Guida di amministrazione

AWS Wickr

AWS Wickr: Guida di amministrazione

Table of Contents

Che cos'è AWS Wickr?

AWSWickr è un servizio end-to-end crittografato che aiuta le organizzazioni e le agenzie governative a comunicare in modo sicuro tramite one-to-one messaggistica di gruppo, chiamate vocali e video, condivisione di file, condivisione dello schermo e altro ancora. Wickr può aiutare i clienti a superare gli obblighi di conservazione dei dati associati alle app di messaggistica di livello consumer e facilitare la collaborazione in modo sicuro. I controlli amministrativi e di sicurezza avanzati aiutano le organizzazioni a soddisfare i requisiti legali e normativi e a creare soluzioni personalizzate per le sfide legate alla sicurezza dei dati.

Le informazioni possono essere registrate in un archivio dati privato e controllato dal cliente per scopi di conservazione e controllo. Gli utenti dispongono di un controllo amministrativo completo sui dati, che include l'impostazione delle autorizzazioni, la configurazione di opzioni di messaggistica effimere e la definizione di gruppi di sicurezza. Wickr si integra con servizi aggiuntivi come Active Directory (AD), single sign-on () con SSO OpenID Connect () e altro ancora. OIDC Puoi creare e gestire rapidamente una rete Wickr tramite e automatizzare in modo sicuro i flussi di lavoro utilizzando i AWS Management Console bot di Wickr. Per iniziare, consulta Configurazione per AWS Wickr.

Argomenti

Caratteristiche di Wickr

Sicurezza e privacy migliorate

Wickr utilizza la crittografia Advanced Encryption Standard (AES) a 256 bit per ogni end-to-end funzionalità. Le comunicazioni sono crittografate localmente sui dispositivi degli utenti e rimangono indecifrabili durante il transito verso chiunque non sia il mittente e il destinatario. Ogni messaggio, chiamata e file viene crittografato con una nuova chiave casuale e solo i destinatari previsti (nemmeno AWS) può decrittografarli. Che si tratti di condividere dati sensibili e regolamentati, discutere di questioni legali o relative alle risorse umane o persino condurre operazioni militari tattiche, i clienti utilizzano Wickr per comunicare quando la sicurezza e la privacy sono fondamentali.

Conservazione dei dati

Le funzionalità amministrative flessibili sono progettate non solo per salvaguardare le informazioni sensibili, ma anche per conservare i dati secondo quanto richiesto dagli obblighi di conformità, dalla conservazione legale e per scopi di controllo. I messaggi e i file possono essere archiviati in un archivio dati sicuro e controllato dal cliente.

Accesso flessibile

Gli utenti hanno accesso a più dispositivi (dispositivi mobili, desktop) e la capacità di funzionare in ambienti con larghezza di banda ridotta, compresi quelli disconnessi e in comunicazione. out-of-band

Controlli amministrativi

Gli utenti dispongono di un controllo amministrativo completo sui dati, che include l'impostazione delle autorizzazioni, la configurazione di opzioni di messaggistica temporanea responsabili e la definizione di gruppi di sicurezza.

Integrazioni e bot potenti

Wickr si integra con servizi aggiuntivi come Active Directory, single sign-on () con SSO OpenID Connect () e altro ancora. OIDC I clienti possono creare e gestire rapidamente una rete Wickr tramite Wickr e automatizzare in modo sicuro i flussi di lavoro con Wickr AWS Management Console Bots.

Di seguito è riportato un elenco delle offerte di collaborazione di Wickr:

- Messaggi individuali e di gruppo: chatta in modo sicuro con il tuo team in stanze con un massimo di 500 membri
- Chiamate audio e video: organizza chiamate in conferenza con un massimo di 70 persone
- Condivisione dello schermo e trasmissione: presente con un massimo di 500 partecipanti
- Condivisione e salvataggio di file: trasferisci fino a 5 file GBs con spazio di archiviazione illimitato
- Effimero: controlla la scadenza e i timer burn-on-read
- Federazione globale: Connect con utenti Wickr al di fuori della rete

> **Note**
>
> Le reti Wickr negli AWS GovCloud Stati Uniti occidentali possono essere federate solo con altre reti Wickr negli Stati Uniti occidentali. AWS GovCloud

Accedere a Wickr

Wickr è disponibile negli Stati Uniti orientali (Virginia settentrionale), Canada (Centrale), Europa (Londra), Asia Pacifico (Sydney), Europa (Francoforte), Europa (Stoccolma), Europa (Zurigo), Asia Pacifico (Singapore) e Asia Pacifico (Tokyo). Regioni AWS Wickr è disponibile anche nella versione (Stati Uniti occidentali). WickrGov AWS GovCloud Regione AWS

Gli amministratori accedono a Wickr all'indirizzo AWS Management Console . https://console.aws.amazon.com/wickr/ Prima di iniziare a utilizzare Wickr, è necessario completare le guide e. Configurazione per AWS Wickr Guida introduttiva a AWS Wickr

> **Note**
>
> Il servizio Wickr non dispone di un'interfaccia di programmazione delle applicazioni (). API

Gli utenti finali accedono a Wickr tramite il client Wickr. Per ulteriori informazioni, consulta la Guida per l'utente di WickrAWS.

Prezzi

Wickr è disponibile in diversi piani per singoli utenti, piccoli team e grandi aziende. Per ulteriori informazioni, consulta la pagina dei prezzi di AWSWickr.

Documentazione per l'utente finale di Wickr

Se sei un utente finale del client Wickr e hai bisogno di accedere alla relativa documentazione, consulta la Guida per l'utente di Wickr. AWS

Configurazione per AWS Wickr

Se sei un nuovo AWS cliente, completa i prerequisiti di configurazione elencati in questa pagina prima di iniziare a utilizzare AWS Wickr. Per queste procedure di configurazione, si utilizza il AWS Identity and Access Management (IAM) servizio. Per informazioni complete suIAM, consulta la Guida IAM per l'utente.

Argomenti

Registrati per AWS

Se non hai un Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
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.

   Quando ti iscrivi a un Account AWS, un Utente root dell'account AWSviene creato. L'utente root ha accesso a tutti Servizi AWS e le risorse presenti nell'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 di un utente root.

Creazione di un utente IAM

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center (Consigliato)	Utilizza credenziali a breve termine per accedere AWS. Ciò è in linea con le best practice per la sicurezza. Per informazioni sulle migliori pratiche, consulta le migliori pratiche di sicurezza IAM nella Guida per l'IAMutente.	Seguendo le istruzioni riportate in Guida introduttiva in AWS IAM Identity Center Guida per l'utente.	Configurare l'accesso programmatico configurando il AWS CLI da usare AWS IAM Identity Center nella AWS Command Line Interface Guida per l'utente.
In IAM (Non consigliato)	Usa credenziali a lungo termine per accedere AWS.	Segui le istruzioni riportate nella sezione Creazione del primo utente e gruppo di utenti IAM amministratore nella Guida per l'IAMutente.	Configura l'accesso programmatico gestendo le chiavi di accesso per IAM gli utenti nella Guida per l'IAMutente.

> **Note**
>
> Puoi anche assegnare la politica `AWSWickrFullAccess` gestita per concedere l'autorizzazione amministrativa completa al servizio Wickr. Per ulteriori informazioni, consulta AWS politica gestita: AWSWickrFullAccess.

Cosa c'è dopo

Hai completato i passaggi di configurazione dei prerequisiti. Per iniziare a configurare Wickr, consulta. Nozioni di base

Guida introduttiva a AWS Wickr

In questa guida, ti mostriamo come iniziare a usare Wickr creando una rete, configurando la tua rete e creando utenti.

Argomenti

Prerequisiti

Prima di iniziare, assicurati di completare i seguenti prerequisiti, se non l'hai già fatto:

- Iscriviti ad Amazon Web Services (AWS). Per ulteriori informazioni, consulta Configurazione per AWS Wickr.
- Assicurati di disporre delle autorizzazioni necessarie per amministrare Wickr. Per ulteriori informazioni, consulta AWS politica gestita: AWSWickrFullAccess.
- Assicurati di consentire l'elenco delle porte e dei domini appropriati per Wickr. Per ulteriori informazioni, consulta Elenco delle porte e dei domini consentiti.

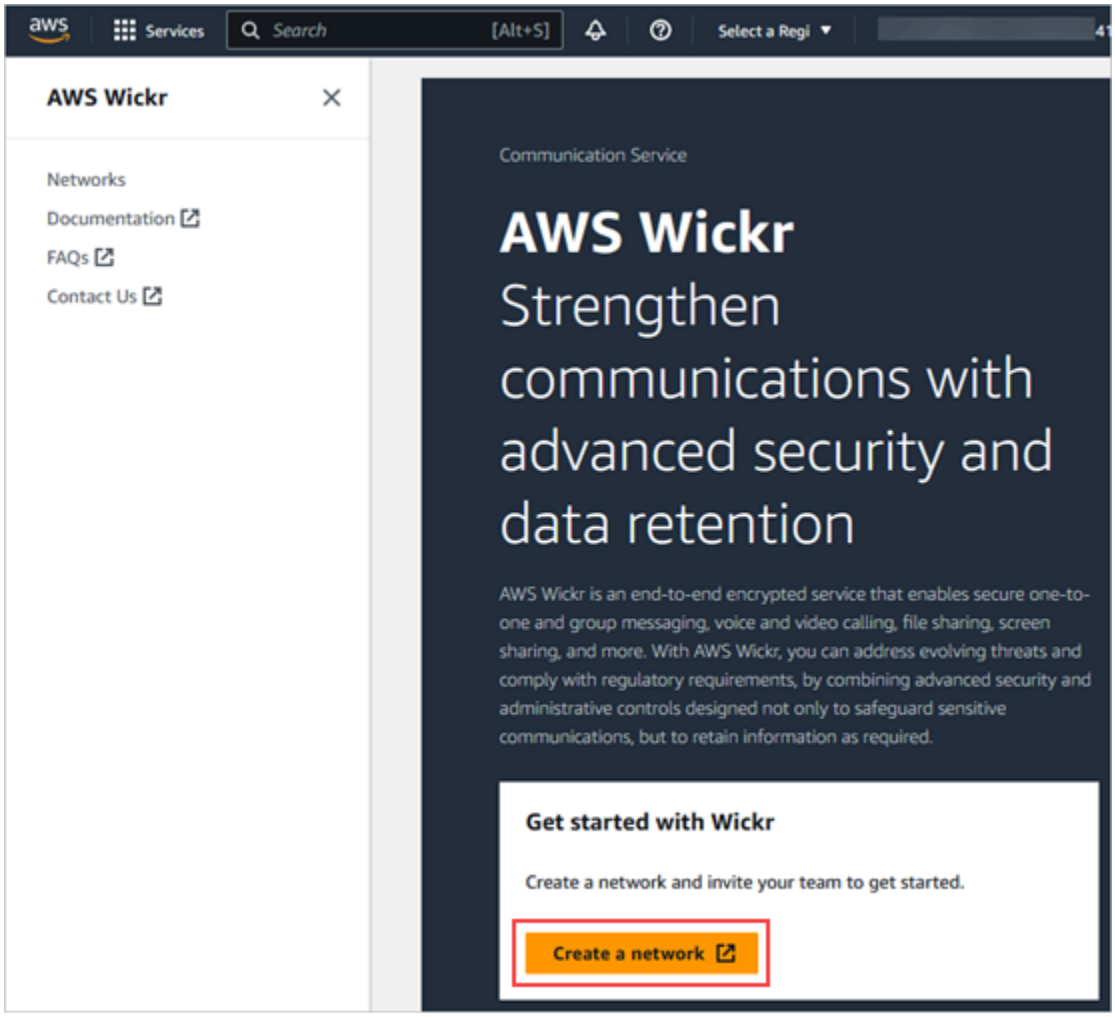
Fase 1: Creare una rete

Completa la seguente procedura per creare una rete Wickr per il tuo account.

1. Apri il file AWS Management Console per Wickr su. https://console.aws.amazon.com/wickr/

> **Note**
>
> Se non hai mai creato una rete Wickr prima, vedrai la pagina informativa del servizio Wickr. Dopo aver creato una o più reti Wickr, vedrai la pagina Reti, che contiene un elenco di tutte le reti Wickr che hai creato.

2. Scegli Crea una rete.



3. Inserisci un nome per la tua rete nella casella di testo Nome rete. Scegli un nome che i membri della tua organizzazione riconosceranno, ad esempio il nome della tua azienda o il nome del tuo team.
4. Scegli un piano. Puoi scegliere uno dei seguenti piani di rete Wickr:

   - Standard: per team di piccole e grandi aziende che necessitano di controlli amministrativi e flessibilità.

- Versione di prova gratuita Premium o Premium: per le aziende che richiedono i massimi limiti di funzionalità, controlli amministrativi granulari e conservazione dei dati.

Gli amministratori possono scegliere l'opzione di prova gratuita premium, disponibile per un massimo di 30 utenti e della durata di tre mesi. Questa offerta è aperta a nuovi piani di prova gratuiti e standard. Gli amministratori possono effettuare l'upgrade o il downgrade ai piani Premium o Standard durante il periodo di prova gratuito premium.

Per ulteriori informazioni sui piani e sui prezzi di Wickr disponibili, consulta la pagina dei prezzi di Wickr.

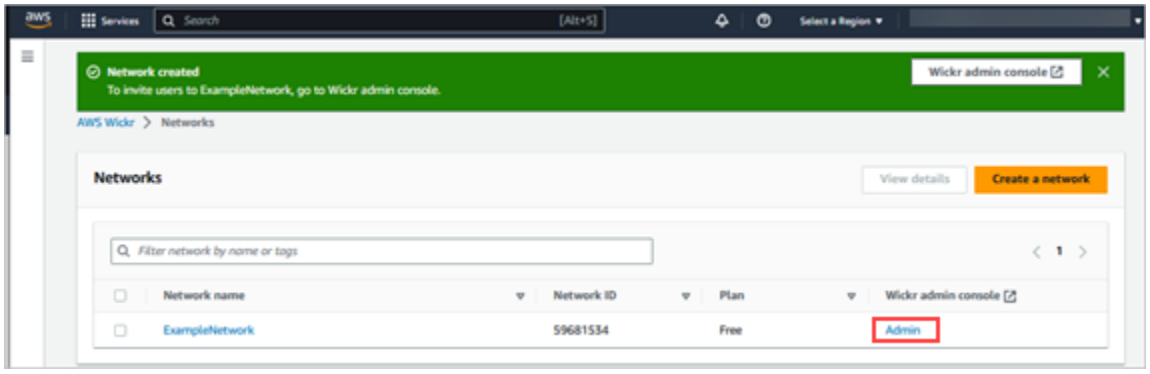
5. (Facoltativo) Scegli Aggiungi nuovo tag per aggiungere un tag alla tua rete. I tag sono costituiti da una coppia di valori chiave. I tag possono essere utilizzati per cercare e filtrare le risorse o tenere traccia AWS dei costi. Per ulteriori informazioni, consulta Tag di rete.
6. Scegli Crea rete.

   Verrai reindirizzato alla pagina Reti di AWS Management Console for Wickr e la nuova rete verrà elencata nella pagina.

Passaggio 2: configura la tua rete

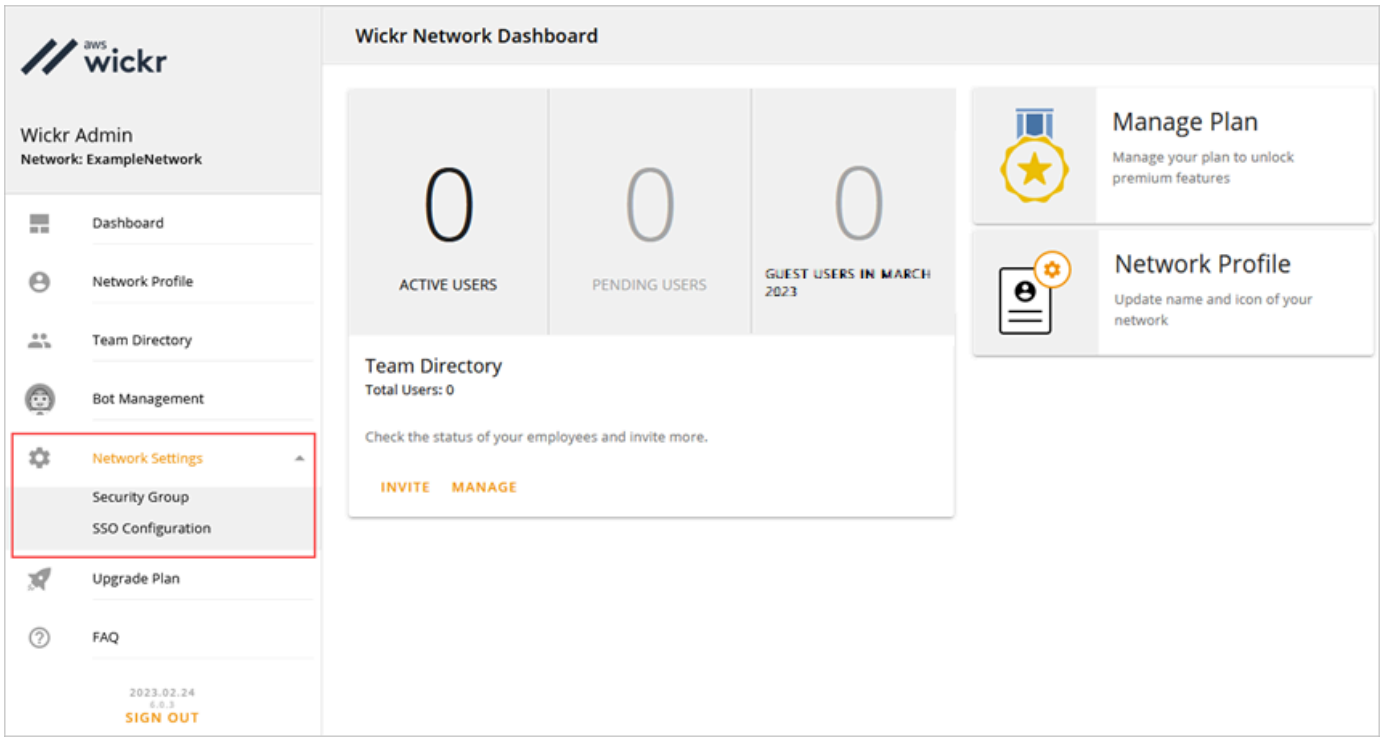
Completa la seguente procedura per accedere alla console di amministrazione di Wickr, dove puoi aggiungere utenti, aggiungere gruppi di sicurezzaSSO, configurare e configurare la conservazione dei dati e altre impostazioni di rete.

1. Nella pagina Reti, scegli il link Amministratore per accedere alla Wickr Admin Console per quella rete.



   Verrai reindirizzato alla console di amministrazione di Wickr per la rete selezionata.

2. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete.



Sono disponibili le seguenti opzioni di impostazione della rete. Per ulteriori informazioni sulla configurazione di queste impostazioni, vedereGestisci la tua rete AWS Wickr.

- Gruppo di sicurezza: gestisci i gruppi di sicurezza e le relative impostazioni, come i criteri di complessità delle password, le preferenze di messaggistica, le funzioni di chiamata, le funzioni di sicurezza e la federazione esterna. Per ulteriori informazioni, consulta Gruppi di sicurezza.
- SSOConfigurazione: configura SSO e visualizza l'indirizzo dell'endpoint per la tua rete Wickr. Wickr supporta i SSO provider che utilizzano solo OpenID Connect (). OIDC I provider che utilizzano Security Assertion Markup Language () SAML non sono supportati. Per ulteriori informazioni, consulta Configurazione Single Sign-On.

Fase 3: Creare e invitare utenti

Puoi creare utenti nella tua rete Wickr usando i seguenti metodi:

- Single Sign-on: se configuriSSO, puoi invitare utenti condividendo il tuo ID aziendale di Wickr. Gli utenti finali si registrano a Wickr utilizzando l'ID aziendale fornito e il proprio indirizzo e-mail di lavoro. Per ulteriori informazioni, consulta Configurazione Single Sign-On.

- Invito: puoi creare manualmente utenti in AWS Management Console for Wickr e ricevere loro un invito via e-mail. Gli utenti finali possono registrarsi a Wickr scegliendo il link nell'e-mail.

> **Note**
>
> Puoi anche abilitare gli utenti ospiti per la tua rete Wickr. La funzione utente ospite è attualmente in anteprima. Per ulteriori informazioni, consulta Utenti ospiti

Completa le seguenti procedure per creare o invitare utenti.

> **Note**
>
> Anche gli amministratori sono considerati utenti e devono invitare se stessi a SSO o a reti esterne a SSO Wickr.

SSO

Scrivi e invia un'email agli SSO utenti che devono iscriversi a Wickr. Includi le seguenti informazioni nella tua email:

- Il tuo codice identificativo aziendale su Wickr. Specifichi un ID aziendale per la tua rete Wickr durante la configurazione. SSO Per ulteriori informazioni, consulta Configura SSO.
- L'indirizzo email che devono usare per registrarsi.
- Quindi URL per scaricare il client Wickr. Gli utenti possono scaricare i client Wickr dalla pagina dei download di Wickr all'indirizzo AWS download/. https://aws.amazon.com/wickr/

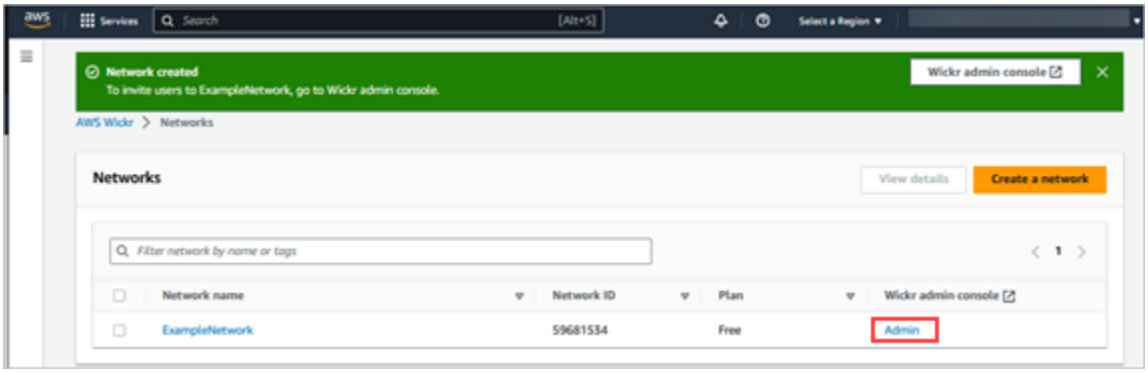
  > **Note**
  >
  > Se hai creato la tua rete Wickr in AWS GovCloud (Stati Uniti occidentali), chiedi ai tuoi utenti di scaricare e installare il client. WickrGov Per tutte le altre AWS regioni, chiedi ai tuoi utenti di scaricare e installare il client Wickr standard. Per ulteriori informazioni in merito AWS WickrGov, consulta la Guida AWS WickrGovper l'AWS GovCloud (US) utente.

Quando gli utenti si registrano alla rete Wickr, vengono aggiunti alla directory del team di Wickr con lo stato di attivo.

Non-SSO

Per creare manualmente utenti Wickr e inviare inviti:

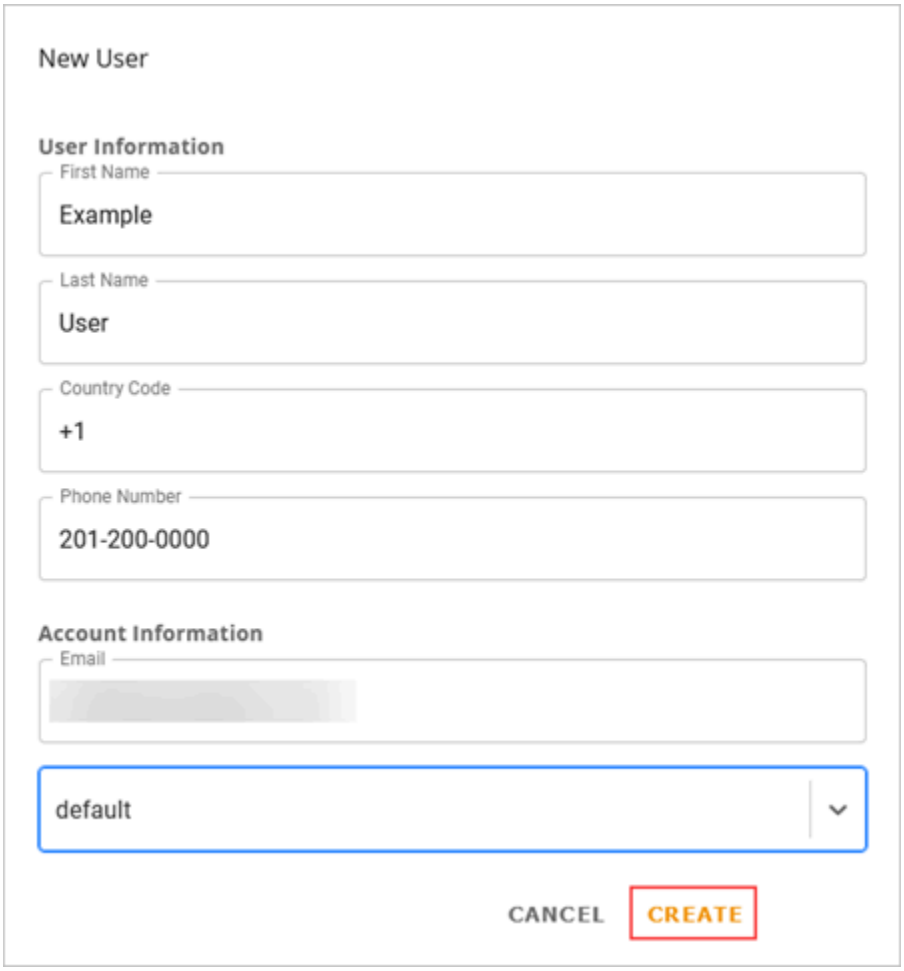
1. Apri il file AWS Management Console per Wickr all'indirizzo. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore, per accedere alla Console di amministrazione di Wickr per quella rete.



Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica. Nella console di amministrazione di Wickr, puoi aggiungere utenti, aggiungere gruppi di sicurezza, configurareSSO, configurare la conservazione dei dati e impostazioni aggiuntive per la rete specifica selezionata.

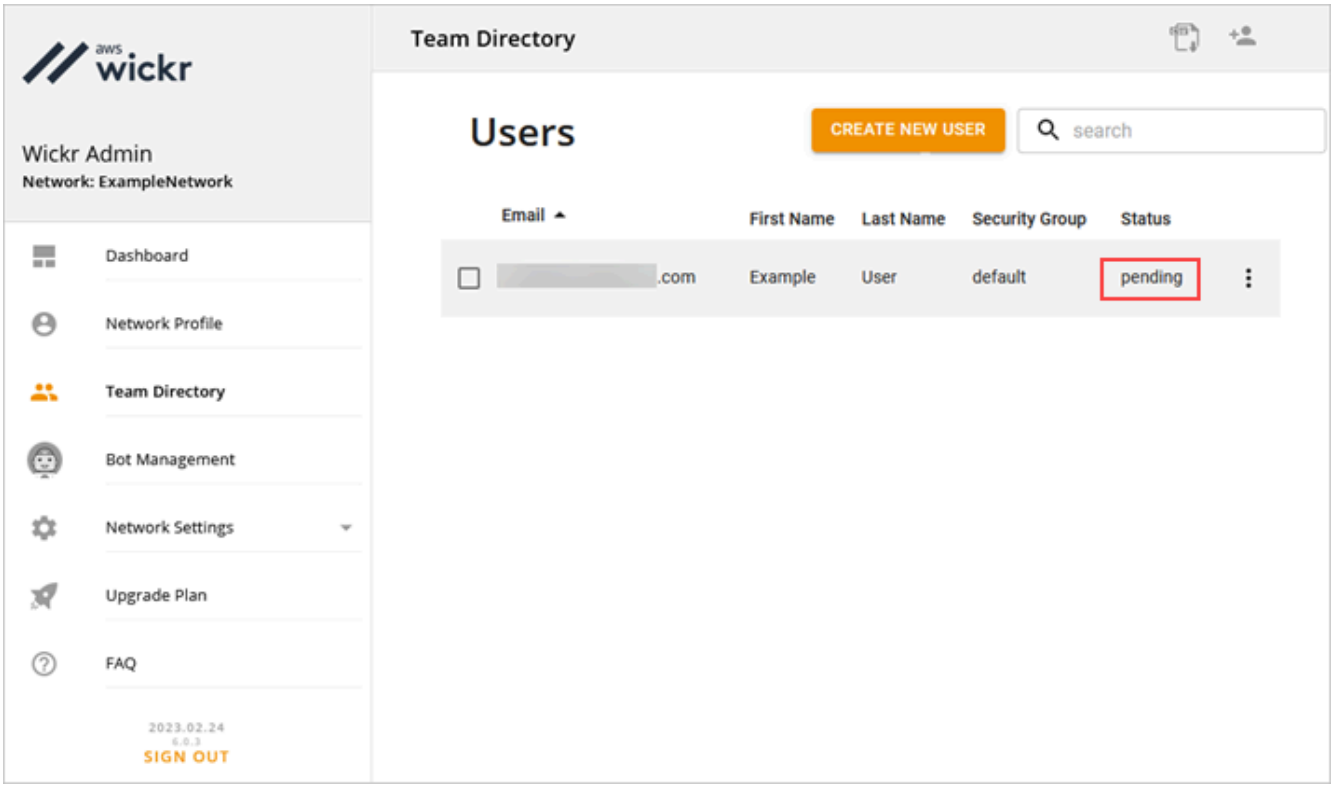
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utenti, quindi scegli Team Directory.

   Nella pagina Utenti, puoi aggiungere singoli utenti scegliendo Crea nuovo utente. Puoi anche aggiungere utenti in blocco scegliendo l'icona Aggiungi utenti nel riquadro di navigazione in alto. Scegli l'CSVicona Scarica per scaricare un CSV modello che puoi modificare e caricare con il tuo elenco di utenti.
4. Inserisci il nome, il cognome, il prefisso internazionale, il numero di telefono e l'indirizzo email dell'utente. L'indirizzo e-mail è l'unico campo obbligatorio. Assicurati di scegliere il gruppo di sicurezza appropriato per l'utente.
5. Scegli Create (Crea) .



Wickr invia un'email di invito all'indirizzo specificato per l'utente. L'e-mail fornisce i link per il download delle applicazioni client di Wickr e un link per la registrazione a Wickr. Per ulteriori informazioni sull'aspetto di questa esperienza per l'utente finale, consulta Scarica l'app Wickr e accetta l'invito nella Guida per l'utente di Wickr. AWS

Man mano che gli utenti si registrano a Wickr utilizzando il link contenuto nell'e-mail, il loro stato nella directory del team di Wickr cambierà da In sospeso a Attivo.



Passaggi successivi

Hai completato la procedura iniziale. Per gestire Wickr, consulta le seguenti guide:

- Gestisci la tua rete AWS Wickr
- Gestione degli utenti in AWS Wickr

Trasferisci Wickr Pro a Wickr AWS

> **Note**
>
> Wickr Pro è stato interrotto. Se hai perso l'accesso a Wickr Pro, segui i passaggi di questa guida per passare a Wickr. AWS

In questa guida, ti mostriamo come effettuare il trasferimento da Wickr Pro e iniziare a utilizzare Wickr. AWS

Segui i passaggi di questa guida se disponi di una rete Wickr Pro esistente, ma ne hai già una. NOT Account AWS Contatta l'assistenza in qualsiasi momento se hai bisogno di assistenza.

Se la tua organizzazione ha già un AWS account, completa il modulo Migra da Wickr Pro a Wickr e AWS il supporto di AWS Wickr ti aiuterà.

Avrai bisogno di un Account AWS ID per gestire la tua rete Wickr come. AWS Servizio AWS Per ulteriori informazioni su cos' Account AWS è un e su come gestire l'account, consulta la Guida di riferimento per la gestione degli AWS account.

Argomenti

Fase 1: Creare un AWS account

Completa la seguente procedura per creare un AWS account.

1. Se la tua organizzazione non dispone di un ID AWS account esistente, puoi iniziare creando un ID AWS account autonomo. Ecco alcune cose fondamentali di cui avrai bisogno a tal fine:

   - Una carta di credito/debito per la fatturazione
   - Un indirizzo e-mail accessibile da un gruppo (consigliato, non richiesto)
   - Seleziona un AWS Support piano. Per ulteriori informazioni, consulta Modifica AWS Support dei piani.

   > **Note**
   >
   > Puoi sempre modificare il tuo AWS Support piano man mano che scopri di più sulle tue esigenze.

2. Imposta l'accesso amministrativo IAM come procedura consigliata per la sicurezza (facoltativa ma consigliata). Per ulteriori informazioni, vedere AWS Identity and Access Management. Per istruzioni più specifiche sull'accesso amministrativo di AWS Wickr, consulta la politica AWS gestita:. AWSWickrFullAccess

3. Una volta completati i passaggi precedenti, potrai accedere a per trovare il AWS Management Console tuo Account AWS ID a 12 cifre sotto il nome del tuo account.

Passaggio 2: recupera il tuo ID di rete Wickr

Completa la seguente procedura per recuperare il tuo ID di rete Wickr.

1. Accedi alla tua attuale console di amministrazione Wickr e seleziona le reti che desideri migrare, quindi scegli Profilo di rete.
2. La pagina del profilo di rete mostra il tuo ID di rete ed è un ID numerico a 8 cifre.

Fase 3: Inviare una richiesta

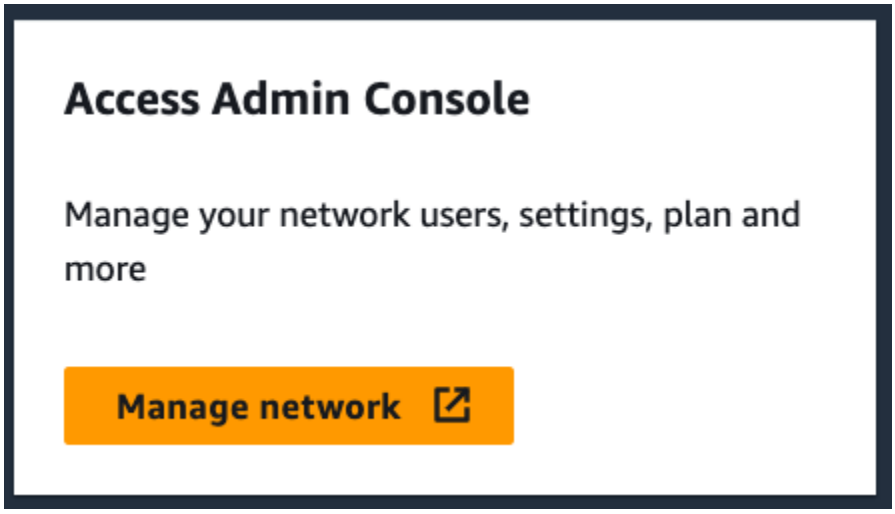
Ora che hai il tuo Account AWS ID e l'ID di rete Wickr Pro, dovrai completare il modulo Migra da Wickr Pro a Wickr. AWS

Una volta completato, in genere entro 14 giorni, un rappresentante dell'assistenza AWS Wickr ti contatterà per confermare che la tua rete Wickr è stata aggiunta alla tua. Account AWS

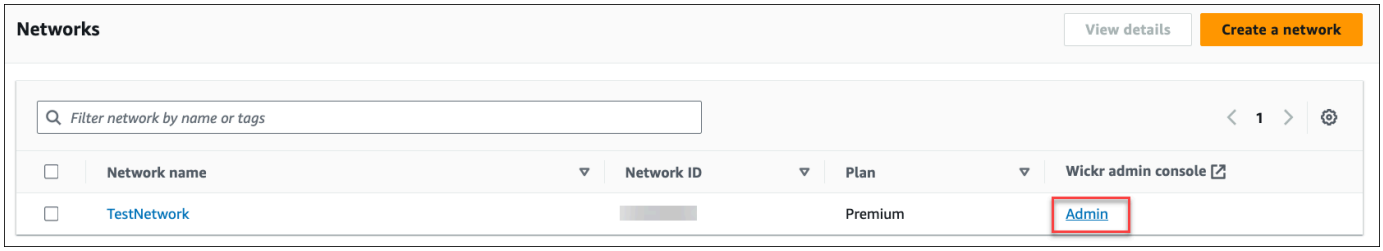
Passaggio 4: accedi alla tua console AWS

> **Note**
>
> Segui questi passaggi per AFTER ricevere la conferma che la tua rete Wickr Pro è stata aggiunta al tuo. Account AWS

1. Puoi accedere alla AWS console come utente root OPPURE con un IAM utente che hai creato in precedenza (come consigliato) nel passaggio 2 per AWS Wickr.
2. Accedi al tuo servizio AWS Wickr. Puoi farlo dal menu Servizi o cercando AWS Wickr nella barra di ricerca.
3. Nella pagina AWS Wickr, scegli Gestisci rete per accedere all'elenco delle reti Wickr.



4. Nella pagina Reti, nella colonna della console di amministrazione di Wickr, seleziona il link Amministratore a destra del nome di rete desiderato.



5. Il trasferimento è ora completo! Vedrai la dashboard della tua rete Wickr.

La fatturazione per la tua rete verrà ora trasferita al tuo. Account AWS Attendi fino a 3 giorni lavorativi prima che l'assistenza riceva una conferma. Dopo aver ricevuto la conferma, puoi visualizzare e pagare la fattura tramite la AWS console.

Gestisci la tua rete AWS Wickr

Nella sezione Impostazioni di rete del AWS Management Console per Wickr puoi gestire il nome della rete Wickr, i gruppi di sicurezza, la SSO configurazione e le impostazioni di conservazione dei dati.

Argomenti

Profilo di rete

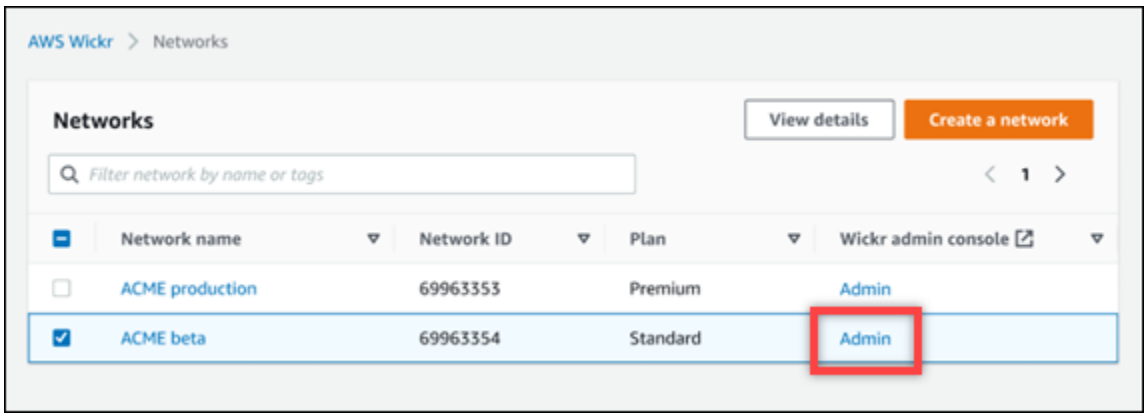
Puoi modificare il nome della tua rete Wickr e visualizzare il tuo ID di rete nella sezione Profilo di rete del AWS Management Console per Wickr.

Argomenti

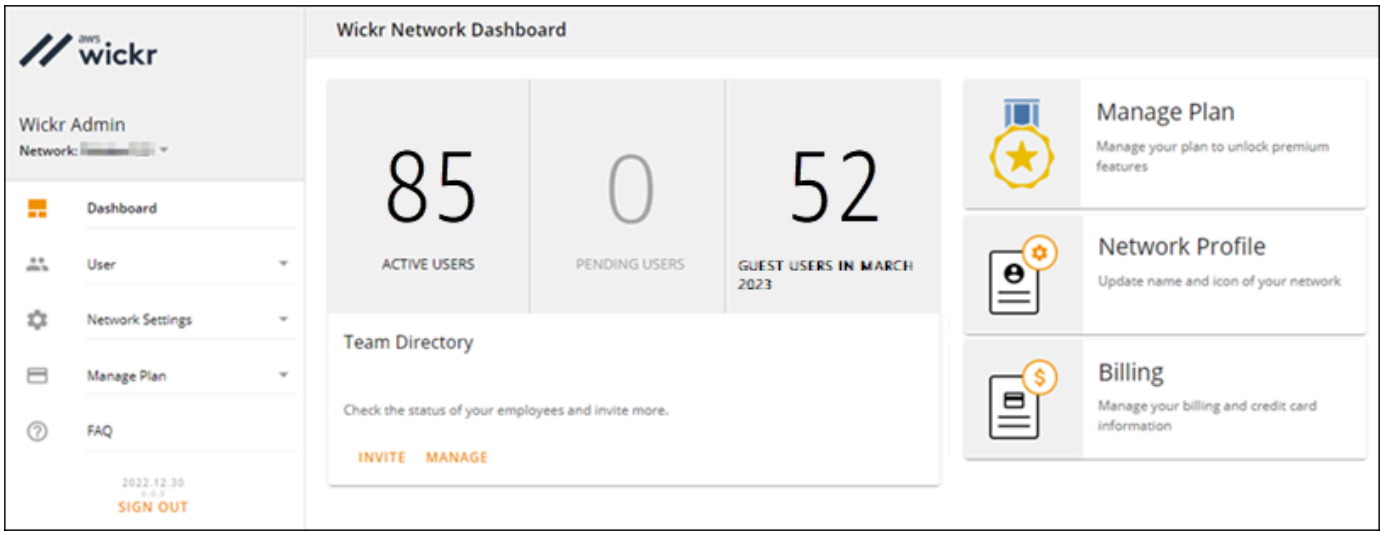
Visualizza il profilo di rete

Completa la seguente procedura per visualizzare il profilo di rete e l'ID di rete Wickr.

1. Aprire il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.



Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.



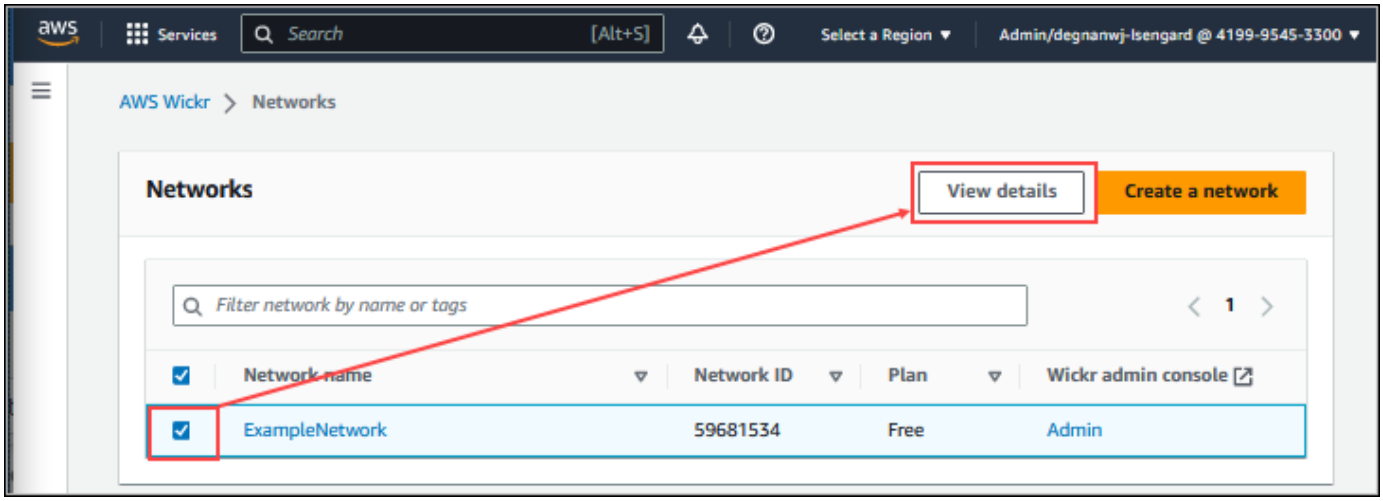
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Profilo di rete.

   La pagina del profilo di rete mostra il nome e l'ID di rete di Wickr. È possibile utilizzare l'ID di rete per configurare la federazione.

Modifica il nome della rete

Completa la seguente procedura per modificare il nome della tua rete Wickr.

1. Apri il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Scegli Gestisci rete.
3. Nella pagina Reti, seleziona la casella di controllo accanto al nome della rete che desideri modificare, quindi scegli Visualizza dettagli.



4. Nella sezione Panoramica della rete, scegli Modifica.
5. Inserisci il nuovo nome di rete nella casella di testo Nome rete.
6. Scegli Salva modifiche per salvare il nuovo nome di rete.

Gruppi di sicurezza

Nella sezione Gruppi di sicurezza del AWS Management Console per Wickr, puoi gestire i gruppi di sicurezza e le relative impostazioni, come le politiche di complessità delle password, le preferenze di messaggistica, le funzioni di chiamata, le funzionalità di sicurezza e la federazione delle reti.

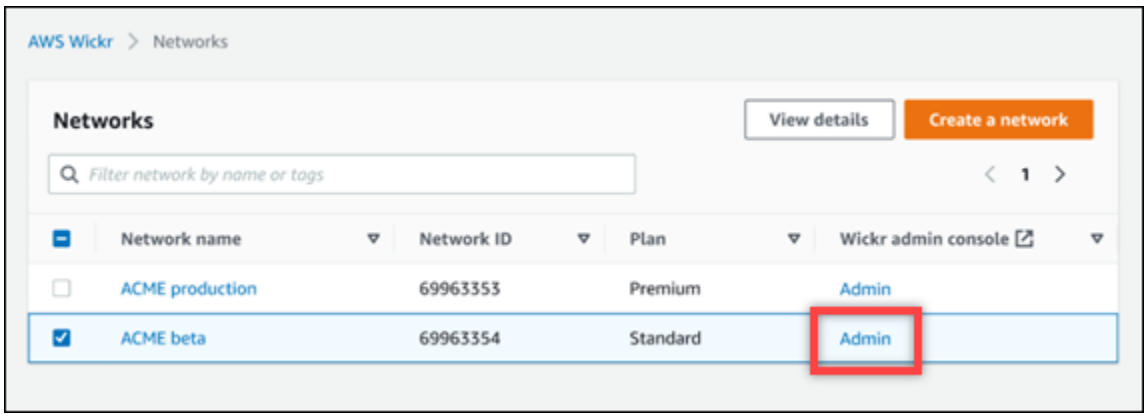
Argomenti

- Visualizza i gruppi di sicurezza
- Creazione di un gruppo di sicurezza
- Modificare un gruppo di sicurezza
- Eliminare un gruppo di sicurezza

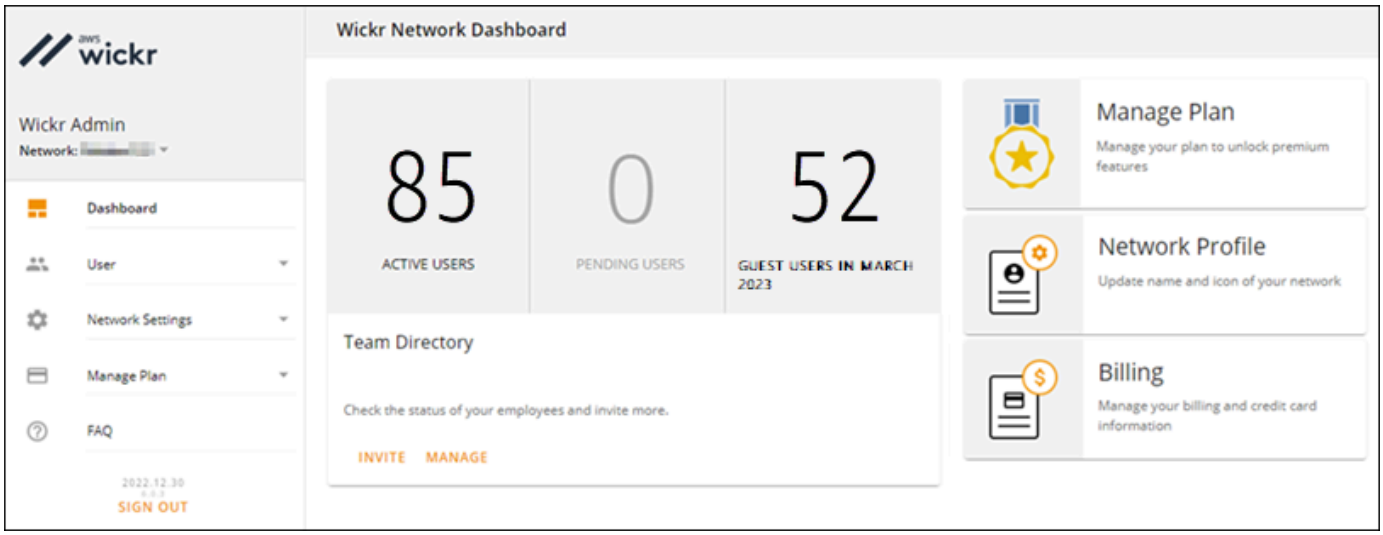
Visualizza i gruppi di sicurezza

Completare la procedura seguente per visualizzare i gruppi di sicurezza.

1. Aprire il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.



Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.



3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Gruppo di sicurezza.

   La pagina Gruppi di sicurezza mostra i gruppi di sicurezza Wickr attuali e ti dà la possibilità di visualizzarne i dettagli o crearne uno nuovo.

Creazione di un gruppo di sicurezza

Completa la seguente procedura per creare un gruppo di sicurezza.

1. Aprire il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.

3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Security Group.
4. Scegli Nuovo gruppo per creare un nuovo gruppo di sicurezza.

   Un nuovo gruppo di sicurezza con un nome predefinito viene aggiunto automaticamente all'elenco dei gruppi di sicurezza.

   Per ulteriori informazioni sulla modifica del nuovo gruppo di sicurezza, vedereModificare un gruppo di sicurezza.

Modificare un gruppo di sicurezza

Completare la procedura seguente per modificare un gruppo di sicurezza.

1. Aprire il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Security Group.
4. Scegli Dettagli accanto al nome del gruppo di sicurezza che desideri modificare.

   La pagina Dettagli del gruppo di sicurezza mostra le impostazioni per il gruppo di sicurezza in diverse schede.
5. Sono disponibili le seguenti schede e le impostazioni corrispondenti:

   - Nome del gruppo di sicurezza: scegli l'icona a forma di matita accanto al nome del gruppo per modificare il nome.
   - Generale: modifica la configurazione di base del gruppo.
   - Messaggistica: gestisci le funzionalità di messaggistica per i membri del gruppo.
   - Chiamate: gestisci le funzionalità di chiamata per i membri del gruppo.
   - Sicurezza: configura funzionalità di sicurezza aggiuntive per il gruppo.
   - Federazione: capacità di comunicare tra reti. Questa funzionalità può essere configurata nella console di amministrazione per una rete a livello di gruppo di sicurezza. AWSWickr ha 2 tipi di federazione: locale e globale.

- Federazione locale: la possibilità di federarsi con AWS utenti di altre reti all'interno della stessa regione. Ad esempio, se ci sono due reti in Canada con la federazione locale abilitata, queste saranno in grado di comunicare tra loro.
- Federazione globale: la possibilità di federarsi con utenti aziendali o AWS utenti di una rete diversa che appartengono ad altre regioni. Ad esempio, se c'è un utente in una rete nell'area del Canada e un utente in una rete nell'area di Londra e la federazione globale è attivata per entrambe le reti, saranno in grado di comunicare tra loro.
- Federazione con restrizioni: la possibilità di federarsi con reti specifiche (Enterprise o AWS) appartenenti a diverse regioni. Gli amministratori possono consentire l'elenco di reti specifiche con cui i loro utenti possono federarsi. Dopo la restrizione, gli utenti possono comunicare solo con gli utenti delle reti consentite. Per utilizzare la federazione con restrizioni, entrambe le reti devono inserirsi reciprocamente nelle impostazioni del gruppo di sicurezza nella scheda federazione.

6. Scegli Salva per salvare le modifiche apportate ai dettagli del gruppo di sicurezza.

Eliminare un gruppo di sicurezza

Completa la seguente procedura per eliminare un gruppo di sicurezza.

1. Aprire il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Security Group.
4. Scegli l'icona con i puntini di sospensione verticali accanto al nome del gruppo di sicurezza che desideri eliminare.
5. Scegli Rimuovi per eliminare il gruppo di sicurezza.

   Quando elimini un gruppo di sicurezza a cui sono stati assegnati utenti, tali utenti vengono aggiunti automaticamente al gruppo di sicurezza predefinito. Per modificare il gruppo di sicurezza assegnato agli utenti, vedereModifica utenti.

Configurazione Single Sign-On

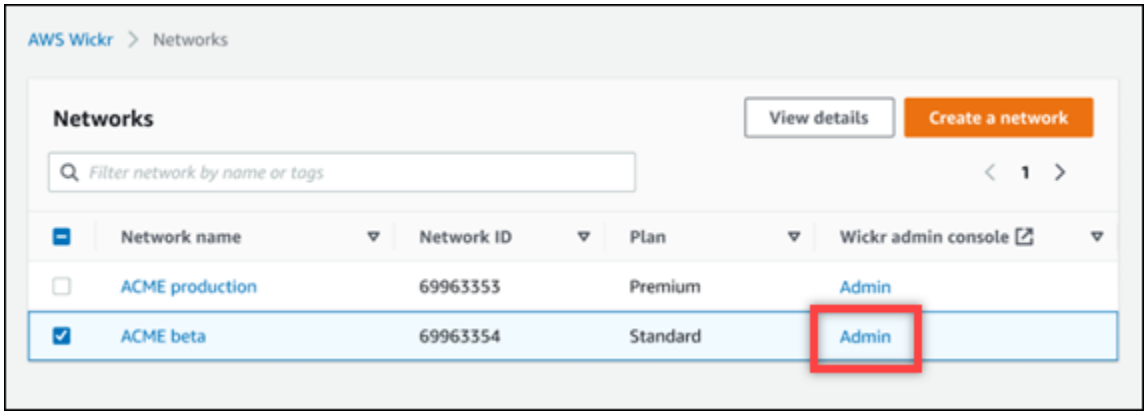
Nella sezione SSOConfigurazione di AWS Management Console per Wickr, puoi configurare Wickr in modo che utilizzi un sistema Single Sign-On per l'autenticazione. SSOfornisce un ulteriore livello di sicurezza se abbinato a un sistema di autenticazione a più fattori () appropriato. MFA Wickr supporta i SSO provider che utilizzano solo OpenID Connect (). OIDC I provider che utilizzano Security Assertion Markup Language () SAML non sono supportati.

Argomenti

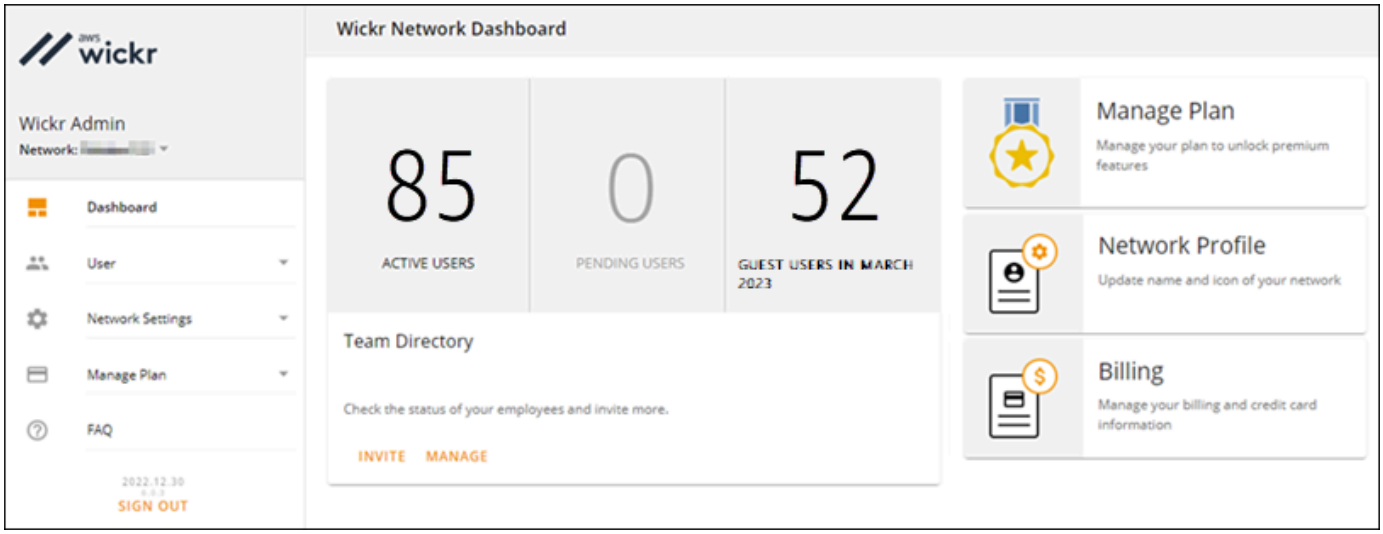
Visualizza i dettagli SSO

Completa la seguente procedura per visualizzare l'attuale configurazione Single Sign-On per la tua rete Wickr, se presente. Puoi anche visualizzare l'endpoint di rete per la tua rete Wickr.

1. Apri il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.



Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.



3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli SSO Configurazione.

   La pagina Single Sign-on e LDAP configurazione mostra l'endpoint di rete Wickr e la configurazione corrente. SSO

Configura SSO

Per ulteriori informazioni sulla configurazioneSSO, consulta le seguenti guide:

> **Important**
>
> Quando configuriSSO, specifichi un ID aziendale per la tua rete Wickr. Assicurati di annotare l'ID aziendale per la tua rete Wickr. È necessario fornirlo agli utenti finali quando si inviano e-mail di invito. Gli utenti finali devono specificare l'ID aziendale al momento della registrazione alla rete Wickr.

- Configurare l'accesso singolo per Microsoft Entra (Azure AD)
- Configura il single sign-on di Okta

Periodo di grazia per l'aggiornamento dei token

Occasionalmente, possono verificarsi casi in cui i provider di identità riscontrano interruzioni temporanee o prolungate, che possono comportare la disconnessione imprevista degli utenti a

causa di un errore del token di aggiornamento della sessione client. Per evitare questo problema, puoi stabilire un periodo di prova che consenta agli utenti di rimanere connessi anche se il token di aggiornamento del client si guasta durante tali interruzioni.

Ecco le opzioni disponibili per il periodo di grazia:

- Nessun periodo di tolleranza (impostazione predefinita): gli utenti verranno disconnessi immediatamente dopo un errore del token di aggiornamento.
- Periodo di prova di 30 minuti: gli utenti possono rimanere connessi fino a 30 minuti dopo un errore del token di aggiornamento.
- Periodo di prova di 60 minuti: gli utenti possono rimanere connessi fino a 60 minuti dopo un errore del token di aggiornamento.

Configurare l'accesso singolo per Microsoft Entra (Azure AD)

AWSWickr può essere configurato per utilizzare Microsoft Entra (Azure AD) come provider di identità. A tale scopo, completa le seguenti procedure sia in Microsoft Entra che nella console di amministrazione di AWS Wickr.

> **Warning**
>
> Una volta SSO abilitato su una rete, disconnetterà gli utenti attivi da Wickr e li costringerà a riautenticarsi utilizzando il provider. SSO

Passaggio 1: registra AWS Wickr come applicazione in Microsoft Entra

Completa la seguente procedura per registrare AWS Wickr come applicazione in Microsoft Entra.

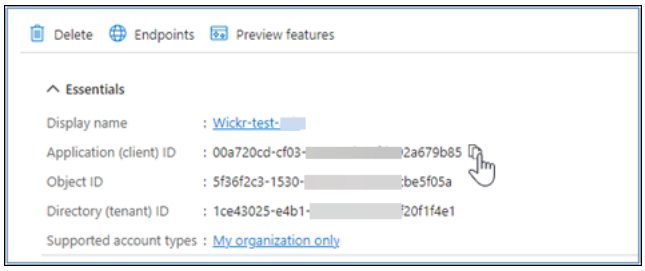
> **Note**
>
> Consulta la documentazione di Microsoft Entra per schermate dettagliate e risoluzione dei problemi. Per ulteriori informazioni, vedi Registrare un'applicazione con la piattaforma di identità Microsoft

1. Nel riquadro di navigazione, scegli Applicazioni, quindi scegli Registrazioni app.

2. Nella pagina Registrazioni delle app, scegli Registra un'applicazione, quindi inserisci il nome dell'applicazione.
3. Seleziona Account solo in questa directory organizzativa (solo directory predefinita - Tenant singolo).
4. In Reindirizzamento URI, seleziona Web, quindi inserisci il seguente indirizzo Web:. `https://messaging-pro-prod.wickr.com/deeplink/oidc.php`

> **Note**
>
> Il reindirizzamento URI può anche essere copiato dalle impostazioni di SSO configurazione nella console di amministrazione di AWS Wickr.

5. Scegli Registrati.
6. Dopo la registrazione, copia/salva l'ID dell'applicazione (client) generato.



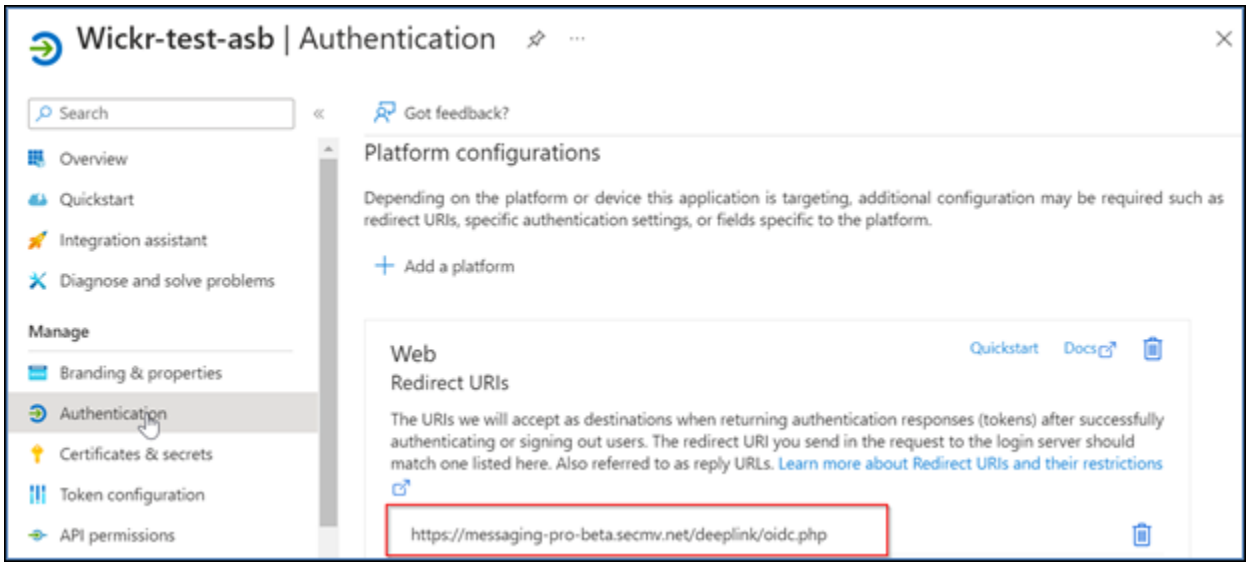
7. Seleziona la scheda Endpoints per prendere nota di quanto segue:
    1. Endpoint di autorizzazione Oauth 2.0 (v2): Ad esempio: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
    2. Modifica questo valore per rimuovere 'oauth2/» e «authorize». Ad esempio, URL fixed avrà questo aspetto: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
    3. Questo verrà denominato SSOEmittente.

Fase 2: Configurazione dell'autenticazione

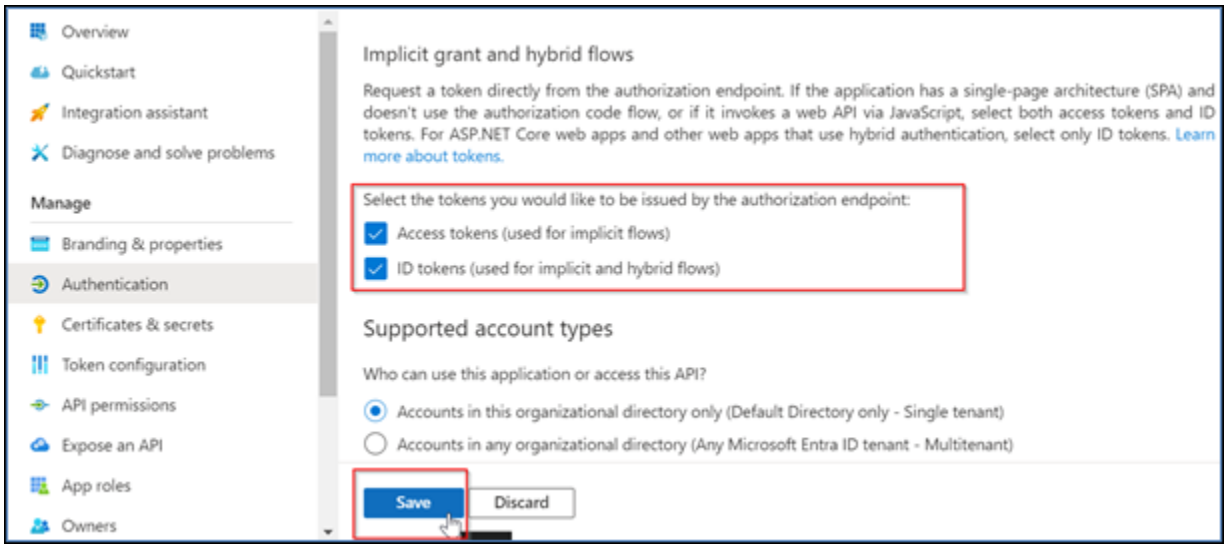
Completare la procedura seguente per configurare l'autenticazione in Microsoft Entra.

1. Nel riquadro di navigazione, scegli Autenticazione.

2. Nella pagina di autenticazione, assicurati che il reindirizzamento Web URI sia lo stesso inserito in precedenza (in Registra AWS Wickr come applicazione).



3. Seleziona i token di accesso utilizzati per i flussi impliciti e i token ID utilizzati per i flussi impliciti e ibridi.
4. Seleziona Salva.

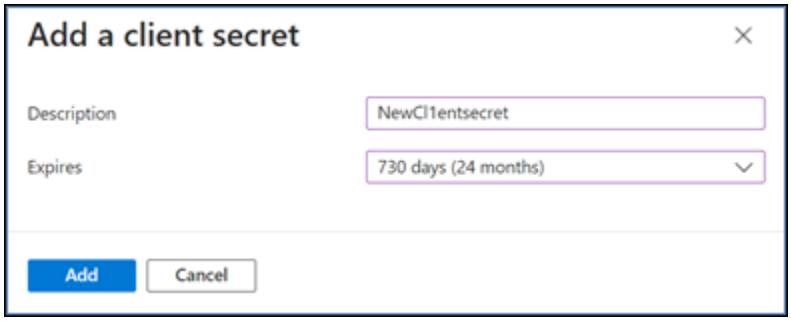


Fase 3: Configurazione di certificati e segreti

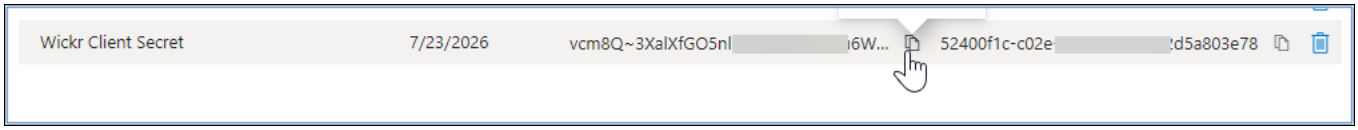
Completa la seguente procedura per configurare certificati e segreti in Microsoft Entra.

1. Nel riquadro di navigazione, scegli Certificati e segreti.
2. Nella pagina Certificati e segreti, seleziona la scheda Client secrets.

3. Nella scheda Client secrets, seleziona Nuovo client secret.
4. Inserisci una descrizione e seleziona un periodo di scadenza per il segreto.
5. Scegli Aggiungi.



6. Dopo aver creato il certificato, copia il valore segreto del client.

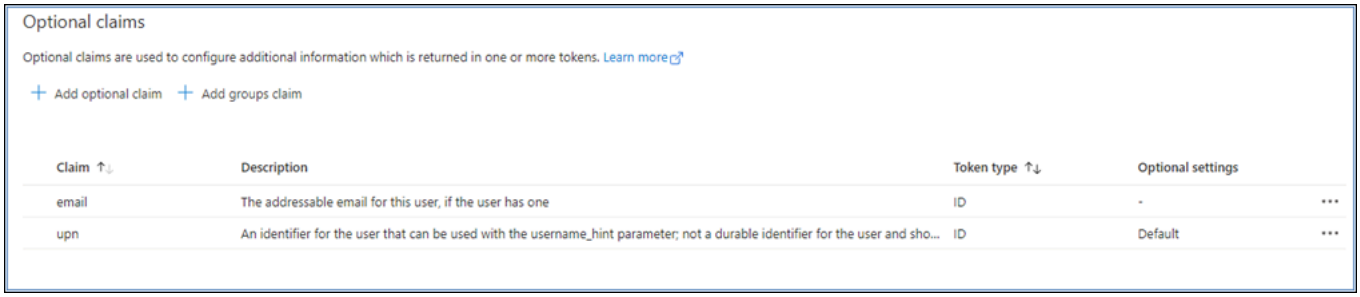


> **Note**
>
> Il valore segreto del client (non l'ID segreto) sarà richiesto per il codice dell'applicazione client. Potresti non essere in grado di visualizzare o copiare il valore segreto dopo aver lasciato questa pagina. Se non lo copi ora, dovrai tornare indietro per creare un nuovo client secret.

Fase 4: Configurazione del token di installazione

Completare la procedura seguente per configurare la configurazione dei token in Microsoft Entra.

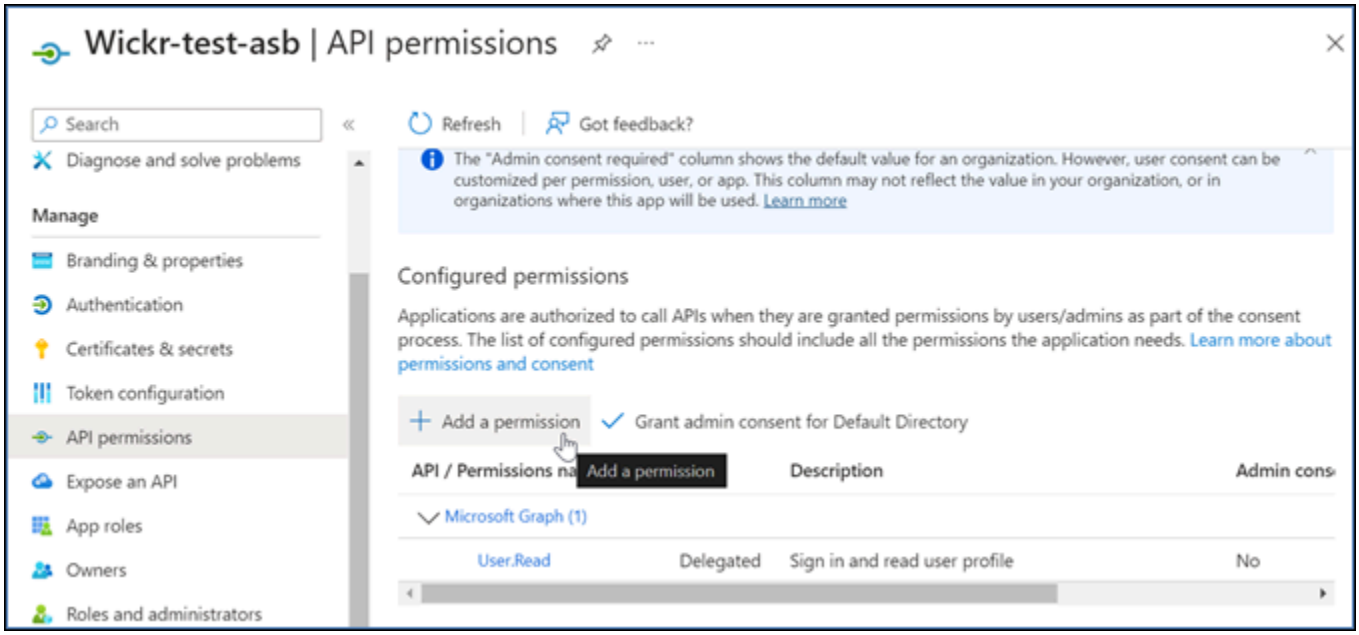
1. Nel riquadro di navigazione, scegli Configurazione token.
2. Nella pagina di configurazione del token, scegli Aggiungi reclamo opzionale.
3. In Reclami opzionali, seleziona il tipo di token come ID.
4. Dopo aver selezionato ID, in Reclamo, seleziona email e upn.
5. Scegli Aggiungi.



Fase 5: Configurazione delle API autorizzazioni

Completare la procedura seguente per configurare API le autorizzazioni in Microsoft Entra.

1. Nel riquadro di navigazione, scegli APIautorizzazioni.
2. Nella pagina delle APIautorizzazioni, scegli Aggiungi un'autorizzazione.



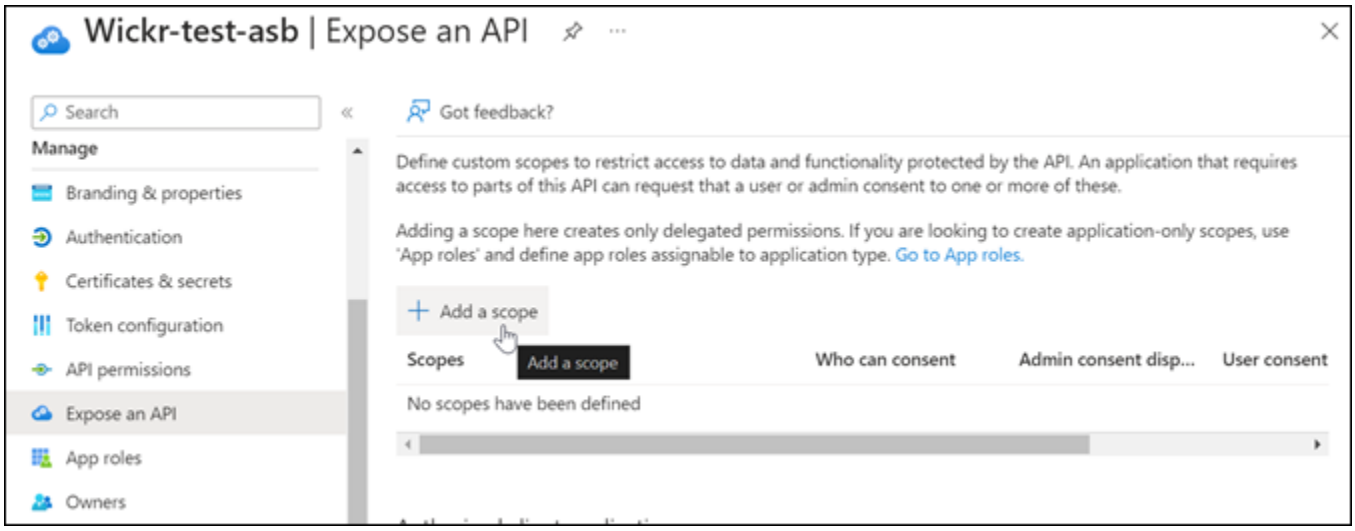
3. Seleziona Microsoft Graph, quindi seleziona Autorizzazioni delegate.
4. Seleziona la casella di controllo per email, offline_access, openid, profile.
5. Scegli Aggiungi autorizzazioni.

Passaggio 6: esporre un API

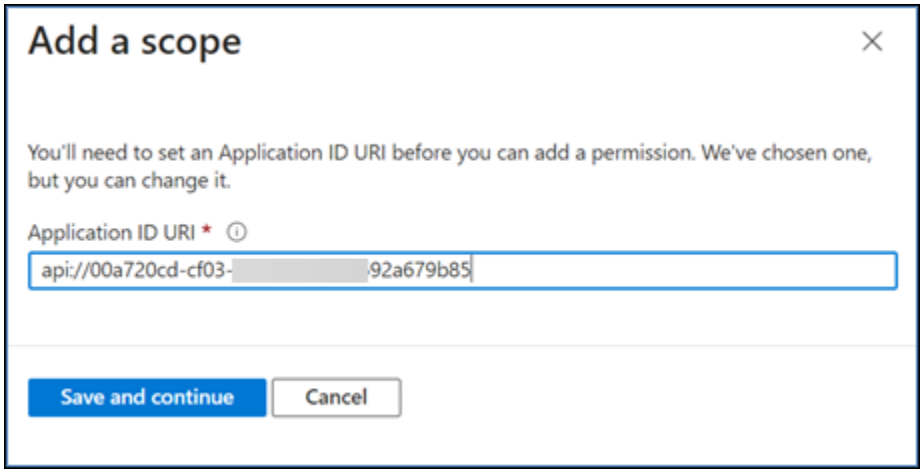
Completare la procedura seguente per esporre un API per ciascuno dei 4 ambiti in Microsoft Entra.

1. Nel riquadro di navigazione, scegli Esporre un. API

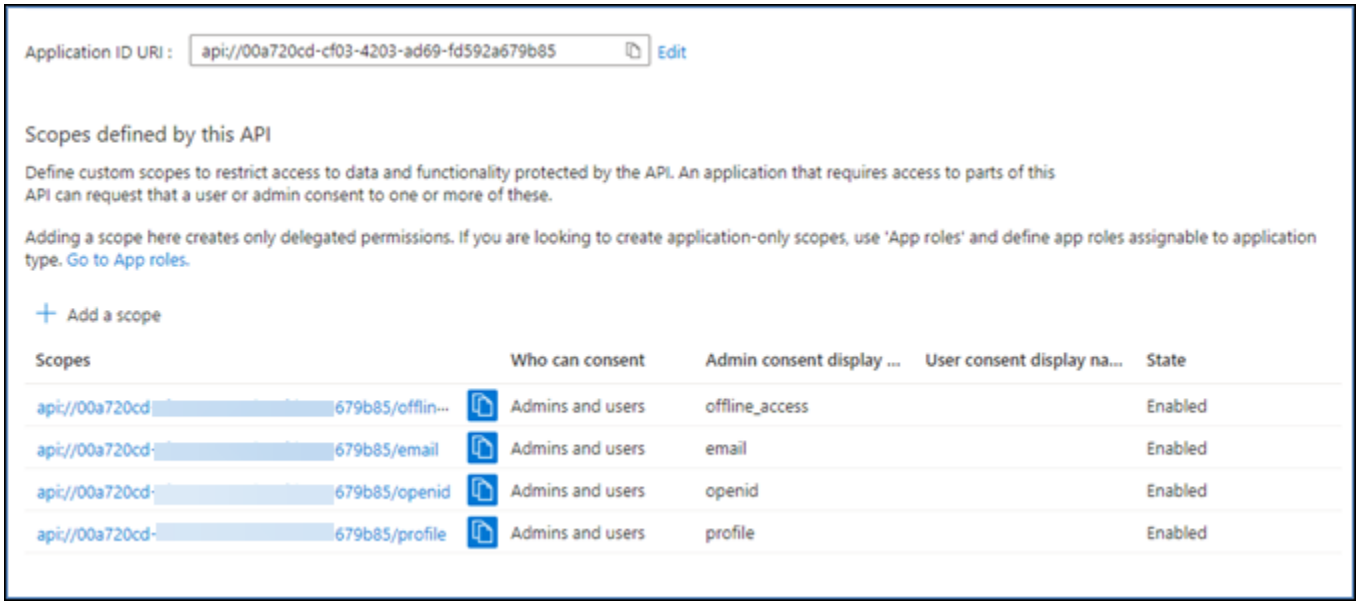
2. Nella API pagina Esporre un ambito, scegli Aggiungi un ambito.



L'ID dell'applicazione URI deve essere compilato automaticamente e l'ID che segue URI deve corrispondere all'ID dell'applicazione (creato in Register AWS Wickr come applicazione).



3. Seleziona Salva e continua.
4. Seleziona il tag Amministratori e utenti, quindi inserisci il nome dell'ambito come offline_access.
5. Seleziona Stato, quindi seleziona Abilita.
6. Scegli Aggiungi ambito.
7. Ripeti i passaggi da 1 a 6 di questa sezione per aggiungere i seguenti ambiti: email, openid e profile.



8. In Applicazioni client autorizzate, scegli Aggiungi un'applicazione client.
9. Seleziona tutti e quattro gli ambiti creati nel passaggio precedente.
10. Immettere o verificare l'ID dell'applicazione (client).
11. Scegli Aggiungi applicazione.

Fase 7: Configurazione di AWS Wickr SSO

Completa la seguente procedura di configurazione nella console AWS Wickr.

1. Apri il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Configurazione. SSO
4. In Network Endpoint, assicurati che il reindirizzamento URI corrisponda al seguente indirizzo web (aggiunto nel passaggio 4 in Registra AWS Wickr come applicazione).

   `https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.
5. In SSO Configurazione, scegli Avvia
6. Inserisci i seguenti dettagli:

   - SSOEmittente: questo è l'endpoint che è stato modificato in precedenza (ad es.). `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`

- SSOID client: si tratta dell'ID dell'applicazione (client) visualizzato nel riquadro Panoramica.
- ID aziendale: può essere un valore di testo univoco che include caratteri alfanumerici e caratteri di sottolineatura. Questa frase è ciò che gli utenti inseriranno al momento della registrazione su nuovi dispositivi.
- Segreto del client: questo è il segreto del client nel pannello Certificati e segreti.
- Ambiti: questi sono i nomi degli ambiti esposti nel riquadro Esponi un API. Inserisci email, profile, offline_access e openid.
- Ambito del nome utente personalizzato: inserisci upn.

Gli altri campi sono facoltativi.

7. Scegli Prova e salva.
8. Seleziona Salva.

SSOla configurazione è completa. Per verificare, ora puoi aggiungere un utente all'applicazione in Microsoft Entra e accedere con l'utente utilizzando SSO un ID aziendale.

Per ulteriori informazioni su come invitare e integrare utenti, consulta Creare e invitare utenti.

Risoluzione dei problemi

Di seguito sono riportati i problemi più comuni che potresti riscontrare e suggerimenti per risolverli.

- SSOIl test di connessione fallisce o non risponde:
  - Assicurati che l'SSOemittente sia configurato come previsto.
  - Assicurati che i campi obbligatori in SSOConfigured siano impostati come previsto.
- Il test di connessione ha esito positivo, ma l'utente non è in grado di effettuare il login:
  - Assicurati che l'utente sia aggiunto all'applicazione Wickr che hai registrato in Microsoft Entra.
  - Assicurati che l'utente stia utilizzando l'ID aziendale corretto, incluso il prefisso. Ad esempio UE1-DemoNetwork w_Drqtva.
  - Il Client Secret potrebbe non essere impostato correttamente nella configurazione di Wickr. AWS SSO Reimpostalo creando un altro segreto del client in Microsoft Entra e imposta il nuovo segreto del client nella configurazione di Wickr SSO.

Leggi le ricevute

Le conferme di lettura su Wickr sono notifiche inviate al mittente per mostrare quando il messaggio è stato letto. Queste ricevute sono disponibili nelle conversazioni. one-on-one Apparirà un solo segno di spunta per i messaggi inviati e un cerchio pieno con un segno di spunta per i messaggi letti. Per visualizzare le conferme di lettura sui messaggi durante le conversazioni esterne, entrambe le reti devono avere le conferme di lettura abilitate.

Gli amministratori possono abilitare o disabilitare le conferme di lettura nel pannello dell'amministratore. Questa impostazione verrà applicata all'intera rete.

Completare la procedura seguente per abilitare o disabilitare le conferme di lettura.

1. Aprire il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Profilo di rete.
3. Nella pagina del profilo di rete, nella sezione Leggi le ricevute, scegli Modifica.
4. Seleziona Abilita o Disattiva.

Tag di rete

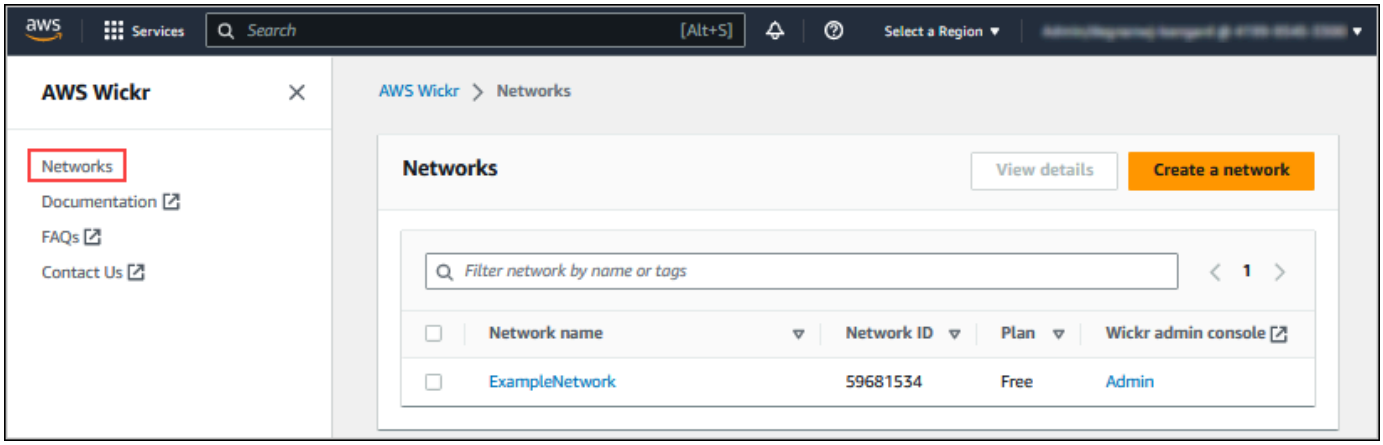
Puoi applicare tag alle reti Wickr. Puoi quindi utilizzare questi tag per cercare e filtrare le tue reti Wickr o tracciare le tue AWS costi. È possibile configurare i tag di rete nella pagina di panoramica della rete del AWS Management Console per Wickr.

Un tag è una coppia chiave-valore applicata a una risorsa per contenere i metadati relativi a quella risorsa. Ogni tag è un'etichetta composta da una chiave e un valore. Per ulteriori informazioni sui tag, consulta anche Cosa sono i tag? e casi d'uso del tagging.

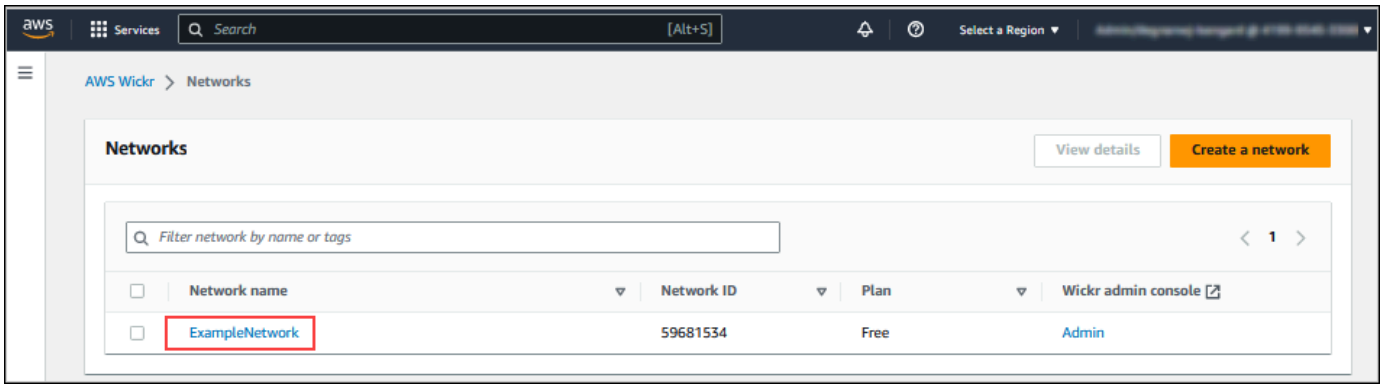
Gestisci i tag di rete

Completa la seguente procedura per gestire i tag di rete per la tua rete Wickr.

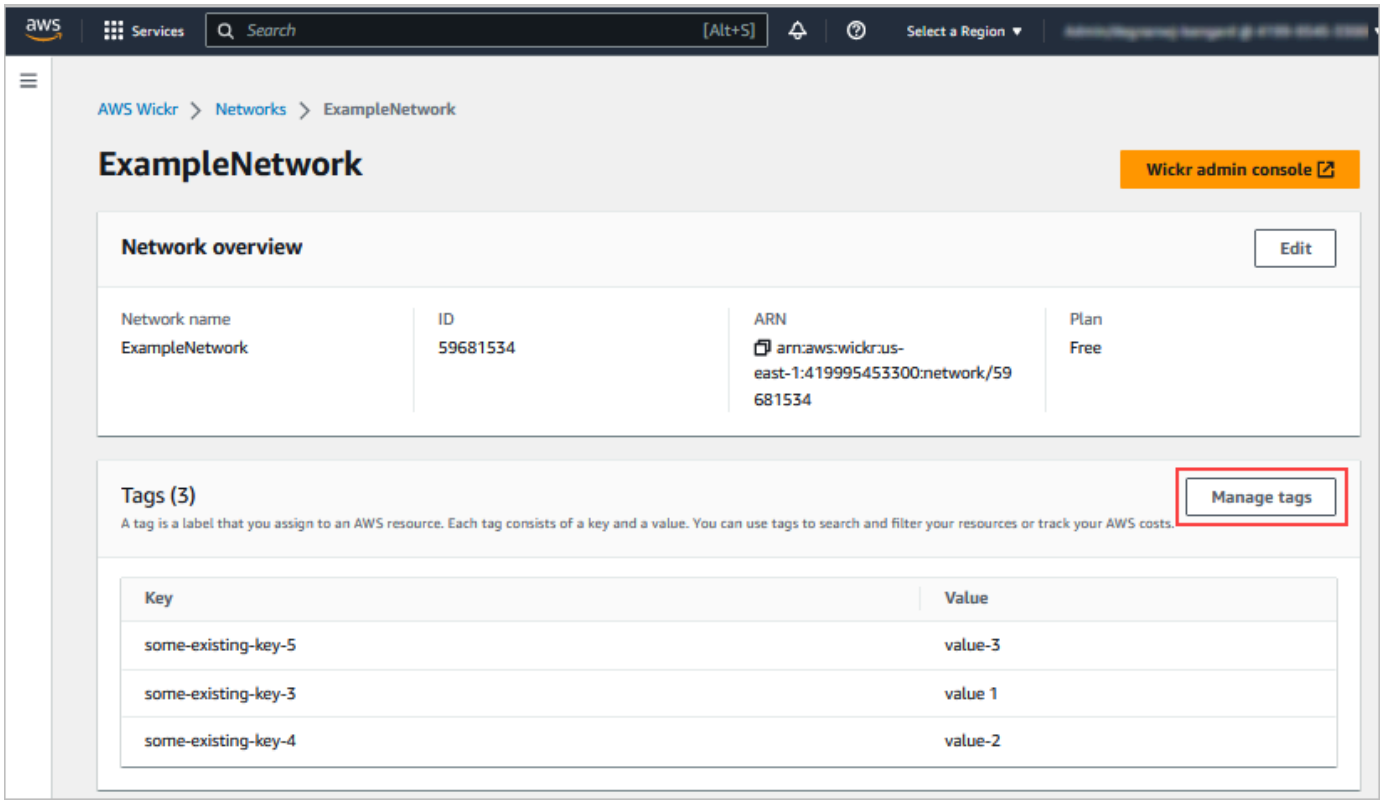
1. Apri il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Seleziona Reti dal pannello di navigazione del AWS Management Console per Wickr.



3. Nella pagina Reti, scegli il nome della rete per la quale desideri gestire i tag.



4. Nella pagina di panoramica della rete, scegli Gestisci tag.



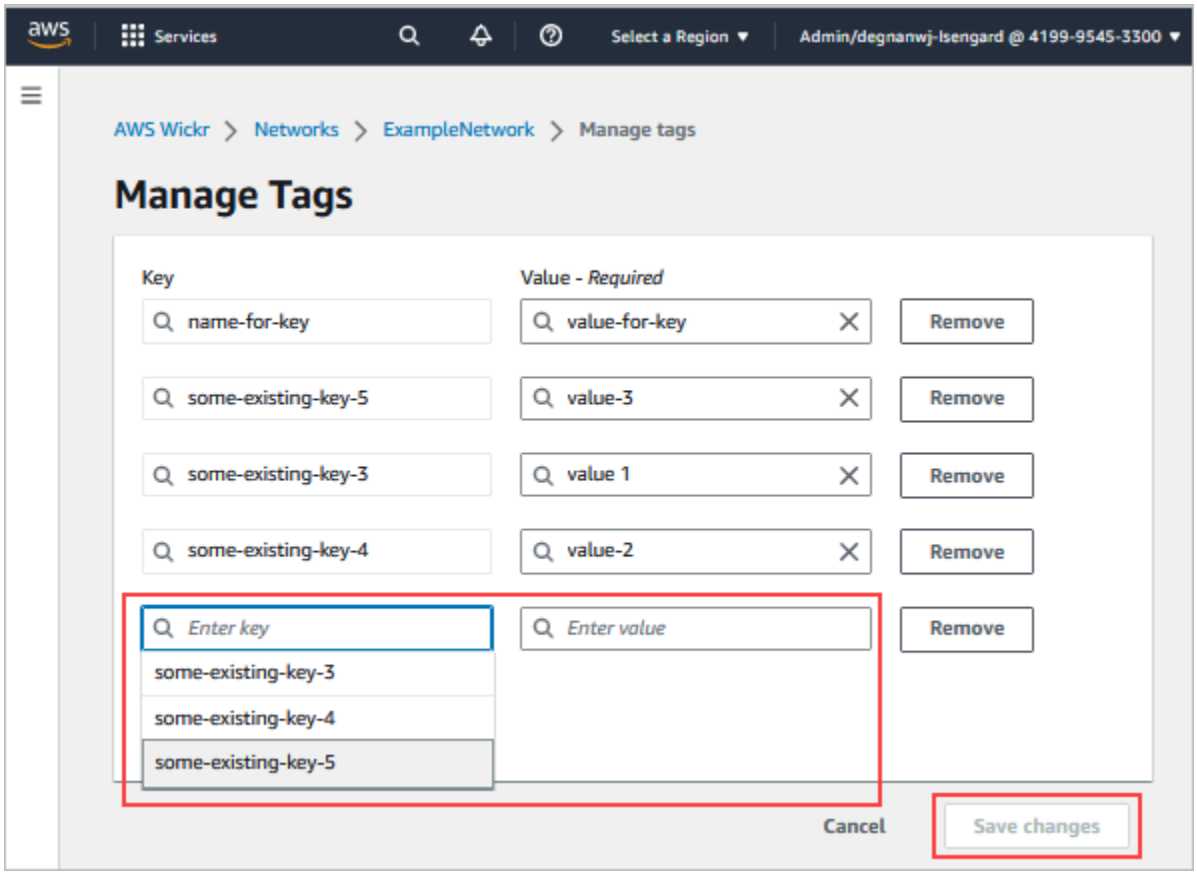
5. Nella pagina Gestisci tag, puoi completare una delle seguenti opzioni:

   - Aggiungi nuovi tag: inserisci nuovi tag sotto forma di chiave e coppia di valori. Scegli Aggiungi nuovo tag per aggiungere più coppie chiave-valore. I tag rispettano la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Aggiungi un tag di rete.
   - Modifica tag esistenti: seleziona il testo della chiave o del valore per un tag esistente, quindi inserisci la modifica nella casella di testo. Per ulteriori informazioni, consulta Modifica un tag di rete.
   - Rimuovi tag esistenti: scegli il pulsante Rimuovi che è elencato accanto al tag che desideri eliminare. Per ulteriori informazioni, consulta Rimuovi un tag di rete.

Aggiungi un tag di rete

Completa la seguente procedura per aggiungere un tag alla tua rete Wickr. Per ulteriori informazioni sulla gestione dei tag, consulta. Gestisci i tag di rete

1. Nella pagina Gestisci tag, scegli Aggiungi nuovo tag.
2. Nei campi vuoti Chiave e Valore che appaiono, inserisci la nuova chiave e il valore del tag.
3. Scegli Salva modifiche per salvare i nuovi tag.

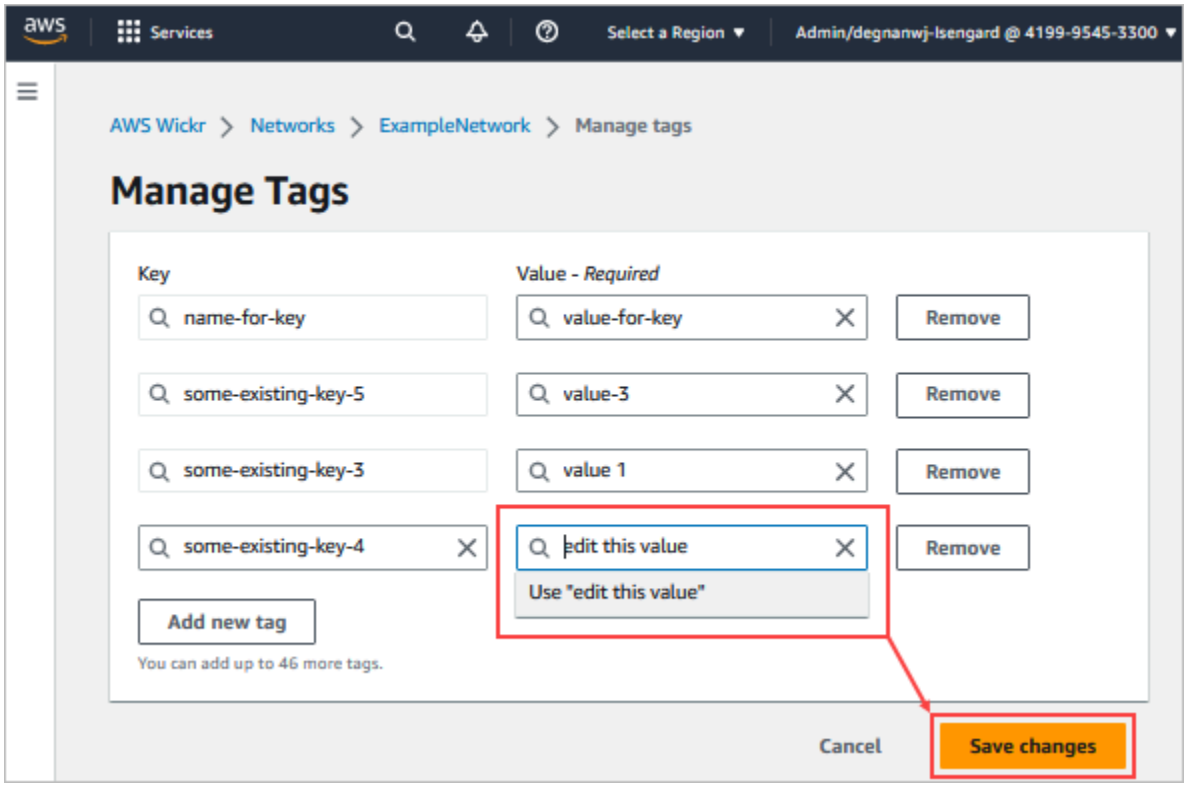


Modifica un tag di rete

Completa la seguente procedura per modificare un tag associato alla tua rete Wickr. Per ulteriori informazioni sulla gestione dei tag, consulta. Gestisci i tag di rete

1. Nella pagina Gestisci tag, modifica il valore di un tag.

> **Note**
>
> Non puoi modificare la chiave di un tag. Rimuovi invece la coppia chiave-valore e aggiungi un nuovo tag utilizzando la nuova chiave.

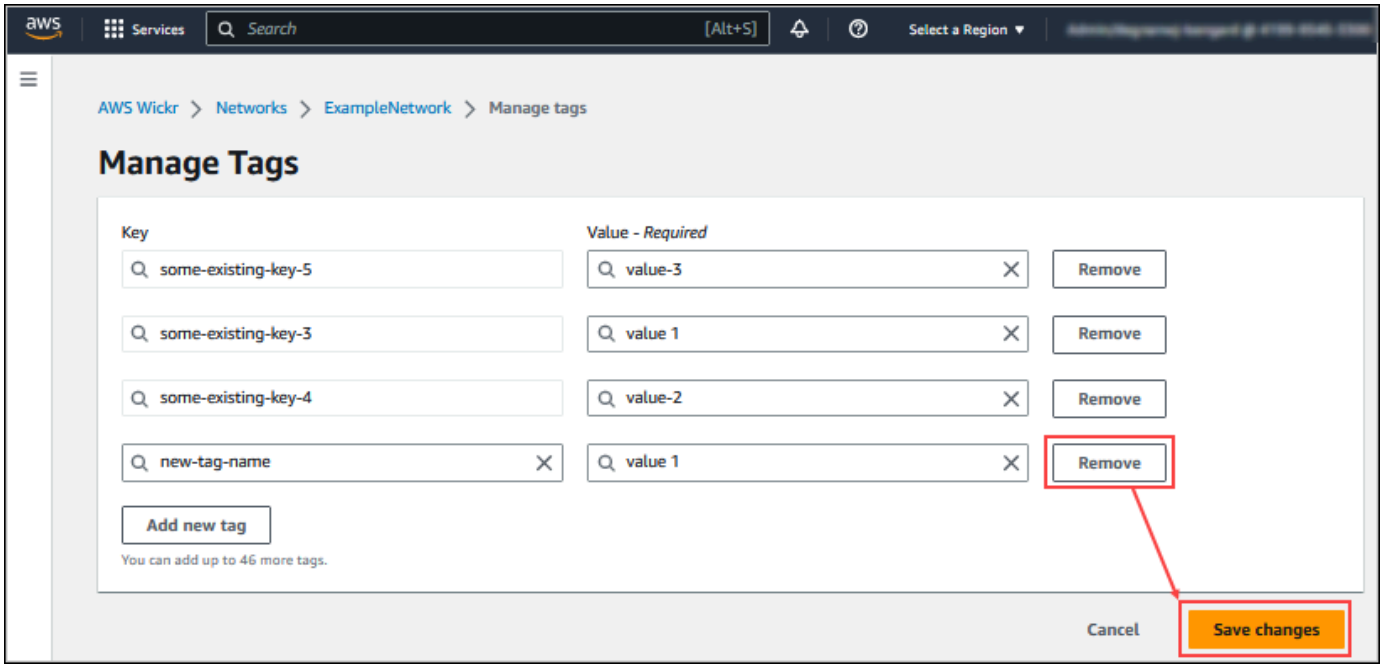


2. Scegli Salva modifiche per salvare le modifiche.

Rimuovi un tag di rete

Completa la seguente procedura per rimuovere un tag dalla tua rete Wickr. Per ulteriori informazioni sulla gestione dei tag, consulta. Gestisci i tag di rete

1. Nella pagina Gestisci tag, scegli Rimuovi per il tag che desideri rimuovere.



2. Scegli Salva modifiche per salvare le modifiche.

Gestisci il piano di rete

Nella sezione Gestisci il piano di AWS Management Console per Wickr, puoi gestire il tuo piano di rete in base alle tue esigenze aziendali.

Per gestire il tuo piano di rete, completa la seguente procedura.

1. Aprire il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Gestisci piano, quindi scegli Il mio piano.
3. Nella pagina Il mio piano, scegli il piano di rete desiderato. Puoi modificare il tuo attuale piano di rete scegliendo una delle seguenti opzioni:

   - Standard: per team di piccole e grandi aziende che necessitano di controlli amministrativi e flessibilità.
   - Versione di prova gratuita Premium o Premium: per le aziende che richiedono i massimi limiti di funzionalità, controlli amministrativi granulari e conservazione dei dati.

     Gli amministratori possono scegliere l'opzione di prova gratuita premium, disponibile per un massimo di 30 utenti e della durata di tre mesi. Questa offerta è aperta a nuovi piani di prova

gratuiti e standard. Gli amministratori possono effettuare l'upgrade o il downgrade ai piani Premium o Standard durante il periodo di prova gratuito premium.

> **Note**
>
> Per interrompere l'utilizzo e la fatturazione sulla rete, rimuovi tutti gli utenti, inclusi gli utenti sospesi, dalla rete.

Limitazioni della prova gratuita Premium

Le seguenti limitazioni si applicano alla prova gratuita premium:

- Se un piano è già stato sottoscritto in precedenza a una prova gratuita premium, non sarà idoneo per un'altra prova.
- Solo una rete per ogni rete AWS l'account può essere registrato a una prova gratuita premium.
- La funzione utente ospite non è disponibile durante la prova gratuita premium.
- Se una rete standard ha più di 30 utenti, non sarà possibile passare a una versione di prova gratuita premium.

Conservazione dei dati

AWSWickr Data retention può conservare tutte le conversazioni in rete. Ciò include le conversazioni dirette con messaggi e le conversazioni in gruppi o stanze tra membri della rete (interni) e quelle con altri team (esterni) con cui è federata la rete. La conservazione dei dati è disponibile solo per gli utenti del piano AWS Wickr Premium e per i clienti aziendali che optano per la conservazione dei dati. Per ulteriori informazioni sul piano Premium, consulta la pagina dei prezzi di Wickr

Quando un amministratore di rete configura e attiva la conservazione dei dati per la propria rete, tutti i messaggi e i file condivisi nella rete vengono conservati in conformità con le politiche di conformità dell'organizzazione. Questi output di file.txt sono accessibili dall'amministratore di rete in una posizione esterna (ad esempio: storage locale, bucket Amazon S3 o qualsiasi altro storage a scelta dell'utente), da dove possono essere analizzati, cancellati o trasferiti.

> **Note**
>
> Wickr non accede mai ai tuoi messaggi e file. Pertanto, è tua responsabilità configurare un sistema di conservazione dei dati.

Argomenti

Visualizza i dettagli sulla conservazione dei dati

Completa la seguente procedura per visualizzare i dettagli sulla conservazione dei dati per la tua rete Wickr. Puoi anche abilitare o disabilitare la conservazione dei dati per la tua rete Wickr.

1. Apri il AWS Management Console per Wickr presso. https://console.aws.amazon.com/wickr/
2. Scegli Gestisci rete.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Conservazione dei dati.

   La pagina Data Retention mostra i passaggi per impostare la conservazione dei dati e l'opzione per attivare o disattivare la funzione di conservazione dei dati. Per ulteriori informazioni sulla configurazione della conservazione dei dati, vedere. Configurare la conservazione dei dati

> **Note**
>
> Quando la conservazione dei dati è attivata, un messaggio Data Retention Turned On sarà visibile a tutti gli utenti della rete per informarli della rete abilitata alla conservazione.

Configurare la conservazione dei dati

Per configurare la conservazione dei dati per la tua rete AWS Wickr, devi distribuire l'immagine Docker del bot di conservazione dei dati in un contenitore su un host, come un computer locale

o un'istanza in Amazon Elastic Compute Cloud (Amazon EC2). Dopo aver distribuito il bot, puoi configurarlo per archiviare i dati localmente o in un bucket Amazon Simple Storage Service (Amazon S3). Puoi anche configurare il bot di conservazione dei dati per utilizzare altri AWS servizi come AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) e (). AWS Key Management Service AWS KMS I seguenti argomenti descrivono come configurare ed eseguire il bot di conservazione dei dati per la rete Wickr.

Argomenti

Prerequisiti per configurare la conservazione dei dati

Prima di iniziare, devi ottenere il nome del bot di conservazione dei dati (etichettato come nome utente) e la password iniziale da AWS Management Console for Wickr. È necessario specificare entrambi questi valori la prima volta che si avvia il bot di conservazione dei dati. È inoltre necessario abilitare la conservazione dei dati nella console. Per ulteriori informazioni, consulta Visualizza i dettagli sulla conservazione dei dati.

Password

La prima volta che avvii il bot di conservazione dei dati, specifichi la password iniziale utilizzando una delle seguenti opzioni:

- La variabile di `WICKRIO_BOT_PASSWORD` ambiente. Le variabili di ambiente del bot di conservazione dei dati sono descritte nella Variabili di ambiente sezione successiva di questa guida.
- Il valore della password in Secrets Manager identificato dalla variabile di `AWS_SECRET_NAME` ambiente. I valori di Secrets Manager per il bot di conservazione dei dati sono descritti nella I valori di Secrets Manager sezione successiva di questa guida.

- Immettete la password quando richiesto dal bot di conservazione dei dati. Dovrai eseguire il bot di conservazione dei dati con accesso TTY interattivo utilizzando l'`-ti`opzione.

Una nuova password verrà generata quando si configura il bot di conservazione dei dati per la prima volta. Se è necessario reinstallare il bot di conservazione dei dati, si utilizza la password generata. La password iniziale non è valida dopo l'installazione iniziale del bot di conservazione dei dati.

La nuova password generata verrà visualizzata come illustrato nell'esempio seguente.

> **Important**
>
> Conserva la password in un luogo sicuro. Se si perde la password, non sarà possibile reinstallare il bot di conservazione dei dati. Non condividere questa password. Offre la possibilità di avviare la conservazione dei dati per la rete Wickr.

```
******************************************************************
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
 "HuEXAMPLERAW4lGgEXAMPLEn"
 ******************************************************************
```

Opzioni di archiviazione

Dopo aver abilitato la conservazione dei dati e configurato il bot di conservazione dei dati per la rete Wickr, acquisirà tutti i messaggi e i file inviati all'interno della rete. I messaggi vengono salvati in file limitati a una dimensione o un limite di tempo specifici che possono essere configurati utilizzando una variabile di ambiente. Per ulteriori informazioni, consulta Variabili di ambiente.

È possibile configurare una delle seguenti opzioni per l'archiviazione di questi dati:

- Archivia localmente tutti i messaggi e i file acquisiti. Questa è l'opzione predefinita. È responsabilità dell'utente spostare i file locali su un altro sistema per l'archiviazione a lungo termine e assicurarsi che la memoria o lo spazio sul disco host non si esauriscano.
- Archivia tutti i messaggi e i file acquisiti in un bucket Amazon S3. Il bot di conservazione dei dati salverà tutti i messaggi e i file decrittografati nel bucket Amazon S3 specificato. I messaggi e i file acquisiti vengono rimossi dal computer host dopo essere stati salvati correttamente nel bucket.

- Archivia tutti i messaggi e i file acquisiti crittografati in un bucket Amazon S3. Il bot di conservazione dei dati crittograferà nuovamente tutti i messaggi e i file acquisiti utilizzando una chiave fornita dall'utente e li salverà nel bucket Amazon S3 specificato. I messaggi e i file acquisiti vengono rimossi dal computer host dopo essere stati correttamente ricrittografati e salvati nel bucket. Avrai bisogno di un software per decrittografare i messaggi e i file.

  Per ulteriori informazioni sulla creazione di un bucket Amazon S3 da utilizzare con il bot di conservazione dei dati, consulta Creating a bucket nella Amazon S3 User Guide

Variabili di ambiente

Puoi utilizzare le seguenti variabili di ambiente per configurare il bot di conservazione dei dati. Puoi impostare queste variabili di ambiente utilizzando l'`-e`opzione quando esegui l'immagine Docker del bot di conservazione dei dati. Per ulteriori informazioni, consulta Avvia il bot di conservazione dei dati.

> **Note**
>
> Queste variabili di ambiente sono opzionali se non diversamente specificato.

Utilizza le seguenti variabili di ambiente per specificare le credenziali del bot di conservazione dei dati:

- `WICKRIO_BOT_NAME`— Il nome del bot di conservazione dei dati. Questa variabile è necessaria quando si esegue l'immagine Docker del bot di conservazione dei dati.
- `WICKRIO_BOT_PASSWORD`— La password iniziale per il bot di conservazione dei dati. Per ulteriori informazioni, consulta Prerequisiti per configurare la conservazione dei dati. Questa variabile è necessaria se non si prevede di avviare il bot di conservazione dei dati con una richiesta di password o se non si prevede di utilizzare Secrets Manager per archiviare le credenziali del bot di conservazione dei dati.

Utilizzate le seguenti variabili di ambiente per configurare le funzionalità di streaming di conservazione dei dati predefinite:

- `WICKRIO_COMP_MESGDEST`— Il nome del percorso della directory in cui verranno trasmessi i messaggi. Il valore predefinito è `/tmp/<botname>/compliance/messages`.

- `WICKRIO_COMP_FILEDEST`— Il nome del percorso della directory in cui verranno trasmessi i file. Il valore predefinito è `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME`— Il nome di base per i file dei messaggi ricevuti. Il valore predefinito è `receivedMessages`.
- `WICKRIO_COMP_FILESIZE`— La dimensione massima per un file di messaggi ricevuti in kibibyte (KiB). Un nuovo file viene avviato quando viene raggiunta la dimensione massima. Il valore predefinito è`1000000000`, ad esempio, 1024 GiB.
- `WICKRIO_COMP_TIMEROTATE`— La quantità di tempo, in minuti, per la quale il bot di conservazione dei dati inserirà i messaggi ricevuti in un file di messaggi ricevuti. Un nuovo file viene avviato quando viene raggiunto il limite di tempo. È possibile utilizzare la dimensione o la durata del file solo per limitare la dimensione del file dei messaggi ricevuti. Il valore predefinito è`0`, ad esempio senza limiti.

Utilizzate la seguente variabile di ambiente per definire l'impostazione predefinita Regione AWS da utilizzare.

- `AWS_DEFAULT_REGION`— L'impostazione predefinita Regione AWS da utilizzare per AWS servizi come Secrets Manager (non utilizzato per Amazon S3 oAWS KMS). La `us-east-1` regione viene utilizzata per impostazione predefinita se questa variabile di ambiente non è definita.

Utilizzate le seguenti variabili di ambiente per specificare il segreto di Secrets Manager da utilizzare quando scegliete di utilizzare Secrets Manager per archiviare le credenziali del bot di conservazione dei dati e le informazioni sul AWS servizio. Per ulteriori informazioni sui valori che è possibile memorizzare in Secrets Manager, vedere[l valori di Secrets Manager](#).

- `AWS_SECRET_NAME`— Il nome del segreto di Secrets Manager che contiene le credenziali e le informazioni AWS di servizio necessarie al bot di conservazione dei dati.
- `AWS_SECRET_REGION`— Il luogo Regione AWS in cui si trova il AWS segreto. Se si utilizzano AWS segreti e questo valore non è definito, verrà utilizzato il `AWS_DEFAULT_REGION` valore.

> **Note**
>
> È possibile memorizzare tutte le seguenti variabili di ambiente come valori in Secrets Manager. Se scegli di utilizzare Secrets Manager e memorizzi questi valori lì, non è necessario specificarli come variabili di ambiente quando esegui l'immagine Docker del bot di

conservazione dei dati. È sufficiente specificare la variabile di `AWS_SECRET_NAME` ambiente descritta in precedenza in questa guida. Per ulteriori informazioni, consulta I valori di Secrets Manager.

Utilizza le seguenti variabili di ambiente per specificare il bucket Amazon S3 quando scegli di archiviare messaggi e file in un bucket.

- `WICKRIO_S3_BUCKET_NAME`— Il nome del bucket Amazon S3 in cui verranno archiviati messaggi e file.
- `WICKRIO_S3_REGION`— La AWS regione del bucket Amazon S3 in cui verranno archiviati messaggi e file.
- `WICKRIO_S3_FOLDER_NAME`— Il nome della cartella opzionale nel bucket Amazon S3 in cui verranno archiviati messaggi e file. Il nome di questa cartella sarà preceduto dalla chiave per i messaggi e i file salvati nel bucket Amazon S3.

Utilizza le seguenti variabili di ambiente per specificare i AWS KMS dettagli quando scegli di utilizzare la crittografia lato client per crittografare nuovamente i file quando li salvi in un bucket Amazon S3.

- `WICKRIO_KMS_MSTRKEY_ARN`— L'Amazon Resource Name (ARN) della chiave AWS KMS master utilizzata per crittografare nuovamente i file e i file dei messaggi sul bot di conservazione dei dati prima che vengano salvati nel bucket Amazon S3.
- `WICKRIO_KMS_REGION`— La AWS regione in cui si trova la chiave master. AWS KMS

Utilizza la seguente variabile di ambiente per specificare i dettagli di Amazon SNS quando scegli di inviare eventi di conservazione dei dati a un argomento Amazon SNS. Gli eventi inviati includono l'avvio, lo spegnimento e le condizioni di errore.

- `WICKRIO_SNS_TOPIC_ARN`— L'ARN dell'argomento Amazon SNS a cui desideri inviare gli eventi di conservazione dei dati.

Utilizza la seguente variabile di ambiente a cui inviare i parametri di conservazione dei dati. CloudWatch Se specificato, le metriche verranno generate ogni 60 secondi.

- `WICKRIO_METRICS_TYPE`— Imposta il valore di questa variabile di ambiente su cui `cloudwatch` inviare le metriche. CloudWatch

I valori di Secrets Manager

È possibile utilizzare Secrets Manager per archiviare le credenziali del bot di conservazione dei dati e le informazioni sul AWS servizio. Per ulteriori informazioni sulla creazione di un segreto di Secrets Manager, consulta Creare un AWS Secrets Manager segreto nella Guida per l'utente di Secrets Manager.

Il segreto di Secrets Manager può avere i seguenti valori:

- `password`— La password del bot di conservazione dei dati.
- `s3_bucket_name`— Il nome del bucket Amazon S3 in cui verranno archiviati messaggi e file. Se non è impostato, verrà utilizzato lo streaming di file predefinito.
- `s3_region`— La AWS regione del bucket Amazon S3 in cui verranno archiviati messaggi e file.
- `s3_folder_name`— Il nome della cartella opzionale nel bucket Amazon S3 in cui verranno archiviati messaggi e file. Il nome di questa cartella sarà preceduto dalla chiave per i messaggi e i file salvati nel bucket Amazon S3.
- `kms_master_key_arn`— L'ARN della chiave AWS KMS master utilizzata per crittografare nuovamente i file dei messaggi e i file sul bot di conservazione dei dati prima che vengano salvati nel bucket Amazon S3.
- `kms_region`— La AWS regione in cui si trova la chiave master. AWS KMS
- `sns_topic_arn`— L'ARN dell'argomento Amazon SNS a cui desideri inviare gli eventi di conservazione dei dati.

Politica IAM di utilizzare la conservazione dei dati con i servizi AWS

Se prevedi di utilizzare altri AWS servizi con il bot di conservazione dei dati di Wickr, devi assicurarti che l'host abbia il ruolo e la policy AWS Identity and Access Management (IAM) appropriati per accedervi. Puoi configurare il bot di conservazione dei dati per utilizzare Secrets Manager, Amazon S3 CloudWatch, Amazon SNS e. AWS KMS La seguente policy IAM consente l'accesso ad azioni specifiche per questi servizi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Puoi creare una policy IAM più rigorosa identificando gli oggetti specifici per ogni servizio a cui desideri consentire l'accesso ai contenitori del tuo host. Rimuovi le azioni per i AWS servizi che non intendi utilizzare. Ad esempio, se intendi utilizzare solo un bucket Amazon S3, utilizza la seguente politica, che rimuove `secretsmanager:GetSecretValue` le azioni, `sns:Publishkms:GenerateDataKey`, e. `cloudwatch:PutMetricData`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Se utilizzi un'istanza Amazon Elastic Compute Cloud (Amazon EC2) per ospitare il tuo bot di conservazione dei dati, crea un ruolo IAM utilizzando il case comune di Amazon EC2 e assegna una policy utilizzando la definizione di policy riportata sopra.

Avvia il bot di conservazione dei dati

Prima di eseguire il bot di conservazione dei dati, è necessario determinare come configurarlo. Se prevedi di eseguire il bot su un host che:

- Non avrai accesso ai AWS servizi, quindi le tue opzioni sono limitate. In tal caso utilizzerai le opzioni di streaming dei messaggi predefinite. È necessario decidere se limitare la dimensione

dei file dei messaggi acquisiti a una dimensione o a un intervallo di tempo specifici. Per ulteriori informazioni, consulta Variabili di ambiente.

- Avrai accesso ai AWS servizi, quindi dovresti creare un segreto di Secrets Manager per archiviare le credenziali del bot e i dettagli di configurazione AWS del servizio. Dopo aver configurato i AWS servizi, è possibile procedere all'avvio dell'immagine Docker del bot di conservazione dei dati. Per ulteriori informazioni sui dettagli che è possibile memorizzare in un segreto di Secrets Manager, vedere I valori di Secrets Manager

Le sezioni seguenti mostrano alcuni comandi per eseguire l'immagine Docker del bot di conservazione dei dati. In ciascuno dei comandi di esempio, sostituisci i seguenti valori di esempio con i tuoi:

- *compliance_1234567890_bot*con il nome del tuo bot di conservazione dei dati.
- *password*con la password per il bot di conservazione dei dati.
- *wickr/data/retention/bot*con il nome del segreto di Secrets Manager da utilizzare con il bot di conservazione dei dati.
- *bucket-name*con il nome del bucket Amazon S3 in cui verranno archiviati messaggi e file.
- *folder-name*con il nome della cartella nel bucket Amazon S3 in cui verranno archiviati messaggi e file.
- *us-east-1*con la AWS regione della risorsa che stai specificando. Ad esempio, la regione della chiave AWS KMS master o la regione del bucket Amazon S3.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*con l'Amazon Resource Name (ARN) della tua chiave AWS KMS master da utilizzare per crittografare nuovamente i file e i file dei messaggi.

Avvia il bot con una variabile di ambiente basata sulla password (nessun servizio) AWS

Il seguente comando Docker avvia il bot di conservazione dei dati. La password viene specificata utilizzando la variabile di `WICKRIO_BOT_PASSWORD` ambiente. Il bot inizia a utilizzare lo streaming di file predefinito e a utilizzare i valori predefiniti nella Variabili di ambiente sezione di questa guida.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
wickr/bot-compliance-cloud:latest
```

Avvia il bot richiedendo la password (nessun AWS servizio)

Il seguente comando Docker avvia il bot di conservazione dei dati. La password viene inserita quando richiesta dal bot di conservazione dei dati. Inizierà a utilizzare lo streaming di file predefinito utilizzando i valori predefiniti definiti nella Variabili di ambiente sezione di questa guida.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest

docker attach compliance_1234567890_bot
.
.
.
Enter the password:************
Re-enter the password:************
```

Esegui il bot utilizzando l'`-ti`opzione per ricevere la richiesta della password. È inoltre necessario eseguire il `docker attach` *<container ID or container name>* comando immediatamente dopo aver avviato l'immagine docker in modo da ottenere la richiesta della password. È necessario eseguire entrambi questi comandi in uno script. Se lo alleghi all'immagine docker e non vedi il prompt, premi Invio e vedrai il prompt.

Avvia il bot con una rotazione dei file di messaggi di 15 minuti (nessun servizio) AWS

Il seguente comando Docker avvia il bot di conservazione dei dati utilizzando variabili di ambiente. Inoltre lo configura per ruotare i file dei messaggi ricevuti a 15 minuti.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=15 \
wickr/bot-compliance-cloud:latest
```

Avvia il bot e specifica la password iniziale con Secrets Manager

È possibile utilizzare Secrets Manager per identificare la password del bot di conservazione dei dati. Quando avvii il bot di conservazione dei dati, dovrai impostare una variabile di ambiente che specifichi il Secrets Manager in cui sono archiviate queste informazioni.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

Il `wickrpro/compliance/compliance_1234567890_bot` segreto contiene il seguente valore segreto, visualizzato come testo non crittografato.

```
{
    "password":"password"
}
```

Avvia il bot e configura Amazon S3 con Secrets Manager

Puoi utilizzare Secrets Manager per ospitare le credenziali e le informazioni sul bucket Amazon S3. Quando avvii il bot di conservazione dei dati, dovrai impostare una variabile di ambiente che specifichi il Secrets Manager in cui sono archiviate queste informazioni.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

Il `wickrpro/compliance/compliance_1234567890_bot` segreto contiene il seguente valore segreto, visualizzato come testo non crittografato.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

I messaggi e i file ricevuti dal bot verranno inseriti nel `bot-compliance` bucket nella cartella denominata. `network1234567890`

Avvia il bot e configura Amazon S3 e AWS KMS con Secrets Manager

Puoi utilizzare Secrets Manager per ospitare le credenziali, il bucket Amazon S3 AWS KMS e le informazioni sulla chiave principale. Quando avvii il bot di conservazione dei dati, dovrai impostare una variabile di ambiente che specifichi il Secrets Manager in cui sono archiviate queste informazioni.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

Il `wickrpro/compliance/compliance_1234567890_bot` segreto contiene il seguente valore segreto, visualizzato come testo non crittografato.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab",
    "kms_region":"us-east-1"
}
```

I messaggi e i file ricevuti dal bot verranno crittografati utilizzando la chiave KMS identificata dal valore ARN, quindi inseriti nel bucket «bot-compliance» nella cartella denominata «network1234567890». Assicurati di avere la configurazione appropriata della politica IAM.

Avvia il bot e configura Amazon S3 utilizzando variabili di ambiente

Se non desideri utilizzare Secrets Manager per ospitare le credenziali del bot di conservazione dei dati, puoi avviare l'immagine Docker del bot di conservazione dei dati con le seguenti variabili di ambiente. È necessario identificare il nome del bot di conservazione dei dati utilizzando la variabile di `WICKRIO_BOT_NAME` ambiente.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bucket-name' \
```

```
-e WICKRIO_S3_FOLDER_NAME='folder-name' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

Puoi utilizzare i valori di ambiente per identificare le credenziali del bot di conservazione dei dati, le informazioni sui bucket Amazon S3 e le informazioni di configurazione per lo streaming di file predefinito.

Interrompi il bot di conservazione dei dati

Il software in esecuzione sul bot di conservazione dei dati acquisirà i `SIGTERM` segnali e si spegnerà correttamente. Utilizzate il `docker stop` *`<container ID or container name>`* comando, come mostrato nell'esempio seguente, per inviare il `SIGTERM` comando all'immagine Docker del bot di conservazione dei dati.

```
docker stop compliance_1234567890_bot
```

Ottieni i registri di conservazione dei dati

Il software in esecuzione sull'immagine Docker del bot di conservazione dei dati verrà emesso nei file di registro nella directory. `/tmp/`*`<botname>`*`/logs` Ruoteranno fino a un massimo di 5 file. È possibile ottenere i log eseguendo il seguente comando.

```
docker logs <botname>
```

Esempio:

```
docker logs compliance_1234567890_bot
```

Metriche ed eventi di conservazione dei dati

Di seguito sono riportate le metriche di Amazon CloudWatch (CloudWatch) e gli eventi di Amazon Simple Notification Service (AmazonSNS) attualmente supportati dalla versione 5.116 del bot di conservazione dei dati di AWS Wickr.

Argomenti

- CloudWatch metriche
- SNSEventi Amazon

CloudWatch metriche

Le metriche vengono generate dal bot a intervalli di 1 minuto e trasmesse al CloudWatch servizio associato all'account su cui è in esecuzione l'immagine Docker del bot di conservazione dei dati.

Di seguito sono riportate le metriche esistenti supportate dal bot di conservazione dei dati.

Parametro	Descrizione
Messaggi_Rx	Messaggi ricevuti.
Messaggi_Rx_Failed	Errori nell'elaborazione dei messaggi ricevuti.
Messaggi salvati	Messaggi salvati nel file dei messaggi ricevuti.
Messaggi salvati non riusciti	Errore nel salvataggio dei messaggi nel file dei messaggi ricevuti.
File_salvati	File ricevuti.
Files_Saved_Bytes	Numero di byte per i file ricevuti.
File_salvato_fallito	Errore nel salvataggio dei file.
Accessi	Login (normalmente questo sarà 1 per ogni intervallo).
Errori di accesso	Errori di accesso (normalmente questo sarà 1 per ogni intervallo).
Errori S3_Post	Errori durante la pubblicazione di file e file di messaggi nel bucket Amazon S3.
Watchdog_Failures	Guasti di Watchdog.
Watchdog_Warnings	Avvertenze Watchdog.

Le metriche vengono generate per essere utilizzate da. CloudWatch Lo spazio dei nomi utilizzato per i bot è. `WickrIO` Ogni metrica ha una serie di dimensioni. Di seguito è riportato l'elenco delle dimensioni pubblicate con le metriche precedenti.

Dimensione	Valore
Id	Il nome utente del bot.
Dispositivo	Descrizione di uno specifico dispositivo o istanza del bot. Utile se utilizzi più dispositivi o istanze bot.
Product	Il prodotto per il bot. Può essere `WickrPro_` o `WickrEnterprise_` con `AlphaBeta`, o `Production` aggiunto.
BotType	Il tipo di bot. Etichettato come Conformità per i bot di conformità.
Rete	L'ID della rete associata.

SNSEventi Amazon

I seguenti eventi vengono pubblicati SNS sull'argomento Amazon definito dal valore Amazon Resource Name (ARN) identificato utilizzando la variabile di `WICKRIO_SNS_TOPIC_ARN` ambiente o il valore segreto di `sns_topic_arn` Secrets Manager. Per ulteriori informazioni, consulta Variabili di ambiente e I valori di Secrets Manager.

Gli eventi generati dal bot di conservazione dei dati vengono inviati come JSON stringhe. I seguenti valori sono inclusi negli eventi a partire dalla versione 5.116 del bot di conservazione dei dati.

Nome	Valore
complianceBot	Il nome utente del bot di conservazione dei dati.
dataTime	La data e l'ora in cui si è verificato l'evento.
dispositivo	Una descrizione del dispositivo o dell'istanza bot specifici. Utile se si eseguono più istanze di bot.
dockerImage	L'immagine Docker associata al bot.

Nome	Valore
dockerTag	Il tag o la versione dell'immagine Docker.
message	Il messaggio dell'evento. Per ulteriori informazioni, consulta Eventi critici e Eventi normali.
notificationType	Questo valore saràBot Event.
severity	La gravità dell'evento. Può essere normal o critical.

Devi iscriverti all'SNSargomento Amazon per poter ricevere gli eventi. Se ti iscrivi utilizzando un indirizzo e-mail, ti verrà inviata un'e-mail contenente informazioni simili all'esempio seguente.

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "wickr/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

Eventi critici

Questi eventi causeranno l'arresto o il riavvio del bot. Il numero di riavvii è limitato per evitare di causare altri problemi.

Errori di accesso

Di seguito sono riportati i possibili eventi che possono essere generati quando il bot non riesce ad accedere. Ogni messaggio indicherà il motivo dell'errore di accesso.

Tipo di evento	Messaggio di evento
accesso fallito	Credenziali errate. Controlla la password.

Tipo di evento	Messaggio di evento
accesso fallito	Utente non trovato.
accesso non riuscito	L'account o il dispositivo è sospeso.
provisioning	L'utente è uscito dal comando.
provisioning	Password errata per il `config.wickr` file.
provisioning	Impossibile leggere il `config.wickr` file.
accesso non riuscito	Tutti gli accessi non sono riusciti.
accesso non riuscito	Nuovo utente ma il database esiste già.

Eventi più critici

Tipo di evento	Messaggi di eventi
Account sospeso	W ickrIOClient Main:: slotAdminUser Sospendi: codice (%1): motivo: %2»
BotDevice Sospeso	Il dispositivo è sospeso!
WatchDog	Il SwitchBoard sistema è inattivo per più di <*N*Il sistema è inattivo per più di minuti
Guasti S3	Impossibile inserire il file <*`file-name`* ≫ sul bucket S3. Errore: <*`AWS-error`* >
Chiave di fallback	SERVERSUBMIITEDFALLBACKKEY: non è una chiave di fallback attiva dal client riconosci uta. Invia i log a Desktop Engineering.

Eventi normali

Di seguito sono riportati gli eventi che avvisano l'utente del normale funzionamento. Troppe ricorrenze di questo tipo di eventi in un determinato periodo di tempo possono essere motivo di preoccupazione.

Dispositivo aggiunto all'account

Questo evento viene generato quando un nuovo dispositivo viene aggiunto all'account del bot di conservazione dei dati. In alcune circostanze, questa può essere un'indicazione importante del fatto che qualcuno ha creato un'istanza del bot di conservazione dei dati. Di seguito è riportato il messaggio relativo a questo evento.

```
A device has been added to this account!
```

Non ha effettuato l'accesso

Questo evento viene generato quando il bot ha effettuato correttamente l'accesso. Di seguito è riportato il messaggio relativo a questo evento.

```
Logged in
```

Arresto

Questo evento viene generato quando il bot si spegne. Se l'utente non l'ha avviato in modo esplicito, potrebbe essere un'indicazione di un problema. Di seguito è riportato il messaggio relativo a questo evento.

```
Shutting down
```

Aggiornamenti disponibili

Questo evento viene generato all'avvio del bot di conservazione dei dati e indica che è disponibile una versione più recente dell'immagine Docker associata. Questo evento viene generato all'avvio del bot e su base giornaliera. Questo evento include il campo `versions` array che identifica le nuove versioni disponibili. Di seguito è riportato un esempio di come si presenta questo evento.

```
{
```

```
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
  "dockerImage": "wickr/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```


Che cos'è ATAK?

L'Android Team Awareness Kit (ATAK), o Android Tactical Assault Kit (anche ATAK) per uso militare, è un'infrastruttura geospaziale per smartphone e un'applicazione di consapevolezza della situazione che consente una collaborazione sicura sulla geografia. Sebbene sia stato inizialmente progettato per l'uso nelle zone di combattimento, ATAK è stato adattato per adattarsi alle missioni delle agenzie locali, statali e federali.

Argomenti

- Abilita ATAK nella dashboard di Wickr Network
- Informazioni aggiuntive su ATAK
- Installa e associa il plugin Wickr per ATAK
- Componi e ricevi una chiamata
- Inviare un file
- Invia un messaggio vocale sicuro (Push-to-talk)
- Girandola (accesso rapido)
- Navigazione

Abilita ATAK nella dashboard di Wickr Network

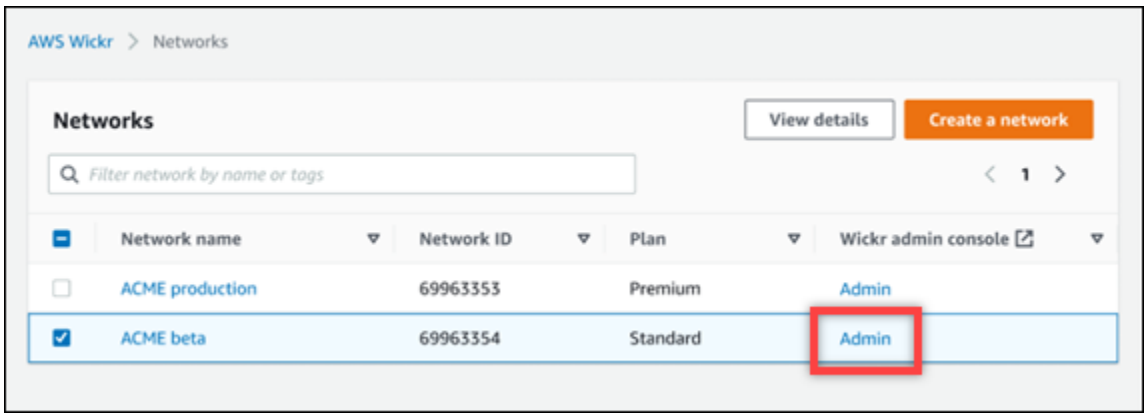
AWS Wickr supporta molte agenzie che utilizzano Android Tactical Assault Kit (ATAK). Tuttavia, fino ad ora, gli operatori ATAK che utilizzano Wickr hanno dovuto abbandonare l'applicazione per farlo. Per contribuire a ridurre le interruzioni e i rischi operativi, Wickr ha sviluppato un plug-in che migliora

ATAK con funzionalità di comunicazione sicure. Con il plug-in Wickr per ATAK, gli utenti possono inviare messaggi, collaborare e trasferire file su Wickr all'interno dell'applicazione ATAK. Ciò elimina le interruzioni e la complessità della configurazione con le funzionalità di chat di ATAK.

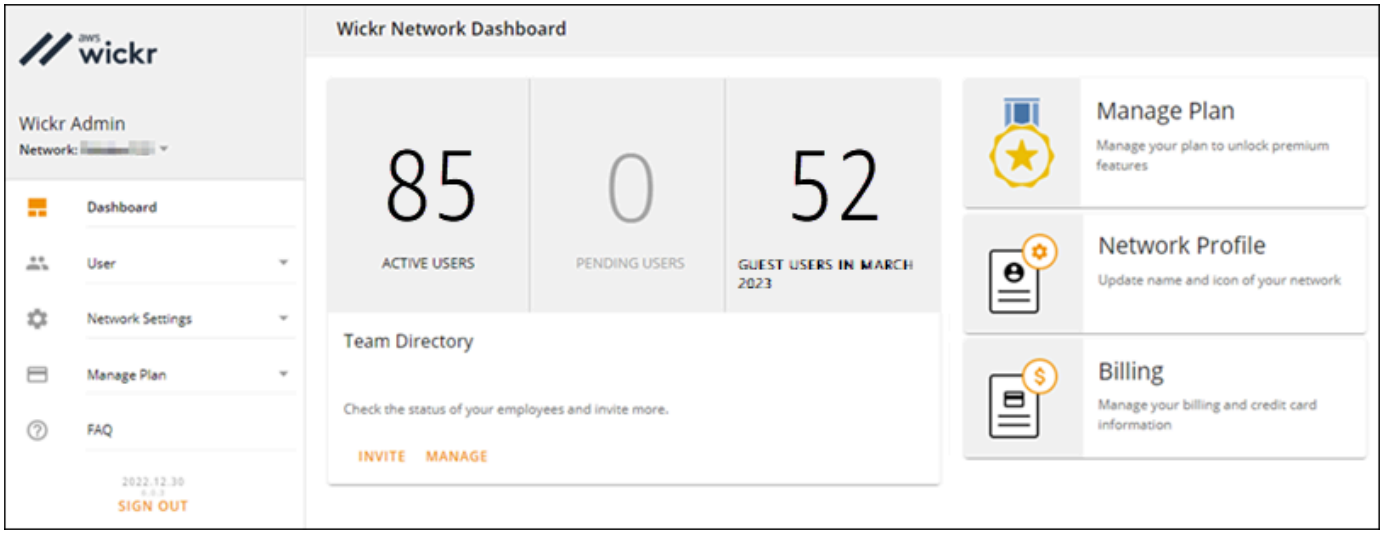
Abilita ATAK nella dashboard di Wickr Network

Completa la seguente procedura per abilitare ATAK nella dashboard di rete Wickr.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.



Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.



3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Gruppo di sicurezza.
4. Scegli Dettagli accanto al gruppo di sicurezza desiderato per il quale desideri abilitare ATAK.

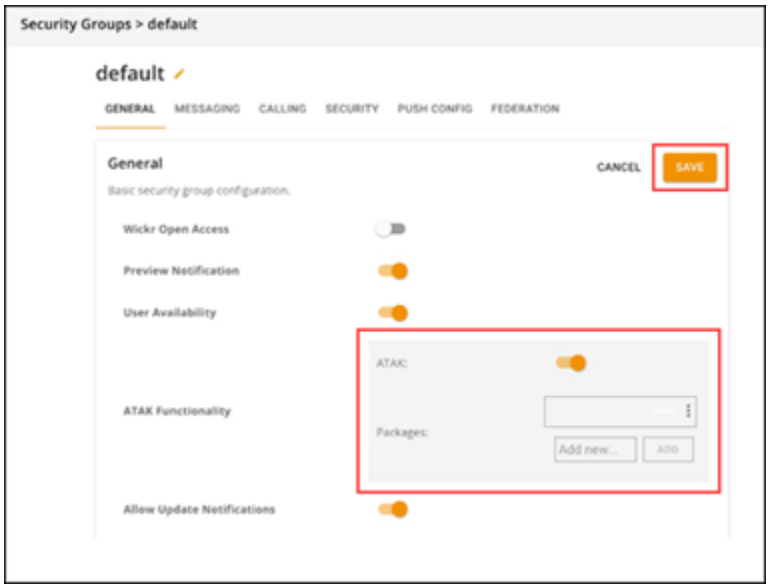
5. Nella scheda General (Generale), seleziona Edit (Modifica).
6. Nella sezione Funzionalità ATAK:

   a. Immettete il nome del pacchetto nella casella di testo Pacchetti. È possibile inserire uno dei seguenti valori a seconda della versione di ATAK che gli utenti installeranno e utilizzeranno:

      - `com.atakmap.app.civ`— Inserisci questo valore nella casella di testo Pacchetti se gli utenti finali di Wickr installeranno e utilizzeranno la versione civile dell'applicazione ATAK sui propri dispositivi Android.
      - `com.atakmap.app.mil`— Inserisci questo valore nella casella di testo Pacchetti se gli utenti finali di Wickr installeranno e utilizzeranno la versione militare dell'applicazione ATAK sui propri dispositivi Android.

   b. Fai scorrere l'interruttore ATAK verso destra per attivare la funzionalità.

   c. Selezionare Salva.



ATAK è ora abilitato per la rete Wickr selezionata e il gruppo di sicurezza selezionato. Dovresti chiedere agli utenti Android del gruppo di sicurezza per il quale hai abilitato la funzionalità ATAK di installare il plugin Wickr per ATAK. Per ulteriori informazioni, consulta Installare e associare il plugin Wickr ATAK.

Informazioni aggiuntive su ATAK

Per ulteriori informazioni sul plugin Wickr per ATAK, consulta quanto segue:

- Panoramica del plugin Wickr ATAK

- Informazioni aggiuntive sul plugin Wickr ATAK

Installa e associa il plugin Wickr per ATAK

L'Android Team Awareness Kit (ATAK) è una soluzione Android utilizzata dalle agenzie militari, statali e governative statunitensi che richiedono funzionalità di consapevolezza situazionale per la pianificazione, l'esecuzione e la risposta agli incidenti delle missioni. ATAK ha un'architettura a plugin che consente agli sviluppatori di aggiungere funzionalità. Consente agli utenti di navigare utilizzando il GPS e i dati delle mappe geospaziali sovrapposti alla consapevolezza della situazione in tempo reale degli eventi in corso. In questo documento, vi mostriamo come installare il plugin Wickr per ATAK su un dispositivo Android e associarlo al client Wickr. Ciò consente di inviare messaggi e collaborare su Wickr senza uscire dall'applicazione ATAK.

Installa il plugin Wickr per ATAK

Completa la seguente procedura per installare il plugin Wickr per ATAK su un dispositivo Android.

1. Vai al Google Play Store e installa il plug-in Wickr for ATAK.
2. Apri l'applicazione ATAK sul tuo dispositivo Android.
3. Nell'applicazione ATAK, scegli l'icona del menu
   ( )
   in alto a destra dello schermo, quindi scegli Plugin.
4. Seleziona Importa.
5. Nel pop-up Seleziona il tipo di importazione, scegli Local SD e vai al punto in cui hai salvato il plugin Wickr per il file.apk ATAK.
6. Scegli il file del plugin e segui le istruzioni per installarlo.

   > **Note**
   >
   > Se ti viene chiesto di inviare il file del plug-in per la scansione, scegli No.

7. L'applicazione ATAK ti chiederà se desideri caricare il plugin. Scegli OK.

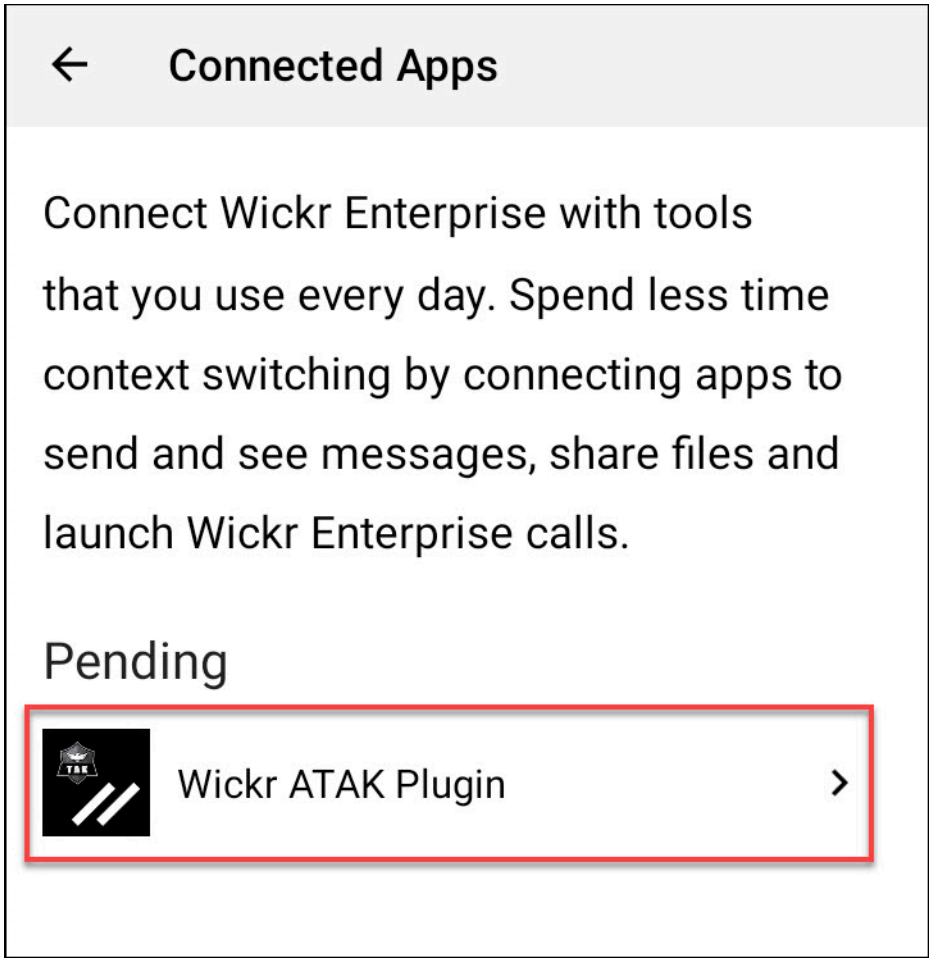
Il plugin Wickr per ATAK è ora installato. Continua con la seguente sezione Associa ATAK a Wickr per completare il processo.

Associa ATAK a Wickr

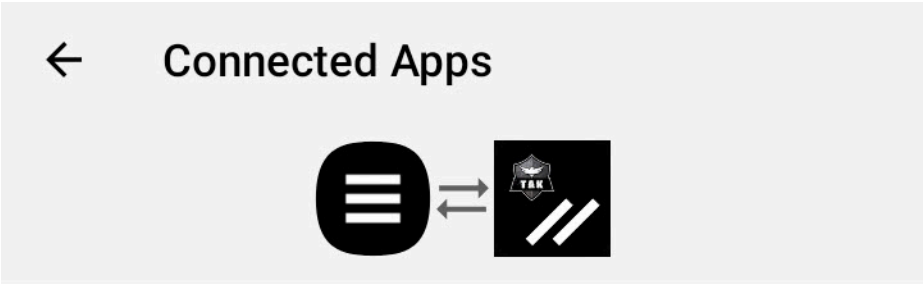
Completa la seguente procedura per associare l'applicazione ATAK a Wickr dopo aver installato con successo il plugin Wickr per ATAK.

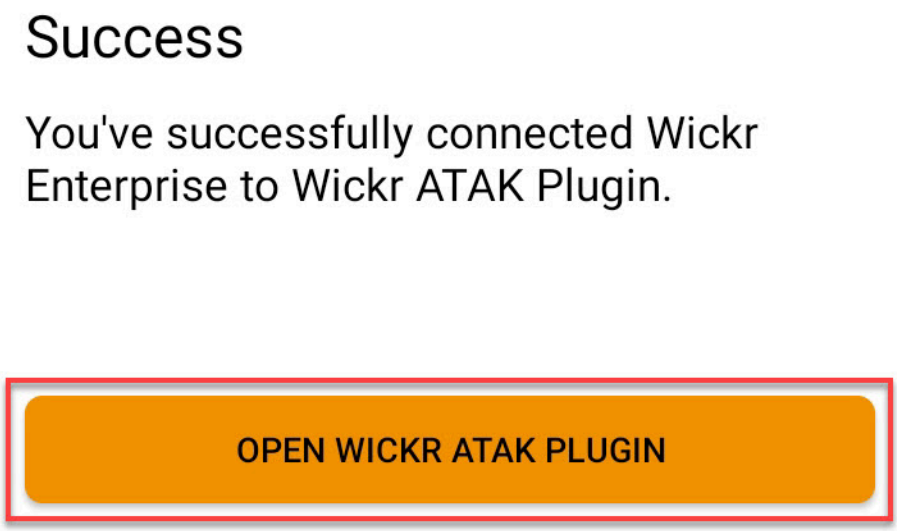
1. Nell'applicazione ATAK, scegliete l'icona del menu () in alto a destra dello schermo, quindi scegliete Wickr Plugin.
2. Scegliete Pair Wickr.

   Apparirà una richiesta di notifica che ti chiederà di rivedere le autorizzazioni per il plugin Wickr per ATAK. Se la richiesta di notifica non viene visualizzata, apri il client Wickr e vai su Impostazioni, quindi su App connesse. Dovresti vedere il plugin nella sezione In sospeso dello schermo.



3. Scegli Approva per accoppiare.
4. Scegli il pulsante Open Wickr ATAK Plugin per tornare all'applicazione ATAK.



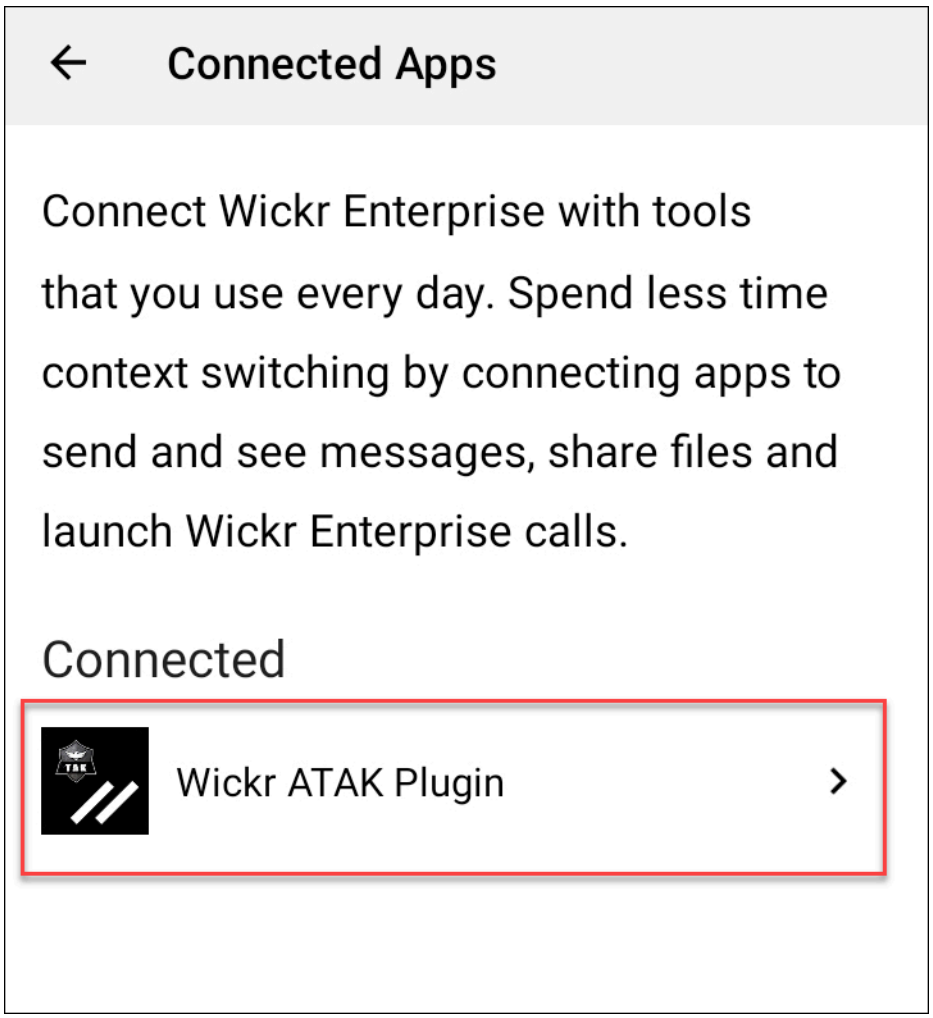


Ora hai abbinato correttamente il plug-in ATAK e Wickr e puoi utilizzare il plug-in per inviare messaggi e collaborare utilizzando Wickr senza uscire dall'applicazione ATAK.

Annulla l'associazione tra ATAK e Wickr

Completa la seguente procedura per annullare l'associazione del plugin ATAK con Wickr.

1. Nell'app nativa, scegli Impostazioni, quindi scegli App connesse.
2. Nella schermata App connesse, scegli Wickr ATAK Plugin.



3. Nella schermata del plugin Wickr ATAK, scegli Rimuovi nella parte inferiore dello schermo.

   Viene visualizzata una schermata di conferma che non stai più utilizzando l'API. Ora hai disaccoppiato con successo il plugin ATAK.

Componi e ricevi una chiamata

È possibile comporre e ricevere una chiamata nel plug-in Wickr per ATAK.

Completate la seguente procedura per chiamare e ricevere una chiamata.

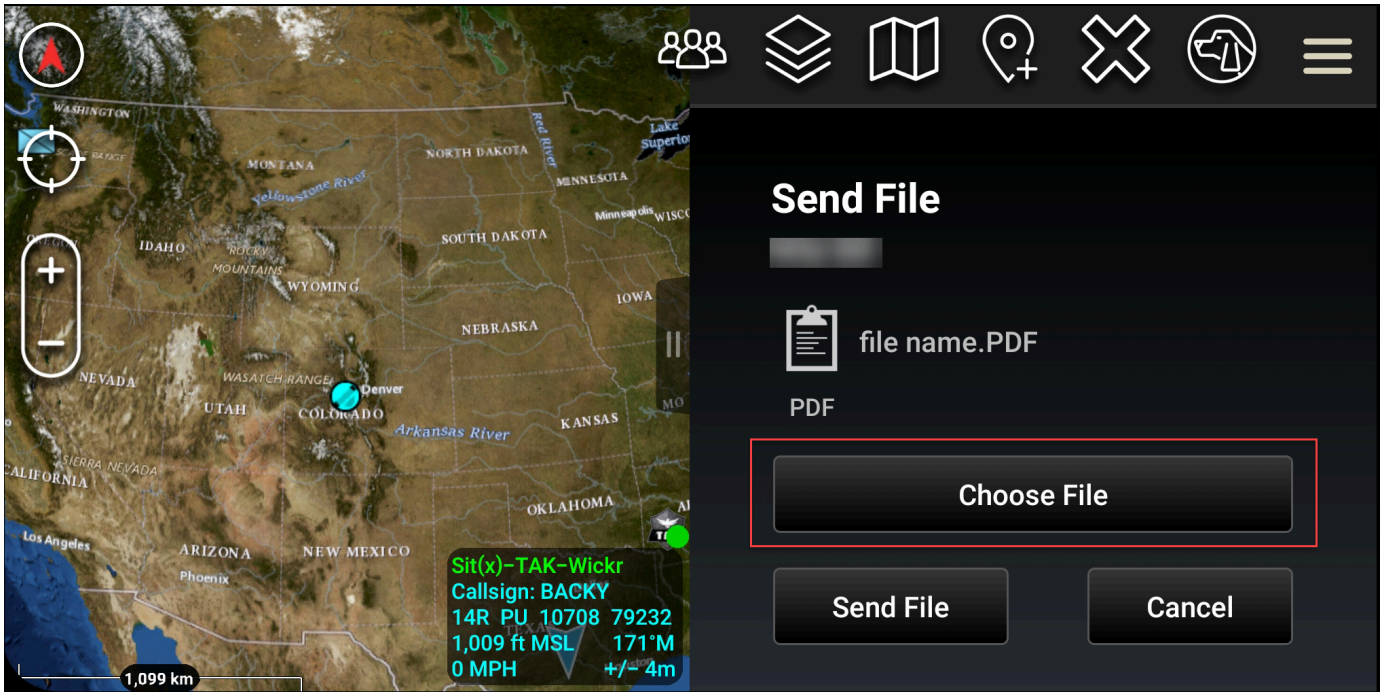
1. Apri una finestra di chat.
2. Nella visualizzazione Mappa, scegli l'icona dell'utente che desideri chiamare.
3. Scegli l'icona del telefono in alto a destra dello schermo.
4. Una volta connesso, puoi tornare alla visualizzazione del plug-in ATAK e ricevere una chiamata.

Inviare un file

Puoi inviare un file nel plugin Wickr per ATAK.

Completa la seguente procedura per inviare un file.

1. Apri una finestra di chat.
2. Nella visualizzazione Mappa, cerca l'utente a cui desideri inviare un file.
3. Quando trovi l'utente a cui desideri inviare un file, seleziona il suo nome.
4. Nella schermata Invia file, seleziona Scegli file, quindi vai al file che desideri inviare.



5. Nella finestra del browser, scegli il file desiderato.
6. Nella schermata Invia file, scegli Invia file.

   Viene visualizzata l'icona di download, che indica che il file selezionato è in fase di download.

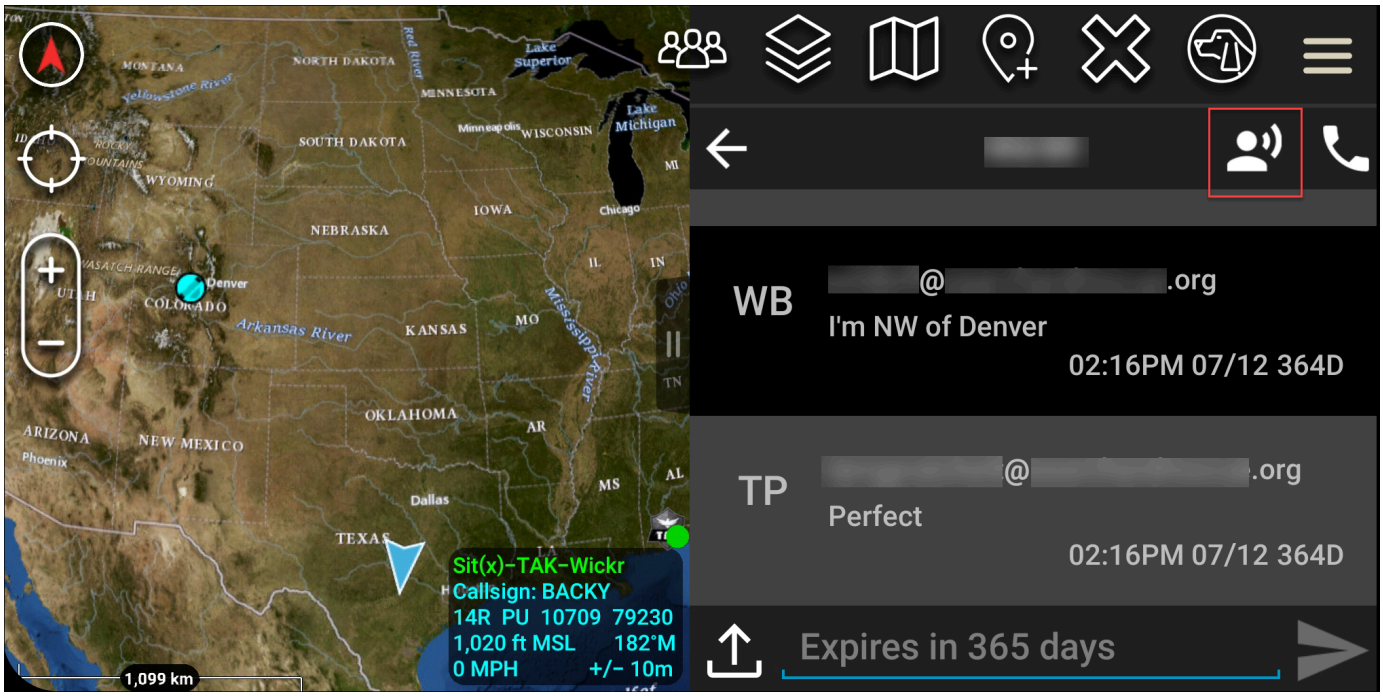
Invia un messaggio vocale sicuro (Push-to-talk)

Puoi inviare un messaggio vocale sicuro (Push-to-talk) nel plugin Wickr per ATAK.

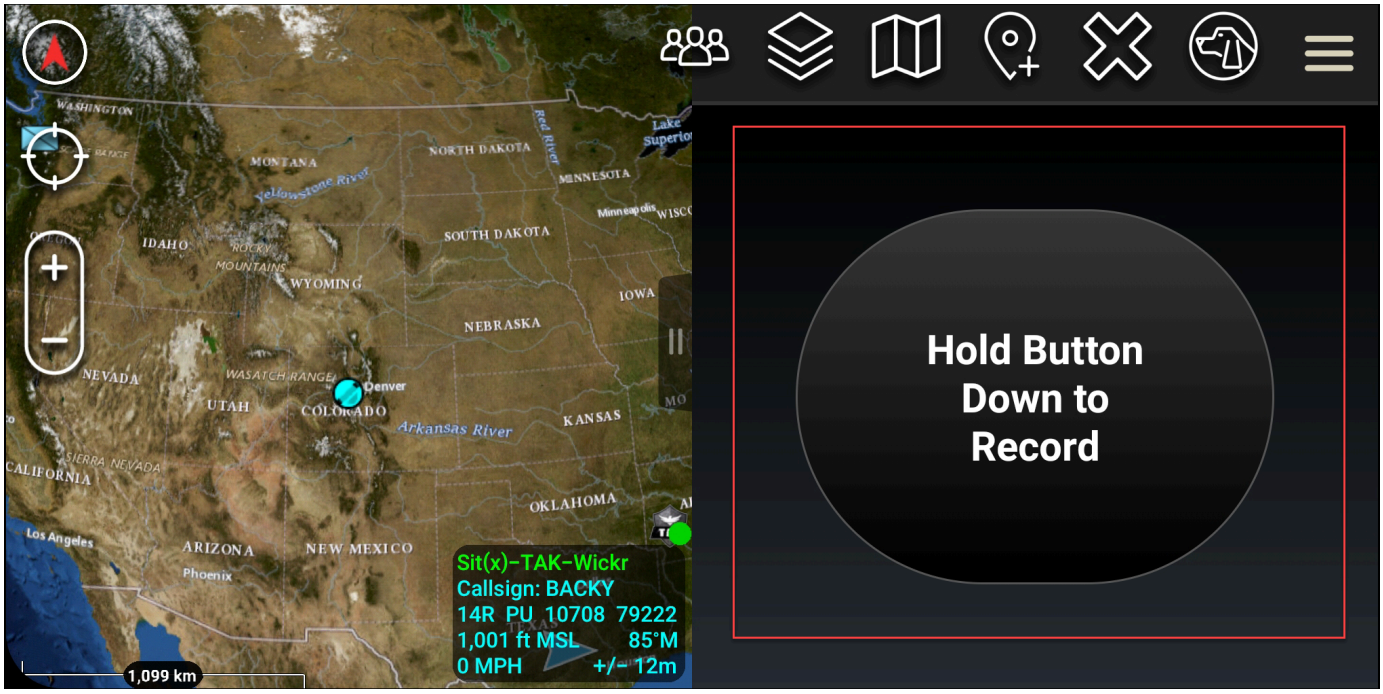
Completa la seguente procedura per inviare un messaggio vocale sicuro.

1. Apri una finestra di chat.

2. Scegli l'icona Push-to-Talk nella parte superiore dello schermo, indicata dall'icona di una persona che parla.



3. Seleziona e tieni premuto il pulsante Tieni premuto il pulsante per registrare.



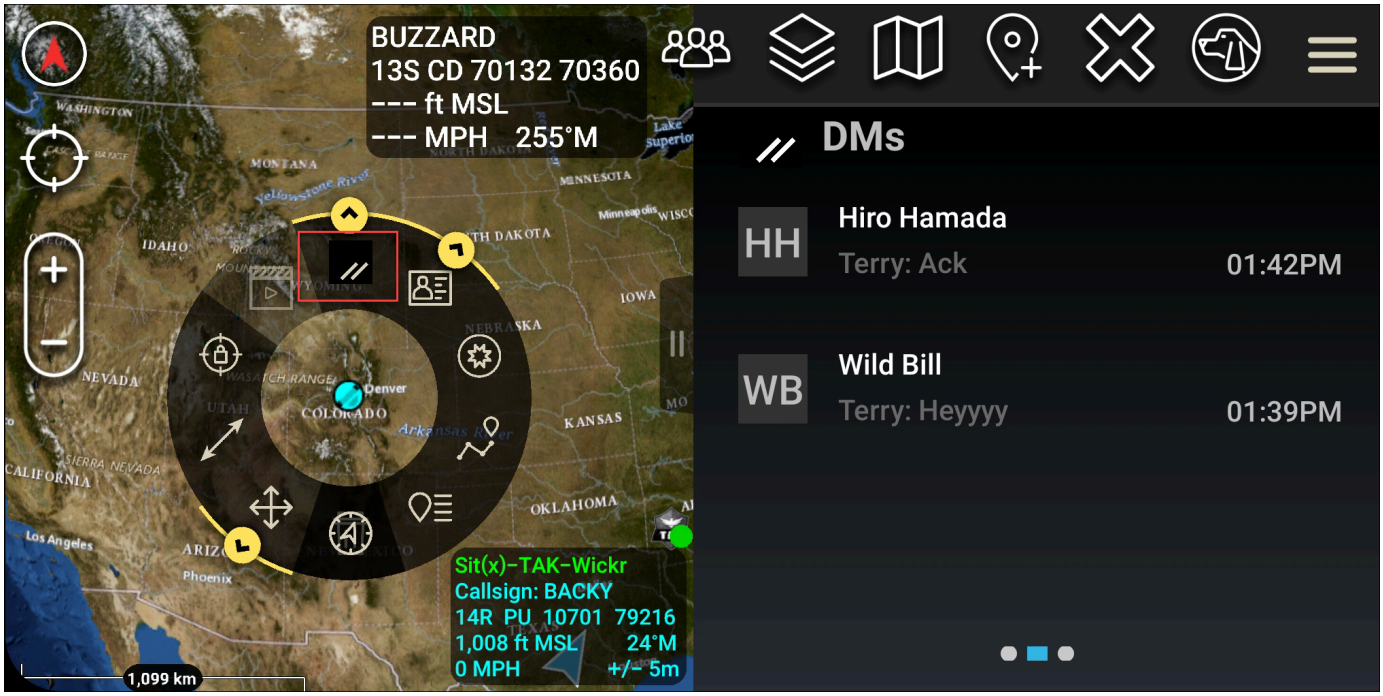
4. Registra il tuo messaggio.
5. Dopo aver registrato il messaggio, rilascia il pulsante per inviarlo.

Girandola (accesso rapido)

La girandola o la funzione di accesso rapido viene utilizzata per one-one-one conversazioni o messaggi diretti.

Completare la seguente procedura per utilizzare la girandola.

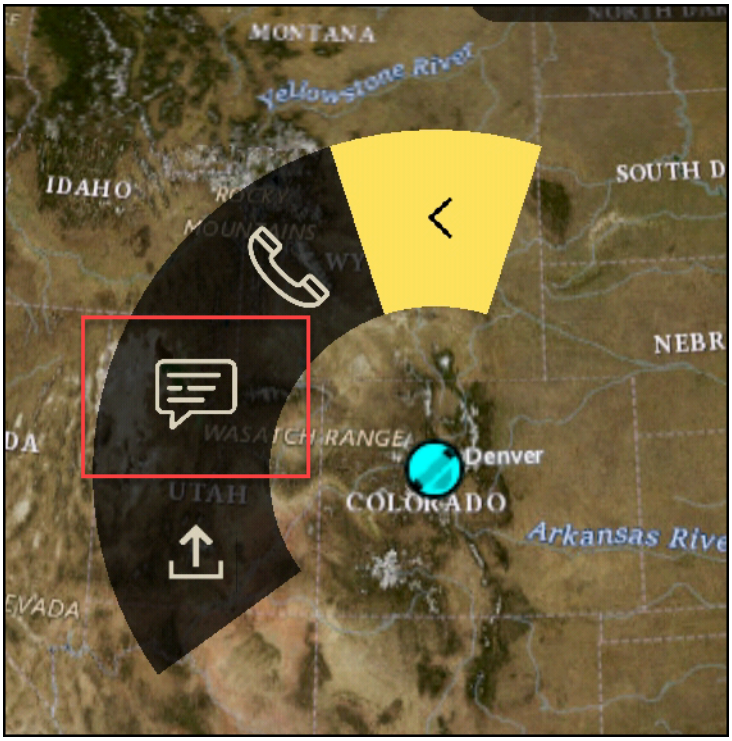
1. Apri contemporaneamente la visualizzazione a schermo diviso della mappa ATAK e del plug-in Wickr for ATAK. La mappa mostra i tuoi compagni di squadra o le tue risorse nella visualizzazione della mappa.
2. Scegli l'icona utente per aprire la girandola.
3. Scegli l'icona Wickr per visualizzare le opzioni disponibili per l'utente selezionato.



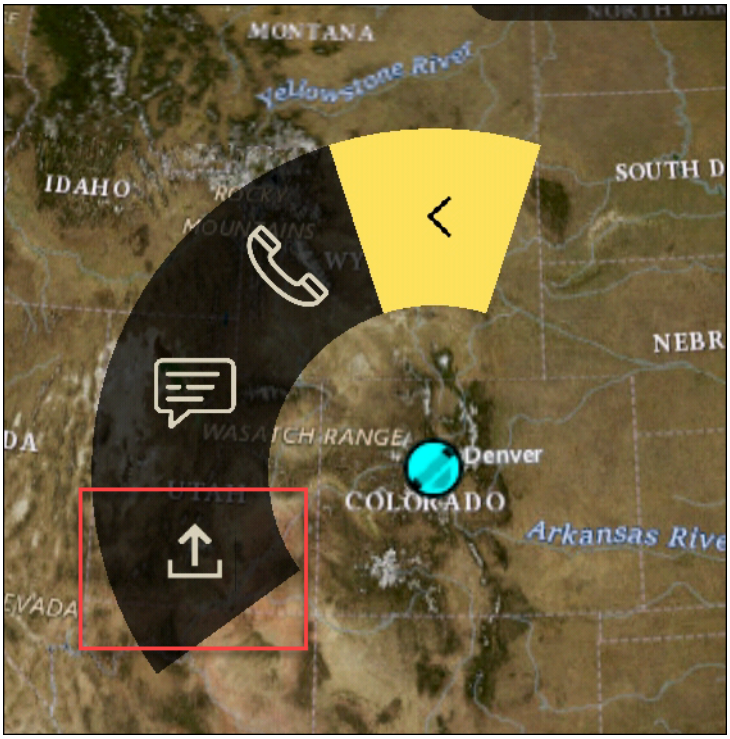
4. Sulla girandola, scegli una delle seguenti icone:

   - Telefono: scegli di chiamare.

- Messaggio: scegli di chattare.



- Invio file: scegli di inviare un file.



Navigazione

L'interfaccia utente del plug-in contiene tre visualizzazioni del plug-in, indicate dalle forme blu e bianche nella parte inferiore destra dello schermo. Scorri verso sinistra e destra per navigare tra le viste.

- Visualizzazione Contatti: crea una conversazione di gruppo o di stanza con messaggi diretti.
- Visualizzazione messaggi diretti: crea una one-to-one conversazione. La funzionalità di chat funziona come nell'app nativa di Wickr. Questa funzionalità ti consente di rimanere nella visualizzazione Mappa e di comunicare con gli altri tramite il plug-in.
- Visualizzazione delle stanze: le stanze esistenti nell'app nativa vengono trasferite. Tutto ciò che viene fatto nel plugin si riflette nell'app nativa di Wickr.

> **Note**
>
> Alcune funzioni, come l'eliminazione di una stanza, possono essere eseguite solo nell'app nativa e di persona per evitare modifiche involontarie da parte degli utenti e interferenze causate dalle apparecchiature sul campo.

Elenco delle porte e dei domini consentiti

Consenti elenca le seguenti porte per garantire il corretto funzionamento di Wickr:

Porte

- TCPporta 443 (per messaggi e allegati)
- UDPporte 16384-16584 (per chiamare)

Domini e indirizzi da inserire nell'elenco dei domini consentiti per regione

Se è necessario consentire l'elenco di tutti i possibili domini di chiamata e gli indirizzi IP del server, consulta il seguente elenco di potenziali per regione. CIDRs Controlla periodicamente questo elenco, poiché è soggetto a modifiche.

> **Note**
>
> Le e-mail di registrazione e verifica vengono inviate da donotreply@wickr.email.

Stati Uniti orientali (Virginia settentrionale)

Domini:	• gw-pro-prod.wickr.com • api.messaging. wickr.us-east-1.amazonaws.com
CIDRindirizzi:	• 44.211.195.0/27 • 44,21383,32/28
Indirizzi IP:	• 44.211.195.0 • 44,211,1951 • 44,211,195,2 • 44,211,195,3 • 44,211,195,4 • 44,211,195,5 • 44,211,195,6

- 44,211,195,7
- 44,211,195,8
- 44,211,195,9
- 44,211,195,10
- 44,211,195,11
- 44,211,195,12
- 44,211,195,13
- 44,211,195,14
- 44,211,195,15
- 44,211,195,16
- 44,211,195,17
- 44,211,195,18
- 44,211,195,19
- 44,211,195,20
- 44,211,195,21
- 44,211,195,22
- 44,211,195,23
- 44,211,195,24
- 44,211,195,25
- 44,211,195,26
- 44,211,195,27
- 44,211,195,28
- 44,211,195,29
- 44,211,195,30
- 44,211,195,31
- 44,213,83,32
- 44,213,83,33
- 44,213,83,34
- 44,213,83,35
- 44,213,83,36

	• 44,213,83,37 • 44,213,83,38 • 44,213,83,39 • 44,213,83,40 • 44,21383,41 • 44,213,83,42 • 44,213,83,43 • 44,213,83,44 • 44,213,83,45 • 44,213,83,46 • 44,213,83,47

Asia Pacifico (Singapore)

Dominio:	• api.messaging. wickr.ap-southeast-1.amazonaws.com
CIDRindirizzi:	• 47.129.23.144/28
Indirizzi IP:	• 47.129.23.144 • 47129,223,145 • 47129,223,146 • 47129,223,147 • 47129,223,148 • 47129,223,149 • 4712923,150 • 47129,223,151 • 47129,223,152 • 47129,223,153 • 47129,223,154 • 47129,223,155 • 4712923,156

	• 4712923,157 • 4712923,158 • 47129,223,159

Asia Pacifico (Sydney)

Dominio:	• api.messaging. wickr.ap-southeast-2.amazonaws.com
CIDRindirizzi:	• 3.27.180.208/28
Indirizzi IP:	• 3.27.180.208 • 3,27,180209 • 3,27,180,210 • 3,27,180,211 • 3,27,180,212 • 3,27,180,213 • 3,27,180,214 • 3,27,180,215 • 3,27,180,216 • 3,27,180,217 • 3,27,180,218 • 3,27,180,219 • 3,27,180220 • 3,27,180221 • 3,27,180222 • 3,27,180223

Asia Pacifico (Tokyo)

Dominio:	• api.messaging. wickr.ap-northeast-1.amazonaws.com

CIDRindirizzi:	• 57.181.142.240/28
Indirizzi IP:	• 57.181.142.240 • 57,181,142241 • 57,181,142242 • 57,181,142243 • 57,181,142244 • 57,181,142,245 • 57,181,142246 • 57,181,142,247 • 57,181,142,248 • 57,181,142,249 • 57,181,142,250 • 57,181,142251 • 57,181,142,252 • 57,181,142,253 • 57,181,142,254 • 57,181,142,255

Canada (Centrale)

Dominio:	• api.messaging. wickr.ca-central-1.amazonaws.com
CIDRindirizzi:	• 15.156.152.96/28
Indirizzi IP:	• 15.156.152.96 • 15,156,152,97 • 15,156,152,98 • 15,156,152,99 • 15,156,152,100 • 15,156,152,101

	• 15,156,152,102 • 15,156,152,103 • 15,156,152,1104 • 15,156,152,105 • 15,156,152,106 • 15,156,152,107 • 15,156,152,108 • 15,156,152109 • 15,156,152110 • 15,156,152,111

Europa (Francoforte)

Dominio:	• api.messaging. wickr.eu-central-1.amazonaws.com
CIDRindirizzi:	• 3.78.252.32/28
Indirizzi IP:	• 3.78.252.32 • 3,78,252,33 • 3,78,252,34 • 3,78,252,35 • 3,78,252,36 • 3,78,252,37 • 3,78,252,38 • 3,78,252,39 • 3,78,252,40 • 3,78,252,41 • 3,78,252,42 • 3,78,252,43 • 3,78,252,44 • 3,78,252,45

	• 3,78,252,46 • 3,78,252,47

Europa (Londra)

Dominio:	• api.messaging. wickr.eu-west-2.amazonaws.com
CIDRindirizzi:	• 13.43.91.48/28
Indirizzi IP:	• 13.43.91.48 • 13,491,49 • 1343,91,50 • 13,491,51 • 13,491,52 • 13,491,53 • 13,491,54 • 1343,91,55 • 1343,91,56 • 13,491,57 • 13,491,58 • 13,491,59 • 1343,91,60 • 13,491,61 • 13,491,62 • 13,491,63

Europa (Stoccolma)

Dominio:	• api.messaging. wickr.eu-north-1.amazonaws.com

CIDRindirizzi:	• 13.60.1.64/28
Indirizzi IP:	• 13.60.1.64 • 13,601,65 • 13,601,66 • 13,601,67 • 13,601,68 • 13,601,69 • 13,601,70 • 13,601,71 • 13,601,72 • 13,601,73 • 13,601,74 • 13,601,75 • 13,601,76 • 13,60,1,77 • 13,601,78 • 13,601,79

Europa (Zurigo)

Dominio:	• api.messaging. wickr.eu-central-2.amazonaws.com
CIDRindirizzi:	• 16.63.106.224/28
Indirizzi IP:	• 16.63.106.224 • 16,6106,225 • 16,6106,226 • 16,6106,227 • 16,6106,228 • 16,6106,229

	• 16,6106,230 • 16,6106,231 • 16,6106,232 • 16,6106,233 • 16,6106,234 • 16,6106,235 • 16,6106,236 • 16,6106,237 • 16,6106,238 • 16,6106,239

AWS GovCloud (Stati Uniti occidentali)

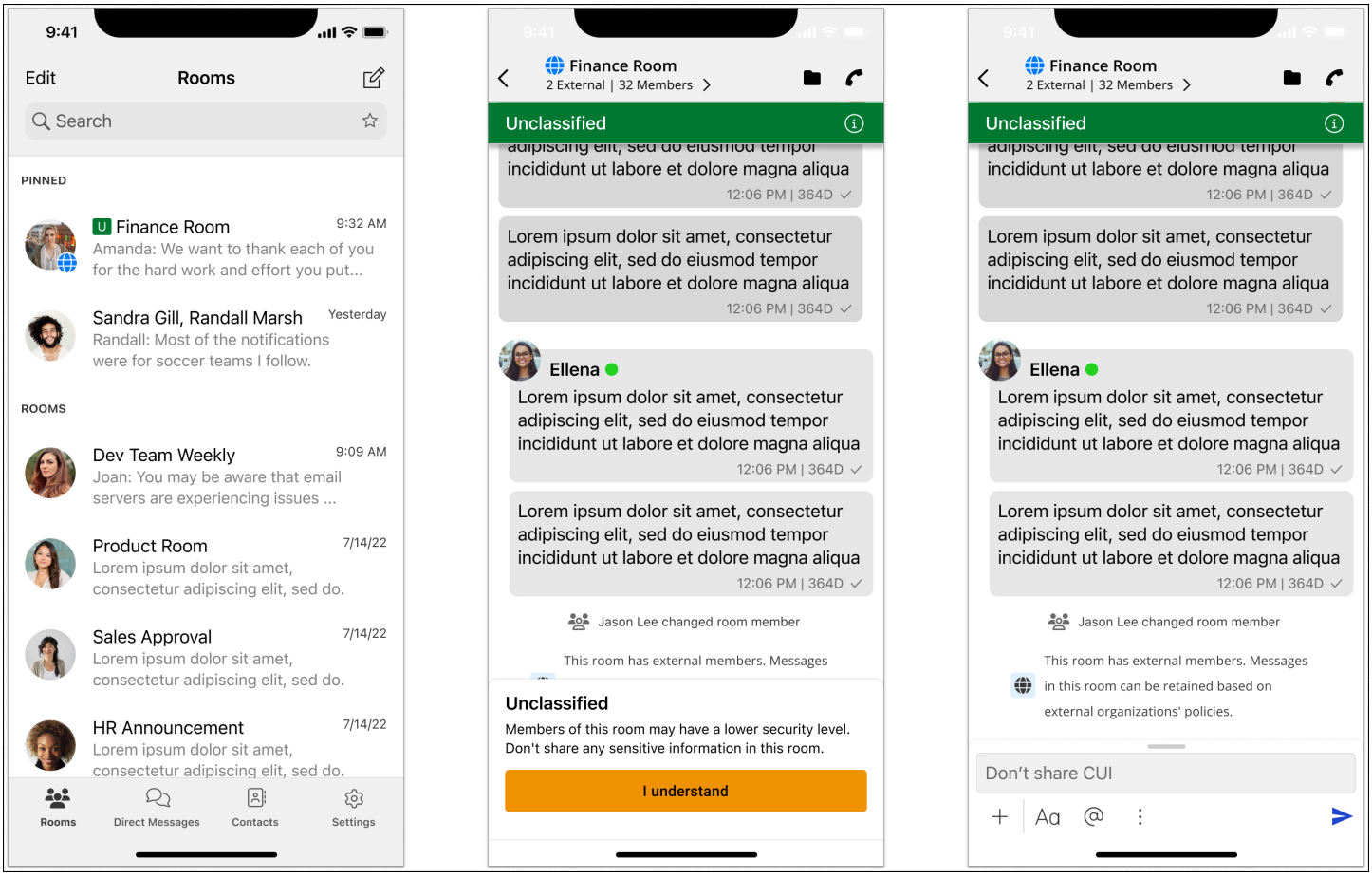
Dominio:	• api.messaging.wickr. us-gov-west-1. amazonaws.com
CIDRindirizzi:	• 3.30.186.208/28
Indirizzi IP:	• 3.30.186.208 • 3,30,186209 • 3,30,186,210 • 3,30,186,211 • 3,30,186,212 • 3,30,186,213 • 3,30,186,214 • 3,30,186,215 • 3,30,186,216 • 3,30,186,217 • 3,30,186,218 • 3,30,186,219 • 3,30,186220 • 3,30,186,221

- 3,30,186,222
- 3,30,186223

GovCloud classificazione e federazione transfrontaliera

AWS Wickr offre WickrGov client personalizzati per gli GovCloud utenti. La GovCloud Federazione consente la comunicazione tra GovCloud utenti e utenti commerciali. La funzionalità di classificazione transfrontaliera consente di modificare l'interfaccia utente alle conversazioni per GovCloud gli utenti. In qualità di GovCloud utente, è necessario attenersi a rigide linee guida relative alla classificazione definita dal governo. Quando GovCloud gli utenti interagiscono con utenti commerciali (Enterprise, AWS Wickr, utenti Guest), vedranno visualizzati i seguenti avvisi non classificati:

- Un tag U nell'elenco delle camere
- Un riconoscimento non classificato nella schermata del messaggio
- Un banner non classificato in cima alla conversazione



> **Note**
>
> Questi avvisi verranno visualizzati solo quando un GovCloud utente sta conversando o fa parte di una stanza con utenti esterni. Scompariranno se gli utenti esterni abbandonano la conversazione. Nelle conversazioni tra GovCloud utenti non verrà visualizzato alcun avviso.

Gestione degli utenti in AWS Wickr

Nella sezione Utenti di AWS Management Console for Wickr puoi visualizzare gli utenti e i bot di Wickr correnti e modificarne i dettagli.

Argomenti

Elenco del team

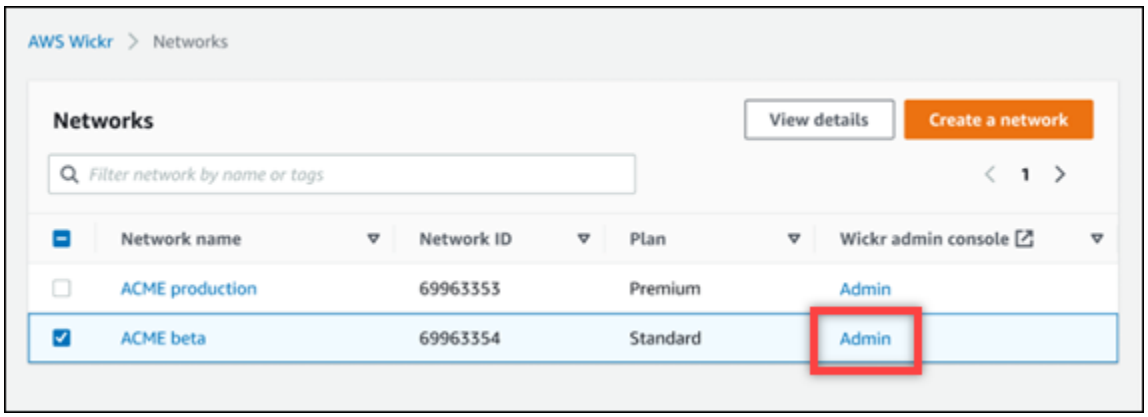
Puoi visualizzare gli attuali utenti di Wickr e modificarne i dettagli nella sezione Utente di AWS Management Console for Wickr.

Argomenti

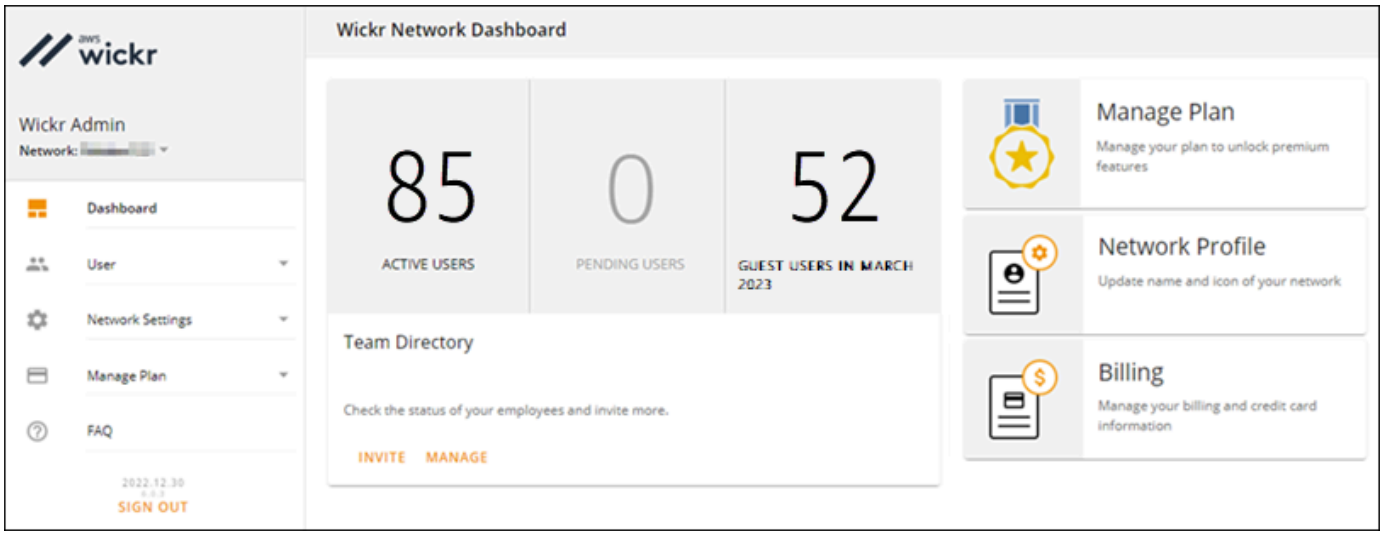
Visualizzazione degli utenti

Completa la seguente procedura per visualizzare gli utenti registrati nella tua rete Wickr.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.



Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.



3. Nel riquadro di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Team Directory.

   La pagina Team Directory mostra gli utenti registrati alla rete Wickr, incluso il nome, l'indirizzo email, il gruppo di sicurezza assegnato e lo stato attuale. Per gli utenti attuali, puoi visualizzare i loro dispositivi, modificarne i dettagli, sospenderli, eliminarli e trasferirli a un'altra rete Wickr.

Creazione di utenti

Completate la seguente procedura per creare un utente.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.

2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.
3. Nel riquadro di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Team Directory.
4. Scegli Crea nuovo utente.
5. Nel modulo visualizzato, inserisci il nome, il cognome, il prefisso internazionale, il numero di telefono e l'indirizzo email dell'utente. L'indirizzo e-mail è l'unico campo obbligatorio. Assicurati di scegliere il gruppo di sicurezza appropriato per l'utente. Wickr invierà un'email di invito all'indirizzo specificato per l'utente.
6. Scegli Crea.

   All'utente viene inviata un'e-mail. L'e-mail fornisce i link per il download delle applicazioni client di Wickr e un link per la registrazione a Wickr. Man mano che gli utenti si registrano a Wickr utilizzando il link contenuto nell'e-mail, il loro stato nella directory del team di Wickr cambierà da In sospeso a Attivo.

Modifica utenti

Completare la procedura seguente per modificare un utente.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.
3. Nel riquadro di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Team Directory.
4. Scegli l'icona con i puntini di sospensione verticali accanto al nome dell'utente che desideri eliminare.
5. Puoi scegliere una delle seguenti opzioni:

   - Dispositivi: visualizza i dispositivi che l'utente ha configurato con il client Wickr.

- Modifica: modifica i dettagli dell'utente, come il nome, il prefisso internazionale, il numero di telefono (opzionale) e il gruppo di sicurezza assegnato.
- Sospendi: sospendi l'utente in modo che non possa accedere alla tua rete Wickr nel client Wickr. Quando sospendi un utente che è attualmente connesso alla tua rete Wickr dal client, quell'utente viene automaticamente disconnesso.
- Elimina: elimina l'utente dalla tua rete Wickr.

Eliminare gli utenti

Completa la seguente procedura per eliminare un utente.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.
3. Nel riquadro di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Team Directory.
4. Scegli l'icona con i puntini di sospensione verticali accanto al nome dell'utente che desideri eliminare.
5. Scegli Elimina per eliminare l'utente.

   Quando elimini un utente, quell'utente non è più in grado di accedere alla tua rete Wickr nel client Wickr.

Eliminazione di utenti in blocco

Puoi eliminare e sospendere in blocco gli utenti della rete Wickr nella sezione Utente della Console di amministrazione di Wickr per Wickr.

> **Note**
>
> L'opzione per l'eliminazione in blocco degli utenti si applica solo quando l'SSO non è abilitato.

Per eliminare in blocco gli utenti della rete Wickr utilizzando un modello CSV, completa la procedura seguente.

1. Apri il file per Wickr all'indirizzo AWS Management Console https://console.aws.amazon.com/wickr/.
2. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Team Directory.

   La pagina Team Directory mostra gli utenti registrati nella tua rete Wickr.
3. Nella pagina Team Directory, scegli Gestisci utenti.
4. Nella finestra pop-up Gestisci utenti, scegli Elimina utenti.
5. Scarica il modello CSV di esempio. Per scaricare il modello di esempio, scegli Scarica modello.
6. Completa il modello aggiungendo l'email degli utenti che desideri eliminare in blocco dalla tua rete.
7. Carica il modello CSV completato. Puoi trascinare il file nella casella di caricamento o selezionare scegli un file.
8. Seleziona la casella di controllo, riconosco che l'eliminazione dell'utente non è reversibile.
9. Scegli Elimina utenti.

> **Note**
>
> Questa azione inizierà immediatamente a eliminare gli utenti e potrebbe richiedere alcuni minuti. Gli utenti eliminati non saranno più in grado di accedere alla rete Wickr nel client Wickr.

Per eliminare in blocco gli utenti della rete Wickr scaricando un file CSV della directory del team, completa la procedura seguente.

1. Apri il file per Wickr all'indirizzo AWS Management Console https://console.aws.amazon.com/wickr/.
2. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Team Directory.

   La pagina Team Directory mostra gli utenti registrati nella tua rete Wickr.
3. Seleziona l'icona di download CSV nell'angolo in alto a destra della pagina Team Directory.

4. Dopo aver scaricato il modello CSV della directory del team, rimuovi le righe degli utenti che non devono essere eliminate.
5. Nella pagina Team Directory, scegli Gestisci utenti.
6. Nella finestra pop-up Gestisci utenti, scegli Elimina utenti.
7. Carica il modello CSV della directory del team. Puoi trascinare il file nella casella di caricamento o selezionare Scegli un file.
8. Seleziona la casella di controllo, riconosco che l'eliminazione dell'utente non è reversibile.
9. Scegli Elimina utenti.

> **Note**
>
> Questa azione inizierà immediatamente a eliminare gli utenti e potrebbe richiedere alcuni minuti. Gli utenti eliminati non saranno più in grado di accedere alla rete Wickr nel client Wickr.

Sospensione in blocco degli utenti

Puoi sospendere in blocco gli utenti della rete Wickr nella sezione Utente della Console di amministrazione di Wickr per Wickr.

> **Note**
>
> L'opzione di sospendere in blocco gli utenti si applica solo quando l'SSO non è abilitato.

Per sospendere in blocco gli utenti della rete Wickr, completa la procedura seguente.

1. Apri il file per Wickr all'indirizzo AWS Management Console https://console.aws.amazon.com/wickr/.
2. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Team Directory.

   La pagina Team Directory mostra gli utenti registrati nella tua rete Wickr.
3. Nella pagina Team Directory, scegli Gestisci utenti.
4. Nella finestra pop-up Gestisci utenti, scegli Sospendi utenti.

5. Scarica il modello CSV di esempio. Per scaricare il modello di esempio, scegli Scarica modello.
6. Completa il modello aggiungendo l'e-mail degli utenti che desideri sospendere in blocco dalla rete.
7. Carica il modello CSV completato. Puoi trascinare il file nella casella di caricamento o selezionare scegli un file.
8. Dopo aver caricato il file CSV, scegli Sospendi utenti.

> **Note**
>
> Questa azione inizierà immediatamente a sospendere gli utenti e potrebbe richiedere alcuni minuti. Gli utenti sospesi non possono accedere alla tua rete Wickr nel client Wickr. Quando sospendi un utente che è attualmente connesso alla tua rete Wickr nel client, quell'utente viene automaticamente disconnesso.

Utenti ospiti

La funzionalità utente ospite di Wickr consente ai singoli utenti ospiti di accedere al client Wickr e collaborare con gli utenti della rete Wickr. Gli amministratori di Wickr possono abilitare o disabilitare gli utenti ospiti per le loro reti Wickr nella pagina Security Group della console di amministrazione di Wickr.

Dopo aver abilitato la funzionalità, gli utenti ospiti invitati alla rete Wickr possono interagire con gli utenti della rete Wickr. Verrà applicata una tariffa alla funzionalità Account AWS per gli utenti ospiti. Per ulteriori informazioni sui prezzi della funzione utente ospite, consulta la pagina dei prezzi di Wickr nella sezione Prezzi dei componenti aggiuntivi.

Argomenti

- Abilita o disabilita gli utenti ospiti
- Visualizza il numero di utenti ospiti
- Visualizza l'utilizzo mensile
- Visualizza gli utenti ospiti
- Blocca un utente ospite

Abilita o disabilita gli utenti ospiti

Completa la seguente procedura per abilitare o disabilitare gli utenti ospiti per la tua rete Wickr.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Impostazioni di rete, quindi scegli Security Group.
4. Scegli Dettagli per un gruppo di sicurezza specifico.

   > **Note**
   >
   > Puoi abilitare gli utenti ospiti solo per singoli gruppi di sicurezza. Per abilitare gli utenti guest per tutti i gruppi di sicurezza della rete Wickr, è necessario abilitare la funzionalità per ogni gruppo di sicurezza della rete.
5. Scegli la scheda Federazione nella pagina dei dettagli del gruppo di sicurezza.
6. L'opzione per consentire l'accesso agli utenti ospiti sarà disponibile in due posizioni:

   - Federazione locale: per le reti negli Stati Uniti orientali (Virginia del Nord), scegli Modifica accanto alla sezione Federazione locale della pagina.
   - Federazione globale: per tutte le altre reti in altre regioni, scegli Modifica accanto alla sezione Federazione globale della pagina.
7. Seleziona Consenti agli utenti guest di abilitare gli utenti guest per il gruppo di sicurezza o deselezionalo per disabilitarlo.
8. Scegli Salva per salvare la modifica e renderla effettiva per il gruppo di sicurezza.

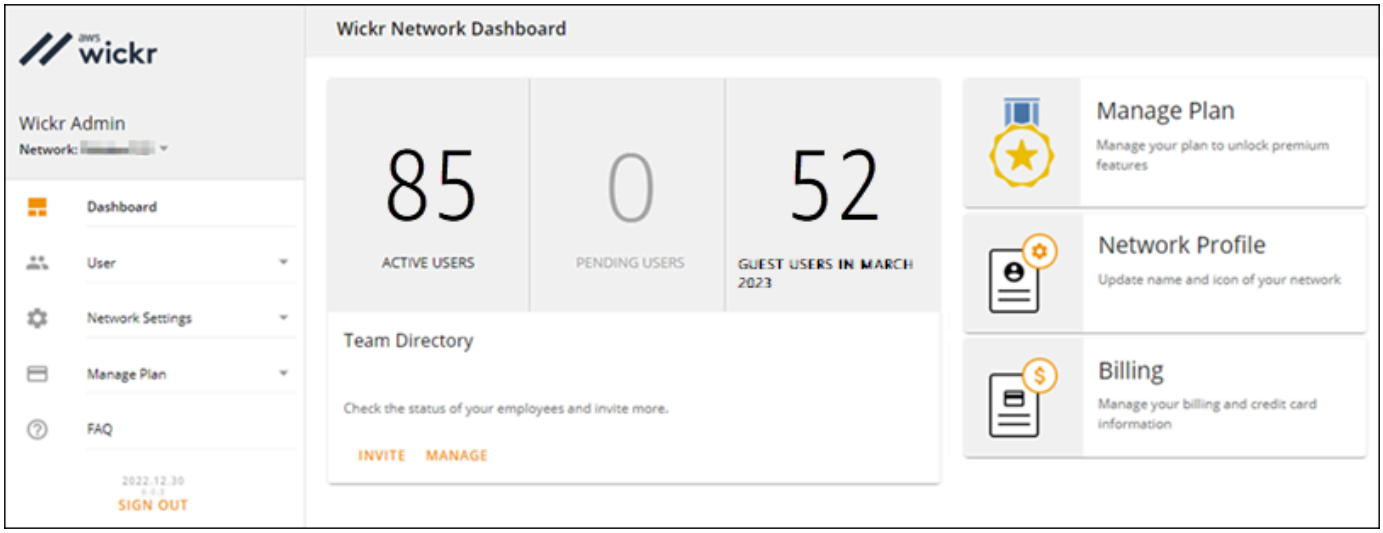
   Gli utenti registrati nel gruppo di sicurezza specifico della rete Wickr possono ora interagire con gli utenti ospiti. Per ulteriori informazioni, consulta Utenti ospiti nella Guida per l'utente di Wickr.

Visualizza il numero di utenti ospiti

Completa la seguente procedura per visualizzare il numero di utenti ospiti per la tua rete Wickr.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.

   Verrai reindirizzato alla console di amministrazione di Wickr per una rete specifica. La pagina Dashboard mostra il numero di utenti ospiti nella tua rete Wickr, come mostrato nell'esempio seguente.



Visualizza l'utilizzo mensile

Puoi visualizzare il numero di utenti ospiti con cui la tua rete ha comunicato durante un periodo di fatturazione. Per visualizzare l'utilizzo mensile, completa i passaggi seguenti.

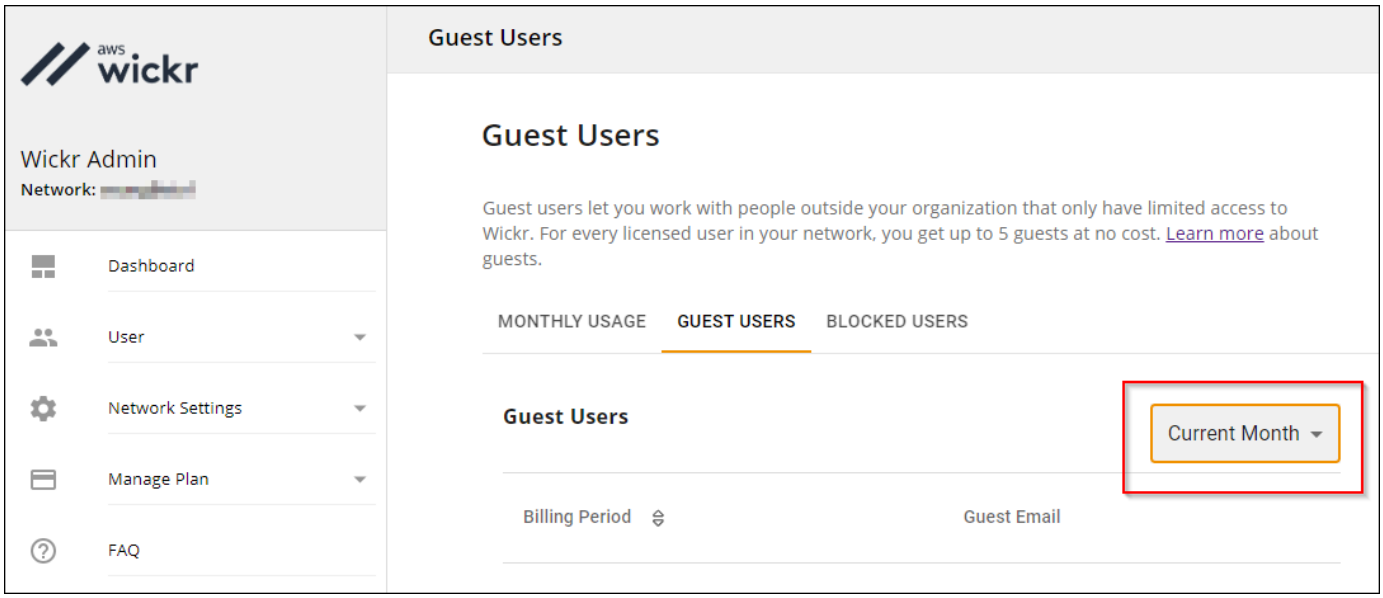
1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Utenti ospiti.
4. Nella pagina Utenti ospiti, scegli la sezione Utilizzo mensile.

> **Note**
>
> I dati di fatturazione degli ospiti vengono aggiornati ogni 24 ore.

Visualizza gli utenti ospiti

Puoi visualizzare un elenco di utenti ospiti con cui un utente della rete ha comunicato durante un periodo di fatturazione specifico. Per visualizzare gli utenti ospiti, completa i passaggi seguenti.

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Utenti ospiti.
4. Nella pagina Utenti ospiti, scegli la sezione Utenti ospiti.
5. Per visualizzare gli utenti ospiti per un mese specifico, seleziona il mese corrispondente dal menu a discesa.



Blocca un utente ospite

Gli utenti bloccati non possono comunicare con nessuno nella tua rete.

Per bloccare un utente ospite

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Utenti ospiti.
4. Nella pagina Utenti ospiti, scegli la sezione Utenti ospiti.
5. La sezione Utenti ospiti mostra gli utenti ospiti che hanno comunicato nella tua rete Wickr.
6. Nella sezione Utenti ospiti, trova l'e-mail dell'utente ospite che desideri bloccare.
7. Sul lato destro del nome dell'utente ospite, seleziona i tre puntini e scegli Blocca.
8. Scegli Blocca nella finestra pop-up.
9. Per visualizzare l'elenco degli utenti bloccati nella tua rete Wickr, scegli la sezione Utenti bloccati.

Per sbloccare un utente ospite

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nella pagina Reti, scegli il link Amministratore per accedere alla console di amministrazione di Wickr per quella rete.
3. Nel pannello di navigazione della console di amministrazione di Wickr, scegli Utente, quindi scegli Utenti ospiti.
4. Nella pagina Utenti ospiti, scegli la sezione Utenti bloccati.
5. La sezione Utenti bloccati mostra gli utenti ospiti bloccati nella tua rete Wickr.
6. Nella sezione Utenti bloccati, trova l'email dell'utente ospite che desideri sbloccare.
7. Sul lato destro del nome dell'utente ospite, seleziona i tre puntini e scegli Sblocca.
8. Scegli Sblocca nella finestra pop-up.

Sicurezza in Wickr AWS

Sicurezza nel cloud presso AWS è la massima priorità. Come AWS cliente, trae vantaggio da data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e tu. 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 in esecuzione AWS servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito del AWS Programmi di conformità . Per maggiori informazioni sui programmi di conformità che si applicano a AWS Wickr, vedi AWS Servizi rientranti nell'ambito del programma di conformità .
- 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 Wickr. I seguenti argomenti mostrano come configurare Wickr per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a usarne altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Wickr.

Argomenti

Protezione dei dati in Wickr AWS

Il AWS modello di responsabilità condivisa modello di di si applica alla protezione dei dati in AWS Wickr. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutte le Cloud AWS. L'utente è responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per Servizi AWS che usi. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta AWS Modello di responsabilità condivisa e post sul GDPR blog sul AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS credenziali e configura singoli utenti con AWS IAM Identity Center oppure 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:

- Usa l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per l'acquisizione AWS attività, vedi Lavorare con i CloudTrail sentieri in AWS CloudTrail Guida per l'utente.
- Utilizzo AWS soluzioni di 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 sono necessari FIPS 140-3 moduli crittografici convalidati per l'accesso AWS tramite un'interfaccia a riga di comando o unAPI, utilizza un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo vivamente 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 Wickr o altri Servizi AWS utilizzando la console, API AWS CLI, oppure AWS SDKs. 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. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Gestione delle identità e degli accessi per Wickr AWS

AWS Identity and Access Management () IAM è un Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso a AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse di Wickr. IAMè un Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Come si usa AWS Identity and Access Management (IAM) differisce, a seconda del lavoro che svolgi in Wickr.

Utente del servizio: se utilizzi il servizio Wickr per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Wickr 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 Wickr, consulta. Risoluzione dei problemi relativi all'identità e all'accesso AWS a Wickr

Amministratore del servizio: se sei responsabile delle risorse di Wickr della tua azienda, probabilmente hai pieno accesso a Wickr. È tuo compito determinare a quali funzionalità e risorse di Wickr devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM Wickr, consulta. Come funziona AWS Wickr con IAM

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a Wickr. Per visualizzare esempi di policy basate sull'identità di Wickr che puoi utilizzare in, consulta. IAM Esempi di policy basate sull'identità per Wickr AWS

Autenticazione con identità

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

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

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

Se accedi AWS programmaticamente, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le credenziali dell'utente. Se non usi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, vedi Firma AWS APIrichieste nella Guida IAM per l'utente.

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

Account AWS utente root

Quando crei un Account AWS, inizi con un'unica identità di accesso con accesso completo a tutti Servizi AWS e le risorse presenti nell'account. Questa identità è denominata Account AWS utente 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 l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura ottimale, 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, un provider di identità Web, il AWS Directory Service, la directory Identity Center o qualsiasi utente che accede Servizi AWS utilizzando le credenziali fornite tramite una fonte di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un set di utenti e gruppi nella propria fonte di identità per utilizzarli su tutti i Account AWS e applicazioni. Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nel AWS IAM Identity Center Guida per l'utente.

IAM users and groups

Un IAMutente è un'identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo 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, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

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 Quando creare un IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo nel AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un AWS CLI oppure AWS APIoperazione o utilizzando un comando personalizzatoURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli 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 informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella AWS IAM Identity Center Guida per l'utente.
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere un IAM ruolo per assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo 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 conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra più account, consulta l'accesso alle risorse tra account IAM nella Guida per l'utente. IAM
- Accesso a più servizi: alcuni Servizi AWS usa le funzionalità in 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 diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni in AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire

un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi a valle. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse da completare. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di 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 di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi vengono visualizzati nel Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e in fase di creazione AWS CLI oppure AWS APIrichieste. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS assegnare un ruolo a un'EC2istanza e renderlo disponibile a tutte le relative applicazioni, è necessario creare un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso in AWS creando politiche e allegandole a AWS identità o risorse. Una politica è un oggetto in 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 in AWS come JSON documenti. Per

ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, il AWS CLI, o AWS API.

Policy basate su identità

I criteri basati sull'identità sono documenti relativi ai criteri di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM 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 all'interno del Account AWS. Le politiche gestite includono AWS politiche gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di 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 azioni 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 usare AWS politiche gestite da IAM una politica basata sulle risorse.

Liste 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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportanoACLs. Per ulteriori informazioniACLs, consulta la panoramica di Access control list (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 di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM 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 suoi 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 nella Guida per l'utente. IAM IAM
- 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 le politiche di sessione nella Guida per l'IAMutente.

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 AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'IAMutente.

AWS politiche gestite per AWS Wickr

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile da usare AWS politiche gestite piuttosto che scrivere politiche da soli. Ci vogliono tempo ed esperienza per creare politiche gestite dai IAM clienti che forniscano al team solo le autorizzazioni di cui ha bisogno. Per iniziare rapidamente, puoi utilizzare il nostro AWS politiche gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel Account AWS. Per ulteriori informazioni su AWS politiche gestite, vedere AWS politiche gestite nella Guida IAM per l'utente.

Servizi AWS mantenere e aggiornare AWS politiche gestite. Non è possibile modificare le autorizzazioni in AWS politiche gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a un AWS politica gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino un AWS politica gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da un AWS politica gestita, in modo che gli aggiornamenti delle politiche non compromettano le autorizzazioni esistenti.

AWS politica gestita: AWSWickrFullAccess

Puoi allegare la `AWSWickrFullAccess` politica alle tue IAM identità. Questa politica concede l'autorizzazione amministrativa completa al servizio Wickr, incluso il AWS Management Console per Wickr nel AWS Management Console. Per ulteriori informazioni sull'associazione di criteri a un'identità, vedere Aggiungere e rimuovere le autorizzazioni di IAM identità nella AWS Identity and Access Management Guida per l'utente.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `wickr`— Concede l'autorizzazione amministrativa completa al servizio Wickr.

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

```
}
```

Wickr aggiorna AWS policy gestite

Visualizza i dettagli sugli aggiornamenti di AWS le politiche gestite per Wickr da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al RSS feed nella pagina di cronologia dei documenti di Wickr.

Modifica	Descrizione	Data
AWSWickrFullAccess: nuova policy	Wickr ha aggiunto una nuova politica che concede l'autorizzazione amministrativa completa al servizio Wickr, inclusa la console di amministrazione Wickr nel AWS Management Console.	28 novembre 2022
Wickr ha iniziato a tenere traccia delle modifiche	Wickr ha iniziato a tracciare le modifiche per il suo AWS politiche gestite.	28 novembre 2022

Come funziona AWS Wickr con IAM

Prima di utilizzare IAM per gestire l'accesso a Wickr, scopri quali IAM funzionalità sono disponibili per l'uso con Wickr.

IAMfunzionalità che puoi usare con Wickr AWS

IAMcaratteristica	supporto Wickr
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	No

IAMcaratteristica	supporto Wickr
Chiavi di condizione delle policy	No
ACLs	No
ABAC(tag nelle politiche)	No
Credenziali temporanee	No
Autorizzazioni del principale	No
☻Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come Wickr e altri AWS i servizi funzionano con la maggior parte delle IAM funzionalità, vedi AWS servizi compatibili con IAM la Guida per l'IAMutente.

Politiche basate sull'identità per Wickr

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un utente, un gruppo di utenti o un IAM ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. 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 ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per Wickr

Per visualizzare esempi di politiche basate sull'identità di Wickr, vedi. Esempi di policy basate sull'identità per Wickr AWS

Politiche basate sulle risorse all'interno di Wickr

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di policy allegati JSON a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di 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 azioni 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 abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica 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 IAM amministratore 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 la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per Wickr

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome di quelle associate AWS APIoperazione. Esistono alcune eccezioni, come le azioni di sola autorizzazione che non hanno un'operazione corrispondente. API 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 Wickr, consulta Azioni definite da AWS Wickr nel Service Authorization Reference.

Le azioni politiche in Wickr utilizzano il seguente prefisso prima dell'azione:

```
wickr
```

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

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

Per visualizzare esempi di politiche basate sull'identità di Wickr, vedi. Esempi di policy basate sull'identità per Wickr AWS

Risorse politiche per Wickr

Supporta risorse politiche: No

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni 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 Wickr e relativiARNs, consulta Resources Defined by AWS Wickr nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare le caratteristiche ARN di ciascuna risorsa, consulta Azioni definite da Wickr. AWS

Per visualizzare esempi di politiche basate sull'identità di Wickr, vedere. Esempi di policy basate sull'identità per Wickr AWS

Chiavi relative alle condizioni delle policy per Wickr

Supporta le chiavi delle condizioni delle politiche specifiche del servizio: No

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni 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. Puoi 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 specificate più `Condition` elementi in un'istruzione o più chiavi in un singolo `Condition` elemento, AWS li valuta utilizzando un'`AND`operazione logica. Se specificate più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'`OR`operazione logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il relativo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per vedere tutto AWS chiavi di condizione globali, vedi AWS chiavi di contesto della condizione globale nella Guida IAM per l'utente.

Per visualizzare un elenco delle chiavi di condizione di Wickr, consulta Condition Keys for AWS Wickr nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi usare una chiave di condizione, vedi Azioni definite da Wickr. AWS

Per visualizzare esempi di politiche basate sull'identità di Wickr, vedi. Esempi di policy basate sull'identità per Wickr AWS

ACLsin Wickr

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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

ABACcon Wickr

Supporti ABAC (tag nelle politiche): No

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

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 suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con Wickr

Supporta credenziali temporanee: No

Medio Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, tra cui Servizi AWS lavorare con credenziali temporanee, vedere Servizi AWS che funzionano con IAM la Guida per l'IAMutente.

Stai utilizzando credenziali temporanee se accedi a AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedi 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 sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI oppure AWS API. 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, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni principali per diversi servizi per Wickr

Supporta sessioni di accesso diretto (): No FAS

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

Ruoli di servizio per Wickr

Supporta i ruoli di servizio: No

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

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

Ruoli collegati ai servizi per Wickr

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 di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi vengono visualizzati nel Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, vedere AWS servizi che funzionano con. 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 Wickr AWS

Per impostazione predefinita, un nuovo IAM utente non ha i permessi per fare nulla. Un IAM amministratore deve creare e assegnare IAM politiche che consentano agli utenti di amministrare il servizio Wickr. AWS Di seguito viene illustrato un esempio di policy di autorizzazione.

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

Questa politica di esempio offre agli utenti le autorizzazioni per creare, visualizzare e gestire le reti Wickr utilizzando AWS Management Console per Wickr. Per ulteriori informazioni sugli elementi contenuti in una dichiarazione IAM politica, vedere. Politiche basate sull'identità per Wickr Per informazioni su come creare una IAM politica utilizzando questi documenti di esempioJSON, consulta Creazione di politiche nella JSON scheda della Guida per l'IAMutente.

Argomenti

- Best practice per le policy
- Utilizzo di AWS Management Console per Wickr

- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse Wickr nel tuo account. Queste azioni possono comportare costi per Account AWS. Quando crei o modifichi politiche basate sull'identità, segui queste linee guida e consigli:

- Inizia con AWS politiche gestite e passaggio alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza il AWS politiche gestite che concedono autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Si consiglia di ridurre ulteriormente le autorizzazioni definendo AWS politiche gestite dai clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta AWS politiche gestite o AWS politiche gestite per le funzioni lavorative nella Guida per IAM l'utente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi 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 per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare le condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se disponi di uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attivala MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Utilizzo di AWS Management Console per Wickr

Allega il `AWSWickrFullAccess` AWS politica gestita alle tue IAM identità per concedere loro la piena autorizzazione amministrativa al servizio Wickr, inclusa la console di amministrazione di Wickr nel AWS Management Console. Per ulteriori informazioni, vedereAWS politica gestita: AWSWickrFullAccess.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla propria identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando a livello di codice il AWS CLI oppure AWS API.

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

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso AWS a Wickr

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

Argomenti

- Non sono autorizzato a eseguire un'azione amministrativa nel AWS Management Console per Wickr

Non sono autorizzato a eseguire un'azione amministrativa nel AWS Management Console per Wickr

Se il file AWS Management Console perché Wickr indica che non sei autorizzato a eseguire un'azione, quindi devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'`mateojackson`IAMutente tenta di utilizzare il AWS Management Console affinché Wickr crei, gestisca o visualizzi reti Wickr nel AWS Management Console per Wickr ma non dispone delle autorizzazioni e. `wickr:CreateAdminSession` `wickr:ListNetworks`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wickr:ListNetworks
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le sue politiche per consentirgli di accedere a AWS Management Console per Wickr utilizzando le azioni and. `wickr:CreateAdminSession` `wickr:ListNetworks` Per ulteriori informazioni, consulta Esempi di policy basate sull'identità per Wickr AWS e AWS politica gestita: AWSWickrFullAccess.

Convalida della conformità

Per un elenco di AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere AWS Servizi rientranti nell'ambito del programma di conformità . Per informazioni generali, vedere AWS Programmi di conformità di conformità.

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

La tua responsabilità di conformità quando usi Wickr è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità della tua azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide rapide su sicurezza e conformità Guide introduttive implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità su AWS.
- AWS Risorse per la conformità : questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua località.
- Valutazione delle risorse con regole in AWS Config Guida per gli sviluppatori — AWS Config; valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS il servizio fornisce una visione completa dello stato di sicurezza all'interno AWS che consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in Wickr AWS

Il AWS l'infrastruttura globale è costruita attorno Regioni AWS e zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sull' Regioni AWS e zone di disponibilità, vedi AWS Infrastruttura globale.

Oltre al AWS infrastruttura globale, Wickr offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati. Per ulteriori informazioni, consulta Conservazione dei dati.

Sicurezza dell'infrastruttura in Wickr AWS

In quanto servizio gestito, AWS Wickr è protetto da AWS procedure di sicurezza di rete globali descritte nel white paper Amazon Web Services: Overview of Security Processes.

Analisi della configurazione e della vulnerabilità in Wickr AWS

La configurazione e i controlli IT sono una responsabilità condivisa tra AWS e tu, nostro cliente. Per ulteriori informazioni, consulta il AWS modello di responsabilità condivisa.

È tua responsabilità configurare Wickr in base a specifiche e linee guida, istruire periodicamente i tuoi utenti a scaricare l'ultima versione del client Wickr, assicurarti di utilizzare l'ultima versione del bot di conservazione dei dati di Wickr e monitorare l'utilizzo di Wickr da parte degli utenti.

Le migliori pratiche di sicurezza per Wickr AWS

Wickr offre una serie di funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Per prevenire potenziali eventi di sicurezza associati all'uso di Wickr, segui queste best practice:

- Implementa l'accesso con privilegi minimi e crea ruoli specifici da utilizzare per le azioni di Wickr. Usa i IAM modelli per creare un ruolo. Per ulteriori informazioni, consulta AWS politiche gestite per AWS Wickr.
- Accedi a AWS Management Console per Wickr autenticandosi su AWS Management Console prima di iniziare. Non condividere le credenziali personali della console. Tutti gli utenti di Internet possono accedere alla console, ma non possono accedere o avviare una sessione se non dispongono di credenziali valide per la console.

Monitoraggio di AWS Wickr

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

- 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 AWS CloudTrail Guida per l'utente. Per ulteriori informazioni sulla registrazione delle chiamate all'API Wickr utilizzando CloudTrail, consulta. Registrazione delle chiamate API AWS Wickr utilizzando AWS CloudTrail

Registrazione delle chiamate API AWS Wickr utilizzando AWS CloudTrail

AWS Wickr è integrato conAWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Wickr. CloudTrail acquisisce tutte le chiamate API per Wickr come eventi. Le chiamate acquisite includono chiamate provenienti da Wickr e chiamate in codice alle operazioni dell'API Wickr. AWS Management Console Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Wickr. 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 a Wickr, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli. Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrailutente.

Informazioni su Wickr in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in Wickr, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con CloudTrail la cronologia degli eventi.

Per una registrazione continua degli eventi del tuo sitoAccount AWS, compresi gli eventi per Wickr, 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 percorso registra gli eventi di tutte le Regioni nella partizione AWSe distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. 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 Wickr vengono registrate da. CloudTrail Ad esempio, le chiamate a e le `CreateAdminSession` `ListNetworks` azioni generano voci nei file di registro. CloudTrail

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 servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprendere le voci dei file di registro di Wickr

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'`CreateAdminSession`azione.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T08:19:24Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateAdminSession",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkId": 56019692
    },
    "responseElements": {
        "sessionCookie": "***",
        "sessionNonce": "***"
    },
    "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
    "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T07:54:09Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "BOT_Network",
        "accessLevel": "3000"
    },
    "responseElements": null,
```

```
    "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
    "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
```

```
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
```

```
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
    "eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T23:06:04Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
            "some-existing-key-3": "value 1"
        }
    },
    "responseElements": null,
    "requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
    "eventID": "26147035-8130-4841-b908-4537845fac6a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Dashboard di analisi

Puoi utilizzare la dashboard di analisi per visualizzare in che modo la tua organizzazione utilizza AWS Wickr. La procedura seguente spiega come accedere alla dashboard di analisi utilizzando la console AWS Wickr.

Per accedere alla dashboard di analisi

1. Apri il file AWS Management Console per Wickr all'indirizzo https://console.aws.amazon.com/wickr/.
2. Nel riquadro di navigazione, scegliere Analytics (Analisi).

   La pagina Analytics mostra le metriche per la tua rete in diverse schede.

Nella pagina Analytics, troverai un filtro temporale nell'angolo in alto a destra di ogni scheda. Questo filtro si applica all'intera pagina. Inoltre, nell'angolo in alto a destra di ogni scheda, puoi esportare i punti dati per l'intervallo di tempo selezionato scegliendo l'opzione Esporta disponibile.

> **Note**
>
> L'ora selezionata è in UTC (Universal Time Coordinated).

Sono disponibili le seguenti schede:

- Visualizza una panoramica:
  - Registrati: il numero totale di utenti registrati, inclusi gli utenti attivi e sospesi sulla rete nel periodo selezionato. Non include gli utenti in sospeso o invitati.
  - In sospeso: il numero totale di utenti in sospeso sulla rete nel periodo selezionato.
  - Registrazione utente: il grafico mostra il numero totale di utenti registrati nell'intervallo di tempo selezionato.
  - Dispositivi: il numero di dispositivi in cui l'app è stata attiva.
  - Versioni client: il numero di dispositivi attivi classificati in base alle relative versioni client.

- I membri visualizzano:
  - Stato: utenti attivi sulla rete entro il periodo di tempo selezionato.
  - Utenti attivi:
    - Il grafico mostra il numero di utenti attivi nel tempo e può essere aggregato per giorno, settimana o mese (entro l'intervallo di tempo selezionato sopra).
    - Il numero di utenti attivi può essere suddiviso per piattaforma, versione client o gruppo di sicurezza. Se un gruppo di sicurezza è stato eliminato, il conteggio totale verrà visualizzato come Eliminato#.

- I messaggi vengono visualizzati:
  - Messaggi inviati: il numero di messaggi unici inviati da tutti gli utenti e i bot sulla rete nel periodo di tempo selezionato.
  - Chiamate: numero di chiamate uniche effettuate da tutti gli utenti della rete.
  - File: numero di file inviati dagli utenti in rete (inclusi memo vocali).
  - Dispositivi: il grafico a torta mostra il numero di dispositivi attivi classificati in base al sistema operativo.
  - Versioni client: il numero di dispositivi attivi classificati in base alle relative versioni client.

Cronologia dei documenti

La tabella seguente descrive le versioni della documentazione per Wickr.

Modifica	Descrizione	Data
La classificazione e la federazione transfrontaliere sono ora disponibili	La funzionalità di classific azione transfrontaliera consente di modificare l'interfa ccia utente alle conversazioni per gli GovCloud utenti. Per ulteriori informazioni, vedere Classificazione e federazione GovCloud transfrontaliere.	25 giugno 2024
La funzione di conferma di lettura è ora disponibile	Gli amministratori di Wickr possono ora abilitare o disabilit are la funzionalità di conferma di lettura nella Console di amministrazione. Per ulteriori informazioni, consulta Leggi le conferme.	23 aprile 2024
Global Federation ora supporta la federazione con restrizioni e gli amministratori possono visualizzare le analisi di utilizzo nella Console di amministrazione	La Federazione globale ora supporta la federazione con restrizioni. Funziona per le reti Wickr in altre. Regioni AWS Per ulteriori informazioni, consulta Gruppi di sicurezza . Inoltre, gli amministratori possono ora visualizzare le proprie analisi di utilizzo nella dashboard di Analytics in Admin Console. Per ulteriori informazioni, consulta la dashboard di Analytics.	28 marzo 2024

È ora disponibile una prova gratuita di tre mesi del piano Premium di AWS Wickr	Gli amministratori di Wickr possono ora scegliere un piano Premium di prova gratuita di tre mesi per un massimo di 30 utenti. Durante la prova gratuita, sono disponibili tutte le funzionalità del piano Standard e Premium, inclusi controlli amministrativi illimitati e conservazione dei dati. La funzione utente ospite non è disponibile durante la prova gratuita Premium. Per ulteriori informazioni, consulta Gestisci il piano.	9 febbraio 2024
La funzionalità utente ospite è disponibile a livello generale e sono stati aggiunti altri controlli amministrativi	Gli amministratori di Wickr possono ora accedere a una serie di nuove funzionalità, tra cui l'elenco di utenti ospiti, la possibilità di eliminare o sospendere gli utenti in blocco e l'opzione per impedire agli utenti ospiti di comunicare nella rete Wickr. Per ulteriori informazioni, consulta Utenti ospiti.	8 novembre 2023
Wickr è ora disponibile in Europa (Francoforte) Regione AWS	Wickr è ora disponibile in Europa (Francoforte). Regione AWS Per ulteriori informazioni, consulta Accedere a Wickr.	26 ottobre 2023

Le reti Wickr ora hanno la possibilità di federarsi tra Regioni AWS	Le reti Wickr ora hanno la possibilità di federarsi tra di loro. Regioni AWSPer ulteriori informazioni, consulta Gruppi di sicurezza.	29 settembre 2023
Wickr è ora disponibile in Europa (Londra) Regione AWS	Wickr è ora disponibile in Europa (Londra). Regione AWS Per ulteriori informazioni, consulta Accedere a Wickr.	23 agosto 2023
Wickr è ora disponibile in Canada (Central) Regione AWS	Wickr è ora disponibile in Canada (Central). Regione AWS Per ulteriori informazioni, consulta Accedere a Wickr.	3 luglio 2023
La funzione utente ospite è ora disponibile in anteprima	Gli utenti ospiti possono accedere al client Wickr e collaborare con gli utenti della rete Wickr. Per ulteriori informazioni, consulta Utenti ospiti (anteprima).	31 maggio 2023
AWSWickr è ora integrato con AWS CloudTrail ed è ora disponibile in AWS GovCloud (Stati Uniti occidentali) come WickrGov	AWSWickr è ora integrato con. AWS CloudTrail Per ulteriori informazioni, consulta Registrazione delle chiamate AWS API Wickr utilizzan do. AWS CloudTrail Inoltre, Wickr è ora disponibile in AWS GovCloud (Stati Uniti occidentali) come. WickrGov Per ulteriori informazioni, consulta la Guida AWS WickrGovper l'AWS GovCloud (US) utente.	30 marzo 2023

Etichettatura e creazione di reti multiple	Il tagging ora è supportato in WickrAWS. Per maggiori informazioni, consulta Tag di rete. Ora è possibile creare più reti in Wickr. Per maggiori informazioni, vedi Creare una rete.	7 marzo 2023
Versione iniziale	Versione iniziale della Wickr Administration Guide	28 novembre 2022

Note di rilascio

Per aiutarti a tenere traccia degli aggiornamenti e dei miglioramenti in corso a Wickr, pubblichiamo avvisi di rilascio che descrivono le modifiche recenti.

Giugno 2024

- La classificazione e la federazione transfrontaliere sono ora disponibili per gli utenti. GovCloud Per ulteriori informazioni, vedere Classificazione e federazione GovCloud transfrontaliere.

aprile 2024

- Wickr ora supporta le conferme di lettura. Per ulteriori informazioni, consulta Leggi le ricevute.

Marzo 2024

- La federazione globale ora supporta la federazione con restrizioni, dove la federazione globale può essere abilitata solo per reti selezionate che vengono aggiunte in base alla federazione limitata. Funziona per le reti Wickr in altre. Regioni AWS Per ulteriori informazioni, consulta Gruppi di sicurezza.
- Gli amministratori possono ora visualizzare le proprie analisi di utilizzo nella dashboard di Analytics in Admin Console. Per ulteriori informazioni, consulta la dashboard di Analytics.

Febbraio 2024

- AWSWickr offre ora una prova gratuita di tre mesi del suo piano Premium per un massimo di 30 utenti. Le modifiche e le limitazioni includono:
  - Tutte le funzionalità del piano Standard e Premium, come i controlli amministrativi illimitati e la conservazione dei dati, sono ora disponibili nella versione di prova gratuita Premium. La funzione utente ospite non è disponibile durante la prova gratuita Premium.
  - La versione di prova gratuita precedente non è più disponibile. Puoi aggiornare la tua prova gratuita o il tuo piano Standard esistente a una prova gratuita Premium se non hai già utilizzato la prova gratuita Premium. Per ulteriori informazioni, consulta Gestisci il piano.

Novembre 2023

- La funzionalità per gli utenti ospiti è ora disponibile a livello generale. Le modifiche e le aggiunte includono:
  - Possibilità di segnalare abusi da parte di altri utenti di Wickr.
  - Gli amministratori possono visualizzare un elenco di utenti ospiti con cui una rete ha interagito e i conteggi mensili di utilizzo.
  - Gli amministratori possono impedire agli utenti ospiti di comunicare con la propria rete.
  - Prezzi aggiuntivi per gli utenti ospiti.

- Miglioramenti del controllo amministrativo
  - Possibilità di eliminare/sospendere gli utenti in blocco.
  - SSOImpostazione aggiuntiva per configurare un periodo di prova per l'aggiornamento dei token.

Ottobre 2023

- Miglioramenti
  - Wickr è ora disponibile in Europa (Francoforte). Regione AWS

Settembre 2023

- Miglioramenti
  - Le reti Wickr ora hanno la possibilità di federarsi tra loro. Regioni AWSPer ulteriori informazioni, consulta Gruppi di sicurezza.

Agosto 2023

- Miglioramenti
  - Wickr è ora disponibile in Europa (Londra). Regione AWS

Luglio 2023

- Miglioramenti
  - Wickr è ora disponibile in Canada (Central). Regione AWS

Maggio 2023

- Miglioramenti
  - È stato aggiunto il supporto per gli utenti ospiti. Per ulteriori informazioni, consulta Utenti ospiti.

Marzo 2023

- Wickr è ora integrato con. AWS CloudTrail Per ulteriori informazioni, consulta Registrazione delle chiamate API AWS Wickr utilizzando AWS CloudTrail.
- Wickr è ora disponibile in AWS GovCloud (Stati Uniti occidentali) come. WickrGov Per ulteriori informazioni, consulta la Guida AWS WickrGovper l'AWS GovCloud (US) utente.
- Wickr ora supporta il tagging. Per ulteriori informazioni, consulta Tag di rete. Ora è possibile creare più reti in Wickr. Per ulteriori informazioni, consulta Fase 1: Creare una rete.

Febbraio 2023

- Wickr ora supporta l'Android Tactical Assault Kit (). ATAK Per ulteriori informazioni, consulta Abilita ATAK nella dashboard di Wickr Network.

gennaio 2023

- Il Single Sign-on (SSO) può ora essere configurato su tutti i piani, inclusi Free Trial e Standard.

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.