aws

Guida per l'utente

Amazon Uno

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Uno: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Cos'è Amazon One Enterprise?

Amazon One Enterprise è un nuovo servizio di autenticazione palmare che fornisce ai dipendenti un accesso sicuro agli edifici e alle risorse aziendali, senza l'uso di badge o passcode PINs.

Argomenti

Dispositivo Amazon One

Il dispositivo Amazon One è progettato per Amazon One Enterprise, un servizio di identità sicuro e palmare per il controllo degli accessi aziendali. Tieni presente le seguenti specifiche del dispositivo:

- Input utente: Palm Biometrics, QR Code matching
- Interfaccia host: Wi-Fi (2.4 GHz e 5 GHz), Ethernet, 2x USB Type-A, 1 USB Type-B
- Feedback degli utenti: touchscreen da 5,5 pollici, Lightring, altoparlante, cuffie
- Protocollo di controllo dell'accesso fisico: OSDP e Wiegand
- Alimentazione: POE, ingresso 110/220 VAC, adattatore AC/DC in dotazione, 30 W @ 15 V
- Sicurezza: interruttori antimanomissione
- Dimensioni (HxWxD mm): 86 x 85 x 256

Console Amazon One Enterprise

Amazon One Enterprise include una console che può essere utilizzata nei seguenti modi:

- Un responsabile IT o di struttura utilizza Amazon One Enterprise per creare e gestire un sito. Il sito assomiglia a una sede fisica per le attività svolte dal team durante il monitoraggio e la gestione dei dispositivi e dei profili utente di Amazon One Enterprise. Le attività di IT o di facility manager includono:
  - Creazione di un sito per contenere tutte le istanze dei dispositivi Amazon One in una posizione fisica
  - Aggiungere un utente amministratore per la gestione del sito e un utente installatore per accedere ai codici QR di attivazione

- Un amministratore utilizza Amazon One Enterprise per creare istanze di dispositivi e gestire i dispositivi Amazon One. Le attività di amministrazione includono:
  - Creazione di un'istanza di dispositivo in un sito
  - Creazione di un modello di configurazione da applicare a un'istanza del dispositivo
  - Monitoraggio dello stato del dispositivo e aggiornamento delle configurazioni del dispositivo
  - Annullamento delle iscrizioni degli utenti

- Un installatore utilizza Amazon One Enterprise per accedere ai codici QR di attivazione per attivare i dispositivi. Le attività dell'installatore includono:
  - Accesso a un codice QR di attivazione sulla console
  - Selezione di un codice QR corrispondente all'istanza del dispositivo da attivare
  - Scansione del codice QR selezionato con il dispositivo Amazon One installato

Acquisto di dispositivi Amazon One

Contattaci per saperne di più su Amazon One Enterprise e un membro del team di Business Development ti contatterà per condividere maggiori dettagli sulla nostra offerta, compresi i prezzi, e rispondere a qualsiasi domanda tu possa avere.

Prezzi di Amazon One Enterprise

Contattaci per ulteriori informazioni sui prezzi di Amazon One Enterprise.

Come funziona Amazon One

Amazon One è un servizio biometrico basato sul cloud che utilizza un dispositivo Amazon One per autenticare un utente con i dati biometrici palmari. Puoi ordinare dispositivi Amazon One contattandoci.

Dopo aver installato il dispositivo Amazon One, puoi attivare e registrare i dispositivi con il tuo account AWS sulla console Amazon One e sull'applicazione di autenticazione. Puoi visualizzare i profili biometrici degli utenti registrati. Se necessario, puoi annullare la loro iscrizione ed eliminare i loro dati biometrici.

Amazon One Console funge da hub centralizzato per la gestione delle attività operative, come il tracciamento dei dispositivi e la visualizzazione delle fatture mensili. Gli utenti possono iscriversi scansionando i palmi delle mani presso le stazioni di registrazione supervisionate in loco. Una volta registrati, gli utenti possono entrare o uscire senza problemi da luoghi sicuri posizionando il palmo della mano su un dispositivo abilitato ad Amazon One.

Argomenti

Flusso di lavoro Amazon One

Di seguito viene descritto in dettaglio il flusso di lavoro di base di Amazon One:

1. Acquista e installa i dispositivi Amazon One contattandoci.
2. Dopo aver installato il dispositivo, attiva Amazon One.
3. Accedi al tuo account Amazon One.
4. Configura i dispositivi di registrazione e immissione degli utenti.
5. Registra i palmi delle mani dei dipendenti.
6. Utilizza le funzionalità di gestione e monitoraggio per garantire lo stato dei dispositivi, mantenere aggiornate le configurazioni e tenere traccia delle iscrizioni degli utenti per una supervisione completa.

Termini chiave di Amazon One

Questi sono i termini chiave per Amazon One:

- Sito: il cliente gestiva gli edifici fisici in cui il cliente installa i dispositivi Amazon One. Un sito deve soddisfare i requisiti di infrastruttura, rete e alimentazione dei dispositivi Amazon One.
- Dispositivo: un dispositivo biometrico Amazon One con scansione palmare per l'autenticazione.
- Istanza del dispositivo: una rappresentazione logica di un dispositivo con configurazioni. L'uso di istanze di dispositivi consente di scambiare dispositivi Amazon One ereditando automaticamente le configurazioni e i nomi precedentemente impostati. Un'istanza di dispositivo ha un nome definito dall'utente (convenzione di denominazione condivisa con il software di controllo degli accessi) e una serie di configurazioni di comunicazione. Le istanze del dispositivo hanno tre stati principali:
  - Richiede una configurazione
  - Pronto per l'attivazione
  - Attivo
- Modello di configurazione: un set completo di configurazioni applicato a un'istanza del dispositivo.

Configurazione della console Amazon One

Questo capitolo spiega i passaggi di base per iniziare a usare la console Amazon One.

Configurazione di un sito, istanze di dispositivi e modelli di configurazione: segui questi passaggi per creare un framework per aggiungere una posizione fisica in cui ospitare i tuoi dispositivi Amazon One, quindi per configurarli e gestirli utilizzando la console Amazon One Enterprise. Utilizzerai questo processo solo occasionalmente, o anche solo una volta, a seconda del numero di siti, istanze di dispositivi e modelli di configurazione.

Argomenti

Registrazione ad un account AWS

Se non hai un account AWS, completa la procedura seguente per crearne uno.

Registrazione per creare un account AWS

1. Aprire https://portal.aws.amazon.com/billing/signup
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Durante la registrazione per un account AWS, viene creato un utente root per l'account AWS stesso. L'utente root ha accesso a tutte le risorse e i servizi AWS in tale account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root

Al termine del processo di registrazione, riceverai una e-mail di conferma. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/ e selezionando Il mio account

Crea un utente con accesso amministrativo

Dopo aver registrato un account AWS, proteggi l'utente root del tuo account AWS, abilita AWS IAM Identity Center e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Argomenti

Protezione del tuo account AWS

Ora che hai effettuato l'accesso al tuo account Amazon One, proteggi il tuo account.

Per proteggere l'utente root del tuo account AWS

1. Accedi alla Console di gestione AWS come proprietario dell'account selezionando Utente root e inserendo l'indirizzo e-mail del tuo account AWS.
2. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso tramite utente root, consulta Signing in as the root user nella AWS Sign-In User Guide.
3. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitazione di un dispositivo MFA virtuale per l'utente root dell'account AWS (console) nella Guida per l'utente di IAM.

Creazione di un utente con accesso amministrativo

Ora che hai protetto il tuo account Amazon One, crea un utente con accesso amministrativo.

Per creare un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Enabling AWS IAM Identity Center nella AWS IAM Identity Center User Guide.
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo della directory IAM Identity Center come fonte di identità, consulta Configurare l'accesso utente con la directory IAM Identity Center predefinita nella AWS IAM Identity Center User Guide.

Accedere come amministratore

Ora che hai creato un utente con accesso amministrativo, accedi come amministratore.

Per accedere come utente con accesso amministrativo

- Accedi con il tuo utente IAM Identity Center, utilizzando l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per assistenza nell'accesso mediante un utente del Centro identità IAM, consulta Accesso al portale di accesso AWS nella Guida per l'utente di Accedi ad AWS.

Assegnazione dell'accesso a utenti aggiuntivi

Ora che hai effettuato l'accesso come amministratore, puoi assegnare l'accesso ad altri utenti.

Per assegnare l'accesso ad altri utenti

- Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

  Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center.

Aggiungi utenti Amazon One

Oltre agli utenti amministratori, puoi aggiungere anche utenti che non dispongono delle autorizzazioni di amministratore. Ad esempio, questi utenti potrebbero essere installatori che accedono alla console

Amazon One solo per recuperare i codici QR di attivazione dei dispositivi per attivare i dispositivi Amazon One.

Per aggiungere un utente Amazon One

1. Segui la procedura di accesso appropriata al tuo tipo di utente, come descritto in Come accedere alla AWS Guida per l'Accedi ad AWS utente.
2. Nel riquadro di navigazione, seleziona Utenti, quindi seleziona Aggiungi utenti.
3. Nella pagina Specify user details (Specifica dettagli utente), in User details (Dettagli utente), in User name (Nome utente), immetti il nome del nuovo utente. Questo è il nome di accesso per AWS.

   > **Note**
   >
   > Il numero e la dimensione delle risorse IAM in un Account AWS sono limitati. Per ulteriori informazioni, consulta le quote IAM e AWS STS. I nomi utente possono essere una combinazione di un massimo di 64 lettere, cifre e i seguenti caratteri: più (+), uguale (=), virgola (,), punto (.), segno (@), trattino basso (_) e trattino (-). I nomi devono essere univoci nell'account. Non fanno distinzione tra maiuscole e minuscole. Ad esempio, non è possibile creare due utenti chiamati TESTUSER e testuser. Quando un nome utente viene utilizzato in una policy o come parte di un ARN, il nome fa distinzione tra maiuscole e minuscole. Quando un nome utente viene visualizzato ai clienti nella console, ad esempio durante il processo di accesso, il nome utente non fa distinzione tra maiuscole e minuscole.
4. Ti verrà chiesto se stai fornendo l'accesso alla console a una persona. Seleziona Fornisci l'accesso utente a — opzionale. AWS Management Console
5. Seleziona Voglio creare un utente IAM.
6. Per Console password (Password console), scegli una delle opzioni seguenti:
   - Password generata automaticamente: all'utente viene assegnata una password generata casualmente che soddisfa i criteri relativi alle password dell'account. È possibile visualizzare o scaricare le password quando si arriva alla pagina Retrieve password (Recupera password).
   - Password personalizzata: all'utente viene assegnata la password inserita nel campo.
7. (Facoltativo) Per impostazione predefinita, gli utenti devono creare una nuova password al successivo accesso. L'opzione di accesso (scelta consigliata) è selezionata per garantire che all'utente venga richiesto di modificare la password al primo accesso.

> **Note**
>
> Se un amministratore ha attivato l'impostazione di policy per le password dell'account Allow users to change their own password (Consenti a tutti gli utenti di cambiare la loro password), questa casella di controllo non esegue alcuna operazione. In caso contrario, viene allegata automaticamente una policy AWS gestita denominata `IAMUserChangePassword` ai nuovi utenti. La policy concede agli utenti l'autorizzazione a modificare le proprie password.

8. Seleziona Avanti.
9. Nella pagina Imposta autorizzazioni, scegli Allega direttamente le politiche.
10. Seleziona le politiche che desideri allegare all'utente.

    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

> **Note**
>
> AmazonOneEnterpriseInstallerAccess la politica gestita fornirà all'utente l'accesso ai codici QR di attivazione solo nella console Amazon One Enterprise. Questa politica è ideale per le aziende che assumono una terza parte per installare i dispositivi Amazon One.

11. Seleziona Avanti.
12. (Facoltativo) Nella pagina Review and create (Rivedi e crea), in Tags (Tag), seleziona Add new tag (Aggiungi nuovo tag) per aggiungere i metadati all'utente collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'utilizzo dei tag con IAM, consulta Tagging delle risorse IAM.
13. Rivedi tutte le scelte che hai fatto fino a questo punto. Una volta pronto per continuare, seleziona Create user (Crea utente).
14. Nella pagina Retrieve password (Recupera password), ottieni la password assegnata all'utente:

    - Seleziona Show (Mostra) accanto alla password per visualizzare la password dell'utente in modo da poterla registrare manualmente.

- Seleziona Scarica .csv per scaricare le credenziali di accesso dell'utente come file.csv da salvare in un luogo sicuro.

15. Seleziona Email sign-in instructions (Istruzioni di accesso via e-mail). Il client di posta elettronica locale si apre con una bozza che è possibile personalizzare e inviare all'utente. Il modello dell'email include i seguenti dettagli per ciascun utente:

    - Nome utente
    - URL della pagina per l'accesso all'account. Utilizza il seguente esempio, sostituendo il numero ID dell'account corretto o l'alias dell'account:

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

    > **Important**
    >
    > La password dell'utente non è inclusa nel messaggio generato. È necessario fornirla all'utente rispettando le linee guida sulla sicurezza dell'organizzazione.

Creazione di un sito

Ora che hai effettuato l'accesso AWS Management Console, puoi utilizzare la console Amazon One per creare il tuo sito.

> **Important**
>
> Amazon One è disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale).

Per creare un sito

1. Apri la console Amazon One all'indirizzo https://console.aws.amazon.com/one-enterprise.
2. Scegli Vai alla panoramica.
3. Nel riquadro di navigazione, scegli Siti.
4. Scegli Crea siti.
5. In Informazioni sul sito, in Nome sito, inserisci un nome per il sito.

6. In Indirizzo fisico, inserisci l'indirizzo del sito in cui verranno installati i tuoi dispositivi Amazon One.
7. (Facoltativo) Per aggiungere un tag al sito, inserisci una coppia chiave-valore in Tag, quindi scegli Aggiungi nuovo tag. Per rimuovere questo tag prima di creare il sito, scegliete Rimuovi.
8. Scegli Crea sito per creare il sito.

Crea istanze di dispositivo

Ora che hai creato un sito nella Console di gestione AWS, puoi utilizzare la console Amazon One per creare istanze di dispositivi.

Per creare un'istanza di dispositivo

1. Apri la console Amazon One all'indirizzo https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli le istanze del dispositivo. Assicurati di essere nella scheda Istanze non attivate.
3. In Dettagli dell'istanza, scegli un sito dal menu a discesa Sito o crea un nuovo sito scegliendo il pulsante Crea sito.
4. Inserisci manualmente il nome di ogni singola istanza del dispositivo.
5. (Facoltativo) Per aggiungere un tag all'istanza del dispositivo, inserisci una coppia chiave-valore in Tag, quindi scegli Aggiungi nuovo tag. Per rimuovere questo tag prima di creare l'istanza del dispositivo, scegliete Rimuovi.
6. Scegli Crea istanze per creare le istanze del dispositivo.

> **Note**
>
> Nota: le istanze del dispositivo devono essere configurate prima che possa avvenire l'installazione.

Crea un modello di configurazione

Ora che hai creato le istanze del dispositivo, puoi utilizzare la console Amazon One per creare un modello di configurazione.

Per creare un modello di configurazione

1. Apri la console Amazon One all'indirizzo https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Modelli di configurazione.
3. Scegli Crea modello.
4. In Informazioni sul modello, in Nome modello, inserisci un nome per il modello di configurazione.
5. In Configurazioni del dispositivo, seleziona una modalità operativa.

   To configure Enrollment operating mode

   1. (Facoltativo) In Configurazione Wi-Fi, inserisci le tue credenziali Wi-Fi.
   2. (Facoltativo) Per aggiungere un tag al sito, inserisci una coppia chiave-valore in Tag, quindi scegli Aggiungi nuovo tag. Per rimuovere questo tag prima di creare il sito, scegliete Rimuovi.
   3. Scegli Configura.

   To configure Entry operating mode

   1. In Impostazioni del pannello di controllo, fornisci le impostazioni di comunicazione per consentire ai dispositivi Amazon One di comunicare con il tuo pannello di controllo.
   2. In Impostazioni del formato del badge, fornisci le impostazioni di configurazione che specificano il layout del formato del badge aziendale.
   3. (Facoltativo) In Configurazione Wi-Fi, inserisci le tue credenziali Wi-Fi.
   4. (Facoltativo) Per aggiungere un tag al sito, inserisci una coppia chiave-valore in Tag, quindi scegli Aggiungi nuovo tag. Per rimuovere questo tag prima di creare il sito, scegliete Rimuovi.
   5. Scegli Configura.

> **Important**
>
> È necessario configurare almeno un dispositivo Enrollment e un dispositivo Entry per abilitare tutte le funzionalità di Amazon One per un accesso sicuro.

Configura un'istanza del dispositivo per l'attivazione

Dopo aver creato un'istanza del dispositivo, configuri l'istanza del dispositivo con un modello di configurazione creato in precedenza (vediCrea un modello di configurazione) oppure puoi aggiungere configurazioni manualmente.

Per configurare un'istanza del dispositivo per l'attivazione

1. Apri la console Amazon One all'indirizzo https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Device Instances. Assicurati di essere nella scheda Istanze non attivate.
3. Seleziona una o più istanze da configurare.
4. Scegli Configura.
5. In Configurazioni del dispositivo, seleziona uno dei due metodi di input:

    a. Per l'opzione Usa modello, scegli un modello dal menu a discesa. Rivedi o apporta modifiche a queste informazioni di configurazione importate.

    Per l'opzione Crea modello, consultaCrea un modello di configurazione.

    b. Per l'opzione Inserimento manuale, selezionare una modalità operativa.

    To configure Enrollment operating mode

        a. (Facoltativo) In Configurazione Wi-Fi, fornite una credenziale Wi-Fi.
        b. (Facoltativo) Per aggiungere un tag al sito, inserisci una coppia chiave-valore in Tag, quindi scegli Aggiungi nuovo tag. Per rimuovere questo tag prima di creare il sito, scegliete Rimuovi.
        c. Scegli Configura.

    To configure Entry operating mode

        a. In Impostazioni del pannello di controllo, fornisci le impostazioni di comunicazione per consentire ai dispositivi Amazon One di comunicare con il tuo pannello di controllo.
        b. In Impostazioni del formato del badge, fornisci le impostazioni di configurazione che specificano il layout del formato del badge aziendale.
        c. (Facoltativo) In Configurazione Wi-Fi, fornite una credenziale Wi-Fi.

d. (Facoltativo) Per aggiungere un tag al sito, inserisci una coppia chiave-valore in Tag, quindi scegli Aggiungi nuovo tag. Per rimuovere questo tag prima di creare il sito, scegliete Rimuovi.

e. Scegli Configura.

6. Nella tabella Istanze non attivate, dovrebbe essere visualizzato lo stato dell'istanza.

7. Verifica che i codici QR di attivazione siano disponibili per l'attivazione. Nel riquadro di navigazione, scegli Codice QR di attivazione.
8. Dall'elenco a discesa Seleziona un sito, seleziona un sito.
9. In Informazioni sul sito, convalida l'indirizzo del sito.
10. In Codici QR di attivazione, ogni istanza del dispositivo ha un codice QR corrispondente. Scegli Ottieni codice QR per mostrare i codici QR di attivazione.

> **Important**
>
> È necessario configurare almeno un dispositivo Enrollment e un dispositivo Entry per abilitare tutte le funzionalità di Amazon One per un accesso sicuro.

Installazione e attivazione di Amazon One

Dopo aver configurato correttamente la console Amazon One, i passaggi successivi prevedono l'installazione dei dispositivi Amazon One sul tuo sito e la verifica che siano attivati correttamente. Questo processo include il posizionamento fisico dei dispositivi in aree designate, il collegamento alla rete e il completamento del processo di attivazione per consentire l'identificazione degli utenti e le funzionalità di transazione senza interruzioni. Una volta attivati, i tuoi dispositivi Amazon One saranno pronti a offrire un'esperienza sicura e senza contatto per i tuoi clienti o dipendenti.

> **Note**
>
> Questa sezione si concentra sull'installazione e utilizza un browser mobile per accedere e AWS Management Console ottenere i codici QR di attivazione del dispositivo.

Argomenti

Comprensione dei requisiti

Un dispositivo Amazon One può essere installato in qualsiasi sede aziendale o aziendale dotata di porte controllabili elettricamente.

Requisiti del pannello di controllo

I dispositivi Amazon One possono connettersi alla maggior parte dei pannelli di controllo degli accessi standard come lettore. I dispositivi Amazon One supportano i seguenti protocolli:

- OSDP (v1 e v2)

- Wiegand

Requisiti di rete

I dispositivi Amazon One devono essere sempre connessi a Internet per il normale funzionamento. La connettività Internet può essere fornita tramite Ethernet cablata o Wi-Fi. La larghezza di banda minima richiesta è di 10 Mbps.

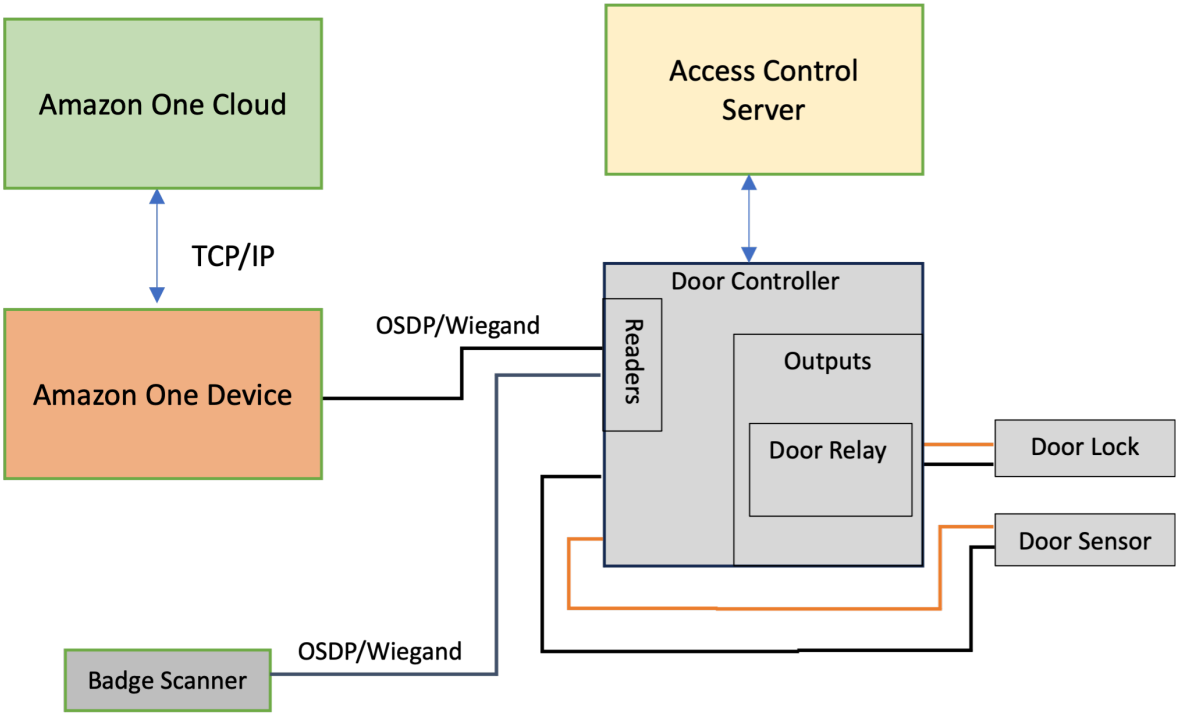
Requisiti di alimentazione

I dispositivi Amazon One possono essere alimentati in due modi:

- Utilizzando l'adattatore di alimentazione da 120 V fornito nella confezione.
- Utilizzando un dispositivo con tecnologia PoE+.

Comprensione dei concetti di installazione

Per proteggere adeguatamente l'accesso agli edifici, Amazon One consiglia di installare il dispositivo come parte di un tipico ambiente di controllo degli accessi, come descritto nel seguente diagramma a blocchi.



Un ambiente di controllo degli accessi è in genere costituito dai seguenti componenti:

- Dispositivo Amazon One: questo è il dispositivo di riconoscimento palmare che eseguirà l'autenticazione biometrica per identificare la persona che sta tentando di accedere a un'area sicura dell'edificio.
- Server di controllo degli accessi: questo componente controlla in genere i diritti di accesso degli utenti all'area sicura. I badge IDs delle persone che hanno accesso all'area sono memorizzati su questo server. Questo server memorizza nella cache i controller delle porte pertinenti IDs ai controller di porta appropriati.
- Controller della porta:
  - Un dispositivo Amazon One si collega al server Door Controller tramite un'interfaccia OSDP.
  - Se è necessaria un'interfaccia Wiegand, è possibile utilizzare un convertitore COTS. OSDP-to-Wiegand
  - Una volta completata l'autenticazione, il dispositivo Amazon One invia il badge ID dell'utente al controller della porta.
  - Il controller della porta risponde con una decisione, che consente quindi al dispositivo Amazon One di visualizzare un messaggio Accesso concesso o Accesso negato.
- Scanner per badge: uno scanner per badge viene in genere utilizzato per scansionare i badge RFID e inviare il numero del badge al server di controllo degli accessi. Con Amazon One, uno scanner di badge si collega al dispositivo Amazon One, permettendo agli utenti di scansionare i propri badge e associarli ai profili palmari.

Installazione di Amazon One Pedestal

Amazon One Pedestal è un componente chiave del sistema di identificazione e transazione Amazon One, progettato per offrire agli utenti un'esperienza senza interruzioni e senza contatto. Questo dispositivo è dotato di autenticazione biometrica sicura. Puoi integrarlo in varie località per fornire soluzioni di accesso o di pagamento senza intoppi.

Questa sezione fornisce i requisiti di localizzazione e step-by-step le istruzioni per l'installazione di Amazon One Pedestal. Una preparazione e un'installazione adeguate sono fondamentali per garantire che il sistema funzioni in modo sicuro ed efficiente, offrendo agli utenti un'esperienza fluida e affidabile.

Prerequisiti e preparazione per l'installazione di Amazon One Pedestal

Prima di iniziare l'installazione, assicurati che siano soddisfatte le seguenti condizioni per una configurazione sicura ed efficace:

- Requisiti di alimentazione: se utilizzate POE+ (Power over Ethernet) per alimentare il dispositivo, verificate che il cablaggio Cat6 sia già installato e che sia disponibile un iniettore o switch POE + per l'uso. In alternativa, se si utilizza l'alimentazione AC (120 V), assicurarsi che una presa AC accessibile si trovi a meno di 20 piedi dal piedistallo.
- Configurazione fisica: il pavimento deve essere orizzontale, pulito e privo di detriti per garantire un'installazione stabile e sicura del piedistallo.

- Posizionamento sul piedistallo: installa il piedistallo in un luogo in cui non blocchi porte, corsie o punti di accesso, permettendo un facile spostamento nell'area.
- Gestione dei cavi: posiziona e fissa tutti i cavi in eccesso all'interno del piedistallo per evitare ingombri e prevenire potenziali danni durante il normale utilizzo.

Una volta confermati questi prerequisiti, è possibile procedere con il processo di installazione.

Per installare Amazon One Pedestal

1. Rimuovi Amazon One Pedestal dalla confezione.
2. Rimuovi lo sportello svitando entrambe le viti antimanomissione M4.
3. Collegare il cavo di alimentazione.
4. Fate passare il cavo attraverso il foro della piastra di base del piedistallo.
5. Avvolgi il cavo di alimentazione in eccesso all'interno del piedistallo.
6. Fate passare il cavo Ethernet (Cat5E o superiore) attraverso la piastra inferiore del piedistallo e collegatelo alla porta Ethernet.
7. Installa un anello in ferrite sul cavo Ethernet a 2 pollici sopra la base del piedistallo.
8. Alimenta il cavo RS485 seriale dal pannello di controllo degli accessi (o dal lettore di badge) al piedistallo, con 1 piede di lunghezza in più.
9. Installa un anello in ferrite sul RS485 cavo a 2 pollici sopra la base del piedistallo.
10. Collega l'alimentazione alla presa e conferma che il dispositivo Amazon One si accenda.
11. Ricollega la porta al piedistallo e riavvita le due viti antimanomissione M4 per fissarla.

Dopo aver installato il tuo dispositivo Amazon One, sei pronto per attivarlo.

Installazione del dispositivo Amazon One montabile a parete

Il dispositivo Amazon One montabile a parete è un sistema di identificazione biometrica versatile e compatto progettato per offrire un'esperienza senza interruzioni e senza contatto agli utenti in vari ambienti. Utilizza una tecnologia avanzata di riconoscimento palmare per l'accesso o il pagamento sicuri, il che lo rende ideale per luoghi ad alto traffico come spazi commerciali, ingressi di uffici e altro ancora.

Questa sezione descrive i requisiti di localizzazione necessari e i passaggi dettagliati per l'installazione del dispositivo Amazon One montabile a parete per garantire prestazioni e sicurezza ottimali.

Prerequisiti e preparazione per l'installazione del dispositivo Amazon One montabile a parete

Prima di iniziare l'installazione, assicurati che siano soddisfatte le seguenti condizioni per garantire che il dispositivo funzioni in modo efficace e sia configurato correttamente nel tuo spazio:

- Solo per uso interno: il dispositivo Amazon One montabile a parete è destinato esclusivamente all'uso interno, quindi assicurati che sia installato in un ambiente appropriato.
- Requisiti della parete: la parete deve essere orizzontale per garantire il corretto allineamento e la funzionalità del dispositivo.
- Altezza di montaggio: dopo l'installazione, la parte superiore del supporto a parete deve essere posizionata a non più di 44-46 pollici da terra, garantendo un facile accesso per gli utenti.
- Gestione dei cavi: assicurati che tutti i cavi in eccesso siano collocati dietro il supporto a parete e fissati saldamente per evitare danni o ingombri.
- Power Over Ethernet (PoE++): se utilizzi Power Over Ethernet (PoE++), verifica che sia disponibile uno switch o un iniettore (midspan) IEEE 802.3bt (Tipo 3) Classe 6 PoE++ (end span). La fonte PoE++ deve essere elencata o certificata e conforme agli standard IEC 62368-1. È importante sottolineare che la fonte PoE++ deve trovarsi all'interno dello stesso edificio del dispositivo. Utilizzate solo una fonte PoE++ approvata con il dispositivo AOE.
- Ingresso di alimentazione a 15 V DC: se si utilizza un ingresso di alimentazione a 15 V DC, assicurarsi che venga utilizzato solo un alimentatore NEC di classe 2 o un alimentatore approvato a potenza limitata. L'alimentatore deve essere elencato o certificato per motivi di sicurezza e compatibilità.

Utensili necessari

- Punta da trapano da 1/4» per pareti asciutte o murature se sono necessari ancoraggi a parete
- Spelafili
- Punta da trapano da 7/64 pollici per la perforazione di fori pilota
- Cacciavite #2 Phillips
- Cacciavite a testa piatta da 0,5 mm x 2 mm
- Driver Torx T12 Secure
- Matita

- Livello

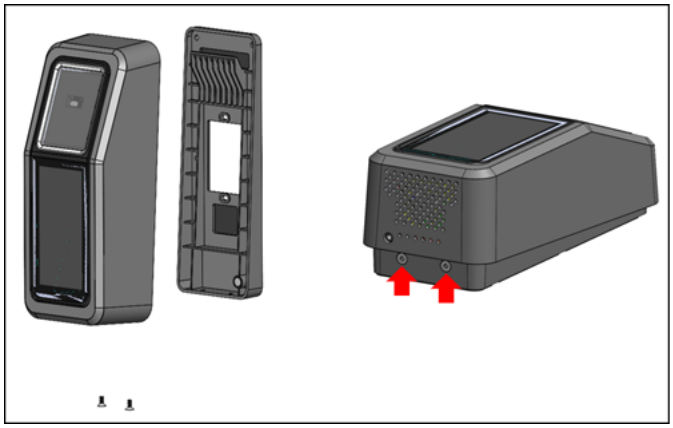
Incluso nel dispositivo Amazon One montabile a parete

- 6 x ancoraggi per cartongesso #8
- 6 x viti #8 -32 lunghe 1 pollice
- 2 x viti a macchina #6 -32 da 1 pollice
- 2 connettori per morsettiera a 6 posizioni
- 2 viti a testa piatta Torx Security M4x10

Una volta confermati questi prerequisiti, puoi procedere con i passaggi di installazione per montare e configurare in modo sicuro il dispositivo Amazon One montabile a parete.

Per installare la piastra di montaggio a parete per il tuo dispositivo Amazon One

1. Rimuovi il dispositivo Amazon One dalla confezione.
2. Separa la piastra di montaggio dal tuo dispositivo Amazon One rimuovendo le due viti di sicurezza Torx inferiori.

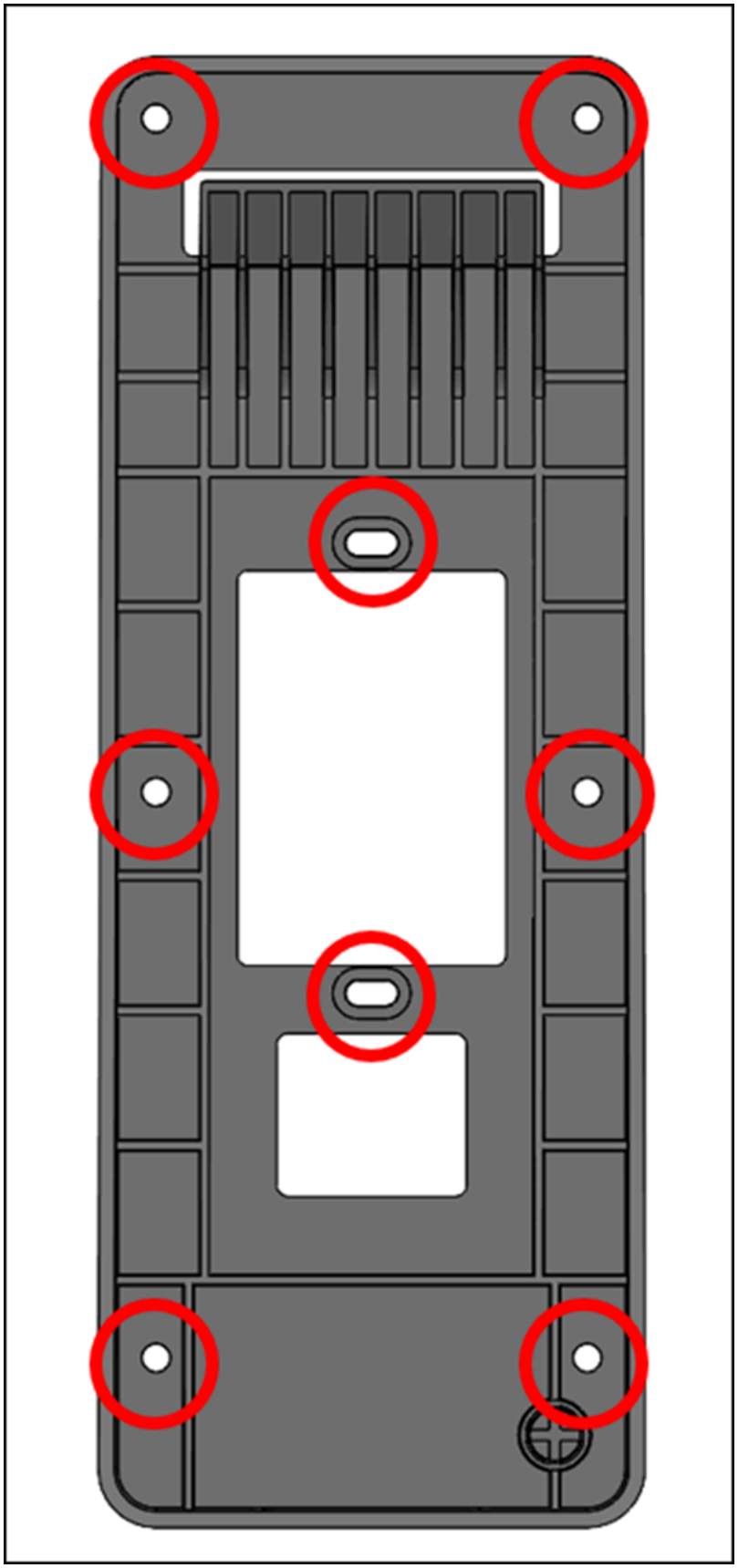


3. Posizionare la piastra di montaggio sulla parete nella posizione desiderata. Utilizzate la staffa come modello per contrassegnare i sei fori esterni per le viti, come mostrato nell'immagine seguente.

   (Facoltativo) Se nella posizione di installazione è disponibile una scatola a gruppo singolo, effettuate le seguenti operazioni:

   - Montate liberamente la piastra sulla scatola del gruppo inserendo le viti della macchina #6 -32 in dotazione attraverso i fori oblunghi.

- Accertarsi che la piastra di montaggio sia a livello.
- Utilizzate la piastra di montaggio come modello per contrassegnare le sei posizioni delle viti con una matita. È possibile utilizzare i fori oblunghi e la vite #6 -32 come supporto aggiuntivo per la piastra di montaggio. Non utilizzare le posizioni delle viti #6 -32 come mezzo principale per montare la piastra a parete.



4. Se lo installi su superfici in stucco, cartongesso, mattoni o cemento, fai dei fori da 1/4» in ogni punto contrassegnato, quindi installa gli ancoraggi a parete premendoli nel foro fino a quando l'ancoraggio non è a filo con la parete.

   Se si monta su una superficie in legno, gli ancoraggi non sono necessari e sono necessari solo fori pilota da 7/64 pollici nei punti contrassegnati.
5. Fissate liberamente la piastra da parete alla parete utilizzando le viti per legno #8 nelle posizioni di ancoraggio.
6. Dopo aver posizionato tutti i dispositivi di fissaggio, assicurati che la piastra di montaggio sia orizzontale.
7. Stringere le viti per fissare la piastra di montaggio alla parete.

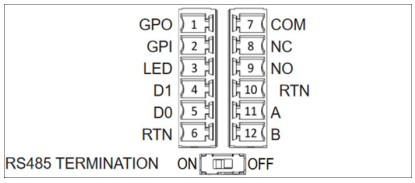
Per collegare il tuo dispositivo Amazon One montabile a parete

Puoi configurare il dispositivo Amazon One con i protocolli di controllo degli accessi OSDP e Weigand. Per semplificare l'installazione, il dispositivo Amazon One utilizza connettori a morsettiera (Mfg P/N: Phoenix Contact 1767694). Hai anche la possibilità di configurare il dispositivo Amazon One per controllare direttamente i dispositivi esterni utilizzando il relè interno o le connessioni General Purpose Input and Output.

1. Per determinare la configurazione di cablaggio appropriata per la tua applicazione, consulta lo schema e la tabella delle connessioni seguenti.

   Per le caratteristiche elettriche dettagliate dei segnali, fare riferimento alle istruzioni di cablaggio.

   Connessioni



Pin	Connessione	Descrizione	Utilizzo	
1	GPO	uscita per uso generico	Segnale di uscita digitale - Opzionale	

Pin	Connessione	Descrizione	Utilizzo	
2	GPI	Input per uso generico	Segnale di ingresso digitale: opzionale	
3	CONDOTTO	LED Wiegand	LED Wiegand — opzionale	
4	D1	Wiegand D1	Wiegand data 1 - Filo bianco	
5	D0	Wiegand D0	Dati Wiegand 0 - Filo verde	
6	RTN	Ritorno del segnale	Wiegand Ground — Filo nero	
7	Com	Relè comune	Relè di contatto comune - Filo bianco	
8	NC	Relè normalmente chiuso	Relè di contatto normalmente chiuso - Filo arancione	
9	NO	Relè normalmente aperto	Relè di contatto normalmente aperto - Filo giallo	
10	RTN	Ritorno del segnale	Ritorno OSDP: filo nero	
11	A	RS485_A/D1/ Orologio	OSDP D1 — Filo bianco	

Pin	Connessione	Descrizione	Utilizzo	
12	B	RS485_B/D0/ Dati	OSDP D0 — Filo verde	

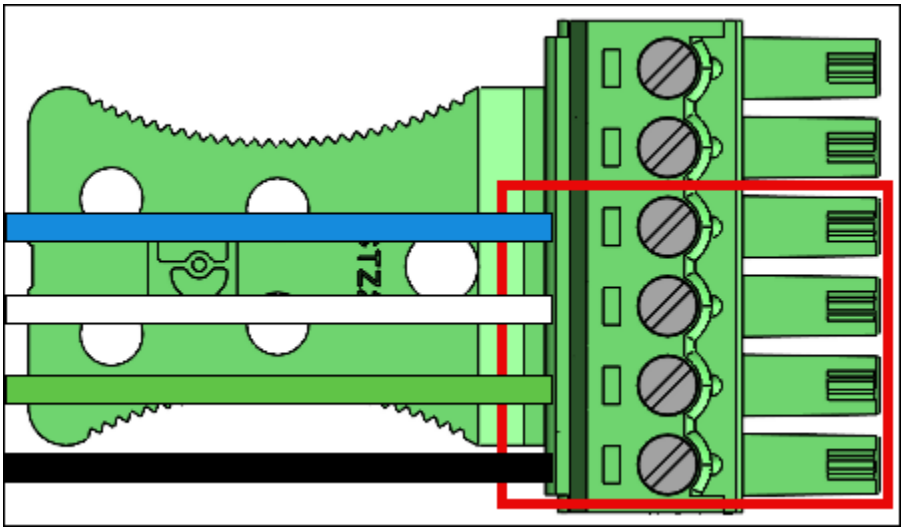
2. Quando si installa un filo, togliere 3 mm-5 mm dall'estremità del filo.
3. Inserire l'estremità spellata del filo nella posizione del terminale desiderata.
4. Utilizzando un cacciavite a testa piatta, ruotate la vite di fissaggio del terminale in senso orario per fissarla sul filo finché non aderisce perfettamente. Non stringere eccessivamente.
5. Dopo il fissaggio, tira delicatamente il filo per assicurarti che sia posizionato.
6. Dopo aver effettuato i collegamenti necessari, inserisci la spina nella presa corrispondente della morsettiera del tuo dispositivo Amazon One.
7. Inserisci il cavo Ethernet Cat6 nella presa. RJ45
8. Posiziona il dispositivo Amazon One in modo che il gancio sulla piastra a muro scivoli nell'apertura sul retro del dispositivo.
9. Assicurati che i cavi non rimangano intrappolati tra il dispositivo e la piastra di montaggio e lascia che il dispositivo ruoti e si posizioni in posizione.
10. Fissa il tuo dispositivo Amazon One alla piastra di montaggio con due viti a testa piatta Torx Security M4x10.
11. Stringi a mano le viti. Non stringere eccessivamente.

Per collegare il tuo dispositivo Amazon One montabile a parete

Installa solo i cavi necessari per la tua applicazione.

Connessioni Wiegand

- Inserire il filo blu nel Pin 3 (LED).
- Inserire il filo bianco nel Pin 4 (D1).
- Inserire il filo verde nel Pin 5 (D0).
- Inserire il filo nero nel Pin 6 (RTN).



Cablaggio di uscita Wiegand

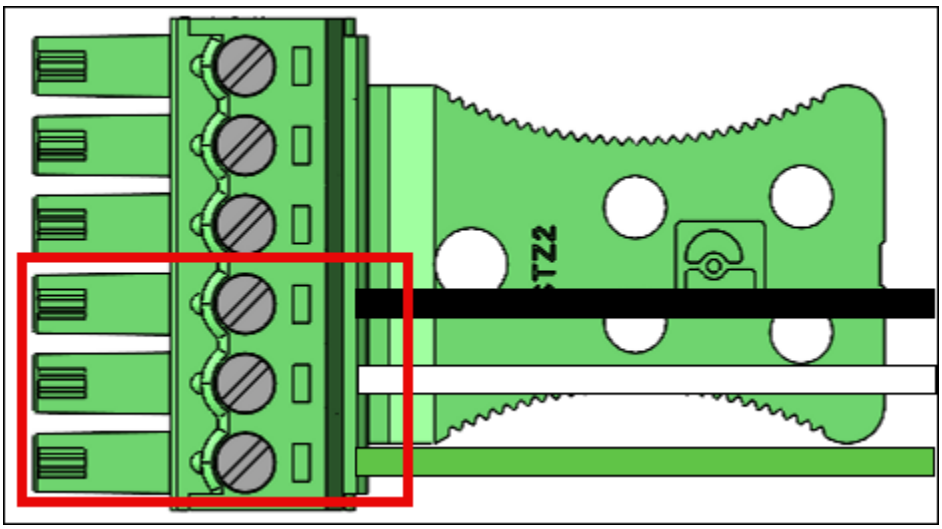
Pin	Connessione	Descrizione	Utilizzo
3	CONDOTTO	LED Wiegand	Ingresso LED Wiegand — opzionale (5V TTL)
4	D1	Wiegand D1	Uscita Wiegand D1 (5 V TTL)
5	D0	Wiegand D0	Uscita Wiegand D0 (5 V TTL)
6	RTN	Ritorno del segnale	Riferimento Wiegand GND

Ruotare RS485 l'interruttore di terminazione su «ON» se il dispositivo è l'ultima unità sulla linea. Questo interruttore attiva la terminazione del resistore da 120 Ohm sulla linea.

RS485 connessioni

- Inserire il filo nero nel Pin 10 (RTN).
- Inserire il filo bianco nel Pin 11 (A).

- Inserire il filo verde nel Pin 12 (B).

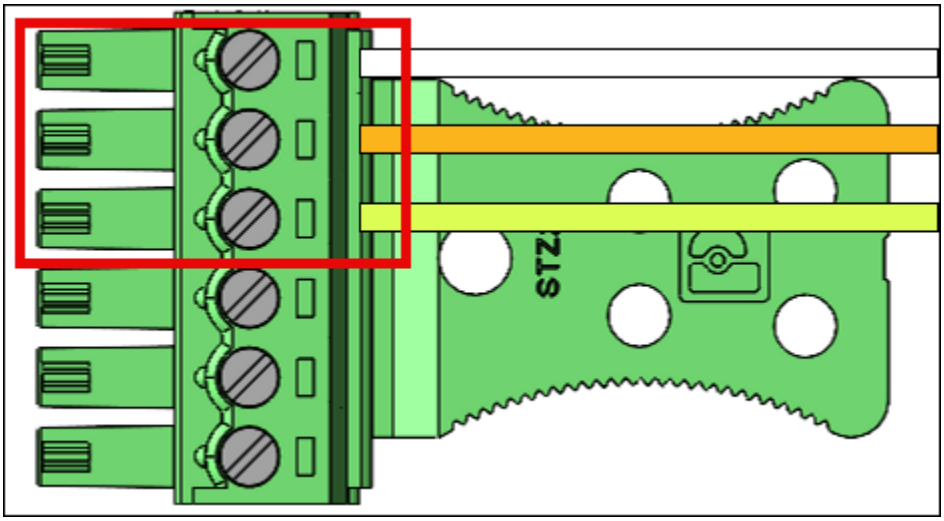


RS485 cablaggio

Pin	Connessione	Descrizione	Utilizzo
10	RTN	Ritorno del segnale	Ground (Terreno)
11	A	RS485_A/D1/ Orologio	RS485 segnale non invertente
12	B	RS485_B/D0/ Dati	RS485 segnale di inversione

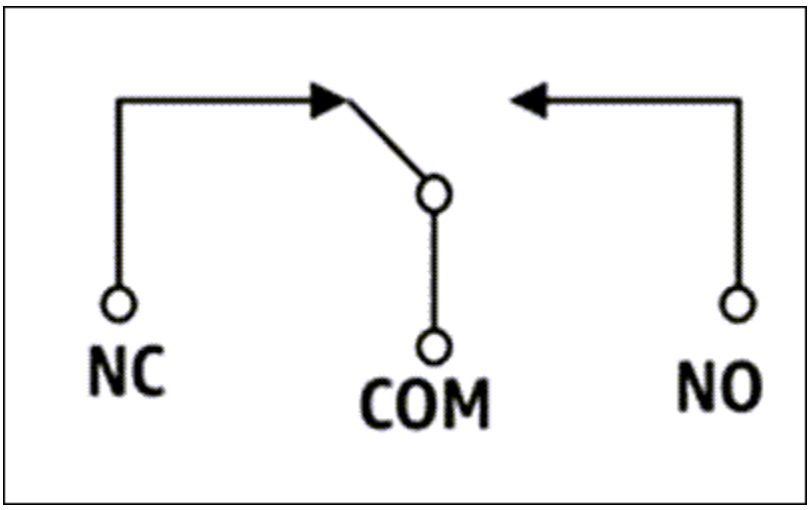
connessioni a relè

- Inserire il filo bianco nel Pin 7 (COM).
- Inserire il filo arancione nel Pin 8 (NC).
- Inserire il filo giallo nel Pin 9 (NO).



Cablaggio del relè

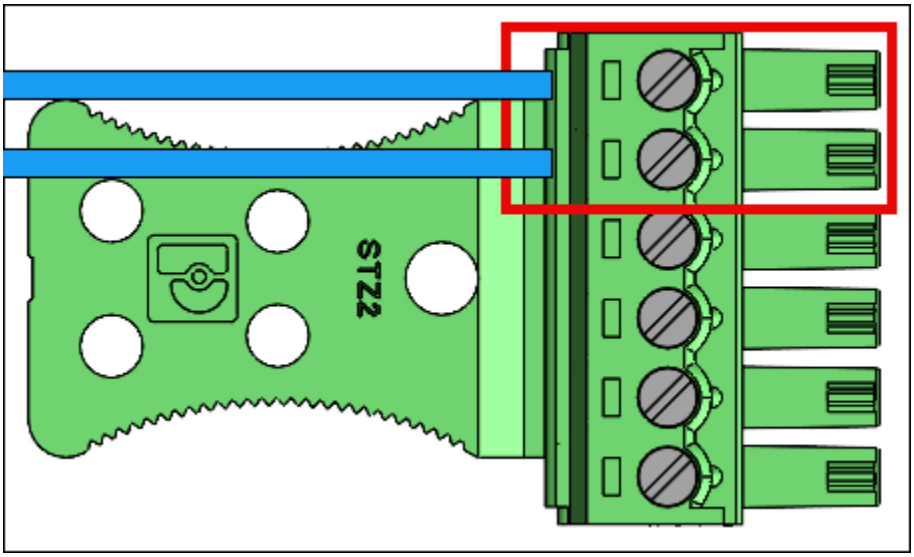
Pin	Connessione	Descrizione	Utilizzo
7	COM	Relè comune	Relè di contatto comune - Filo bianco
8	NC	Relè normalmente chiuso	Relè di contatto normalmente chiuso - Filo arancione
9	NO	Relè normalmente aperto	Relè di contatto normalmente aperto - Filo giallo



Il relè deve funzionare secondo i valori di sicurezza specificati 30VAC/60VDC, 60W max.

Connessioni di ingresso/uscita digitali

- Inserire il cavo blu nel Pin 1 (GPO).
- Inserire il filo blu nel Pin 2 (GPI).



Cablaggio digitale di ingresso/uscita

Pin	Connessione	Descrizione	Utilizzo	
1	GPO	uscita per uso generico	Segnale di uscita digitale (5V)	

Pin	Connessione	Descrizione	Utilizzo	
2	GPI	Input per uso generico	Segnale di ingresso digitale (3,6 V - 5 V)	

- Le connessioni di ingresso/uscita digitali devono funzionare come indicato.

Dopo aver installato il tuo dispositivo Amazon One, sei pronto per attivarlo.

Installazione di Amazon One Device I/O Hub per un accesso sicuro

Il dispositivo Amazon One con I/O Hub è parte integrante del sistema Amazon One Enterprise, progettato per migliorare la sicurezza e semplificare il controllo degli accessi per una varietà di ambienti. Il dispositivo sfrutta il riconoscimento biometrico palmare per fornire un'autenticazione sicura e senza contatto per gli utenti, il che lo rende ideale per l'uso in aree ad alta sicurezza come edifici per uffici, punti di accesso limitati o strutture che richiedono una gestione degli accessi senza interruzioni. L'I/O Hub funge da ponte tra il dispositivo e l'infrastruttura di sicurezza esistente, abilitando la comunicazione con serrature, allarmi e altri sistemi di controllo degli accessi.

Questa sezione fornisce i requisiti di localizzazione e step-by-step le istruzioni per l'installazione del dispositivo Amazon One con I/O Hub. Una preparazione e un'installazione adeguate sono fondamentali per garantire che il sistema funzioni in modo sicuro ed efficiente, offrendo agli utenti un'esperienza fluida e affidabile.

Prerequisiti e preparazione per l'installazione di Amazon One Device con I/O Hub

Prima di iniziare l'installazione, assicurati che siano soddisfatte le seguenti condizioni per garantire una configurazione sicura, protetta ed efficace:

- Solo per uso interno: il dispositivo Amazon One con I/O Hub è progettato esclusivamente per uso interno. Assicurati che sia installato in un ambiente appropriato.
- Power Over Ethernet (PoE++): se utilizzi Power Over Ethernet (PoE++), verifica che sia disponibile uno switch PoE++ IEEE 802.3bt (Tipo 3) Classe 6 (end span) o un iniettore (midspan). La fonte PoE++ deve essere elencata o certificata e conforme agli standard IEC 62368-1. È importante sottolineare che la fonte PoE++ deve trovarsi all'interno dello stesso edificio del dispositivo. Utilizzate solo una fonte PoE++ approvata con il dispositivo AOE.

- Ingresso di alimentazione a 15 V DC: se si utilizza un ingresso di alimentazione a 15 V DC, assicurarsi che venga utilizzato solo un alimentatore certificato NEC di classe 2 o a potenza limitata. L'alimentatore deve essere elencato o certificato per motivi di sicurezza. Per ulteriori dettagli, consulta la sezione DC opzionale riportata di seguito.

Strumenti necessari

- Spelafili
- Cacciavite #2 Phillips
- Cacciavite a testa piatta da 0,5 mm x 2 mm

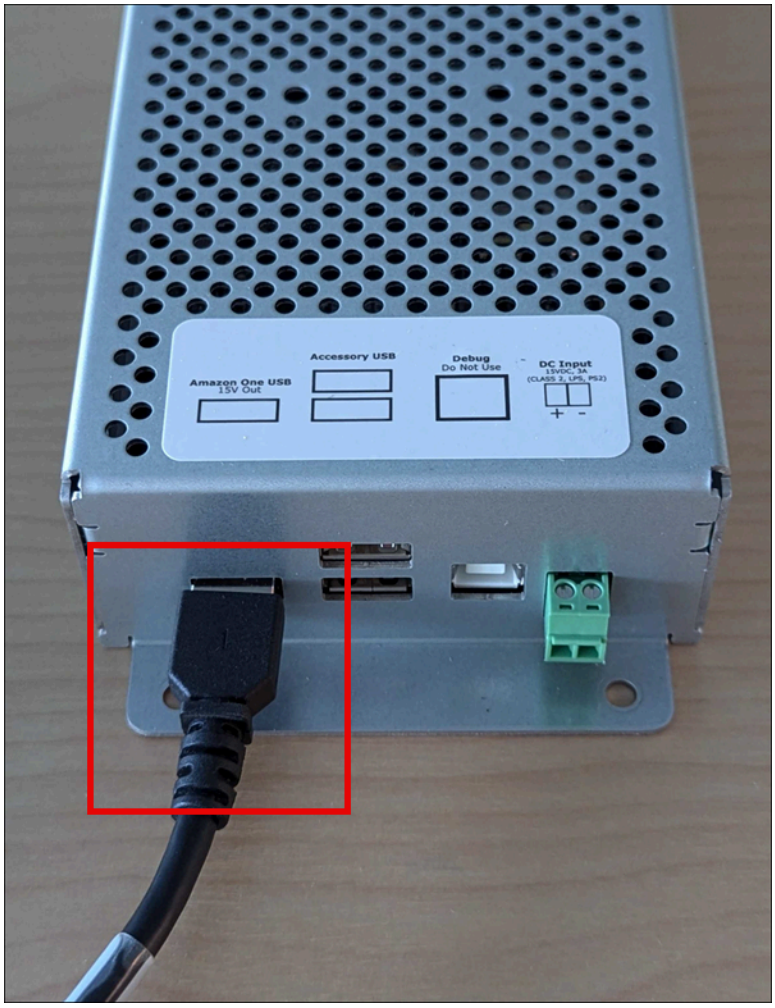
Incluso nel dispositivo Amazon One con I/O Hub

- 2 connettori per morsettiera a 6 posizioni
- Connettore DC
- Cavo alimentazione/dati da 72"

Una volta confermati questi prerequisiti, puoi procedere con il processo di installazione, garantendo una configurazione sicura ed efficiente del tuo dispositivo Amazon One con I/O Hub. Una preparazione adeguata contribuirà a garantire che il dispositivo funzioni come previsto e si integri senza problemi nel tuo sistema di accesso sicuro.

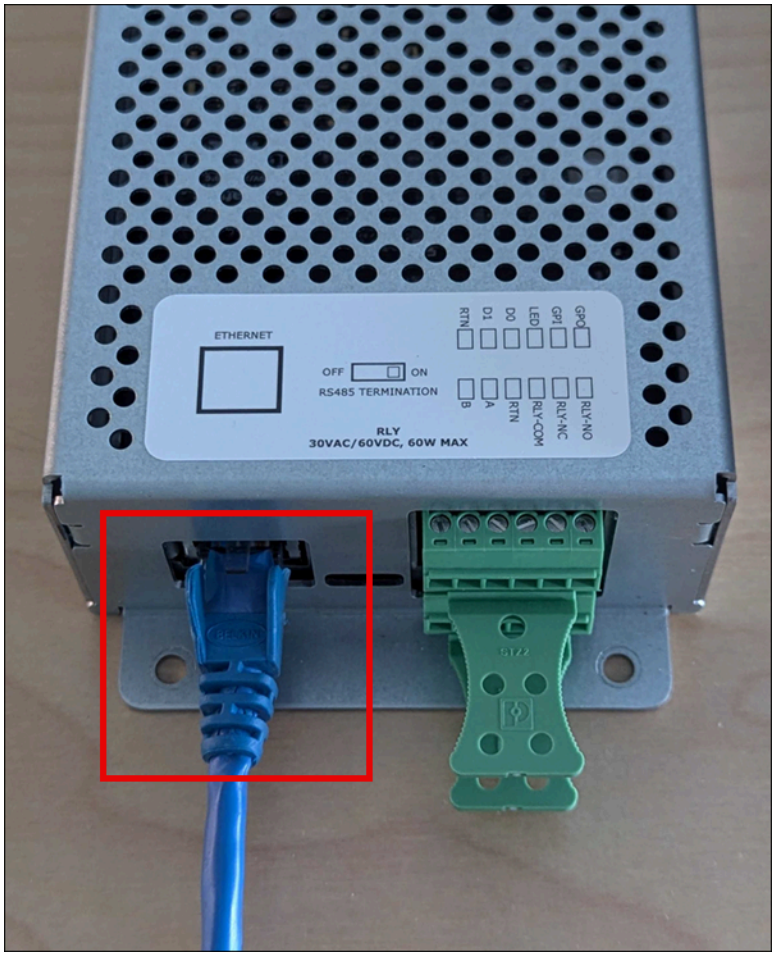
Per installare l'hub di I/O per il tuo dispositivo Amazon One

1. Rimuovi il dispositivo Amazon One con I/O Hub dalla confezione.
2. Proteggi l'hub I/O nella posizione desiderata.
3. Collega il cavo USB Amazon One alla porta dell'hub I/O.



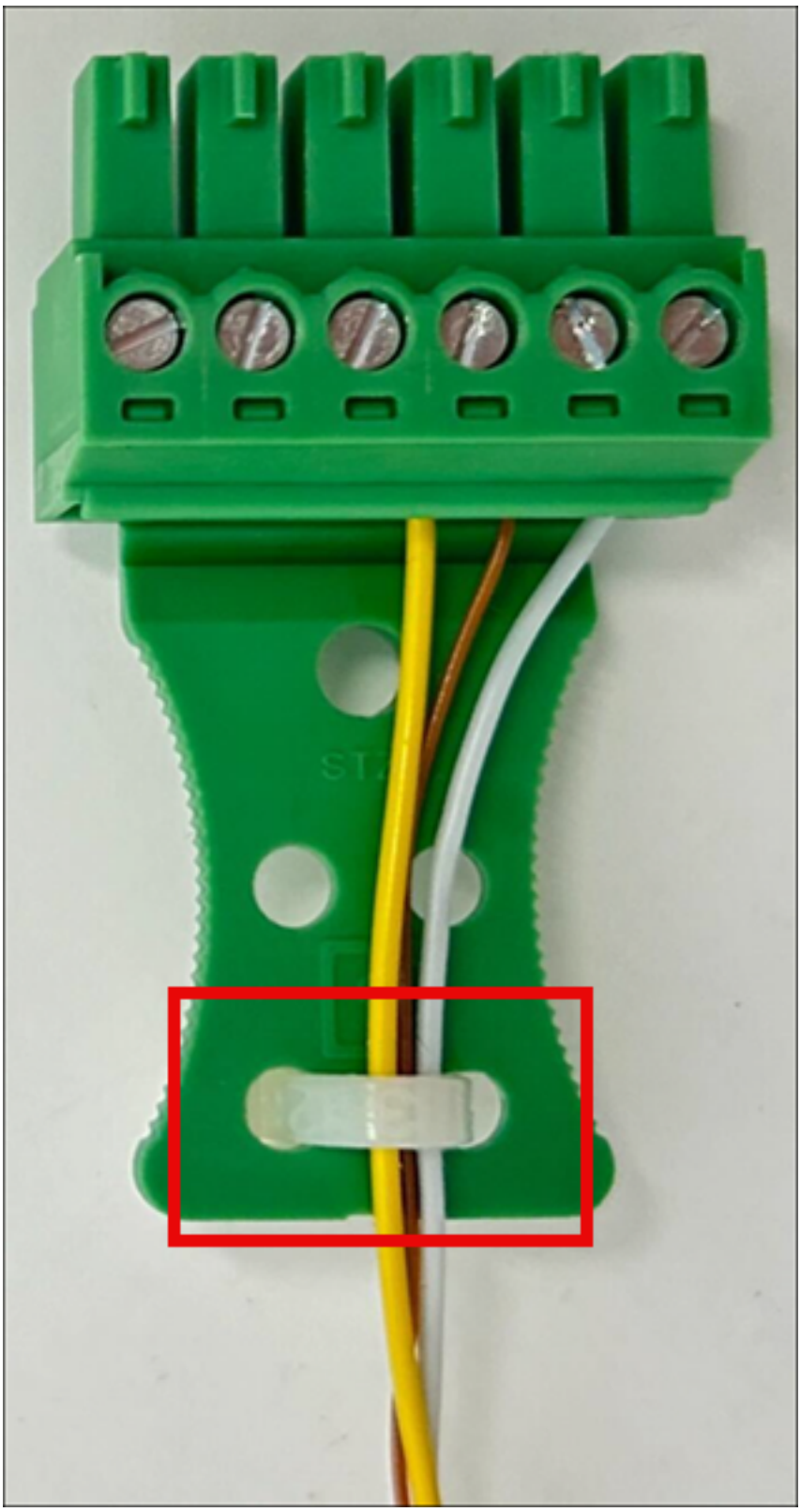
4. Per l'alimentazione POE++, collegare il cavo Ethernet dalla sorgente POE++ alla porta dell'hub I/O.

   Opzionale: per l'alimentazione DC, fare riferimento alla sezione relativa all'installazione del cablaggio DC riportata di seguito.



Per collegare l'hub di I/O per il tuo dispositivo Amazon One

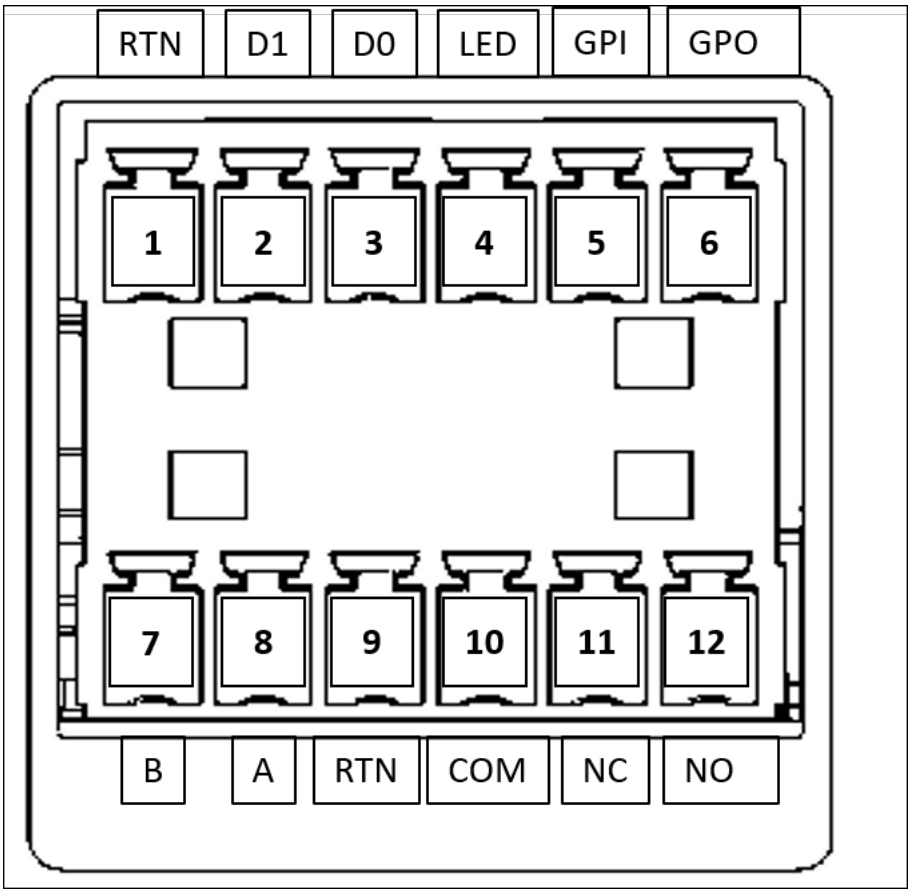
- Installa un anello antigoccia per evitare che liquidi scorrano accidentalmente lungo il cavo e finiscano nell'hub I/O.
- Collegare un morsetto antistrappo per proteggere i fili da danni o sollecitazioni, come mostrato nell'immagine seguente.



1. Inserire i connettori della morsettiera nell'hub I/O.

2. Inserite solo i cavi necessari per l'applicazione tramite i connettori della morsettiera. Fare riferimento alla tabella e agli schemi di cablaggio seguenti.

Connessioni



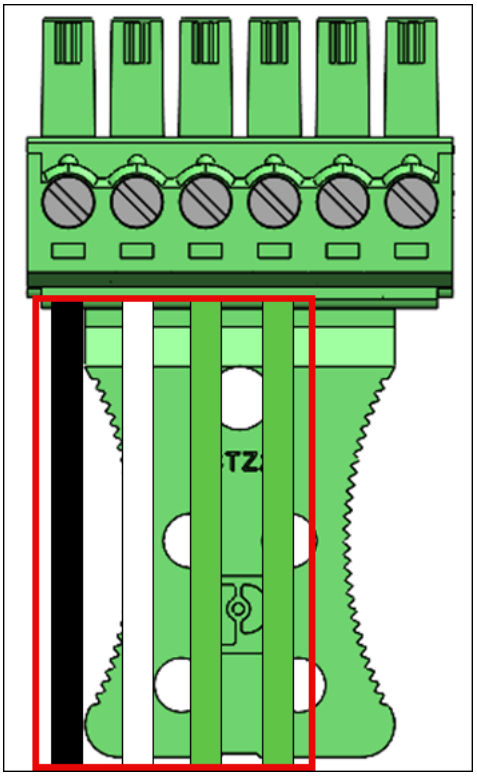
Pin	Connessione	Descrizione	Utilizzo	
1	RTN	Ritorno del segnale	Wiegand ground — Filo nero	
2	D1	Wiegand D1	Wiegand Data 1 - Filo bianco	
3	D0	Wiegand D0	Dati Wiegand 0 - Filo verde	
4	CONDOTTO	LED Wiegand	LED Wiegand — opzionale	

Pin	Connessione	Descrizione	Utilizzo	
5	GPI	Input per uso generico	Segnale di ingresso digitale: opzionale	
6	GPO	uscita per uso generico	Segnale di uscita digitale - Opzionale	
7	B	RS485_B/D0/ Dati	OSDP D0 — Filo verde	
8	A	RS485_A/D1/ Orologio	OSDP D1 — Filo bianco	
9	RTN	Ritorno del segnale	Ritorno OSDP: filo nero	
10	COM	Relè comune	Relè di contatto comune - Filo bianco	
11	NC	Relè normalmente chiuso	Relè di contatto normalmente chiuso - Filo arancione	
12	NO	Relè normalmente aperto	Relè di contatto normalmente aperto - Filo giallo	

Connessioni Wiegand

- Inserire il filo nero nel Pin 1 (RTN).
- Inserire il filo bianco nel Pin 2 (D1).
- Inserire il filo verde nel Pin 3 (D0).

- Opzionale: inserire il filo verde nel Pin 4 (LED).



Connessioni a relè

- Inserire il filo bianco nel Pin 10 (COM).
- Inserire il filo arancione nel Pin 11 (NC).
- Inserire il filo giallo nel Pin 12 (NO).

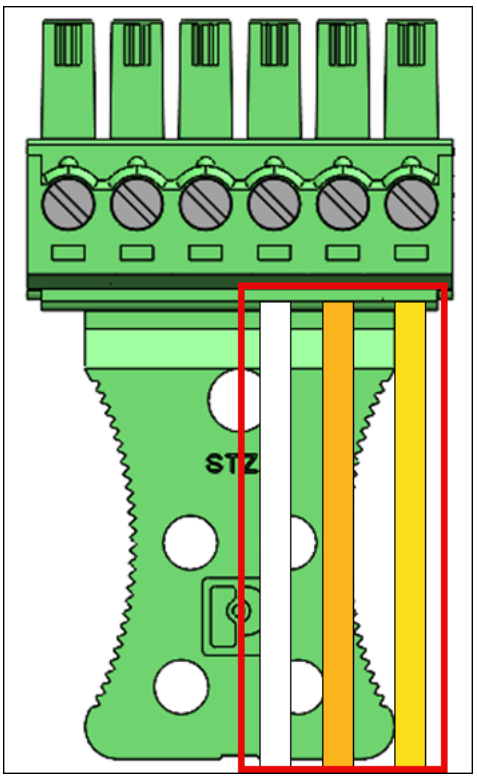
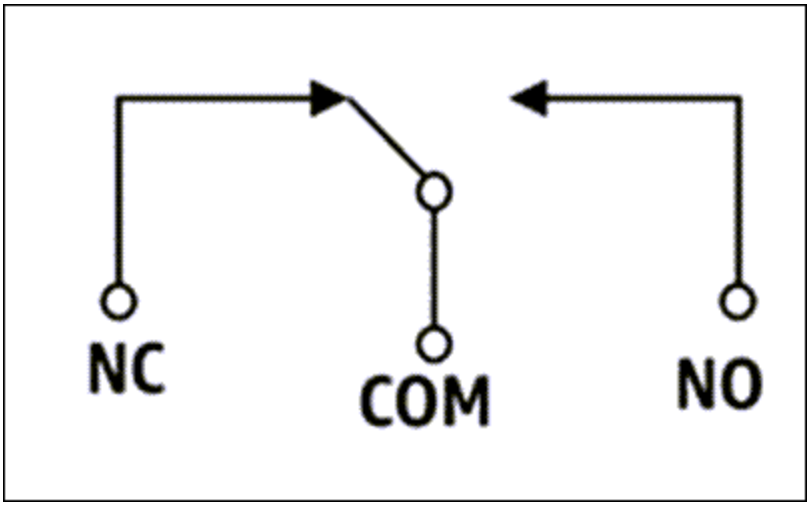


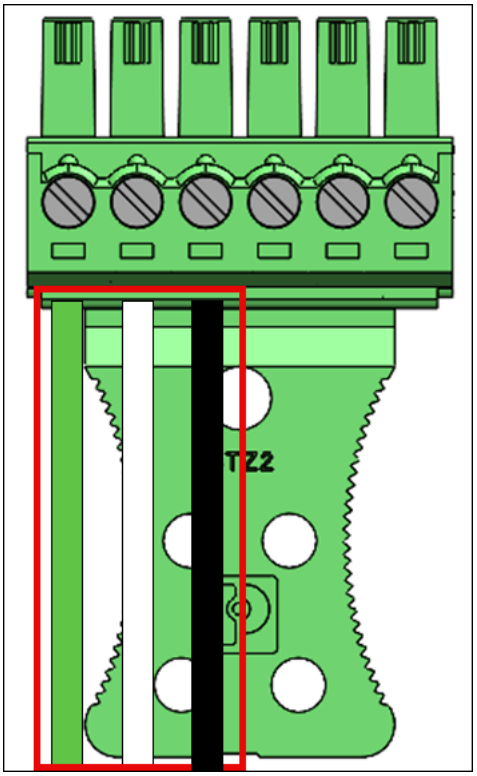
Diagramma del relè



Il relè deve funzionare secondo i valori di sicurezza specificati 30VAC/60VDC, 60W max.

RS485 connessioni

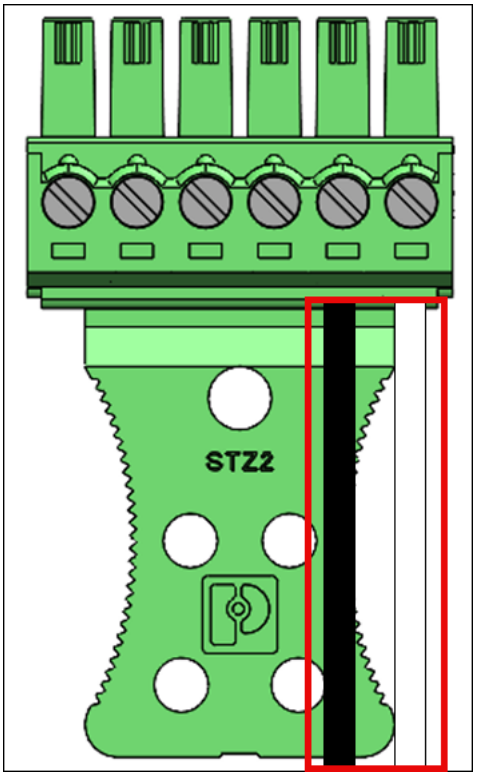
- Inserire il filo verde nel Pin 7 (B).
- Inserire il filo bianco nel Pin 8 (A).
- Inserire il filo nero nel Pin 9 (RTN).



Attivare RS485 l'interruttore di terminazione su «ON» se il dispositivo è l'ultima unità sulla linea. Questo interruttore attiva la terminazione del resistore da 120 Ohm sulla linea.

Connessioni di ingresso/uscita digitali

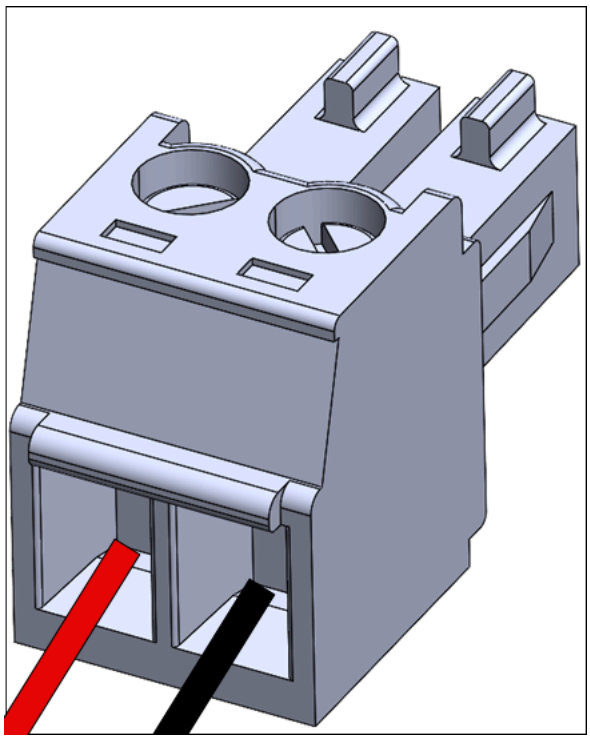
- Inserire il cavo nero nel Pin 5 (GPI).
- Inserire il filo bianco nel Pin 6 (GPO).



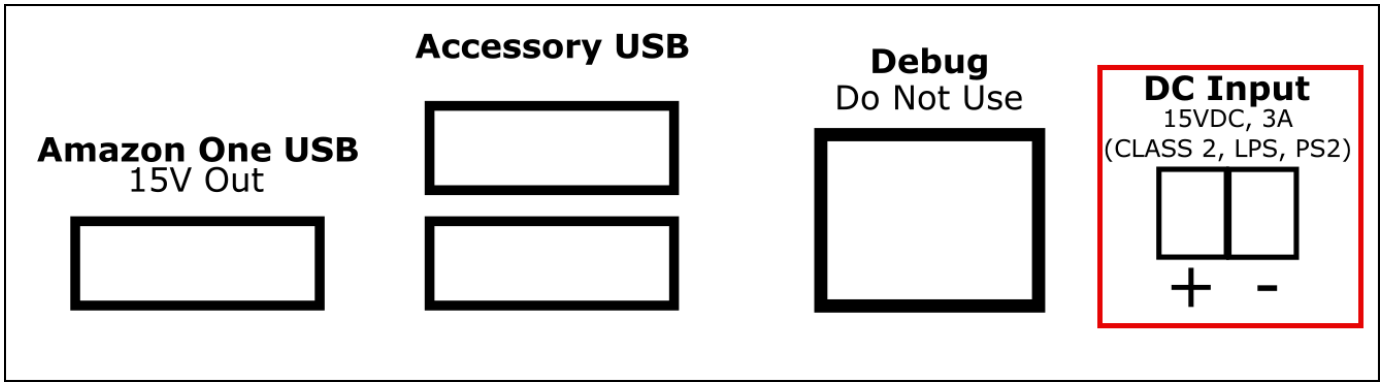
- Le connessioni di ingresso/uscita digitali devono funzionare come indicato.

Opzionale: per installare il cablaggio DC

1. Togliere 3 mm-5 mm dall'estremità di un filo rosso per il polo positivo (+) e un filo nero per il negativo (-).
2. Inserire l'estremità spellata del cavo DC nella spina DC.



3. Avvitare il cavo nella posizione desiderata.
4. Inserire la spina DC cablata nella porta di ingresso DC.



Dopo aver installato il tuo dispositivo Amazon One, sei pronto per attivarlo.

Attivazione del dispositivo Amazon One

Quando il tuo dispositivo Amazon One è installato e acceso, sei pronto per attivarlo.

Per attivare il tuo dispositivo Amazon One

1. Sul dispositivo Amazon One, tocca lo schermo per iniziare.

2. Scegli Ethernet o Wifi per connetterti a Internet.

   Non appena il dispositivo sarà connesso a Internet, inizierà a scaricare il pacchetto software più recente.
3. Quando la schermata mostra Download del software completato! , seleziona OK.
4. Seleziona il codice QR.

   La schermata del dispositivo Amazon One mostrerà il codice QR di scansione.
5. Per recuperare il codice QR di attivazione, apri la console Amazon One Enterprise all'indirizzo https://console.aws.amazon.com/one-enterprise.

   > **Note**
   >
   > Ti consigliamo vivamente di concedere autorizzazioni limitate ai tuoi installatori in modo che abbiano accesso solo ai codici QR di attivazione nella tua console Amazon One Enterprise. Per informazioni, consulta Aggiungi utenti Amazon One.
6. Nel pannello di navigazione, scegli Codici QR di attivazione.
7. Dall'elenco a discesa Seleziona un sito, seleziona il sito in cui è installato il dispositivo Amazon One.
8. In Informazioni sul sito, conferma l'indirizzo del sito.
9. In Codici QR di attivazione, cerca il nome dell'istanza del dispositivo che stai attivando e seleziona il codice Ottieni QR corrispondente per recuperare il codice QR.
10. Scansiona il codice QR con il dispositivo Amazon One. Tieni presente che il codice QR viene aggiornato periodicamente per motivi di sicurezza, puoi utilizzare un codice QR solo una volta.
11. Inserisci il codice postale del sito e seleziona Conferma impostazioni dopo aver verificato che venga visualizzato il sito corretto.
12. Quando la schermata del dispositivo Amazon One mostra Attivazione completata! , il dispositivo è pronto per l'uso.

Registrazione e inserimento di utenti

Ora che il tuo dispositivo Amazon One è attivato, i tuoi dipendenti possono iniziare a registrare i palmi delle mani e autenticarli per ottenere l'accesso.

Argomenti

Creazione di una policy sugli endpoint

Prima che gli utenti possano autenticare i palmi delle mani per l'accesso, dovranno completare la procedura di registrazione. Il personale addetto alla sicurezza deve sempre verificare l'identità dell'utente prima di consentirgli la registrazione.

Per registrare i palmi delle mani su un dispositivo Amazon One

1. Sul dispositivo di registrazione Amazon One Enterprise, premi Inizia.
2. Scansiona il badge di un dipendente con lo scanner di badge collegato al tuo dispositivo di registrazione Amazon One Enterprise.

   Quando il badge viene scansionato correttamente, la schermata del dispositivo Amazon One mostra Badge scansionato.
3. Leggi le Condizioni d'uso, quindi premi OK.
4. Leggi Consenso - Le tue informazioni biometriche su Palm e premi Accetto se acconsenti.
5. Segui le istruzioni sullo schermo per completare la procedura di registrazione.

Autenticazione per l'ingresso

Dopo aver registrato correttamente i palmi delle mani, sei pronto per l'autenticazione con il palmo della mano sul tuo dispositivo di accesso Amazon One Enterprise.

Per autenticare il palmo della mano per l'accesso su un dispositivo Amazon One

- Passa il palmo della mano sul dispositivo e segui le istruzioni sullo schermo per scansionare il palmo della mano.

Gestione degli utenti

Puoi utilizzare la pagina di gestione degli utenti registrati per tenere traccia degli utenti registrati e per eliminare i dati biometrici degli utenti. Un utente il cui codice biometrico associato viene eliminato non avrà più accesso ai dispositivi Amazon One per l'autenticazione.

Argomenti

Visualizzazione degli utenti registrati

La procedura seguente descrive in dettaglio come iscrivere gli utenti.

Per visualizzare gli utenti registrati

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Gestione utenti registrati.
3. In Utenti iscritti, troverai tutti gli utenti registrati e i seguenti dettagli:
    - Badge ID: informazioni identificative del badge acquisite da un lettore di badge RFID al momento dell'iscrizione.
    - Fonte di registrazione: dettagli del dispositivo Amazon One utilizzato per la registrazione.
    - Data di registrazione: data e ora dell'iscrizione.

Eliminazione degli utenti registrati e dei relativi dati biometrici

La procedura seguente descrive in dettaglio come eliminare gli utenti registrati e i relativi dati biometrici.

Per eliminare gli utenti registrati e i relativi dati biometrici

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Gestione utenti registrati.

3. In Utenti registrati, seleziona il badge ID dell'utente di cui desideri eliminare i dati biometrici palmari.
4. Scegli Elimina dati biometrici.
5. Scegli Elimina per confermare l'eliminazione dei dati biometrici dell'utente.

> **Important**
>
> Questa azione comporta l'eliminazione permanente dei dati biometrici palmari di un utente da Amazon One Enterprise. L'utente dovrà registrarsi nuovamente con un dispositivo di registrazione Amazon One Enterprise per poter utilizzare Amazon One Enterprise per l'autenticazione. L'eliminazione dei dati biometrici di un utente eliminerà definitivamente anche altri attributi del profilo, come il badge ID, da Amazon One Enterprise.

Gestione dei dispositivi Amazon One

Dopo l'installazione e l'attivazione, il dispositivo Amazon One inizia a segnalare lo stato del dispositivo sulla console Amazon One Enterprise. Puoi utilizzare la console Amazon One Enterprise per eseguire attività di gestione dei dispositivi come il riavvio dei dispositivi o l'aggiornamento delle configurazioni.

Argomenti

Manutenzione e pulizia dei dispositivi Amazon One

La manutenzione del dispositivo Amazon One offre l'ambiente operativo e l'esperienza ottimali del dispositivo.

Prima di pulire il dispositivo Amazon One, verifica quanto segue:

- Sebbene non sia necessario abilitare o disabilitare Amazon One, assicurati che i dispositivi siano collegati all'alimentazione, che dispongano di connettività di rete e che tutte le periferiche e i dispositivi complementari (se applicabile) siano collegati.
- Segnala i problemi all'amministratore se la connettività di rete non è disponibile (in tal caso sarà visibile una schermata di errore sul dispositivo Amazon One), una schermata di errore sarà visibile sul dispositivo Amazon One o un problema di connessione del dispositivo sarà visibile sulla console.
- Dispositivi fisicamente sicuri in modo che persone non autorizzate non possano manometterli.
- Ispeziona visivamente i dispositivi Amazon One ogni giorno, verificando eventuali connessioni non autorizzate al dispositivo Amazon One.
- Ispeziona tutti i lati del dispositivo alla ricerca di eventuali segni di manomissione, comprese le viti visibili del dispositivo e del rivestimento, per assicurarti che non vi siano spazi vuoti o aperture che espongano i componenti/circuiti interni di entrambi i dispositivi Amazon One.
- In caso di errori o guasti, segui le istruzioni sullo schermo del dispositivo Amazon One o consulta la guida alla risoluzione dei problemi per risolvere i problemi.

Per pulire il dispositivo Amazon One

La pulizia regolare del dispositivo Amazon One rimuove eventuali macchie o segni come impronte digitali e impronte delle mani.

> **Note**
>
> Non utilizzare altri prodotti per la pulizia diversi da quelli elencati in questa guida. Il programma di pulizia consigliato è una o due volte alla settimana oppure ogni volta che sporco, polvere o macchie sono visibili sul dispositivo, ma mai più di una volta al giorno.

1. Pulisci il dispositivo Amazon One con salviette con alcol isopropilico (IPA). Pulisci solo la superficie tattile del dispositivo. Non toccare la finestra ottica e non utilizzare altri prodotti per la pulizia a meno che non venga richiesto da Amazon One.
2. Elimina eventuali striature con un panno in microfibra asciutto.
3. Spolvera leggermente (non strofinare) lo sporco o i detriti visibili dalla finestra ottica. Limita la pulizia della finestra ottica a non più di una volta al giornoand/or when the window is visually dirty (e.g., finger/hand prints/smudges). Questa parte del dispositivo non è pensata per essere toccata, ma potrebbero verificarsi contatti involontari da parte di nuovi clienti.
4. Usa un detergente per smart card KIC per pulire l'interno di un lettore di schede, se applicabile.
5. Pulisci il dispositivo una o due volte alla settimana o ogni volta che sporco, polvere o macchie sono visibili sul dispositivo.

Gestione del sito

Un sito rappresenta una posizione fisica in cui sono installate e operative una raccolta di istanze di dispositivi. Puoi utilizzare i siti per organizzare i dispositivi Amazon One che condividono lo stesso indirizzo fisico.

Argomenti

Modifica del nome del sito

La procedura seguente descrive come modificare il nome del sito per il dispositivo.

Per modificare il nome del sito

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Sito.
3. In Siti, seleziona il sito di cui intendi modificare il nome.
4. Scegli Modifica.
5. In Informazioni sul sito, inserisci il nome e la descrizione del sito desiderati (opzionale).
6. Scegli Salva le modifiche da aggiornare.

Aggiornamento dell'indirizzo del sito

La procedura seguente descrive come aggiornare l'indirizzo del sito per il dispositivo.

Per aggiornare l'indirizzo del sito

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Sito.
3. In Siti, seleziona il sito di cui intendi aggiornare l'indirizzo.
4. In Istanze del dispositivo, assicurati che il numero di istanze attivate sia 0.
5. (Facoltativo) Se il numero di istanze attivate è diverso da 0, vedi
6. Scegli Modifica.
7. In Indirizzo fisico inserisci l'indirizzo fisico corretto.
8. Scegli Salva modifiche per aggiornare.

Gestione delle istanze del dispositivo

Un'istanza di dispositivo è una rappresentazione logica di un dispositivo con configurazioni. L'uso di istanze di dispositivi consente di scambiare dispositivi Amazon One ereditando automaticamente le configurazioni e i nomi precedentemente impostati. Un'istanza di dispositivo ha un nome definito dall'utente (convenzione di denominazione condivisa con il software di controllo degli accessi) e una serie di configurazioni di comunicazione.

Argomenti

Visualizzazione dello stato dell'istanza del dispositivo

La procedura seguente descrive in dettaglio come visualizzare lo stato dell'istanza del dispositivo.

Per visualizzare lo stato dell'istanza del dispositivo

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Istanza del dispositivo.
3. In Istanze attivate, vedrai un elenco di dispositivi Amazon One attivati.
4. Scegli il nome dell'istanza del dispositivo per visualizzare i dettagli dell'istanza del dispositivo.

Riavvio di un dispositivo Amazon One

La procedura seguente descrive in dettaglio come riavviare il dispositivo Amazon One.

Per riavviare un dispositivo Amazon One

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Istanza del dispositivo.
3. In Istanze attivate, scegli il nome dell'istanza del dispositivo che desideri riavviare.
4. Scegli Riavvia per riavviare il dispositivo Amazon One.

Aggiornamento delle configurazioni dei dispositivi Amazon One

La procedura seguente descrive in dettaglio come aggiornare le configurazioni dei dispositivi Amazon One.

Per aggiornare le configurazioni dei dispositivi Amazon One

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Istanza del dispositivo.
3. In Istanze attivate, scegli il nome dell'istanza del dispositivo che desideri aggiornare.
4. In Configurazioni del dispositivo, scegli Modifica.

> **Note**
>
> Per modificare la modalità del dispositivo Amazon One, devi prima disattivare l'istanza del dispositivo e quindi configurarla con la modalità dispositivo desiderata (vediConfigura un'istanza del dispositivo per l'attivazione). Quindi, puoi seguire la procedura di attivazione del dispositivo (vediAttivazione del dispositivo Amazon One).

5. Dopo aver apportato le modifiche desiderate, scegli Aggiorna le configurazioni del dispositivo per confermare l'aggiornamento.

Aggiornamento delle credenziali Wi-Fi

La procedura seguente descrive come aggiornare le credenziali Wi-Fi.

Per aggiornare le credenziali Wi-Fi

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.
2. Nel pannello di navigazione, scegli Istanza del dispositivo.
3. In Istanze attivate, scegli il nome dell'istanza del dispositivo che desideri aggiornare.
4. In Rete, scegli Modifica.
5. In Configurazioni Wi-Fi, apporta le modifiche desiderate.
6. Scegli Aggiorna rete per confermare l'aggiornamento.

Disattivazione delle istanze del dispositivo

La procedura seguente descrive in dettaglio come disattivare le istanze del dispositivo.

Per disattivare le istanze del dispositivo

1. Apri la console Amazon One Enterprise in https://console.aws.amazon.com/one-enterprise.

2. Nel pannello di navigazione, scegli Istanza del dispositivo.
3. In Istanze attivate, seleziona il nome dell'istanza del dispositivo che desideri disattivare.
4. Scegli Disattiva dispositivo.
5. Per confermare la disattivazione, digita «disattiva» nella casella del messaggio e scegli Disattiva dispositivo.

Sicurezza

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per maggiori informazioni sui programmi di conformità applicabili ad Amazon One Enterprise, consulta AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon One Enterprise. I seguenti argomenti mostrano come configurare Amazon One Enterprise per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon One Enterprise.

Argomenti

Protezione dei dati in Amazon One Enterprise

Il modello di responsabilità AWS condivisa si applica alla protezione dei dati in Amazon One Enterprise. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati

su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon One Enterprise o altro Servizi AWS utilizzando la console, l'API o AWS SDKs. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Per utilizzare la crittografia predefinita dei dati inattivi

Amazon One Enterprise fornisce la crittografia di default per proteggere i dati sensibili archiviati utilizzando le chiavi di crittografia AWS.

Chiavi di proprietà di AWS: Amazon One Enterprise utilizza queste chiavi di default per crittografare automaticamente i dati sensibili degli utenti finali. Non puoi visualizzare, gestire o utilizzare le chiavi di proprietà di AWS o verificarne l'utilizzo. Tuttavia, non è necessario effettuare alcuna operazione o modificare programmi per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta le chiavi di proprietà di AWS nella AWS Key Management Service Developer Guide.

Crittografia dei dati in transito

Amazon One Enterprise utilizza Transport Layer Security (TLS) per proteggere i dati e Signature Version 4 per autenticare tutte le richieste API in entrata verso i servizi AWS. Questa crittografia è abilitata per impostazione predefinita.

Gestione delle identità e degli accessi per Amazon One Enterprise

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon One Enterprise. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon One Enterprise.

Utente del servizio: se utilizzi il servizio Amazon One Enterprise per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon One Enterprise per svolgere il tuo lavoro, potresti aver bisogno di

autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon One Enterprise, consultaRisoluzione dei problemi relativi all'identità e all'accesso ad Amazon One.

Amministratore del servizio: se sei responsabile delle risorse Amazon One Enterprise presso la tua azienda, probabilmente hai pieno accesso ad Amazon One Enterprise. È tuo compito determinare a quali funzionalità e risorse di Amazon One Enterprise devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon One Enterprise, consultaCome funziona Amazon One Enterprise con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad Amazon One Enterprise. Per visualizzare esempi di policy basate sull'identità di Amazon One Enterprise che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon One Enterprise

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con

utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere

credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su

come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon One Enterprise con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon One Enterprise, scopri quali funzionalità IAM sono disponibili per l'uso con Amazon One Enterprise.

Funzionalità IAM che puoi utilizzare con Amazon One Enterprise

Funzionalità IAM	Supporto per Amazon One Enterprise
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come Amazon One Enterprise e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Amazon One Enterprise

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Amazon One Enterprise

Per visualizzare esempi di politiche basate sull'identità di Amazon One Enterprise, consulta. Esempi di policy basate sull'identità per Amazon One Enterprise

Politiche basate sulle risorse all'interno di Amazon One Enterprise

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per Amazon One Enterprise

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di Amazon One Enterprise, consultaOperazioni, risorse e chiavi di condizione per Amazon One Enterprise.

Le azioni politiche in Amazon One Enterprise utilizzano il seguente prefisso prima dell'azione:

```
one
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

È possibile specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

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

Per visualizzare esempi di politiche basate sull'identità di Amazon One Enterprise, consulta. Esempi di policy basate sull'identità per Amazon One Enterprise

Risorse relative alle policy per Amazon One Enterprise

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`.

Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse Amazon One Enterprise e i relativi ARNs tipi di risorse e per scoprire quali azioni è possibile utilizzare per specificare l'ARN di ciascuna risorsa, consulta. Operazioni, risorse e chiavi di condizione per Amazon One Enterprise

Per visualizzare esempi di politiche basate sull'identità di Amazon One Enterprise, consulta. Esempi di policy basate sull'identità per Amazon One Enterprise

Chiavi delle condizioni delle politiche per Amazon One Enterprise

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di condizione di Amazon One Enterprise e per scoprire con quali azioni e risorse puoi utilizzare una chiave di condizione, consultaOperazioni, risorse e chiavi di condizione per Amazon One Enterprise.

Per visualizzare esempi di politiche basate sull'identità di Amazon One Enterprise, consulta. Esempi di policy basate sull'identità per Amazon One Enterprise

ACLs in Amazon One Enterprise

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Amazon One Enterprise

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Amazon One Enterprise

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per Amazon One Enterprise

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Amazon One Enterprise

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Amazon One Enterprise. Modifica i ruoli di servizio solo quando Amazon One Enterprise fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Amazon One Enterprise

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon One Enterprise

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon One Enterprise. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon One Enterprise, incluso il formato di ARNs per ogni tipo di risorsa, consulta Operazioni, risorse e chiavi di condizione per Amazon One Enterprise il Service Authorization Reference.

Argomenti

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon One Enterprise nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio

se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Amazon One Enterprise

Per accedere alla console Amazon One Enterprise, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon One Enterprise presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la console Amazon One Enterprise, collega anche Amazon One Enterprise `ConsoleAccess` o la policy `ReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica

include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o in modo programmatico. AWS CLI 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": "*"
        }
    ]
}
```

Accesso in sola lettura ad Amazon One Enterprise

L'esempio seguente mostra una policy AWS gestita `AmazonOneEnterpriseReadOnlyAccess` che concede l'accesso in sola lettura ad Amazon One Enterprise.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "one:Get*",
        "one:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Nelle istruzioni della policy, l'elemento `Effect` specifica se le operazioni sono consentite o negate. L'elemento `Action` elenca le operazioni specifiche che l'utente è autorizzato a eseguire. L'elemento `Resource` elenca le risorse AWS su cui l'utente è autorizzato a eseguire tali operazioni. Per le policy che controllano l'accesso alle azioni di Amazon One Enterprise, l'`Resource`elemento è sempre impostato su`*`, un carattere jolly che significa «tutte le risorse».

I valori nell'`Action`elemento corrispondono a quelli APIs supportati dai servizi. Le azioni sono precedute da `config:` un'indicazione che si riferiscono alle azioni di Amazon One Enterprise. Puoi utilizzare il carattere jolly `*` nell'elemento `Action`, come negli esempi seguenti:

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

  Ciò consente tutte le azioni di Amazon One Enterprise che terminano con DeviceInstance "" (`GetDeviceInstanceConfiguration`,`CreateDeviceInstanceConfiguration`).
- `"Action": ["one:*"]`

  Ciò consente tutte le azioni di Amazon One Enterprise, ma non le azioni per altri AWS servizi.
- `"Action": ["*"]`

  Ciò consente tutte le AWS azioni. Questa autorizzazione è adatta a un utente che funge da AWS amministratore del tuo account.

La politica di sola lettura non concede l'autorizzazione dell'utente per azioni quali `CreateDeviceInstanceUpdateDeviceInstance`, e. `DeleteDeviceInstance` Agli utenti con questo criterio non è consentito creare un'istanza di dispositivo, aggiornare un'istanza del dispositivo o eliminare un'istanza del dispositivo. Per l'elenco delle azioni di Amazon One Enterprise, consultaOperazioni, risorse e chiavi di condizione per Amazon One Enterprise.

Accesso completo ad Amazon One Enterprise

L'esempio seguente mostra una politica che garantisce l'accesso completo ad Amazon One Enterprise. Concede agli utenti l'autorizzazione a eseguire tutte le azioni di Amazon One Enterprise.

> **Important**
>
> Questa policy concede autorizzazioni ampie. Prima di concedere l'accesso completo, prendi in considerazione l'idea di iniziare con un set di autorizzazioni minimo e concedere le autorizzazioni aggiuntive quando necessario. Questa è una best practice preferibile ad iniziare con autorizzazioni che siano troppo permissive e cercare di limitarle in un secondo momento.

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

Autorizzazioni supportate a livello di risorsa per le azioni dell'API Amazon One Enterprise Rule

Il concetto di autorizzazioni a livello di risorsa indica la possibilità di specificare le risorse su cui gli utenti sono autorizzati a eseguire operazioni. Amazon One Enterprise supporta le autorizzazioni a livello di risorsa per determinate azioni API delle regole di Amazon One Enterprise. Ciò significa che per determinate azioni delle regole di Amazon One Enterprise, puoi controllare le condizioni in base alle quali gli utenti sono autorizzati a utilizzare tali azioni. Queste condizioni possono essere azioni da eseguire o specifiche risorse che gli utenti sono autorizzati a utilizzare.

La tabella seguente descrive le azioni dell'API delle regole di Amazon One Enterprise che attualmente supportano le autorizzazioni a livello di risorsa. Descrive inoltre le risorse supportate e le relative risorse per ogni azione. ARNs Quando si specifica un ARN, è possibile utilizzare il carattere

jolly * nei percorsi; ad esempio, quando non è possibile o non si desidera specificare la risorsa esatta. IDs

> **Important**
>
> Se un'azione API delle regole di Amazon One Enterprise non è elencata in questa tabella, significa che non supporta le autorizzazioni a livello di risorsa. Se un'azione delle regole di Amazon One Enterprise non supporta le autorizzazioni a livello di risorsa, puoi concedere agli utenti le autorizzazioni per utilizzare l'azione, ma devi specificare un* per l'elemento risorsa della tua dichiarazione politica.

Operazione API	Risorse
CreateDeviceInstance	Istanza del dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
GetDeviceInstance	Istanza del dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
UpdateDeviceInstance	Istanza del dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteDeviceInstance	Istanza del dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceActivationQrCode	Istanza del dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteAssociatedDevice	Istanza del dispositivo

Operazione API	Risorse
	arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
RebootDevice	Istanza del dispositivo arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceInstanceConfiguration	Configurazione dell'istanza del dispositivo arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*
GetDeviceInstanceConfiguration	Configurazione dell'istanza del dispositivo arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*
CreateSite	Site arn:aws:one *region:accountID* ::site/ *siteId*
DeleteSite	Site arn:aws:one ::site/ *region:accountID siteId*
GetSiteAddress	Site arn:aws:one ::site/ *region:accountID siteId*
UpdateSite	Site arn:aws:one ::site/ *region:accountID siteId*
UpdateSiteAddress	Site arn:aws:one ::site/ *region:accountID siteId*

Operazione API	Risorse
CreateDeviceConfigurationTemplate	Modello di configurazione del dispositivo arn:aws:one::/*region:accountID* device-configuration-template*templateId*
DeleteDeviceConfigurationTemplate	Modello di configurazione del dispositivo arn:aws:one::/*region:accountID* device-configuration-template*templateId*
GetDeviceConfigurationTemplate	Modello di configurazione del dispositivo arn:aws:one::/*region:accountID* device-configuration-template*templateId*
UpdateDeviceConfigurationTemplate	Modello di configurazione del dispositivo arn:aws:one::/*region:accountID* device-configuration-template*templateId*

Se, ad esempio, si desidera consentire l'accesso in lettura e negare l'accesso in scrittura a regole specifiche a utenti specifici.

Nella prima policy, consenti alla AWS Config regola di leggere azioni come quelle relative alle regole `GetSite` specificate.

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

```
            }
        ]
    }
```

Nella seconda policy, neghi le azioni di scrittura sulla regola di Amazon One Enterprise sulla regola specifica.

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

Con le autorizzazioni a livello di risorsa, puoi consentire l'accesso in lettura e negare l'accesso in scrittura per eseguire azioni specifiche sulle azioni API delle regole di Amazon One Enterprise.

Informazioni aggiuntive

Per ulteriori informazioni sulla creazione di utenti, gruppi, policy e autorizzazioni IAM, consulta Creazione del primo utente e del primo gruppo di amministratori IAM e Gestione degli accessi nella Guida per l'utente di IAM.

AWS politiche gestite per Amazon One Enterprise

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta Policy gestite da AWSnella Guida per l'utente di IAM.

AmazonOneEnterpriseFullAccess

Questa politica concede autorizzazioni amministrative che consentono l'accesso a tutte le risorse e le operazioni di Amazon One Enterprise.

`one:*`Consente di eseguire tutte le azioni di Amazon One Enterprise.

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

AmazonOneEnterpriseReadOnlyAccess

Questa politica concede autorizzazioni di sola lettura a tutte le risorse e le operazioni di Amazon One Enterprise.

`one:Get*`Ottiene le risorse Amazon One Enterprise.

`one:List*`Elenca le risorse di Amazon One Enterprise.

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

AmazonOneEnterpriseInstallerAccess

Questa politica concede autorizzazioni di lettura e scrittura limitate che consentono di creare un codice QR di attivazione per qualsiasi istanza di dispositivo configurata per attivare il dispositivo in qualsiasi sito.

`one:CreateDeviceActivationQrCode`Ti consente di creare un codice QR per attivare il dispositivo.

`one:GetDeviceInstance`Ti consente di recuperare le informazioni su un'istanza di dispositivo Amazon One.

`one:GetSite`Ti consente di recuperare le informazioni su un sito Amazon One Enterprise.

`one:GetSiteAddress`Consenti di recuperare l'indirizzo fisico di un sito Amazon One Enterprise.

`one:ListDeviceInstances`Ti consente di elencare le istanze dei dispositivi Amazon One.

`one:ListSites`Ti consente di elencare i siti 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 si aggiorna alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per Amazon One Enterprise che sono stati apportati da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Amazon One Enterprise.

Modifica	Descrizione	Data
Aggiunto Amazon One Enterprise AmazonOne MetricPublishAccess	La politica di autorizzazione dei ruoli denominata AmazonOneMetricPublishAccess consente ad Amazon One Enterprise di eseguire CloudWatch: PutMetricData su CloudWatch Namespace AWS/. AmazonOne	6 febbraio 2025

Modifica	Descrizione	Data
Amazon One Enterprise ha iniziato a tracciare le modifiche	Amazon One Enterprise ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	1 dicembre 2023

Operazioni, risorse e chiavi di condizione per Amazon One Enterprise

Amazon One Enterprise (prefisso del servizio: `one`) fornisce le seguenti risorse, operazioni e chiavi di contesto della condizione specifiche del servizio per l'utilizzo nelle policy di autorizzazione di IAM.

Argomenti

Operazioni definite da Amazon One Enterprise

Puoi specificare le seguenti operazioni nell'elemento `Action` di un'istruzione di policy IAM. Utilizza le policy per concedere le autorizzazioni per eseguire un'operazione in AWS. Quando utilizzi un'operazione in una policy, in genere consenti o rifiuti l'accesso all'operazione API o al comando CLI con lo stesso nome. Tuttavia, in alcuni casi, una singola operazione controlla l'accesso a più di una operazione. In alternativa, alcune operazioni richiedono operazioni differenti.

La colonna Tipi di risorsa della tabella Operazioni indica se ogni operazione supporta le autorizzazioni a livello di risorsa. Se non vi è nessun valore in corrispondenza di questa colonna, è necessario specificare tutte le risorse ("*") alle quali si applica la policy nell'elemento `Resource` dell'istruzione di policy. Se la colonna include un tipo di risorsa, puoi specificare un ARN di quel tipo in una istruzione con tale operazione. Se l'operazione ha una o più risorse richieste, il chiamante deve disporre dell'autorizzazione per utilizzare l'operazione con tali risorse. Le risorse richieste sono indicate nella tabella con un asterisco (*). Se si limita l'accesso alle risorse con l'elemento `Resource` in una policy IAM, è necessario includere un ARN o un modello per ogni tipo di risorsa richiesta.

Alcune operazioni supportano più tipi di risorse. Se il tipo di risorsa è facoltativo (non indicato come obbligatorio), puoi scegliere di utilizzare uno tra i tipi di risorsa facoltativi.

La colonna Chiavi di condizione della tabella Operazioni contiene le chiavi che è possibile specificare nell'elemento `Condition` di un'istruzione di policy. Per ulteriori informazioni sulle chiavi di condizione associate alle risorse per il servizio guarda la colonna Chiavi di condizione della tabella Tipi di risorsa.

> **Note**
>
> Le chiavi relative alle condizioni delle risorse sono elencate nella tabella Tipi di risorse. Nella colonna Tipi di risorse (*obbligatorio) della tabella Operazioni è presente un collegamento al tipo di risorsa che si applica a un'operazione. Il tipo di risorsa nella tabella Tipi di risorse include la colonna Chiavi di condizione, che contiene le chiavi delle condizioni delle risorse che si applicano a un'operazione nella tabella Operazioni.

Per dettagli sulle colonne nella tabella seguente, consultare Tabella delle operazioni.

Operazioni	Descrizione	Livello di accesso	Tipi di risorsa (*obbligatorio)	Chiavi di condizione	Operazioni dipendenti
CreateDeviceInstance	Concedi l'autorizzazione per creare un'istanza del dispositivo	Scrittura		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	Concedi l'autorizzazione per ottenere informazioni sull'istanza del dispositivo	Lettura	istanza del dispositivo*		
ListDeviceInstances	Concedi l'autorizzazione a elencare le istanze del dispositivo	Lettura			

Operazioni	Descrizione	Livello di accesso	Tipi di risorsa (*obbligatorio)	Chiavi di condizione	Operazioni dipendenti
UpdateDeviceInstance	Concedi l'autorizzazione per aggiornare l'istanza del dispositivo	Scrittura	istanza del dispositivo*		
DeleteDeviceInstance	Concedi l'autorizzazione per eliminare l'istanza del dispositivo	Scrittura	istanza del dispositivo*		
CreateDeviceActivationQrCode	Concedi l'autorizzazione a creare un codice QR per attivare un dispositivo su un'istanza del dispositivo	Scrittura	istanza del dispositivo*		
DeleteAssociatedDevice	Concedi l'autorizzazione a eliminare l'associazione tra dispositivo e istanza del dispositivo	Scrittura	istanza del dispositivo*		
RebootDevice	Concedi l'autorizzazione per riavviare il dispositivo	Scrittura	istanza del dispositivo*		
CreateDeviceInstanceConfiguration	Concedi l'autorizzazione per creare la configurazione dell'istanza del dispositivo	Scrittura			

Operazioni	Descrizione	Livello di accesso	Tipi di risorsa (*obbligatorio)	Chiavi di condizione	Operazioni dipendenti
GetDeviceInstanceConfiguration	Concedi l'autorizzazione per ottenere informazioni sulla configurazione dell'istanza del dispositivo	Lettura	configurazione*		
CreateSite	Concedi l'autorizzazione a creare il sito	Scrittura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	Concedi l'autorizzazione per eliminare l'istanza del dispositivo	Scrittura	siti*		
GetSite	Concedi il permesso di ottenere informazioni sul sito	Lettura	siti*		
ListSites	Concedi l'autorizzazione a pubblicare siti	Lettura			
GetSiteAddress	Concedi l'autorizzazione a ottenere informazioni sull'indirizzo del sito	Lettura	siti*		
UpdateSite	Concedi l'autorizzazione all'aggiornamento del sito	Scrittura	siti*		
UpdateSiteAddress	Concedi l'autorizzazione ad aggiornare l'indirizzo del sito	Scrittura	siti*		

Operazioni	Descrizione	Livello di accesso	Tipi di risorsa (*obbligatorio)	Chiavi di condizione	Operazioni dipendenti
CreateDeviceConfigurationTemplate	Concedi l'autorizzazione a creare un'istanza del dispositivo	Scrittura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	Concedi l'autorizzazione per eliminare il modello di configurazione del dispositivo	Scrittura	device-configuration-template*		
GetDeviceConfigurationTemplate	Concedi l'autorizzazione a ottenere informazioni sul modello di configurazione del dispositivo	Lettura	device-configuration-template*		
ListDeviceConfigurationTemplates	Concedi l'autorizzazione a elencare i modelli di configurazione dei dispositivi	Lettura			
UpdateDeviceConfigurationTemplate	Concedi l'autorizzazione all'aggiornamento del modello di configurazione del dispositivo	Scrittura	device-configuration-template*		

Operazioni	Descrizione	Livello di accesso	Tipi di risorsa (*obbligatorio)	Chiavi di condizione	Operazioni dipendenti
TagResource	Concede l'autorizzazione per applicare un tag a una risorsa.	Assegnazione di tag	istanza del dispositivo, sito, device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede l'autorizzazione per rimuovere un tag da una risorsa.	Assegnazione di tag	istanza del dispositivo, sito, device-configuration-template	aws:TagKeys	
ListTagForResources	Concede l'autorizzazione per elencare i tag per una risorsa	Lettura			

Tipi di risorsa definiti da Amazon One Enterprise

I seguenti tipi di risorse sono definiti da questo servizio e possono essere utilizzati nell'elemento `Resource` delle istruzioni di policy delle autorizzazioni IAM. Ogni operazione nella Tabella delle operazioni identifica i tipi di risorse che possono essere specificati con tale operazione. Un tipo di risorsa può anche definire quali chiavi di condizione puoi includere in una policy. Queste chiavi vengono visualizzate nell'ultima colonna della tabella Tipi di risorsa. Per dettagli sulle colonne nella tabella seguente, consulta Tabella dei tipi di risorsa.

Tipi di risorsa	ARN	Chiavi di condizione
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}

Chiavi di condizione per Amazon One Enterprise

Amazon One Enterprise definisce le seguenti chiavi di condizione che possono essere utilizzate nell'elemento `Condition` di una policy IAM. Puoi utilizzare queste chiavi per perfezionare ulteriormente le condizioni in base alle quali si applica l'istruzione di policy. Per dettagli sulle colonne nella tabella seguente, consulta Tabella delle chiavi di condizione.

Per visualizzare le chiavi di condizione globali disponibili per tutti i servizi, consulta Chiavi di condizione globali disponibili.

Chiavi di condizione	Descrizione	Tipo
aws:RequestTag/${TagKey}	Filtra l'accesso in base ai tag dalla richiesta	Stringa
aws:ResourceTag/${TagKey}	Filtra l'accesso in base ai tag associati alla risorsa	Stringa
aws:TagKeys	Filtra l'accesso in base alle chiavi di tag dalla richiesta	ArrayOfString

Convalida della conformità per Amazon One Enterprise

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty

può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Monitoraggio di Amazon One Enterprise

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon One Enterprise e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare Amazon One Enterprise, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon EventBridge può essere utilizzato per automatizzare i AWS servizi e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Monitoraggio degli eventi di Amazon One Enterprise su Amazon EventBridge

Puoi monitorare gli eventi di Amazon One Enterprise in EventBridge, che fornisce un flusso di dati in tempo reale dalle tue applicazioni, applicazioni software-as-a-service (SaaS) e AWS servizi. EventBridgeindirizza tali dati verso obiettivi come Amazon AWS Lambda Simple Notification Service. Questi eventi forniscono un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse.

Iscriviti agli eventi di Amazon One Enterprise

Gli eventi di modifica dello stato del dispositivo e del profilo utente di Amazon One vengono pubblicati utilizzando EventBridge e possono essere abilitati nella EventBridge console creando una nuova regola. Sebbene gli eventi non siano ordinati, hanno un timestamp che consente di utilizzare i dati. Gli eventi vengono emessi secondo il principio del massimo sforzo.

Per iscriversi agli eventi Amazon One Enterprise

1. Accedi alla tua console AWS all'indirizzo https://console.aws.amazon.com/events/.
2. Apri la EventBridge console all'indirizzo https://console.aws.amazon.com/events/.
3. Nel pannello di navigazione, in Autobus, scegli Regole.
4. Scegli Crea regola.
5. Nella pagina di dettaglio della regola predefinita, assegna un nome alla regola.
6. Scegli Rule with an event pattern (Regola con un modello di eventi), quindi seleziona Next (Successivo).
7. Nella pagina Crea modello di evento, in Origine evento, verifica che siano selezionati AWS gli eventi o gli eventi dei EventBridge partner.
8. In Tipo di evento di esempio, scegli AWS Events.
9. Per Metodo di creazione, scegli Modello personalizzato.
10. Nella sezione Modello di evento, aggiungi un JSON con origine dell'evento `aws:one` e il tipo di dettaglio richiesto:

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

    Puoi scegliere il tipo di dettaglio richiesto dall'elenco precedente e rimuovere ciò che non è richiesto.
11. Scegli Next (Successivo).
12. Nella pagina Seleziona destinazioni, seleziona una destinazione a tua scelta, che include una funzione Lambda, una coda SQS o un argomento SNS. Per informazioni sulla configurazione degli obiettivi, consulta Amazon EventBridge targets.

    Ad esempio, per vedere quando qualcuno arriva, scegli «Riconoscimento riuscito». Quindi guarda i dettagli dell'evento (riportati nell'Appendice) per vedere chi ha partecipato.

Per completare il flusso di lavoro, puoi eseguire un'API esterna o un altro obiettivo.

13. Facoltativamente, puoi configurare i tag.
14. Nella pagina Esamina e crea, scegli Crea regola. Per ulteriori informazioni sulla configurazione delle regole, consulta le EventBridgeregole nella Guida per l' EventBridge utente.

Tipi di eventi di modifica dello stato del dispositivo

Gli eventi di modifica dello stato del dispositivo vengono generati in JSON. Per ogni tipo di evento, viene inviato un blob JSON alla destinazione di tua scelta, come configurato nella regola. Sono disponibili i seguenti tipi di dettagli:

Lo stato di salute del dispositivo è stato modificato in integro

Il dispositivo ha superato tutti i controlli sanitari.

Lo stato di salute del dispositivo è stato modificato in critico

Il dispositivo non ha superato uno o più controlli di integrità.

La connettività del dispositivo è stata modificata in modalità offline

Il dispositivo non è connesso a Internet.

La connettività del dispositivo è passata a online

Il dispositivo è connesso a Internet.

risorse

Contiene l'elenco degli arn DeviceInstance per i quali è stato pubblicato l'evento Device Status Change.

metadata

Nome del sito

- Nome del sito in cui è presente DeviceInstance.

SiteRan

- Arn per il sito in cui è presente DeviceInstance.

dati

Connettività attuale

- Indica se DeviceInstance è connesso o disconnesso da Internet.
- Valori possibili: CONNECTED, DISCONNECTED

CONNETTIVITÀ PRECEDENTE

- Indica se DeviceInstance era connesso o disconnesso da Internet prima dell'evento.
- Valori possibili: CONNECTED, DISCONNECTED

currentHealthStatus

- Indica se DeviceInstance ha superato tutti i controlli di integrità.
- Valori possibili: HEALTHY, CRITICAL

previousHealthStatus

- Indica se DeviceInstance ha superato tutti i controlli di integrità all'ultimo controllo.
- Valori possibili: HEALTHY, CRITICAL

assetTagId

- Il assetTagId dispositivo associato a DeviceInstance.

deviceInstanceName

- Il nome della DeviceInstance per la quale è stato pubblicato l'evento di stato del dispositivo.

Tipi di eventi del profilo utente

I tipi di dettagli degli eventi relativi al profilo utente sono:

Nuova iscrizione avvenuta con successo

Quando un utente si è registrato con successo.

Nuova annullamento dell'iscrizione avvenuto con successo

Quando un utente ha annullato la registrazione con successo.

Iscrizione non riuscita

Quando un utente non è riuscito a registrarsi.

Annullamento della registrazione non riuscito

Quando un utente non è riuscito ad annullare la registrazione.

Riconoscimento riuscito

Quando un utente esegue correttamente la scansione del palmo per l'autenticazione.

Riconoscimento non riuscito

Quando il riconoscimento di una scansione del palmo non è riuscito.

risorse

Contiene l'elenco degli arn del profilo utente per i quali è stato pubblicato l'evento del profilo utente.

dati

accountId

- L' AWS account pertinente per il dispositivo che ha avviato la richiesta.

Fonte della richiesta

- Questo è il deviceInstanceId dispositivo che ha avviato la richiesta.

Timestamp creato

- L'ora della creazione dell'evento.

Status dell'utente

- Lo stato attuale dell'utente.
- Valori possibili: ACTIVE, DELETED

ID associato

- L'id associato dell'utente, ad esempio l'id del badge.

motivo

- Questo valore verrà visualizzato in caso di eventi non riusciti. Contiene il motivo per cui l'evento non ha avuto successo.

Eventi di esempio

Gli esempi seguenti mostrano gli eventi per Amazon One Enterprise.

Argomenti

Lo stato di salute del dispositivo è stato modificato in integro

Il dispositivo ha superato tutte le condizioni e lo stato di salute dell'istanza del dispositivo è passato da STATO CRITICO a SANO.


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


Lo stato di salute del dispositivo è passato a critico

Il dispositivo non ha superato uno o più controlli di integrità e lo stato di integrità dell'istanza del dispositivo è passato a CRITICO da HEALTHY.

```
{
  "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 connettività del dispositivo è passata a online

Il dispositivo è connesso a Internet e lo stato di connettività dell'istanza del dispositivo è cambiato in CONNESSO da DISCONNESSO.

```
{
  "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 connettività del dispositivo è passata a offline

Il dispositivo non è connesso a Internet e lo stato di connettività dell'istanza del dispositivo è cambiato in DISCONNESSO da CONNESSO.

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

Registrazione delle chiamate API Amazon One Enterprise tramite AWS CloudTrail

Amazon One Enterprise è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon One Enterprise. CloudTrail acquisisce tutte le chiamate API per Amazon One Enterprise come eventi. Le chiamate acquisite includono chiamate dalla console Amazon One Enterprise e chiamate in codice alle operazioni dell'API Amazon One Enterprise. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon One Enterprise. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata fatta ad Amazon One Enterprise, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni su Amazon One Enterprise in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Amazon One Enterprise, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi della tua azienda Account AWS, compresi gli eventi per Amazon One Enterprise, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni di Amazon One Enterprise vengono registrate CloudTrail e documentate in. Operazioni, risorse e chiavi di condizione per Amazon One Enterprise Ad esempio, le chiamate a `RebootDevice` e `ListSites` le `DeleteDeviceInstance` azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di registro di Amazon One Enterprise

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateSite`azione.


```
{
    "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"
}
```

Risoluzione dei problemi con Amazon One

Se hai problemi con l'applicazione Amazon One o uno dei tuoi dispositivi Amazon One, utilizza questi suggerimenti per risolvere il problema. Quindi, se il problema persiste, contatta AWS Support.

Argomenti

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon One

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon One Enterprise e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in Amazon One

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `one:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `one:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon One

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon One Enterprise supporta queste funzionalità, consultaCome funziona Amazon One Enterprise con IAM.
- Per sapere come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Risoluzione dei problemi relativi alla console Amazon One

Se hai problemi con l'applicazione Amazon One o uno dei tuoi dispositivi Amazon One, utilizza questi suggerimenti per risolvere il problema. Quindi, se il problema persiste, contatta AWS Support.

Argomenti

- Non riesco a creare un sito
- Non riesco a creare un'istanza del dispositivo
- Non riesco a creare un modello di configurazione
- Non riesco a creare un codice QR di attivazione

Non riesco a creare un sito

- Contatta l'amministratore della console Amazon One per fornirti l'accesso.
- Se il problema persiste, contatta AWS Support.

Non riesco a creare un'istanza del dispositivo

- Contatta l'amministratore della console Amazon One per fornirti l'accesso.
- Se il problema persiste, contatta AWS Support.

Non riesco a creare un modello di configurazione

- Contatta l'amministratore della console Amazon One per fornirti l'accesso.
- Se il problema persiste, contatta AWS Support.

Non riesco a creare un codice QR di attivazione

- Contatta l'amministratore della console Amazon One per fornirti l'accesso.
- Se il problema persiste, contatta AWS Support.

Risoluzione dei problemi relativi al dispositivo Amazon One

Se hai problemi con la console Amazon One o uno dei tuoi dispositivi Amazon One, utilizza questi suggerimenti per risolvere il problema. Quindi, se il problema persiste, contatta AWS Support.

Argomenti

- L'istanza del dispositivo non esiste
- Sito non trovato
- Il codice postale non corrisponde
- Il timeout del gateway è scaduto
- Non riesco a configurare il dispositivo
- Il dispositivo è stato riavviato con messaggio di errore e codice di errore
- Logo Amazon sullo schermo del dispositivo senza ulteriori attività
- Temporaneamente non disponibile
- Qualcosa è andato storto da parte nostra
- Temporaneamente fuori servizio
- Il dispositivo Amazon One presenta danni fisici
- Impossibile leggere Palm
- Palm non riconosciuto
- Dispositivo bloccato a causa di una prolungata inattività
- Dispositivo bloccato a causa di un evento di manomissione

Schermo vuoto

Ciò si verifica quando il dispositivo non è alimentato o si blocca durante il riavvio.

Esegui le seguenti operazioni per risolvere questo problema:

- Attendi qualche istante (meno di 30 secondi) nel caso in cui il dispositivo si stia riavviando.
- Se l'anello luminoso lampeggia mentre il dispositivo è spento, attendi fino a 30 secondi.
- Controlla se il cavo di alimentazione è collegato sia alla presa di corrente che alla parte posteriore del dispositivo Amazon One. Inoltre, verifica che il cavo non sia danneggiato.
- Controlla la fonte di alimentazione.
- Verifica che tutti i cavi siano collegati correttamente ad Amazon One e all'hub USB.
- Riavvia il dispositivo dalla console.
- Se il riavvio del dispositivo non risolve il problema, scollega l'hub USB Amazon One dall'alimentazione e ricollegalo.
- Se il problema persiste, contatta AWS Support.

Non riesco a connettermi al Wi-Fi o alla rete

Ciò si verifica quando il dispositivo perde la connettività.

Esegui le seguenti operazioni per risolvere questo problema:

- Se sei connesso al Wi-Fi, usa un altro dispositivo per verificare se il Wi-Fi è presente nelle reti disponibili.
- Controlla se il router Wi-Fi è acceso e si trova nel raggio d'azione.
- Il dispositivo si riconnetterà una volta ripristinata la rete.
- Se il problema persiste, contatta il supporto AWS.

Riavvio di un dispositivo con avvisi attivi

Quando viene richiesto un riavvio dalla console, l'operazione attende fino a 15 minuti prima che il dispositivo riceva il comando e tenti il riavvio, anche se è offline o presenta problemi di rete.

Esegui le seguenti operazioni per risolvere questo problema:

- Attendi il completamento del riavvio.
- Se il problema persiste, contatta il supporto AWS.

Errore di sistema

Ciò si verifica a causa di un errore interno.

Esegui le seguenti operazioni per risolvere questo problema:

- Scegli Riavvia sullo schermo per riavviare l'applicazione.
- Dopo 2 tentativi, se il problema non viene risolto, contatta AWS Support.

Il codice QR non è riconosciuto

Ciò si verifica a causa di un codice QR non autorizzato o di un codice QR scaduto.

Esegui le seguenti operazioni per risolvere questo problema:

- Scegli Riprova per tornare alla schermata del codice QR.

- Crea un nuovo codice QR sulla console AWS, quindi scansiona il codice QR valido.

Impossibile leggere il codice QR

Ciò si verifica quando l'applicazione non è in grado di leggere il codice QR.

Effettuate le seguenti operazioni per risolvere questo problema:

- Scegli Riprova per tornare alla schermata del codice QR.
- Se il problema persiste, annulla il flusso di lavoro di attivazione e riavvia.

Sono stati rilevati più codici QR

Ciò si verifica quando vengono scansionati più codici QR.

Effettua le seguenti operazioni per risolvere questo problema:

- Scegli Riprova per tornare alla schermata del codice QR.
- Scansiona solo un codice QR valido alla volta.

L'istanza del dispositivo non esiste

Ciò si verifica quando l'istanza del dispositivo viene eliminata o non esiste nella console AWS.

Esegui quanto segue per risolvere questo problema:

- Scegli Riprova per tornare alla schermata del codice QR.
- Controlla la console AWS per l'istanza corretta del dispositivo. Se l'istanza del dispositivo è mancante, contatta il tuo amministratore.
- Crea un nuovo codice QR per l'istanza del dispositivo, quindi scansiona il nuovo codice QR.

Sito non trovato

Ciò si verifica quando il sito viene eliminato o non esiste nella console AWS.

Esegui quanto segue per risolvere questo problema:

- Controlla la console AWS per le informazioni sul sito. Se il sito non esiste, contatta il tuo amministratore.

Il codice postale non corrisponde

Ciò si verifica quando si immette un codice postale diverso da quello configurato per il dispositivo.

Esegui le seguenti operazioni per risolvere questo problema:

- Scegli Riprova per tornare alla schermata del codice postale.
- Verifica di avere il codice postale corretto del sito.
- Se il problema persiste, contatta l'amministratore per controllare il codice postale del sito sulla console AWS.

Il timeout del gateway è scaduto

Ciò si verifica quando non viene ricevuta alcuna risposta dal gateway entro un periodo di tempo specificato.

Effettuate le seguenti operazioni per risolvere questo problema:

- Scegli Riavvia per riavviare l'applicazione.
- Dopo due tentativi, se il problema non viene risolto, contatta AWS Support.

Non riesco a configurare il dispositivo

Ciò si verifica quando l'operazione non è riuscita a salvare la configurazione sul disco del dispositivo.

Effettuate le seguenti operazioni per risolvere questo problema:

- Scegli Riavvia per riavviare l'applicazione.
- Dopo due tentativi, se il problema non viene risolto, contatta AWS Support.

Il dispositivo è stato riavviato con messaggio di errore e codice di errore

Esegui quanto segue per risolvere questo problema:

- Scegli Riavvia e lascia che il dispositivo si ripristini.

- Se il dispositivo non si ripristina, scollega l'hub USB dall'alimentazione e ricollegalo.
- Se il problema persiste, contatta AWS Support.

Logo Amazon sullo schermo del dispositivo senza ulteriori attività

Esegui quanto segue per risolvere questo problema:

- Attendi qualche istante (meno di 30 secondi) nel caso in cui il dispositivo si stia riavviando.
- Scollegare l'hub USB dall'alimentazione e ricollegarlo.
- Se il problema persiste, contatta AWS Support.

Temporaneamente non disponibile

Esegui quanto segue per risolvere questo problema:

- Assicurati che le connessioni USB con il dispositivo/sistema host siano sicure.
- Scollegare e ricollegare tutti i cavi che entrano nell'hub USB.
- Se il problema persiste, contatta AWS Support.

Qualcosa è andato storto da parte nostra

Ciò si verifica quando si verifica un errore interno.

Esegui le seguenti operazioni per risolvere questo problema:

1. Spegnere il dispositivo.
2. Scollegalo dalla sua rete di alimentazione.
3. Attendere 30 secondi.
4. Ricollega il dispositivo alla fonte di alimentazione.
5. Accendere il dispositivo.
6. Se il problema persiste, contatta AWS Support.

Temporaneamente fuori servizio

Ciò si verifica quando il dispositivo è stato messo fuori servizio da Amazon One.

Esegui quanto segue per risolvere questo problema:

- Contatta AWS Support.

Il dispositivo Amazon One presenta danni fisici

Esegui quanto segue per risolvere questo problema:

- Contatta AWS Support per i passaggi successivi e fornisci quanti più dettagli possibili, ad esempio cosa è successo, quando è successo e perché è successo.

Impossibile leggere Palm

Esegui quanto segue per risolvere questo problema:

- Verifica che il dispositivo Amazon One sia privo di striature e sbavature.
- Assicurati che il palmo del cliente sia privo di occlusioni come bende, maniche e sporcizio/olio in quantità significativa.
- Se il problema persiste e il dispositivo non legge alcun palmo, contatta AWS Support.

Palm non riconosciuto

Esegui quanto segue per risolvere questo problema:

- Chiedi al cliente di provare a usare l'altro palmo della mano.
- Assicurati che il cliente sia già registrato. In caso contrario, chiedi loro di registrarsi online o sul dispositivo.
- Se il problema persiste e il dispositivo non legge alcun contatto palmare, contatta AWS Support.

Dispositivo bloccato a causa di una prolungata inattività

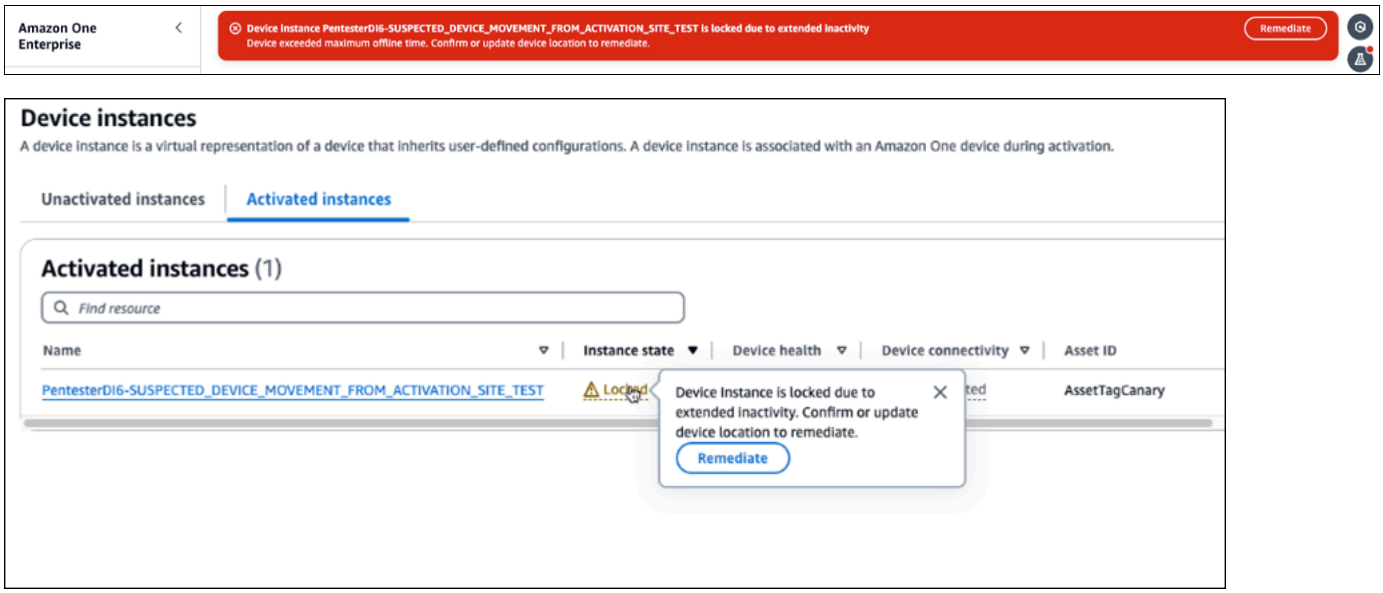
Quando il dispositivo sospetta di essere stato spostato dal sito di attivazione, blocca gli utenti. Ciò si verifica quando il dispositivo supera il limite massimo di 120 ore di utilizzo offline.

Esegui le seguenti operazioni per sbloccare il dispositivo:

1. Accedi alla tua console AWS e scegli l'istanza del dispositivo.

2. Dal banner di errore nella parte superiore della pagina, seleziona Remediate.

   Facoltativamente: da Istanze attivate, seleziona Bloccato e scegli Ripara.



3. Se il dispositivo si trova ancora nel sito di attivazione originale, scegli Sì, il dispositivo si trova in questo sito.
4. Se il dispositivo si trova in un sito diverso, scegli No, il dispositivo si trova in un sito diverso. Scegliendo No si disattiva il dispositivo. Attiva il dispositivo nel nuovo sito.

Dispositivo bloccato a causa di un evento di manomissione

Per motivi di sicurezza, il dispositivo Amazon One verrà bloccato in caso di manomissione.

Esegui quanto segue per risolvere questo problema:

- Contatta AWS Support.

Cronologia dei documenti per la Amazon One Enterprise User Guide

La tabella seguente descrive le versioni della documentazione per Amazon One Enterprise.

Modifica	Descrizione	Data
Aggiorna	È stata aggiunta la sezione Service-Linked Roles	4 febbraio 2025
Aggiorna	Aggiunto: contenuti basati su scenari	10 ottobre 2024
Aggiorna	Argomento aggiunto: Risoluzione dei problemi della console Amazon One Enterprise	10 ottobre 2024
Aggiorna	Argomento aggiunto: Risoluzione dei problemi del dispositivo Amazon One Enterprise	10 ottobre 2024
Aggiorna	Capitolo aggiunto: Configurazione di Amazon One Enterprise	10 ottobre 2024
Aggiorna	Argomento aggiunto: Manutenzione e pulizia dei dispositivi Amazon One Enterprise	10 ottobre 2024
Aggiorna	Contenuti riorganizzati	10 ottobre 2024
Aggiorna	Argomento aggiunto: Installazione dell'hub I/O del dispositivo Amazon One Enterprise per un accesso sicuro	14 agosto 2024

Aggiorna	Argomento aggiunto: Installazione di un dispositivo Amazon One Enterprise montabile a parete	5 giugno 2024
Versione iniziale	Versione iniziale della Amazon One Enterprise User Guide	27 novembre 2023

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.