



Manual do usuário

Amazon One Enterprise



Amazon One Enterprise: Manual do usuário

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon One Enterprise?	1
Dispositivo Amazon One	1
Console Amazon One Enterprise	2
Compra de dispositivos Amazon One	3
Preços do Amazon One Enterprise	3
Como funciona o Amazon One Enterprise	4
Fluxo de trabalho do Amazon One Enterprise	4
Termos-chave do Amazon One Enterprise	5
Configurando o Amazon One Enterprise	6
Cadastrar-se em uma conta da AWS	6
Criar um usuário com acesso administrativo	7
Protegendo sua conta AWS	7
Criação de um usuário com acesso administrativo	7
Entrando como administrador	8
Atribuindo acesso a usuários adicionais	8
Adicionar usuários do Amazon One Enterprise	8
Criar uma unidade	11
Crie instâncias de dispositivos	12
Crie um modelo de configuração	12
Configurar uma instância de dispositivo para ativação	14
Instalando e ativando o Amazon One	16
Entendendo os requisitos	16
Padrões compatíveis	16
Requisito de rede	17
Requisito de energia	17
Entendendo os conceitos de instalação	17
Instalação do pedestal Amazon One Enterprise	18
Instalação do dispositivo Amazon One montável na parede	20
Instalação do Amazon One Device I/O Hub para acesso seguro	31
Ativando o dispositivo Amazon One	42
Inscrevendo e inserindo usuários	44
Criação de uma política de endpoint	44
Autenticação para entrada	44
Gerenciamento de usuários	45

Visualizando usuários inscritos	45
Excluindo usuários inscritos e seus dados biométricos	45
Gerenciando dispositivos Amazon One	47
Manutenção e limpeza de dispositivos Amazon One	47
Para limpar o dispositivo Amazon One	48
Gerenciamento do site	48
Alterando o nome do site	49
Atualizando o endereço do site	49
Gerenciamento de instâncias de dispositivos	49
Visualizando o status da instância do dispositivo	50
Reinicializando um dispositivo Amazon One	50
Atualizando as configurações do dispositivo Amazon One	50
Atualizando credenciais de Wi-Fi	51
Desativando instâncias do dispositivo	51
Segurança	53
Proteção de dados	53
Para usar a criptografia padrão de dados em repouso	55
Para gerenciar sua própria chave de cliente	55
Criptografia de dados em trânsito	56
Gerenciamento de identidade e acesso	56
Público	57
Autenticando com identidades	57
Gerenciando acesso usando políticas	61
Como o Amazon One Enterprise trabalha com IAM	64
Exemplos de políticas baseadas em identidade	71
AWS políticas gerenciadas	80
Ações, recursos e chaves de condição	83
Ações	83
Tipos de recursos	88
Chaves de condição	89
Validação de conformidade	90
Monitorar	92
Eventos de monitoramento	92
Inscreva-se nos eventos do Amazon One Enterprise	92
Tipos de eventos de alteração de status do dispositivo	93
Tipos de eventos de perfil de usuário	95

Eventos de exemplo	96
O status de integridade do dispositivo foi alterado para íntegro	96
O status de integridade do dispositivo foi alterado para crítico	97
A conectividade do dispositivo foi alterada para online	98
A conectividade do dispositivo foi alterada para off-line	98
Nova inscrição bem-sucedida	99
CloudTrail troncos	100
Informações sobre o Amazon One Enterprise em CloudTrail	100
Entendendo as entradas do arquivo de log do Amazon One Enterprise	101
Solução de problemas	104
Solução de problemas de identidade e acesso	104
Não estou autorizado a realizar uma ação no Amazon One Enterprise	104
Quero permitir que pessoas de fora da minha Conta da AWS acessem meus recursos do Amazon One Enterprise	105
Solução de problemas do console Amazon One	105
Não consigo criar um site	106
Não consigo criar uma instância de dispositivo	106
Não consigo criar um modelo de configuração	106
Não consigo criar um código QR de ativação	106
Solução de problemas do dispositivo Amazon One	106
Tela em branco	107
Não consigo me conectar ao Wi-Fi ou à rede	108
Erro do sistema	108
O código QR não é reconhecido	108
Não é possível ler o código QR	109
Vários códigos QR detectados	109
A instância do dispositivo não existe	109
Site não encontrado	109
ZIPO código não corresponde	110
O tempo limite do gateway atingiu o tempo limite	110
Não consigo configurar o dispositivo	110
Dispositivo reiniciado com mensagem de erro e código de erro	110
Logotipo da Amazon na tela do dispositivo sem nenhuma atividade adicional	111
Temporariamente indisponível	111
Dispositivo bloqueado	111
Algo deu errado do nosso lado	111

Temporariamente fora de serviço	112
O dispositivo Amazon One tem danos físicos	112
Não é possível ler a palma da mão	112
Palm não reconhecido	112
Dispositivo bloqueado devido à inatividade prolongada	113
Histórico do documento	114
.....	cxvi

O que é o Amazon One Enterprise?

O Amazon One Enterprise é um novo serviço de autenticação baseado em palma que fornece aos funcionários acesso seguro a edifícios e ativos corporativos, sem o uso de crachás ou senhas/PINs.

Tópicos

- [Dispositivo Amazon One](#)
- [Console Amazon One Enterprise](#)
- [Compra de dispositivos Amazon One](#)
- [Preços do Amazon One Enterprise](#)

Dispositivo Amazon One

O dispositivo Amazon One foi projetado para o Amazon One Enterprise, um serviço de identidade seguro baseado em palma para controle de acesso corporativo. Observe as seguintes especificações do dispositivo:

- Entradas do usuário — Palm Biometrics, correspondência de QR Code
- Interface de host — Wi-Fi (2.4 GHz e 5GHz), Ethernet, 2x USB Tipo A, 1 Tipo B USB
- Feedback do usuário — tela sensível ao toque de 5,5", iluminação, alto-falante, fone de ouvido
- Protocolo de controle de acesso físico — OSDP e Wiegand
- Fonte de alimentação — POE, adaptador AC para DC de 110/220 VAC de entrada fornecido, 30W a 15V
- Segurança — Interruptores de adulteração
- Dimensão (HxWxD mm) — 86 x 85 x 256



Console Amazon One Enterprise

O Amazon One Enterprise inclui um console, que pode ser usado das seguintes formas:

- Um gerente de TI ou de instalações usa o Amazon One Enterprise para criar e gerenciar um site. O site se assemelha a um local físico para as tarefas que a equipe executa ao monitorar e gerenciar dispositivos e perfis de usuário do Amazon One Enterprise. As tarefas do gerente de TI ou de instalações incluem:
 - Criação de um site para conter todas as instâncias do dispositivo Amazon One em um local físico
 - Adicionar um usuário administrador para gerenciar o site e um usuário instalador para acessar os códigos QR de ativação

- Um administrador usa o Amazon One Enterprise para criar instâncias de dispositivos e gerenciar dispositivos Amazon One. As tarefas administrativas incluem:
 - Criação de uma instância de dispositivo em um site
 - Criação de um modelo de configuração para ser aplicado a uma instância do dispositivo
 - Monitorando a integridade do dispositivo e atualizando as configurações do dispositivo
 - Cancelamento de inscrições de usuários
- Um instalador usa o Amazon One Enterprise para acessar códigos QR de ativação para ativar dispositivos. As tarefas do instalador incluem:
 - Acessando um código QR de ativação no console
 - Selecionar um código QR que corresponda à instância do dispositivo a ser ativada
 - Digitalizando o código QR selecionado com o dispositivo Amazon One instalado

Compra de dispositivos Amazon One

[Entre em contato conosco](#) para saber mais sobre o Amazon One Enterprise, e um membro da equipe de desenvolvimento de negócios entrará em contato para compartilhar mais detalhes sobre nossa oferta, incluindo preços, e responder a quaisquer perguntas que você possa ter.

Preços do Amazon One Enterprise

[Entre em contato conosco](#) para saber mais sobre os preços do Amazon One Enterprise.

Como funciona o Amazon One Enterprise

O Amazon One Enterprise é um serviço biométrico baseado em nuvem que usa um dispositivo Amazon One para autenticar um usuário com a biometria da palma da mão. Você pode solicitar dispositivos Amazon One [entrando em contato conosco](#), e você pode se inscrever no serviço de acesso seguro Amazon One Enterprise no AWS Management Console.

Depois de instalar o Amazon One Enterprise, você pode ativar dispositivos e registrá-los Conta da AWS no Amazon One Enterprise Console e no aplicativo de autenticação. No console, você pode visualizar o perfil biométrico de um funcionário inscrito e cancelar a inscrição de um funcionário. Quando os funcionários deixam sua empresa ou perdem o crachá, você pode excluir seus dados biométricos.

O Amazon One Enterprise Console também atua como um local centralizado para gerenciar atividades operacionais, como rastrear dispositivos instalados e visualizar faturas mensais.

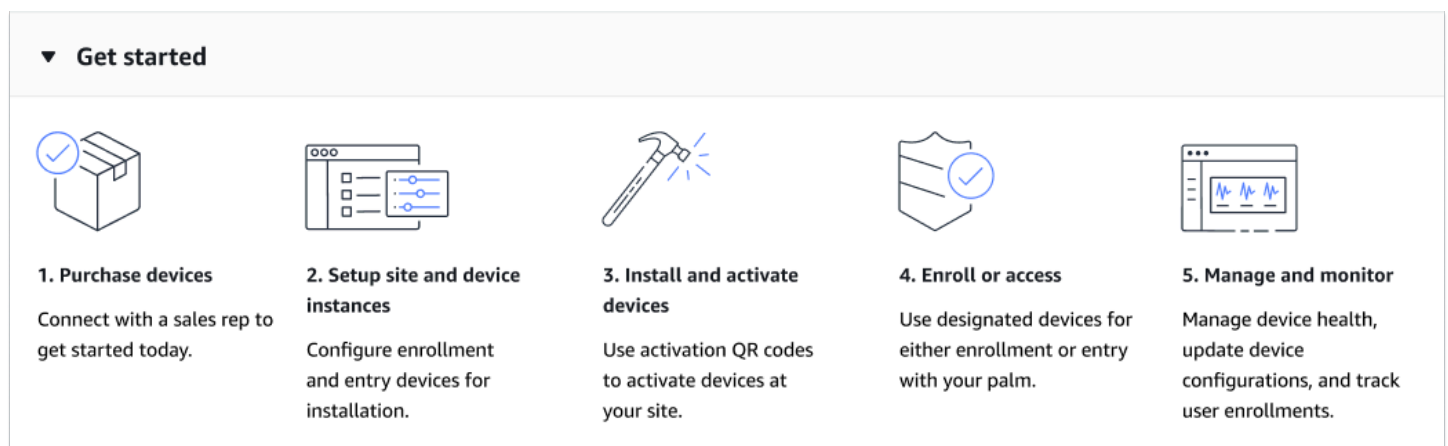
Os funcionários podem se inscrever digitalizando seus crachás e palmas nas estações de inscrição supervisionadas no local. Depois que os funcionários são inscritos, eles podem passar a palma da mão sobre um dispositivo Amazon One para entrar ou sair de um local seguro.

Tópicos

- [Fluxo de trabalho do Amazon One Enterprise](#)
- [Termos-chave do Amazon One Enterprise](#)

Fluxo de trabalho do Amazon One Enterprise

O diagrama a seguir mostra o fluxo de trabalho básico do Amazon One Enterprise.



1. Compre um dispositivo Amazon One [entrando em contato conosco](#).
2. Crie sites e instâncias de dispositivos, configurando o registro e os dispositivos de entrada para instalação.
3. Após a instalação, ative os dispositivos Amazon One digitalizando um código QR seguro específico para a instância do dispositivo.
4. Peça aos funcionários que inscrevam as palmas das mãos e, em seguida, se autentiquem com as palmas das mãos para obter acesso.
5. Use os recursos de gerenciamento e monitoramento: garanta a integridade do dispositivo, mantenha as configurações atualizadas e acompanhe as inscrições de usuários para uma supervisão abrangente.

Termos-chave do Amazon One Enterprise

Estes são os principais termos do Amazon One Enterprise:

- **Local** — O cliente gerenciou edifícios físicos nos quais o cliente instala dispositivos Amazon One Enterprise. Um site deve atender aos requisitos de instalação, rede e energia para seus dispositivos Amazon One Enterprise.
- **Dispositivo** — Um dispositivo biométrico de escaneamento de palma da Amazon One Enterprise para autenticação.
- **Instância do dispositivo** — Uma representação lógica de um dispositivo com configurações. O uso de instâncias de dispositivos permite a troca de dispositivos Amazon One e, ao mesmo tempo, herda automaticamente as configurações e os nomes definidos anteriormente. Uma instância de dispositivo tem um nome definido pelo usuário (convenção de nomenclatura compartilhada com seu software de controle de acesso) e um conjunto de configurações de comunicação. As instâncias do dispositivo têm três estados principais:
 - Precisa de configuração
 - Pronto para ativação
 - Ativo
- **Modelo de configuração** — Um conjunto completo de configurações aplicadas em uma instância do dispositivo.

Configurando o Amazon One Enterprise

Este capítulo explica as etapas básicas para começar a usar o Amazon One Enterprise.

Configurando um site, instâncias de dispositivos e modelos de configuração — Siga estas etapas para criar uma estrutura para adicionar um local físico para abrigar seus dispositivos Amazon One e, em seguida, configurá-los e gerenciá-los usando o console Amazon One Enterprise. Você usará esse processo apenas ocasionalmente, ou mesmo apenas uma vez, dependendo do número de sites, instâncias do dispositivo e seus modelos de configuração.

Tópicos

- [Cadastrar-se em uma conta da AWS](#)
- [Criar um usuário com acesso administrativo](#)
- [Adicionar usuários do Amazon One Enterprise](#)
- [Criar uma unidade](#)
- [Crie instâncias de dispositivos](#)
- [Crie um modelo de configuração](#)
- [Configurar uma instância de dispositivo para ativação](#)

Cadastrar-se em uma conta da AWS

Se você não tiver uma AWS conta, conclua as etapas a seguir para criar uma.

Para se inscrever em uma AWS conta

1. Abra o <https://portal.aws.amazon.com/billing/signup>
2. Siga as instruções online.

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

Quando você se inscreve AWS em uma conta, um usuário raiz da AWS conta é criado. O usuário root tem acesso a todos os AWS serviços e recursos da conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário e use somente o usuário raiz para realizar [tarefas que exijam acesso do usuário raiz](#)

AWSenvia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando <https://aws.amazon.com/> e escolhendo Minha conta

Criar um usuário com acesso administrativo

Depois de se inscrever em uma AWS conta, proteja o usuário raiz da AWS conta, ative o AWS IAM Identity Center e crie um usuário administrativo para que você não use o usuário raiz nas tarefas diárias.

Tópicos

- [Protegendo sua conta AWS](#)
- [Criação de um usuário com acesso administrativo](#)
- [Entrando como administrador](#)
- [Atribuindo acesso a usuários adicionais](#)

Protegendo sua conta AWS

Agora que você fez login na sua conta Amazon One Enterprise, proteja sua conta.

Para proteger sua AWS conta de usuário root

1. Faça login no AWS Management Console como proprietário da conta, escolhendo Usuário raiz e inserindo o endereço de e-mail AWS da sua conta.
2. Na próxima página, insira sua senha.

Para obter ajuda para fazer login usando o usuário root, consulte Como fazer login como usuário root no Guia do usuário AWS de login.

3. Ative a autenticação multifator (MFA) para seu usuário root.

Para obter instruções, consulte Habilitar um MFA dispositivo virtual para o usuário raiz da sua AWS conta (console) no Guia IAM do usuário.

Criação de um usuário com acesso administrativo

Agora que você protegeu sua conta Amazon One Enterprise, crie um usuário com acesso administrativo.

Para criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

Para obter instruções, consulte [Habilitando o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center](#).

2. No IAM Identity Center, conceda acesso administrativo a um usuário.

Para obter um tutorial sobre como usar o diretório do IAM Identity Center como sua fonte de identidade, consulte [Configurar o acesso do usuário com o diretório padrão do IAM Identity Center no Guia do usuário do AWS IAM Identity Center](#).

Entrando como administrador

Agora que você criou um usuário com acesso administrativo, entre como administrador.

Para entrar como usuário com acesso administrativo

- Faça login com seu usuário do IAM Identity Center, usando o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte [Como fazer login no portal de AWS acesso no Guia do usuário AWS de login](#).

Atribuindo acesso a usuários adicionais

Agora que você entrou como administrador, pode atribuir acesso a outros usuários.

Para atribuir acesso a usuários adicionais

- Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

Para obter instruções, consulte [Adicionar grupos no Guia do usuário do AWS IAM Identity Center](#).


Adicionar usuários do Amazon One Enterprise

Além dos usuários administradores, você também pode adicionar usuários que não têm permissões administrativas. Por exemplo, esses usuários podem ser instaladores que acessam o console do

Amazon One Enterprise somente para recuperar códigos QR de ativação do dispositivo para ativar dispositivos Amazon One.

Para adicionar um usuário do Amazon One Enterprise

1. Siga o procedimento de login adequado ao seu tipo de usuário, conforme descrito em [Como fazer login AWS no](#) Guia do Início de Sessão da AWS usuário.
2. No painel de navegação, selecione Usuários e, em seguida, selecione Adicionar usuários.
3. Na página Especificar detalhes do usuário, em Detalhes do usuário, em Nome de usuário, insira o nome do novo usuário. É o nome de login para a AWS.

 Note

O número e o tamanho dos IAM recursos em um Conta da AWS são limitados. Para obter mais informações, consulte [IAMe AWS STS cotas](#). Os nomes de usuário podem ser uma combinação de até 64 letras, dígitos e os seguintes caracteres: mais (+), igual (=), vírgula (,), ponto (.), sinal de arroba (@), sublinhado (_) e hífen (-). Os nomes devem ser exclusivos dentro de uma conta. Eles não são diferenciados por letras maiúsculas e minúsculas. Por exemplo, você não pode criar dois usuários chamados TESTUSERe testuser. Quando um nome de usuário é usado em uma política ou como parte de umaARN, o nome diferencia maiúsculas de minúsculas. Quando é exibido para os clientes no console, por exemplo, como durante o processo de login, o nome de usuário não diferencia maiúsculas de minúsculas.

4. Será exibida uma mensagem perguntado se você está fornecendo acesso ao console para uma pessoa. Selecione Fornecer acesso ao usuário ao — AWS Management Console opcional.
5. Selecione Quero criar um IAM usuário.
6. Em Senha do console, selecione uma das opções a seguir:
 - Senha gerada automaticamente — O usuário recebe uma senha gerada aleatoriamente que atende à política de [senha da conta](#). É possível visualizar ou baixar a senha ao acessar a página Recuperar senha.
 - Senha personalizada — O usuário recebe a senha que você digita no campo.
7. (Opcional) Por padrão, os usuários devem criar uma nova senha no próximo login (recomendado) é selecionada para garantir que o usuário precise alterar sua senha na primeira vez em que fizer login.

Note

Se um administrador tiver habilitado a configuração [Permitir que os usuários alterem sua própria senha da política de senha da conta](#), essa caixa de seleção não terá nenhum efeito. Caso contrário, ele associa automaticamente uma política AWS gerenciada nomeada [IAMUserChangePassword](#) aos novos usuários. A política concede a eles permissão para alterar suas próprias senhas.

8. Escolha Próximo.
9. Na página Definir permissões, selecione Anexar políticas diretamente.
10. Selecione as políticas que você deseja anexar ao usuário.
 - [AmazonOneEnterpriseReadOnlyAccess](#)
 - [AmazonOneEnterpriseInstallerAccess](#)

Note

[AmazonOneEnterpriseInstallerAccess](#) a política gerenciada fornecerá ao usuário acesso aos códigos QR de ativação somente no console do Amazon One Enterprise. Essa política é ideal para empresas que contratam terceiros para instalar dispositivos Amazon One.

11. Escolha Próximo.
12. (Opcional) Na página Revisar e criar, em Etiquetas, selecione Adicionar nova etiqueta para adicionar metadados ao usuário anexando etiquetas aos pares de chave-valor. Para obter mais informações sobre o uso de tags em IAM, consulte [IAM Recursos de marcação](#).
13. Revise todas as escolhas que você fez até agora. Quando você estiver pronto para continuar, selecione Criar usuário.
14. Na página Recuperar senha, obtenha a senha atribuída ao usuário:
 - Selecione Exibir ao lado da senha para visualizar a senha do usuário e poder gravá-la manualmente.
 - Selecione Baixar o.csv para baixar as credenciais de login do usuário como um arquivo.csv que você pode salvar em um local seguro.

15. Selecione Instruções de login de e-mail. Seu cliente de e-mail local é aberto com um rascunho que você pode personalizar e enviar ao usuário. O modelo de e-mail inclui os seguintes detalhes de cada usuário:

- Nome do usuário
- URL para a página de login da conta. Use o exemplo a seguir, substituindo o número de ID ou alias da conta:

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

Important

A senha do usuário não é incluída no e-mail gerado. É necessário fornecer a senha ao usuário de forma que esteja em conformidade com as diretrizes de segurança de sua organização.

Criar uma unidade

Agora que você fez login no AWS Management Console, você pode usar o console do Amazon One Enterprise para criar seu site.

Important

O Amazon One Enterprise está disponível somente na região Leste dos EUA (Norte da Virgínia).

Como criar uma unidade

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. Escolha Ir para a visão geral.
3. No painel de navegação, selecione Locais.
4. Escolha Criar sites.
5. Em Informações do site, em Nome do site, insira um nome para o site.

6. Em Endereço físico, insira o endereço do site em que seus dispositivos Amazon One serão instalados.
7. (Opcional) Para adicionar uma tag ao site, insira um par de valores-chave em Tags e escolha Adicionar nova tag. Para remover essa tag antes de criar o site, escolha Remover.
8. Escolha Criar site para criar o site.

Crie instâncias de dispositivos

Agora que você criou um site no AWS Management Console, você pode usar o console Amazon One Enterprise para criar instâncias de dispositivos.

Para criar uma instância de dispositivo

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Instâncias do dispositivo. Verifique se você está na guia Instâncias não ativadas.
3. Em Detalhes da instância, escolha um site na lista suspensa Site ou crie um novo site escolhendo o botão Criar site.
4. Insira manualmente o nome de cada instância individual do dispositivo.
5. (Opcional) Para adicionar uma tag à instância do dispositivo, insira um par de valores-chave em Tags e escolha Adicionar nova tag. Para remover essa tag antes de criar a instância do dispositivo, escolha Remover.
6. Escolha Criar instâncias para criar as instâncias do dispositivo.

Note

Observação: as instâncias do dispositivo precisam ser configuradas antes que a instalação possa ocorrer.

Crie um modelo de configuração

Agora que você criou instâncias de dispositivos, você pode usar o console do Amazon One Enterprise para criar um modelo de configuração.

Para criar um modelo de configuração

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Modelos de configuração.
3. Selecione Criar modelo.
4. Em Informações do modelo, em Nome do modelo, insira um nome para o modelo de configuração.
5. Em Configurações do dispositivo, selecione um modo de operação.

To configure Enrollment operating mode

1. (Opcional) Em Configuração de Wi-Fi, forneça suas credenciais de Wi-Fi.
2. (Opcional) Para adicionar uma tag ao site, insira um par de valores-chave em Tags e escolha Adicionar nova tag. Para remover essa tag antes de criar o site, escolha Remover.
3. Selecione Configurar.

To configure Entry operating mode

1. Em Configurações do painel de controle, forneça as configurações de comunicação para que os dispositivos Amazon One se comuniquem com seu painel de controle.
2. Em Configurações do formato do selo, forneça as configurações que especificam o layout do formato do crachá da sua empresa.
3. (Opcional) Em Configuração de Wi-Fi, forneça suas credenciais de Wi-Fi.
4. (Opcional) Para adicionar uma tag ao site, insira um par de valores-chave em Tags e escolha Adicionar nova tag. Para remover essa tag antes de criar o site, escolha Remover.
5. Selecione Configurar.

Important

Você deve configurar pelo menos um dispositivo de inscrição e um dispositivo de entrada para habilitar todos os recursos do Amazon One Enterprise para acesso seguro.

Configurar uma instância de dispositivo para ativação

Depois que uma instância do dispositivo é criada, você configura a instância do dispositivo com um modelo de configuração criado anteriormente (consulte [Crie um modelo de configuração](#)) ou pode adicionar configurações manualmente.

Para configurar uma instância de dispositivo para ativação

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Instâncias do dispositivo. Verifique se você está na guia Instâncias não ativadas.
3. Selecione uma ou mais instâncias para configurar.
4. Selecione Configurar.
5. Em Configurações do dispositivo, selecione um dos dois métodos de entrada:
 - a. Para a opção Usar modelo, escolha um modelo no menu suspenso. Revise ou faça alterações nessas informações de configuração importadas.

Para a opção Criar modelo, consulte [Crie um modelo de configuração](#).


- b. Para a opção Entrada manual, selecione um Modo operacional.


To configure Enrollment operating mode

- a. (Opcional) Em Configuração de Wi-Fi, forneça uma credencial de Wi-Fi.
- b. (Opcional) Para adicionar uma tag ao site, insira um par de valores-chave em Tags e escolha Adicionar nova tag. Para remover essa tag antes de criar o site, escolha Remover.
- c. Selecione Configurar.

To configure Entry operating mode

- a. Em Configurações do painel de controle, forneça as configurações de comunicação para que os dispositivos Amazon One se comuniquem com seu painel de controle.
- b. Em Configurações do formato do selo, forneça as configurações que especificam o layout do formato do crachá da sua empresa.
- c. (Opcional) Em Configuração de Wi-Fi, forneça uma credencial de Wi-Fi.

- d. (Opcional) Para adicionar uma tag ao site, insira um par de valores-chave em Tags e escolha Adicionar nova tag. Para remover essa tag antes de criar o site, escolha Remover.
 - e. Selecione Configurar.
6. Na tabela Instâncias não ativadas, o estado da instância deve ser exibido  **Ready for activation**
7. Valide se os códigos QR de ativação estão disponíveis para ativação. No painel de navegação, escolha Código QR de ativação.
8. Na lista suspensa Selecionar um site, selecione um site.
9. Em Informações do site, valide o endereço do site.
10. Em Códigos QR de ativação, cada instância do dispositivo tem um código QR correspondente. Escolha Obter código QR para mostrar os códigos QR de ativação.

 **Important**

Você deve configurar pelo menos um dispositivo de inscrição e um dispositivo de entrada para habilitar todos os recursos do Amazon One Enterprise para acesso seguro.

Instalando e ativando o Amazon One

Depois que o console do Amazon One Enterprise estiver configurado, as próximas etapas são instalar os dispositivos Amazon One Enterprise em seu site e ativá-los.

Note

Esta seção se concentra na instalação e usa um navegador móvel para acessar e AWS Management Console obter códigos QR de ativação do dispositivo.

Tópicos

- [Entendendo os requisitos](#)
- [Entendendo os conceitos de instalação](#)
- [Instalação do pedestal Amazon One Enterprise](#)
- [Instalação do dispositivo Amazon One montável na parede](#)
- [Instalação do Amazon One Device I/O Hub para acesso seguro](#)
- [Ativando o dispositivo Amazon One](#)

Entendendo os requisitos

Um dispositivo Amazon One pode ser instalado em qualquer local corporativo ou comercial que tenha portas que possam ser controladas eletricamente.

Requisito do painel de controle

Os dispositivos Amazon One podem se conectar à maioria dos painéis de controle de acesso padrão como um leitor. Os dispositivos Amazon One oferecem suporte aos seguintes protocolos:

- OSDP(v1 e v2)
- Wiegand

Requisito de rede

Os dispositivos Amazon One devem estar sempre conectados à Internet para operação normal. A conectividade com a Internet pode ser fornecida por Ethernet com fio ou Wi-Fi. A largura de banda mínima exigida é de 10 Mbps.

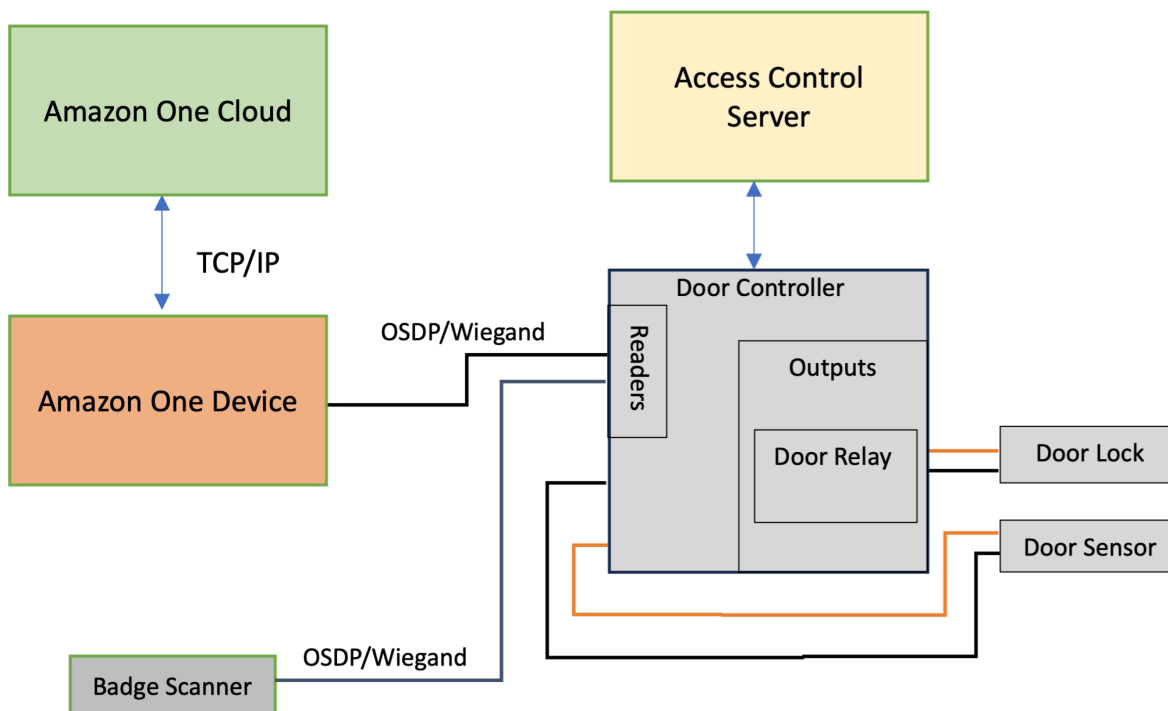
Requisito de energia

Os dispositivos Amazon One podem ser alimentados de duas maneiras:

- Usando o adaptador de alimentação de 120 V fornecido na caixa.
- Usando um dispositivo habilitado para PoE+.

Entendendo os conceitos de instalação

Para proteger adequadamente o acesso ao prédio, a Amazon One Enterprise recomenda que você instale o dispositivo como parte de um ambiente típico de controle de acesso, conforme descrito no diagrama de blocos a seguir.



Um ambiente de controle de acesso normalmente consiste nos seguintes componentes:

- **Dispositivo Amazon One:** é o dispositivo de reconhecimento de palma que executará a autenticação biométrica para identificar a pessoa que está tentando acessar uma área segura do prédio.
- **Servidor de controle de acesso:** esse componente normalmente controla os direitos de acesso dos usuários à área segura. Os crachás IDs das pessoas que têm acesso à área geralmente são armazenados nesse servidor. Esse servidor armazena em cache o que é relevante IDs para os controladores de porta apropriados.
- **Controlador de porta:**
 - Um dispositivo Amazon One se conecta ao servidor Door Controller por meio de uma OSDP interface.
 - Se uma interface Wiegand for necessária, um COTS OSDP-to-Wiegand conversor pode ser usado.
 - Após a autenticação bem-sucedida, o dispositivo Amazon One envia o ID do crachá do usuário para o Door Controller.
 - O Door Controller responde com uma decisão, que então permite que o dispositivo Amazon One exiba uma mensagem de Acesso concedido ou Acesso negado.
- **Scanner de crachá:** Um scanner de crachá é normalmente usado para digitalizar RFID crachás e enviar o número do crachá para o servidor de controle de acesso. Com o Amazon One Enterprise, um scanner de crachás é conectado ao dispositivo Amazon One de inscrição para permitir que os crachás dos funcionários sejam digitalizados e associados aos perfis de suas palmas.

Instalação do pedestal Amazon One Enterprise

Esta seção descreve os requisitos de localização e as etapas necessárias para instalar um pedestal Amazon One Enterprise.



Antes de iniciar a instalação, verifique se os seguintes pré-requisitos foram atendidos:

- Se estiver usando POE + para alimentar o dispositivo, certifique-se de que o cabeamento Cat6 esteja instalado e que um injetor ou chave POE + esteja disponível para uso.
- Se a fonte de alimentação CA (120 V) estiver sendo usada, a tomada CA deve estar disponível a menos de 20 pés do AOE pedestal.
- O piso deve estar nivelado e limpo.
- O pedestal não deve bloquear a porta ou a faixa.
- Todo o excesso de cabo deve ser mantido dentro do pedestal e protegido.

Para instalar o pedestal do dispositivo Amazon One

1. Remova o pedestal Amazon One Enterprise da embalagem.
2. Remova a porta desparafusando os dois parafusos resistentes a violações M4.
3. Conecte o cabo de alimentação. Passe o cabo pelo orifício na placa base do pedestal.
4. Enrole qualquer excesso de cabo de alimentação dentro do pedestal.
5. Passe o cabo Ethernet (Cat5E ou superior) pela placa inferior do pedestal e conecte-o à porta Ethernet.
6. Passe o cabo Ethernet (Cat5E ou superior) pela placa inferior do pedestal e conecte-o à porta Ethernet.
7. Instale um laço de ferrite no cabo Ethernet 2 polegadas acima da base do pedestal.
8. Passe o cabo RS485 serial do painel de controle de acesso (ou do leitor de crachás) até o pedestal, com 1 pé de excesso de comprimento.
9. Instale um laço de ferrite no RS485 cabo 2 polegadas acima da base do pedestal.
10. Conecte a alimentação à tomada e confirme se o dispositivo Amazon One está ligado.
11. Reconecte a porta ao pedestal e aperte novamente os dois parafusos de resistência à violação M4 para prendê-los.

Instalação do dispositivo Amazon One montável na parede

Esta seção detalha os requisitos de localização e as etapas necessárias para instalar seu dispositivo Amazon One montável na parede.

Antes de iniciar a instalação, verifique o seguinte:

- O dispositivo Amazon One montável na parede é apenas para uso interno.
- A parede está nivelada.
- A parte superior do suporte de parede não deve estar a mais de 44-46" do solo após a montagem.
- Todo o excesso de cabo está atrás do suporte de parede e preso.
- Para alimentação via Ethernet (PoE++):

Certifique-se de que um switch IEEE 802.3bt (Tipo 3) Classe 6 POE ++ (endspan) ou injetor (midspan) esteja disponível para uso, que esteja listado ou certificado e esteja em conformidade com 62368-1. IEC

Use somente AOE com uma fonte de PoE++ aprovada.

A fonte PoE++ deve estar localizada no mesmo prédio.

- Para entrada de alimentação de 15V DC, você só deve usar o dispositivo Amazon One com uma fonte de alimentação de NEC Classe 2 ou com limitação de energia aprovada que esteja listada ou certificada.

Ferramentas necessárias:

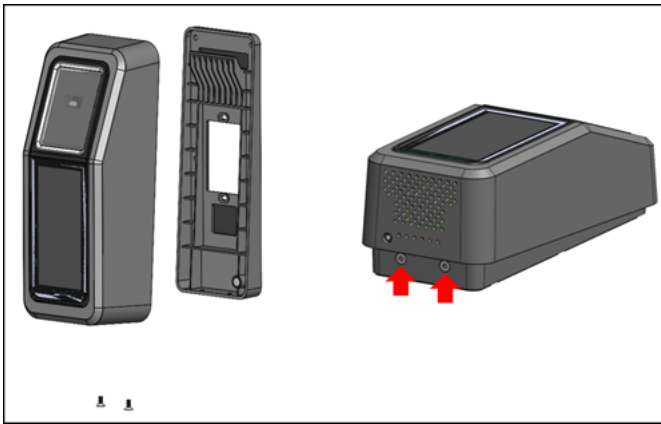
- Broca de parede seca ou alvenaria de 1/4" se forem necessárias âncoras de parede
- Decapador de fios
- Broca de 7/64" para fazer furos piloto
- Chave de fenda Phillips #2
- Chave de fenda de cabeça plana de 0,5 mm x 2 mm
- Controlador Torx seguro T12
- Lápis
- Nível

Incluído no dispositivo Amazon One montável na parede:

- 6x #8 Ancoragens de drywall
- 6x #8 -32 Parafusos de 1 polegada de comprimento
- 2x #6 -32 Parafusos de máquina de 1 polegada
- 2x conectores de bloco de terminais de 6 posições
- 2 parafusos de cabeça plana Torx Security M4x10

Para instalar a placa de montagem na parede do seu dispositivo Amazon One

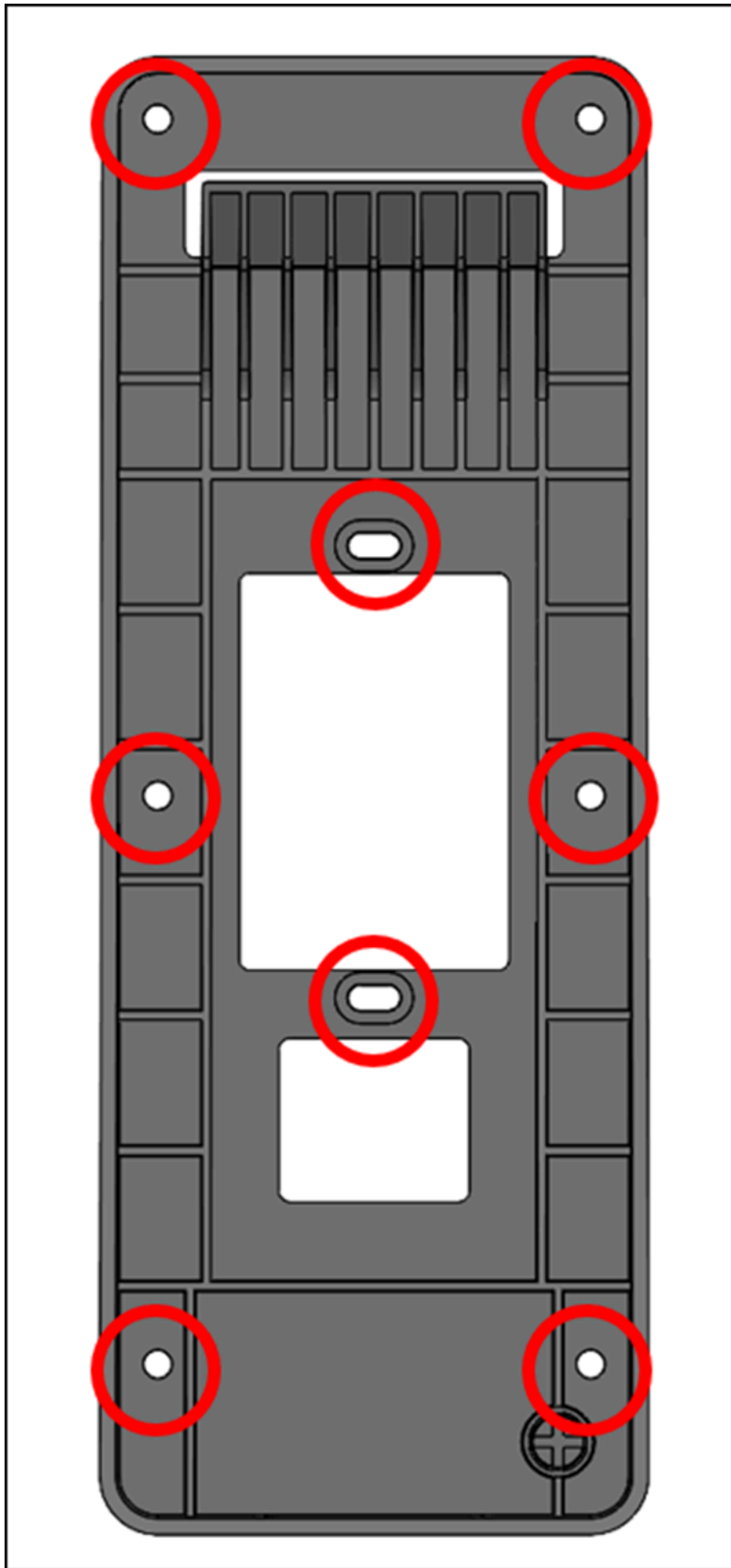
1. Remova seu dispositivo Amazon One da embalagem.
2. Separe a placa de montagem do seu dispositivo Amazon One removendo os dois parafusos de segurança Torx inferiores.



3. Posicione a placa de montagem na parede no local desejado. Use o suporte como modelo para marcar os seis orifícios externos dos parafusos, conforme mostrado na imagem a seguir.

(Opcional) Se uma caixa de grupo único estiver disponível na posição de instalação, faça o seguinte:

- Monte frouxamente a placa na caixa giratória inserindo os parafusos da máquina #6 -32 incluídos nos orifícios oblongos.
- Verifique se a placa de montagem está nivelada.
- Use a placa de montagem como modelo para marcar as seis posições dos parafusos com um lápis. Você pode usar os orifícios oblongos e o parafuso #6 -32 como suporte extra para a placa de montagem. Não use as posições dos parafusos #6 -32 como principal meio de montagem da placa de parede.



4. Se for montado em superfícies de estuque, drywall, tijolo ou concreto, faça furos de 1/4" em cada local marcado e, em seguida, instale as âncoras de parede pressionando-as no orifício até que a âncora fique nivelada com a parede.

Se for montado em uma superfície de madeira, as âncoras não são necessárias e somente orifícios piloto de 7/64" são necessários nos locais marcados.

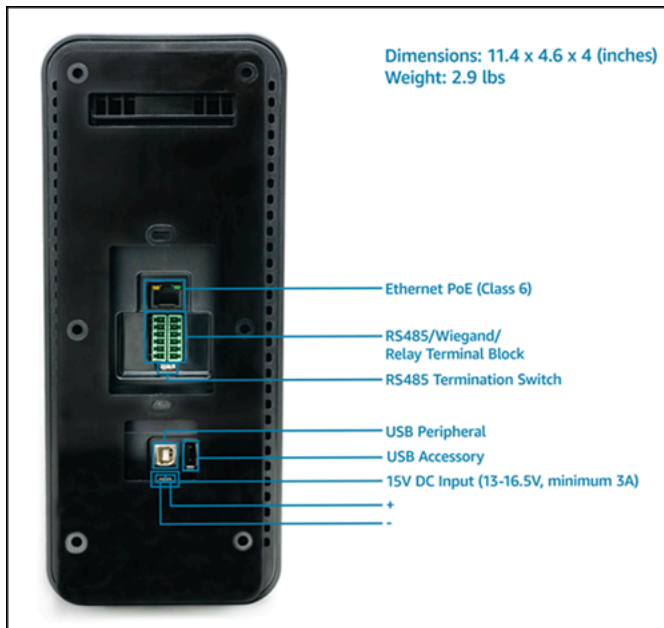
5. Fixe frouxamente a placa de parede na parede usando os parafusos de madeira #8 nas posições de ancoragem.
6. Depois que todos os fixadores estiverem no lugar, verifique se a placa de montagem está nivelada.
7. Aperte os parafusos para fixar a placa de montagem na parede.

Para conectar seu dispositivo Amazon One montável na parede

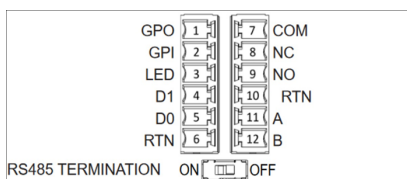
Você pode configurar o dispositivo Amazon One com OSDP os protocolos de controle de acesso Weigand. Para simplificar a instalação, o dispositivo Amazon One utiliza conectores de bloco de terminais (Mfg P/N: Phoenix Contact 1767694). Você também tem a opção de configurar o dispositivo Amazon One para controlar diretamente dispositivos externos usando o relé interno ou as conexões de entrada e saída de uso geral.

1. Para determinar a configuração de fiação apropriada para sua aplicação, consulte o diagrama a seguir e a Tabela de Conexões.

Para obter as características elétricas detalhadas dos sinais, consulte as instruções de fiação.



Conexões



Pin	Conexão	Descrição	Use
1	GPO	Saída de uso geral	Sinal de saída digital - opcional
2	GPI	Entrada de uso geral	Sinal de entrada digital — Opcional
3	LED	Wiegand LED	Wiegand — Opcional LED
4	D1	Wiegand D1	Dados Wiegand 1 — Fio branco
5	D0	Wiegand D0	Dados Wiegand 0 — Fio verde

Pin	Conexão	Descrição	Use
6	RTN	Retorno do sinal	Wiegand Ground — Fio preto
7	Com	Relé comum	Relé de contato comum — Fio branco
8	NC	Relé normalmente fechado	Relé de contato normalmente fechado — fio laranja
9	NO	Relé normalmente aberto	Relé de contato normalmente aberto — fio amarelo
10	RTN	Retorno do sinal	OSDPretorno — Fio preto
11	A	RS485_A/D1/ Relógio	OSDPD1 — Fio branco
12	B	RS485_B/D0/ Dados	OSDPD0 — Fio verde

- Ao instalar um fio, retire 3mm-5mm da extremidade do fio.
- Insira a extremidade descascada do fio na posição desejada do terminal.
- Usando uma chave de fenda de ponta chata, gire o parafuso de retenção do terminal no sentido horário para prender o fio até que esteja bem encaixado. Não aperte demais.
- Após a fixação, puxe suavemente o fio para garantir que ele esteja encaixado.
- Depois de fazer as conexões necessárias, insira o plugue no receptáculo correspondente do bloco de terminais do seu dispositivo Amazon One.
- Insira o cabo Ethernet Cat6 na tomada. RJ45

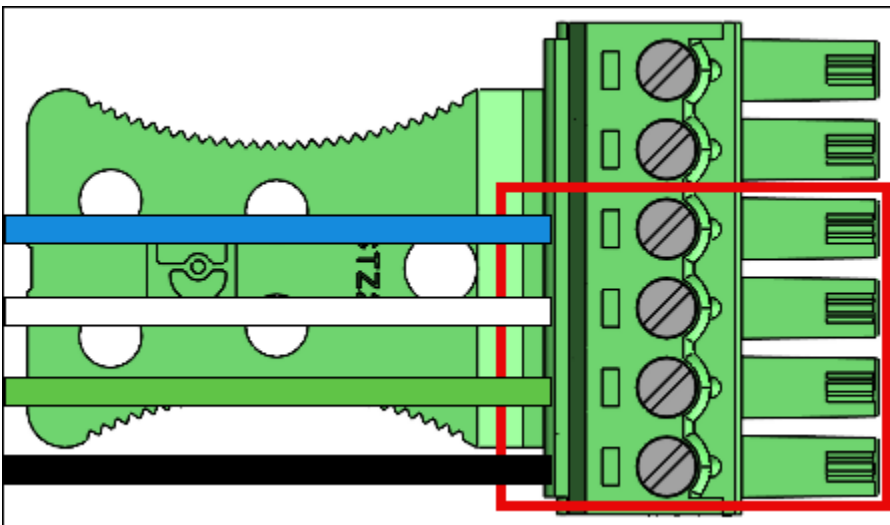
8. Posicione o dispositivo Amazon One de forma que o gancho na placa de parede deslize para dentro da abertura na parte traseira do dispositivo.
9. Certifique-se de que os cabos não estejam presos entre o dispositivo e a placa de montagem e deixe o dispositivo girar e se encaixar na posição correta.
10. Proteja seu dispositivo Amazon One na placa de montagem com dois parafusos de cabeça plana Torx Security M4x10.
11. Aperte manualmente os parafusos. Não aperte demais.

Para conectar seu dispositivo Amazon One montável na parede

Instale somente os fios necessários para sua aplicação.

Conexões Wiegand

- Insira o fio azul no pino 3 (LED).
- Insira o fio branco no pino 4 (D1).
- Insira o fio verde no pino 5 (D0).
- Insira o fio preto no pino 6 (RTN).



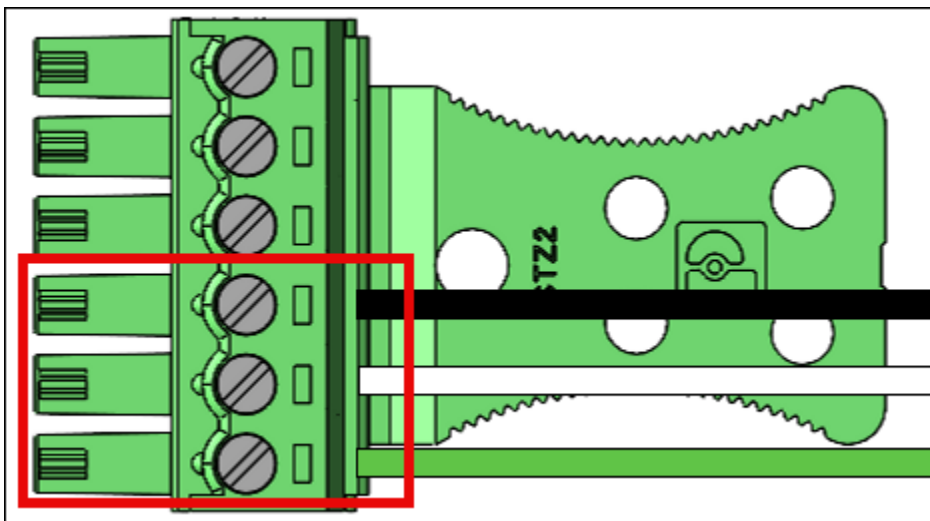
Fiação de saída Wiegand

Pin	Conexão	Descrição	Use
3	LED	Wiegand LED	LED Entrada Wiegand — Opcional (5V) TTL
4	D1	Wiegand D1	Saída Wiegand D1 (5V) TTL
5	D0	Wiegand D0	Saída Wiegand D0 (5V) TTL
6	RTN	Retorno do sinal	Referência Wiegand GND

Ligue o interruptor de RS485 terminação se o dispositivo for a última unidade na linha. Essa chave ativa a terminação do resistor de 120 Ohms na linha.

RS485 conexões

- Insira o fio preto no pino 10 (RTN).
- Insira o fio branco no pino 11 (A).
- Insira o fio verde no pino 12 (B).

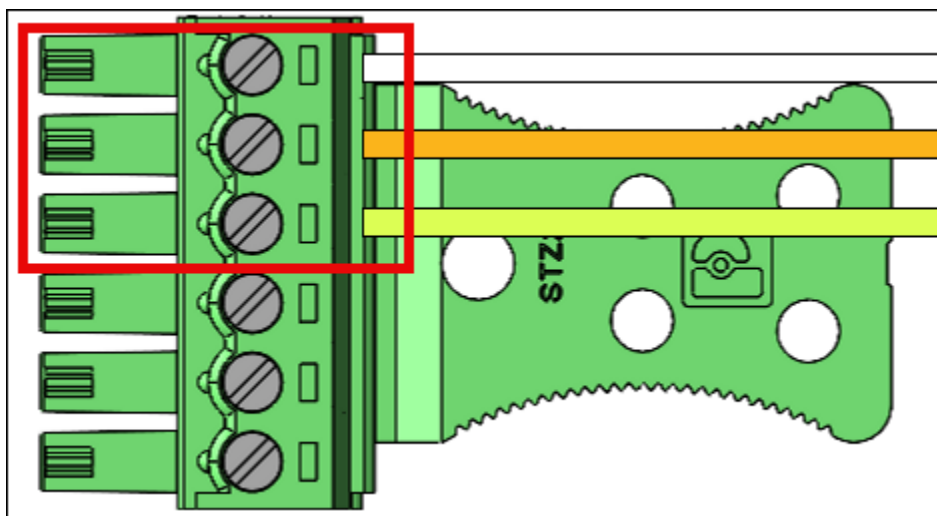


RS485fiação

Pin	Conexão	Descrição	Use
10	RTN	Retorno do sinal	Ground
11	A	RS485_A/D1/ Relógio	RS485sinal não inversor
12	B	RS485_B/D0/ Dados	RS485sinal inversor

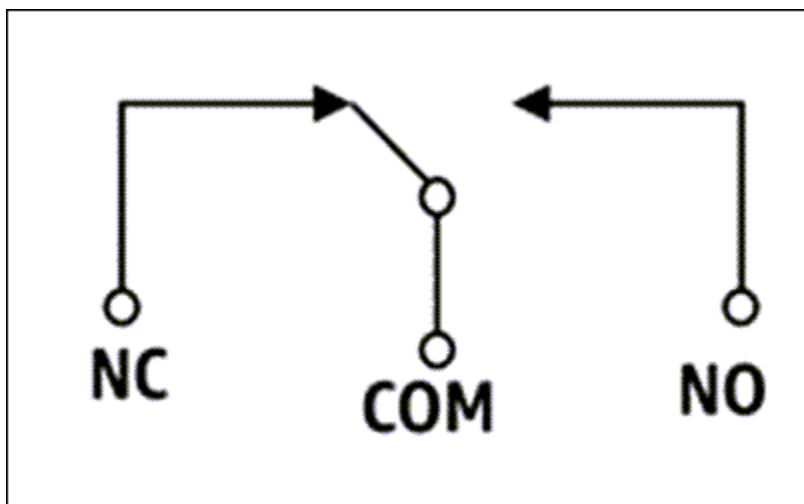
Conexões de relé

- Insira o fio branco no pino 7 (COM).
- Insira o fio laranja no pino 8 (NC).
- Insira o fio amarelo no pino 9 (NO).



Fiação de relé

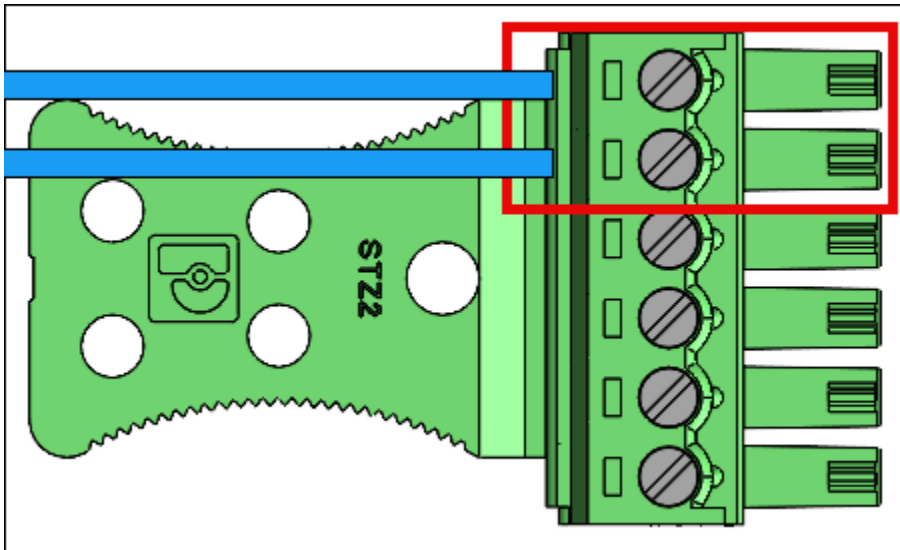
Pin	Conexão	Descrição	Use
7	COM	Relé comum	Relé de contato comum — fio branco
8	NC	Relé normalmente fechado	Relé de contato normalmente fechado — fio laranja
9	NO	Relé normalmente aberto	Relé de contato normalmente aberto — fio amarelo



O relé deve ser operado de acordo com as classificações de segurança especificadas VAC 30/60VDC, 60W máx.

Conexões de entrada/saída digitais

- Insira o fio azul no pino 1 (GPO).
- Insira o fio azul no pino 2 (GPI).



Pin	Conexão	Descrição	Use
1	GPO	Saída de uso geral	Sinal de saída digital (5V)
2	GPI	Entrada de uso geral	Sinal de entrada digital (3.6V — 5V)

- As conexões de entrada/saída digital devem ser operadas conforme listado.

Consulte [Ativando o dispositivo Amazon One](#) para ativar seu dispositivo Amazon One.

Instalação do Amazon One Device I/O Hub para acesso seguro

Esta seção detalha os requisitos de localização e as etapas necessárias para instalar seu dispositivo Amazon One Enterprise (AOE) com o I/O Hub.

Antes de iniciar a instalação, verifique o seguinte:

- O dispositivo Amazon One com I/O Hub é somente para uso interno.
- Para alimentação via Ethernet (PoE++):

Certifique-se de que um switch IEEE 802.3bt (Tipo 3) Classe 6 POE ++ (endspan) ou injetor (midspan) esteja disponível para uso, que esteja listado ou certificado e esteja em conformidade com 62368-1. IEC

Use somente o dispositivo Amazon One com uma fonte de PoE++ aprovada.

A fonte PoE++ deve estar localizada no mesmo prédio.

- Para entrada de alimentação de 15 V DC, você só deve usar o dispositivo Amazon One com uma fonte de alimentação aprovada de NEC Classe 2 ou com limitação de energia que esteja listada ou certificada. Consulte a seção DC opcional abaixo.

Ferramentas necessárias:

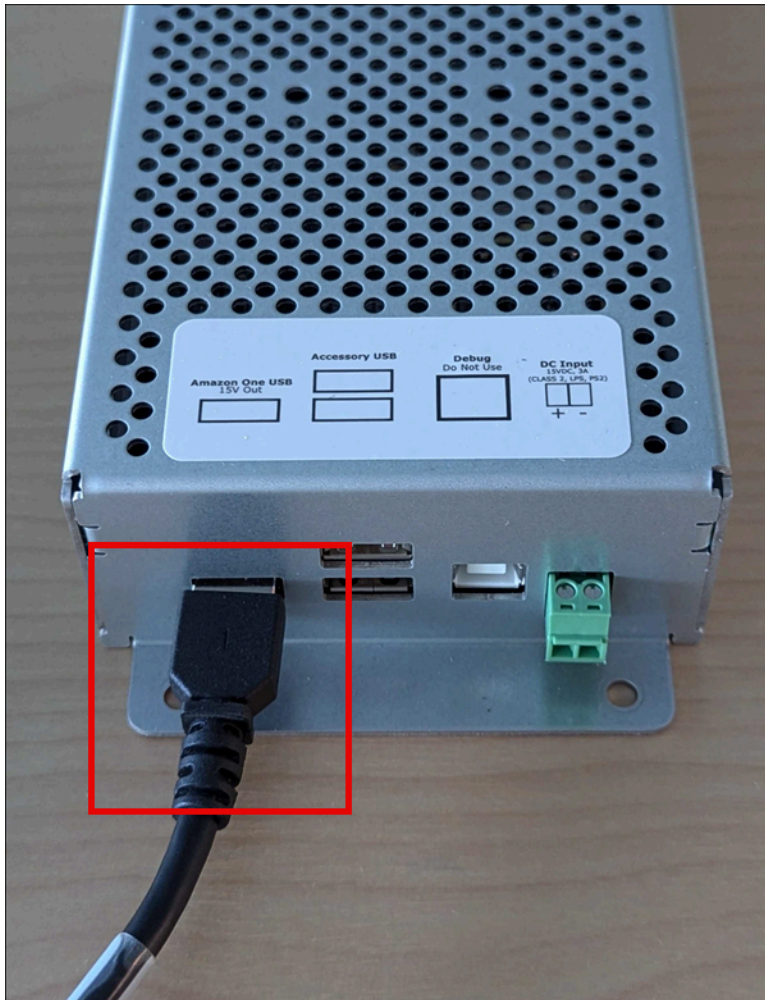
- Decapador de fios
- Chave de fenda Phillips #2
- Chave de fenda de cabeça plana de 0,5 mm x 2 mm

Incluído no dispositivo Amazon One com I/O Hub:

- 2x conectores de bloco de terminais de 6 posições
- Conector de plugue DC
- Cabo de alimentação/dados de 72"

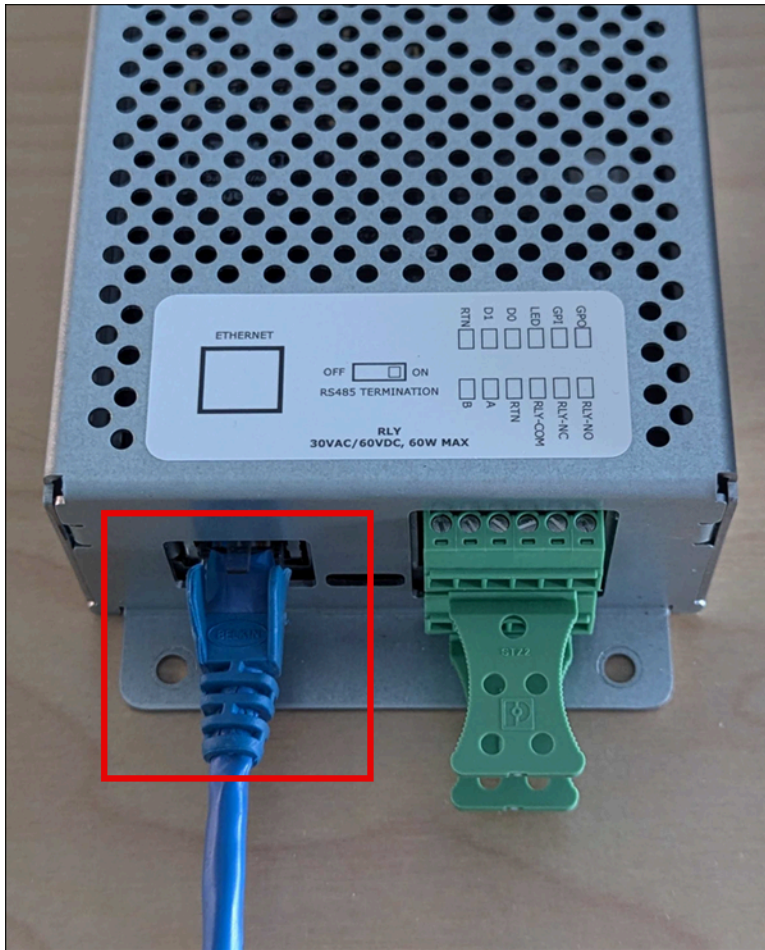
Para instalar o hub de E/S para seu dispositivo Amazon One

1. Remova seu dispositivo Amazon One com o I/O Hub da embalagem.
2. Proteja o hub de E/S no local desejado.
3. Conecte o USB cabo Amazon One na porta do hub de E/S.



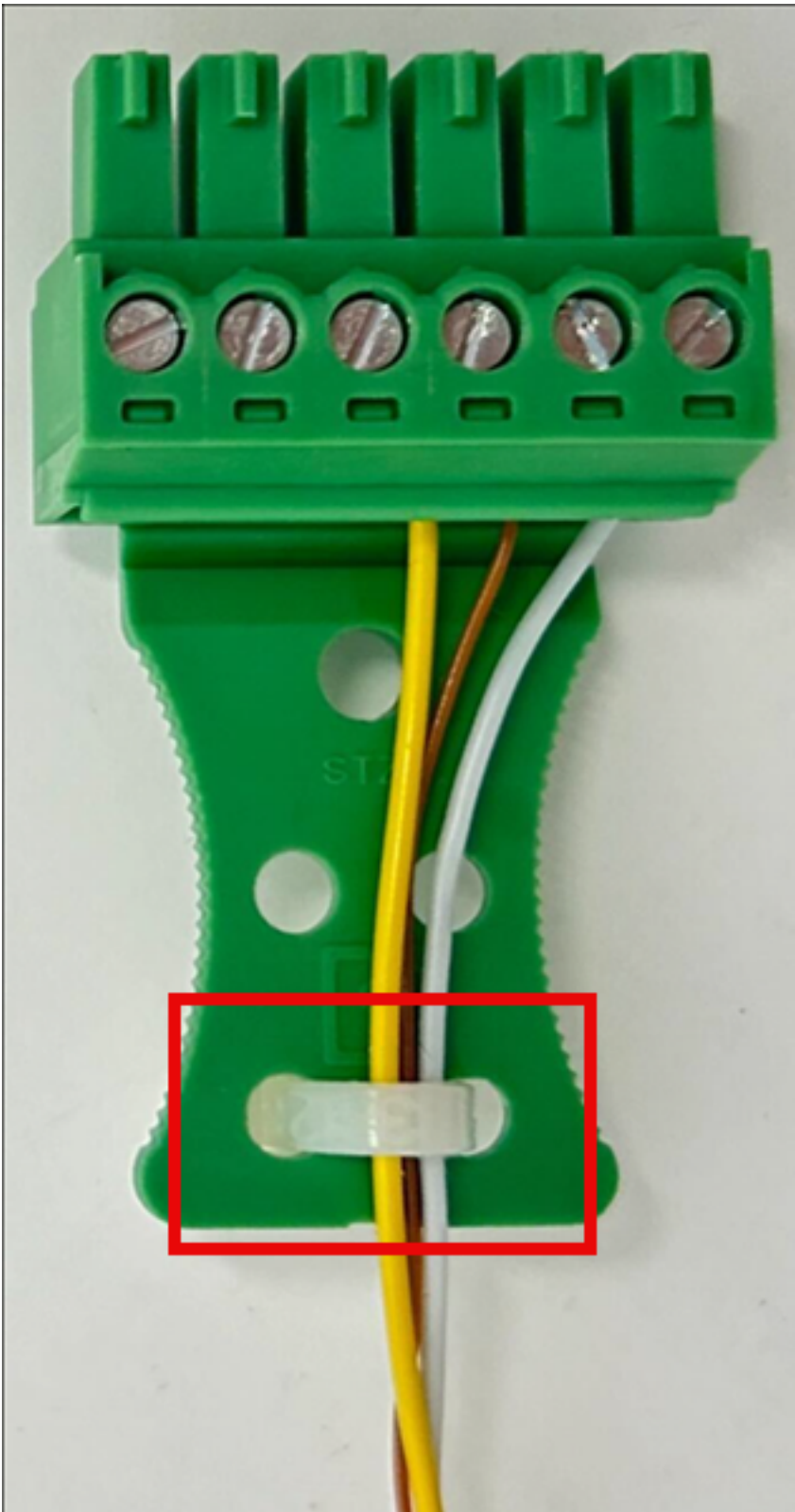
4. Para alimentação POE ++, conecte o cabo Ethernet da fonte POE ++ à porta do hub de E/S.

Opcional: Para alimentação DC, consulte a seção de instalação da fiação DC abaixo.



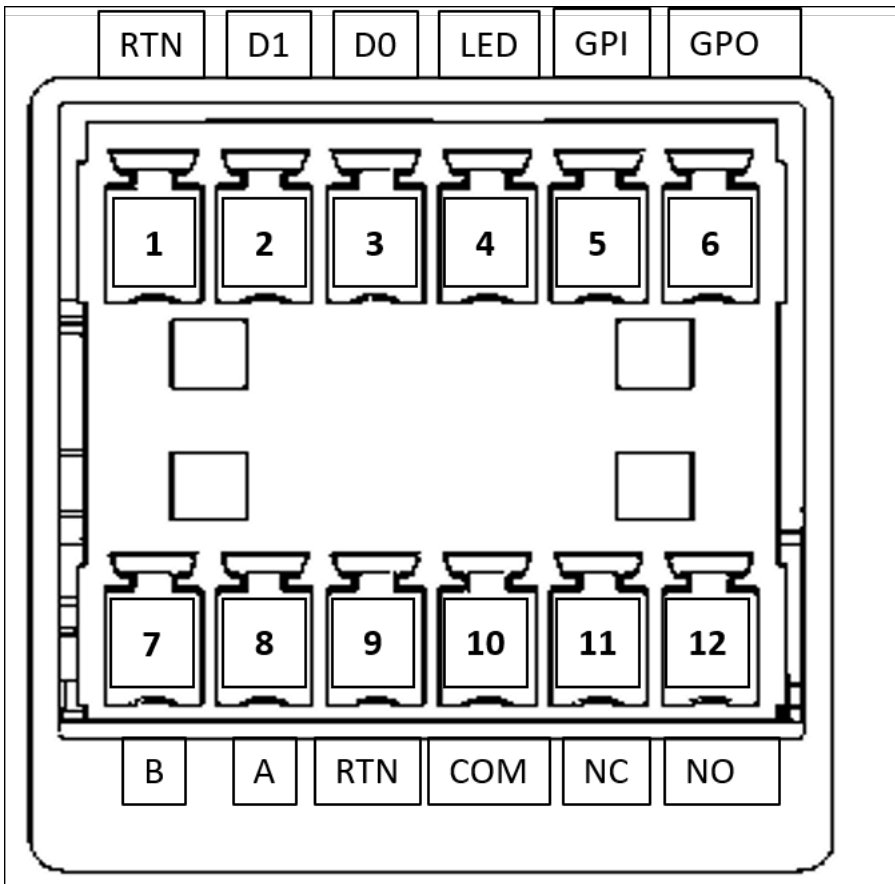
Para conectar o hub de E/S ao seu dispositivo Amazon One

- Instale um circuito de gotejamento para evitar que líquidos escorram acidentalmente pelo cabo e entrem no hub de E/S.
- Conecte uma braçadeira de alívio de tensão para proteger os fios contra danos ou estresse, conforme mostrado na imagem a seguir.



1. Insira somente os fios necessários para sua aplicação através dos plugues do bloco de terminais. Consulte a tabela de fiação e os diagramas a seguir.

2. Insira os plugues do bloco de terminais no hub de E/S.

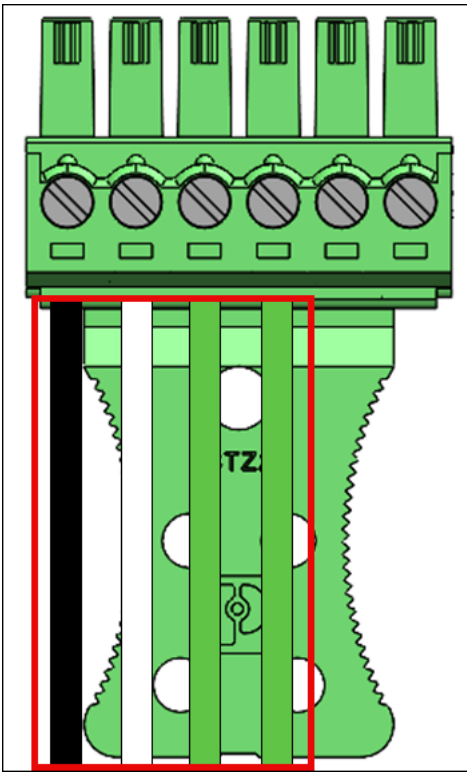


Pin	Conexão	Descrição	Use
1	RTN	Retorno do sinal	Wiegand ground — Fio preto
2	D1	Wiegand D1	Wiegand Data 1 — Fio branco
3	D0	Wiegand D0	Dados Wiegand 0 — Fio verde
4	LED	Wiegand LED	Wiegand — Opcional LED

Pin	Conexão	Descrição	Use
5	GPI	Entrada de uso geral	Sinal de entrada digital — Opcional
6	GPO	Saída de uso geral	Sinal de saída digital - opcional
7	B	RS485_B/D0/ Dados	OSDPD0 — Fio verde
8	A	RS485_A/D1/ Relógio	OSDPD1 — Fio branco
9	RTN	Retorno do sinal	OSDPretorno — Fio preto
10	COM	Relé comum	Relé de contato comum — Fio branco
11	NC	Relé normalmente fechado	Relé de contato normalmente fechado — fio laranja
12	NO	Relé normalmente aberto	Relé de contato normalmente aberto — fio amarelo

Conexões Wiegand

- Insira o fio preto no pino 1 (RTN).
- Insira o fio branco no pino 2 (D1).
- Insira o fio verde no pino 3 (D0).
- Opcional: insira o fio verde no pino 4 (LED).



Conexões de relé

- Insira o fio branco no pino 10 (COM).
- Insira o fio laranja no pino 11 (NC).
- Insira o fio amarelo no pino 12 (NO).

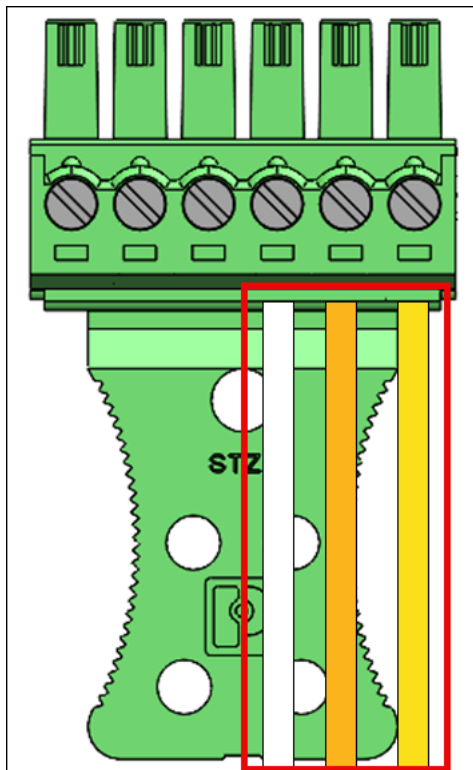
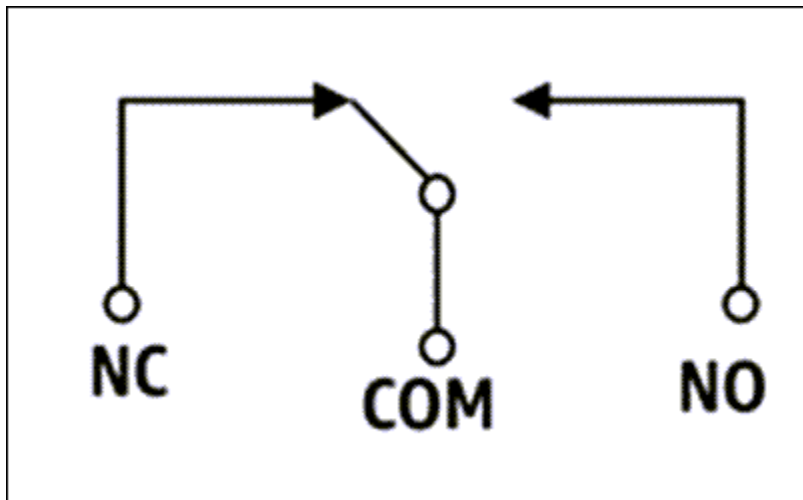


Diagrama de relé

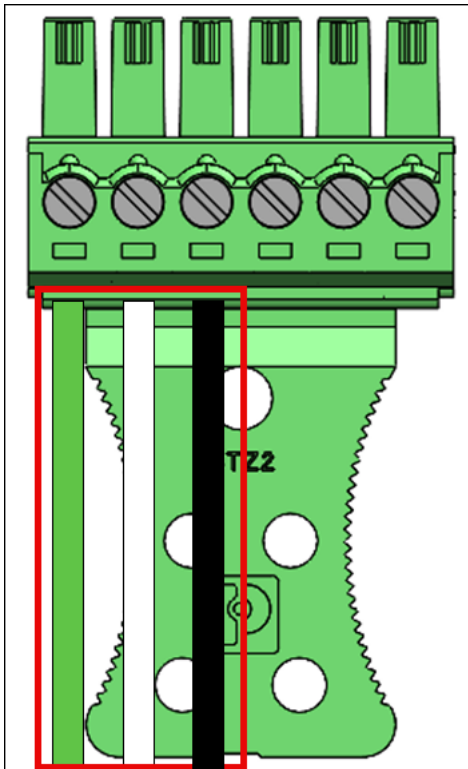


O relé deve ser operado de acordo com as classificações de segurança especificadas VAC 30/60VDC, 60W máx.

RS485conexões

- Insira o fio verde no pino 7 (B).
- Insira o fio branco no pino 8 (A).

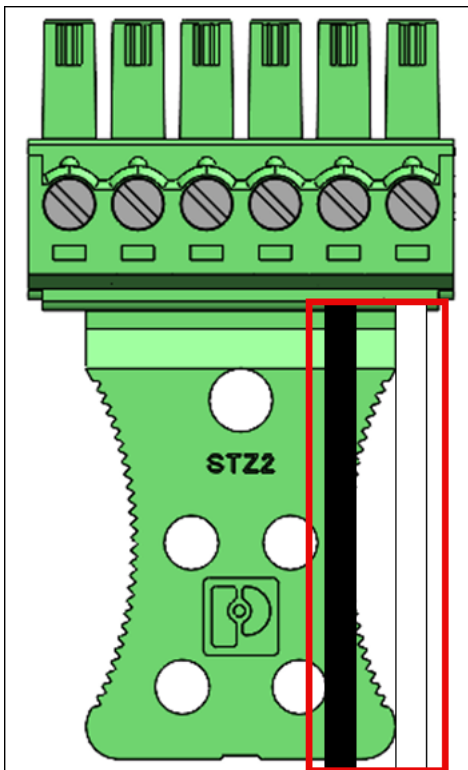
- Insira o fio preto no pino 9 (RTN).



Ligue o interruptor de RS485 terminação se o dispositivo for a última unidade na linha. Essa chave ativa a terminação do resistor de 120 Ohms na linha.

Conexões de entrada/saída digitais

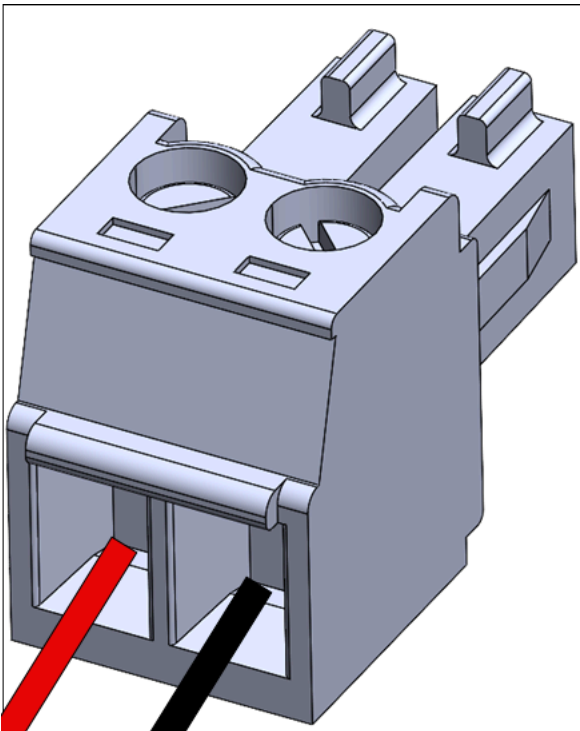
- Insira o fio preto no pino 5 (GPI).
- Insira o fio branco no pino 6 (GPO).



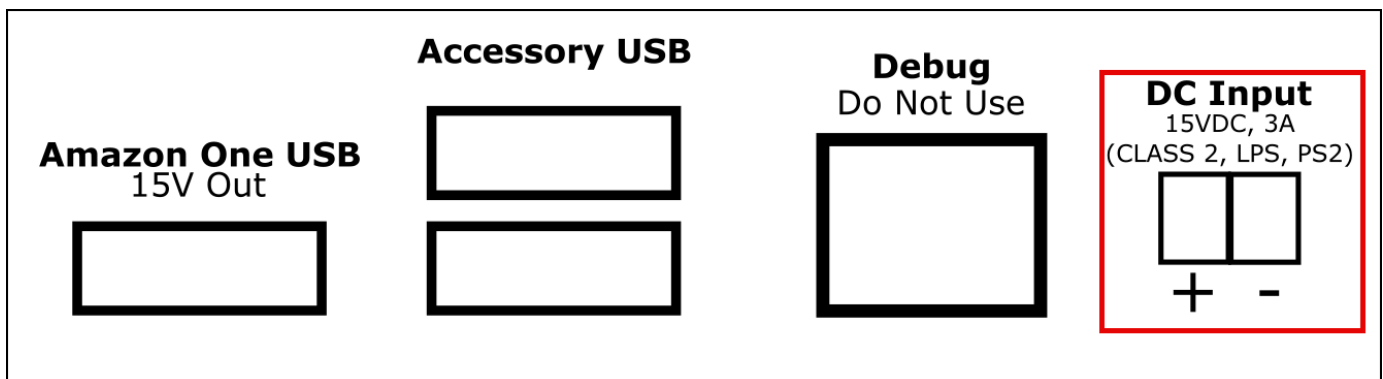
- As conexões de entrada/saída digital devem ser operadas conforme listado.

Opcional: Para instalar a fiação DC

1. Retire 3 mm-5 mm da extremidade de um fio vermelho para positivo (+) e um fio preto para negativo (-).
2. Insira a extremidade descascada do fio DC no plugue DC.



3. Enrosque o fio na posição.
4. Insira o plugue DC com fio na porta de entrada DC.



Ativando o dispositivo Amazon One

Quando seu dispositivo Amazon One estiver instalado e ligado, você estará pronto para ativá-lo.

Para ativar seu dispositivo Amazon One


1. No dispositivo Amazon One, toque na tela para começar.
2. Escolha Ethernet ou Wifi para se conectar à Internet.

Assim que o dispositivo estiver conectado à Internet, ele começará a baixar o pacote de software mais recente.

3. Quando a tela mostra o download do software concluído! , selecione OK.
4. Selecione o código QR.

A tela do dispositivo Amazon One mostrará o código QR Scan.

5. [Para recuperar o código QR de ativação, abra o console do Amazon One Enterprise em https://console.aws.amazon.com/one-enterprise.](https://console.aws.amazon.com/one-enterprise)

 Note

É altamente recomendável que você conceda permissão limitada aos seus instaladores para que eles tenham acesso somente aos códigos QR de ativação no console do Amazon One Enterprise. Consulte [Adicionar usuários do Amazon One Enterprise](#).

6. No painel de navegação, escolha Códigos QR de ativação.
7. Na lista suspensa Selecionar um site, selecione o site em que o dispositivo Amazon One está instalado.
8. Em Informações do site, confirme o endereço do site.
9. Em Códigos QR de ativação, procure o nome da instância do dispositivo que você está ativando e selecione o código QR correspondente para recuperar o código QR.
10. Escaneie o código QR com o dispositivo Amazon One. Observe que o código QR é atualizado periodicamente por motivos de segurança. Você só pode usar um código QR uma vez.
11. Insira o CEP do site e selecione Confirmar configurações depois de verificar se o site correto é exibido.
12. Quando a tela do dispositivo Amazon One mostra Ativação concluída! , o dispositivo está pronto para uso.

Inscrivendo e inserindo usuários

Agora que seu dispositivo Amazon One está ativado, seus funcionários podem começar a inscrever suas palmas e autenticá-las para obter acesso.

Tópicos

- [Criação de uma política de endpoint](#)
- [Autenticação para entrada](#)

Criação de uma política de endpoint

Antes que os usuários possam autenticar suas palmas para entrar, eles terão que passar pelo processo de inscrição. O pessoal de segurança deve sempre verificar a identidade do usuário antes de permitir que ele se inscreva.

Para inscrever suas palmas em um dispositivo Amazon One

1. No dispositivo de inscrição Amazon One Enterprise, pressione Começar.
2. Digitalize o crachá de um funcionário com o scanner de crachás conectado ao seu dispositivo de inscrição Amazon One Enterprise.

Quando o crachá é digitalizado com sucesso, a tela do dispositivo Amazon One mostra o crachá digitalizado.

3. Leia os Termos de Uso e pressione OK.
4. Leia Consent - Your Palm Biometric Information e pressione Concordo se você consentir.
5. Siga as instruções na tela para concluir o processo de inscrição.

Autenticação para entrada

Depois de inscrever com sucesso seus palms, você estará pronto para se autenticar com o palmeiro em seu dispositivo de entrada Amazon One Enterprise.

Para autenticar sua palma para entrada em um dispositivo Amazon One

- Passe o mouse sobre o dispositivo e siga as instruções na tela para escanear a palma da mão.

Gerenciamento de usuários

Você pode usar a página de gerenciamento de usuários inscritos para acompanhar os usuários inscritos e excluir a biometria do usuário. Um usuário cuja biometria associada foi excluída não terá mais acesso aos dispositivos Amazon One para autenticação.

Tópicos

- [Visualizando usuários inscritos](#)
- [Excluindo usuários inscritos e seus dados biométricos](#)

Visualizando usuários inscritos

O procedimento a seguir detalha como inscrever usuários.

Para ver os usuários inscritos

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Gerenciamento de usuários registrados.
3. Em Usuários inscritos, você encontrará todos os usuários inscritos e os seguintes detalhes:
 - ID do crachá — Informações do identificador do crachá capturadas por um leitor de RFID crachá no momento da inscrição.
 - Fonte de inscrição — Detalhes do dispositivo Amazon One que foi usado para inscrição.
 - Data de inscrição — Data e hora da inscrição.

Excluindo usuários inscritos e seus dados biométricos

O procedimento a seguir detalha como excluir usuários inscritos e seus dados biométricos.

Para excluir usuários inscritos e seus dados biométricos

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Gerenciamento de usuários registrados.
3. Em Usuários inscritos, selecione a ID do crachá do usuário cujos dados biométricos da palma da mão você deseja excluir.

4. Escolha Excluir biometria.
5. Escolha Excluir para confirmar a exclusão dos dados biométricos do usuário.

 Important

Essa ação resulta na exclusão permanente da biometria da palma da mão de um usuário do Amazon One Enterprise. O usuário precisará se inscrever novamente com um dispositivo de inscrição do Amazon One Enterprise para poder usar o Amazon One Enterprise para autenticação. A exclusão biométrica de um usuário também excluirá permanentemente outros atributos do perfil, como ID de crachá do Amazon One Enterprise.

Gerenciando dispositivos Amazon One

Depois que seu dispositivo Amazon One é instalado e ativado, ele começa a relatar a integridade do dispositivo no console Amazon One Enterprise. Você pode usar o console do Amazon One Enterprise para realizar tarefas de gerenciamento de dispositivos, como reinicializar dispositivos ou atualizar configurações.

Tópicos

- [Manutenção e limpeza de dispositivos Amazon One](#)
- [Gerenciamento do site](#)
- [Gerenciamento de instâncias de dispositivos](#)

Manutenção e limpeza de dispositivos Amazon One

A manutenção do seu dispositivo Amazon One fornece o ambiente operacional e a experiência ideais do dispositivo.

Antes de limpar o dispositivo Amazon One, verifique o seguinte:

- Embora você não precise ativar ou desativar o Amazon One, certifique-se de que os dispositivos estejam conectados à energia, tenham conectividade de rede e que todos os dispositivos periféricos e complementares (se aplicável) estejam conectados.
- Escale os problemas para seu administrador se a conectividade de rede não estiver disponível (uma tela de erro ficará visível no dispositivo Amazon One se isso ocorrer), uma tela de erro estará visível no dispositivo Amazon One ou um problema de conexão do dispositivo estará visível no console.
- Proteja fisicamente os dispositivos para que pessoas não autorizadas não possam manipulá-los.
- Inspeção visualmente os dispositivos Amazon One diariamente, verificando se há conexões não autorizadas com o dispositivo Amazon One.
- Inspeção todos os lados do dispositivo em busca de sinais de adulteração, incluindo parafusos visíveis do dispositivo e da caixa, para garantir que não haja lacunas/aberturas expondo os componentes/circuitos internos do dispositivo Amazon One.
- Em caso de erros ou falhas, siga as instruções na tela do dispositivo Amazon One ou consulte o guia de solução de problemas para corrigir problemas.

Para limpar o dispositivo Amazon One

Limpar seu dispositivo Amazon One remove regularmente quaisquer manchas ou marcas, como impressões digitais e impressões de mãos.

Note

Não use nenhum outro produto de limpeza além dos listados neste guia. O cronograma de limpeza recomendado é uma ou duas vezes por semana, ou sempre que sujeira, poeira ou manchas estiverem visíveis no dispositivo, mas nunca mais do que uma vez por dia.

1. Limpe o dispositivo Amazon One com toalhetes de álcool isopropílico (IPA). Limpe apenas a superfície de toque do dispositivo. Não toque na janela óptica nem use qualquer outro produto de limpeza, a menos que seja instruído pela Amazon One.
2. Limpe as manchas com um pano seco de microfibra.
3. Limpe levemente (não limpe) qualquer sujeira ou detritos visíveis da janela óptica. Limite a limpeza da janela óptica a não mais do que uma vez por dia and/or when the window is visually dirty (e.g., finger/hand prints/smudges). Essa parte do dispositivo não deve ser tocada, mas pode haver toques inadvertidos de novos clientes.
4. Use um limpador de cartão KIC inteligente para limpar o interior de um leitor de cartão, se aplicável.
5. Limpe o dispositivo uma ou duas vezes por semana ou sempre que houver sujeira, poeira ou manchas visíveis no dispositivo.

Gerenciamento do site

Um site representa um local físico em que uma coleção de instâncias de dispositivos está instalada e operando. Você pode usar sites para organizar dispositivos Amazon One que compartilham o mesmo endereço físico.

Tópicos

- [Alterando o nome do site](#)
- [Atualizando o endereço do site](#)

Alterando o nome do site

O procedimento a seguir detalha como alterar o nome do site do seu dispositivo.

Para alterar o nome do site

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Site.
3. Em Sites, selecione o site para o qual você pretende editar o nome.
4. Selecione a opção Editar.
5. Em Informações do site, insira o nome e a descrição do site desejados (opcional).
6. Escolha Salvar alterações para atualizar.

Atualizando o endereço do site

O procedimento a seguir detalha como atualizar o endereço do site do seu dispositivo.

Para atualizar o endereço do site

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Site.
3. Em Sites, selecione o site para o qual você pretende atualizar o endereço.
4. Em Instâncias do dispositivo, verifique se o número de instâncias ativadas é 0.
5. (Opcional) Se o número de instâncias ativadas não for 0, consulte
6. Selecione a opção Editar.
7. Em Endereço físico, insira o endereço físico correto.
8. Escolha Salvar alterações para atualizar.

Gerenciamento de instâncias de dispositivos

Uma instância de dispositivo é uma representação lógica de um dispositivo com configurações. O uso de instâncias de dispositivos permite a troca de dispositivos Amazon One e, ao mesmo tempo, herda automaticamente as configurações e os nomes definidos anteriormente. Uma instância de dispositivo tem um nome definido pelo usuário (convenção de nomenclatura compartilhada com seu software de controle de acesso) e um conjunto de configurações de comunicação.

Tópicos

- [Visualizando o status da instância do dispositivo](#)
- [Reiniciando um dispositivo Amazon One](#)
- [Atualizando as configurações do dispositivo Amazon One](#)
- [Atualizando credenciais de Wi-Fi](#)
- [Desativando instâncias do dispositivo](#)

Visualizando o status da instância do dispositivo

O procedimento a seguir detalha como visualizar o status da instância do seu dispositivo.

Para ver o status da instância do dispositivo

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Instância do dispositivo.
3. Em Instâncias ativadas, você verá uma lista de dispositivos Amazon One ativados.
4. Escolha o nome da instância do dispositivo para ver os detalhes da instância do dispositivo.

Reiniciando um dispositivo Amazon One

O procedimento a seguir detalha como reiniciar seu dispositivo Amazon One.

Para reiniciar um dispositivo Amazon One

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Instância do dispositivo.
3. Em Instâncias ativadas, escolha o nome da instância do dispositivo que você deseja reiniciar.
4. Escolha Reiniciar para reiniciar o dispositivo Amazon One.


Atualizando as configurações do dispositivo Amazon One

O procedimento a seguir detalha como atualizar as configurações do dispositivo Amazon One.

Para atualizar as configurações do dispositivo Amazon One

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.

2. No painel de navegação, escolha Instância do dispositivo.
3. Em Instâncias ativadas, escolha o nome da instância do dispositivo que você deseja atualizar.
4. Em Configurações do dispositivo, escolha Editar.

 Note

Para alterar o modo de dispositivo Amazon One, você deve primeiro desativar a instância do dispositivo e depois configurá-la com o modo de dispositivo desejado (consulte [Configurar uma instância de dispositivo para ativação](#)). Em seguida, você pode passar pelo processo de ativação do dispositivo (consulte [Ativando o dispositivo Amazon One](#)).

5. Depois de fazer as alterações desejadas, escolha Atualizar configurações do dispositivo para confirmar a atualização.

Atualizando credenciais de Wi-Fi

O procedimento a seguir detalha como atualizar as credenciais de Wi-Fi.

Para atualizar as credenciais do Wifi

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Instância do dispositivo.
3. Em Instâncias ativadas, escolha o nome da instância do dispositivo que você deseja atualizar.
4. Em Rede, escolha Editar.
5. Em Configurações de Wi-Fi, faça as alterações desejadas.
6. Escolha Atualizar rede para confirmar a atualização.

Desativando instâncias do dispositivo

O procedimento a seguir detalha como desativar as instâncias do dispositivo.

Para desativar instâncias do dispositivo

1. Abra o console do Amazon One Enterprise em <https://console.aws.amazon.com/one-enterprise>.
2. No painel de navegação, escolha Instância do dispositivo.

3. Em Instâncias ativadas, selecione o nome da instância do dispositivo que você deseja desativar.
4. Escolha Desativar dispositivo.
5. Para confirmar a desativação, digite 'desativar' na caixa de mensagem e escolha Desativar dispositivo.

Segurança

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 Amazon One Enterprise, 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.

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

Tópicos

- [Proteção de dados no Amazon One Enterprise](#)
- [Gerenciamento de identidade e acesso para Amazon One Enterprise](#)
- [Ações, recursos e chaves de condição do Amazon One Enterprise](#)
- [Validação de conformidade para Amazon One Enterprise](#)

Proteção de dados no Amazon One Enterprise

O [modelo de responsabilidade AWS compartilhada](#) de se aplica à proteção de dados no Amazon One Enterprise. 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 obter mais informações sobre privacidade de dados, consulte [Privacidade de dados FAQ](#). Para obter informações sobre proteção de dados na Europa, consulte o [Modelo de Responsabilidade AWS Compartilhada e GDPR](#) a postagem no blog AWS de segurança.

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 a autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- 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 FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou uma API, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

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 Amazon One Enterprise ou outro Serviços da AWS usando o console, API, AWS CLI, ou AWS SDKs. 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, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Para usar a criptografia padrão de dados em repouso

O Amazon One Enterprise fornece criptografia por padrão para proteger dados confidenciais em repouso usando chaves de AWS criptografia.

AWSchaves próprias — A Amazon One Enterprise usa essas chaves por padrão para criptografar automaticamente dados confidenciais do usuário final. Você não pode visualizar, gerenciar ou usar chaves AWS próprias nem auditar seu uso. No entanto, não é necessário tomar nenhuma medida nem alterar qualquer programa para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte chaves AWS próprias no Guia do desenvolvedor do AWS Key Management Service.

Para gerenciar sua própria chave de cliente

Chaves gerenciadas pelo cliente — O Amazon One Enterprise oferece suporte ao uso de uma chave de cliente simétrica que você cria, possui e gerencia. Isso adiciona uma segunda camada de criptografia sobre a AWS criptografia existente. O Amazon One Enterprise oferece suporte à criptografia de dados confidenciais de clientes, como dados de usuários, configurações de dispositivos, senhas de Wi-Fi etc. Esse recurso inclui a opção de adicionar uma camada de segurança autogerenciada para ajudar a atender aos requisitos regulatórios e de conformidade da sua organização. Para obter mais informações sobre como habilitar chaves gerenciadas pelo cliente, consulte Atualizar configurações de criptografia no Amazon One Enterprise.

Como você tem controle total dessa camada de criptografia, é possível realizar tarefas como:

- Estabelecer e manter as políticas de chave
- Estabelecendo e mantendo IAM políticas de KMS permissões
- Material criptográfico de chave rotativa na cadência que você controla
- Adicionar etiquetas

Para obter mais informações, consulte a chave gerenciada pelo cliente no Guia do desenvolvedor do AWS Key Management Service.

Note

Embora o Amazon One Enterprise habilite automaticamente a criptografia em repouso usando chaves AWS próprias para proteger dados confidenciais do cliente sem nenhum

custo, cobranças são AWS KMS cobradas pelo uso de uma chave gerenciada pelo cliente. Para obter mais informações sobre preços, consulte os preços do AWS Key Management Service. Para obter mais informações sobre AWSKMS, consulte [O que é o AWS Key Management Service?](#)

Você pode remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, o Amazon One Enterprise não poderá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados. Por exemplo, se você tentar obter informações criptografadas de dados de configurações de usuários e dispositivos que o Amazon One Enterprise não pode acessar, a operação retornará uma `AccessDeniedException` error.

Criptografia de dados em trânsito

O Amazon One Enterprise usa o Transport Layer Security (TLS) para proteger os dados e o Signature versão 4 para autenticar todas as API solicitações de entrada para AWS os serviços. Essa criptografia é ativada por padrão.

Gerenciamento de identidade e acesso para Amazon One Enterprise

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. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do Amazon One Enterprise. IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como o Amazon One Enterprise trabalha com IAM](#)
- [Exemplos de políticas baseadas em identidade para o Amazon One Enterprise](#)
- [AWS políticas gerenciadas para o Amazon One Enterprise](#)

Público

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

Usuário do serviço — Se você usa o serviço Amazon One Enterprise para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Amazon One Enterprise para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Amazon One Enterprise, consulte [Solução de problemas de identidade e acesso ao Amazon One Enterprise](#).

Administrador de serviços — Se você é responsável pelos recursos do Amazon One Enterprise em sua empresa, provavelmente tem acesso total ao Amazon One Enterprise. É seu trabalho determinar quais recursos e recursos do Amazon One Enterprise seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar IAM o Amazon One Enterprise, consulte [Como o Amazon One Enterprise trabalha com IAM](#).

IAM administrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Amazon One Enterprise. Para ver exemplos de políticas baseadas em identidade do Amazon One Enterprise que você pode usar IAM, consulte [Exemplos de políticas baseadas em identidade para o Amazon One Enterprise](#)

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do 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 entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. 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 você mesmo assinar solicitações, consulte [Assinar AWS API solicitações](#) no Guia IAM do usuário.

Independente 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 e [Uso da autenticação multifator \(MFA\) AWS no Guia do IAMusuário](#).

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 puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do IAM usuário.

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 são acessadas 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 obter informações sobre o IAM Identity Center, consulte [O que é o IAM Identity Center?](#) no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um [IAMusuário](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham 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 IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo](#) no Guia do IAMusuário.

Um [IAMgrupo](#) é uma identidade que especifica uma coleção de IAM usuários. 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 IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

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 IAM usuário \(em vez de uma função\)](#) no Guia do IAM usuário.

IAMfunções

Uma [IAMfunção](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console [trocando de funções](#). Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte [Métodos para assumir uma função](#) no Guia IAM do usuário.

IAMfunções 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 obter

informações sobre funções para federação, consulte [Criação de uma função para um provedor de identidade terceirizado](#) no Guia IAM do usuário. Se você usa o IAM Identity Center, configura 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 uma função em IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Manual do Usuário do AWS IAM Identity Center .

- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente 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 funções e políticas baseadas em recursos para acesso entre contas, consulte [Acesso a recursos entre contas IAM no Guia](#) do IAM usuário.
- 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 aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
- Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. 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. FAS as solicitações 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 FAS solicitações, consulte [Encaminhar sessões de acesso](#).
- Função de serviço — Uma função de serviço é uma [IAM função](#) que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamente IAM. Para obter mais informações, consulte [Criação de uma função para delegar permissões a uma AWS service \(Serviço da AWS\)](#) no Guia do IAM usuário.
- 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 presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS

e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte [Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte [Quando criar uma IAM função \(em vez de um usuário\)](#) no Guia do IAM usuário.

Gerenciando 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 JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte [Visão geral das JSON políticas](#) no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas 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 permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar 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 do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criação de IAM políticas no Guia](#) do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente 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 [Escolha entre políticas gerenciadas e políticas em linha no Guia](#) do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem 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 um principal especificado 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 localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

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

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a [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 recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAM usuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para IAM entidades](#) no Guia IAM do usuário.
- **Políticas de controle de serviço (SCPs)** — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte [Políticas de controle de serviços](#) no Guia AWS Organizations do Usuário.
- **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 atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia IAM do usuário.

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 política estão envolvidos, consulte [Lógica de avaliação](#) de políticas no Guia IAM do usuário.

Como o Amazon One Enterprise trabalha com IAM

Antes de usar IAM para gerenciar o acesso ao Amazon One Enterprise, saiba quais IAM recursos estão disponíveis para uso com o Amazon One Enterprise.

IAMrecursos que você pode usar com o Amazon One Enterprise

IAMrecurso	Suporte do Amazon One Enterprise
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC(tags nas políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para ter uma visão de alto nível de como o Amazon One Enterprise e outros AWS serviços funcionam com a maioria dos IAM recursos, consulte [AWS os serviços que funcionam com IAM](#) no Guia do IAM usuário.

Políticas baseadas em identidade para Amazon One Enterprise

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criação de IAM políticas no Guia](#) do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e 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 perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a [referência IAM JSON de elementos de política](#) no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para o Amazon One Enterprise

Para ver exemplos de políticas baseadas em identidade do Amazon One Enterprise, consulte [Exemplos de políticas baseadas em identidade para o Amazon One Enterprise](#)

Políticas baseadas em recursos no Amazon One Enterprise

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem 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 um principal especificado 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 habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. 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 IAM administrador 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 Acesso a recursos entre contas IAM no Guia do IAM usuário](#).

Ações políticas para o Amazon One Enterprise

Compatível com ações de políticas: Sim

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

O `Action` elemento de uma JSON política 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 AWS API operação associada. Há algumas exceções, como ações somente de permissão que não têm uma operação correspondente. API Algumas operações também 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 Amazon One Enterprise, consulte [Ações, recursos e chaves de condição do Amazon One Enterprise](#).

As ações de política no Amazon One Enterprise usam o seguinte prefixo antes da ação:

```
one
```

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

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

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

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

Para ver exemplos de políticas baseadas em identidade do Amazon One Enterprise, consulte.

[Exemplos de políticas baseadas em identidade para o Amazon One Enterprise](#)

Recursos de políticas para o Amazon One Enterprise

Compatível com recursos de políticas: Sim

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

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

Para ações que não oferecem compatibilidade com 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 ver uma lista dos tipos de recursos do Amazon One Enterprise e seus ARNs, e para saber quais ações você pode usar para especificar cada recurso, consulte [Ações, recursos e chaves de condição do Amazon One Enterprise](#). ARN

Para ver exemplos de políticas baseadas em identidade do Amazon One Enterprise, consulte.

[Exemplos de políticas baseadas em identidade para o Amazon One Enterprise](#)

Chaves de condição de política para o Amazon One Enterprise

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar AWS JSON políticas 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 `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões

condicionais que usem [agentes 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 `Condition` elemento, 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 antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte [elementos de IAM política: variáveis e tags](#) no Guia IAM do usuário.

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 IAM do usuário.

Para ver uma lista das chaves de condição do Amazon One Enterprise e saber com quais ações e recursos você pode usar uma chave de condição, consulte [Ações, recursos e chaves de condição do Amazon One Enterprise](#).

Para ver exemplos de políticas baseadas em identidade do Amazon One Enterprise, consulte [Exemplos de políticas baseadas em identidade para o Amazon One Enterprise](#)

ACLs no Amazon One Enterprise

Suportes ACLs: Não

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

ABAC com o Amazon One Enterprise

Suportes ABAC (tags nas políticas): Sim

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e

recursos é a primeira etapa do ABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

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

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 chaves de condição `aws:TagKeys`.

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 obter mais informações sobre ABAC, consulte [O que é ABAC?](#) no Guia do IAM usuário. Para ver um tutorial com etapas de configuração ABAC, consulte [Usar controle de acesso baseado em atributos \(ABAC\) no Guia](#) do IAM usuário.

Usando credenciais temporárias com o Amazon One Enterprise

Compatível com credenciais temporárias: Sim

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 esse trabalho IAM](#) no Guia do IAM usuário.

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 obter mais informações sobre a troca de funções, consulte [Alternando para uma função \(console\)](#) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. 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 obter mais informações, consulte [Credenciais de segurança temporárias em IAM](#).

Permissões principais entre serviços para o Amazon One Enterprise

Suporta sessões de acesso direto (FAS): Sim

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa 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. FASas solicitações 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 FAS solicitações, consulte [Encaminhar sessões de acesso](#).

Funções de serviço para o Amazon One Enterprise

Compatível com perfis de serviço: não

Uma função de serviço é uma [IAMfunção](#) que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte [Criação de uma função para delegar permissões a uma AWS service \(Serviço da AWS\)](#) no Guia do IAM usuário.

Warning

Alterar as permissões de uma função de serviço pode interromper a funcionalidade do Amazon One Enterprise. Edite funções de serviço somente quando o Amazon One Enterprise fornecer orientação para fazer isso.

Funções vinculadas a serviços para Amazon One Enterprise

Compatível com 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 presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte [AWS serviços que funcionam](#) com. IAM Encontre um serviço na tabela que inclua um Yes na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para o Amazon One Enterprise

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Amazon One Enterprise. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte [Criação de IAM políticas no Guia](#) do IAMusuário.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Amazon One Enterprise, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição do Amazon One Enterprise](#) a Referência de Autorização de Serviço.

Tópicos

- [Melhores práticas de política](#)
- [Usando o console Amazon One Enterprise](#)
- [Permitir que usuários visualizem suas próprias permissões](#)
- [Acesso somente para leitura ao Amazon One Enterprise](#)
- [Acesso total ao Amazon One Enterprise](#)
- [Permissões em nível de recurso suportadas para ações de regras corporativas do Amazon One API](#)
- [Informações adicionais](#)

Melhores práticas de política

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

- Comece com as políticas AWS gerenciadas e avance 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 obter mais informações, consulte [políticas AWS gerenciadas](#) ou [políticas AWS gerenciadas para funções de trabalho](#) no Guia IAM do usuário.

- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte [Políticas e permissões IAM no](#) Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas 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 IAM JSON da política: Condição](#) no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação da política do IAM Access Analyzer](#) no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte [Configurando o API acesso MFA protegido](#) no Guia do IAM usuário.

Para obter mais informações sobre as melhores práticas em IAM, consulte [as melhores práticas de segurança IAM no](#) Guia IAM do usuário.

Usando o console Amazon One Enterprise

Para acessar o console do Amazon One Enterprise, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Amazon One Enterprise em seu Conta da AWS. Se você criar uma política baseada em

identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que eles estão tentando realizar.

Para garantir que usuários e funções ainda possam usar o console do Amazon One Enterprise, anexe também a política *ReadOnly* AWS gerenciada *ConsoleAccess* ou o Amazon One Enterprise às entidades. Para obter mais informações, consulte [Adicionar permissões a um usuário](#) no Guia do IAM usuário.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
}
]
```

Acesso somente para leitura ao Amazon One Enterprise

O exemplo a seguir mostra uma política AWS gerenciada `AmazonOneEnterpriseReadOnlyAccess` que concede acesso somente de leitura ao Amazon One Enterprise.

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

Nas declarações da política, o elemento `Effect` especifica se as ações são permitidas ou negadas. O elemento `Action` lista as ações específicas que o usuário tem permissão para realizar. O elemento `Resource` lista os recursos da AWS nos quais o usuário tem permissão para realizar essas ações. Para políticas que controlam o acesso às ações do Amazon One Enterprise, o `Resource` elemento é sempre definido como `*`, um curinga que significa “todos os recursos”.

Os valores no `Action` elemento correspondem aos APIs que os serviços suportam. As ações são precedidas por `config:` para indicar que se referem às ações do Amazon One Enterprise. Você pode usar o caractere curinga `*` no elemento `Action`, como nos exemplos a seguir:

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

Isso permite que todas as ações do Amazon One Enterprise terminem com DeviceInstance "" (GetDeviceInstanceConfiguration,CreateDeviceInstanceConfiguration).

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

Isso permite todas as ações do Amazon One Enterprise, mas não ações para outros AWS serviços.

- "Action": ["*"]

Isso permite todas as AWS ações. Essa permissão é adequada para um usuário que atua como AWS administrador da sua conta.

A política de somente leitura não concede permissão ao usuário para ações como CreateDeviceInstanceUpdateDeviceInstance, e. DeleteDeviceInstance Os usuários com essa política não têm permissão para criar uma instância de dispositivo, atualizar uma instância de dispositivo ou excluir uma instância de dispositivo. Para obter a lista de ações do Amazon One Enterprise, consulte [Ações, recursos e chaves de condição do Amazon One Enterprise](#).

Acesso total ao Amazon One Enterprise

O exemplo a seguir mostra uma política que concede acesso total ao Amazon One Enterprise. Ele concede aos usuários a permissão para realizar todas as ações do Amazon One Enterprise.

Important

Essa política concede amplas permissões. Antes de conceder acesso total, comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Essa é uma prática mais recomendada do que começar com permissões que são muito permissivas e tentar restringi-las posteriormente.

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

```

    "Resource": "*"
  },
]
}

```

Permissões em nível de recurso suportadas para ações de regras corporativas do Amazon One API

Permissões no nível do recurso se referem à capacidade de especificar em quais recursos os usuários têm permissão para realizar ações. O Amazon One Enterprise oferece suporte a permissões em nível de recursos para determinadas ações de regras do Amazon One Enterprise. API Isso significa que, para determinadas ações de regras do Amazon One Enterprise, você pode controlar as condições sob as quais os usuários podem usar essas ações. Essas condições podem ser ações que precisam ser concluídas ou recursos específicos que os usuários têm permissão para usar.

A tabela a seguir descreve as API ações de regras do Amazon One Enterprise que atualmente oferecem suporte a permissões em nível de recurso. Também descreve os recursos suportados e seus ARNs para cada ação. Ao especificar um ARN, você pode usar o caractere curinga * em seus caminhos; por exemplo, quando você não pode ou não deseja especificar o recurso exato. IDs

Important

Se uma API ação de regra do Amazon One Enterprise não estiver listada nesta tabela, ela não oferece suporte a permissões em nível de recurso. Se uma ação de regra do Amazon One Enterprise não oferecer suporte a permissões em nível de recurso, você poderá conceder aos usuários permissões para usar a ação, mas precisará especificar um * para o elemento de recurso da sua declaração de política.

API Ação	Recursos
CreateDeviceInstance	Instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i>
GetDeviceInstance	Instância do dispositivo

APIAção	Recursos
	arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i>
UpdateDeviceInstance	Instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i>
DeleteDeviceInstance	Instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i>
CreateDeviceActivationQrCode	Instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i>
DeleteAssociatedDevice	Instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i>
RebootDevice	Instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i>
CreateDeviceInstanceConfiguration	Configuração da instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i> /configuração/ <i>version</i>
GetDeviceInstanceConfiguration	Configuração da instância do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :instância do dispositivo/ <i>deviceInstanceId</i> /configuração/ <i>version</i>

APIAção	Recursos
CreateSite	Site arn:aws:one: <i>region</i> : <i>accountID</i> :site/ <i>siteId</i>
DeleteSite	Site arn:aws:one: <i>region</i> : <i>accountID</i> :site/ <i>siteId</i>
GetSiteAddress	Site arn:aws:one: <i>region</i> : <i>accountID</i> :site/ <i>siteId</i>
UpdateSite	Site arn:aws:one: <i>region</i> : <i>accountID</i> :site/ <i>siteId</i>
UpdateSiteAddress	Site arn:aws:one: <i>region</i> : <i>accountID</i> :site/ <i>siteId</i>
CreateDeviceConfigurationTemplate	Modelo de configuração do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :device-configuration-template/ <i>templateId</i>
DeleteDeviceConfigurationTemplate	Modelo de configuração do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :device-configuration-template/ <i>templateId</i>
GetDeviceConfigurationTemplate	Modelo de configuração do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :device-configuration-template/ <i>templateId</i>
UpdateDeviceConfigurationTemplate	Modelo de configuração do dispositivo arn:aws:one: <i>region</i> : <i>accountID</i> :device-configuration-template/ <i>templateId</i>

Por exemplo, você deseja permitir acesso de leitura e negar acesso de gravação para regras específicas a determinados usuários.

Na primeira política, você permite que a AWS Config regra leia ações, como `GetSite` nas regras especificadas.

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

Na segunda política, você nega que a regra do Amazon One Enterprise escreva ações na regra específica.

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

Com permissões em nível de recurso, você pode permitir acesso de leitura e negar acesso de gravação para realizar ações específicas nas ações de regras do Amazon One Enterprise. API

Informações adicionais

Para saber mais sobre a criação de IAM usuários, grupos, políticas e permissões, consulte [Como criar seu primeiro IAM usuário e gerenciamento de grupos e acessos de administradores](#) no Guia do IAM usuário.

AWS políticas gerenciadas para o Amazon One Enterprise

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo [políticas gerenciadas pelo cliente da](#) específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas API operações são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte [as políticas AWS gerenciadas](#) no Guia IAM do usuário.

AmazonOneEnterpriseFullAccess

Essa política concede permissões administrativas que permitem o acesso a todos os recursos e operações do Amazon One Enterprise.

`one:*` Permite que você execute todas as ações do Amazon One Enterprise.

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

AmazonOneEnterpriseReadOnlyAccess

Essa política concede permissões somente de leitura para todos os recursos e operações do Amazon One Enterprise.

`one:Get*` Obtém os recursos do Amazon One Enterprise.

`one:List*` Lista os recursos do Amazon One Enterprise.

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

```
}
```

AmazonOneEnterpriseInstallerAccess

Essa política concede permissões limitadas de leitura e gravação que permitem que você crie um código QR de ativação para qualquer instância de dispositivo configurada para ativar o dispositivo em qualquer local.

`one:CreateDeviceActivationQrCode` Permite criar um código QR para ativar o dispositivo.

`one:GetDeviceInstance` Permite que você busque as informações sobre uma instância do dispositivo Amazon One.

`one:GetSite` Permite que você busque as informações sobre um site do Amazon One Enterprise.

`one:GetSiteAddress` Permite que você busque o endereço físico de um site do Amazon One Enterprise.

`one:ListDeviceInstances` Permite que você liste as instâncias do dispositivo Amazon One.

`one:ListSites` Permite que você liste os sites do Amazon One Enterprise.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InstallerAccessStatementID",
      "Effect": "Allow",
      "Action": [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon One Enterprise atualiza políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Amazon One Enterprise que foram feitas desde que esse serviço começou a monitorar essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o RSS feed na página de histórico de documentos corporativos do Amazon One.

Alteração	Descrição	Data
A Amazon One Enterpris e começou a monitorar as mudanças	A Amazon One Enterpris e começou a monitorar as mudanças em suas políticas AWS gerenciadas.	1.º de dezembro de 2023

Ações, recursos e chaves de condição do Amazon One Enterprise

O Amazon One Enterprise (prefixo do serviço:one) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em IAM políticas de permissão.

Tópicos

- [Ações definidas pelo Amazon One Enterprise](#)
- [Tipos de recursos definidos pelo Amazon One Enterprise](#)
- [Chaves de condição do Amazon One Enterprise](#)

Ações definidas pelo Amazon One Enterprise

Você pode especificar as seguintes ações no `Action` elemento de uma declaração de IAM política. Use políticas para conceder permissões para executar uma operação na AWS. Quando você usa uma ação em uma política, geralmente permite ou nega acesso à API operação ou ao CLI comando com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma declaração com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o Resource elemento em uma IAM política, deverá incluir um padrão ARN ou para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento Condition da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

Note

As chaves de condição do recurso estão listadas na tabela [Tipos de recursos](#). Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte [Tabela de ações](#).

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeviceInstance	Conceder permissão para criar uma instância do dispositivo	Escrever		aws:RequestTag/\${TagKey} aws:TagKeys	
GetDeviceInstance	Conceda permissão para obter informações sobre a instância do dispositivo	Leitura	instância do dispositivo*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDeviceInstances	Conceda permissão para listar instâncias do dispositivo	Leitura			
UpdateDeviceInstance	Conceder permissão para atualizar a instância do dispositivo	Escrever	instância do dispositivo*		
DeleteDeviceInstance	Conceder permissão para excluir a instância do dispositivo	Escrever	instância do dispositivo*		
CreateDeviceActivationQRCode	Conceder permissão para criar um código QR para ativar um dispositivo em uma instância do dispositivo	Escrever	instância do dispositivo*		
DeleteAssociatedDevice	Conceder permissão para excluir a associação entre dispositivo e instância de dispositivo	Escrever	instância do dispositivo*		
RebootDevice	Conceder permissão para reinicializar o dispositivo	Escrever	instância do dispositivo*		
CreateDeviceInstanceConfiguration	Conceder permissão para criar a configuração da instância do dispositivo	Escrever			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDeviceInstanceConfiguration	Conceda permissão para obter informações sobre a configuração da instância do dispositivo	Leitura	configuração*		
CreateSite	Conceder permissão para criar um site	Escrever		aws:RequestTag/\${TagKey} aws:TagKeys	
DeleteSite	Conceder permissão para excluir a instância do dispositivo	Escrever	sites*		
GetSite	Conceder permissão para obter informações sobre o site	Leitura	sites*		
ListSites	Conceder permissão para listar sites	Leitura			
GetSiteAddress	Conceda permissão para obter informações sobre o endereço do site	Leitura	sites*		
UpdateSite	Conceder permissão para atualizar o site	Escrever	sites*		
UpdateSiteAddress	Conceder permissão para atualizar o endereço do site	Escrever	sites*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeviceConfigurationTemplate	Conceder permissão para criar uma instância do dispositivo	Escrever		aws:RequestTag/\${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	Conceder permissão para excluir o modelo de configuração do dispositivo	Escrever	device-configuration-template*		
GetDeviceConfigurationTemplate	Conceder permissão para obter informações sobre o modelo de configuração do dispositivo	Leitura	device-configuration-template*		
ListDeviceConfigurationTemplates	Conceder permissão para listar modelos de configuração de dispositivos	Leitura			
UpdateDeviceConfigurationTemplate	Conceder permissão para atualizar o modelo de configuração do dispositivo	Escrever	device-configuration-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso	Tags	instância do dispositivo, site, device-configuration-template	aws:RequestTag/\${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	instância do dispositivo, site, device-configuration-template	aws:TagKeys	
ListTagForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			

Tipos de recursos definidos pelo Amazon One Enterprise

Os tipos de recursos a seguir são definidos por esse serviço e podem ser usados no Resource elemento das declarações de política de IAM permissão. Cada ação na [Tabela de ações](#) identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte [Tabela de tipos de recursos](#).

Tipos de recursos	ARN	Chaves de condição
Device Instance	arn:aws:one: <i>region:accountID</i> :device-instance/ <i>deviceInstanceId</i>	aws:ResourceTag/\${TagKey}
Device Instance Configuration	arn:aws:one: <i>region:accountID</i> :device-instance/ <i>deviceInstanceId</i> /configuration/ <i>version</i>	
Site	arn:aws:one: <i>region:accountID</i> :site/ <i>siteId</i>	aws:ResourceTag/\${TagKey}
Device Configuration Template	arn:aws:one: <i>region:accountID</i> :device-configuration-template/ <i>templateId</i>	aws:ResourceTag/\${TagKey}

Chaves de condição do Amazon One Enterprise

O Amazon One Enterprise define as seguintes chaves de condição que podem ser usadas no Condition elemento de uma IAM política. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte [Tabela de chaves de condição](#).

Para visualizar as chaves de condição globais disponíveis para todos os serviços, consulte [Chaves de condição globais disponíveis](#).

Chaves de condição	Descrição	Tipo
aws:RequestTag/\${TagKey}	Filtra o acesso baseado em etiquetas a partir da solicitação	String
aws:ResourceTag/\${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso baseado nas chaves da etiqueta a partir da solicitação	ArrayOfString

Validação de conformidade para Amazon One Enterprise

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#) [Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. 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 Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para HIPAA segurança e conformidade na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

Note

Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a [Referência de serviços HIPAA elegíveis](#).

- 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.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o

Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO).

- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#)— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Monitorando o Amazon One Enterprise

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

- A Amazon EventBridge pode ser usada para automatizar seus AWS serviços e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o [Guia EventBridge do usuário da Amazon](#).
- AWS CloudTrail captura API chamadas 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 obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Monitorando eventos do Amazon One Enterprise na Amazon EventBridge

Você pode monitorar eventos do Amazon One Enterprise em EventBridge, que fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos software-as-a-service (SaaS) e AWS serviços. EventBridge encaminha esses dados para destinos como o AWS Lambda Amazon Simple Notification Service. Esses eventos fornecem um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos.

Inscreva-se nos eventos do Amazon One Enterprise

Os eventos de alteração de status do dispositivo e do perfil do usuário do Amazon One são publicados usando EventBridge e podem ser habilitados no EventBridge console criando uma nova regra. Embora os eventos não sejam ordenados, eles têm um registro de data e hora que permite consumir os dados. Os eventos são emitidos com base no [melhor esforço](#).

Para se inscrever nos eventos do Amazon One Enterprise

1. Abra o EventBridge console em <https://console.aws.amazon.com/events/>.
2. No painel de navegação, em Ônibus, escolha Regras.
3. Escolha Criar Regra.
4. Na página de detalhes da regra padrão, atribua um nome à regra, escolha Regra com um padrão de evento e escolha Avançar.
5. Na página Criar padrão de evento, em Origem do evento, verifique se AWS eventos ou eventos de EventBridge parceiros estão selecionados.
6. Em Tipo de evento de amostra, escolha Inserir meu próprio.
7. Copie e cole de um dos [Eventos de exemplo](#).
8. Em Método de criação, escolha Padrão personalizado. Na seção Padrão do evento, adicione um JSON com a fonte do evento como `aws:one` e o tipo de detalhe necessário e, em seguida, escolha Avançar.
9. Na página Selecionar destino (s), selecione um destino de sua escolha, que inclua uma função, SQS fila ou tópico do Lambda. SNS Para obter informações sobre a configuração de alvos, consulte [EventBridge Destinos da Amazon](#).
10. Opcionalmente, você pode configurar tags.
11. Na página Revisar e criar, escolha Criar regra. Para obter mais informações sobre a configuração de regras, consulte [EventBridge as regras](#) no Guia do EventBridge usuário.

Tipos de eventos de alteração de status do dispositivo

Os eventos de alteração do status do dispositivo são gerados em JSON. Para cada tipo de evento, um JSON blob é enviado para o destino de sua escolha, conforme configurado na regra. Os seguintes tipos de detalhes estão disponíveis:

O status de saúde do dispositivo foi alterado para saudável

O dispositivo passou em todas as verificações de saúde.

O status de saúde do dispositivo foi alterado para crítico

O dispositivo falhou em uma ou mais verificações de saúde.

Conectividade do dispositivo alterada para offline

O dispositivo não está conectado à Internet.

Conectividade do dispositivo alterada para online

O dispositivo está conectado à internet.

recursos

Contém a lista de deviceInstance arn para os quais o evento Device Status Change foi publicado.

metadata

siteName

- Nome do site onde o deviceInstance está presente.

siteArn

- Arn para o site em que deviceInstance está presente.

data

currentConnectivity

- Representa se o deviceInstance está conectado ou desconectado da Internet.
- Valores possíveis:CONNECTED, DISCONNECTED

previousConnectivity

- Representa se deviceInstance ele estava conectado ou desconectado da Internet antes do evento.
- Valores possíveis:CONNECTED, DISCONNECTED

currentHealthStatus

- Representa se ele deviceInstance foi aprovado em todas as verificações de saúde.
- Valores possíveis:HEALTHY, CRITICAL

previousHealthStatus

- Representa se ele deviceInstance passou em todas as verificações de saúde quando foi verificado pela última vez.
- Valores possíveis:HEALTHY, CRITICAL

assetTagId

- O assetTagId do dispositivo associado adeviceInstance.

deviceInstanceName

- O nome do evento `deviceInstance` para o qual o evento de status do dispositivo foi publicado.

Tipos de eventos de perfil de usuário

Os tipos de detalhes do evento relacionados ao perfil do usuário são:

Nova inscrição bem-sucedida

Quando um usuário se inscreveu com sucesso.

Novo cancelamento de inscrição bem-sucedido

Quando um usuário cancelou a inscrição com sucesso.

Inscrição malsucedida

Quando um usuário não conseguiu se inscrever.

Cancelamento de inscrição malsucedido

Quando um usuário não conseguiu cancelar a inscrição.

Reconhecimento bem-sucedido

Quando um usuário digitaliza a palma da mão para autenticação com sucesso.

Reconhecimento malsucedido

Quando o reconhecimento de uma palma falhou.

recursos

Contém a lista de `arn` de perfil de usuário para os quais o evento de perfil de usuário foi publicado.

data

`accountId`

- A AWS conta relevante para o dispositivo que iniciou a solicitação.

`requestSource`

- Essa é a `deviceInstanceId` do dispositivo que iniciou a solicitação.

`createdTimestamp`

- A hora em que o evento está sendo criado.

userStatus

- O status atual do usuário.
- Valores possíveis: ACTIVE, DELETED

associatedId

- O ID associado do usuário, por exemplo, o ID do crachá.

razão

- Esse valor será apresentado para eventos malsucedidos. Ele contém o motivo pelo qual o evento não teve sucesso.

Eventos de exemplo

Os exemplos a seguir mostram eventos do Amazon One Enterprise.

Tópicos

- [O status de integridade do dispositivo foi alterado para íntegro](#)
- [O status de integridade do dispositivo foi alterado para crítico](#)
- [A conectividade do dispositivo foi alterada para online](#)
- [A conectividade do dispositivo foi alterada para off-line](#)
- [Nova inscrição bem-sucedida](#)

O status de integridade do dispositivo foi alterado para íntegro

O dispositivo passou por toda a integridade e o status de integridade da instância do dispositivo foi alterado para HEALTHY do status de CRITICAL integridade.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Health Status Changed To Healthy",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
```

```
"version": "1.0.0",
"metadata": {
  "siteName": "Site name",
  "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
},
"data": {
  "currentHealthStatus": "HEALTHY",
  "previousHealthStatus": "CRITICAL",
  "assetTagId": "0000195169",
  "deviceInstanceName": "Device name"
}
}
```

O status de integridade do dispositivo foi alterado para crítico

O dispositivo falhou em uma ou mais verificações de saúde e o status de integridade da instância do dispositivo mudou para CRITICAL de HEALTHY.

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

A conectividade do dispositivo foi alterada para online

O dispositivo está conectado à Internet e o status de conectividade da instância do dispositivo é alterado para CONNECTED de DISCONNECTED.

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

A conectividade do dispositivo foi alterada para off-line

O dispositivo não está conectado à Internet e o status de conectividade da instância do dispositivo foi alterado para DISCONNECTED de CONNECTED.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Offline",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
```

```

"resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
"detail": {
  "version": "1.0.0",
  "metadata": {
    "siteName": "Site name",
    "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
  },
  "data": {
    "currentConnectivity": "DISCONNECTED",
    "previousConnectivity": "CONNECTED",
    "assetTagId": "0000195169",
    "deviceInstanceName": "Device name"
  }
}
}

```

Nova inscrição bem-sucedida

Um evento em que um usuário se inscreveu com sucesso.

```

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

```

Registrando API chamadas do Amazon One Enterprise usando AWS CloudTrail

O Amazon One Enterprise é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Amazon One Enterprise. CloudTrail captura todas as API chamadas para o Amazon One Enterprise como eventos. As chamadas capturadas incluem chamadas do console do Amazon One Enterprise e chamadas de código para as API operações do Amazon One Enterprise. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon One Enterprise. 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 à Amazon One Enterprise, o endereço IP a partir 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 o Amazon One Enterprise em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Amazon One Enterprise, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para obter um registro contínuo dos eventos em sua empresa Conta da AWS, incluindo eventos do Amazon One Enterprise, 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 AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. 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 as informações a seguir.

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

Todas as ações do Amazon One Enterprise são registradas CloudTrail e documentadas no [Ações, recursos e chaves de condição do Amazon One Enterprise](#). Por exemplo, chamadas para o ListSites RebootDevice e DeleteDeviceInstance 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 root ou AWS Identity and Access Management (IAM).
- 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 AWS serviço.

Para obter mais informações, consulte o [CloudTrail userIdentityelemento](#).

Entendendo as entradas do arquivo de log do Amazon One Enterprise

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 contém 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 API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

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

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAKDBG0AT6C2EXAMPLE:J_D0E",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_D0E",
    "accountId": "123456789012",
    "accessKeyId": "AKIALAVPULGA71EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAKDBG0AT6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
        "accountId": "123456789012",
        "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
        "creationDate": "2023-10-11T06:28:04Z",
        "mfaAuthenticated": "false"
    }
}
},
"eventTime": "2023-10-11T07:19:09Z",
"eventSource": "one.amazonaws.com",
"eventName": "CreateSite",
"awsRegion": "us-east-1",
"sourceIPAddress": "XXX.XXX.XXX.XXX",
"userAgent": "userAgent",
"requestParameters": {
    "name": "****",
    "description": "****",
    "address": {
        "addressLine1": "****",
        "addressLine2": "****",
        "addressLine3": "****",
        "city": "EXAMPLE_CITY",
        "postalCode": "12345",
        "countryCode": "EXAMPLE_COUNTRY",
        "stateOrRegion": "EXAMPLE_STATE"
    },
    "clientToken": "abc12d34-567e-8910-1112-12fghi0jk131"
},
"responseElements": {
    "stateOrRegion": "EXAMPLE_STATE",
    "createdAtInMillis": 1697008749263,
    "city": "EXAMPLE_CITY",
    "countryCode": "EXAMPLE_COUNTRY",
    "deviceInstanceCount": 0,
    "postalCode": "12345",
    "name": "****",
    "description": "****",
    "siteId": " abCdefG12hijkl",
    "siteArn": "arn:aws:one:us-east-1:123456789012:site/abCdefG12hijkl",
    "tags": "****"
},
"requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
```



```
"eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",  
"readOnly": false,  
"eventType": "AwsApiCall",  
"managementEvent": true,  
"recipientAccountId": "123456789012",  
"eventCategory": "Management"  
}
```

Solução de problemas do Amazon One Enterprise

Se você tiver problemas com o dispositivo Amazon One ou com um dos seus dispositivos Amazon One, use essas sugestões para solucionar o problema. Então, se você ainda estiver tendo problemas, entre em contato com o AWS Support.

Tópicos

- [Solução de problemas de identidade e acesso ao Amazon One Enterprise](#)
- [Solução de problemas do console Amazon One](#)
- [Solução de problemas do dispositivo Amazon One](#)

Solução de problemas de identidade e acesso ao Amazon One Enterprise

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon One Enterprise e IAM.

Tópicos

- [Não estou autorizado a realizar uma ação no Amazon One Enterprise](#)
- [Quero permitir que pessoas de fora da minha Conta da AWS acessem meus recursos do Amazon One Enterprise](#)

Não estou autorizado a realizar uma ação no Amazon One Enterprise

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um `my-example-widget` recurso fictício, mas não tem as permissões fictícias `GetWidget`.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação `one:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas de fora da minha Conta da AWS acessem meus recursos do Amazon One Enterprise

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon One Enterprise oferece suporte a esses recursos, consulte [Como o Amazon One Enterprise trabalha com IAM](#).
- Para saber como fornecer acesso aos seus recursos em todas as Contas da AWS que você possui, consulte [Fornecer acesso a um IAM usuário em outra Conta da AWS de sua propriedade](#) no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte [Fornecer Contas da AWS acesso a terceiros](#) no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte [Fornecendo acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do IAM usuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a [recursos entre contas IAM no Guia](#) do IAM usuário.

Solução de problemas do console Amazon One

Se você tiver problemas com o Amazon One Console ou com um dos seus dispositivos Amazon One, use essas sugestões para solucionar o problema. Então, se você ainda estiver tendo problemas, entre em contato com o AWS Support.

Tópicos

- [Não consigo criar um site](#)

- [Não consigo criar uma instância de dispositivo](#)
- [Não consigo criar um modelo de configuração](#)
- [Não consigo criar um código QR de ativação](#)

Não consigo criar um site

- Entre em contato com o administrador do Amazon One Console para fornecer acesso.
- Se o problema persistir, entre em contato com o AWS Support.

Não consigo criar uma instância de dispositivo

- Entre em contato com o administrador do Amazon One Console para fornecer acesso.
- Se o problema persistir, entre em contato com o AWS Support.

Não consigo criar um modelo de configuração

- Entre em contato com o administrador do Amazon One Console para fornecer acesso a você.
- Se o problema persistir, entre em contato com o AWS Support.

Não consigo criar um código QR de ativação

- Entre em contato com o administrador do Amazon One Console para fornecer acesso a você.
- Se o problema persistir, entre em contato com o AWS Support.

Solução de problemas do dispositivo Amazon One

Se você tiver problemas com o Amazon One Console ou com um dos seus dispositivos Amazon One, use essas sugestões para solucionar o problema. Então, se você ainda estiver tendo problemas, entre em contato com o AWS Support.

Tópicos

- [Tela em branco](#)
- [Não consigo me conectar ao Wi-Fi ou à rede](#)

- [Erro do sistema](#)
- [O código QR não é reconhecido](#)
- [Não é possível ler o código QR](#)
- [Vários códigos QR detectados](#)
- [A instância do dispositivo não existe](#)
- [Site não encontrado](#)
- [ZIPO código não corresponde](#)
- [O tempo limite do gateway atingiu o tempo limite](#)
- [Não consigo configurar o dispositivo](#)
- [Dispositivo reiniciado com mensagem de erro e código de erro](#)
- [Logotipo da Amazon na tela do dispositivo sem nenhuma atividade adicional](#)
- [Temporariamente indisponível](#)
- [Dispositivo bloqueado](#)
- [Algo deu errado do nosso lado](#)
- [Temporariamente fora de serviço](#)
- [O dispositivo Amazon One tem danos físicos](#)
- [Não é possível ler a palma da mão](#)
- [Palm não reconhecido](#)
- [Dispositivo bloqueado devido à inatividade prolongada](#)

Tela em branco

Isso ocorre quando o dispositivo não tem energia ou fica preso durante a reinicialização.

Execute o seguinte para solucionar esse problema:

- Aguarde alguns instantes (menos de 30 segundos) caso o dispositivo esteja sendo reinicializado.
- Se o anel luminoso estiver pulsando enquanto o dispositivo estiver vazio, aguarde até 30 segundos.
- Verifique se o cabo de alimentação está conectado à tomada elétrica e firmemente na parte traseira do dispositivo Amazon One. Além disso, verifique se o cabo não está danificado.

- Verifique a fonte de alimentação.
- Verifique se todos os cabos estão conectados corretamente ao Amazon One e ao USB hub.
- Reinicie o dispositivo a partir do console.
- Se a reinicialização do dispositivo não resolver o problema, desconecte o USB hub Amazon One da fonte de alimentação e conecte-o novamente.
- Se o problema persistir, entre em contato com o AWS Support.

Não consigo me conectar ao Wi-Fi ou à rede

Isso ocorre quando o dispositivo perde a conectividade.

Execute o seguinte para solucionar esse problema:

- Se estiver conectado ao Wi-Fi, use outro dispositivo para verificar se o Wi-Fi aparece nas redes disponíveis.
- Verifique se o roteador Wi-Fi está ligado e dentro do alcance.
- O dispositivo será reconectado quando a rede se recuperar.
- Se o problema persistir, entre em contato com o AWS suporte.

Erro do sistema

Isso ocorre devido a um erro interno.

Execute o seguinte para solucionar esse problema:

- Escolha Reiniciar na tela para reiniciar o aplicativo.
- Depois de duas tentativas, se o problema não for resolvido, entre em contato com o AWS Support.

O código QR não é reconhecido

Isso ocorre devido a um código QR não autorizado ou a um código QR expirado.

Execute o seguinte para solucionar esse problema:

- Escolha Tentar novamente para voltar à tela do código QR.

- Crie um novo código QR no AWS console e, em seguida, digitalize o código QR válido.

Não é possível ler o código QR

Isso ocorre quando o aplicativo não consegue ler o código QR.

Execute o seguinte para solucionar esse problema:

- Escolha Tentar novamente para voltar à tela do código QR.
- Se o problema persistir, cancele o fluxo de trabalho de ativação e reinicie.

Vários códigos QR detectados

Isso ocorre quando vários códigos QR são digitalizados.

Execute o seguinte para solucionar esse problema:

- Escolha Tentar novamente para voltar à tela do código QR.
- Digitalize somente um código QR válido por vez.

A instância do dispositivo não existe

Isso ocorre quando a instância do dispositivo é excluída ou não existe no AWS console.

Execute o seguinte para solucionar esse problema:

- Escolha Tentar novamente para voltar à tela do código QR.
- Verifique se há a instância correta do dispositivo no AWS console. Se a instância do dispositivo estiver ausente, entre em contato com seu administrador.
- Crie um novo código QR para essa instância do dispositivo e, em seguida, digitalize o novo código QR.

Site não encontrado

Isso ocorre quando o site é excluído ou não existe no AWS console.

Execute o seguinte para solucionar esse problema:

- Verifique o AWS console para obter as informações do site. Se o site não existir, entre em contato com seu administrador.

ZIPO código não corresponde

Isso ocorre ao inserir um ZIP código diferente daquele configurado para o dispositivo.

Execute o seguinte para solucionar esse problema:

- Escolha Tentar novamente para voltar à tela ZIP Código.
- Verifique se você tem o ZIP código do site correto.
- Se o problema persistir, entre em contato com o administrador para verificar o ZIP código do site no AWS console.

O tempo limite do gateway atingiu o tempo limite

Isso ocorre quando não há resposta do gateway dentro de um tempo especificado.

Execute o seguinte para solucionar esse problema:

- Escolha Reiniciar para reiniciar o aplicativo.
- Depois de duas tentativas, se o problema não for resolvido, entre em contato com o AWS Support.

Não consigo configurar o dispositivo

Isso ocorre quando a operação falhou ao salvar a configuração no disco do dispositivo.

Execute o seguinte para solucionar esse problema:

- Escolha Reiniciar para reiniciar o aplicativo.
- Depois de duas tentativas, se o problema não for resolvido, entre em contato com o AWS Support.

Dispositivo reiniciado com mensagem de erro e código de erro

Execute o seguinte para solucionar esse problema:

- Escolha Reiniciar e deixe o dispositivo se recuperar.

- Se o dispositivo não se recuperar, desconecte o USB hub da fonte de alimentação e reconecte-o.
- Se o problema persistir, entre em contato com o AWS Support.

Logotipo da Amazon na tela do dispositivo sem nenhuma atividade adicional

Execute o seguinte para solucionar esse problema:

- Aguarde alguns instantes (menos de 30 segundos) caso o dispositivo esteja sendo reinicializado.
- Desconecte o USB hub da fonte de alimentação e reconecte-o.
- Se o problema persistir, entre em contato com o AWS Support.

Temporariamente indisponível

Execute o seguinte para solucionar esse problema:

- Certifique-se de que as USB conexões com o dispositivo/sistema host estejam seguras.
- Desconecte e reconecte todos os cabos que entram no USB hub.
- Se o problema persistir, entre em contato com o AWS Support.

Dispositivo bloqueado

Por motivos de segurança, o dispositivo Amazon One será bloqueado no caso de qualquer evento de adulteração.

Execute o seguinte para solucionar esse problema:

- Entre em contato com o AWS Support.

Algo deu errado do nosso lado

Isso ocorre quando há um erro interno.

Execute o seguinte para solucionar esse problema:

1. Desligue o dispositivo.

2. Desconecte-o da fonte de alimentação.
3. Aguarde 30 segundos.
4. Conecte o dispositivo novamente à fonte de alimentação.
5. Ligue o dispositivo.
6. Se o problema persistir, entre em contato com o AWS Support.

Temporariamente fora de serviço

Isso ocorre quando o dispositivo é retirado de serviço pelo Amazon One.

Execute o seguinte para solucionar esse problema:

- Entre em contato com o AWS Support.

O dispositivo Amazon One tem danos físicos

Execute o seguinte para solucionar esse problema:

- Entre em contato com o AWS Support para saber as próximas etapas e forneça o máximo de detalhes possível, como o que aconteceu, quando aconteceu e por que aconteceu.

Não é possível ler a palma da mão

Execute o seguinte para solucionar esse problema:

- Verifique novamente se o dispositivo Amazon One está livre de riscos e manchas.
- Certifique-se de que a palma da mão do cliente esteja livre de oclusões, como bandagens, mangas e sujeira ou óleo significativos.
- Se o problema persistir e o dispositivo não ler nenhuma palma, entre em contato com o AWS Support.

Palm não reconhecido

Execute o seguinte para solucionar esse problema:

- Peça ao cliente que tente usar a outra palma da mão.

- Certifique-se de que o cliente já esteja inscrito. Caso contrário, faça com que eles se inscrevam on-line ou no dispositivo.
- Se o problema persistir e o dispositivo não ler nenhum contato com a palma da mão, entre em contato com o AWS Support.

Dispositivo bloqueado devido à inatividade prolongada

Quando o dispositivo suspeita que foi movido do site de ativação, ele bloqueia os usuários. Isso ocorre quando o dispositivo excede o tempo máximo off-line.

Faça o seguinte para desbloquear o dispositivo:

1. No banner de erro na parte superior da página, selecione Remediar.
2. Se o dispositivo ainda estiver no local de ativação, escolha Sim, o dispositivo está neste site.
3. Se o dispositivo estiver em um site diferente, escolha Não, o dispositivo está em um site diferente. Escolher Não desativa o dispositivo. Ative o dispositivo no novo site.

Histórico de documentos do Guia do usuário do Amazon One Enterprise

A tabela a seguir descreve os lançamentos da documentação do Amazon One Enterprise.

Alteração	Descrição	Data
Atualização	Adicionado: conteúdo baseado em cenários	10 de outubro de 2024
Atualização	Tópico adicionado: Solução de problemas do console Amazon One Enterprise	10 de outubro de 2024
Atualização	Tópico adicionado: Solução de problemas do dispositivo Amazon One Enterprise	10 de outubro de 2024
Atualização	Capítulo adicionado: Configurando o Amazon One Enterprise	10 de outubro de 2024
Atualização	Tópico adicionado: Manutenção e limpeza de dispositivos Amazon One Enterprise	10 de outubro de 2024
Atualização	Conteúdo reorganizado	10 de outubro de 2024
Atualização	Tópico adicionado: Instalação do hub de E/S do dispositivo Amazon One Enterprise para acesso seguro	14 de agosto de 2024
Atualização	Tópico adicionado: Instalação de um dispositivo Amazon One Enterprise montável na parede	5 de junho de 2024

[Lançamento inicial](#)

Versão inicial do Guia do
usuário do Amazon One
Enterprise

27 de novembro de 2023

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.