aws

Guía del usuario

Amazon Uno

Amazon Uno: 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 5 GHz), Ethernet, 2 puertos USB tipo A, 1 puerto USB tipo B
- Comentarios de los usuarios: pantalla táctil de 5,5 pulgadas, Lightring, altavoz y auriculares
- Protocolo de control de acceso físico: OSDP y Wiegand
- Fuente de alimentación: POE, entrada de 110/220 VCA, adaptador de CA a CC incluido, 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 información 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

Amazon One es un servicio biométrico basado en la nube que utiliza un dispositivo Amazon One para autenticar a un usuario con los datos biométricos de la palma de la mano. Puedes pedir dispositivos Amazon One poniéndote en contacto con nosotros.

Tras instalar el dispositivo Amazon One, puede activar y registrar sus dispositivos con su cuenta de AWS en la consola Amazon One y en la aplicación de autenticación. Puede ver los perfiles biométricos de los usuarios inscritos. Si es necesario, puede cancelar su inscripción y eliminar sus datos biométricos.

La consola Amazon One sirve como un centro centralizado para gestionar las actividades operativas, como el seguimiento de los dispositivos y la visualización de las facturas mensuales. Los usuarios pueden inscribirse escaneando la palma de la mano en los puestos de inscripción supervisados del establecimiento. Una vez inscritos, los usuarios pueden entrar o salir sin problemas de ubicaciones seguras con solo colocar la palma de la mano sobre un dispositivo compatible con Amazon One.

Temas

Flujo de trabajo de Amazon One

A continuación se detalla el flujo de trabajo básico de Amazon One:

1. Para comprar e instalar los dispositivos Amazon One, ponte en contacto con nosotros.
2. Después de instalar el dispositivo, activa Amazon One.
3. Inicia sesión en tu cuenta de Amazon One.
4. Configura los dispositivos de registro y entrada de usuarios.
5. Inscriba las palmas de los empleados.
6. Utilice las funciones de administración y monitoreo para garantizar el estado del dispositivo, mantener las configuraciones actualizadas y realizar un seguimiento de las inscripciones de usuarios para una supervisión integral.

Términos clave de Amazon One

Estos son los términos clave de Amazon One:

- Sitio: el cliente administraba edificios físicos donde instala los dispositivos Amazon One. Un sitio debe cumplir con los requisitos de instalaciones, redes y alimentación de tus dispositivos Amazon One.
- Dispositivo: un dispositivo biométrico Amazon One Palm que escanea la palma de la mano 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.

Configuración de la consola Amazon One

En este capítulo se explican los pasos básicos para empezar a utilizar la consola Amazon One.

Configuración de un sitio, instancias de dispositivos y plantillas de configuración: siga estos pasos para crear un marco que le permita añadir una ubicación física en la que alojar sus dispositivos Amazon One y, a continuación, configurarlos y gestionarlos mediante la consola Amazon One Enterprise. Utilizará este proceso solo de vez en cuando, o incluso solo una vez, en función de la cantidad de sitios, instancias de dispositivos y plantillas de configuración.

Temas

Inscribirse en una cuenta de AWS

Si no dispone de una cuenta de AWS, siga estos pasos para crear una.

Para inscribirse en una cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
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 registra una cuenta de AWS, se crea un usuario raíz propio de ella. Este usuario tiene acceso a todos los recursos y los servicios de AWS en la cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente al usuario root para realizar tareas que requieran dicho acceso

AWS le enviará un email de confirmación tras completar el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a Mi cuenta https://aws.amazon.com/ y seleccionando Mi cuenta

Creación de un usuario con acceso administrativo

Después de registrarse para obtener una cuenta de AWS, proteja el usuario raíz de su cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario raíz para las tareas diarias.

Temas

Protección de su cuenta de AWS

Ahora que has iniciado sesión en tu cuenta de Amazon One, protege tu cuenta.

Para proteger el usuario raíz de su cuenta de AWS

1. Inicie sesión en la consola de administración de AWS como propietario de la cuenta; para ello, seleccione el usuario raíz e introduzca la dirección de correo electrónico de su cuenta de AWS.
2. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con un usuario root, consulte Iniciar sesión como usuario root en la Guía del usuario de AWS Sign-In.
3. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario raíz (consola) de la cuenta de AWS en la Guía del usuario de IAM.

Crear un usuario con acceso administrativo

Ahora que has protegido tu cuenta de Amazon One, crea un usuario con acceso administrativo.

Para crear un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Para obtener instrucciones, consulte Habilitar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre el uso del directorio del Centro de identidad de IAM como fuente de identidad, consulte Configurar el acceso de los usuarios con el directorio predeterminado del Centro de identidad de IAM en la Guía del usuario del Centro de identidades de IAM de AWS.

Iniciar sesión como administrador

Ahora que ha creado un usuario con acceso administrativo, inicie sesión como administrador.

Para iniciar sesión como usuario con acceso administrativo

- Inicie sesión con su usuario del Centro de Identidad de IAM mediante la URL de inicio de sesión que se envió a su dirección de correo electrónico cuando creó el usuario del Centro de Identidad de IAM.

  Si necesita ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de acceso de AWS en la Guía del usuario de Inicio de sesión en AWS.

Asignación de acceso a usuarios adicionales

Ahora que ha iniciado sesión como administrador, puede asignar el acceso a usuarios adicionales.

Para asignar el acceso a usuarios adicionales

- 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 la Guía del usuario de AWS IAM Identity Center.

Añadir usuarios de Amazon One

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 Amazon One solo para recuperar los códigos QR de activación del dispositivo y activar los dispositivos Amazon One.

Para añadir un usuario de Amazon One

1. Siga el procedimiento de inicio de sesión correspondiente a su tipo de usuario, tal como se describe en Cómo iniciar sesión AWS en la Guía del AWS Sign-In usuario.
2. En el panel de navegación, seleccione Usuarios y, a continuación, seleccione 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 el nombre de inicio de sesión para AWS.

   > **Note**
   >
   > La cantidad y el tamaño de los recursos de IAM en una Cuenta de AWS son limitados. Para obtener más información, consulte Cuotas de IAM y AWS STS. Los nombres de usuario pueden ser una combinación de hasta 64 letras, dígitos y los siguientes caracteres: más (+), igual (=), coma (,), punto (.), signo de flecha (@), 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 llamados TESTUSER y testuser. Cuando se utiliza un nombre de usuario en una política o como parte de un ARN, 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: opcional. AWS Management Console
5. Seleccione Deseo crear un usuario de IAM.
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, se asociará automáticamente una política de AWS administrada denominada `IAMUserChangePassword` a 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 acerca del uso de etiquetas en IAM, consulte Etiquetado de los recursos de IAM.
13. Revisa todas las opciones que has tomado hasta este momento. 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
    - URL de 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.

Crear un sitio

Ahora que has iniciado sesión en AWS Management Console, puedes usar la consola de Amazon One para crear tu sitio.

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

Para crear un sitio

1. Abre la consola de Amazon One 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.

Cree instancias de dispositivos

Ahora que ha creado un sitio en la consola de administración de AWS, puede usar la consola Amazon One para crear instancias de dispositivos.

Para crear una instancia de dispositivo

1. Abre la consola de Amazon One en https://console.aws.amazon.com/one-enterprise.
2. En el panel de navegación, selecciona instancias de dispositivo. 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.

Cree una plantilla de configuración

Ahora que has creado instancias de dispositivos, puedes usar la consola de Amazon One para crear una plantilla de configuración.

Para crear una plantilla de configuración

1. Abre la consola de Amazon One 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 para un acceso seguro.

Configure una instancia de dispositivo para la activación

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

Para configurar una instancia de dispositivo para su activación

1. Abre la consola de Amazon One 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 realice cambios en esta información de configuración importada.

    Para ver la opción Crear plantilla, consulteCree 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 para un acceso seguro.

Instalación y activación de Amazon One

Tras configurar correctamente la consola Amazon One, los siguientes pasos incluyen instalar los dispositivos Amazon One en su sitio y asegurarse de que estén activados correctamente. Este proceso incluye colocar físicamente los dispositivos en áreas designadas, conectarlos a la red y completar el proceso de activación para permitir una perfecta identificación de los usuarios y realizar transacciones. Una vez activados, tus dispositivos Amazon One estarán listos para ofrecer una experiencia segura y sin contacto a tus clientes o empleados.

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

Temas

Comprender 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 un lector. 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.

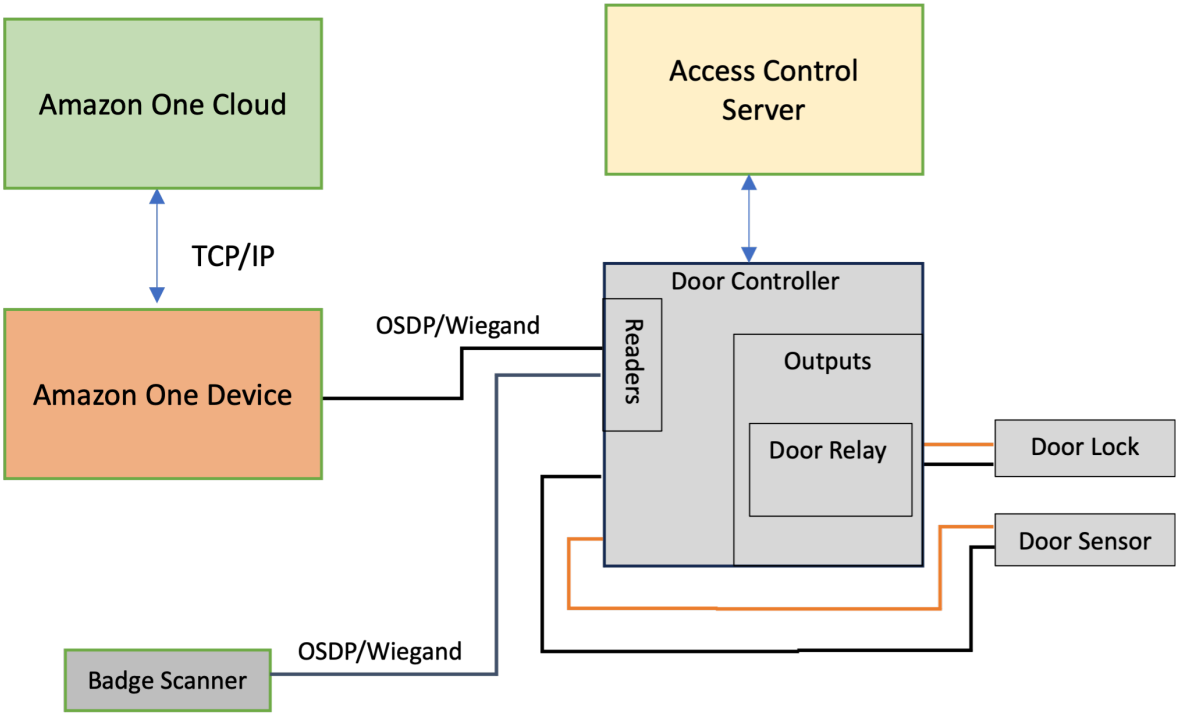
Requisito de alimentación

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 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 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 interfaz OSDP.
  - Si se necesita una interfaz Wiegand, se puede utilizar un OSDP-to-Wiegand convertidor COTS.
  - Tras la autenticación correcta, el dispositivo Amazon One envía la identificación del usuario al controlador de la puerta.
  - El controlador de la puerta responde con una decisión que, a su vez, permite que el dispositivo Amazon One muestre un mensaje de acceso concedido o de acceso denegado.
- Escáner de tarjetas: normalmente se utiliza un escáner de tarjetas para escanear tarjetas RFID y enviar el número de tarjeta al servidor de control de acceso. Con Amazon One, un escáner de credenciales se conecta al dispositivo Amazon One, lo que permite a los usuarios escanear sus credenciales, lo que las asocia con los perfiles de sus palmas.

Instalación de Amazon One Pedestal

El pedestal Amazon One es un componente clave del sistema de identificación y transacciones de Amazon One, diseñado para ofrecer a los usuarios una experiencia fluida y sin contacto. Este dispositivo cuenta con una autenticación biométrica segura. Puede integrarlo en varias ubicaciones para proporcionar soluciones de pago o acceso sin problemas.

En esta sección se proporcionan los requisitos de ubicación y step-by-step las instrucciones para instalar Amazon One Pedestal. La preparación e instalación adecuadas son fundamentales para garantizar que el sistema funcione de forma segura y eficiente, y ofrecer a los usuarios una experiencia fluida y fiable.

Requisitos previos y preparación para instalar el pedestal Amazon One

Antes de iniciar la instalación, asegúrese de que se cumplen las siguientes condiciones para una configuración segura y eficaz:

- Requisitos de alimentación: si utiliza POE+ (alimentación a través de Ethernet) para alimentar el dispositivo, compruebe que el cableado Cat6 ya esté instalado y que haya un inyector o conmutador POE+ disponible para su uso. Como alternativa, si se utiliza alimentación de CA (120 V), asegúrese de que haya una toma de CA accesible ubicada a menos de 20 pies del pedestal.
- Configuración física: el suelo debe estar nivelado, limpio y libre de suciedad para garantizar una instalación estable y segura del pedestal.

- Ubicación del pedestal: instale el pedestal en un lugar donde no bloquee las puertas, los carriles o los puntos de acceso, lo que permitirá moverse fácilmente por el área.
- Gestión de cables: coloque y asegure todos los cables sobrantes dentro del pedestal para evitar el desorden y evitar posibles daños durante el uso normal.

Una vez confirmados estos requisitos previos, puede continuar con el proceso de instalación.

Para instalar Amazon One Pedestal

1. Retira el pedestal Amazon One del embalaje.
2. Retire la puerta desatornillando los dos tornillos M4 a prueba de manipulaciones.
3. Enchufe el cable de alimentación.
4. Pase el cable a través del orificio de la placa base del pedestal.
5. Enrolle cualquier cable de alimentación sobrante dentro del pedestal.
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 fijar la puerta al pedestal y vuelva a atornillar los dos tornillos M4 antisabotaje para fijarla.

Tras instalar tu dispositivo Amazon One, estarás listo para activarlo.

Instalación del dispositivo Amazon One que se puede montar en la pared

El dispositivo Amazon One, que se puede montar en la pared, es un sistema de identificación biométrica versátil y compacto diseñado para proporcionar una experiencia perfecta y sin contacto a los usuarios en diversos entornos. Utiliza una tecnología avanzada de reconocimiento de la palma

de la mano para acceder o pagar de forma segura, lo que lo hace ideal para ubicaciones con mucho tráfico, como espacios comerciales, entradas de oficinas y más.

En esta sección se describen los requisitos de ubicación necesarios y los pasos detallados para instalar el dispositivo Amazon One que se puede montar en la pared a fin de garantizar un rendimiento y una seguridad óptimos.

Requisitos previos y preparación para instalar el dispositivo Amazon One de montaje en pared

Antes de comenzar la instalación, asegúrate de que se cumplen las siguientes condiciones para garantizar que el dispositivo funcione de manera efectiva y que esté correctamente configurado en tu espacio:

- Solo para uso en interiores: el dispositivo Amazon One, que se puede montar en la pared, está diseñado únicamente para uso en interiores, así que asegúrate de instalarlo en un entorno adecuado.
- Requisitos de pared: la pared debe estar nivelada para garantizar la correcta alineación y funcionalidad del dispositivo.
- Altura de montaje: la parte superior del soporte de pared debe colocarse a una distancia no superior a 44-46 pulgadas del suelo después de la instalación, lo que garantiza la facilidad de acceso para los usuarios.
- Gestión de cables: asegúrese de que todos los cables sobrantes queden colocados detrás del soporte de pared y sujetos de forma segura para evitar que se estropeen o se ensucien.
- Alimentación a través de Ethernet (PoE++): si utiliza alimentación a través de Ethernet (PoE++), compruebe que esté disponible un conmutador PoE++ de clase 6 IEEE 802.3bt (tipo 3) o un inyector (tramo medio). La fuente PoE++ debe estar listada o certificada y cumplir con las normas IEC 62368-1. Es importante destacar que la fuente PoE++ debe estar ubicada en el mismo edificio que el dispositivo. Utilice únicamente una fuente PoE++ aprobada con el dispositivo AOE.
- Entrada de alimentación de 15 V DC: si utiliza una entrada de alimentación de 15 V DC, asegúrese de que solo se utilice una fuente de alimentación NEC de clase 2 o una fuente de alimentación aprobada para limitaciones de potencia. La fuente de alimentación debe estar listada o certificada para garantizar su seguridad y compatibilidad.

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

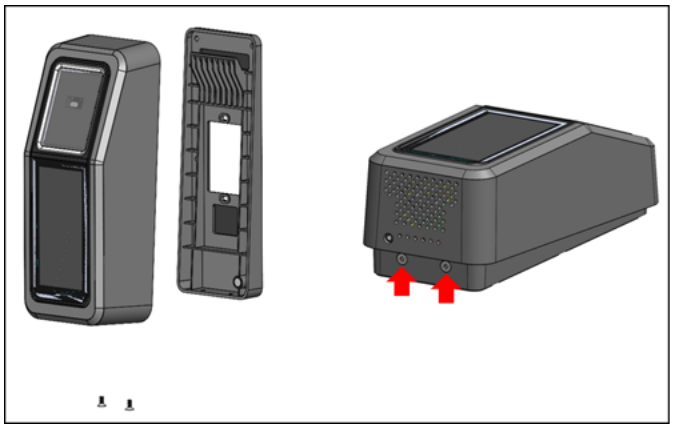
Incluido con el dispositivo Amazon One que se puede montar en la pared

- 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

Una vez confirmados estos requisitos previos, puede continuar con los pasos de instalación para montar y configurar de forma segura el dispositivo Amazon One que se puede montar en la pared.

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

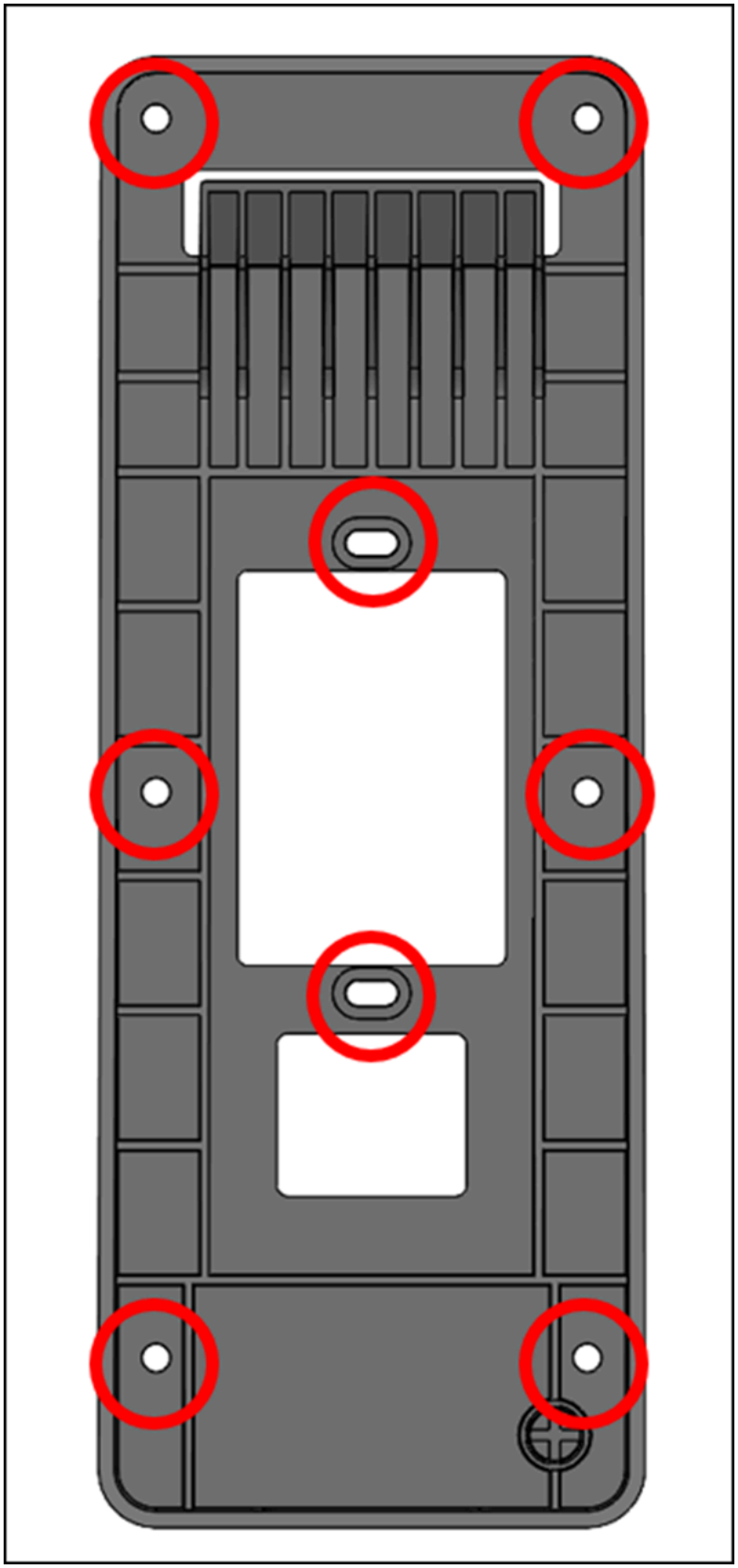
1. Retira tu dispositivo Amazon One del embalaje.
2. Separa la placa de montaje de tu dispositivo Amazon One quitando los dos tornillos de seguridad Torx inferiores.



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.

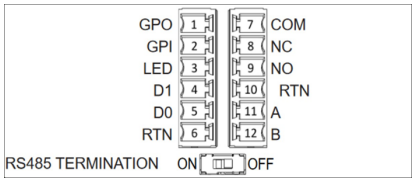
Para conectar tu dispositivo Amazon One que se puede montar en la pared

Puede configurar el dispositivo Amazon One con los protocolos de control de acceso OSDP y 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	

Pin	Connection	Descripción	Uso
2	GPI	Entrada de uso general	Señal de entrada digital: opcional
3	GUIÓ	LED Wiegand	LED Wiegand: opcional
4	D1	Wiegand D1	Wiegand data 1 — Cable blanco
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	Retorno OSDP: cable negro

Pin	Connection	Descripción	Uso
11	A	RS485_A/D1/ Reloj	OSDP D1 — Cable blanco
12	B	RS485_B/D0/ Datos	OSDP D0 — Cable verde

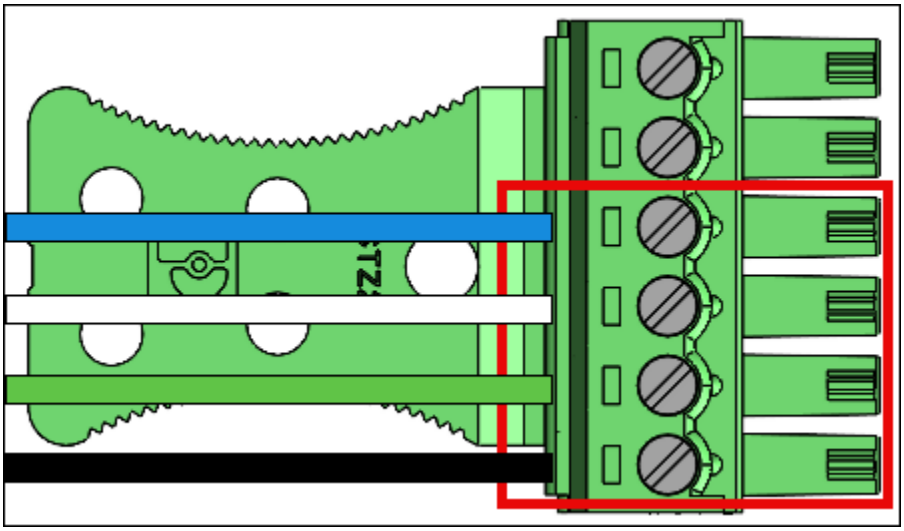
2. Al instalar un cable, separe entre 3 y 5 mm del extremo del cable.
3. Inserte el extremo pelado del cable en la posición de terminal deseada.
4. Con un destornillador de punta plana, gire el tornillo de retención del terminal en el sentido de las agujas del reloj para sujetar el cable hasta que quede 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

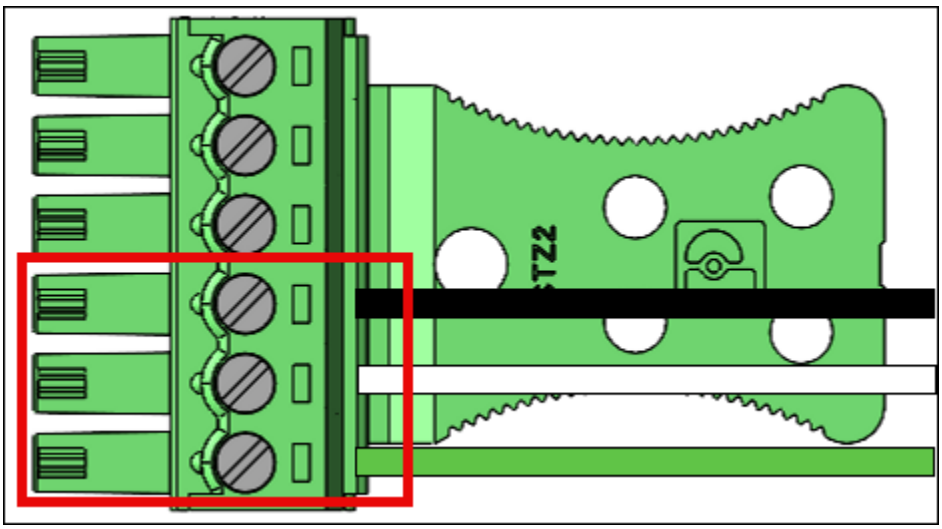
Pin	Connection	Descripción	Uso
3	GUIÓ	LED Wiegand	Entrada LED Wiegand: opcional (TTL de 5 V)
4	D1	Wiegand D1	Salida Wiegand D1 (5 V TTL)
5	D0	Wiegand D0	Salida Wiegand D0 (5 V TTL)
6	RTN	Retorno de señal	Referencia GND de Wiegand

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.

RS485 conexiones

- 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).

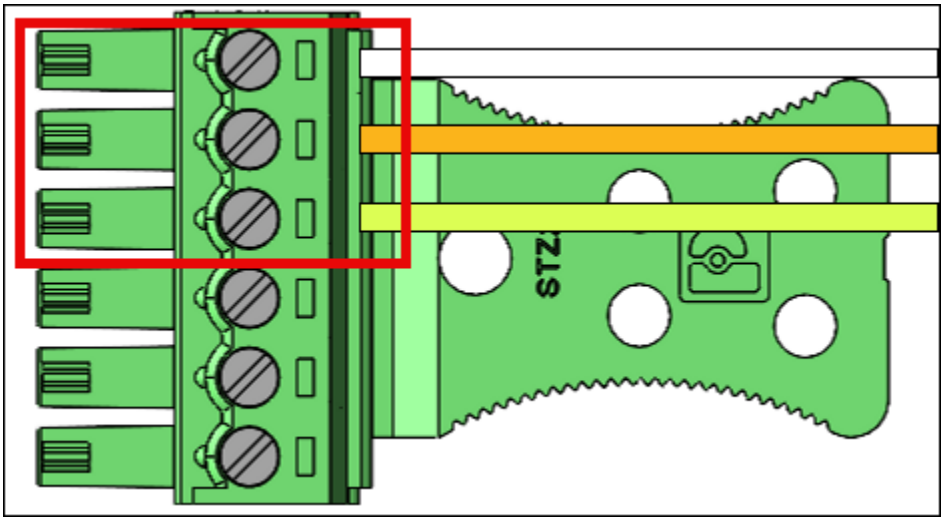


RS485 cableado

Pin	Connection	Descripción	Uso
10	RTN	Retorno de señal	Suelo
11	A	RS485_A/D1/ Reloj	RS485 señal no inversora
12	B	RS485_B/D0/ Datos	RS485 señal inversora

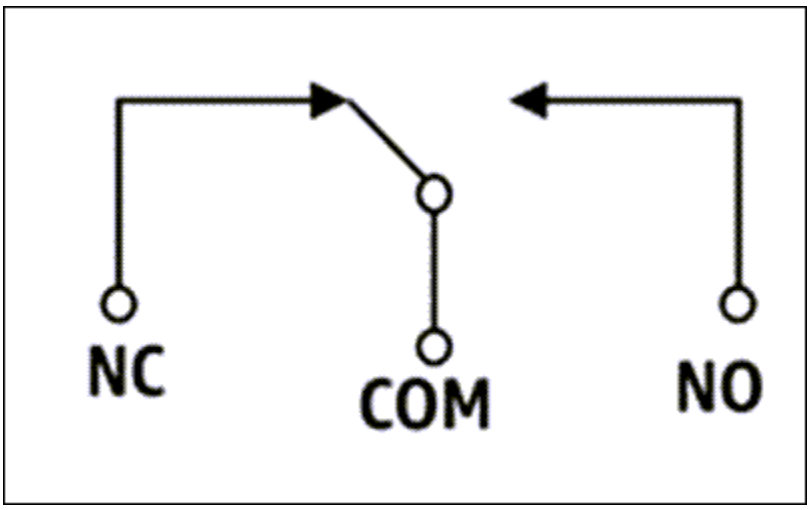
conexiones de relé

- 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

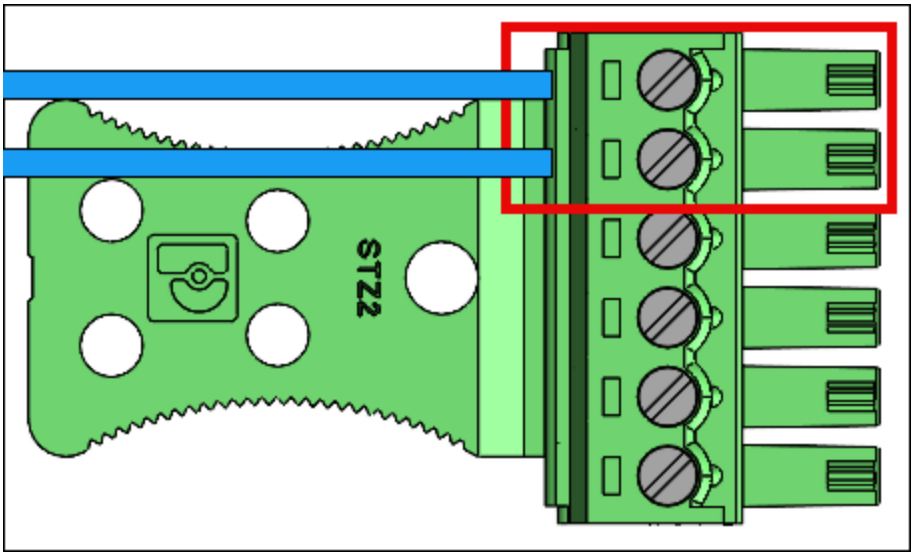
Pin	Connection	Descripción	Uso
7	COM	Relé común	Relé de contacto común: cable blanco
8	NC	Relé normalmente cerrado	Relé de contacto normalmente cerrado: cable naranja
9	NO	El relé está normalmente abierto	El relé de contacto está normalmente abierto: cable amarillo



El relé debe funcionar de acuerdo con las clasificaciones de seguridad especificadas: 30 VAC/60 VDC, 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).



Cableado de entrada/salida digital

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

Tras instalar tu dispositivo Amazon One, estarás listo para activarlo.

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

El dispositivo Amazon One con hub de E/S es una parte integral del sistema Amazon One Enterprise, diseñado para mejorar la seguridad y agilizar el control de acceso para una variedad de entornos. El dispositivo aprovecha el reconocimiento biométrico de la palma de la mano para proporcionar a los usuarios una autenticación segura y sin contacto, lo que lo hace ideal para su uso en áreas de alta seguridad, como edificios de oficinas, puntos de entrada restringidos o instalaciones que requieren una gestión de acceso perfecta. El concentrador de E/S actúa como un puente entre el dispositivo y la infraestructura de seguridad existente, lo que permite la comunicación con las cerraduras de las puertas, las alarmas y otros sistemas de control de acceso.

En esta sección se proporcionan los requisitos de ubicación y step-by-step las instrucciones para instalar el dispositivo Amazon One con I/O Hub. La preparación e instalación adecuadas son fundamentales para garantizar que el sistema funcione de forma segura y eficiente, y ofrecer a los usuarios una experiencia fluida y fiable.

Requisitos previos y preparación para instalar el dispositivo Amazon One con hub de E/S

Antes de iniciar la instalación, asegúrate de que se cumplen las siguientes condiciones para garantizar una configuración segura y eficaz:

- Solo para uso en interiores: el dispositivo Amazon One con hub de E/S está diseñado solo para uso en interiores. Asegúrese de que esté instalado en un entorno adecuado.

- Alimentación a través de Ethernet (PoE++): si utiliza alimentación a través de Ethernet (PoE++), compruebe que esté disponible un conmutador PoE++ IEEE 802.3bt (tipo 3) de clase 6 (extremo) o un inyector (intervalo medio). La fuente PoE++ debe estar listada o certificada y cumplir con las normas IEC 62368-1. Es importante destacar que la fuente PoE++ debe estar ubicada en el mismo edificio que el dispositivo. Utilice únicamente una fuente PoE++ aprobada con el dispositivo AOE.

- Entrada de alimentación de 15 V CC: si utiliza una entrada de alimentación de 15 V CC, asegúrese de utilizar únicamente una fuente de alimentación NEC de clase 2 o homologada con alimentación limitada. La fuente de alimentación debe figurar en la lista o estar certificada por motivos de seguridad. Para obtener más información, consulte 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

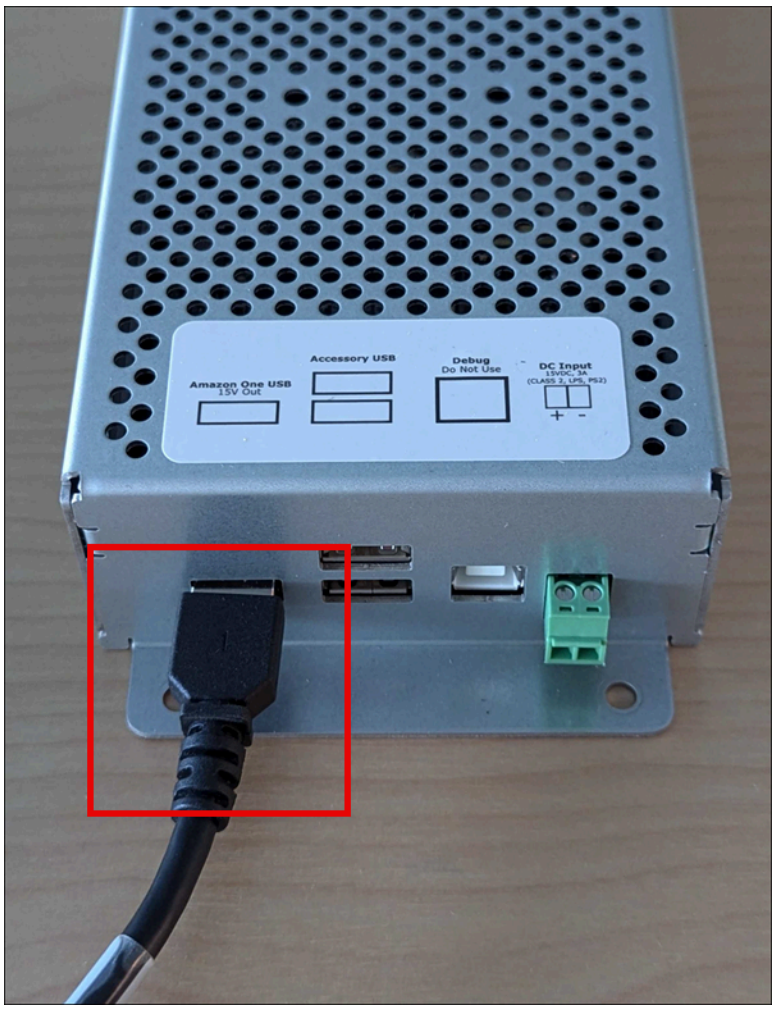
Incluido con el dispositivo Amazon One con hub de E/S

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

Una vez confirmados estos requisitos previos, puede continuar con el proceso de instalación y garantizar una configuración segura y eficiente de su dispositivo Amazon One con I/O Hub. Una preparación adecuada ayudará a garantizar que el dispositivo funcione según lo previsto y se integre sin problemas en su sistema de acceso seguro.

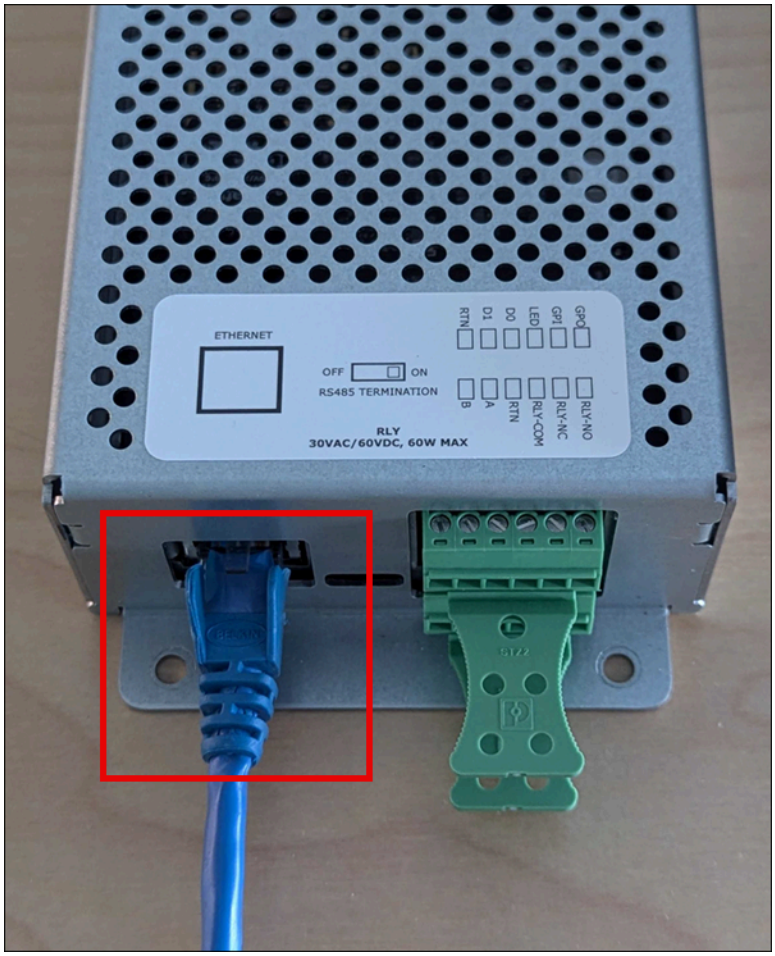
Para instalar el hub de E/S para tu dispositivo Amazon One

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 cable USB de Amazon One al puerto del hub de E/S.



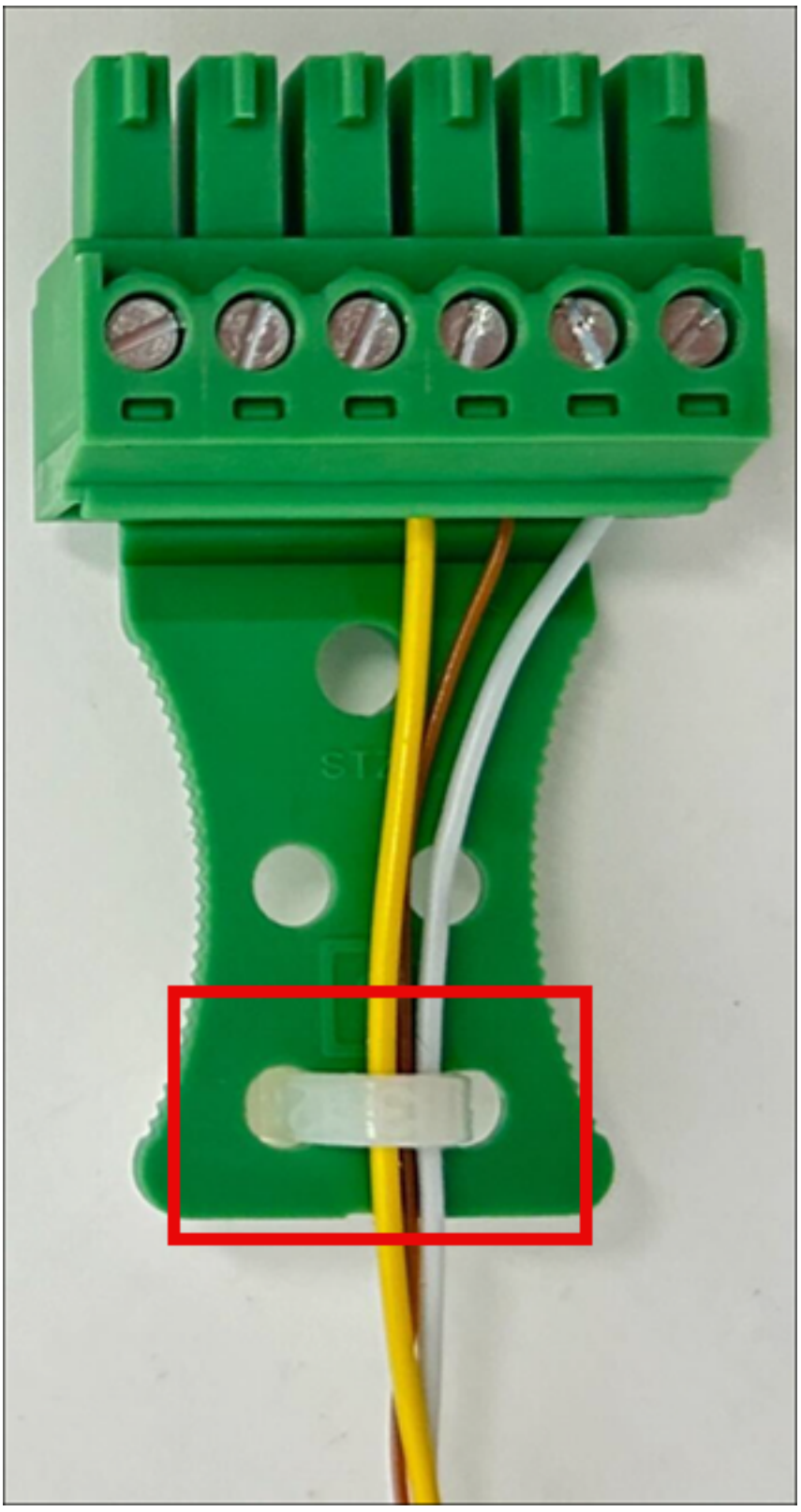
4. Para la alimentación POE++, conecte el cable Ethernet de la fuente POE++ al puerto del hub de E/S.

   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

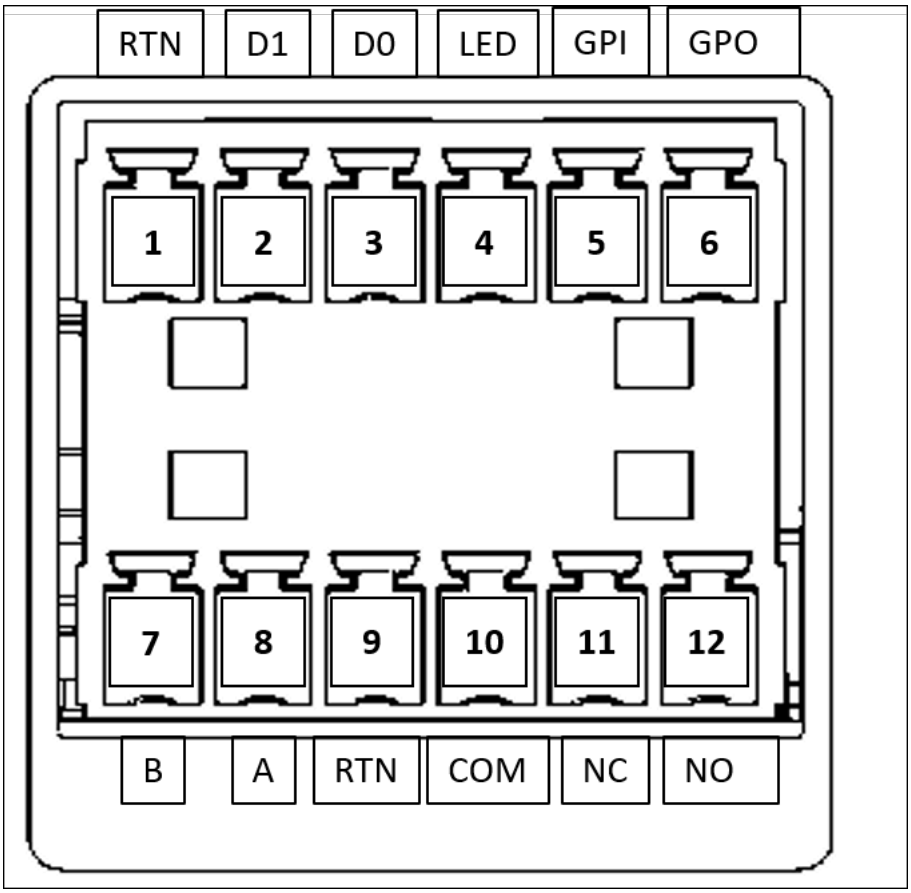
- Instale un circuito de goteo para evitar que los líquidos corran accidentalmente por el cable y entren en el hub de E/S.
- Coloque una pinza limitadora de tensión para proteger los cables de daños o tensiones, como se muestra en la siguiente imagen.



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

2. 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.

Conexiones



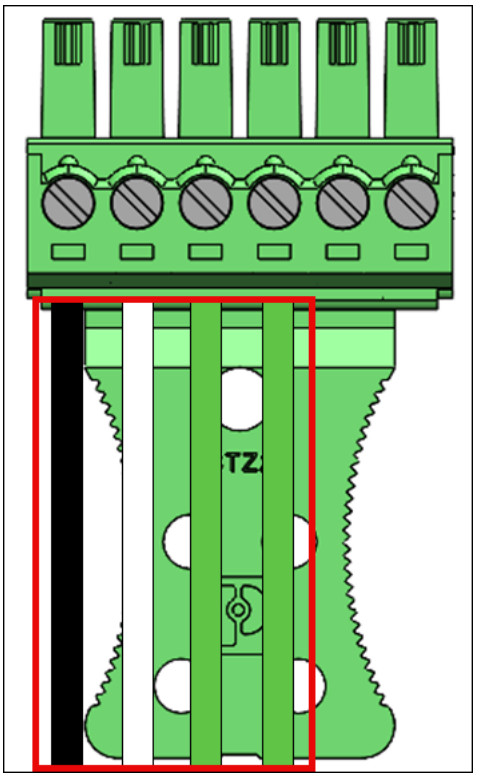
Pin	Connection	Descripción	Uso
1	RTN	Retorno de señal	Wiegand Ground — Cable negro
2	D1	Wiegand D1	Wiegand Data 1 — Cable blanco
3	D0	Wiegand D0	Datos de Wiegand 0 — Cable verde

Pin	Connection	Descripción	Uso	
4	GUIÓ	LED Wiegand	LED Wiegand: opcional	
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	OSDP D0 — Cable verde	
8	A	RS485_A/D1/ Reloj	OSDP D1 — Cable blanco	
9	RTN	Retorno de señal	Retorno OSDP: cable negro	
10	COM	Relé común	Relé de contacto común: cable blanco	
11	NC	Relé normalmen te 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).

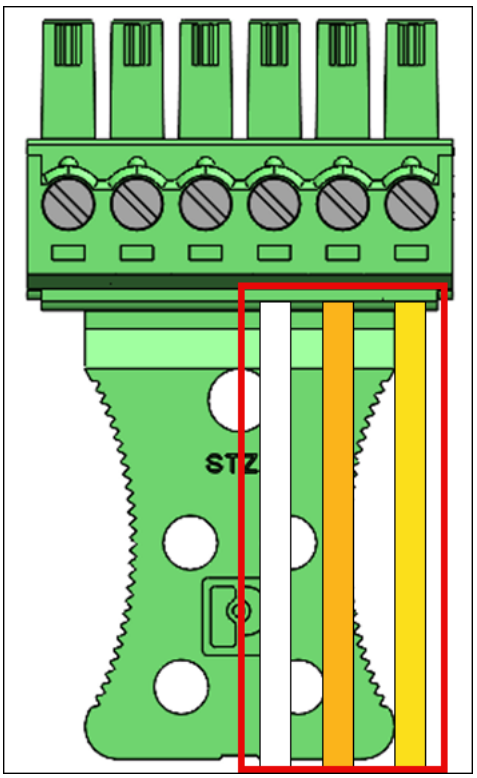
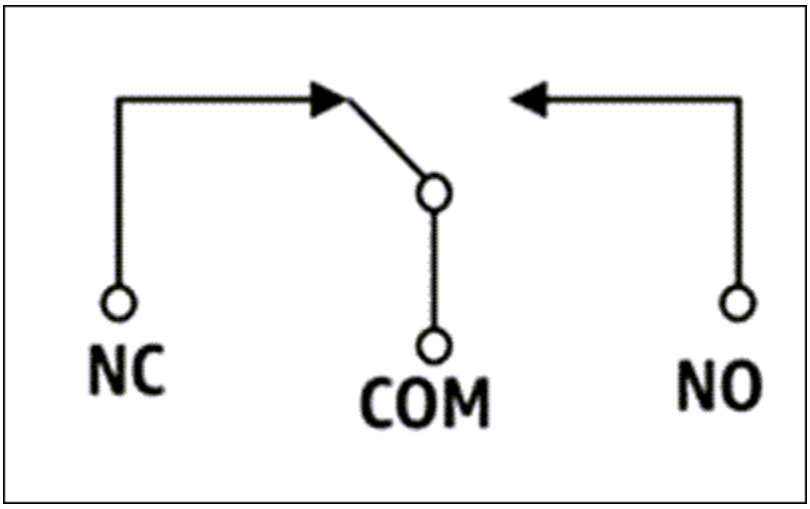


Diagrama de relés

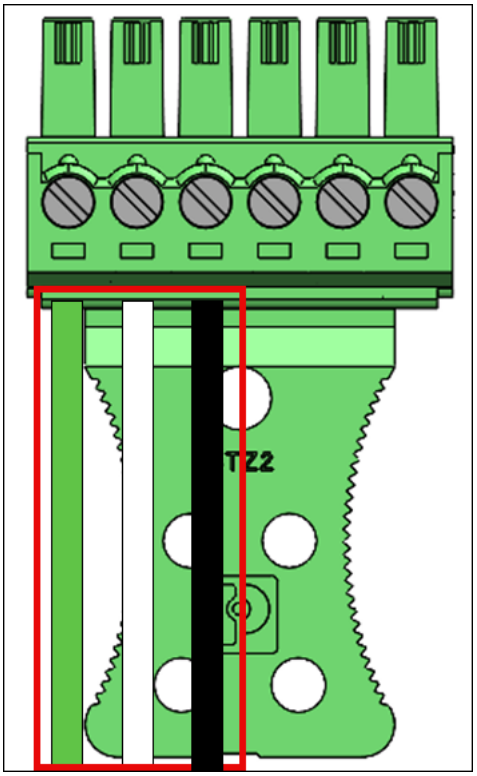


El relé debe funcionar de acuerdo con las clasificaciones de seguridad especificadas: 30 VAC/60 VDC, 60 W como máximo.

RS485 conexiones

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

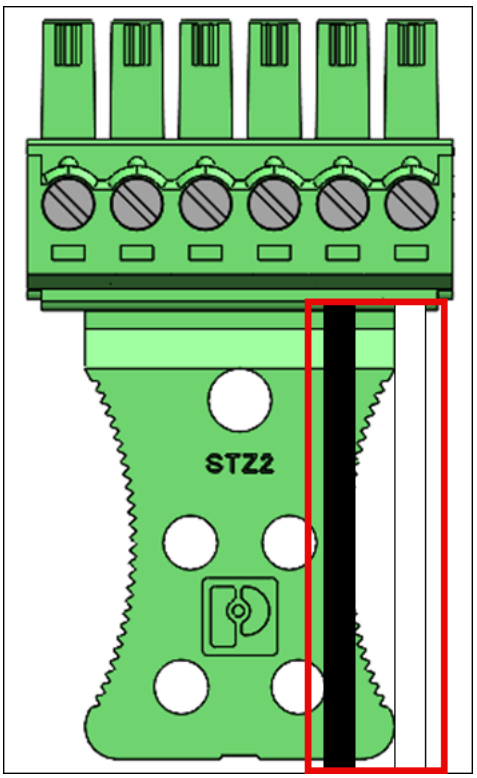
- Inserte el cable negro en el pin 9 (RTN).



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

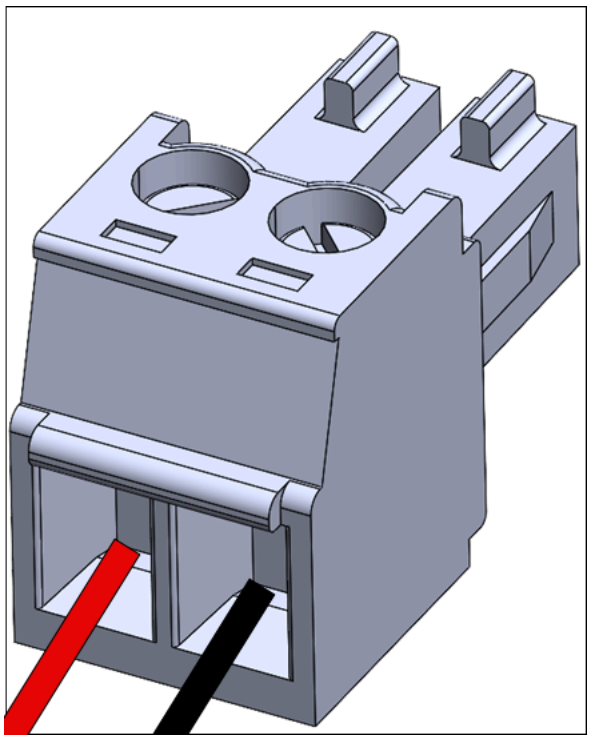
- Inserte el cable negro en el pin 5 (GPI).
- Inserte el cable blanco en el pin 6 (GPO).



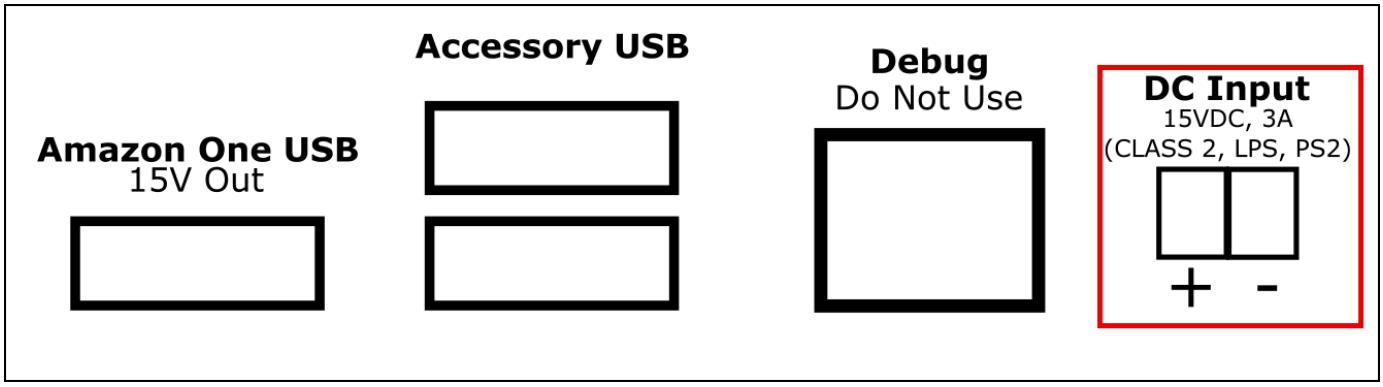
- Las conexiones de entrada/salida digital deben funcionar como se indica.

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.



Tras instalar tu dispositivo Amazon One, estarás listo para activarlo.

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.

   En cuanto el dispositivo se conecte a Internet, empezará a descargar el paquete de software más reciente.
3. ¡Cuando la pantalla muestre que la descarga del software ha finalizado! , 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 Añadir usuarios de Amazon One.
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. Ten en cuenta que el código QR se actualiza periódicamente por motivos de seguridad. Solo puedes usar un código QR una vez.
11. Introduce el código postal del sitio y selecciona Confirmar la configuración después de comprobar que se muestra el sitio correcto.
12. Cuando la pantalla del dispositivo Amazon One muestre ¡Activación completa! , el dispositivo está listo para su uso.

Inscripción e introducción de usuarios

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

Creación de una política de punto de conexión

Antes de que los usuarios puedan autenticar sus palmas de las 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.

Autenticarse para ingresar

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

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.

Temas

Ver los usuarios inscritos

El siguiente procedimiento detalla cómo inscribir a los usuarios.

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 credencial capturada por un lector de credenciales RFID 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.

Eliminar los usuarios inscritos y sus datos biométricos

El siguiente procedimiento detalla cómo eliminar los usuarios inscritos y sus datos biométricos.

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 Amazon One

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

Mantenimiento y limpieza de los dispositivos Amazon One

El mantenimiento de tu dispositivo Amazon One proporciona un entorno operativo y una experiencia de uso óptimos.

Antes de limpiar el dispositivo Amazon One, asegúrate de lo siguiente:

- Si bien no tienes que activar o desactivar Amazon One, asegúrate de que los dispositivos estén conectados a la alimentación, tengan conectividad de red y que todos los periféricos y dispositivos complementarios (si corresponde) estén conectados.
- Si la conectividad de red no está disponible (aparecerá una pantalla de error en el dispositivo Amazon One si esto ocurre), si aparece una pantalla de error en el dispositivo Amazon One, si aparece una pantalla de error en el dispositivo Amazon One o si aparece un problema de conexión en la consola.
- Proteja físicamente los dispositivos para que personas no autorizadas no puedan manipularlos.
- Inspeccione visualmente los dispositivos Amazon One a diario y compruebe si hay conexiones no autorizadas a los dispositivos Amazon One.
- Inspecciona todos los lados del dispositivo en busca de señales de manipulación, incluidos los tornillos visibles del dispositivo y la carcasa, para asegurarte de que no haya huecos o aberturas que expongan los componentes internos o los circuitos de ninguno de los dispositivos Amazon One.
- En caso de errores o fallos, sigue las instrucciones que aparecen en la pantalla del dispositivo Amazon One o consulta la guía de solución de problemas para solucionar los problemas.

Para limpiar el dispositivo Amazon One

Al limpiar tu dispositivo Amazon One con regularidad, se eliminan manchas o marcas, como huellas dactilares y huellas de manos.

> **Note**
>
> No utilices ningún otro producto de limpieza que no sea el indicado en esta guía. El programa de limpieza recomendado es una o dos veces por semana, o siempre que haya suciedad, polvo o manchas visibles en el dispositivo, pero nunca más de una vez al día.

1. Limpia el dispositivo Amazon One con toallitas de alcohol isopropílico (IPA). Limpia únicamente la superficie táctil del dispositivo. No toques la ventana óptica ni utilices ningún otro producto de limpieza a menos que Amazon One te lo indique.
2. Limpia cualquier mancha con un paño de microfibra seco.
3. Limpie ligeramente (no limpie) cualquier suciedad o residuo visible de la ventana óptica. Limite la limpieza de la ventana óptica a no más de una vez al díaand/or when the window is visually dirty (e.g., finger/hand prints/smudges). Esta parte del dispositivo no está diseñada para ser tocada, pero nuevos clientes podrían tocarla inadvertidamente.
4. Utilice un limpiador de tarjetas inteligentes KIC para limpiar el interior de un lector de tarjetas, si corresponde.
5. Limpie el dispositivo una o dos veces por semana, o siempre que haya suciedad, polvo o manchas visibles en el dispositivo.

Administración del sitio

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

Temas

Cambiar el nombre del sitio

El siguiente procedimiento detalla cómo cambiar el nombre del sitio para su dispositivo.

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.

Actualización de la dirección del sitio

El siguiente procedimiento detalla cómo actualizar la dirección del sitio de su dispositivo.

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
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.

Temas

Visualización del estado de la instancia del dispositivo

El siguiente procedimiento detalla cómo ver el estado de la instancia de tu dispositivo.

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.

Reiniciar un dispositivo Amazon One

El siguiente procedimiento detalla cómo reiniciar tu dispositivo Amazon One.

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.

Actualización de las configuraciones de los dispositivos Amazon One

El siguiente procedimiento detalla cómo actualizar las configuraciones de los dispositivos 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 (consulteConfigure una instancia de dispositivo para la 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.

Actualización de las credenciales de Wi-fi

El siguiente procedimiento detalla cómo actualizar las credenciales de Wi-Fi.

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.

Desactivar instancias de dispositivos

El siguiente procedimiento detalla cómo desactivar las instancias de dispositivos.

Para desactivar las instancias de dispositivos

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

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. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa 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

El modelo de se aplica a 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. Eres responsable de mantener el control sobre el contenido alojado en

esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las 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:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contienen Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (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 trabaja con Amazon One Enterprise u otro Servicios de AWS mediante la consola, la API o AWS SDKs. AWS CLI Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para 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 cifrado de AWS.

Claves propiedad de AWS: 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 propiedad de AWS, 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 propiedad de AWS en la Guía para desarrolladores de AWS Key Management Service.

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 solicitudes de API entrantes a los servicios de AWS. Este cifrado está activado de forma predeterminada.

Administración de identidad y acceso para Amazon One Enterprise

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Amazon One Enterprise. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice 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 ayudarle 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.

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. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con Amazon One Enterprise, consulteCómo funciona Amazon One Enterprise con IAM.

Administrador de IAM: si es administrador de IAM, puede que le interese obtener más información sobre cómo 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 utilizar en IAM, consulte. Ejemplos de políticas basadas en identidad para Amazon One Enterprise

Autenticación con identidades

La autenticación es la forma en que inicias sesión para AWS usar tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), 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, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

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

Si accede 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 utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

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

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza 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 las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

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 Identidad o cualquier usuario al 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 una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes 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 los recursos de IAM.

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 Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes 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 acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- 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 usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto 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 Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto 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 AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON 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. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza 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 el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, 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 más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades puedes 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 roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes 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 políticas AWS gestionadas de IAM en una política basada 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. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, 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 puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes 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, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations 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 puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

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 se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon One Enterprise con IAM

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

Funciones de IAM que puede utilizar con Amazon One Enterprise

Característica de IAM	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 políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No

Característica de IAM	Soporte para Amazon One Enterprise
Roles vinculados al servicio	No

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

Políticas basadas en identidad para Amazon One Enterprise

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, 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 más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, 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 asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

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 política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para

el recurso al que se asocia la política, la política define qué acciones puedes 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 toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de 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 administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para Amazon One Enterprise

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. 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 usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes 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, utiliza 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 el ARN de cada recurso, consulte. Acciones, 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

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 las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes 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. Puedes crear expresiones condicionales que utilizan 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 elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única 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 puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

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

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

ACLs en Amazon One Enterprise

Soporta ACLs: 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. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Amazon One Enterprise

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta 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 sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Amazon One Enterprise

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante 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 tu 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 roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS 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 de servicios cruzados para Amazon One Enterprise

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Funciones de servicio para Amazon One Enterprise

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de 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 puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con 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 la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

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
- Uso de la consola Amazon One Enterprise
- Cómo permitir a los usuarios consultar sus propios permisos
- Acceso de solo lectura a Amazon One Enterprise

- Acceso completo a Amazon One Enterprise
- Permisos a nivel de recursos compatibles para las acciones de la API de Amazon One Enterprise Rule
- Información adicional

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 generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

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 que tiene en su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

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

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

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

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

Acceso de solo lectura a Amazon One Enterprise

El siguiente ejemplo muestra una política AWS 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 elemento `Resource` enumera los recursos de AWS en los que el usuario puede realizar estas 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 de `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 otros AWS servicios.
- `"Action": ["*"]`

  Esto permite todas AWS las 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 la API de Amazon One Enterprise Rule

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 la API de reglas 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 acciones de la API de reglas de Amazon One Enterprise que actualmente admiten permisos a nivel de recursos. También describe los recursos compatibles y los ARNs correspondientes a cada acción. Al especificar un ARN, puede usar el comodín * en sus rutas; por ejemplo, cuando no puede o no quiere especificar el recurso exacto. IDs

> **Important**
>
> Si una acción de la API de reglas 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.

Acción API	Recursos
CreateDeviceInstance	Instancia de dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
GetDeviceInstance	Instancia de dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
UpdateDeviceInstance	Instancia de dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteDeviceInstance	Instancia de dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceActivationQrCode	Instancia de dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteAssociatedDevice	Instancia de dispositivo

Acción API	Recursos
	arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
RebootDevice	Instancia de dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceInstanceConfiguration	Configuración de instancia de dispositivo arn:aws:one :device-instance/ /configuration/ *region:accountID deviceInstanceId version*
GetDeviceInstanceConfiguration	Configuración de instancia de dispositivo arn:aws:one :device-instance/ /configuration/ *region:accountID deviceInstanceId version*
CreateSite	Sitio arn:aws:one :site/ *region:accountID siteId*
DeleteSite	Sitio arn:aws:one ::site/ *region:accountID siteId*
GetSiteAddress	Sitio arn:aws:one ::site/ *region:accountID siteId*
UpdateSite	Sitio arn:aws:one ::site/ *region:accountID siteId*
UpdateSiteAddress	Sitio arn:aws:one ::site/ *region:accountID siteId*

Acción API	Recursos
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, se permite que la AWS Config regla lea acciones como, por ejemplo, `GetSite` en 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 la API de reglas de Amazon One Enterprise.

Información adicional

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

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 estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

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 a la fuente RSS de la página de historial de Amazon One Enterprise Document.

Cambio	Descripción	Fecha
Se ha añadido Amazon One Enterprise AmazonOne MetricPublishAccess	La política de permisos de roles denominada AmazonOneMetricPublishAccess permite que Amazon One Enterprise funcione CloudWatch: PutMetricData en el espacio de CloudWatch nombres AWS/. AmazonOne	6 de febrero de 2025

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

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 las políticas de permisos de IAM.

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 elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI 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 un ARN de ese tipo en una instrucción con dicha 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 elemento `Resource` de una política de IAM, debe incluir un ARN o patrón 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	Otorgar permiso para crear una instancia de dispositivo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	Otorgue permiso para obtener información sobre la instancia del dispositivo	Lectura	instancia de dispositivo*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeviceInstances	Otorgue permiso para enumerar instancias de dispositivos	Lectura			
UpdateDeviceInstance	Otorgue permiso para actualizar la instancia del dispositivo	Escritura	instancia del 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*		
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	Conceda permiso para crear la configuración de instancias de dispositivos	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDeviceInstanceConfiguration	Otorgue permiso para obtener información sobre la configuración de la instancia del dispositivo	Lectura	configuración*		
CreateSite	Conceder 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	Lectura	sitios*		
ListSites	Otorgue permiso para publicar sitios	Lectura			
GetSiteAddress	Otorgue permiso para obtener información sobre la dirección del sitio	Lectura	sitios*		
UpdateSite	Otorgue permiso para actualizar el sitio	Escritura	sitios*		
UpdateSiteAddress	Otorgue permiso para actualizar la dirección del sitio	Escritura	sitios*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
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	Lectura	device-configuration-template*		
ListDeviceConfigurationTemplates	Otorgue permiso para enumerar las plantillas de configuración de dispositivos	Lectura			
UpdateDeviceConfigurationTemplate	Otorgue permiso para actualizar la plantilla de configuración del dispositivo	Escritura	device-configuration-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
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	Lectura			

Tipos de recurso definidos por Amazon One Enterprise

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. 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 condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. 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/${TagKey}	Filtra el acceso mediante las etiquetas de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
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:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- 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. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan 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, consulta 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, como el PCI DSS, al cumplir 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 uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

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 entregan EventBridge prácticamente 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 las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega 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 las llamadas. Para obtener más información, consulte la AWS CloudTrail Guía del usuario de .

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. Inicie sesión en la consola de AWS en https://console.aws.amazon.com/events/.
2. Abra la EventBridge consola en https://console.aws.amazon.com/events/.
3. En el panel de navegación, en Buses, elija Reglas.
4. Seleccione Creación de regla.
5. En la página de detalles de la regla predeterminada, asigne un nombre a la regla.
6. Elija Rule with an event pattern (Regla con un patrón de evento) y, a continuación, elija Next (Siguiente).
7. En la página Crear un patrón de eventos, en Origen del evento, compruebe que esté seleccionada la opción AWS Eventos o eventos EventBridge asociados.
8. En Ejemplo de tipo de evento, elija AWS Events.
9. En Método de creación, elija Patrón personalizado.
10. En la sección Patrón de eventos, añade un JSON con la fuente del evento como fuente `aws:one` y el tipo de detalle requerido:

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

    Puedes elegir el tipo de detalle necesario de la lista anterior y eliminar lo que no sea obligatorio.
11. Elija Next (Siguiente).
12. En la página Seleccione los destinos, seleccione el destino que desee, que incluya una función Lambda, una cola de SQS o un tema de SNS. Para obtener información sobre la configuración de los objetivos, consulta Amazon EventBridge targets.

    Por ejemplo, para ver cuándo alguien se acerca, selecciona «Reconocimiento exitoso». A continuación, consulta los detalles del evento (que figuran en el apéndice) para ver quién ha registrado el evento.

Para completar tu flujo de trabajo, puedes ejecutar una API externa u otro objetivo.

13. Si lo desea, puede configurar las etiquetas.
14. 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 en JSON. Para cada tipo de evento, se envía un blob JSON al destino que elija, 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.

recursos

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

metadatos

siteName

- Nombre del sitio en el que está presente la DeviceInstance.

SiteArn

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

data

Conectividad actual

- Representa si la DeviceInstance está conectada o desconectada de Internet.
- Valores posibles: CONECTADO, DESCONECTADO

CONECTIVIDAD ANTERIOR

- Representa si la DeviceInstance estaba conectada o desconectada de Internet antes del evento.
- Valores posibles: CONECTADO, DESCONECTADO

currentHealthStatus

- Representa si la DeviceInstance ha superado todas las comprobaciones de estado.
- Valores posibles: SALUDABLE, CRÍTICO

previousHealthStatus

- Indica si la DeviceInstance pasó todas las comprobaciones de estado la última vez que se comprobó.
- Valores posibles: SALUDABLE, CRÍTICO

assetTagId

- El assetTagId del dispositivo asociado a la DeviceInstance.

deviceInstanceName

- El nombre de la instancia de dispositivo para la 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 ha dado 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 una gammagrafía de la palma de la mano.

recursos

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

data

accountId

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

Fuente de la solicitud

- Es el deviceInstanceId del dispositivo que inició la solicitud.

Marca de tiempo creada

- Hora en la que se está creando el evento.

Estado del usuario

- El estado actual del usuario.
- Valores posibles: ACTIVO, ELIMINADO

ID ASOCIADO

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

razón

- 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 de estado CRÍTICO a SALUDABLE.


```
{
    "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 de SALUDABLE a CRÍTICO.

```
{
  "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 de DESCONECTADO a CONECTADO.

```
{
  "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 de CONECTADO a DESCONECTADO.

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

Registro de llamadas a la API 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 llamadas a la API de Amazon One Enterprise como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Amazon One Enterprise y llamadas en código a las operaciones de la API 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 las notificaciones de Amazon SNS 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 le 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 elemento userIdentity de CloudTrail .

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 llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se 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"
}
```

Solución de problemas de Amazon One

Si tienes problemas con la aplicación Amazon One o con uno de tus dispositivos Amazon One, sigue estas sugerencias para solucionar el problema. A continuación, si sigue teniendo problemas, póngase en contacto con AWS Support.

Temas

Solución de problemas de identidad y acceso a Amazon One

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

Temas

No estoy autorizado a realizar ninguna acción en Amazon One

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

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

```
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 gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon One

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 obtener 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 los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Solución de problemas con la consola Amazon One

Si tienes problemas con la aplicación Amazon One o con uno de tus dispositivos Amazon One, sigue estas sugerencias para solucionar el problema. A continuación, si sigue teniendo problemas, póngase en contacto con AWS Support.

Temas

- No puedo crear un sitio

No puedo crear un sitio

- Ponte en contacto con el administrador de Amazon One Console para que te dé acceso.
- Si el problema continúa, póngase en contacto con AWS Support.

No puedo crear una instancia de dispositivo

- Ponte en contacto con el administrador de Amazon One Console para que te dé acceso.
- Si el problema continúa, póngase en contacto con AWS Support.

No puedo crear una plantilla de configuración

- Ponte en contacto con el administrador de Amazon One Console para que te dé acceso.
- Si el problema continúa, póngase en contacto con AWS Support.

No puedo crear un código QR de activación

- Ponte en contacto con el administrador de Amazon One Console para que te dé acceso.
- Si el problema continúa, póngase en contacto con AWS Support.

Solución de problemas del dispositivo Amazon One

Si tienes problemas con Amazon One Console o con uno de tus dispositivos Amazon One, sigue estas sugerencias para solucionar el problema. A continuación, si sigue teniendo problemas, póngase en contacto con AWS Support.

Temas

Pantalla en blanco

Esto ocurre cuando el dispositivo no tiene alimentación o se atasca durante el reinicio.

Realice lo siguiente para solucionar este problema:

- Espere unos instantes (menos de 30 segundos) en caso de que el dispositivo se esté reiniciando.
- Si el anillo luminoso parpadea mientras el dispositivo está apagado, espere 30 segundos como máximo.
- Comprueba si el cable de alimentación está enchufado tanto a la toma de corriente como firmemente en la parte posterior del dispositivo Amazon One. Además, compruebe que el cable no esté dañado.

- Compruebe la fuente de alimentación.
- Comprueba que todos los cables estén conectados correctamente a Amazon One y al hub USB.
- Reinicia el dispositivo desde la consola.
- Si reiniciar el dispositivo no soluciona el problema, desconecta el hub USB Amazon One de la fuente de alimentación y vuelve a enchufarlo.
- Si el problema continúa, póngase en contacto con AWS Support.

No puedo conectarme a una red Wi-Fi o a una red

Esto ocurre cuando el dispositivo pierde la conectividad.

Realice lo siguiente para solucionar este problema:

- Si está conectado a una red Wi-Fi, utilice otro dispositivo para comprobar si la red Wi-Fi aparece en las redes disponibles.
- Comprueba si el router Wi-Fi está encendido y dentro del alcance.
- El dispositivo se volverá a conectar una vez que la red se recupere.
- Si el problema persiste, póngase en contacto con el soporte de AWS.

Reiniciar un dispositivo con alertas activas

Cuando se solicita un reinicio desde la consola, la operación espera hasta 15 minutos hasta que el dispositivo reciba el comando e intente reiniciarse, incluso si está fuera de línea o tiene problemas de red.

Realice lo siguiente para solucionar este problema:

- Espere a que se complete el reinicio.
- Si el problema persiste, póngase en contacto con el soporte de AWS.

Error del sistema

Esto se debe a un error interno.

Realice lo siguiente para solucionar este problema:

- Seleccione Reiniciar en la pantalla para reiniciar la aplicación.

- Tras dos intentos, si el problema no se resuelve, póngase en contacto con AWS Support.

No se reconoce el código QR

Esto se debe a un código QR no autorizado o a un código QR caducado.

Realice lo siguiente para solucionar este problema:

- Selecciona Inténtalo de nuevo para volver a la pantalla de códigos QR.
- Cree un código QR nuevo en la consola de AWS y, a continuación, escanee el código QR válido.

No se puede leer el código QR

Esto ocurre cuando la aplicación no puede leer el código QR.

Realice lo siguiente para solucionar este problema:

- Selecciona Inténtalo de nuevo para volver a la pantalla de códigos QR.
- Si el problema persiste, cancele el flujo de trabajo de activación y reinícielo.

Se detectaron varios códigos QR

Esto ocurre cuando se escanean varios códigos QR.

Realice lo siguiente para solucionar este problema:

- Selecciona Inténtalo de nuevo para volver a la pantalla de códigos QR.
- Escanea solo un código QR válido a la vez.

La instancia del dispositivo no existe

Esto ocurre cuando la instancia del dispositivo se elimina o no existe en la consola de AWS.

Realice lo siguiente para solucionar este problema:

- Selecciona Inténtalo de nuevo para volver a la pantalla de códigos QR.
- Compruebe la instancia de dispositivo correcta en la consola de AWS. Si falta la instancia del dispositivo, póngase en contacto con su administrador.

- Crea un código QR nuevo para la instancia de ese dispositivo y, a continuación, escanea el nuevo código QR.

No se ha encontrado el sitio

Esto ocurre cuando el sitio se elimina o no existe en la consola de AWS.

Realice lo siguiente para solucionar este problema:

- Consulte la consola de AWS para ver la información del sitio. Si el sitio no existe, póngase en contacto con su administrador.

El código postal no coincide

Esto ocurre al introducir un código postal diferente al configurado para el dispositivo.

Realice lo siguiente para solucionar este problema:

- Selecciona Inténtalo de nuevo para volver a la pantalla de códigos postales.
- Comprueba si tienes el código postal correcto del sitio.
- Si el problema persiste, póngase en contacto con el administrador para comprobar el código postal del sitio en la consola de AWS.

Se acabó el tiempo de espera de Gateway

Esto ocurre cuando no hay respuesta de la puerta de enlace dentro de un tiempo específico.

Realice lo siguiente para solucionar este problema:

- Seleccione Reiniciar para reiniciar la aplicación.
- Tras dos intentos, si el problema no se resuelve, póngase en contacto con AWS Support.

No puedo configurar el dispositivo

Esto ocurre cuando la operación no pudo guardar la configuración en el disco del dispositivo.

Realice lo siguiente para solucionar este problema:

- Seleccione Reiniciar para reiniciar la aplicación.
- Tras dos intentos, si el problema no se resuelve, póngase en contacto con AWS Support.

El dispositivo se reinició con un mensaje de error y un código de error

Realice lo siguiente para solucionar este problema:

- Selecciona Reiniciar y deja que el dispositivo se recupere.
- Si el dispositivo no se recupera, desconecta el hub USB de la fuente de alimentación y vuelve a conectarlo.
- Si el problema continúa, póngase en contacto con AWS Support.

Logotipo de Amazon en la pantalla del dispositivo sin más actividad

Realice lo siguiente para solucionar este problema:

- Espere unos instantes (menos de 30 segundos) en caso de que el dispositivo se esté reiniciando.
- Desenchufe el hub USB de la fuente de alimentación y vuelva a conectarlo.
- Si el problema continúa, póngase en contacto con AWS Support.

No disponible temporalmente

Realice lo siguiente para solucionar este problema:

- Asegúrese de que las conexiones USB con el dispositivo/sistema anfitrión sean seguras.
- Desconecte y vuelva a conectar todos los cables que van al hub USB.
- Si el problema continúa, póngase en contacto con AWS Support.

Algo salió mal por nuestra parte

Esto ocurre cuando hay un error interno.

Realice lo siguiente para solucionar este problema:

1. Apague el dispositivo.

2. Desconéctelo de la fuente de alimentación.
3. Espera 30 segundos.
4. Vuelva a conectar el dispositivo a su fuente de alimentación.
5. Encienda el dispositivo.
6. Si el problema continúa, póngase en contacto con AWS Support.

Fuera de servicio temporalmente

Esto ocurre cuando Amazon One ha dejado el dispositivo fuera de servicio.

Realiza lo siguiente para solucionar este problema:

- Póngase en contacto con AWS Support.

El dispositivo Amazon One tiene daños físicos

Realice lo siguiente para solucionar este problema:

- Póngase en contacto con AWS Support para conocer los próximos pasos y proporcionar tantos detalles como sea posible, como qué ocurrió, cuándo ocurrió y por qué ocurrió.

No se puede leer la palma

Realice lo siguiente para solucionar este problema:

- Comprueba que el dispositivo Amazon One no tenga rayas ni manchas.
- Asegúrese de que la palma de la mano del cliente esté libre de oclusiones, como vendajes, mangas y una cantidad considerable de suciedad o aceite.
- Si el problema persiste y el dispositivo no lee ninguna palma de la mano, póngase en contacto con AWS Support.

Palm no se reconoce

Realice lo siguiente para solucionar este problema:

- Haga que el cliente intente usar la otra palma de la mano.

- Asegúrese de que el cliente ya esté inscrito. Si no es así, pídale que se inscriba en línea o en el dispositivo.
- Si el problema persiste y el dispositivo no detecta ningún contacto con la palma de la mano, póngase en contacto con AWS Support.

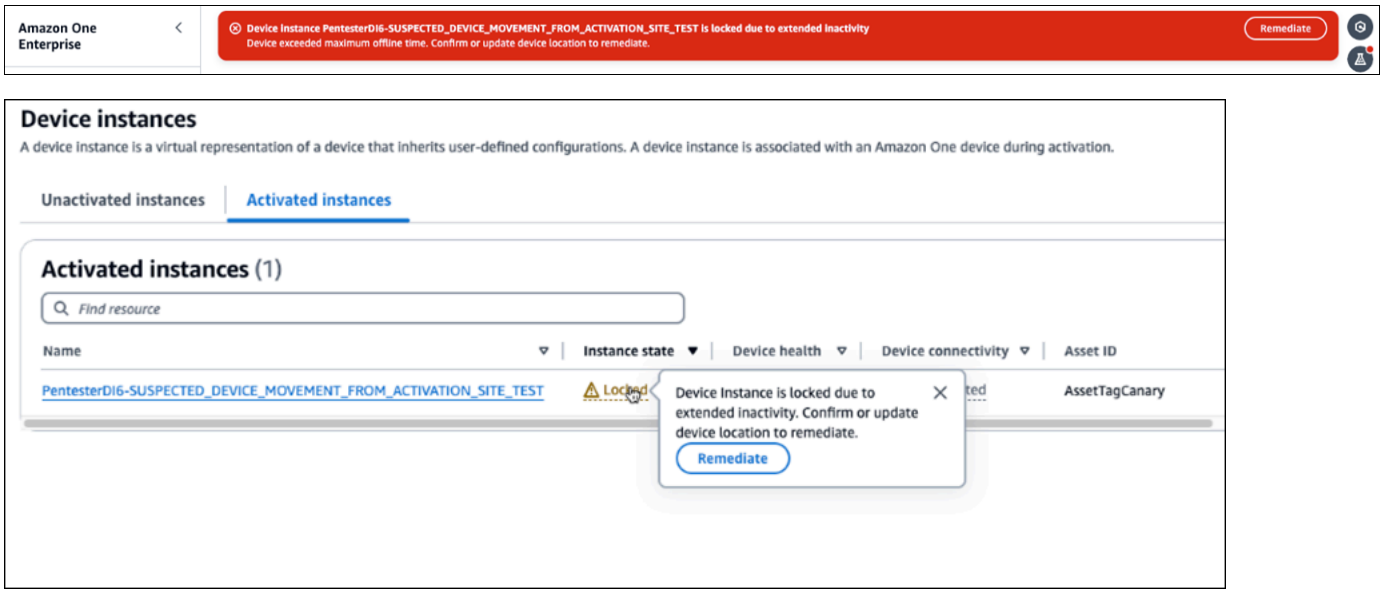
El dispositivo está bloqueado debido a una inactividad prolongada

Cuando el dispositivo sospecha que se ha movido del sitio de activación, bloquea a los usuarios. Esto ocurre cuando el dispositivo supera el máximo de 120 horas de tiempo sin conexión.

Realice lo siguiente para desbloquear el dispositivo:

1. Inicie sesión en la consola de AWS y elija la instancia del dispositivo.
2. En el mensaje de error que aparece en la parte superior de la página, selecciona Remediar.

   Opcionalmente: en Instancias activadas, seleccione Bloqueado y elija Remediar.



3. Si el dispositivo sigue en el sitio de activación original, seleccione Sí, el dispositivo está en este sitio.
4. Si el dispositivo está en un sitio diferente, selecciona No, el dispositivo está en un sitio diferente. Si selecciona No, se desactiva el dispositivo. Active el dispositivo en el nuevo sitio.

El dispositivo se bloqueó debido a una alteración

Por motivos de seguridad, el dispositivo Amazon One se bloqueará en caso de que se produzca alguna alteración.

Realiza lo siguiente para solucionar este problema:

- Póngase en contacto con AWS Support.

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 agregó la sección de roles vinculados a servicios	4 de febrero de 2025
Actualización	Se agregó: contenido basado en escenarios	10 de octubre de 2024
Actualización	Tema agregado: Solución de problemas de la consola Amazon One Enterprise	10 de octubre de 2024
Actualización	Tema añadido: Solución de problemas del dispositivo Amazon One Enterprise	10 de octubre de 2024
Actualización	Capítulo añadido: Configura ción de Amazon One Enterpris e	10 de octubre de 2024
Actualización	Tema añadido: Mantenimiento y limpieza de los dispositivos Amazon One Enterprise	10 de octubre de 2024
Actualización	Contenido reorganizado	10 de octubre de 2024
Actualización	Tema añadido: Instalación del hub de E/S de dispositivos Amazon One Enterprise para un acceso seguro	14 de agosto de 2024
Actualización	Tema añadido: Instalación de un dispositivo Amazon	5 de junio de 2024

	One Enterprise que se puede montar en la pared	
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.