aws

Guia de administração

AWS Wickr

AWS Wickr: Guia de administração

Table of Contents

O que é o AWS Wickr?

O AWS Wickr é um serviço end-to-end criptografado que ajuda organizações e agências governamentais a se comunicarem com segurança por meio one-to-one de mensagens em grupo, chamadas de voz e vídeo, compartilhamento de arquivos, compartilhamento de tela e muito mais. O Wickr pode ajudar os clientes a superar as obrigações de retenção de dados associadas a aplicativos de mensagens para consumidores e facilitar a colaboração com segurança. Controles avançados de administração e segurança ajudam as organizações a atender aos requisitos legais e regulamentares e a criar soluções personalizadas para os desafios de segurança de dados.

As informações podem ser registradas em um armazenamento de dados privado controlado pelo cliente para fins de retenção e auditoria. Os usuários têm um controle administrativo abrangente sobre os dados, o que inclui definir permissões, configurar opções de mensagens efêmeras e definir grupos de segurança. O Wickr se integra a serviços adicionais, como o Active Directory (AD), autenticação única (SSO) com OpenID Connect (OIDC) e muito mais. Você pode criar e gerenciar rapidamente uma rede Wickr por meio do AWS Management Console e automatizar fluxos de trabalho com segurança usando bots Wickr. Para começar, consulte o Configurando o AWS Wickr.

Tópicos

Recursos do Wickr

Segurança e privacidade aprimoradas

O Wickr usa criptografia Advanced Encryption Standard (AES) de 256 end-to-end bits para cada recurso. As comunicações são criptografadas localmente nos dispositivos do usuário e permanecem indecifráveis em trânsito para qualquer pessoa que não seja o remetente e o destinatário. Cada mensagem, chamada e arquivo é criptografado com uma nova chave aleatória, e ninguém além dos destinatários pretendidos (nem mesmo AWS) pode decifrá-los. Quer estejam compartilhando dados confidenciais e regulamentados, discutindo questões jurídicas ou de RH ou até mesmo conduzindo operações militares táticas, os clientes usam o Wickr para se comunicar quando a segurança e a privacidade são fundamentais.

Retenção de dados

Os recursos administrativos flexíveis foram desenvolvidos não apenas para proteger informações confidenciais, mas para reter os dados, conforme necessário, para obrigações de conformidade, retenção legal e auditoria. Mensagens e arquivos podem ser arquivados em um armazenamento de dados seguro e controlado pelo cliente.

Acesso flexível

Os usuários têm acesso a vários dispositivos (celular, desktop) e a capacidade de funcionar em ambientes de baixa largura de banda, incluindo desconectados e comunicações. out-of-band

Controles administrativos

Os usuários têm controle administrativo abrangente sobre os dados, o que inclui definir permissões, configurar opções responsáveis de mensagens efêmeras e definir grupos de segurança.

Integrações e bots potentes

O Wickr se integra a serviços adicionais, como a Active Directory, autenticação única (SSO) com OpenID Connect (OIDC) e muito mais. Os clientes podem criar e gerenciar rapidamente uma rede Wickr por meio do AWS Management Console e automatizar fluxos de trabalho com segurança com o Wickr Bots.

A seguir está um resumo das ofertas de colaboração do Wickr:

- Mensagens individuais e para grupos: converse com segurança com sua equipe em salas com até 500 membros
- Chamadas de áudio e vídeo: realize teleconferências com até 70 pessoas
- Compartilhamento de tela e transmissões: faça apresentações com até 500 participantes
- Compartilhamento e salvamento de arquivos: transfira arquivos de até 5 GB com armazenamento ilimitado
- Efêmero: controle a expiração e os temporizadores burn-on-read
- Federação global: conecte-se com usuários do Wickr fora da sua rede

> **Note**
>
> As redes Wickr em AWS GovCloud (Oeste dos EUA) só podem ser federadas com outras redes Wickr em AWS GovCloud (Oeste dos EUA).

Acessando o Wickr

O Wickr está disponível no Leste dos EUA (Norte da Virgínia), Canadá (Central), Europa (Londres), Ásia-Pacífico (Sydney), Europa (Frankfurt), Europa (Estocolmo), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Tóquio). Regiões da AWS O Wickr também está disponível como WickrGov no AWS GovCloud (Oeste dos EUA). Região da AWS

Os administradores acessam o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/. Antes de começar a usar o Wickr, você deve concluir os guias Configurando o AWS Wickr e Conceitos básicos do AWS Wickr.

> **Note**
>
> O serviço Wickr não tem uma interface de programação de aplicações (API).

Os usuários finais acessam o Wickr por meio do cliente Wickr. Para obter mais informações, consulte o Guia do usuário do AWS Wickr.

Definição de preço

O Wickr está disponível em diferentes planos para indivíduos, pequenas equipes e grandes empresas. Para obter mais informações, consulte Definição de preço do AWS Wickr.

Documentação do usuário final do Wickr

Se você for um usuário final do cliente Wickr e precisar acessar sua documentação, consulte o Guia do usuário do AWS Wickr.

Configurando o AWS Wickr

Se você for um cliente novo da AWS, preencha os pré-requisitos de configuração listados nesta página antes de começar a usar o AWS Wickr. Para esses procedimentos de configuração, utilize o serviço do AWS Identity and Access Management (IAM). Para obter informações completas sobre o IAM, consulte o Guia do usuário do IAM.

Tópicos

Cadastrar para AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de aplicação envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

Criar um usuário do IAM

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade do IAM (Recomendado)	Use credenciais de curto prazo para acessar a AWS. Isso está de acordo com as práticas recomendadas de segurança. Para obter informações sobre as práticas recomendadas, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.	Seguindo as instruções em Conceitos básicos no AWS IAM Identity Center Guia do usuário.	Para configurar o acesso programático, consulte Configurar a AWS CLI para usar o AWS IAM Identity Center no AWS Command Line Interface Guia do usuário.
No IAM (Não recomendado)	Use credenciais de curto prazo para acessar a AWS.	Seguindo as instruções em Criar o seu primeiro usuário administrador e um grupo de usuários do IAM no Guia do usuário do IAM.	Para configurar o acesso programático, consulte Gerenciamento chaves de acesso de usuários do IAM no Guia do usuário do IAM.

> **Note**
>
> Você também pode atribuir a política gerenciada `AWSWickrFullAccess` para conceder permissão administrativa total ao serviço Wickr. Para ter mais informações, consulte AWS política gerenciada: AWSWickrFullAccess.

Próximas etapas

Você concluiu as etapas de configuração de pré-requisito. Para começar a configurar o Wickr, consulte Conceitos básicos.

Conceitos básicos do AWS Wickr

Neste guia, mostraremos como começar a usar o Wickr criando uma rede, configurando sua rede e criando usuários.

Tópicos

Pré-requisitos

Antes de iniciar, conclua os pré-requisitos a seguir, se ainda não o fez:

- Cadastre-se na Amazon Web Services (AWS). Para ter mais informações, consulte Configurando o AWS Wickr.
- Certifique-se de que você tenha as permissões necessárias para administrar o Wickr. Para ter mais informações, consulte AWS política gerenciada: AWSWickrFullAccess.
- Certifique-se de permitir as listas das portas e domínios apropriados para o Wickr. Para ter mais informações, consulte Lista de portas e domínios para permitir.

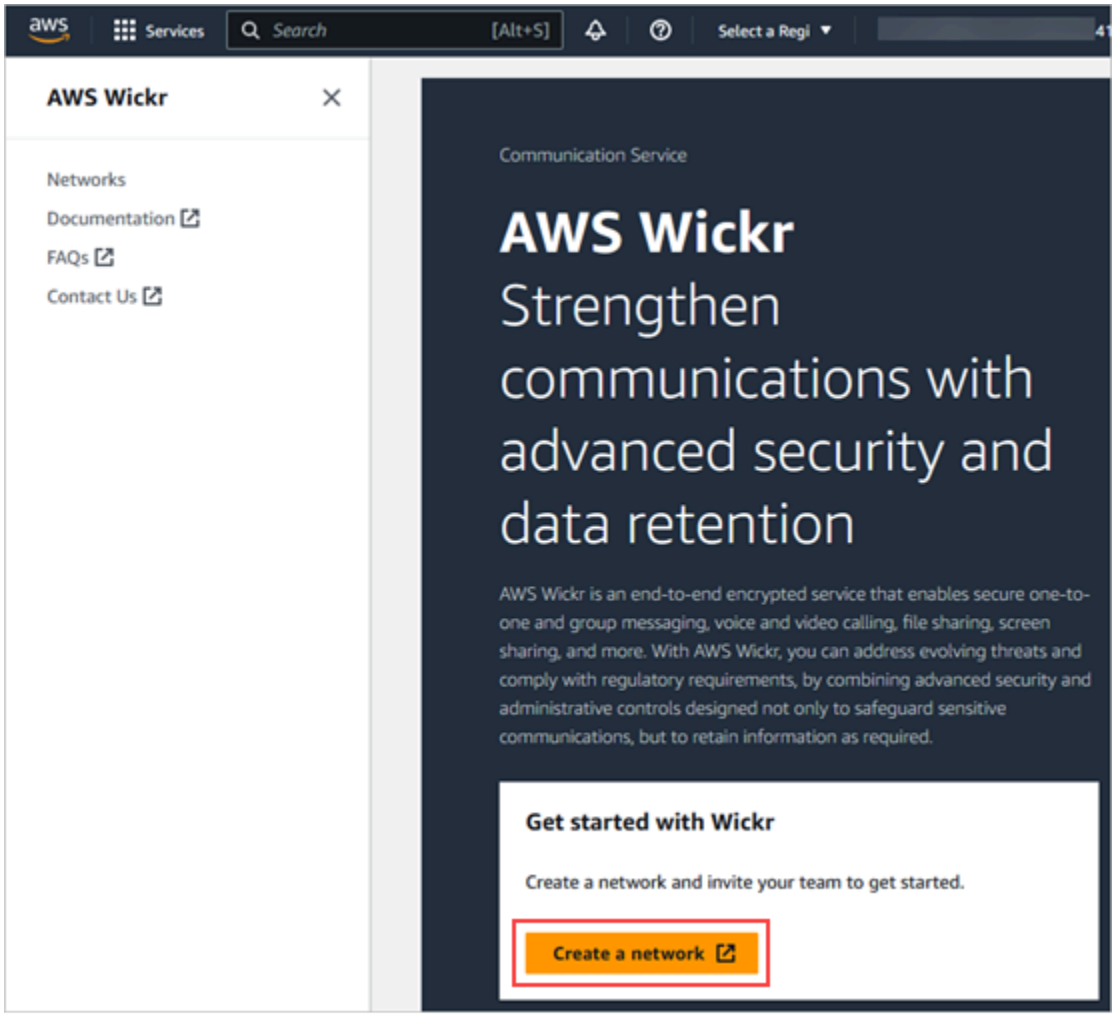
Etapa 1: criar uma rede

Conclua o procedimento a seguir para criar uma rede no Wickr para a sua conta.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.

> **Note**
>
> Se você ainda não criou uma rede do Wickr, você verá a página informativa do serviço Wickr. Depois de criar uma ou mais redes no Wickr, você verá a página Redes, que contém uma exibição em lista de todas as redes que você criou no Wickr.

2. Escolha Criar uma rede.



3. Insira um nome para sua rede na caixa de texto Nome da rede. Escolha um nome que os membros da sua organização reconheçam, como o nome da sua empresa ou o nome da sua equipe.
4. Escolha um plano. Você pode escolher um dos seguintes planos de rede Wickr:

   - Padrão — Para equipes de pequenas e grandes empresas que precisam de flexibilidade e controles administrativos.

- Teste gratuito Premium ou Premium — Para empresas que exigem os mais altos limites de recursos, controles administrativos granulares e retenção de dados.

Os administradores podem escolher a opção de teste gratuito premium, que está disponível para até 30 usuários e dura três meses. Esta oferta está aberta a planos padrão e de teste novos, gratuitos e gratuitos. Os administradores podem fazer upgrade ou downgrade para os planos Premium ou Standard durante o período de teste gratuito premium.

Para obter mais informações sobre os planos e preços do Wickr, consulte a página de preços do Wickr.

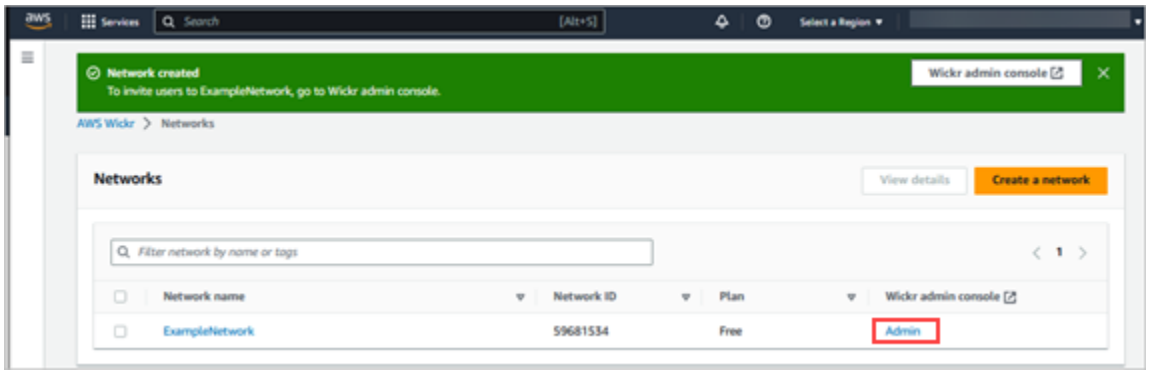
5. (Opcional) Selecione Adicionar nova tag para adicionar uma tag à sua rede. Uma tag consiste em um par chave-valor. As tags podem ser usadas para pesquisar e filtrar recursos ou monitorar seus custos na AWS . Para obter mais informações, consulte Gerenciar tags de rede.
6. Escolha Criar rede.

Você é redirecionado para a página Redes do AWS Management Console for Wickr, e a nova rede será listada na página.

Etapa 2: Configurar sua rede

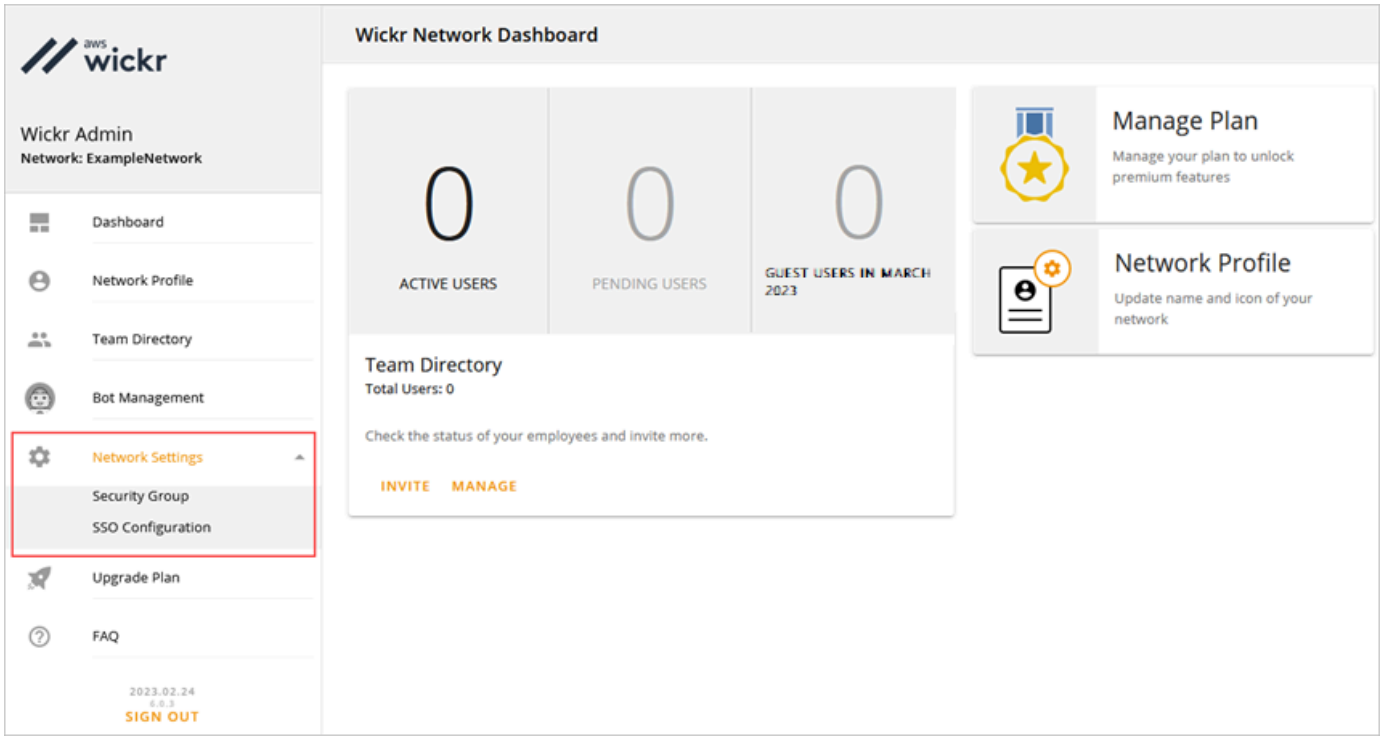
Conclua o procedimento a seguir para acessar o Wickr Admin Console, onde você pode adicionar usuários, adicionar grupos de segurança, configurar o SSO, definir a retenção de dados e outras configurações de rede.

1. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.



Você será redirecionado para o Wickr Admin Console para a rede selecionada.

2. No painel de navegação do Wickr Admin Console, selecione Configurações de rede.



As seguintes opções de configuração de rede estão disponíveis: Para obter mais informações sobre como definir essas configurações, consulte Gerencie sua rede AWS Wickr.

- Grupos de Segurança — gerencia grupos de segurança e suas configurações, como políticas de complexidade de senhas, preferências de mensagens, recursos de chamada, recursos de segurança e federação externa. Para ter mais informações, consulte Grupos de segurança.
- Configuração de SSO — configure o SSO e visualize o endereço do endpoint da sua rede Wickr. O Wickr oferece suporte a provedores de SSO que usam somente o OpenID Connect (OIDC). Não há suporte para provedores que usam Security Assertion Markup Language (SAML). Para ter mais informações, consulte Configuração de autenticação única.

Etapa 3: Criar e convidar usuários

Você pode criar usuários na sua rede do Wickr usando os seguintes métodos:

- Login único — se você configurar o SSO, você poderá convidar usuários compartilhando o ID da sua empresa Wickr. Os usuários finais se registram no Wickr usando o ID da empresa fornecido e seu endereço de e-mail comercial. Para ter mais informações, consulte Configuração de autenticação única.

- Convite — você pode criar usuários manualmente no AWS Management Console para Wickr e receber um convite por e-mail. Os usuários finais podem se registrar no Wickr selecionando o link no e-mail.

> **Note**
>
> Você também pode habilitar usuários convidados para sua rede do Wickr. O recurso de usuário convidado está atualmente em pré-visualização. Para obter mais informações, consulte Usuários convidados.

Siga os seguintes procedimentos para criar ou convidar usuários.

> **Note**
>
> Os administradores também são considerados usuários e devem se convidar para as redes do Wickr com ou sem SSO.

SSO

Escreva e envie um e-mail para os usuários do SSO que devem se inscrever no Wickr. No e-mail, inclua as seguintes informações:

- O ID da sua empresa no Wickr. Ao configurar o SSO, você especifica um ID para a empresa para sua rede Wickr. Para ter mais informações, consulte Configure o SSO.
- O endereço de e-mail que eles devem usar para se inscrever.
- O URL para baixar o cliente Wickr. Os usuários podem baixar os clientes do Wickr na página de downloads do AWS Wickr em https://aws.amazon.com/wickr/download/.

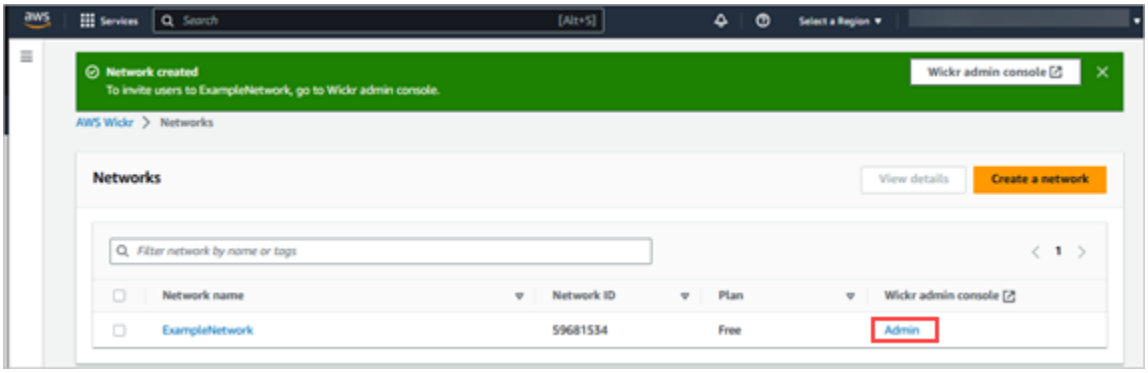
> **Note**
>
> Se você criou sua rede Wickr em AWS GovCloud (Oeste dos EUA), instrua seus usuários a baixar e instalar o cliente. WickrGov Para todas as outras AWS regiões, instrua seus usuários a baixar e instalar o cliente Wickr padrão. Para obter mais informações sobre AWS WickrGov, consulte AWS WickrGovo GuiaAWS GovCloud (US) do usuário.

Conforme os usuários se registram na sua rede do Wickr, eles são adicionados ao diretório da equipe do Wickr com o status ativo.

Non-SSO

Para criar usuários do Wickr manualmente e enviar convites:

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

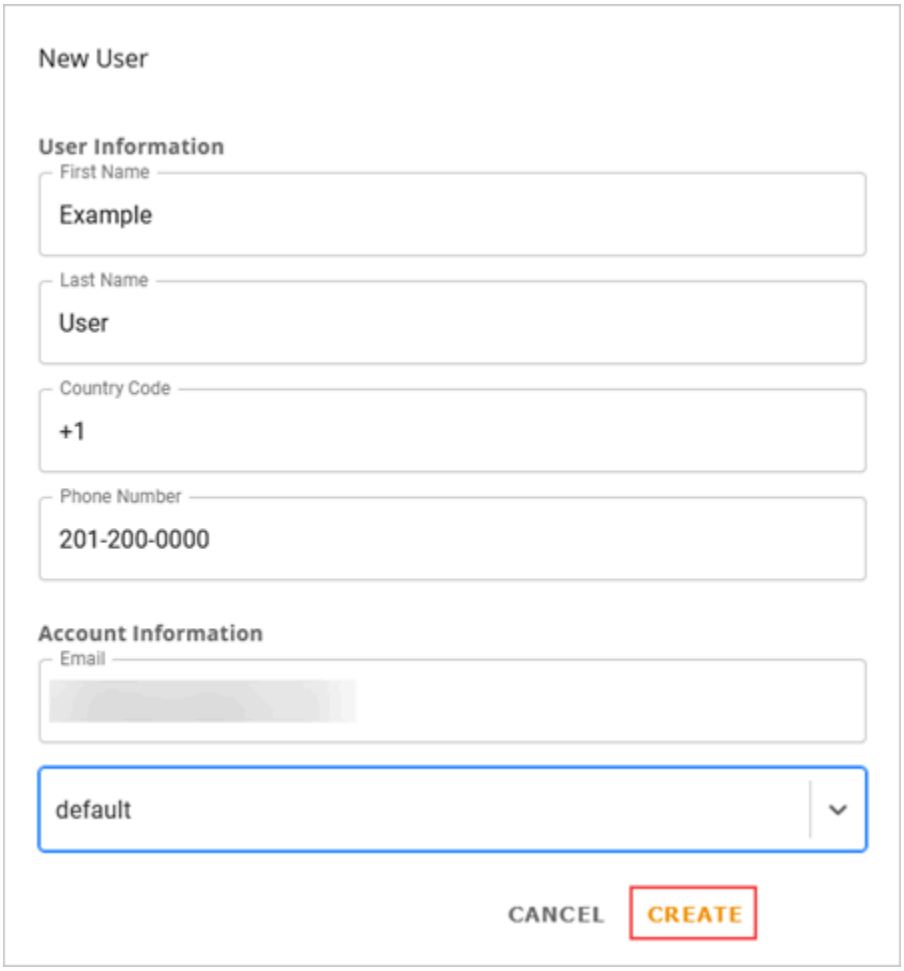


A página Redes.

Você será redirecionado para o Wickr Admin Console de uma rede específica. No Wickr Admin Console, você pode adicionar usuários, adicionar grupos de segurança, configurar o SSO, definir a retenção de dados e configurações adicionais para a rede específica selecionada.

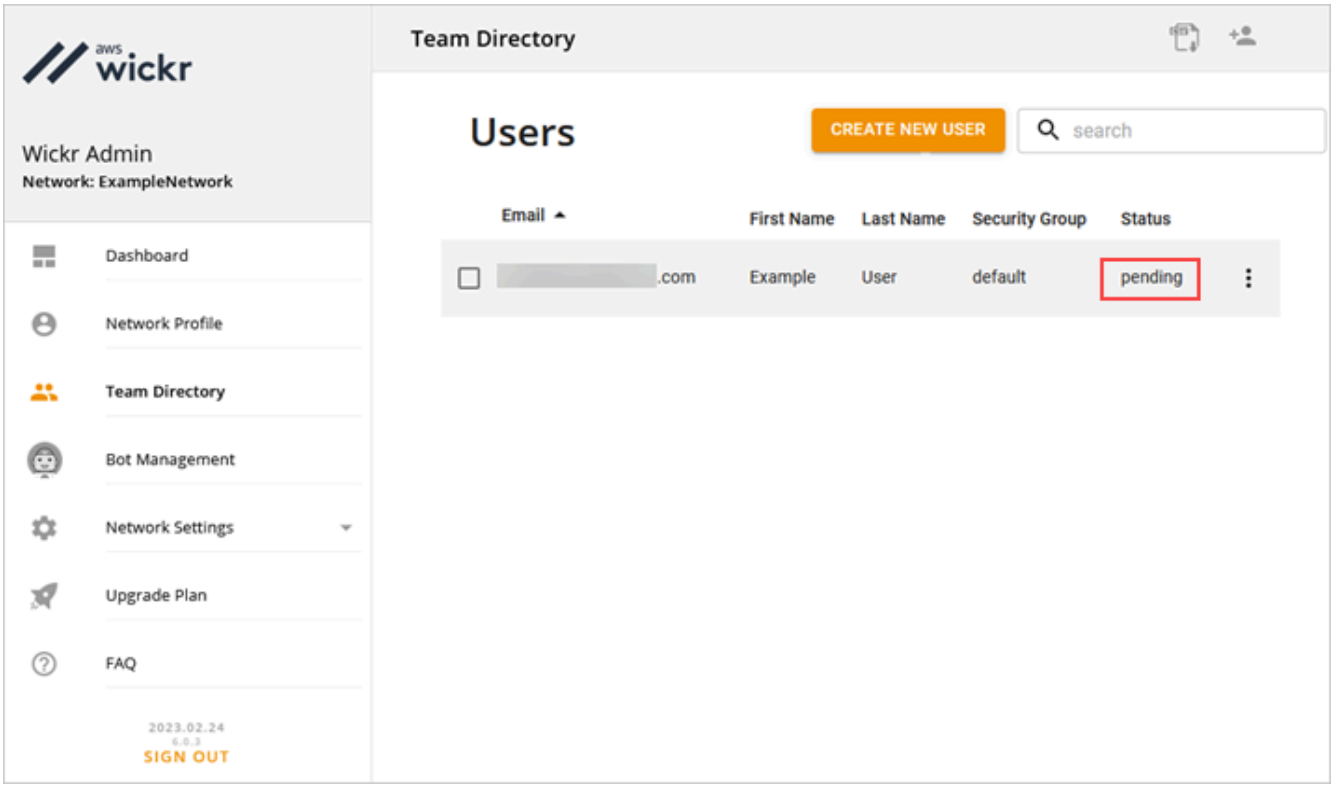
3. No painel de navegação do Wickr Admin Console, selecione Usuários e, em seguida, selecione Diretório da equipe.

   Na página Usuários, você pode adicionar usuários individuais escolhendo Criar novo usuário. Você também pode adicionar usuários em massa escolhendo o ícone Adicionar usuários no painel de navegação superior. Selecione o ícone Download CSV para baixar um modelo de CSV que você pode editar e carregar com sua lista de usuários.
4. Insira o nome, sobrenome, código do país, número de telefone e endereço de e-mail do usuário. O endereço de e-mail é o único campo obrigatório. Certifique-se de escolher o grupo de segurança apropriado para o usuário.
5. Escolha Criar.



O Wickr envia um e-mail de convite para o endereço que você especificar para o usuário. O e-mail fornece links de download para os aplicativos do cliente Wickr e um link para se registrar no Wickr. Para obter mais informações sobre como é essa experiência do usuário final, consulte Baixe o aplicativo Wickr e aceite seu convite no Guia do usuário do AWS Wickr.

Conforme os usuários se cadastram no Wickr usando o link no e-mail, seu status no diretório da equipe do Wickr mudará de Pendente para Ativo.



Próximas etapas

Você concluiu as etapas dos conceitos básicos. Para gerenciar o Wickr, consulte os seguintes guias:

- Gerencie sua rede AWS Wickr
- Gerencie usuários no AWS Wickr

Transfira o Wickr Pro para o AWS Wickr

> **Note**
>
> O Wickr Pro será descontinuado em 27 de março de 2024.

Neste guia, mostraremos como fazer uma migração do Wickr Pro e começar a usar o AWS Wickr.

Siga as etapas deste guia se você tiver uma rede Wickr Pro existente, mas Conta da AWS AINDA NÃO tiver uma. Entre em contato com o suporte em qualquer etapa se precisar de ajuda.

Se sua organização já tiver uma AWS conta, preencha o formulário Migrar do Wickr Pro para o AWS Wickr e o suporte do AWS Wickr o ajudará.

Você precisará de um Conta da AWS ID para gerenciar sua rede AWS Wickr como um AWS service (Serviço da AWS). Para obter mais informações sobre o que Conta da AWS é e como gerenciar a conta, consulte o Guia de referência de gerenciamento deAWS contas.

Tópicos

Etapa 1: criar uma AWS conta

Conclua o procedimento a seguir para criar uma AWS conta.

1. Se sua organização não tiver um ID de conta da AWS existente, você pode começar criando um ID de AWS conta independente. Algumas coisas importantes que você precisará para isso:
   - Um cartão de crédito/débito para cobrança
   - Um endereço de e-mail que pode ser acessado por um grupo (recomendado, não obrigatório)
   - Selecione um AWS Support plano. Para obter mais informações, consulte Alterando planos AWS Support.

   > **Note**
   >
   > Você sempre pode alterar seu AWS Support plano à medida que aprende mais sobre suas necessidades.

2. Configure o acesso administrativo por meio do IAM como uma prática recomendada de segurança (opcional, mas recomendada). Para obter mais informações, consulte Gerenciamento de identidadeAWS e acesso. Para obter instruções mais específicas sobre o acesso administrativo do AWS Wickr, consulte a políticaAWS gerenciada: AWSWickrFullAccess.
3. Depois de concluir as etapas anteriores, você poderá fazer login no AWS Management Console para encontrar seu Conta da AWS ID de 12 dígitos abaixo do nome da sua conta.

Etapa 2: Recuperar seu ID de rede do Wickr

Siga o procedimento a seguir para recuperar seu ID na rede do Wickr.

1. Faça o login no console de administração atual do Wickr, selecione a(s) rede(s) que você deseja migrar e selecione Perfil de rede.
2. A página Perfil de rede exibe seu ID da rede e é um ID numérico de 8 dígitos.

Etapa 3: Enviar uma solicitação

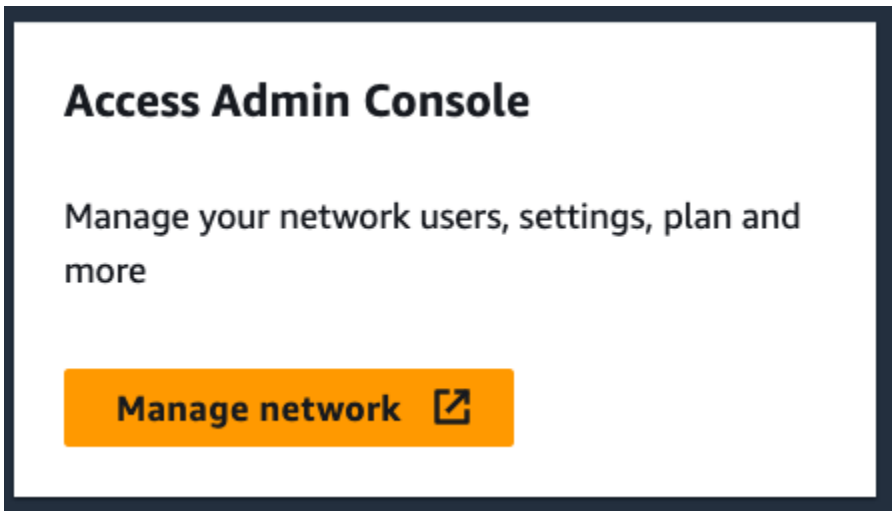
Agora que você tem seu Conta da AWS ID e ID de rede do Wickr Pro, você precisará preencher o formulário Migrar do Wickr Pro para o AWS Wickr.

Quando concluído, normalmente dentro de 14 dias, um representante de suporte do AWS Wickr entrará em contato com você para confirmar que sua rede Wickr foi adicionada à sua Conta da AWS.

Etapa 4: Faça login no seu AWS console

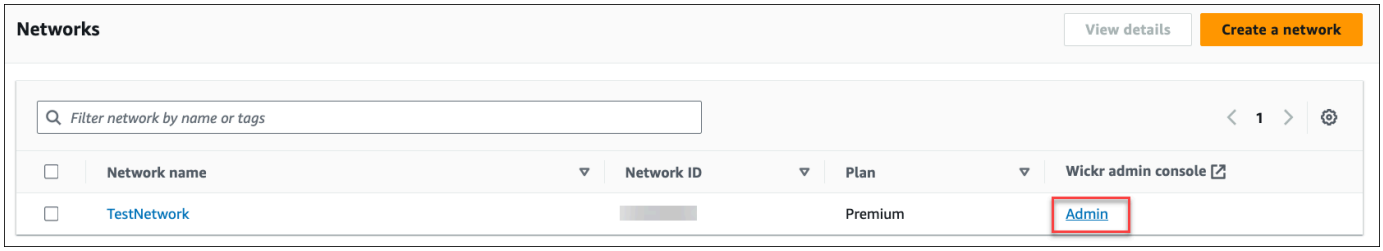
> **Note**
>
> Siga estas etapas DEPOIS de receber a confirmação de que sua rede Wickr Pro foi adicionada à sua Conta da AWS.

1. Você pode fazer login no AWS console como usuário root OU com um usuário do IAM que você criou anteriormente (conforme recomendado) na Etapa 2 para o AWS Wickr.
2. Navegue até seu serviço AWS Wickr. Você pode fazer isso no menu Serviços ou pesquisando por AWS Wickr na barra de pesquisa.
3. Na página do AWS Wickr, selecione Gerenciar rede para acessar sua lista de redes do Wickr.



O botão Gerenciar rede.

4. Na página Redes, na coluna do console de administração do Wickr, selecione o link Admin à direita do nome da rede desejada.



O link de administração do console.

5. Agora a transferência está concluída! Você verá seu painel de rede Wickr.

A cobrança da sua rede agora será transferida para sua Conta da AWS. Aguarde até 3 dias úteis para que o suporte entre em contato com uma confirmação. Depois de receber sua confirmação, você poderá visualizar e pagar sua fatura pelo AWS console.

Gerencie sua rede AWS Wickr

Na seção Configurações de rede do Wickr, você pode gerenciar o AWS Management Console nome da rede Wickr, os grupos de segurança, a configuração de SSO e as configurações de retenção de dados.

Tópicos

Perfil de rede

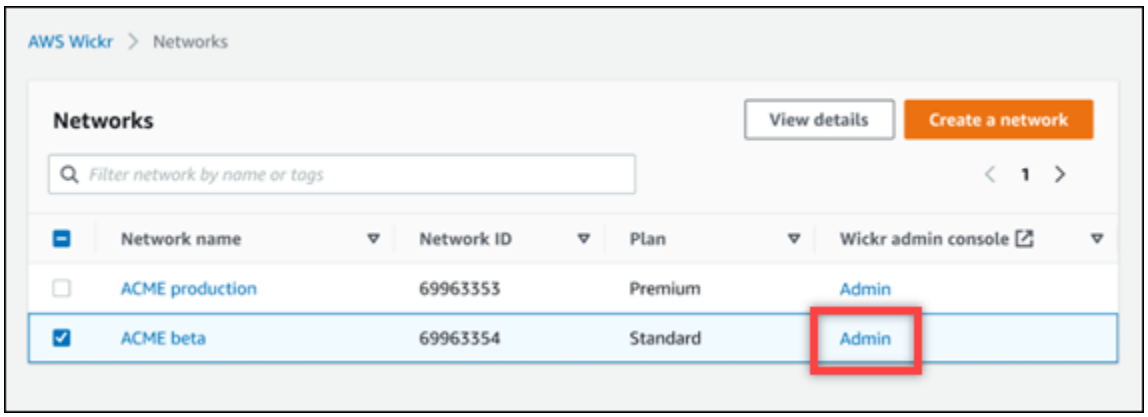
Você pode editar o nome da sua rede Wickr e visualizar seu ID de rede na seção Perfil de rede do AWS Management Console for Wickr.

Tópicos

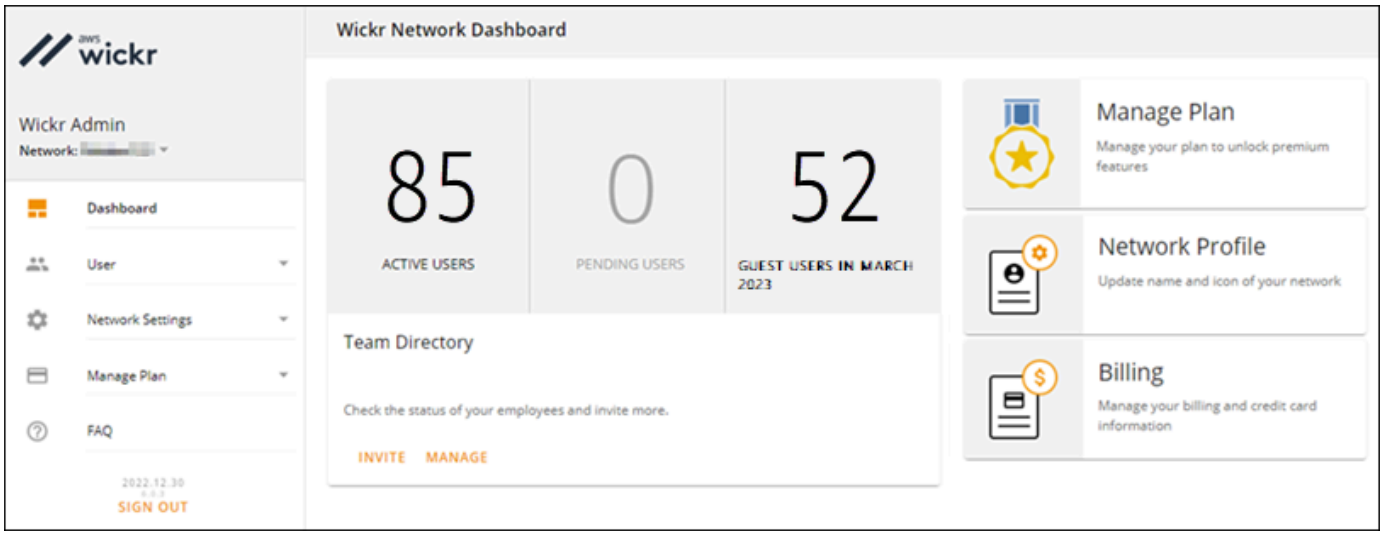
Visualize perfil de rede

Conclua o procedimento a seguir para visualizar seu perfil de rede e ID rede Wickr.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.



Você será redirecionado para o Wickr Admin Console de uma rede específica.



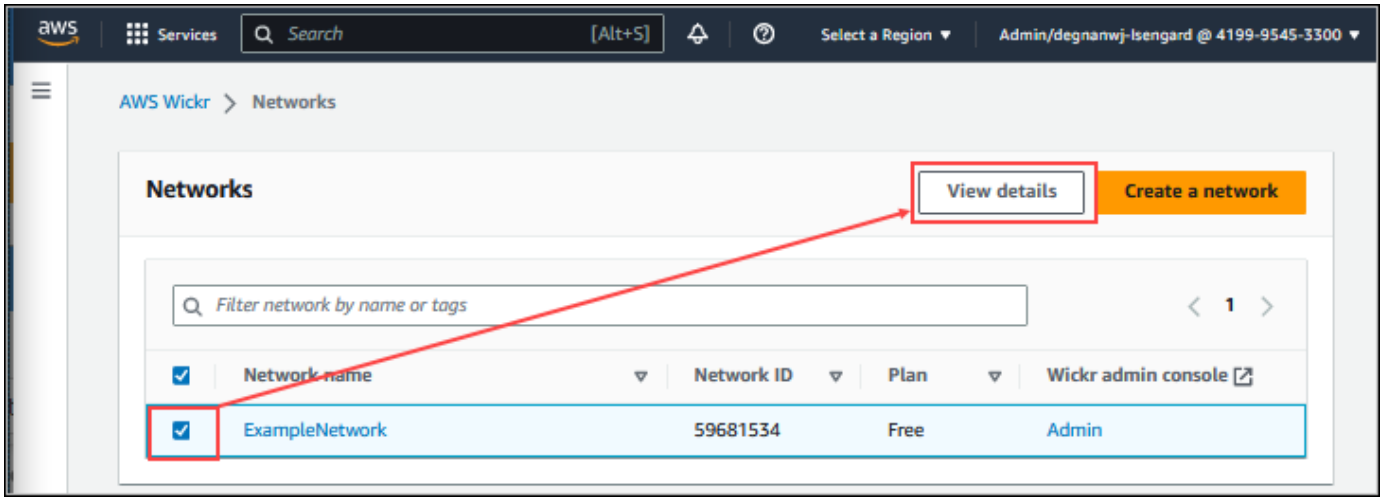
3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Perfil de rede.

   A página Perfil de Rede exibe o nome e o ID da rede do Wickr. Você pode usar o ID da rede para configurar a federação.

Editar nome da rede

Siga o procedimento a seguir para editar seu nome na rede do Wickr.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Escolha Gerenciar rede.
3. Na página Redes, marque a caixa de seleção ao lado do nome da rede que você deseja editar e escolha Exibir detalhes.



4. Na seção Visão geral de redes, selecione Editar.
5. Insira o nome de sua rede na caixa de texto Nome da rede.
6. Escolha Salvar alterações para salvar seu novo nome de rede.

Grupos de segurança

Na seção Grupos de Segurança do AWS Management Console Wickr, você pode gerenciar grupos de segurança e suas configurações, como políticas de complexidade de senhas, preferências de mensagens, recursos de chamada, recursos de segurança e federação de rede.

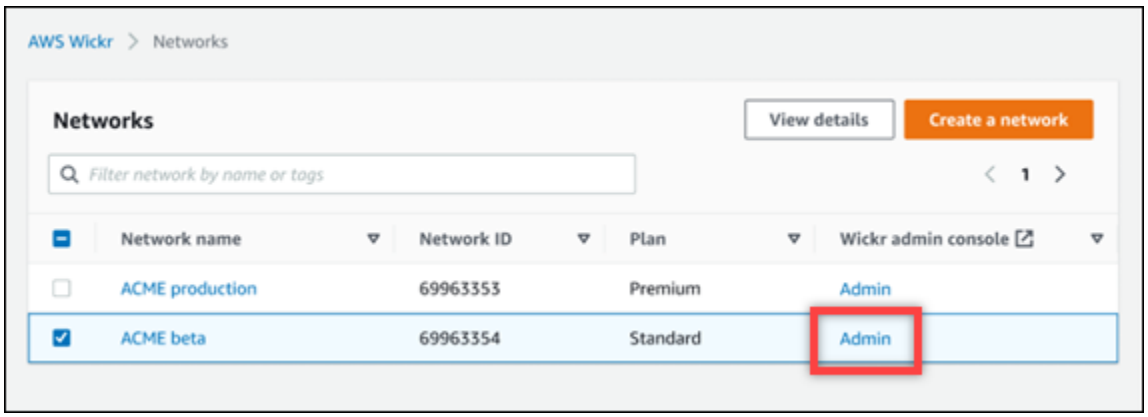
Tópicos

- Visualize grupos de segurança
- Criar um grupo de segurança
- Edite um grupo de segurança
- Exclua um grupo de segurança

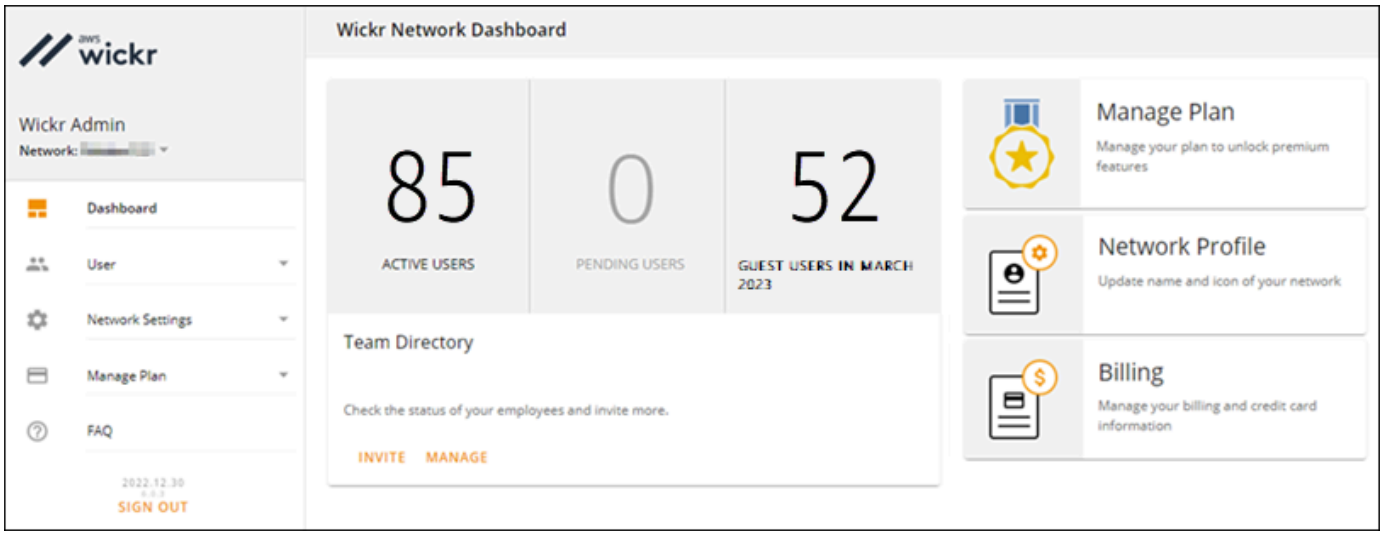
Visualize grupos de segurança

Realize o procedimento a seguir para exibir grupos de segurança.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.



Você será redirecionado para o Wickr Admin Console de uma rede específica.



3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Grupo de segurança.

   A página Grupos de Segurança exibe seus grupos de segurança atuais do Wickr e oferece a opção de visualizar seus detalhes ou criar um novo grupo.

Criar um grupo de segurança

Realize o procedimento a seguir para criar um grupo de segurança.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

   Você será redirecionado para o Wickr Admin Console de uma rede específica.

3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Grupo de segurança.
4. Escolha Novo grupo para criar um novo grupo de segurança.

   Um novo grupo de segurança com um nome padrão é automaticamente adicionado à lista de grupos de segurança.

   Para obter mais informações sobre editar o novo grupo de segurança, consulte Edite um grupo de segurança.

Edite um grupo de segurança

Realize o procedimento a seguir para editar um grupo de segurança.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

   Você será redirecionado para o Wickr Admin Console de uma rede específica.
3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Grupo de segurança.
4. Escolha Detalhes ao lado do nome do grupo de segurança que você deseja editar.

   A página Detalhes do grupo de segurança exibe as configurações do grupo de segurança em guias diferentes.
5. As seguintes guias e configurações correspondentes estão disponíveis:

   - Nome do grupo de segurança — Escolha o ícone de lápis ao lado do nome do grupo para editar o nome do grupo.
   - Geral — Edite a configuração básica do grupo.
   - Mensagens — Gerencie os recursos de mensagens para membros do grupo.
   - Chamadas — Gerencie os recursos de chamada para membros do grupo.
   - Segurança — Configure recursos de segurança adicionais para o grupo.
   - Federação — A capacidade de se comunicar entre redes. Isso pode ser configurado no Admin Console para uma rede no nível do grupo de segurança. O AWS Wickr tem dois tipos de federação: local e global.

- Federação local — A capacidade de se federar com usuários da AWS em outras redes na mesma região. Por exemplo, se houver duas redes no Canadá com a federação local ativada, elas poderão se comunicar entre si.
- Federação global — A capacidade de federar com usuários corporativos ou AWS usuários de uma rede diferente que pertençam a outras regiões. Por exemplo, se houver um usuário em uma rede na região do Canadá e um usuário em uma rede na região de Londres e a federação global estiver ativada para ambas as redes, eles poderão se comunicar entre si.
- Federação restrita — A capacidade de federar com redes específicas (Enterprise ou AWS) pertencentes a diferentes regiões. Os administradores podem listar redes específicas com as quais seus usuários podem se federar. Após a restrição, os usuários só podem se comunicar com usuários nas redes listadas como permitidas. Ambas as redes devem se autorizar mutuamente a partir das configurações do grupo de segurança na guia federação para usar a federação restrita.

6. Escolha Salvar para salvar as edições feitas nos detalhes do grupo de segurança.

Exclua um grupo de segurança

Realize o procedimento a seguir para excluir um grupo de segurança.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

   Você será redirecionado para o Wickr Admin Console de uma rede específica.
3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Grupo de segurança.
4. Escolha o ícone de reticências verticais ao lado do nome do grupo de segurança que você deseja excluir.
5. Escolha Remover para excluir grupo de segurança.

   Quando você exclui um grupo de segurança que tem usuários atribuídos, esses usuários são automaticamente adicionados ao grupo de segurança padrão. Para modificar o grupo de segurança atribuído aos usuários, consulte Editar usuários.

Configuração de autenticação única

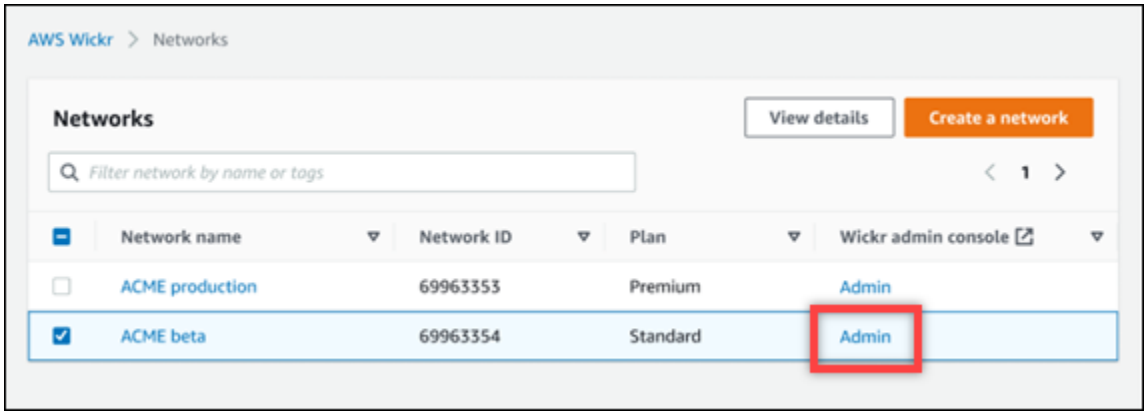
Na seção Configuração de SSO do AWS Management Console para Wickr, você pode configurar o Wickr para usar um sistema de login único para autenticar. O SSO fornece uma camada adicional de segurança quando combinado com um sistema de autenticação multifator (MFA) apropriado. O Wickr oferece suporte a provedores de SSO que usam somente o OpenID Connect (OIDC). Não há suporte para provedores que usam Security Assertion Markup Language (SAML).

Tópicos

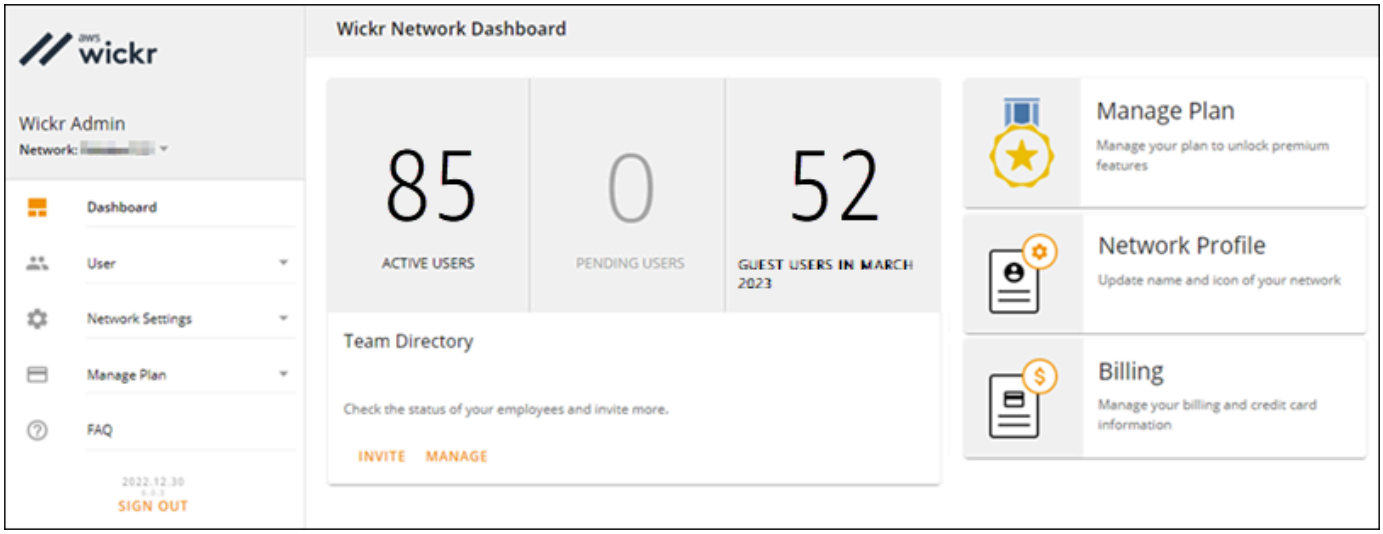
Visualize detalhes do SSO

Realize o procedimento a seguir para visualizar a configuração atual de autenticação única para a sua rede Wickr, se houver. Você também pode visualizar o endpoint de rede da sua rede Wickr.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.



Você será redirecionado para o Wickr Admin Console de uma rede específica.



3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Configuração de SSO.

   A página Single Sign-on e Configuração LDAP exibe seu endpoint de rede Wickr e a configuração atual de SSO.

Configure o SSO

Para obter mais informações sobre como configurar o SSO, consulte os seguintes guias na Central de Ajuda do Wickr:

> **Important**
>
> Ao configurar o SSO, você especifica um ID da empresa para sua rede Wickr. Certifique-se de anotar o ID da empresa da sua rede Wickr. Você deve fornecê-lo aos seus usuários finais ao enviar e-mails de convite. Os usuários finais devem especificar o ID da empresa ao se registrarem na sua rede Wickr.

- Configure o autenticação única do Azure AD
- Configure o login único do Okta

Período de carência para atualização do token

Ocasionalmente, pode haver casos em que os provedores de identidade enfrentem interrupções temporárias ou prolongadas, o que pode fazer com que seus usuários sejam desconectados inesperadamente devido a uma falha no token de atualização da sessão do cliente. Para evitar esse problema, você pode estabelecer um período de carência que permita que seus usuários permaneçam conectados mesmo que o token de atualização do cliente falhe durante essas interrupções.

Aqui estão as opções disponíveis para o período de carência:

- Sem período de carência (padrão): os usuários serão desconectados imediatamente após uma falha na atualização do token.
- Período de carência de 30 minutos: os usuários podem permanecer conectados por até 30 minutos após uma falha no token de atualização.
- Período de carência de 60 minutos: os usuários podem permanecer conectados por até 60 minutos após uma falha no token de atualização.

Gerencie tags de rede

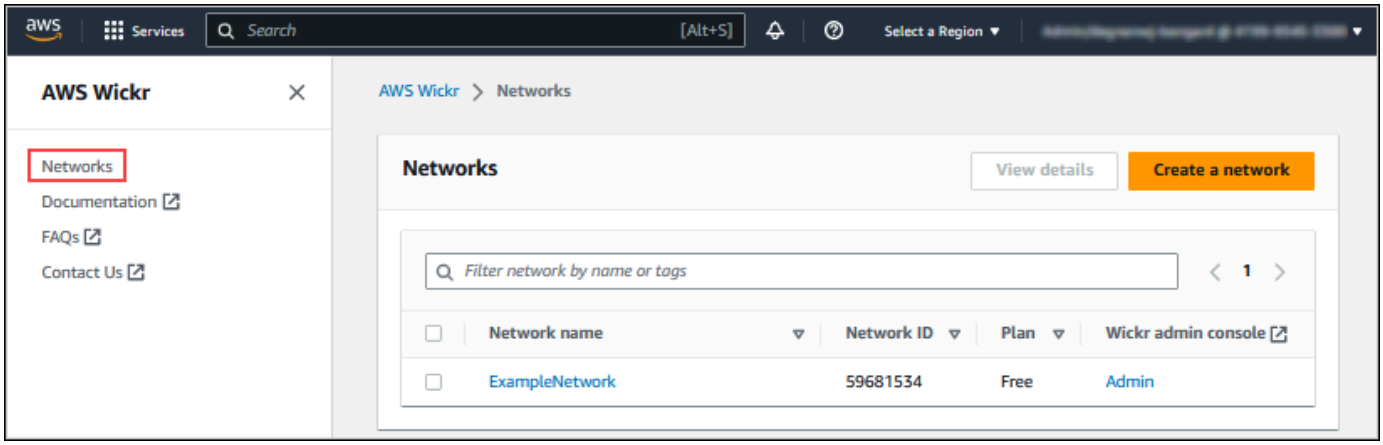
Você pode aplicar tags às redes do Wickr. Você pode então usar essas tags para pesquisar e filtrar suas redes Wickr ou rastrear seus AWS custos. Você pode configurar tags de rede na página de visão geral da rede do AWS Management Console for Wickr.

Uma tag é um par de valores-chave aplicado a um recurso para armazenar metadados sobre esse recurso. Cada tag é um rótulo que consiste em um valor e uma chave. Para obter mais informações sobre tags, consulte também O que são tags? e marcando casos de uso.

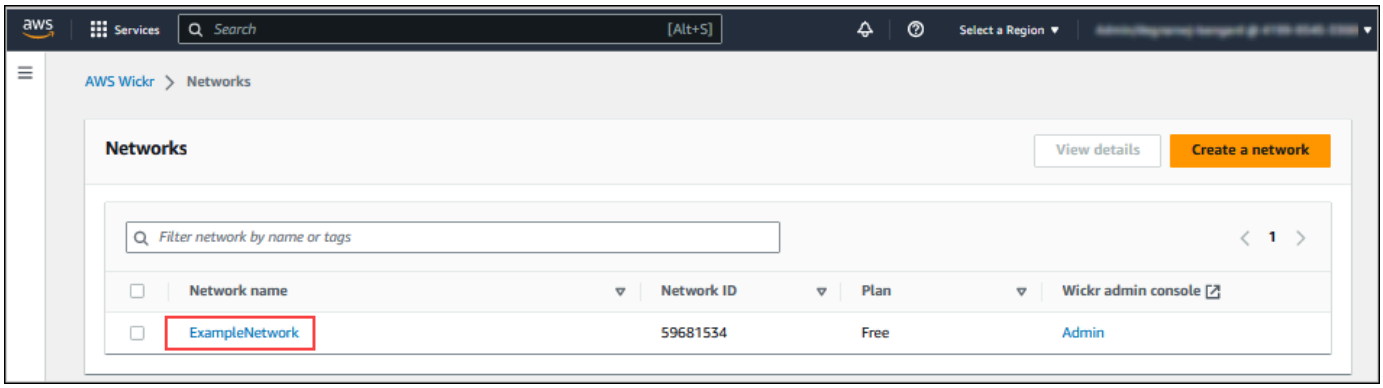
Gerencie tags de rede

Conclua o procedimento a seguir para gerenciar tags de rede para a sua rede Wickr.

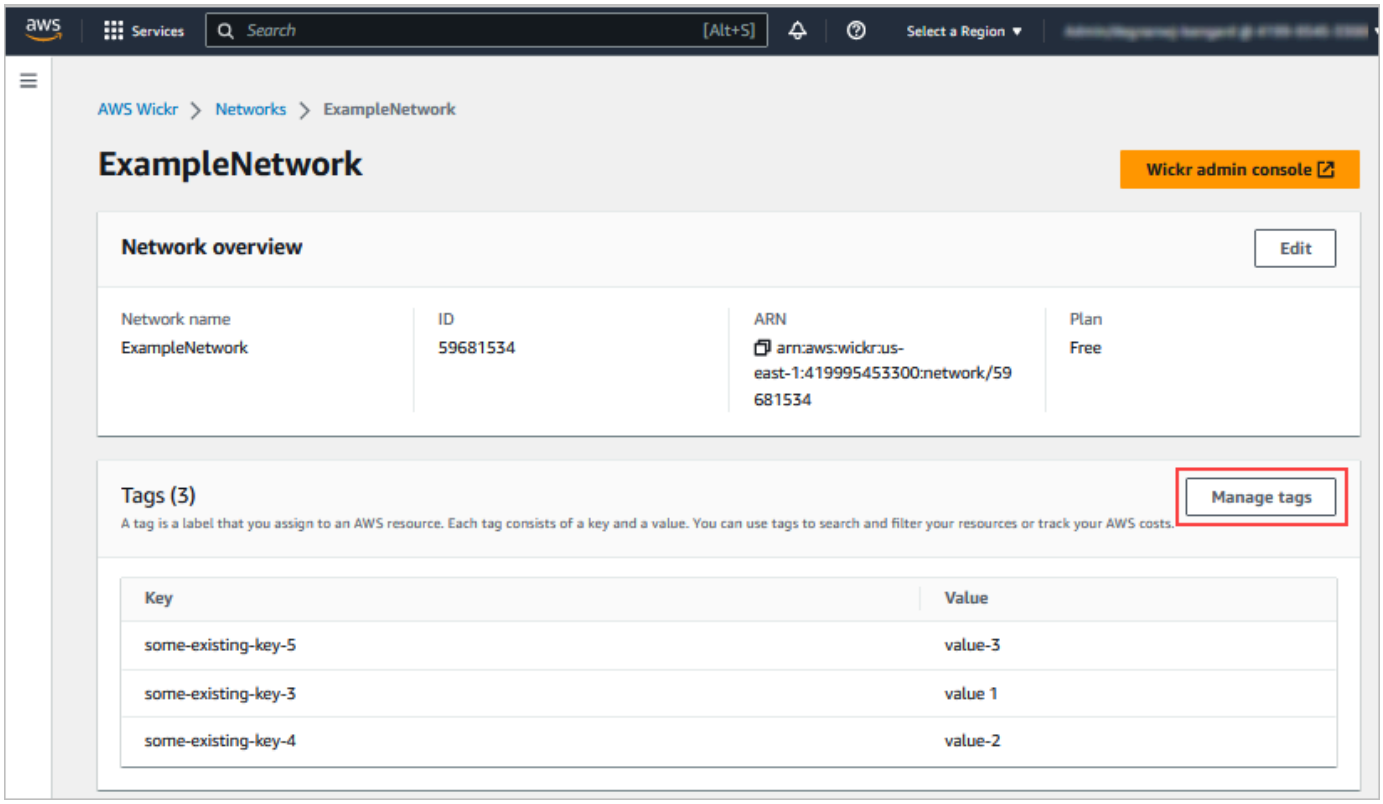
1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Selecione Redes no painel de navegação do AWS Management Console para Wickr.



3. Na página Redes, selecione o nome da rede para a qual você deseja gerenciar tags.



4. Na página Visão geral da rede, escolha Gerenciar tags.



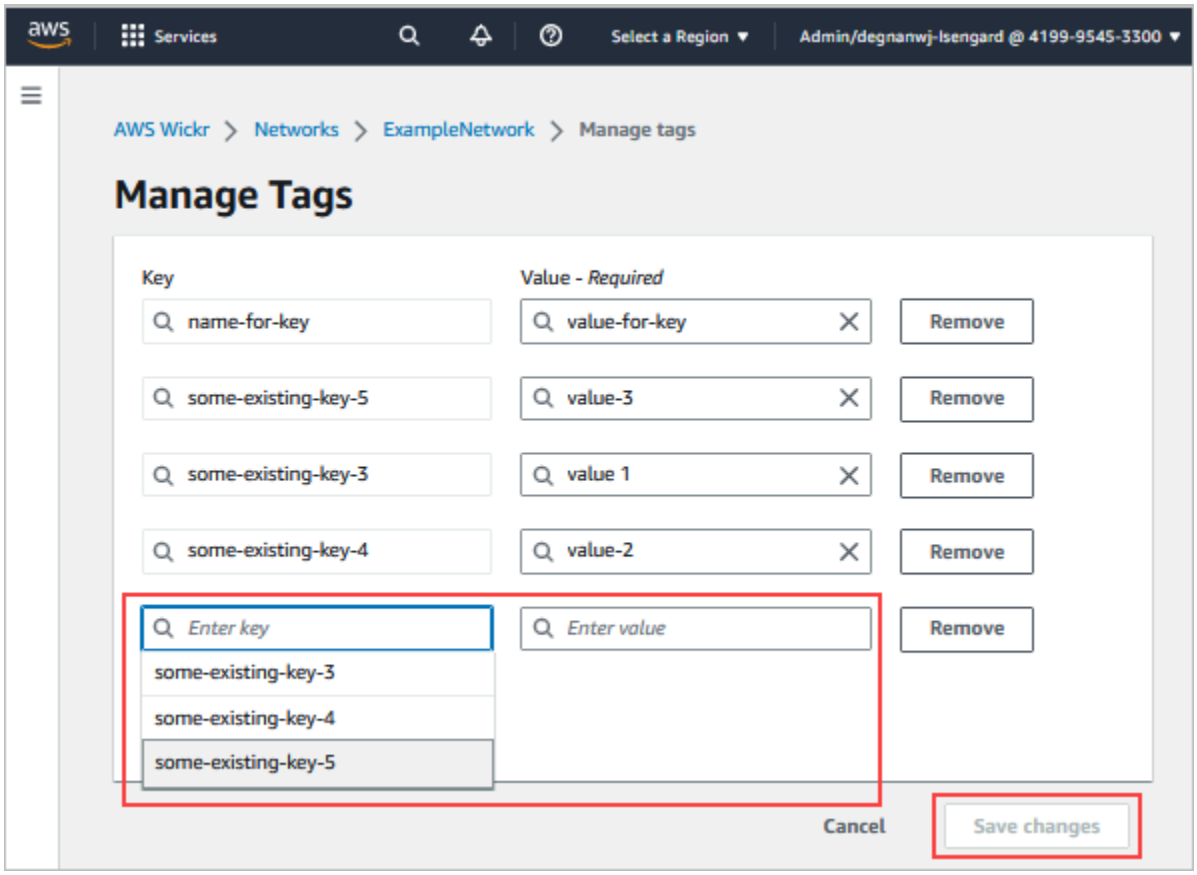
5. Na página Gerenciar tags, você pode concluir uma das seguintes opções:

   - Adicione novas tags — Insira novas tags na forma de um par de chaves e valores. Escolha Adicionar nova tag para adicionar vários pares de valores-chave. As tags diferenciam letras maiúsculas de minúsculas. Para ter mais informações, consulte Adicione um tag de rede.
   - Edite tags existentes — Selecione o texto da chave ou do valor de uma tag existente e, em seguida, insira a modificação na caixa de texto. Para ter mais informações, consulte Edite uma tag de rede.
   - Remove tags existentes — Escolha o botão Remover que está listado ao lado da tag que você deseja excluir. Para ter mais informações, consulte Remova uma marcação de rede.

Adicione um tag de rede

Conclua o procedimento a seguir para adicionar uma tag de rede a sua rede Wickr. Para obter mais informações sobre gerenciamento de tags, consulte Gerencie tags de rede.

1. Na página Gerenciar tags, escolha Adicionar nova tag.
2. Nos campos Chave e Valor em branco que aparecem, insira a nova chave e o valor da tag.
3. Escolha Salvar alterações para salvar o limite.

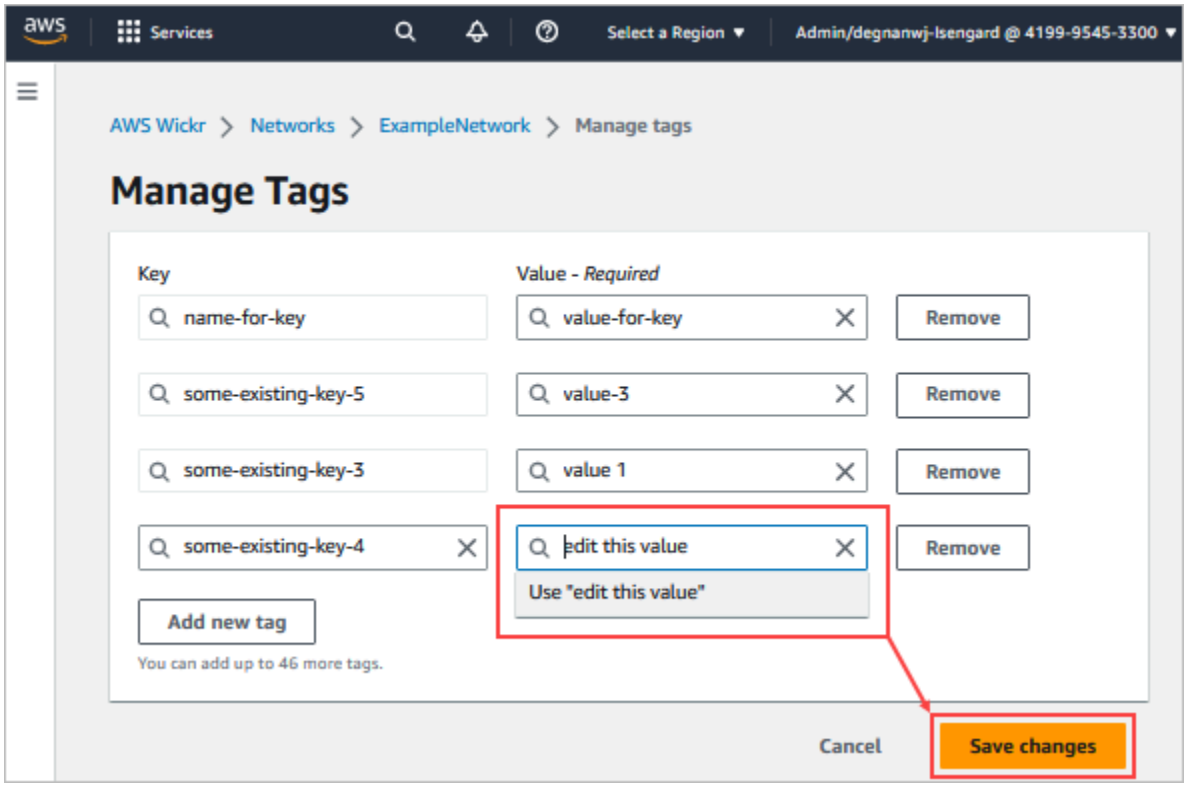


Edite uma tag de rede

Conclua o procedimento a seguir para editar uma tag de rede associada à sua rede Wickr. Para obter mais informações sobre gerenciamento de tags, consulte Gerencie tags de rede.

1. Na página Gerenciar tags, edite o valor de uma tag.

> **Note**
>
> Não é possível editar a chave de uma tag. Em vez disso, remova o par de chave e valor e adicione uma nova tag usando a nova chave.

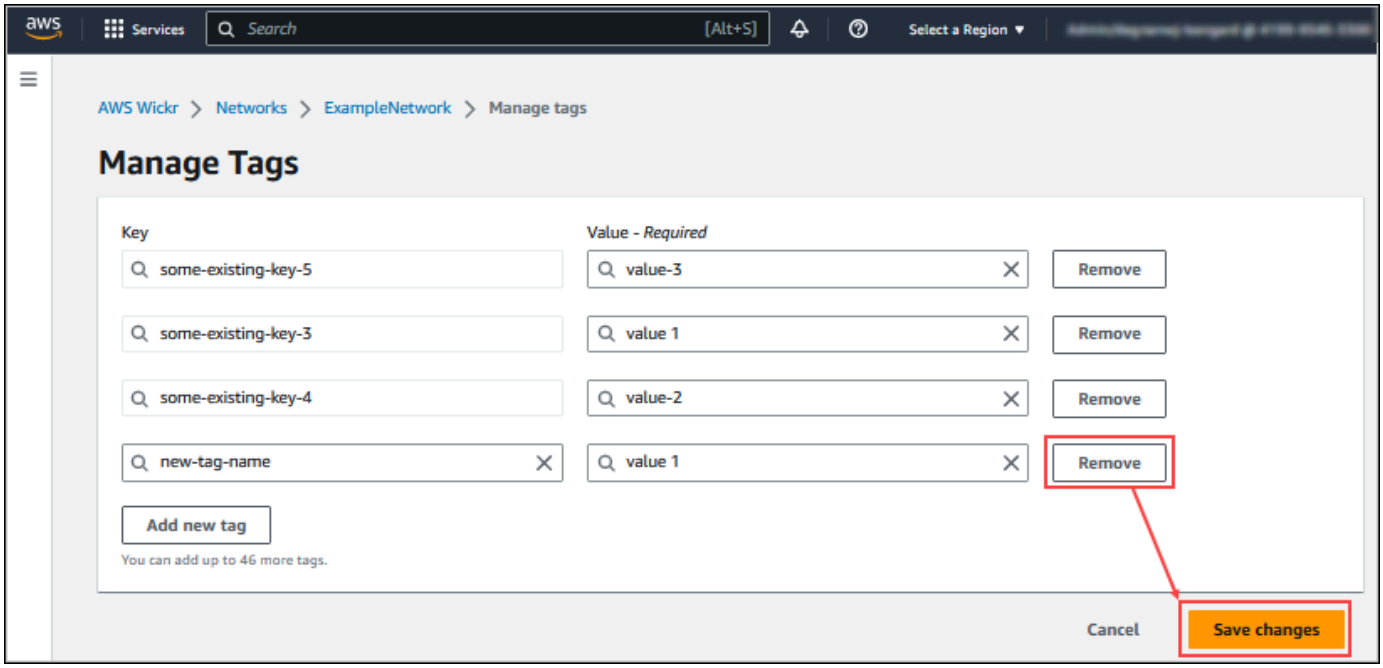


2. Escolha Salvar alterações para salvar as edições.

Remova uma marcação de rede

Conclua o procedimento a seguir para remover uma tag de rede da sua rede Wickr. Para obter mais informações sobre gerenciamento de tags, consulte Gerencie tags de rede.

1. Na página Gerenciar tags, escolha Remover ao lado da tag que você deseja remover.



2. Escolha Salvar alterações para salvar as edições.

Gerenciar plano de rede

Na seção Gerenciar plano do AWS Management Console Wickr, você pode gerenciar seu plano de rede com base nas necessidades de sua empresa.

Para gerenciar seu plano de rede, conclua o procedimento a seguir.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. No painel de navegação do Wickr Admin Console, escolha Gerenciar plano e, em seguida, escolha Meu plano.
3. Na página Meu plano, escolha o plano de rede desejado. Você pode modificar seu plano de rede atual escolhendo uma das seguintes opções:

   - Padrão — Para equipes de pequenas e grandes empresas que precisam de flexibilidade e controles administrativos.
   - Teste gratuito Premium ou Premium — Para empresas que exigem os mais altos limites de recursos, controles administrativos granulares e retenção de dados.

     Os administradores podem escolher a opção de teste gratuito premium, que está disponível para até 30 usuários e dura três meses. Esta oferta está aberta a planos padrão e de teste

novos, gratuitos e gratuitos. Os administradores podem fazer upgrade ou downgrade para os planos Premium ou Standard durante o período de teste gratuito premium.

> **Note**
>
> Para interromper o uso e o faturamento na sua rede, remova todos os usuários, incluindo os usuários suspensos da sua rede.

Limitações do teste gratuito premium

As seguintes limitações se aplicam ao teste gratuito premium:

- Se um plano já tiver sido inscrito em um teste gratuito premium antes, ele não estará qualificado para outro teste.
- Somente uma rede para cada AWS conta pode ser inscrita em um teste gratuito premium.
- O recurso de usuário convidado não está disponível durante o teste gratuito premium.
- Se uma rede padrão tiver mais de 30 usuários, não será possível fazer o upgrade para um teste gratuito premium.

Retenção de dados

A retenção de dados do AWS Wickr pode reter todas as conversas na rede. Isso inclui conversas por mensagem direta e conversas em grupos ou salas entre membros da rede (internos) e aqueles com outras equipes (externas) com as quais sua rede está federada. A retenção de dados só está disponível para usuários do plano AWS Wickr Premium e clientes corporativos que optarem pela retenção de dados. Para obter mais informações sobre o plano Premium, consulte Preços do Wickr

Quando um administrador de rede configura e ativa a retenção de dados para sua rede, todas as mensagens e arquivos compartilhados em sua rede são retidos de acordo com as políticas de conformidade da organização. Essas saídas de arquivo.txt podem ser acessadas pelo administrador da rede em um local externo (por exemplo: armazenamento local, bucket do Amazon S3 ou qualquer outro armazenamento conforme a escolha do usuário), de onde podem ser analisadas, apagadas ou transferidas.

> **Note**
>
> O Wickr nunca acessa suas mensagens e arquivos. Portanto, é sua responsabilidade configurar um sistema de retenção de dados.

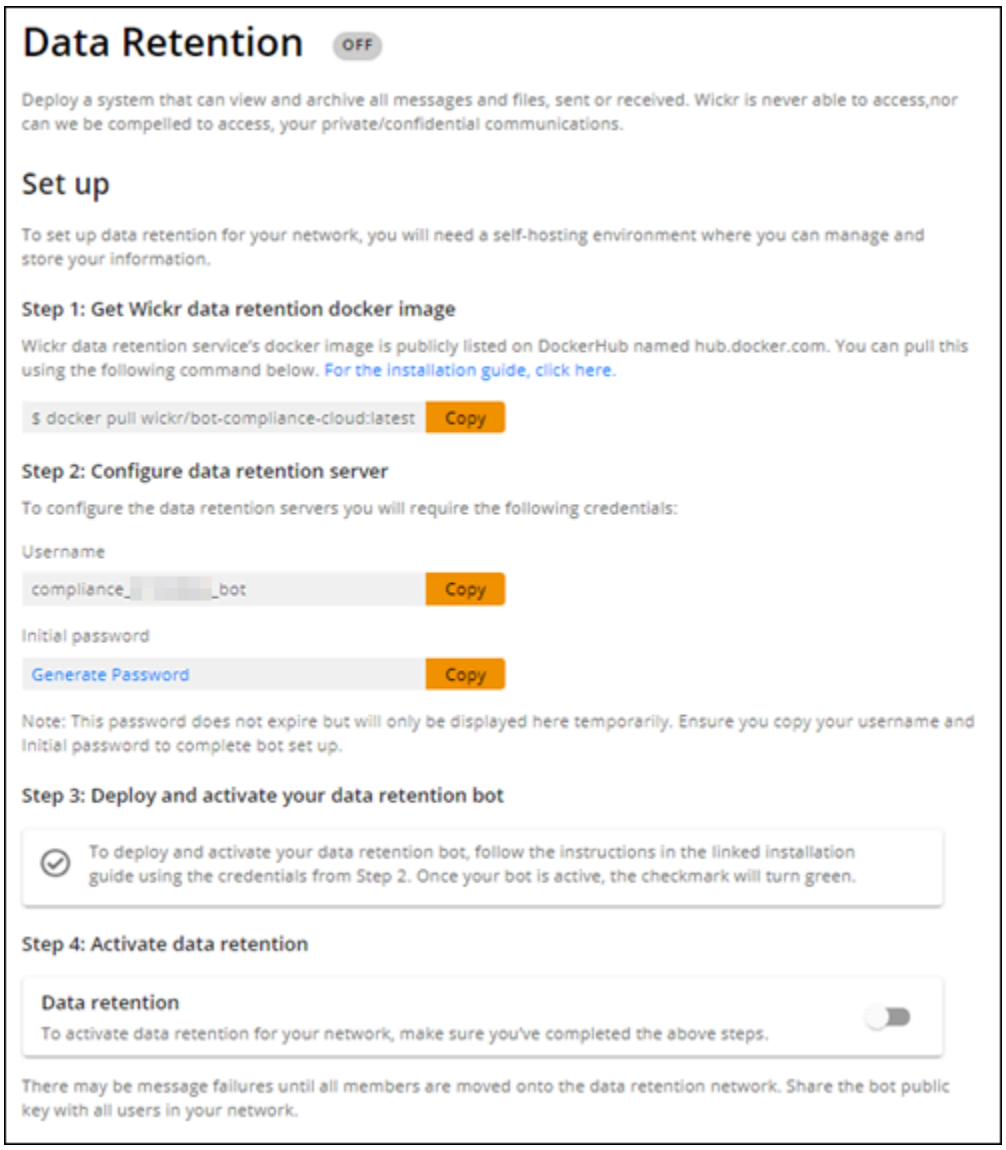
Tópicos

Visualizar detalhes da retenção de dados

Conclua o procedimento a seguir para visualizar os detalhes de retenção de dados da sua rede Wickr. Você também pode habilitar ou desabilitar a retenção de dados para a sua rede Wickr.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Escolha Gerenciar rede.
3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Retenção de dados.

   A página Retenção de dados exibe as etapas para configurar a retenção de dados e a opção de ativar ou desativar o recurso de retenção de dados. Para obter mais informações sobre como configurar a retenção de dados, consulte Configure a retenção de dados.



> **Note**
>
> Quando a retenção de dados for ativada, uma mensagem Retenção de dados ativada ficará visível para todos os usuários em sua rede, informando-os sobre a rede habilitada para retenção.

Configure a retenção de dados

Para configurar a retenção de dados para sua rede AWS Wickr, você deve implantar a imagem do Docker do bot de retenção de dados em um contêiner em um host, como um computador local ou

uma instância no Amazon Elastic Compute Cloud (Amazon EC2). Depois que o bot for implantado, você poderá configurá-lo para armazenar dados localmente ou em um bucket do Amazon Simple Storage Service (Amazon S3). Você também pode configurar o bot de retenção de dados para usar outros AWS serviços como AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) e (). AWS Key Management Service AWS KMS Os tópicos a seguir descrevem como configurar e executar o bot de retenção de dados para sua rede do Wickr.

Tópicos

Pré-requisitos para configurar a retenção de dados

Antes de começar, você deve obter o nome do bot de retenção de dados (rotulado como Nome do usuário) e a senha inicial do AWS Management Console para Wickr. Você deve especificar esses dois valores na primeira vez em que iniciar o bot de retenção de dados. Você também deve ativar a retenção de dados no console. Para ter mais informações, consulte Visualizar detalhes da retenção de dados.

Senha

Na primeira vez que você inicia o bot de retenção de dados, você deve especificar a senha inicial usando uma das seguintes opções:

- A variável de ambiente `WICKRIO_BOT_PASSWORD`. As variáveis de ambiente do bot de retenção de dados são descritas na seção Variáveis de ambiente, mais para frente neste guia.
- O valor da senha no Secrets Manager identificado pela variável de ambiente `AWS_SECRET_NAME`. Os valores do Secrets Manager para o bot de retenção de dados estão descritos na seção Valores do Secrets Manager, mais para frente neste guia.

- Digite a senha quando solicitado pelo bot de retenção de dados. Você precisará executar o bot de retenção de dados com acesso TTY interativo usando a opção `-ti`.

Uma nova senha será gerada quando você configurar o bot de retenção de dados pela primeira vez. Se precisar reinstalar o bot de retenção de dados, use a senha gerada. A senha inicial não é válida após a instalação inicial do bot de retenção de dados.

A nova senha gerada será exibida conforme mostrado no exemplo a seguir.

> **Important**
>
> Salve a senha em um lugar seguro. Se você perder a senha, você não poderá reinstalar o bot de retenção de dados. Não compartilhe essa senha. Ela fornece a capacidade de iniciar a retenção de dados para sua rede do Wickr.

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

Opções de armazenamento

Depois que a retenção de dados for ativada e o bot de retenção de dados estiver configurado para sua rede do Wickr, ele capturará todas as mensagens e arquivos enviados dentro de sua rede. As mensagens são salvas em arquivos limitados a um tamanho ou limite de tempo específicos que podem ser configurados usando uma variável de ambiente. Para ter mais informações, consulte Variáveis de ambiente.

Você pode configurar uma das seguintes opções para armazenar esses dados:

- Armazene todas as mensagens e arquivos capturados localmente. Esta é a opção padrão. É sua responsabilidade mover os arquivos locais para outro sistema para armazenamento a longo prazo e garantir que o disco do host não fique sem memória ou espaço.
- Armazene todas as mensagens e arquivos capturados em um bucket do Amazon S3. O bot de retenção de dados salvará todas as mensagens e arquivos descriptografados no bucket do

Amazon S3 que você especificar. As mensagens e os arquivos capturados são removidos da máquina do host após serem salvos com sucesso no bucket.

- Armazene todas as mensagens e arquivos capturados criptografados em um bucket do Amazon S3. O bot de retenção de dados irá recriptografar todas as mensagens e arquivos capturados usando uma chave fornecida por você e os salvará no bucket do Amazon S3 que você especificar. As mensagens e os arquivos capturados são removidos da máquina do host depois de serem recriptografados com sucesso e salvos no bucket. Você precisará de um software para descriptografar as mensagens e os arquivos.

  Para obter mais informações sobre como criar buckets do Amazon S3 para usar com seu bot de retenção de dados, consulte Criando um bucket, no Guia do usuário do Amazon S3

Variáveis de ambiente

É possível usar as seguintes variáveis de ambiente para definir o bot de retenção de dados. Você define essas variáveis de ambiente usando a opção `-e` ao executar a imagem do Docker do bot de retenção de dados. Para ter mais informações, consulte Inicie o bot de retenção de dados.

> **Note**
>
> Essas variáveis de ambiente são opcionais, a menos que especificado de outra forma.

Use as seguintes variáveis de ambiente para especificar as credenciais do bot de retenção de dados:

- `WICKRIO_BOT_NAME` — o nome do bot de retenção de dados. Essa variável é necessária quando você executa a imagem do Docker do bot de retenção de dados.
- `WICKRIO_BOT_PASSWORD` — a senha inicial do bot de retenção de dados. Para ter mais informações, consulte Pré-requisitos para configurar a retenção de dados. Essa variável é necessária se você não planeja iniciar o bot de retenção de dados com uma solicitação de senha ou não planeja usar o Secrets Manager para armazenar as credenciais do bot de retenção de dados.

Use as seguintes variáveis de ambiente para configurar os recursos de streaming de retenção de dados padrão:

- `WICKRIO_COMP_MESGDEST` — o nome do caminho até o diretório onde as mensagens serão transmitidas. O valor padrão é `/tmp/<botname>/compliance/messages`.
- `WICKRIO_COMP_FILEDEST` — o nome do caminho até o diretório em que os arquivos serão transmitidos. O valor padrão é `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME` — o nome base dos arquivos de mensagens recebidas. O valor padrão é `receivedMessages`.
- `WICKRIO_COMP_FILESIZE` — o tamanho máximo de arquivo de mensagens recebidas em kibibytes (Kib). Um novo arquivo é iniciado quando o tamanho máximo é atingido. O valor padrão é `1000000000`, como em 1024 GiB.
- `WICKRIO_COMP_TIMEROTATE` — a quantidade de tempo, em minutos, durante a qual o bot de retenção de dados colocará as mensagens recebidas em um arquivo de mensagens recebidas. Um novo arquivo é iniciado quando o limite de tempo é atingido. Você só pode usar o tamanho do arquivo ou o tempo para limitar o tamanho do arquivo de mensagens recebidas. O valor padrão é `0`, como em “sem limite”.

Usar a seguinte variável de ambiente para definir o padrão Região da AWS a ser usado.

- `AWS_DEFAULT_REGION` — o padrão Região da AWS a ser usado para serviços AWS como o Secrets Manager (não usado para Amazon S3 ou AWS KMS). A Região `us-east-1` é usada por padrão, se essa variável de ambiente não estiver definida.

Use as seguintes variáveis de ambiente para especificar o segredo do Secrets Manager a ser usado quando você optar por usar o Secrets Manager para armazenar as credenciais do bot de retenção de dados e as informações do serviço AWS. Para obter mais informações sobre os valores que você pode armazenar no Secrets Manager, consulte Valores do Secrets Manager.

- `AWS_SECRET_NAME` — o nome do segredo do Secrets Manager que contém as credenciais e as informações de serviço AWS necessárias para o bot de retenção de dados.
- `AWS_SECRET_REGION` — o Região da AWS no qual o segredo AWS está localizado. Se você estiver usando AWS segredos e esse valor não estiver definido, o valor `AWS_DEFAULT_REGION` será usado.

> **Note**
>
> Você pode armazenar todas as seguintes variáveis de ambiente como valores no Secrets Manager. Se você optar por usar o Secrets Manager e armazenar esses valores lá, não precisará especificá-los como variáveis de ambiente ao executar a imagem do Docker do bot de retenção de dados. Basta especificar a variável de ambiente `AWS_SECRET_NAME` descrita anteriormente neste guia. Para ter mais informações, consulte Valores do Secrets Manager.

Use as seguintes variáveis de ambiente para especificar o bucket do Amazon S3 ao optar por armazenar mensagens e arquivos em um bucket.

- `WICKRIO_S3_BUCKET_NAME` – o nome do bucket do Amazon S3 onde as mensagens e arquivos serão armazenados.
- `WICKRIO_S3_REGION` – a Região AWS do bucket do Amazon S3 onde as mensagens e arquivos serão armazenados.
- `WICKRIO_S3_FOLDER_NAME` – o nome da pasta opcional no bucket do Amazon S3 onde as mensagens e arquivos serão armazenados. O nome da pasta será precedido pela chave para as mensagens e arquivos salvos no bucket do Amazon S3.

Use as seguintes variáveis de ambiente para especificar os detalhes AWS KMS ao optar por usar a criptografia do lado do cliente para recriptografar os arquivos ao salvá-los em um bucket do Amazon S3.

- `WICKRIO_KMS_MSTRKEY_ARN` — o nome do recurso da Amazon (ARN) da chave mestra AWS KMS usada para recriptografar os arquivos de mensagens e os arquivos no bot de retenção de dados antes de serem salvos no bucket do Amazon S3.
- `WICKRIO_KMS_REGION` — a Região AWS onde a chave mestra AWS KMS está localizada.

Use a seguinte variável de ambiente para especificar os detalhes do Amazon SNS ao optar por enviar eventos de retenção de dados para um tópico do Amazon SNS. Os eventos enviados incluem startup, desligamento e condições de erro.

- `WICKRIO_SNS_TOPIC_ARN` – o ARN do tópico do Amazon SNS para o qual você deseja enviar eventos de retenção de dados.

Use a variável de ambiente a seguir para enviar métricas de retenção de dados para CloudWatch. Se especificado, as métricas serão geradas a cada 60 segundos.

- `WICKRIO_METRICS_TYPE`— Defina o valor dessa variável de ambiente como `cloudwatch` para a qual enviar métricas CloudWatch.

Valores do Secrets Manager

Você pode usar o Secrets Manager para armazenar as credenciais do bot de retenção de dados e as informações do serviço AWS. Para obter mais informações sobre a criação de segredos do Secrets Manager, consulte Crie um segredo AWS Secrets Manager no Manual do usuário do Secrets Manager.

O segredo do Secrets Manager pode ter os seguintes valores:

- `password` – a senha do bot de retenção de dados.
- `s3_bucket_name` – o nome do bucket do Amazon S3 onde as mensagens e arquivos serão armazenados. Se não for definido, o streaming de arquivos padrão será usado.
- `s3_region` – a Região AWS do bucket do Amazon S3 onde as mensagens e arquivos serão armazenados.
- `s3_folder_name` – o nome da pasta opcional no bucket do Amazon S3 onde as mensagens e arquivos serão armazenados. O nome da pasta será precedido pela chave para as mensagens e arquivos salvos no bucket do Amazon S3.
- `kms_master_key_arn` – o ARN da chave mestra AWS KMS usada para recriptografar os arquivos de mensagens e arquivos no bot de retenção de dados antes de serem salvos no bucket do Amazon S3.
- `kms_region` – a Região AWS onde a chave mestra AWS KMS está localizada.
- `sns_topic_arn` – o ARN do tópico do Amazon SNS para o qual você deseja enviar eventos de retenção de dados.

Política do IAM para usar a retenção de dados com serviços AWS

Se você planeja usar outros serviços AWS com o bot de retenção de dados do Wickr, você deve garantir que o host tenha o perfil e a política (IAM) AWS Identity and Access Management apropriados para acessá-los. Você pode configurar o bot de retenção de dados para usar o Secrets

Manager, Amazon S3 CloudWatch, Amazon SNS e. AWS KMS A política do IAM a seguir possibilita o acesso a ações específicas para esses serviços.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Você pode criar uma política do IAM mais rígida identificando os objetos específicos de cada serviço que você deseja permitir que os contêineres do seu host acessem. Remova as ações dos serviços AWS que você não pretende utilizar. Por exemplo, se você pretende usar somente um bucket do Amazon S3, use a política a seguir, que remove as ações `secretsmanager:GetSecretValue`, `sns:Publish`, `kms:GenerateDataKey` e `cloudwatch:PutMetricData`.

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

Se você estiver usando uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para hospedar seu bot de retenção de dados, crie um perfil do IAM usando o caso comum do Amazon EC2 e atribua uma política usando a definição de política acima.

Inicie o bot de retenção de dados

Antes de executar o bot de retenção de dados, você deve determinar como deseja configurá-lo. Se você planeja executar o bot em um host que:

- Não terá acesso aos serviços AWS, então suas opções são limitadas. Nesse caso, você usará as opções padrão de streaming de mensagens. Você deve decidir se deseja limitar o tamanho dos arquivos de mensagens capturados a um tamanho ou intervalo de tempo específico. Para ter mais informações, consulte Variáveis de ambiente.
- Se o bot tiver acesso aos serviços AWS, você deverá criar um segredo do Secrets Manager para armazenar as credenciais do bot e os detalhes de configuração do serviço AWS. Depois que os serviços AWS forem configurados, você poderá iniciar a imagem do Docker do bot de retenção de dados. Para obter mais informações sobre os detalhes que você pode armazenar em um segredo do Secrets Manager, consulte Valores do Secrets Manager

As seções a seguir mostram exemplos de comandos para executar a imagem do Docker do bot de retenção de dados. Em cada um dos exemplos de comando, substitua o seguinte exemplo de valores pelos seus próprios valores:

- *compliance_1234567890_bot* pelo nome do seu bot de retenção de dados.
- *password* pela senha do seu bot de retenção de dados.
- *wickr/data/retention/bot* pelo nome do seu segredo do Secrets Manager para usar com seu bot de retenção de dados.
- *bucket-name* pelo nome do bucket do Amazon S3 onde as mensagens e arquivos serão armazenados.
- *folder-name* pelo nome da pasta no bucket do Amazon S3 onde as mensagens e arquivos serão armazenados.
- *us-east-1* pela Região AWS do recurso que você está especificando. Por exemplo, a Região da chave mestra AWS KMS ou a região do bucket do Amazon S3.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab* pelo nome do recurso da Amazon (ARN) da sua chave mestra AWS KMS a ser usada para recriptografar arquivos e arquivos de mensagens.

Inicie o bot com a variável de ambiente com senha (sem serviço AWS)

O comando do Docker a seguir inicia o bot de retenção de dados. A senha é especificada usando a variável de ambiente `WICKRIO_BOT_PASSWORD`. O bot começa a usar o streaming de arquivos padrão e os valores padrão definidos na seção Variáveis de ambiente deste guia.

```
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
```

Inicie o bot com solicitação de senha (sem serviço AWS)

O comando do Docker a seguir inicia o bot de retenção de dados. A senha é inserida quando solicitada pelo bot de retenção de dados. Ele começará a usar o streaming de arquivos padrão usando os valores padrão definidos na seção Variáveis de ambiente deste guia.

```
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:************
```

Execute o bot usando a opção `-ti` de receber a solicitação de senha. Você também deve executar o comando `docker attach <container ID or container name>` imediatamente após iniciar a imagem do docker para receber o prompt de senha. Você deve executar esses dois comandos em um script. Se você anexar à imagem do docker e não ver o prompt, pressione Enter e você verá o prompt.

Inicie o bot com uma rotação de arquivo de mensagem de 15 minutos (sem serviço AWS)

O comando do Docker a seguir inicia o bot de retenção de dados usando variáveis de ambiente. Ele também faz a configuração de rotação dos arquivos de mensagens recebidas para 15 minutos.

```
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
```

Inicie o bot e especifique a senha inicial com o Secrets Manager

Você pode usar o Secrets Manager para identificar a senha do bot de retenção de dados. Ao iniciar o bot de retenção de dados, você precisará definir uma variável de ambiente que especifique ao Secrets Manager onde essas informações são armazenadas.

```
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
```

O segredo `wickrpro/compliance/compliance_1234567890_bot` tem o seguinte valor secreto, mostrado como texto simples.

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

Inicie o bot e configure o Amazon S3 com o Secrets Manager

Você pode usar o Secrets Manager para hospedar as credenciais e as informações do bucket do Amazon S3. Ao iniciar o bot de retenção de dados, você precisará definir uma variável de ambiente que especifique ao Secrets Manager onde essas informações são armazenadas.

```
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
```

O segredo `wickrpro/compliance/compliance_1234567890_bot` tem o seguinte valor secreto, mostrado como texto simples.

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

As mensagens e os arquivos recebidos pelo bot serão colocados no bucket `bot-compliance` na pasta nomeada `network1234567890`.

Inicie o bot e configure o Amazon S3 e AWS KMS com o Secrets Manager

Você pode usar o Secrets Manager para hospedar as credenciais, o bucket do Amazon S3 e as informações da chave mestra AWS KMS. Ao iniciar o bot de retenção de dados, você precisará definir uma variável de ambiente que especifique ao Secrets Manager onde essas informações são armazenadas.

```
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
```

O segredo `wickrpro/compliance/compliance_1234567890_bot` tem o seguinte valor secreto, mostrado como texto simples.

```
{
    "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"
}
```

As mensagens e os arquivos recebidos pelo bot serão criptografados usando a chave KMS identificada pelo valor do ARN e, em seguida, colocados no bucket “bot-compliance'” na pasta chamada “network1234567890”. Certifique-se de que você tem a configuração da política do IAM apropriada.

Inicie o bot e configure o Amazon S3 usando variáveis de ambiente

Se você não quiser usar o Secrets Manager para hospedar as credenciais do bot de retenção de dados, você pode iniciar a imagem do Docker do bot de retenção de dados com as seguintes variáveis de ambiente. Você deve identificar o nome do bot de retenção de dados usando a variável de ambiente `WICKRIO_BOT_NAME`.

```
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
```

Você pode usar valores de ambiente para identificar as credenciais do bot de retenção de dados, informações sobre buckets do Amazon S3 e informações de configuração para o streaming de arquivos padrão.

Interrompa o bot de retenção de dados

O software executado no bot de retenção de dados capturará sinais `SIGTERM` e será desligado normalmente. Use o comando `docker stop` *<container ID or container name>*, conforme mostrado no exemplo a seguir, para emitir o comando `SIGTERM` para a imagem do Docker do bot de retenção de dados.

```
docker stop compliance_1234567890_bot
```

Obtenha os registros de retenção de dados

O software executado na imagem Docker do bot de retenção de dados será enviado para os arquivos de log no diretório `/tmp/`*<botname>*`/logs`. Eles aceitarão um máximo de 5 arquivos. É possível obter os lgos executando o comando a seguir.

```
docker logs <botname>
```

Exemplo:

```
docker logs compliance_1234567890_bot
```

Métricas e eventos de retenção de dados

A seguir estão as métricas do Amazon CloudWatch (CloudWatch) e os eventos do Amazon Simple Notification Service (Amazon SNS) que atualmente são suportados pela versão 5.116 do bot de retenção de dados do AWS Wickr.

Tópicos

CloudWatch métricas

As métricas são geradas pelo bot em intervalos de 1 minuto e transmitidas ao CloudWatch serviço associado à conta na qual a imagem do Docker do bot de retenção de dados está sendo executada.

A seguir estão as métricas existentes suportadas pelo bot de retenção de dados.

Métrica	Descrição
Messages_Rx	Mensagens recebidas.
Messages_Rx_Failed	Falhas no processamento das mensagens recebidas.
Messages_Saved	Mensagens salvas no arquivo de mensagens recebidas.
Messages_Saved_Failed	Falha ao salvar mensagens no arquivo de mensagens recebidas.
Files_Saved	Arquivos recebidos.
Files_Saved_Bytes	O número de bytes recebidos.
Files_Saved_Failed	Falha ao salvar arquivos.
Logins	Logins (normalmente será 1 para cada intervalo).

Métrica	Descrição
Login_Failures	Falhas de login (normalmente será 1 para cada intervalo).
S3_Post_Errors	Erros ao postar arquivos de mensagens e arquivos no bucket do Amazon S3.
Watchdog_Failures	Falhas do Watchdog.
Watchdog_Warnings	Avisos do Watchdog.

As métricas são geradas para serem consumidas por CloudWatch. O namespace usado para bots é. `WickrIO` Cada métrica tem uma matriz de dimensões. A seguir está a lista de dimensões publicadas com as métricas acima.

Dimensão	Valor
Id	O nome de usuário do bot.
Dispositivo	Descrição de uma instância ou dispositivo de bot específico. Útil se você estiver executando vários dispositivos ou instâncias de bots.
Produto	O produto para o bot. Pode ser `WickrPro_` ou `WickrEnterprise_` com `Alpha`, `Beta` ou `Production` anexado.
BotType	O tipo de bot. Rotulado como Conformidade para os bots de conformidade.
Rede	O ID da rede associada.

Eventos do Amazon SNS

Os eventos a seguir são publicados no tópico do Amazon SNS definido pelo valor do Nome do recurso da Amazon (ARN) identificado usando a variável de `WICKRIO_SNS_TOPIC_ARN` ambiente

ou o valor secreto do Secrets Managersns_topic_arn. Para ter mais informações, consulte Variáveis de ambiente e Valores do Secrets Manager.

Os eventos gerados pelo bot de retenção de dados são enviados como cadeias de caracteres JSON. Os valores a seguir estão incluídos nos eventos a partir da versão 5.116 do bot de retenção de dados.

Nome	Valor
complianceBot	O nome de usuário do bot de retenção de dados.
dataTime	Registre a data e a hora em que o evento ocorreu.
Dispositivo	Uma descrição de uma instância ou dispositivo de bot específico. Útil se você estiver executando várias instâncias de bots.
dockerImage	A imagem do Docker associada ao bot.
dockerTag	A tag ou versão da imagem do Docker.
message	A mensagem do evento. Para obter mais informações, consulte Eventos críticos e Eventos normais.
notificationType	Esse valor será `Bot Event`.
severidade	A gravidade do evento. Pode ser `normal` ou `critical`.

Você deve se inscrever no tópico do Amazon SNS para poder receber os eventos. Se você se inscrever usando um endereço de e-mail, um e-mail será enviado para você contendo informações semelhantes ao exemplo a seguir.

```
{
"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"
}
```

Eventos críticos

Esses eventos farão com que o bot pare ou reinicie. O número de reinicializações é limitado para evitar outros problemas.

Falhas de login

A seguir estão os possíveis eventos que podem ser gerados quando o bot não consegue fazer login. Cada mensagem indicará o motivo da falha no login.

Tipo de evento	Mensagem do evento
failedlogin	Credenciais inválidas. Verifique a senha.
failedlogin	Usuário não encontrado.
failedlogin	A conta ou o dispositivo está suspenso.
provisionamento	Usuário saiu do comando.
provisionamento	Senha incorreta para o `config.wickr` arquivo.
provisionamento	Não é possível ler o `config.wickr` arquivo.
failedlogin	Todos os logins falharam.
failedlogin	Novo usuário, mas o banco de dados já existe.

Eventos mais críticos

Tipo de evento	Mensagens de eventos
Uma conta suspensa	WickRioClientMain:: slotAdminUser Suspender: código (% 1): motivo:% 2”
BotDevice Suspenso	Dispositivo suspenso!
WatchDog	O SwitchBoard sistema fica inativo por mais de < *N* > minutos
Falhas do S3	Falha ao colocar o arquivo <*nome do* arquivo≫ no bucket do S3. Erro: <*AWS-error* >
Chave de fallback	CHAVE DE FALLBACK ENVIADA PELO SERVIDOR: Não é uma chave alternativa ativa reconhecida pelo cliente. Envie os registros para a engenharia de desktop.

Eventos normais

A seguir estão os eventos que avisam sobre ocorrências operacionais normais. Muitas ocorrências desses tipos de eventos em um período específico podem ser motivo de preocupação.

Dispositivo adicionado à conta

Esse evento é gerado quando um novo dispositivo é adicionado à conta do bot de retenção de dados. Em algumas circunstâncias, isso pode ser uma indicação importante de que alguém criou uma instância do bot de retenção de dados. A seguir está a mensagem para este evento.

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

Bot logado

Esse evento é gerado quando o bot faz login com sucesso. A seguir está a mensagem para este evento.

```
Logged in
```

Desligar

Esse evento é gerado quando o bot é encerrado. Se o usuário não iniciou isso explicitamente, isso pode ser uma indicação de um problema. A seguir está a mensagem para este evento.

```
Shutting down
```

Atualizações disponíveis

Esse evento é gerado quando o bot de retenção de dados é iniciado e identifica que há uma versão mais recente da imagem associada do Docker disponível. Esse evento é gerado quando o bot é iniciado e diariamente. Esse evento inclui o campo de `versions` matriz que identifica as novas versões disponíveis. Veja a seguir um exemplo da aparência desse 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"
  ]
}
```

O que é o ATAK?

O Android Team Awareness Kit (ATAK) — ou Android Tactical Assault Kit (também ATAK) para uso militar — é um aplicativo de infraestrutura geoespacial e consciência situacional para smartphones que permite colaboração segura em qualquer local geográfico. Embora tenha sido inicialmente projetado para uso em zonas de combate, o ATAK foi adaptado para atender às missões de agências locais, estaduais e federais.

Tópicos

- Habilitar o ATAK no painel da rede do Wickr
- Informações adicionais sobre o ATAK

- Instale e emparelhe o plug-in do Wickr para ATAK
- Disque e receba uma chamada
- Envie um arquivo
- Envie uma mensagem de voz segura (Push-to-talk)
- Cata-vento (acesso rápido)
- Navegação

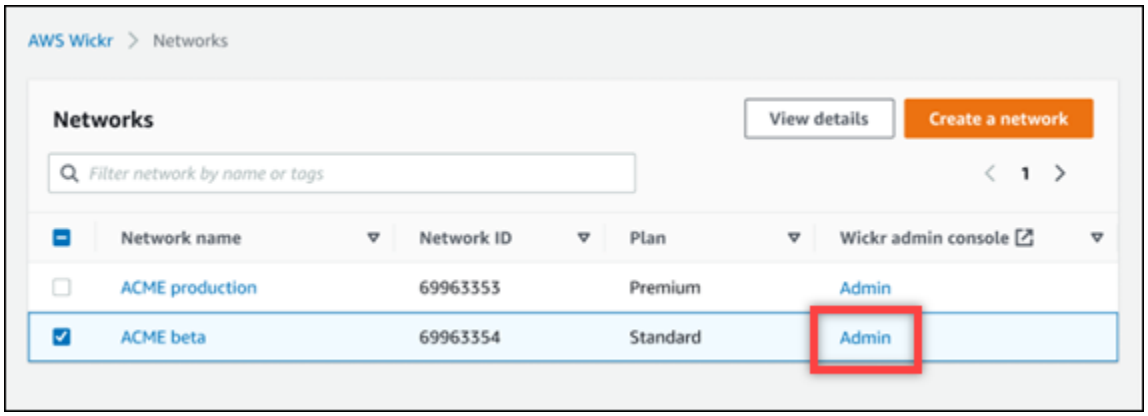
Habilitar o ATAK no painel da rede do Wickr

O AWS Wickr oferece suporte a muitas agências que usam o Android Tactical Assault Kit (ATAK) [Kit de assalto tático Android]. No entanto, até agora, os operadores do ATAK que usam o Wickr tiveram que deixar o aplicativo para fazer isso. Para ajudar a reduzir interrupções e riscos operacionais, a Wickr desenvolveu um plug-in que aprimora o ATAK com recursos de comunicação segura. Com o plug-in Wickr para ATAK, os usuários podem enviar mensagens, colaborar e transferir arquivos no Wickr dentro do aplicativo ATAK. Isso elimina as interrupções e a complexidade da configuração com os recursos de bate-papo do ATAK.

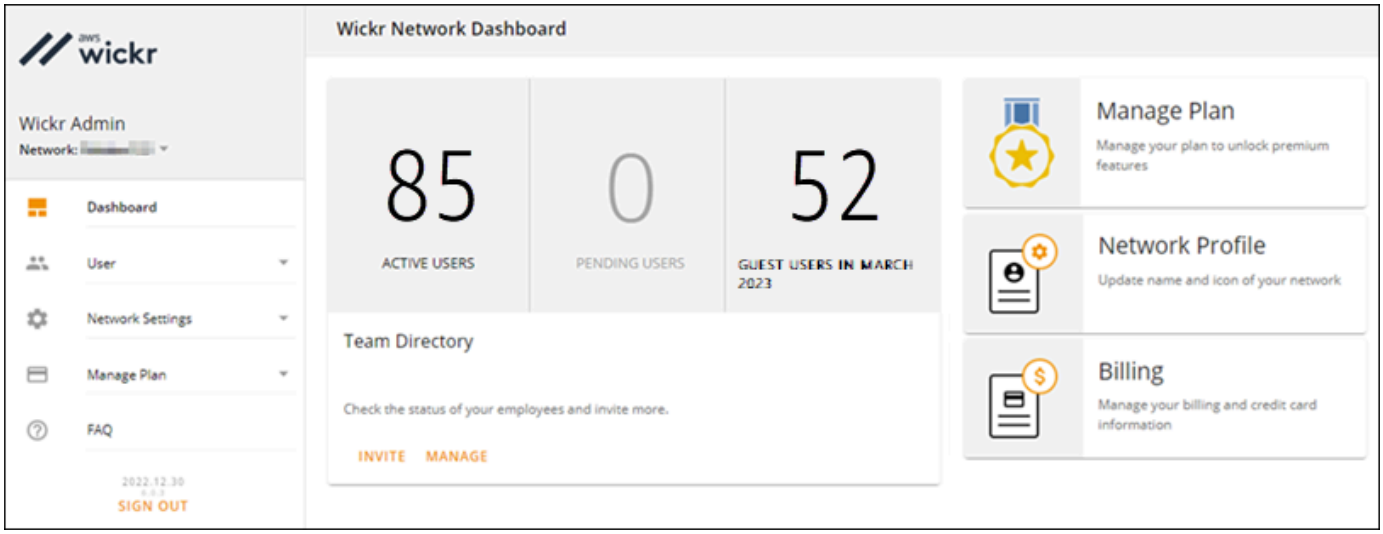
Habilitar o ATAK no painel da rede do Wickr

Conclua o procedimento a seguir para habilitar o ATAK no painel da rede do Wickr.

1. Abra o AWS Management Console para Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.



Você será redirecionado para o Wickr Admin Console de uma rede específica.



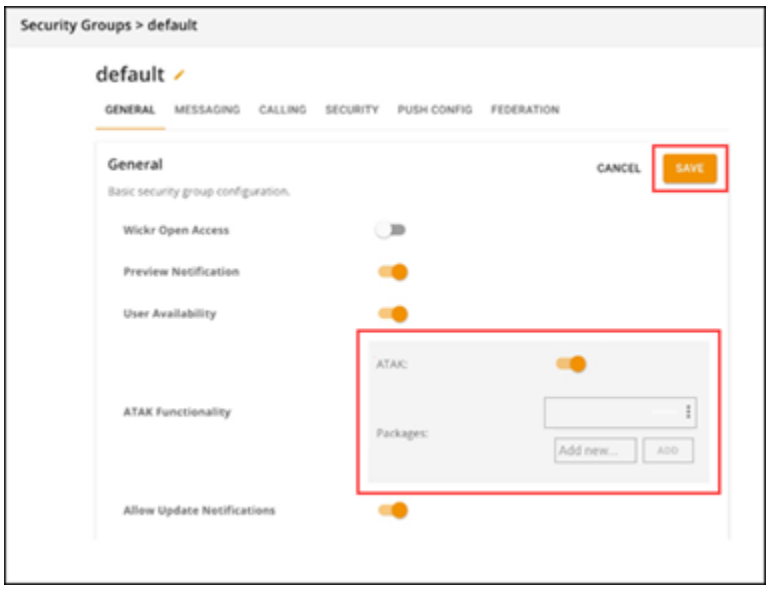
3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Grupo de segurança.
4. O botão Detalhes ao lado do grupo de segurança desejado para o qual você deseja habilitar o ATAK.
5. Na guia Geral, escolha Editar.
6. Na seção Funcionalidade do ATAK:

    a. Insira o nome do pacote na caixa de texto Pacotes. Você pode inserir um dos valores a seguir, dependendo da versão do ATAK que seus usuários instalarão e usarão:

    - `com.atakmap.app.civ` — Insira esse valor na caixa de texto Pacotes se os usuários finais do Wickr quiserem instalar e usar a versão civil do aplicativo ATAK em seus dispositivos Android.
    - `com.atakmap.app.mil` — Insira esse valor na caixa de texto Pacotes se os usuários finais do Wickr quiserem instalar e usar a versão militar do aplicativo ATAK em seus dispositivos Android.

    b. Deslize o botão ATAK para a direita para ativar a funcionalidade.

    c. Escolha Salvar.



O ATAK agora está habilitado para a Rede Wickr selecionada e para o Grupo de Segurança selecionado. Você deve pedir aos usuários do Android no grupo de segurança para o qual você habilitou a funcionalidade ATAK que instalem o plug-in Wickr para ATAK. Para obter mais informações, consulte Instalar e emparelhar o plug-in Wickr ATAK.

Informações adicionais sobre o ATAK

Para obter mais informações sobre o suplemento do Wickr para o ATAK, consulte os seguintes tópicos:

- Visão geral do suplemento Wickr para ATAK
- Informações adicionais sobre o suplemento Wickr para ATAK

Instale e emparelhe o plug-in do Wickr para ATAK

O Android Team Awareness Kit (ATAK) é uma solução Android usada pelas agências militares, estaduais e governamentais dos EUA que exigem recursos de conscientização situacional para planejamento e execução de missões e resposta a incidentes. O ATAK tem uma arquitetura de plug-ins que permite aos desenvolvedores adicionar funcionalidades. Ele permite que os usuários naveguem usando dados de GPS e mapas geoespaciais sobrepostos à consciência situacional em tempo real dos eventos em andamento. Neste documento, mostramos como instalar o plug-in do

Wickr para ATAK em um dispositivo Android e emparelhá-lo com o cliente Wickr. Isso permite que você envie mensagens e colabore no Wickr sem sair do aplicativo ATAK.

Instale o plug-in do Wickr para ATAK

Siga o procedimento a seguir para instalar o plug-in do Wickr para ATAK em um dispositivo Android.

1. Acesse a loja Google Play e instale o plug-in do Wickr para ATAK.
2. Abra o aplicativo ATAK em seu dispositivo Android.
3. No aplicativo ATAK, selecione o ícone do menu () no canto superior direito da tela e selecione Plugins.
4. Escolha Importar.
5. No pop-up Selecionar tipo de importação, selecione Local SD e navegue até onde você salvou o plug-in do Wickr para o arquivo .apk do ATAK.
6. Escolha o arquivo do plug-in e siga as instruções para instalá-lo.

   > **Note**
   >
   > Se for solicitado que você envie o arquivo do plug-in para ser escaneado, escolha Não.

7. O aplicativo ATAK perguntará se você gostaria de carregar o plug-in. Escolha OK.

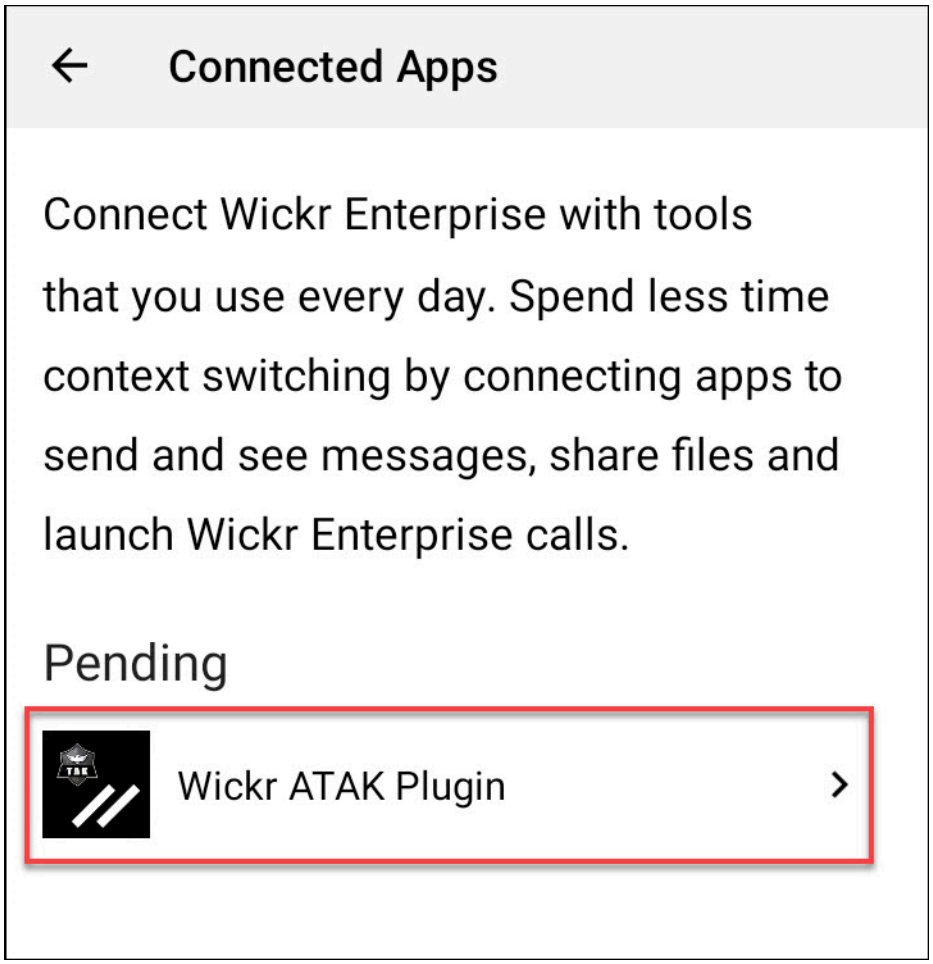
O plug-in do Wickr para ATAK agora está instalado. Continue na seção emparelhe o ATAK com o Wickr a seguir para concluir o processo.

Emparelhe o ATAK com o Wickr

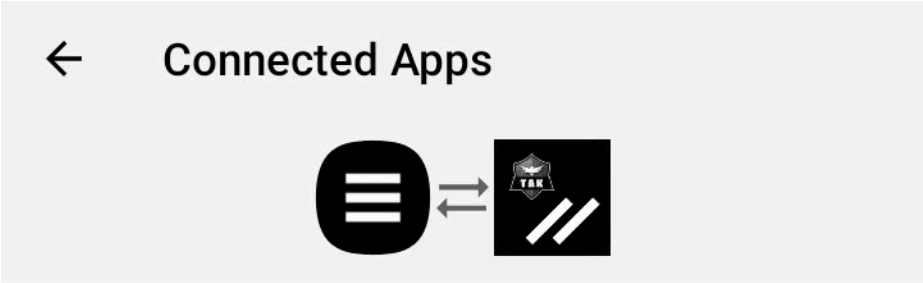
Siga o procedimento a seguir para emparelhar o aplicativo ATAK com o Wickr depois de instalar com sucesso o plug-in do Wickr para ATAK.

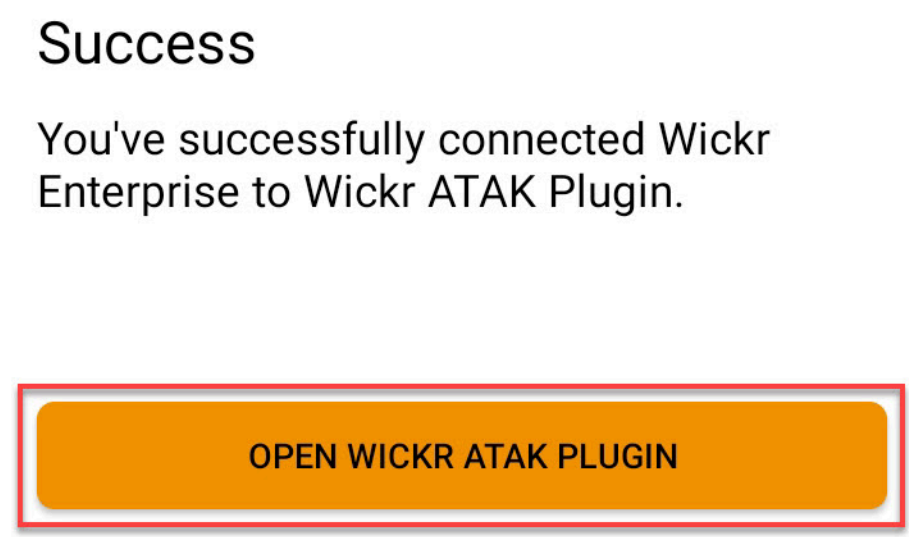
1. No aplicativo ATAK, escolha o ícone () do menu no canto superior direito da tela e escolha Wickr Plugin.
2. Escolha Emparelhar o Wickr.

Um aviso de notificação aparecerá solicitando que você revise as permissões do plug-in do Wickr para ATAK. Se o prompt de notificação não aparecer, abra o cliente Wickr e vá para Configurações e, em seguida, Aplicativos Conectados. Você deve ver o plugin na seção Pendente da tela.



3. Selecione Aprovar para emparelhar.
4. Selecione o botão Abrir plug-in do Wickr para ATAK para voltar ao aplicativo ATAK.



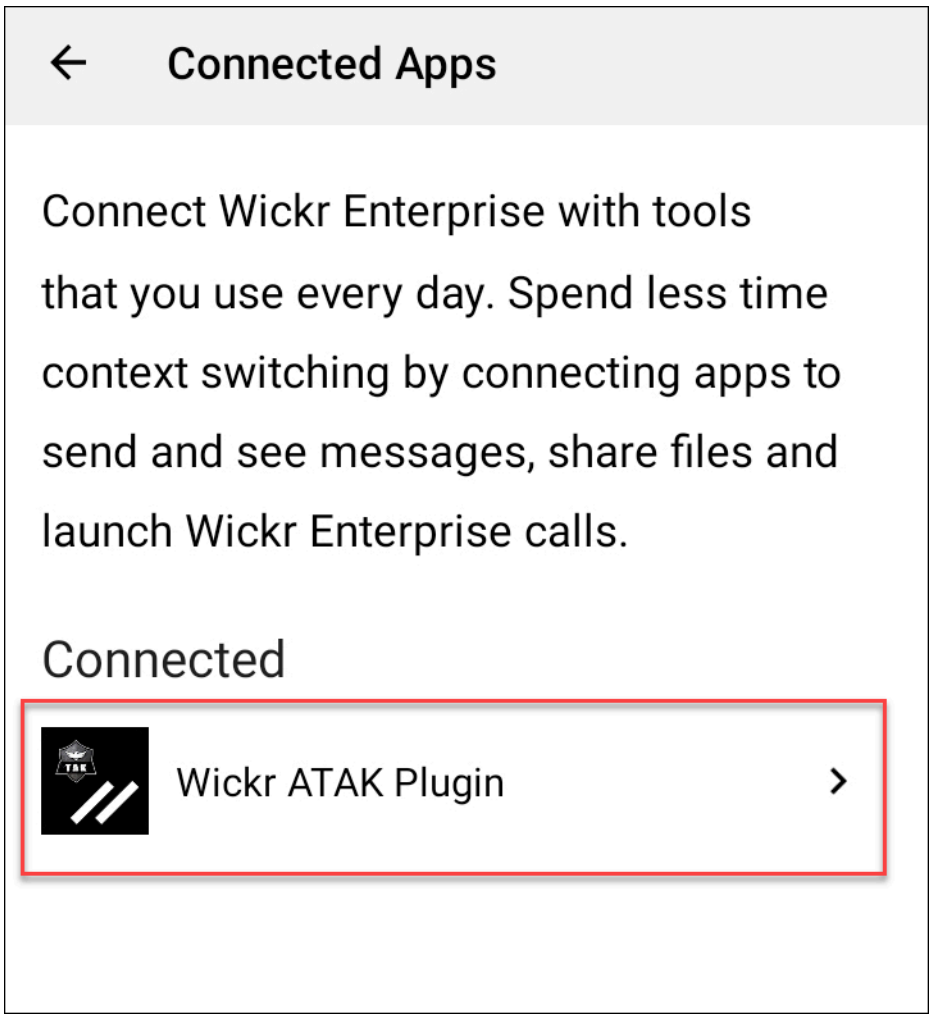


Agora você emparelhou o plug-in ATAK com sucesso e o Wickr pode usar o plug-in para enviar mensagens e colaborar usando o Wickr sem sair do aplicativo ATAK.

Cancele o emparelhamento do ATAK com o Wickr

Conclua o procedimento a seguir para cancelar o emparelhamento do plug-in ATAK com o Wickr.

1. No aplicativo nativo, selecione Configurações e Aplicativos conectados.
2. Na tela Aplicativos conectados, escolha Plug-in Wickr ATAK.



3. Na tela do plug-in Wickr para ATAK, escolha Remover na parte inferior da tela.

   Uma tela de confirmação mostra que você não está mais usando a API. Agora você cancelou o aparelhamento com sucesso do plug-in ATAK.

Disque e receba uma chamada

Você pode discar e receber uma chamada no plugin Wickr para ATAK.

Conclua o procedimento a seguir para discar e receber uma chamada.

1. Abra uma janela do chat.
2. Na visualização do Mapa, escolha o ícone do usuário que você deseja chamar.
3. Escolha o ícone de telefone na parte superior direita da tela.

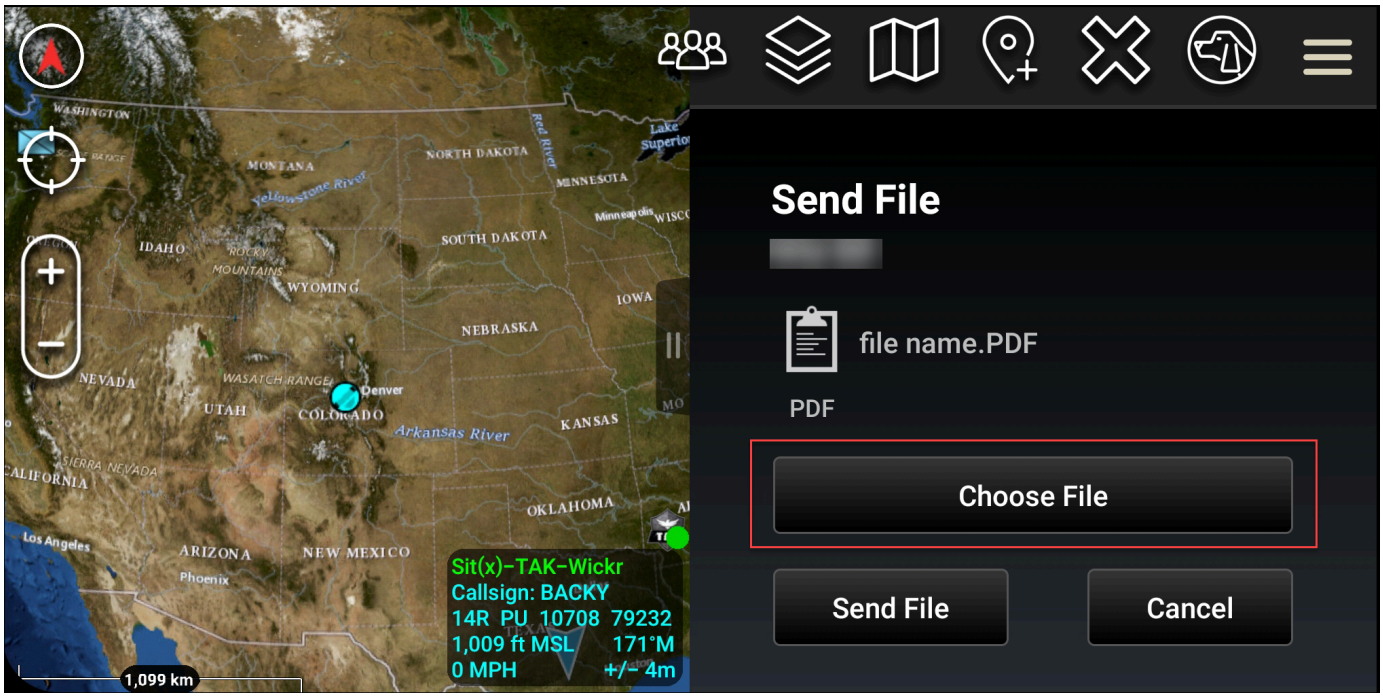
4. Depois de conectado, você pode retornar à visualização do plug-in ATAK e receber uma chamada.

Envie um arquivo

Você pode enviar um arquivo no plugin Wickr para ATAK.

Faça o seguinte procedimento para enviar um arquivo.

1. Abra uma janela do chat.
2. Na visualização do Mapa, procure o usuário para o qual você deseja enviar um arquivo.
3. Quando você encontrar o usuário para o qual deseja enviar um arquivo, selecione o nome dele.
4. Na tela Enviar arquivo, selecione Escolher arquivo e navegue até o arquivo que você deseja enviar.



5. Na janela do navegador, escolha o arquivo desejado.
6. Na tela Enviar arquivo, escolha Enviar arquivo.

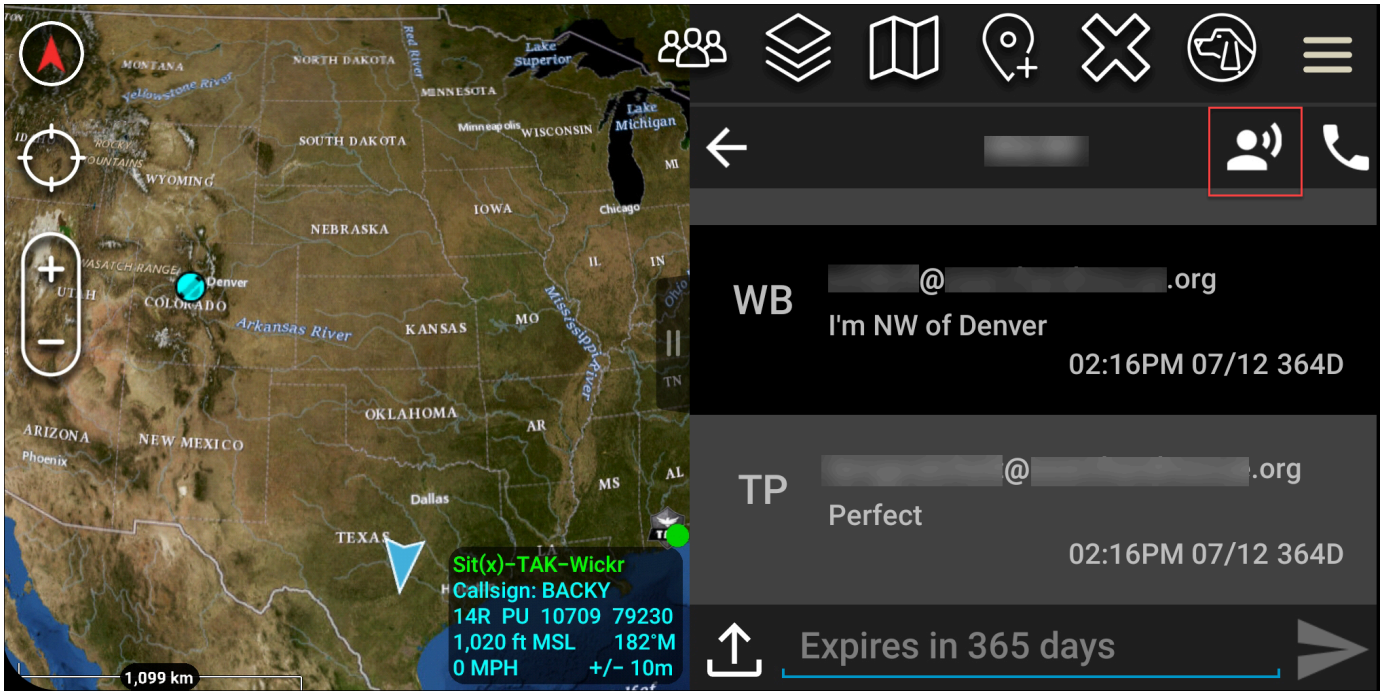
   O ícone de download é exibido, indicando que o arquivo selecionado está sendo baixado.

Envie uma mensagem de voz segura (Push-to-talk)

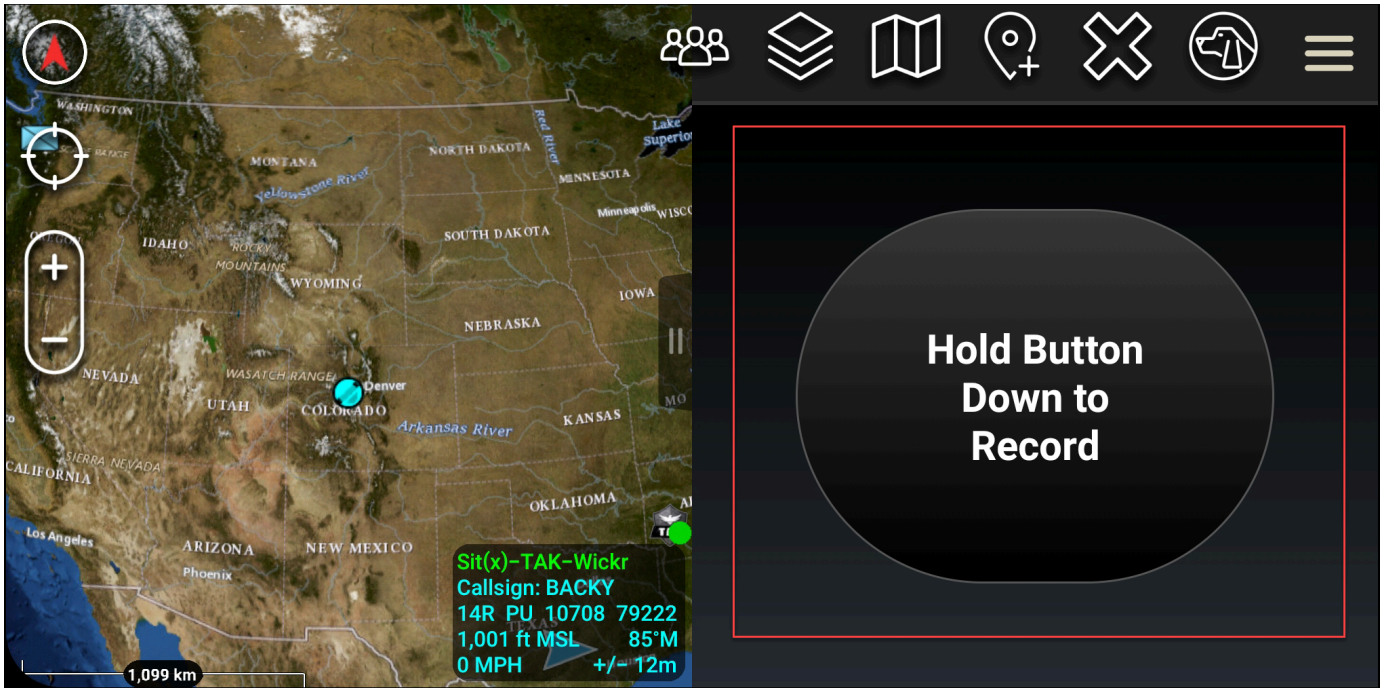
Você pode enviar uma mensagem de voz segura (Push-to-talk) no plugin Wickr para ATAK.

Conclua o procedimento a seguir para enviar uma mensagem de voz segura.

1. Abra uma janela do chat.
2. Escolha o ícone Push-to-talk na parte superior da tela, indicado pelo ícone de uma pessoa falando.



3. Selecione e segure o botão Manter pressionado para gravar.



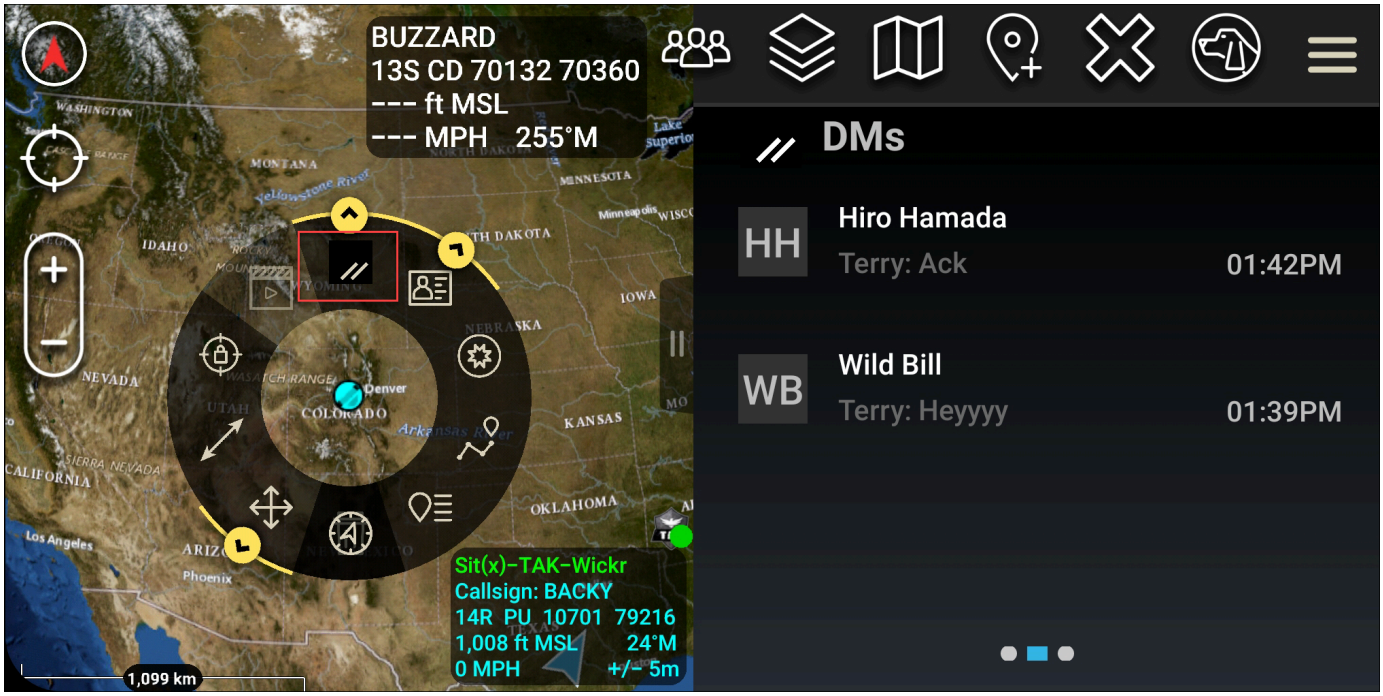
4. Grave sua mensagem.
5. Depois de gravar sua mensagem, solte o botão para enviar.

Cata-vento (acesso rápido)

O cata-vento ou recurso de acesso rápido é usado para one-one-one conversas ou mensagens diretas.

Conclua o procedimento a seguir para usar o cata-vento.

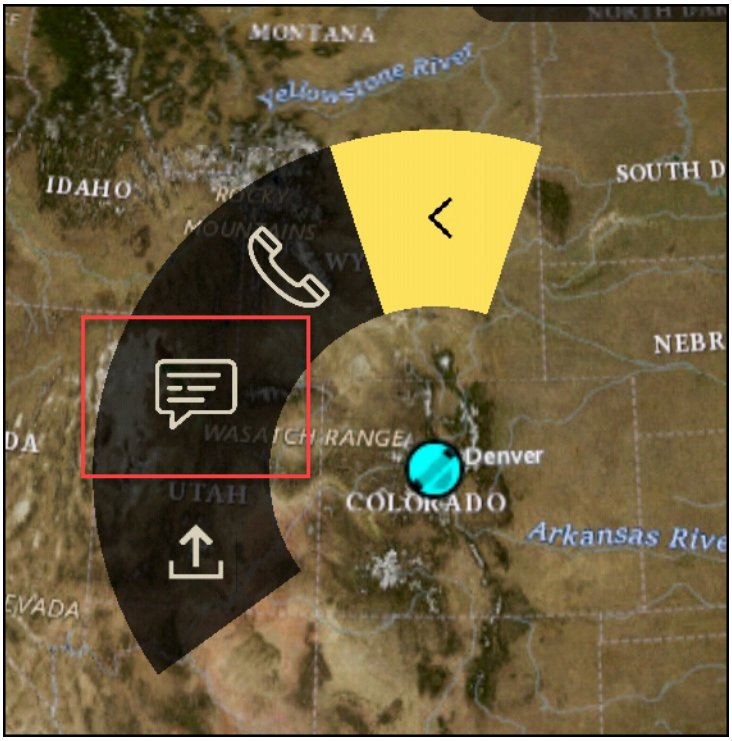
1. Abra a visualização em tela dividida do mapa ATAK e do plugin Wickr para ATAK simultaneamente. O mapa exibe seus colegas de equipe ou ativos na visualização do mapa.
2. Escolha o ícone do usuário para abrir o cata-vento.
3. Escolha o ícone do Wickr para ver as opções disponíveis para o usuário selecionado.



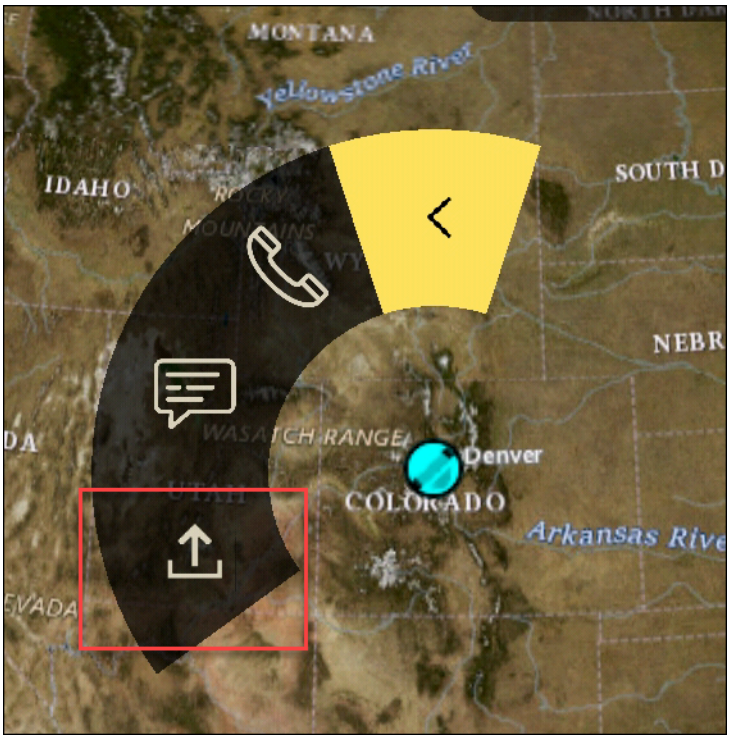
4. No cata-vento, escolha um dos seguintes ícones:

   - Telefone: escolha para ligar.

   - Mensagem: escolha para conversar.



- Envio de arquivo: escolha para enviar um arquivo.



Navegação

A interface do usuário do plug-in contém três visualizações de plug-in que são indicadas pelas formas azul e branca no canto inferior direito da tela. Deslize para a esquerda e para a direita para navegar entre as visualizações.

- Visualização de contatos: crie um grupo de mensagens diretas ou uma conversa em sala.
- Visualização de DMs: crie uma one-to-one conversa. A funcionalidade de chat funciona como no aplicativo nativo do Wickr. Essa funcionalidade permite que você permaneça na visualização do Mapa e se comunique com outras pessoas no plug-in.
- Visualização das salas: as salas existentes no aplicativo nativo são transferidas. Qualquer coisa feita no plug-in é refletida no aplicativo nativo do Wickr.

> **Note**
>
> Certas funções, como excluir uma sala, só podem ser executadas no aplicativo nativo e pessoalmente para evitar modificações não intencionais por usuários e interferências causadas por equipamentos de campo.

Lista de portas e domínios para permitir

Permita listar as seguintes portas e domínios para garantir que o Wickr funcione corretamente:

Portas

- Porta TCP 443 (para mensagens e anexos)
- Portas UDP 16384-16584 (para chamadas)

Domínios regionais

- Europa (Frankfurt): api.messaging.wickr.eu-central-1.amazonaws.com
- Leste dos EUA (Norte da Virgínia): gw-pro-prod .wickr.com, api.messaging. wickr.us-east-1.amazonaws.com
- Europa (Londres): api.messaging.wickr.eu-west-2.amazonaws.com
- Ásia-Pacífico (Sydney): api.messaging.wickr.ap-southeast-2.amazonaws.com
- Canadá (Central): api.messaging.wickr.ca-central-1.amazonaws.com

- AWS GovCloud (Oeste dos EUA): api.messaging.wickr. us-gov-west-1.amazonaws.com

Os e-mails de registro e verificação são enviados de donotreply@wickr.email.

Se você precisar permitir a lista de todos os endereços IP possíveis do servidor de chamadas, você precisará baixar o AllowlistWickr.txt dos possíveis CIDRs e verificá-lo periodicamente, pois ele está sujeito a alterações.

Gerencie usuários no AWS Wickr

Na seção Usuários do AWS Management Console for Wickr, você pode ver os usuários e bots atuais do Wickr e modificar seus detalhes.

Tópicos

Diretório da equipe

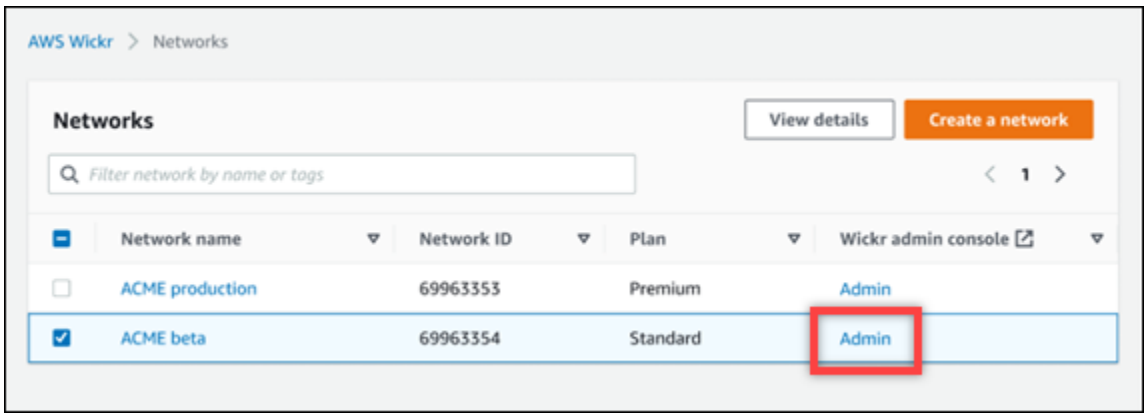
Você pode visualizar os usuários atuais do Wickr e modificar seus detalhes na seção Usuário do AWS Management Console for Wickr.

Tópicos

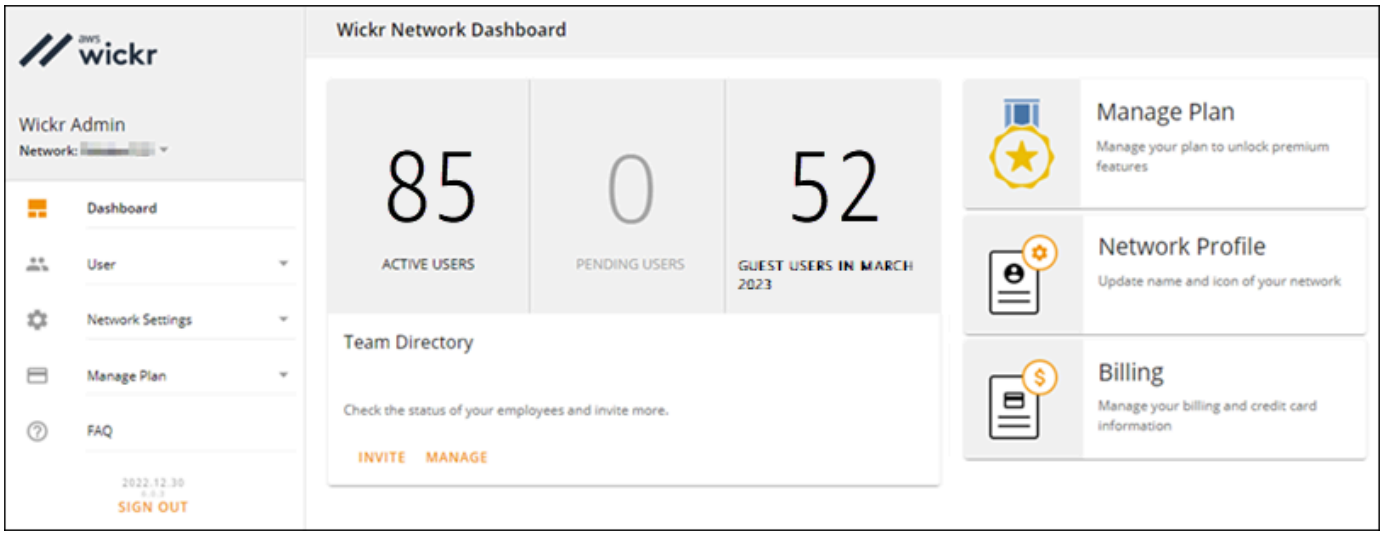
Visualização dos usuários

Conclua o procedimento a seguir para ver os usuários registrados na sua rede Wickr.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.



Você será redirecionado para o Wickr Admin Console de uma rede específica.



3. No painel de navegação do Wickr Admin Console, escolha Usuário e, em seguida, escolha Diretório da equipe.

   A página Diretório da equipe exibe usuários registrados na sua rede Wickr, incluindo nome, endereço de e-mail, grupo de segurança atribuído e status atual. Para usuários atuais, você pode visualizar seus dispositivos, editar seus detalhes, suspender, excluir e trocá-los para outra rede Wickr.

Criar usuários

Faça o seguinte procedimento para criar um usuário.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

Você será redirecionado para o Wickr Admin Console de uma rede específica.

3. No painel de navegação do Wickr Admin Console, escolha Usuário e, em seguida, escolha Diretório da equipe.
4. Escolha Criar novos usuários.
5. No formulário exibido, insira o nome, sobrenome, código do país, número de telefone e endereço de e-mail do usuário. O endereço de e-mail é o único campo obrigatório. Certifique-se de escolher o grupo de segurança apropriado para o usuário. O Wickr enviará um e-mail de convite para o endereço que você especificar para o usuário.
6. Escolha Criar.

   Um e-mail será enviado ao usuário. O e-mail fornece links de download para os aplicativos do cliente Wickr e um link para se registrar no Wickr. Conforme os usuários se cadastram no Wickr usando o link no e-mail, seu status no diretório da equipe do Wickr mudará de Pendente para Ativo.

Editar usuários

Faça o seguinte procedimento para editar um usuário.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

   Você será redirecionado para o Wickr Admin Console de uma rede específica.
3. No painel de navegação do Wickr Admin Console, escolha Usuário e, em seguida, escolha Diretório da equipe.
4. Escolha o ícone de reticências verticais ao lado do nome do usuário que você deseja excluir.
5. Você pode escolher uma das seguintes opções:

   - Dispositivos — Visualizar os dispositivos que o usuário configurou com o cliente Wickr.
   - Editar — Editar os detalhes do usuário, como nome, código do país, número de telefone (opcional) e grupo de segurança atribuído.
   - Suspender — Suspender o usuário para que ele não possa entrar na sua rede Wickr no cliente Wickr. Quando você suspende um usuário que está atualmente conectado à sua rede Wickr no cliente, esse usuário é automaticamente desconectado.
   - Excluir — Exclua o usuário da sua rede Wickr.

Excluir usuários

Faça o seguinte procedimento para excluir um usuário.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

   Você será redirecionado para o Wickr Admin Console de uma rede específica.
3. No painel de navegação do Wickr Admin Console, escolha Usuário e, em seguida, escolha Diretório da equipe.
4. Escolha o ícone de reticências verticais ao lado do nome do usuário que você deseja excluir.
5. Para excluir o host, escolha Excluir.

   Quando você exclui um usuário, esse usuário não consegue mais entrar na sua rede Wickr no cliente Wickr.

Excluir usuários em massa

Você pode excluir e suspender em massa os usuários da rede Wickr na seção Usuário do Wickr Admin Console para Wickr.

Para excluir em massa os usuários da rede Wickr usando um modelo CSV, conclua o procedimento a seguir.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. No painel de navegação do Wickr Admin Console, escolha Usuário e, em seguida, escolha Diretório da equipe.

   A página Diretório da equipe exibe usuários registrados na sua rede Wickr.
3. Na página Diretório da equipe, escolha Gerenciar usuários.
4. Na janela pop-up Gerenciar usuários, escolha Excluir usuários.
5. Faça download do modelo CSV de exemplo. Para baixar o modelo de amostra, escolha Baixar modelo.
6. Preencha o modelo adicionando o e-mail dos usuários que você deseja excluir em massa da sua rede.
7. Faça o upload do modelo CSV completo. Você pode arrastar e soltar o arquivo na caixa de upload ou selecionar escolher um arquivo.

8. Marque a caixa de seleção, Eu reconheço que a exclusão do usuário não é reversível.
9. Escolha Excluir usuários.

> **Note**
>
> Essa ação começará imediatamente a excluir usuários e poderá levar alguns minutos. Os usuários excluídos não conseguem mais entrar na sua rede Wickr pelo cliente Wickr.

Para excluir em massa os usuários da rede Wickr baixando um CSV do diretório da sua equipe, conclua o procedimento a seguir.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. No painel de navegação do Wickr Admin Console, escolha Usuário e, em seguida, escolha Diretório da equipe.

   A página Diretório da equipe exibe usuários registrados na sua rede Wickr.
3. Selecione o ícone de download do CSV no canto superior direito da página do Diretório da equipe.
4. Depois de baixar o modelo CSV do diretório da equipe, remova as linhas de usuários que não precisam ser excluídas.
5. Na página Diretório da equipe, escolha Gerenciar usuários.
6. Na janela pop-up Gerenciar usuários, escolha Excluir usuários.
7. Faça o upload do modelo CSV do diretório da equipe. Você pode arrastar e soltar o arquivo na caixa de upload ou selecionar escolher um arquivo.
8. Marque a caixa de seleção, Eu reconheço que a exclusão do usuário não é reversível.
9. Escolha Excluir usuários.

> **Note**
>
> Essa ação começará imediatamente a excluir usuários e poderá levar alguns minutos. Os usuários excluídos não conseguem mais entrar na sua rede Wickr pelo cliente Wickr.

Suspensão de usuários em massa

Você pode suspender em massa os usuários da rede Wickr na seção Usuário do Wickr Admin Console para Wickr.

Para suspender em massa os usuários da rede Wickr, realize o procedimento a seguir.

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. No painel de navegação do Wickr Admin Console, escolha Usuário e, em seguida, escolha Diretório da equipe.

   A página Diretório da equipe exibe usuários registrados na sua rede Wickr.
3. Na página Diretório da equipe, escolha Gerenciar usuários.
4. Na janela pop-up Gerenciar usuários, escolha Suspender usuários.
5. Faça download do modelo CSV de exemplo. Para baixar o modelo de amostra, escolha Baixar modelo.
6. Preencha o modelo adicionando o e-mail dos usuários que você deseja suspender em massa da sua rede.
7. Faça o upload do modelo CSV completo. Você pode arrastar e soltar o arquivo na caixa de upload ou selecionar escolher um arquivo.
8. Depois de carregar o arquivo CSV, escolha Suspender usuários.

> **Note**
>
> Essa ação começará a suspender usuários imediatamente e poderá levar alguns minutos. Os usuários suspensos não podem entrar na sua rede Wickr pelo cliente Wickr. Quando você suspende um usuário que está atualmente conectado à sua rede Wickr no cliente, esse usuário é automaticamente desconectado.

Usuários convidados

O recurso de usuário convidado do Wickr permite que usuários convidados individuais se conectem ao cliente Wickr e colaborem com os usuários da rede Wickr. Os administradores do Wickr podem habilitar ou desabilitar usuários convidados para suas redes Wickr na página Security Group do console de administração do Wickr.

Depois que o recurso for ativado, usuários convidados para sua rede Wickr podem interagir com usuários em sua rede Wickr. Uma taxa será aplicada ao seu recurso Conta da AWS de usuário convidado. Para obter mais informações sobre preços do recurso de usuário convidado, consulte a página de Preços do Wickr em Preços dos suplementos.

Tópicos

Habilitar ou desabilitar usuários convidados

Conclua o procedimento a seguir para habilitar ou desabilitar usuários convidados para sua rede Wickr.

1. Abra o AWS Management Console para Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

   Você será redirecionado para o Wickr Admin Console de uma rede específica.
3. No painel de navegação do Wickr Admin Console, escolha Configurações de rede e, em seguida, escolha Grupo de segurança.
4. Escolha Detalhes para um grupo de segurança específico.

   > **Note**
   >
   > Você pode habilitar usuários convidados somente para grupos de segurança individuais. Para habilitar usuários convidados para todos os grupos de segurança em sua rede Wickr, você deve habilitar o recurso para cada grupo de segurança em sua rede.
5. Escolha a guia Federação na página de detalhes do grupo de segurança.
6. Há dois locais em que a opção para permitir usuários convidados estará disponível:

   - Federação local — Para redes no Leste dos EUA (Norte da Virgínia), escolha Editar ao lado da seção Federação local da página.

- Federação global — Para todas as outras redes em outras regiões, escolha Editar ao lado da seção Federação global da página.

7. Selecione Permitir que usuários convidados habilitem usuários convidados para o grupo de segurança ou desmarque-o para desativá-lo.
8. Escolha Salvar para salvar a alteração e torná-la efetiva para o grupo de segurança.

   Usuários registrados no grupo de segurança específico da sua rede Wickr agora podem interagir com usuários convidados. Para obter mais informações, consulte Usuários convidados no Guia do usuário do Wickr.

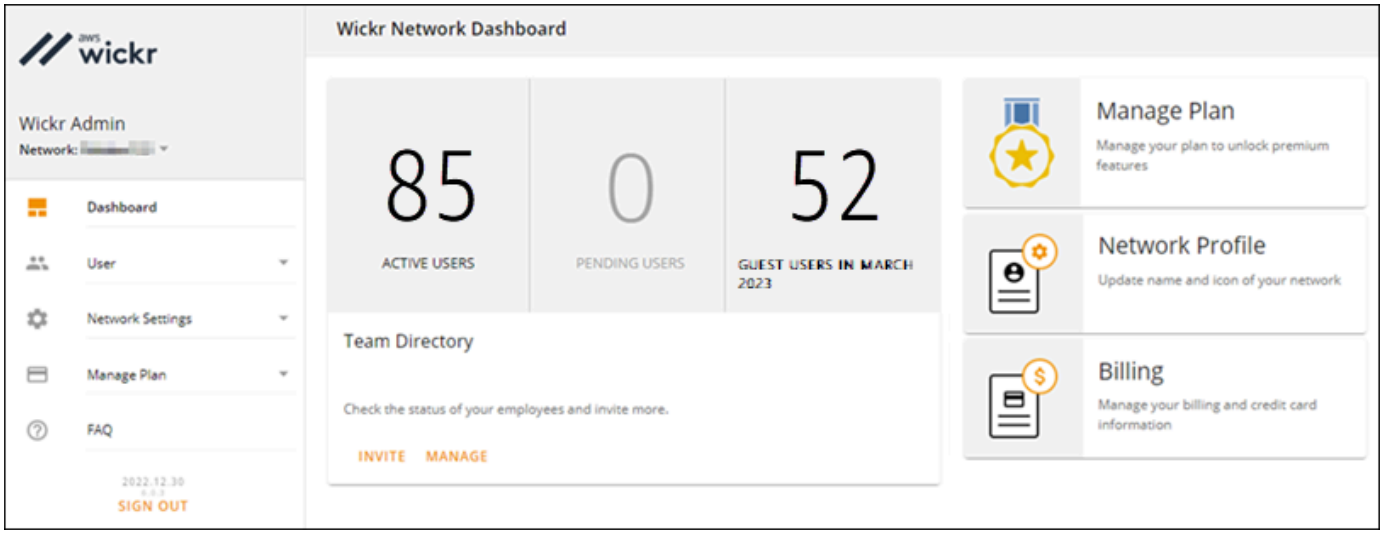
> **Note**
>
> O recurso de usuário convidado do Wickr não está disponível em AWS GovCloud (US) West (AWS WickrGov).

Exibir contagem de usuários convidados

Conclua o procedimento a seguir para ver os usuários convidados para sua rede Wickr.

1. Abra o AWS Management Console para Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.

   Você será redirecionado para o Wickr Admin Console de uma rede específica. A página Painel exibe uma contagem de usuários convidados em sua rede Wickr, conforme mostrado no exemplo a seguir.



Visualizar uso mensalmente

Você pode ver o número de usuários convidados com os quais sua rede se comunicou durante um período de cobrança. Para visualizar seu uso mensal, conclua as etapas a seguir.

1. Abra o AWS Management Console para Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.
3. No painel de navegação do console, selecione Usuários e Adicionar usuário.
4. Na página Usuários convidados, escolha a seção Uso mensal.

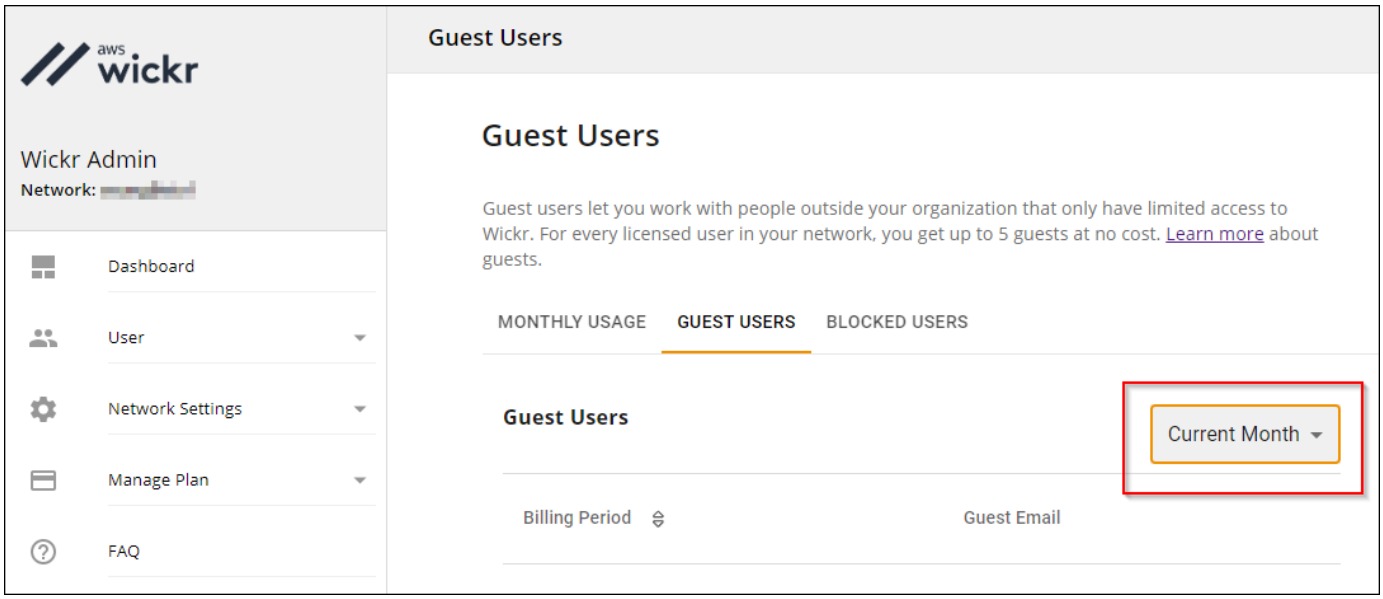
> **Note**
>
> Os dados de cobrança dos hóspedes são atualizados a cada 24 horas.

Visualizar usuários convidados

Você pode ver uma lista de usuários convidados com os quais sua rede se comunicou durante um período de cobrança. Para visualizar seus usuários convidados, conclua as etapas a seguir.

1. Abra o AWS Management Console para Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.
3. No painel de navegação do console, selecione Usuários e Adicionar usuário.
4. Na página Usuários convidados, escolha a seção Usuários convidados.

5. Para visualizar usuários convidados de um mês específico, selecione o mês correspondente no menu suspenso.



Bloquear um usuário convidado

Usuários bloqueados não podem se comunicar com ninguém na sua rede.

Para bloquear um usuário convidado

1. Abra o AWS Management Console para Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.
3. No painel de navegação do console, selecione Usuários e Adicionar usuário.
4. Na página Usuários convidados, escolha a seção Usuários convidados.
5. A seção Usuários convidados mostra os usuários convidados que se comunicaram na sua rede Wickr.
6. Na seção Usuários convidados, encontre o e-mail do usuário convidado que você deseja bloquear.
7. No lado direito do nome do usuário convidado, selecione os três pontos e escolha Bloquear.
8. Escolha Bloquear na janela pop-up.
9. Para ver a lista de usuários bloqueados na sua rede Wickr, escolha a seção Usuários bloqueados.

Para desbloquear um usuário convidado

1. Abra o AWS Management Console para Wickr em https://console.aws.amazon.com/wickr/.
2. Na página Redes, escolha o link Admin para navegar até o Wickr Admin Console dessa rede.
3. No painel de navegação do console, selecione Usuários e Adicionar usuário.
4. Na página Usuários convidados, escolha a seção Usuários bloqueados.
5. A seção Usuários bloqueados mostra os usuários convidados que estão bloqueados na sua rede Wickr.
6. Na seção Usuários bloqueados, encontre o e-mail do usuário convidado que você deseja desbloquear.
7. No lado direito do nome do usuário convidado, selecione os três pontos e escolha Desbloquear.
8. Escolha Desbloquear na janela pop-up.

Segurança no AWS Wickr

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao AWS Wickr, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Wickr. Os tópicos a seguir mostram como configurar o Wickr para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Wickr.

Tópicos

Proteção de dados no AWS Wickr

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no AWS Wickr. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Wickr ou outro Serviços da AWS usando o console, a API ou os AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Identity and Access Management para o AWS Wickr

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar os recursos do Wickr. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Wickr.

Usuário do serviço – se você usa o serviço ACM para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do Wickr para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Wickr, consulte Solução de problemas de identidade e acesso do AWS Wickr.

Administrador do serviço – Se você for o responsável pelos recursos do Wickr na empresa, provavelmente terá acesso total ao Wickr. Cabe a você determinar quais funcionalidades e recursos do Wickr os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações

nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Wickr, consulte Como o AWS Wickr funciona com o IAM.

Administrador do IAM – Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao Wickr. Para visualizar exemplos de políticas baseadas em identidade do Wickr que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Wickr.

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário. Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para mais informações sobre o Centro de Identidade do IAM, consulte “O que é o Centro de Identidade do IAM?” no Guia do usuário do AWS IAM Identity Center .

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários

de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis.. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando uma função de serviço ou uma função vinculada ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado o principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade e seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As

permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

AWS políticas gerenciadas para o AWS Wickr

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

Serviços da AWS manter e atualizar políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos atributos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo atributo for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

AWS política gerenciada: AWSWickrFullAccess

É possível anexar a política `AWSWickrFullAccess` a suas identidades do IAM. Esta política concede permissão administrativa total ao serviço Wickr, incluindo o AWS Management Console for Wickr no AWS Management Console. Para obter informações sobre como anexar políticas a uma

identidade, consulte Adicionar e remover permissões de identidade do IAM no AWS Identity and Access Management Guia do usuário do IAM.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `wickr` – Concede permissão administrativa total ao serviço Wickr.

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

Atualizações do Wickr para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Wickr desde que esse serviço começou a rastrear essas mudanças. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed de RSS na página Document History (Histórico do documento) do Wickr.

Alteração	Descrição	Data
AWSWickrFullAccess – Nova política	O Wickr adicionou uma nova política que concede permissão administrativa total ao serviço Wickr, incluindo o console do administrador do Wickr no AWS Management Console.	28 de novembro de 2022

Alteração	Descrição	Data
O Wickr iniciou o rastreamento das alterações	A Wickr começou a monitorar as mudanças em suas políticas AWS gerenciadas.	28 de novembro de 2022

Como o AWS Wickr funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Wickr, saiba quais recursos do IAM estão disponíveis para uso com o Wickr.

Recursos do IAM que você pode usar com o AWS Wickr

Atributo do IAM	Suporte do Wickr
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
recursos de políticas	Não
Chaves de condição de políticas	Não
ACLs	Não
ABAC (rótulos em políticas)	Não
Credenciais temporárias	Não
Permissões de entidade principal	Não
Perfis de serviço	Não
Perfis vinculados ao serviço	Não

Para ter uma visão de alto nível de como o Wickr e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para o Wickr

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para o Wickr

Para visualizar exemplos de políticas baseadas em identidade do Exemplos de políticas baseadas em identidade para o AWS Wickr, consulte Wickr.

Políticas baseadas em recursos no Wickr

Oferece suporte a políticas baseadas em recurso	Não

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos,

os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações de políticas para o Wickr

Oferece suporte a ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Wickr, consulte Ações definidas pelo AWS Wickr na Referência de autorização do serviço.

As ações de políticas no Wickr usam o seguinte prefixo antes da ação:

```
wickr
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Para visualizar exemplos de políticas baseadas em identidade do Exemplos de políticas baseadas em identidade para o AWS Wickr, consulte Wickr.

Recursos de políticas para o Wickr

Oferece suporte a recursos de políticas	Não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para obter uma lista dos tipos de recursos do Wickr e seus ARNs, consulte Recursos definidos pelo AWS Wickr na Referência de autorização do serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Wickr.

Para visualizar exemplos de políticas baseadas em identidade do Exemplos de políticas baseadas em identidade para o AWS Wickr, consulte Wickr.

Chaves de condição de políticas para o Wickr

Compatível com chaves de condição de política específicas do serviço	Não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam atendentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de condição do Wickr, consulte Chaves de condição do AWS Wickr na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar uma chave de condição, consulte Ações definidas pelo AWS Wickr.

Para visualizar exemplos de políticas baseadas em identidade do Exemplos de políticas baseadas em identidade para o AWS Wickr, consulte Wickr.

ACLs no Wickr

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com Wickr

Oferece suporte a ABAC (tags em políticas)	Não

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar Controle de Acesso Baseado em recursos (ABAC) no Guia do Usuário do IAM.

Usar credenciais temporárias com o Wickr

Oferece suporte a credenciais temporárias	Não

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "Trabalhe com o IAM" no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para mais informações sobre como alternar funções, consulte Alternar para uma função (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal entre serviços para o Wickr

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Não

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço do Wickr

Oferece suporte a perfis de serviço	Não

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para mais

informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de um perfil de serviço pode prejudicar a funcionalidade do Wickr. Edite os perfis de serviço somente quando o Wickr orientar você a fazê-lo.

Funções vinculadas ao serviço para o Wickr

Oferece suporte a perfis vinculados ao serviço	Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço.

Exemplos de políticas baseadas em identidade para o AWS Wickr

Por padrão, um novo usuário do IAM não tem permissões para fazer nada. Um administrador do IAM deve criar e atribuir políticas do IAM que concedam aos usuários a permissão para trabalhar com o serviço AWS Wickr. A seguir, um exemplo de uma política de permissões.

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

```
            "Resource": "*"
        }
    ]
}
```

Esse exemplo de política dá aos usuários permissões para criar, visualizar e gerenciar redes Wickr usando o AWS Management Console for Wickr. Para saber mais sobre os elementos de uma declaração de política do IAM, consulte Políticas baseadas em identidade para o Wickr. Para saber como criar uma política do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na aba JSON no Manual do usuário do IAM.

Tópicos

- Práticas recomendadas de políticas
- Usando o AWS Management Console para Wickr
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Wickr em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas

usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Guia do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o AWS Management Console para Wickr

Anexe a política `AWSWickrFullAccess` AWS gerenciada às suas identidades do IAM para conceder a elas permissão administrativa total ao serviço Wickr, incluindo o console do administrador do Wickr no. AWS Management Console Para ter mais informações, consulte AWS política gerenciada: AWSWickrFullAccess.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

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

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

Solução de problemas de identidade e acesso do AWS Wickr

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Wickr e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação administrativa no AWS Management Console for Wickr

Não estou autorizado a realizar uma ação administrativa no AWS Management Console for Wickr

Se o AWS Management Console for Wickr indicar que você não está autorizado a realizar uma ação, entre em contato com seu administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário do `mateojackson` IAM tenta usar o AWS Management Console for Wickr para criar, gerenciar ou visualizar redes Wickr no AWS Management Console for Wickr, mas não tem as permissões e. `wickr:CreateAdminSession` `wickr:ListNetworks`

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

Nesse caso, Mateo pede ao administrador que atualize suas políticas para permitir que ele acesse o AWS Management Console for Wickr usando as ações `wickr:CreateAdminSession` e. `wickr:ListNetworks` Para ter mais informações, consulte Exemplos de políticas baseadas em identidade para o AWS Wickr e AWS política gerenciada: AWSWickrFullAccess.

Validação de conformidade

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS Serviços no escopo do programa de conformidade AWS . Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar o Wickr é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido sobre sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos com foco em segurança e conformidade em. AWS
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.

- Avaliação de recursos com regras no Guia do AWS Config Desenvolvedor — AWS Config avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes do setor e os regulamentos.
- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência no AWS Wickr

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Wickr oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados. Para ter mais informações, consulte Retenção de dados.

Segurança da infraestrutura no AWS Wickr

Como um serviço gerenciado, o AWS Wickr é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Análise de vulnerabilidade e configuração no AWS Wickr

A configuração e os controles de TI são uma responsabilidade compartilhada entre você AWS e você, nosso cliente. Para obter mais informações, consulte o modelo de responsabilidade AWS compartilhada.

É sua responsabilidade configurar o Wickr de acordo com as especificações e diretrizes, instruir periodicamente seus usuários a baixar a versão mais recente do cliente Wickr, garantir que você

esteja executando a versão mais recente do bot de retenção de dados do Wickr e monitorar o uso do Wickr por seus usuários.

Práticas recomendadas de segurança para o AWS Wickr

O Wickr oferece uma série de recursos de segurança a serem considerados no desenvolvimento e na implementação das suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Para evitar possíveis eventos de segurança associados ao uso do Wickr, siga estas melhores práticas:

- Implemente o acesso com privilégios mínimos e crie funções específicas para serem usadas nas ações do Wickr. Use modelos do IAM para criar uma função. Para ter mais informações, consulte AWS políticas gerenciadas para o AWS Wickr.
- Acesse o AWS Management Console for Wickr autenticando-se no AWS Management Console primeiro. Não compartilhe suas credenciais pessoais do console. Qualquer pessoa na internet pode acessar o console, mas não pode fazer login ou iniciar uma sessão a menos que tenha credenciais válidas para o console.

Monitoramento do AWS Wickr

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do AWS Wickr e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar o Wickr, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail. Para obter mais informações sobre como registrar chamadas da API Wickr usando CloudTrail, consulteRegistro de chamadas da API do AWS Wickr usando AWS CloudTrail.

Registro de chamadas da API do AWS Wickr usando AWS CloudTrail

O AWS Wickr é integrado comAWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Wickr. CloudTrail captura todas as chamadas de API para o Wickr como eventos. As chamadas capturadas incluem as chamadas do AWS Management Console para o Wickr e as chamadas de código para as operações de API do Wickr. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Wickr. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Wickr, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações sobre Wickr em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Wickr, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para obter um registro contínuo de eventos em sua Conta da AWS, inclusive eventos para o Wickr, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especificou Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Wickr são registradas por. CloudTrail Por exemplo, chamadas para o `CreateAdminSession` e `ListNetworks` as ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou usuário do IAM AWS Identity and Access Management
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Noções básicas sobre as entradas do arquivo de log do Wickr

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateAdminSession` ação.


```
{
    "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateNetwork` ação.

```
{
    "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ListNetworks` ação.

```
{
    "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `UpdateNetworkdetails` ação.

```
{
    "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `TagResource` ação.

```
{
    "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ListTagsForResource` ação.

```
{
    "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"
}
```


Painel de análise

Você pode usar o painel de análise para ver como sua organização está utilizando o AWS Wickr. O procedimento a seguir explica como acessar o painel de análise usando o console do AWS Wickr.

Para acessar o painel de análise

1. Abra o AWS Management Console for Wickr em https://console.aws.amazon.com/wickr/.
2. No painel de navegação, escolha Analytics (Análise).

   A página Analytics exibe as métricas da sua rede em diferentes guias.

Na página Analytics, você encontrará um filtro de período de tempo no canto superior direito de cada guia. Esse filtro se aplica à página inteira. Além disso, no canto superior direito de cada guia, você pode exportar os pontos de dados para o intervalo de tempo selecionado escolhendo a opção Exportar disponível.

> **Note**
>
> O horário selecionado está em UTC (Universal Time Coordinated).

As seguintes guias estão disponíveis:

- A visão geral é exibida:
  - Registrado — O número total de usuários registrados, incluindo usuários ativos e suspensos na rede no horário selecionado. Ela não inclui usuários pendentes ou convidados.
  - Pendente — O número total de usuários pendentes na rede no horário selecionado.
  - Registro de usuário — O gráfico exibe o número total de usuários registrados no intervalo de tempo selecionado.
  - Dispositivos — O número de dispositivos em que o aplicativo esteve ativo.
  - Versões do cliente — O número de dispositivos ativos categorizados por suas versões do cliente.

- Os membros exibem:
  - Status — Usuários ativos na rede dentro do período selecionado.
  - Usuários ativos —
    - O gráfico exibe a contagem de usuários ativos ao longo do tempo e pode ser agregado diariamente, semanalmente ou mensalmente (dentro do intervalo de tempo selecionado acima).
    - A contagem de usuários ativos pode ser dividida por plataforma, versão do cliente ou grupo de segurança. Se um grupo de segurança foi excluído, a contagem total será mostrada como Excluído#.

- As mensagens são exibidas:
  - Mensagens enviadas — A contagem de mensagens exclusivas enviadas por todos os usuários e bots na rede no período selecionado.

- Chamadas — Número de chamadas exclusivas feitas por todos os usuários na rede.
- Arquivos — Número de arquivos enviados pelos usuários na rede (inclui memorandos de voz).
- Dispositivos — O gráfico circular exibe o número de dispositivos ativos categorizados por seu sistema operacional.
- Versões do cliente — O número de dispositivos ativos categorizados por suas versões do cliente.

Histórico do documento

A tabela a seguir descreve as versões de documentação para Wickr.

Alteração	Descrição	Data
A Federação Global agora oferece suporte à federação restrita e os administradores podem visualizar as análises de uso no Admin Console	A Federação Global agora oferece suporte à federação restrita. Isso funciona para redes Wickr em outras Regiões da AWS. Para obter mais informações, consulte Grupos de segurança. Além disso, os administradores agora podem ver suas análises de uso no painel do Analytics no Admin Console. Para obter mais informações, consulte Painel do Analytics.	28 de março de 2024
Um teste gratuito de três meses do plano Premium do AWS Wickr já está disponível	Os administradores do Wickr agora podem escolher um plano Premium de teste gratuito de três meses para até 30 usuários. Durante o teste gratuito, todos os recursos dos planos Standard e Premium estão disponíveis, incluindo controles administrativos ilimitados e retenção de dados. O recurso de usuário convidado não está disponível durante o teste gratuito do Premium. Para obter mais informações, consulte Gerenciar plano.	9 de fevereiro de 2024

O recurso de usuário convidado está geralmente disponível e mais controles administrativos foram adicionados	Agora, os administradores do Wickr podem acessar uma série de novos recursos, incluindo a lista de usuários convidados, a capacidad e de excluir ou suspender vários usuários ao mesmo tempo e a opção de impedir que os usuários convidado s se comuniquem na sua rede do Wickr. Para obter mais informações, consulte o Usuários convidados.	8 de novembro de 2023
Wickr já está disponível na Europa (Frankfurt) Região da AWS	O Wickr está agora disponíve l na Europa (Frankfurt) Região da AWS. Para obter mais informações, consulte Acessando o Wickr.	26 de outubro de 2023
As redes Wickr agora têm a capacidade de se federar em Regiões da AWS	As redes do Wickr agora têm a capacidade de se federar em Regiões da AWS. Para obter mais informações, consulte Grupos de segurança.	29 de setembro de 2023
Wickr está agora disponível na Europa (Londres) Região da AWS	O Wickr está agora disponíve l na Europa (Londres) Região da AWS. Para obter mais informações, consulte Acessando o Wickr.	23 de agosto de 2023
Wickr agora está disponível no Canadá (Central) Região da AWS	O Wickr agora está disponíve l no Canadá (Central) Região da AWS. Para obter mais informações, consulte Acessando o Wickr.	3 de julho de 2023

O recurso de usuário convidado agora disponível para pré-visualização	Usuários convidados podem fazer login no cliente do Wickr e colaborar com usuários da rede do Wickr. Para obter mais informações, consulte Usuários convidados (prévia).	31 de maio de 2023
O AWS Wickr agora está integrado AWS CloudTrail e agora está disponível no AWS GovCloud (Oeste dos EUA) como WickrGov	O AWS Wickr agora está integrado com o. AWS CloudTrail Para obter mais informações, consulte Registro de chamadas de API do AWS Wickr usando o AWS CloudTrail. Além disso, o Wickr agora está disponíve l em AWS GovCloud (Oeste dos EUA) como. WickrGov Para obter mais informaçõ es, consulte AWS WickrGovo Guia AWS GovCloud (US) do usuário.	30 de março de 2023
Marcando com tags e criando várias redes	Agora, a marcação com tags é compatível com o AWS Wickr. Para obter mais informaçõ es, consulte Gerenciar tags de rede. Agora, podem ser criadas várias redes no Wickr. Para obter mais informações, consulte Crie uma rede.	7 de março de 2023
Lançamento inicial	Versão inicial do Guia de administração do Wickr	28 de novembro de 2022

Notas de release

Para ajudá-lo a rastrear as atualizações e melhorias contínuas no Wickr, publicamos avisos de lançamento que descrevem as alterações recentes.

Março de 2024

- A Federação Global agora oferece suporte à federação restrita, na qual a federação global só pode ser ativada para redes selecionadas que são adicionadas sob federação restrita. Isso funciona para redes Wickr em outras Regiões da AWS. Para obter mais informações, consulte Grupos de segurança.
- Agora, os administradores podem ver suas análises de uso no painel do Analytics no Admin Console. Para obter mais informações, consulte Painel do Analytics.

Fevereiro de 2024

- O AWS Wickr agora oferece um teste gratuito de três meses de seu plano Premium para até 30 usuários. As mudanças e limitações incluem:
  - Todos os recursos dos planos Standard e Premium, como controles administrativos ilimitados e retenção de dados, agora estão disponíveis no teste gratuito Premium. O recurso de usuário convidado não está disponível durante o teste gratuito do Premium.
  - O teste gratuito anterior não está mais disponível. Você pode atualizar seu teste gratuito ou plano Standard existente para um teste gratuito Premium se ainda não tiver usado o teste gratuito Premium. Para obter mais informações, consulte Gerenciar plano.

Novembro de 2023

- O recurso de usuários convidados agora está disponível ao público em geral. As mudanças e adições incluem:
  - Capacidade de denunciar abusos cometidos por outros usuários do Wickr.
  - Os administradores podem ver uma lista de usuários convidados com os quais uma rede interagiu e as contagens mensais de uso.
  - Os administradores podem impedir que usuários convidados se comuniquem com sua rede.

  - Preços complementares para usuários convidados.

- Melhorias no controle administrativo
  - Capacidade de excluir/suspender usuários em massa.
  - Configuração adicional de SSO para configurar um período de carência para a atualização do token.

Outubro de 2023

- Melhorias
  - O Wickr já está disponível na região da Europa (Frankfurt) Região da AWS.

Setembro de 2023

- Melhorias
  - As redes do Wickr agora têm a capacidade de se federar em Regiões da AWS. Para obter mais informações, consulte Grupos de segurança.

Agosto de 2023

- Melhorias
  - Agora o Wickr está disponível na região Europa (Londres) Região da AWS.

Julho de 2023

- Melhorias
  - Agora, o Wickr está disponível na região Canadá (Central) Região da AWS.

Maio de 2023

- Melhorias

- Adicionado suporte para usuários convidados. Para ter mais informações, consulte Usuários convidados.

Março de 2023

- O Wickr agora está integrado com o. AWS CloudTrail Para ter mais informações, consulte Registro de chamadas da API do AWS Wickr usando AWS CloudTrail.
- O Wickr agora está disponível em AWS GovCloud (Oeste dos EUA) como. WickrGov Para obter mais informações, consulte AWS WickrGovo Guia AWS GovCloud (US) do usuário.
- Agora, o Wickr oferece suporte à marcação. Para ter mais informações, consulte Gerencie tags de rede. Agora, podem ser criadas várias redes no Wickr. Para ter mais informações, consulte Etapa 1: criar uma rede.

Fevereiro de 2023

- Agora, o Wickr é compatível com o Android Tactical Assault Kit (ATAK). Para ter mais informações, consulte Habilitar o ATAK no painel da rede do Wickr.

Janeiro de 2023

- O login único (SSO) agora pode ser configurado em todos os planos, incluindo teste gratuito e padrão.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.