpolíticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones

condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios `Condition` elementos en una declaración o varias claves en un solo `Condition` elemento, AWS los evalúa mediante una `AND` operación lógica. Si especifica varios valores para una sola clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas AWS claves de condición globales, consulte AWS claves de contexto de condiciones globales en la Guía IAM del usuario.

Para ver una lista de claves de condición de Amazon One Enterprise y saber con qué acciones y recursos puede usar una clave de condición, consulteAcciones, recursos y claves de condición para Amazon One Enterprise.

Para ver ejemplos de políticas basadas en la identidad de Amazon One Enterprise, consulte. Ejemplos de políticas basadas en identidad para Amazon One Enterprise

ACLsen Amazon One Enterprise

SoportaACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

ABACcon Amazon One Enterprise

Soportes ABAC (etiquetas en las políticas): Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchas AWS recursos. Etiquetar entidades

y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

Uso de credenciales temporales con Amazon One Enterprise

Compatibilidad con credenciales temporales: sí

Alguno Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluyendo qué Servicios de AWS trabaje con credenciales temporales, consulte Servicios de AWS que funcionan IAM en la Guía IAM del usuario.

Está utilizando credenciales temporales si inicia sesión en AWS Management Console utilizando cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de su empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de rol, consulte Cambiar a un rol (consola) en la Guía del IAMusuario.

Puede crear credenciales temporales manualmente mediante el AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para Amazon One Enterprise

Admite sesiones de acceso directo (FAS): Sí

Cuando utiliza un IAM usuario o un rol para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del director que llama a un Servicio de AWS, combinado con la solicitud Servicio de AWS para realizar solicitudes a los servicios intermedios. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completar. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.

Funciones de servicio para Amazon One Enterprise

Compatible con roles de servicio: No

Una función de servicio es una IAMfunción que asume un servicio para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon One Enterprise. Edita las funciones de servicio solo cuando Amazon One Enterprise te dé instrucciones para hacerlo.

Funciones vinculadas a servicios para Amazon One Enterprise

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir la función de realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de las funciones vinculadas al servicio.

Para obtener más información sobre la creación o la administración de funciones vinculadas a un servicio, consulte AWS servicios con los que funcionan. IAM Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Amazon One Enterprise

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de Amazon One Enterprise. Tampoco pueden realizar tareas mediante el AWS Management Console, AWS Command Line Interface (AWS CLI), o AWS API. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon One Enterprise, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición para Amazon One Enterprise la Referencia de autorización de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de Amazon One Enterprise de su cuenta. Estas acciones pueden suponer costes para su Cuenta de AWS. Al crear o editar políticas basadas en la identidad, siga estas directrices y recomendaciones:

- Comience con AWS políticas gestionadas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice la AWS políticas

gestionadas que conceden permisos para muchos casos de uso habituales. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo AWS políticas gestionadas por el cliente que sean específicas para sus casos de uso. Para obtener más información, consulte AWS políticas gestionadas o AWS políticas gestionadas para las funciones laborales en la Guía IAM del usuario.

- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puede utilizar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de un procedimiento específico Servicio de AWS, como, por ejemplo, AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si tiene un escenario que requiere IAM usuarios o un usuario raíz en su Cuenta de AWS, actívala MFA para mayor seguridad. Para solicitarlo MFA cuando se cancelen API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.

Uso de la consola Amazon One Enterprise

Para acceder a la consola de Amazon One Enterprise, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Amazon One

Enterprise en su Cuenta de AWS. Si creas una política basada en la identidad que sea más restrictiva que los permisos mínimos requeridos, la consola no funcionará según lo previsto para las entidades (usuarios o roles) que cuenten con esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas al AWS CLI o el AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de Amazon One Enterprise, conecte también Amazon One Enterprise *ConsoleAccess* o *ReadOnly* AWS política gestionada para las entidades. Para obtener más información, consulte Añadir permisos a un usuario en la Guía del IAM usuario.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante el AWS CLI o AWS API.

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

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acceso de solo lectura a Amazon One Enterprise

El siguiente ejemplo muestra un AWS política gestionada, `AmazonOneEnterpriseReadOnlyAccess` que concede acceso de solo lectura a Amazon One Enterprise.

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

En las declaraciones de políticas, el elemento `Effect` especifica si las acciones se permiten o se niegan. El elemento `Action` enumera las acciones específicas que puede realizar el usuario. El `Resource` elemento enumera las AWS recursos en los que el usuario puede realizar esas acciones. En el caso de las políticas que controlan el acceso a las acciones de Amazon One Enterprise, el `Resource` elemento siempre se establece en`*`, un comodín que significa «todos los recursos».

Los valores del `Action` elemento corresponden a los APIs que admiten los servicios. Las acciones van precedidas `config:` para indicar que se refieren a acciones de Amazon One Enterprise. Puede utilizar el carácter comodín `*` en el elemento `Action`, como en los siguientes ejemplos:

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

  Esto permite todas las acciones de Amazon One Enterprise que terminen en DeviceInstance "" (`GetDeviceInstanceConfiguration`,`CreateDeviceInstanceConfiguration`).

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

  Esto permite todas las acciones de Amazon One Enterprise, pero no las acciones de otras AWS servicios.

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

  Esto permite que todos AWS acciones. Este permiso es adecuado para un usuario que actúa como AWS administrador de su cuenta.

La política de solo lectura no concede permisos al usuario para realizar acciones como `CreateDeviceInstanceUpdateDeviceInstance`, y. `DeleteDeviceInstance` Los usuarios con esta política no pueden crear una instancia de dispositivo, actualizar una instancia de dispositivo ni eliminar una instancia de dispositivo. Para ver la lista de acciones de Amazon One Enterprise, consulteAcciones, recursos y claves de condición para Amazon One Enterprise.

Acceso completo a Amazon One Enterprise

El siguiente ejemplo muestra una política que concede acceso total a Amazon One Enterprise. Otorga a los usuarios el permiso para realizar todas las acciones de Amazon One Enterprise.

> **Important**
>
> Esta política otorga amplios permisos. Antes de otorgar acceso total, es recomendable empezar con un conjunto mínimo de permisos y otorgar permisos adicionales según sea necesario. Por lo general, es más seguro que comenzar con permisos que son demasiado tolerantes y querer restringirlos más adelante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "one:*"
            ],
            "Resource": "*"
        },
    ]
}
```

Permisos a nivel de recursos compatibles para las acciones de reglas de Amazon One Enterprise API

Los permisos de nivel de recursos hacen referencia a la capacidad de especificar en qué recursos los usuarios tienen permitido realizar acciones. Amazon One Enterprise admite permisos a nivel de recursos para determinadas acciones de reglas API de Amazon One Enterprise. Esto significa que, para determinadas acciones de reglas de Amazon One Enterprise, puedes controlar las condiciones en las que los usuarios pueden usar esas acciones. Estas condiciones pueden ser acciones que se deben cumplir o recursos específicos que los usuarios pueden utilizar.

En la siguiente tabla se describen las API acciones de las reglas de Amazon One Enterprise que actualmente admiten permisos a nivel de recursos. También describe los recursos admitidos y los ARNs correspondientes a cada acción. Al especificar un recursoARN, puede utilizar el comodín * en sus rutas; por ejemplo, cuando no puede o no quiere especificar un recurso IDs exacto.

> **Important**
>
> Si una API acción de regla de Amazon One Enterprise no aparece en esta tabla, significa que no admite permisos a nivel de recursos. Si una acción de regla de Amazon One Enterprise no admite permisos a nivel de recursos, puedes conceder permisos a los usuarios para que usen la acción, pero tendrás que especificar un asterisco (*) para el elemento de recurso de tu declaración de política.

APIAcción	Recursos
CreateDeviceInstance	Instancia de dispositivo arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId*
GetDeviceInstance	Instancia de dispositivo

APIAcción	Recursos
	arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId*
UpdateDeviceInstance	Instancia de dispositivo arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId*
DeleteDeviceInstance	Instancia de dispositivo arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId*
CreateDeviceActivationQrCode	Instancia de dispositivo arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId*
DeleteAssociatedDevice	Instancia de dispositivo arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId*
RebootDevice	Instancia de dispositivo arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId*
CreateDeviceInstanceConfiguration	Configuración de instancia de dispositivo arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId* /configuración/*version*
GetDeviceInstanceConfiguration	Configuración de instancias de dispositivos arn:aws:one:*region:accountID* : instancia de dispositivo/*deviceInstanceId* /configuración/*version*

APIAcción	Recursos
CreateSite	Sitio arn:aws:one:*region:accountID* :sitio/*siteId*
DeleteSite	Sitio arn:aws:one:*region:accountID* :sitio/*siteId*
GetSiteAddress	Sitio arn:aws:one:*region:accountID* :sitio/*siteId*
UpdateSite	Sitio arn:aws:one:*region:accountID* :sitio/*siteId*
UpdateSiteAddress	Sitio arn:aws:one:*region:accountID* :sitio/*siteId*
CreateDeviceConfigurationTemplate	Plantilla de configuración del dispositivo arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
DeleteDeviceConfigurationTemplate	Plantilla de configuración del dispositivo arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
GetDeviceConfigurationTemplate	Plantilla de configuración del dispositivo arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
UpdateDeviceConfigurationTemplate	Plantilla de configuración del dispositivo arn:aws:one:*region:accountID* :device-configuration-template/*templateId*

Por ejemplo, desea permitir a usuarios específicos el acceso de lectura y denegar el acceso de escritura a reglas específicas.

En la primera política, permites que AWS Config la regla lee acciones como las `GetSite` de las reglas especificadas.

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

En la segunda política, deniegas las acciones de escritura de la regla Amazon One Enterprise sobre la regla específica.

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

Con los permisos a nivel de recursos, puede permitir el acceso de lectura y denegar el acceso de escritura para realizar acciones específicas en las acciones de reglas API de Amazon One Enterprise.

Información adicional

Para obtener más información sobre la creación de IAM usuarios, grupos, políticas y permisos, consulte Creación de su primer grupo de IAM usuarios y administradores y administración de acceso en la Guía del IAMusuario.

AWS políticas gestionadas para Amazon One Enterprise

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando haya nuevas API operaciones disponibles para los servicios existentes.

Para obtener más información, consulte las políticas AWS administradas en la Guía del IAM usuario.

AmazonOneEnterpriseFullAccess

Esta política otorga permisos administrativos que permiten el acceso a todos los recursos y operaciones de Amazon One Enterprise.

`one:*`Le permite realizar todas las acciones de Amazon One Enterprise.

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

AmazonOneEnterpriseReadOnlyAccess

Esta política concede permisos de solo lectura a todos los recursos y operaciones de Amazon One Enterprise.

`one:Get*`Obtiene los recursos de Amazon One Enterprise.

`one:List*`Muestra los recursos de Amazon One Enterprise.

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

AmazonOneEnterpriseInstallerAccess

Esta política otorga permisos de lectura y escritura limitados que le permiten crear un código QR de activación para cualquier instancia de dispositivo configurada para activar el dispositivo en cualquier sitio.

`one:CreateDeviceActivationQrCode`Le permite crear un código QR para activar el dispositivo.

`one:GetDeviceInstance`Te permite obtener la información sobre una instancia de dispositivo de Amazon One.

`one:GetSite`Te permiten buscar la información sobre un sitio de Amazon One Enterprise.

`one:GetSiteAddress`Te permite buscar la dirección física de un sitio de Amazon One Enterprise.

`one:ListDeviceInstances`Te permite enumerar las instancias de dispositivos de Amazon One.

`one:ListSites`Te permite enumerar los sitios de 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 actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon One Enterprise que se han realizado desde que este servicio comenzó a realizar el seguimiento de estos

cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase al RSS feed de la página del historial de documentos de Amazon One Enterprise.

Cambio	Descripción	Fecha
Amazon One Enterpris e comenzó a rastrear los cambios	Amazon One Enterpris e comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	1 de diciembre de 2023

Solución de problemas de identidad y acceso a Amazon One Enterprise

Usa la siguiente información para ayudarte a diagnosticar y solucionar problemas comunes que podrías encontrar al trabajar con Amazon One Enterprise yIAM.

Temas

- No estoy autorizado a realizar ninguna acción en Amazon One Enterprise
- Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mis recursos de Amazon One Enterprise

No estoy autorizado a realizar ninguna acción en Amazon One Enterprise

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver detalles sobre un *`my-example-widget`* recurso ficticio, pero no tiene los one:*`GetWidget`* permisos ficticios.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción one:*`GetWidget`*.

Si necesitas ayuda, ponte en contacto con tu AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mis recursos de Amazon One Enterprise

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon One Enterprise admite estas funciones, consulteCómo funciona Amazon One Enterprise con IAM.
- Para obtener información sobre cómo proporcionar acceso a sus recursos en Cuentas de AWS que te pertenezca, consulta Proporcionar acceso a un IAM usuario en otro Cuenta de AWS que le pertenezca en la Guía IAM del usuario.
- Para obtener información sobre cómo proporcionar acceso a sus recursos a terceros Cuentas de AWS, consulte Proporcionar acceso a Cuentas de AWS propiedad de terceros en la Guía IAM del usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. IAM

Acciones, recursos y claves de condición para Amazon One Enterprise

Amazon One Enterprise (prefijo de servicio:one) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en IAM las políticas de permisos.

Temas

- Acciones definidas por Amazon One Enterprise
- Tipos de recurso definidos por Amazon One Enterprise
- Claves de condición de Amazon One Enterprise

Acciones definidas por Amazon One Enterprise

Puede especificar las siguientes acciones en el `Action` elemento de una IAM declaración de política. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando se utiliza una acción en una política, normalmente se permite o deniega el acceso a la API operación o CLI comando con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar uno ARN de ese tipo en una declaración con esa acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el `Resource` elemento de una IAM política, debe incluir un patrón ARN o para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeviceInstance	Conceda permiso para crear una instancia de dispositivo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	Otorgue permiso para obtener información sobre la instancia del dispositivo	Leer	instancia de dispositivo*		
ListDeviceInstances	Otorgue permiso para enumerar instancias de dispositivos	Leer			
UpdateDeviceInstance	Otorgue permiso para actualizar la instancia del dispositivo	Escritura	instancia de dispositivo*		
DeleteDeviceInstance	Otorgue permiso para eliminar la instancia del dispositivo	Escritura	instancia de dispositivo*		
CreateDeviceActivationQrCode	Conceda permiso para crear un código QR para activar un dispositivo en una instancia de dispositivo	Escritura	instancia de dispositivo*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAssociatedDevice	Conceda permiso para eliminar la asociación entre el dispositivo y la instancia del dispositivo	Escritura	instancia de dispositivo*		
RebootDevice	Conceda permiso para reiniciar el dispositivo	Escritura	instancia del dispositivo*		
CreateDeviceInstanceConfiguration	Otorgue permiso para crear la configuración de instancias de dispositivos	Escritura			
GetDeviceInstanceConfiguration	Otorgue permiso para obtener información sobre la configuración de la instancia del dispositivo	Leer	configuración*		
CreateSite	Otorgar permiso para crear un sitio	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	Otorgue permiso para eliminar la instancia del dispositivo	Escritura	sitios*		
GetSite	Otorgue permiso para obtener información sobre el sitio	Leer	sitios*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSites	Otorgue permiso para publicar sitios	Leer			
GetSiteAddress	Otorgue permiso para obtener información sobre la dirección del sitio	Leer	sitios*		
UpdateSite	Otorgue permiso para actualizar el sitio	Escritura	sitios*		
UpdateSiteAddress	Otorgue permiso para actualizar la dirección del sitio	Escritura	sitios*		
CreateDeviceConfigurationTemplate	Otorgue permiso para crear una instancia de dispositivo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	Otorgue permiso para eliminar la plantilla de configuración del dispositivo	Escritura	device-configuration-template*		
GetDeviceConfigurationTemplate	Otorgue permiso para obtener información sobre la plantilla de configuración del dispositivo	Leer	device-configuration-template*		
ListDeviceConfigurationTemplates	Otorgue permiso para enumerar las plantillas de configuración de dispositivos	Leer			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDeviceConfigurationTemplate	Otorgue permiso para actualizar la plantilla de configuración del dispositivo	Escritura	device-configuration-template*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	instancia de dispositivo, sitio, device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	instancia de dispositivo, sitio, device-configuration-template	aws:TagKeys	
ListTagForResources	Concede permiso para enumerar las etiquetas de un recurso	Leer			

Tipos de recurso definidos por Amazon One Enterprise

Este servicio define los siguientes tipos de recursos y se pueden utilizar como `Resource` elemento de las declaraciones de política de IAM permisos. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede

definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
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}

Claves de condición de Amazon One Enterprise

Amazon One Enterprise define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una IAM política. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte Claves de condición globales disponibles.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante las etiquetas de la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso mediante las claves de etiqueta desde la solicitud	ArrayOfString

Validación de conformidad para Amazon One Enterprise

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

  > **Note**
  >
  > No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la Referencia de servicios HIPAA aptos.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.

- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Registro y supervisión de Amazon One Enterprise

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon One Enterprise y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar Amazon One Enterprise, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon se EventBridge puede utilizar para automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios de recursos. Los eventos de AWS los servicios se envían casi EventBridge en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.
- AWS CloudTrailcaptura API las llamadas y los eventos relacionados realizados por su AWS cuenta o en su nombre y envía los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Supervisión de los eventos de Amazon One Enterprise en Amazon EventBridge

Puede monitorear los eventos de Amazon One Enterprise en EventBridge, que ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones software-as-a-service (SaaS) y AWS servicios. EventBridgedirige esos datos a objetivos como AWS Lambda Amazon Simple Notification Service. Estos eventos proporcionan un flujo casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos.

Suscríbete a los eventos de Amazon One Enterprise

Los eventos de cambio de estado del dispositivo y del perfil de usuario de Amazon One se publican mediante EventBridge una nueva regla y se pueden activar en la EventBridge consola. Aunque los eventos no están ordenados, tienen una marca temporal que le permite consumir los datos. Los eventos se emiten en la medida de lo posible.

Para suscribirse a los eventos de Amazon One Enterprise

1. Abre la EventBridge consola en https://console.aws.amazon.com/events/.
2. En el panel de navegación, en Autobuses, elija Reglas.
3. Elija Crear regla.
4. En la página de detalles de la regla predeterminada, asigne un nombre a la regla, elija Regla con un patrón de eventos y, a continuación, elija Siguiente.
5. En la página Crear un patrón de eventos, en Origen del evento, compruebe que esté seleccionada la opción AWS Eventos o eventos EventBridge asociados.
6. En Ejemplo de tipo de evento, selecciona Introducir el mío.
7. Copia y pega desde uno de losEjemplos de eventos.
8. En Método de creación, elija Patrón personalizado. En la sección Patrón de eventos, añada un elemento JSON con la fuente del evento como **`aws:one`** y el tipo de detalle necesario y, a continuación, seleccione Siguiente.
9. En la página Seleccione los destinos, seleccione el destino que desee, que incluya una función, una SQS cola o un tema de Lambda. SNS Para obtener información sobre la configuración de los objetivos, consulta Amazon EventBridge targets.
10. Si lo desea, puede configurar las etiquetas.
11. En la página Revisar y crear, elija Crear regla. Para obtener más información sobre la configuración de reglas, consulte EventBridgelas reglas en la Guía del EventBridge usuario.

Tipos de eventos de cambio de estado del dispositivo

Los eventos de cambio de estado del dispositivo se generan enJSON. Para cada tipo de evento, se envía un JSON blob al destino que elijas, según lo configurado en la regla. Están disponibles los siguientes tipos de detalles:

El estado de salud del dispositivo cambió a saludable

: El dispositivo ha superado todos los controles de estado.

El estado de salud del dispositivo cambió a crítico

: El dispositivo no pasó una o más comprobaciones de estado.

La conectividad del dispositivo cambió a fuera de línea

: El dispositivo no está conectado a Internet.

La conectividad del dispositivo pasó a estar en línea

El dispositivo está conectado a Internet.

resources

Contiene la lista de los deviceInstance arn para los que se publicó el evento de cambio de estado del dispositivo.

metadatos

siteName

- Nombre del sitio en el que deviceInstance está presente.

siteArn

- Arn para el sitio en el que deviceInstance está presente.

datos

currentConnectivity

- Representa si deviceInstance está conectado o desconectado de Internet.
- Valores posibles:CONNECTED, DISCONNECTED

previousConnectivity

- Representa si deviceInstance estaba conectado o desconectado de Internet antes del evento.
- Valores posibles:CONNECTED, DISCONNECTED

currentHealthStatus

- Representa si deviceInstance ha pasado todos los controles de estado.
- Valores posibles:HEALTHY, CRITICAL

previousHealthStatus

- Representa si deviceInstance pasaron todos los controles de estado la última vez que se comprobaron.
- Valores posibles:HEALTHY, CRITICAL

assetTagId

- El assetTagId del dispositivo asociado aldeviceInstance.

deviceInstanceName

- El nombre del objeto deviceInstance para el que se publicó el evento de estado del dispositivo.

Tipos de eventos del perfil de usuario

Los tipos de detalles de eventos relacionados con el perfil de usuario son:

Nueva inscripción exitosa

Cuando un usuario se inscribió correctamente.

Nueva anulación exitosa de la inscripción

Cuando un usuario se dio de baja correctamente.

Inscripción fallida

Cuando un usuario no se pudo inscribir.

Anulación de la inscripción fallida

Cuando un usuario no pudo anular la inscripción.

Reconocimiento exitoso

Cuando un usuario escanea la palma de la mano para comprobar si se ha autenticado correctamente.

Reconocimiento fallido

Cuando falló el reconocimiento de un escáner de la palma de la mano.

resources

Contiene la lista de los campos de perfil de usuario para los que se publicó el evento del perfil de usuario.

datos

accountId

- La AWS cuenta correspondiente al dispositivo que inició la solicitud.

requestSource

- Es la deviceInstanceId del dispositivo que inició la solicitud.

createdTimestamp

- La hora en que se está creando el evento.

userStatus

- El estado actual del usuario.
- Valores posibles:ACTIVE, DELETED

associatedId

- El identificador asociado del usuario, por ejemplo, el identificador de la insignia.

reason

- Este valor se presentará en los eventos fallidos. Contiene el motivo por el que el evento no tuvo éxito.

Ejemplos de eventos

En los siguientes ejemplos se muestran los eventos de Amazon One Enterprise.

Temas

El estado de salud del dispositivo ha cambiado a saludable

El dispositivo pasó a estar en buen estado y el estado de salud de la instancia del dispositivo cambió a estado HEALTHY de CRITICAL salud anterior.


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

El estado de salud del dispositivo cambió a crítico

El dispositivo no pasó una o más comprobaciones de estado y el estado de salud de la instancia del dispositivo cambió a CRITICAL deHEALTHY.

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

```
}
```

La conectividad del dispositivo pasó a estar en línea

El dispositivo está conectado a Internet y el estado de conectividad de la instancia del dispositivo ha cambiado a CONNECTED deDISCONNECTED.

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

La conectividad del dispositivo cambió a fuera de línea

El dispositivo no está conectado a Internet y el estado de conectividad de la instancia del dispositivo ha cambiado a DISCONNECTED deCONNECTED.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Offline",
  "source": "aws.one",
  "account": "123456789012",
```

```
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "DISCONNECTED",
      "previousConnectivity": "CONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

La nueva inscripción se ha realizado correctamente

Un evento en el que un usuario se ha inscrito correctamente.

```
{
    "version": "0",
    "id": "aebc9c86-f20e-75db-caaa-63bf14926f59",
    "detail-type": "New Successful Enrollment",
    "source": "aws.one",
    "account": "679792848029",
    "time": "2023-11-22T02:55:17Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:one:us-east-1:679792848029:user"
    ],
    "detail": {
        "version": "1.0.0",
        "data": {
            "accountId": "679792848029",
            "enrollmentSource": "QfUuUnFqs5accJ",
            "createdTimestamp": "2023-11-22T02:55:17Z",
            "userStatus": "ACTIVE",
            "associatedIds": "[{\"associatedIdType\":\"badge\",\"associatedIdValue\":
\"1111358294500\"}]",
        }
```

```
    }
}
```

Registro de API llamadas de Amazon One Enterprise mediante AWS CloudTrail

Amazon One Enterprise está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon One Enterprise. CloudTrail captura todas las API llamadas de Amazon One Enterprise como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Amazon One Enterprise y llamadas en código a las API operaciones de Amazon One Enterprise. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon One Enterprise. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon One Enterprise, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre Amazon One Enterprise en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Amazon One Enterprise, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos en su empresa Cuenta de AWS, incluidos los eventos de Amazon One Enterprise, cree una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles

- Configuración de SNS las notificaciones de Amazon para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de Amazon One Enterprise se registran CloudTrail y se documentan enAcciones, recursos y claves de condición para Amazon One Enterprise. Por ejemplo, las llamadas a `RebootDevice` y `DeleteDeviceInstance` las acciones generan entradas en los archivos de CloudTrail registro. `ListSites`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el CloudTrail userIdentityelemento.

Descripción de las entradas de los archivos de registro de Amazon One Enterprise

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las API llamadas públicas, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateSite` acción.

```
{
    "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"
}
```

Historial de documentos de la Guía del usuario de Amazon One Enterprise

En la siguiente tabla se describen las versiones de documentación de Amazon One Enterprise.

Cambio	Descripción	Fecha
Actualización	Se ha añadido un tema nuevo: Instalación del hub de E/S del dispositivo Amazon One para un acceso seguro Guía del usuario de Amazon One Enterprise	14 de agosto de 2024
Actualización	Se ha añadido un nuevo tema: Instalación de un dispositivo Amazon One para montaje en pared Guía del usuario de Amazon One Enterprise	5 de junio de 2024
Versión inicial	Versión inicial de la Guía del usuario de Amazon One Enterprise	27 de noviembre de 2023

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.