

ÍNDICE

O que é?	1
Como indicar a recuperação de dispositivo ao cliente	1
Como visualizar a recuperação de dispositivo no Oráculo	4
Outras orientações	5
Autorização de Dispositivos no App Stone	5
Como é solicitada a autorização do dispositivo	6
Autorizar o acesso do novo dispositivo:	13
Rejeitar o acesso do novo dispositivo:	16
Gerenciamento de Dispositivos no App	21
O que é possível fazer a partir do dispositivo primário	21
O que é possível fazer a partir do dispositivo confiável ou não cadastrado	26
Bloqueando, desbloqueando e desconectando dispositivos	28
FAQ	29

O que é?

Caso o cliente precise trocar o dispositivo principal cadastrado para acesso à conta por alguma razão (como mudança de aparelho celular, perda do aparelho, atualização de software, desinstalação do aplicativo, etc), antes era necessário que ele entrasse em contato com o RC e fosse direcionado ao time de Shield.

Hoje, no entanto, **esse procedimento é realizado pelo autosserviço no aplicativo.**

ATENÇÃO: Não deve-se orientar o cliente a desinstalar o app Stone em hipótese alguma.

Como indicar a recuperação de dispositivo ao cliente

Para tratar, é muito simples. Basta seguir o fluxo:

- A) Confirmar se está falando com o Titular da Conta;
- B) Orientar que o cliente realize login no novo dispositivo que deseja cadastrar como primário, e siga o passo a passo abaixo:
 1. Realizar login no aplicativo;
 2. Após realizar o login, o cliente será direcionado para a tela abaixo de autorização

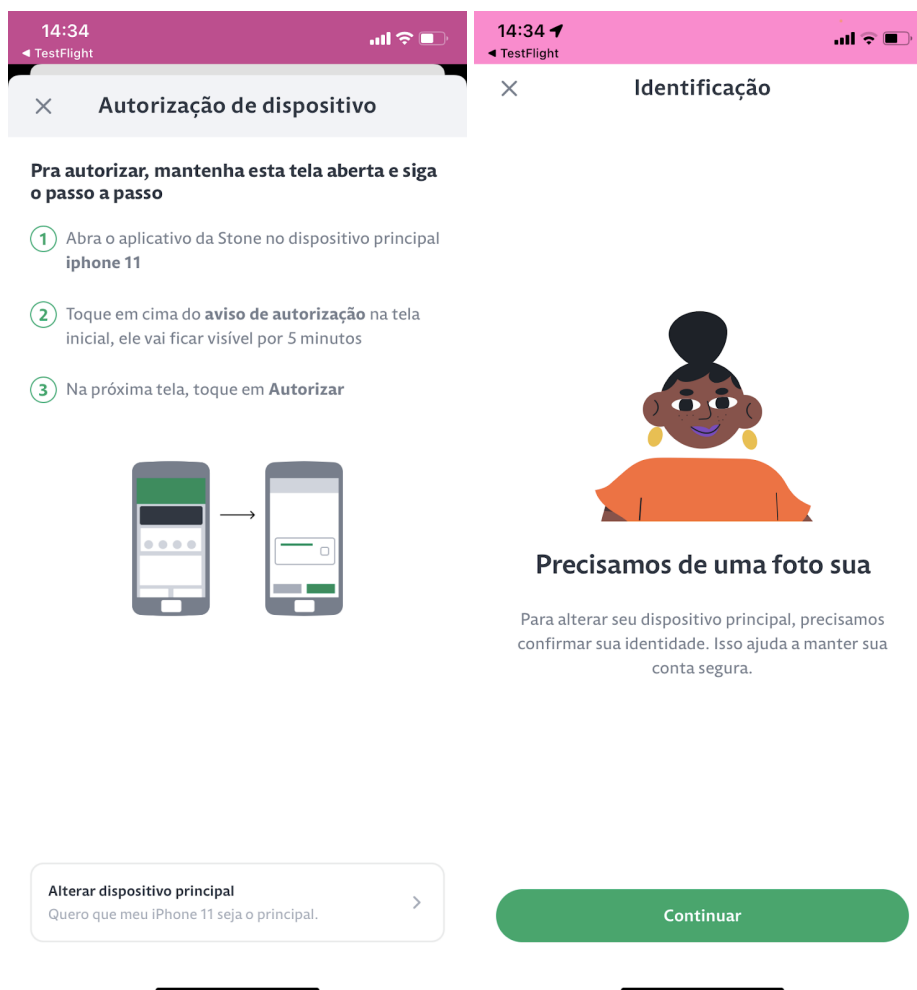
de dispositivo, onde ele precisará clicar em **"Alterar dispositivo principal"**;

3. Após clicar em **"Alterar dispositivo principal"**, aparecerá a tela de identificação, com o texto **"Precisamos de uma foto sua"** e abaixo explicando que, por segurança, é preciso confirmar a identidade dele. O cliente deve clicar em **"Continuar"**.

4. Ao clicar em continuar, o cliente deverá iniciar o processo de envio do KYC (foto do rosto, não é necessário estar com o documento em mãos);

5. Após finalizar o processo de envio do KYC, o cliente deverá aguardar o prazo de até 30 min para ter a sua demanda resolvida.


O registro será feito com a classificação: **Solicitação > Segurança > Cadastro de Dispositivo**, junto às picklists de "Autosserviço Oferecido" e "Motivo Cadastro de Dispositivo".



✕ 12:30

Pra manter sua conta segura, tire uma foto do seu rosto

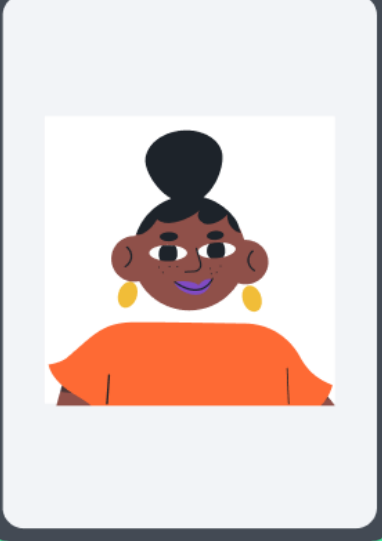
- Escolha um lugar bem iluminado
- Retire acessórios que cobrem seu rosto
- Tenha cuidado pra foto não sair tremida



Tirar com a câmera frontal

Tirar com a câmera traseira


Posicione seu rosto no centro da tela



Começar

← ✕ 12:30

✕ **Identificação**



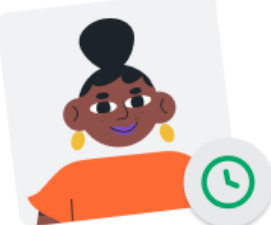
Esse vai ser o dispositivo principal da sua conta

SOBRE O DISPOSITIVO PRINCIPAL

Mais segurança pra sua conta
Outros dispositivos só podem acessar sua conta com autorização. Assim, seus dados ficam mais seguros.

Somente você autoriza outros dispositivos
Você confere as informações dos dispositivos que querem acessar sua conta e autoriza apenas se quiser.

Você define seus dispositivos confiáveis
Os dispositivos confiáveis não precisam da sua autorização toda vez que forem acessar a conta.



Estamos analisando sua foto pra autorizar este dispositivo

Em até 30 minutos vamos te dar uma resposta por e-mail. Por enquanto, não vai ser possível acessar a conta com este dispositivo.

Continuar

Sair

ATENÇÃO (02): O cliente receberá o retorno da ação recuperativa por e-mail.

Como visualizar a recuperação de dispositivo no Oráculo

A ação de Recuperação de Dispositivo aparecerá na parte de auditoria do Oráculo, na aba de Histórico de recuperação de dispositivo (imagem abaixo), onde será possível visualizar o status das solicitações de recuperação feitas pelo cliente.

Histórico de recuperação de dispositivo					
Criado em ↓	Atualizado em	Status	Id do pedido	Itens	Ver mais
07/10/2022 16:34:32	07/10/2022 16:35:21	Concluído	e50b1cea-f0df-4318-a407-1400b57b7c83	Cadastro de dispositivo Selfies	👁
31/08/2022 14:19:44	31/08/2022 14:20:31	Concluído	dbe6c097-eb86-4f8a-9fc3-df516dad9b66	Selfies Cadastro de dispositivo	👁
08/07/2022 14:21:22	08/07/2022 14:24:54	Concluído	7f4a41c-ee4c-4764-9b3e-97efaae58653	Cadastro de dispositivo Selfies	👁
08/07/2022 14:18:04	08/07/2022 14:20:49	Cancelado	8ec1731a-726d-4a79-861d-239f5dc0c2ed	Cadastro de dispositivo Selfies	👁
07/07/2022 16:21:24	07/07/2022 16:22:09	Rejeitado	2934a3e7-1acb-4adc-898e-df37e7a0bfc6	Cadastro de dispositivo Selfies	👁
03/06/2022 16:21:13	03/06/2022 16:23:16	Concluído	ee91ca8a-43f0-4a4b-b68f-ba1999cb9079	Selfies Cadastro de dispositivo	👁
30/05/2022 17:27:28	30/05/2022 17:28:40	Concluído	214972af-779a-43d2-99a3-e78880978078	Cadastro de dispositivo Selfies	👁
24/05/2022 12:17:22	24/05/2022 14:45:45	Concluído	1bced42e-004c-401a-a799-ed67e512ec61	Cadastro de dispositivo Selfies	👁
18/04/2022 13:16:21	18/04/2022 13:18:52	Cancelado	e351a659-a392-4ed4-8562-ee36f33da602	Selfies Cadastro de dispositivo	👁
23/03/2022 15:10:27	18/04/2022 13:10:27	Rejeitado	ea29c0ba-3dfe-4775-b6cb-6635a6d05fdc	Selfies Cadastro de dispositivo	👁

Linhas por página: 10 1-10 de 18 < 1 2 >

Os possíveis status de recuperação podem aparecer:

- **Respondido** - O cliente respondeu o KYC e está na fila de análise;
- **Criado** - O cliente iniciou o processo de recuperação pelo app mas não finalizou (não enviou a foto);
- **Concluído** - O pedido foi aprovado e o dispositivo foi recuperado;
- **Cancelado** - O pedido foi cancelado pelo time;
- **Rejeitado** - O pedido foi recusado após análise.

Caso o cliente entre em contato afirmando ter realizado o autosserviço pelo aplicativo, mas não recebeu um retorno da aprovação (ou a não aprovação), o encantador deverá sondar o status da recuperação no Histórico de recuperação de dispositivo.

Caso tenha havido um rejeite, é preciso entender que o time de Shield pode recusar a análise do autosserviço devido às imagens não estarem no padrão solicitado: não ser o titular, qualidade ruim, adereços, foto da foto e entre outros. Quando Shield não identifica o cliente no processo de validação, acontece o rejeite da foto. Neste caso, basta que o encantador indique que o cliente faça o processo de autosserviço novamente e explique como tirar uma boa foto.

Outras orientações

É de extrema importância que se oriente o cliente a realizar o procedimento com um discurso ajustado e completo. Com isso, ficam aqui sugestões para que adequações sejam realizadas durante o atendimento, visando passar as informações de forma clara e objetiva para a nossa razão.

Pontos essenciais para o atendimento:

1. Explicar porquê o procedimento é realizado via autosserviço, e não mais via atendimento:

“Hoje, o nosso processo de liberação de dispositivo está sendo realizado no próprio aplicativo! Dessa forma, você poderá realizar a qualquer momento do seu dia e sem a necessidade de entrar em contato com a gente! É super fácil, e o retorno costuma ser dentro de 30 minutos.”

2. Orientar o cliente no envio correto da selfie:

“Para a análise ser mais rápida, é necessário que o envio seja feito pelo titular do cadastro, combinado? Além disso, é importante enviar a selfie em um ambiente claro e sem acessórios no rosto, como máscara ou óculos escuro. Outra dica é deixar o celular bem paradinho quando for realizar o envio e é sempre legal dar aquela limpada na câmera para termos uma foto nítida”

3. Solicitar que o cliente olhe o e-mail:

“Ah, e a resposta sobre a liberação será feita por e-mail, tudo bem? Peço que fique de olho por lá, porque em breve chegará a notificação para você”

Autorização de Dispositivos no App Stone

O que é?

É uma funcionalidade do aplicativo que permite o usuário autorizar o acesso de outros dispositivos à sua conta, além de permitir que dispositivos se tornem confiáveis, ou seja, sempre acessem a conta sem solicitar autorização do dispositivo primário cadastrado.

É importante frisar que somente o dispositivo primário pode autorizar o acesso de outros dispositivos à sua conta.

Caso a conta não tenha um dispositivo primário cadastrado, não terá uma solicitação

de autorização.

Lembrando que, por norma do Bacen, a Stone deve ter 100% da base com device cadastrado, então se o cliente estiver sem dispositivo cadastrado, é necessário cadastrar.

Como é solicitada a autorização do dispositivo

A autorização do dispositivo é solicitada no momento em que um dispositivo não cadastrado solicita acesso a uma conta que possui um dispositivo primário cadastrado.

Fluxo:

1. O dispositivo não cadastrado abre o app da Stone, digita o login, senha e clica em entrar;

11:45



Entre na sua conta

E-mail ou CPF

Informe seu e-mail ou CPF

Senha

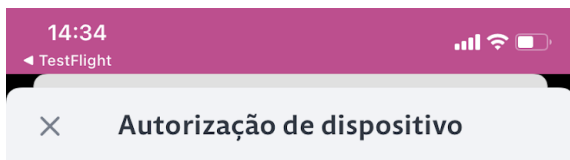
Informe sua senha



Entrar

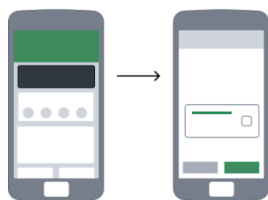
Não consigo entrar

2. Neste momento ele visualiza a tela de autorização de dispositivo;



Pra autorizar, mantenha esta tela aberta e siga o passo a passo

- 1 Abra o aplicativo da Stone no dispositivo principal **iphone 11**
- 2 Toque em cima do **aviso de autorização** na tela inicial, ele vai ficar visível por 5 minutos
- 3 Na próxima tela, toque em **Autorizar**



Alterar dispositivo principal

Quero que meu iPhone 11 seja o principal.



3. Simultaneamente, o dispositivo primário recebe o banner de autorização;



Ao clicar no banner o dono da conta visualiza quantos dispositivos solicitaram acesso. Caso tenha mais de uma autorização pendente, ele visualiza a primeira imagem. Senão, visualiza direto a segunda imagem:

12:30



✕ Autorização de dispositivo

Toque no dispositivo pra conferir as informações.



Windows 10

21:33, Rio de Janeiro - RJ



Windows XP

21:33, Rio de Janeiro - RJ



Xiaomi A2

21:33, Rio de Janeiro - RJ



✕ Autorização de dispositivo

Confira as informações do dispositivo antes de autorizar ou recusar o acesso.

Local aproximado	Rio de Janeiro, RJ
Data e hora	23 dez. às 17:54
Tipo	Celular
Modelo	iphone 11

Esse pedido vence em 00:03:47



O que acontece se eu autorizar?

O dispositivo vai poder conferir saldo, fazer transações, criar boletos e links de pagamento, entre outros.

Dispositivo confiável

Sempre autorizar que esse dispositivo acesse minha conta.



Recusar

Autorizar

17:55



✕ Autorização de dispositivo

Confira as informações do dispositivo antes de autorizar ou recusar o acesso.

Local aproximado **Rio de Janeiro, RJ**

Data e hora **23 dez. às 17:54**

Tipo **Celular**

Modelo **iphone 11**

Esse pedido vence em **00:03:47**



O que acontece se eu autorizar?

O dispositivo vai poder conferir saldo, fazer transações, criar boletos e links de pagamento, entre outros.

Dispositivo confiável

Sempre autorizar que esse dispositivo acesse minha conta.



Recusar

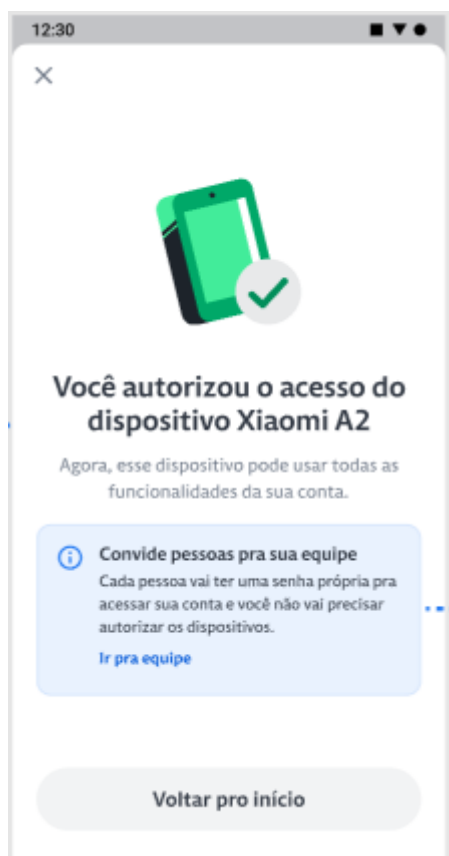
Autorizar

4. O dispositivo primário decide se autoriza ou rejeita a solicitação.

Autorizar o acesso do novo dispositivo:

1. Clicar em "Autorizar".

O dispositivo principal visualiza a tela de confirmação abaixo e o novo dispositivo, que solicitou acesso, visualiza a home da conta.



Autorizar o acesso do novo dispositivo tornando-o confiável:

Para que o dispositivo seja cadastrado como confiável é necessário que, na tela de autorização, o cliente selecione a opção "Dispositivo confiável", clique em "Autorizar" e informe corretamente o PIN (senha de 6 dígitos).

ATENÇÃO(3): Não é possível tornar um acesso via web confiável, apenas o acesso via app que pode se tornar confiável. Isso porque o app gera um número escondido (device_ID) que é salvo para identificação. Dessa forma, no app, se alguém o reinstala, por exemplo, o número muda, razão pela qual perde o cadastro do Device e um novo é solicitado.

Já na WEB, há algo semelhante a isso, no entanto, a numeração muda cada vez que

o cliente acessa pelo navegador, dessa maneira, não há como ser salvo permanente, o que torna impossível identificar se é do mesmo computador.

Fluxo:

1. Clicar no botão "Dispositivo confiável", que ficará verde;
2. Clicar em "Autorizar".

✕ Autorização de dispositivo

Confira as informações do dispositivo antes de autorizar ou recusar o acesso.

Local aproximado	Rio de Janeiro, RJ
Data e hora	03 jan. às 15:27
Tipo	Celular
Modelo	iphone 11

Esse pedido vence em 00:04:43



O que acontece se eu autorizar?

O dispositivo vai poder conferir saldo, fazer transações, criar boletos e links de pagamento, entre outros.

Dispositivo confiável

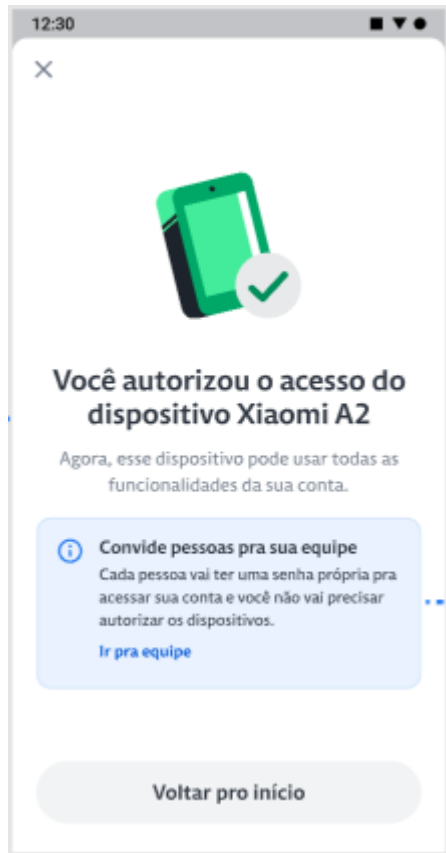
Sempre autorizar que esse dispositivo acesse minha conta.



Recusar

Autorizar

O dispositivo principal visualiza a tela de confirmação abaixo e o dispositivo que solicitou acesso visualiza a home da conta.



Rejeitar o acesso do novo dispositivo:

Na tela autorização de dispositivo, o dispositivo primário clica em "Rejeitar". O dispositivo primário visualiza a tela de rejeite do pedido e o dispositivo que solicitou acesso também visualiza a tela de rejeite da solicitação.

Dispositivo primário:

15:53



Você recusou o acesso do dispositivo iphone 11



Mantenha sua conta segura

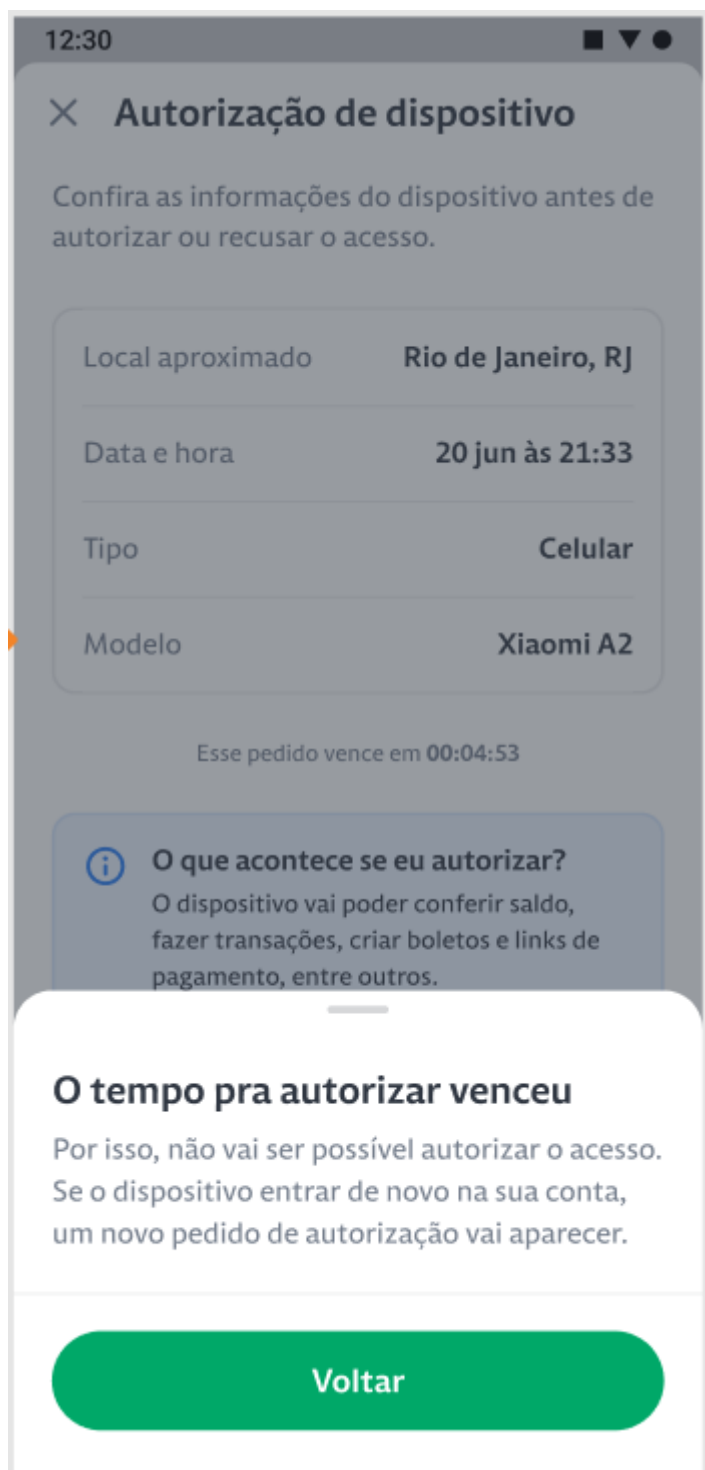
Pra mais segurança, troque sua senha de acesso e não compartilhe.

Trocar senha

Novo dispositivo:



ATENÇÃO (04): O dispositivo primário tem um prazo de 5 minutos para autorizar o novo acesso, caso não haja ação dentro desse prazo, ele verá na tela que o tempo para autorizar venceu.



ATENÇÃO (05): Para bloquear ou desconectar um dispositivo é necessário ir em **Perfil > Acessos e Dispositivos**, e somente o dispositivo primário tem permissão para essas ações. Para isso, confira os passos no artigo de gestão de dispositivos. A árvore para registro desta demanda é: **Dúvida > Segurança (D) > Cadastro de**

Dispositivo.

Gerenciamento de Dispositivos no App

O que é?

É uma funcionalidade do aplicativo que permite ao cliente visualizar quais dispositivos acessaram a conta, além de permitir o bloqueio e desbloqueio de dispositivos e o encerramento de sessões.

Importante frisar que a visualização a partir do dispositivo primário é diferente da visualização dos dispositivos confiáveis ou a de usuários que estão sem um dispositivo primário cadastrado.

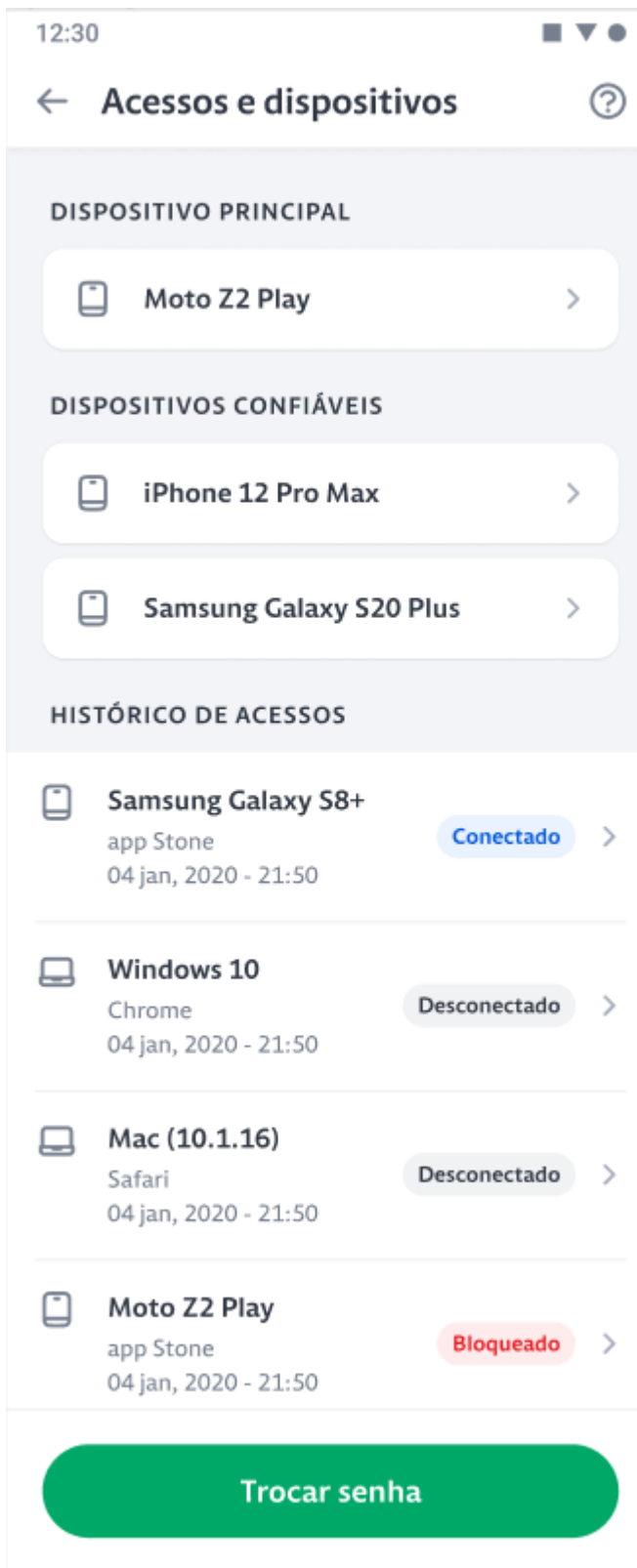
A funcionalidade é acessada na conta em Perfil > Segurança > Acessos e dispositivos.

O que é possível fazer a partir do dispositivo primário

Se a conta estiver sendo acessada a partir do dispositivo primário, o cliente conseguirá

- Visualizar os dispositivos primário e confiáveis cadastrados;
- Checar o histórico de acesso da conta em ordem do acesso mais recente para o mais antigo, incluindo:
 - Tipo do dispositivo que fez o acesso (computador ou dispositivo móvel);
 - Sistema operacional;
 - Data do último acesso;
 - Status do dispositivo (Conectado, Desconectado ou Bloqueado).

ATENÇÃO(6): no histórico é possível visualizar apenas os acessos feitos nos últimos 60 dias



Caso o cliente selecione o “**Dispositivo principal**”, verá informações sobre esse dispositivo (modelo e data e hora do último acesso) mas não será possível executar nenhuma ação (como o bloqueio), por tratar-se do dispositivo que o cliente está acessando no momento.

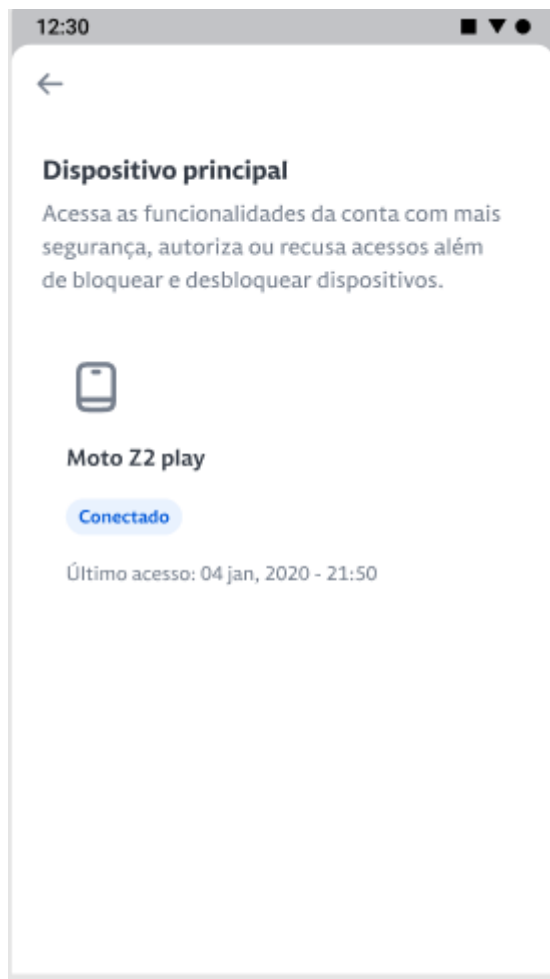
Caso o cliente selecione um dos “**Dispositivos confiáveis**”, verá informações sobre esse dispositivo (modelo, data e hora do último acesso e status do dispositivo) e será possível efetuar o bloqueio dele e a desconexão do dispositivo caso a sessão esteja ativa.

ATENÇÃO (07): caso seja bloqueado, um dispositivo confiável automaticamente deixa de ser confiável, mesmo que seja desbloqueado depois. Para que volte a ser confiável será necessário efetuar novamente o processo de cadastro de confiável.

ATENÇÃO (08): Caso seja desconectado, um dispositivo confiável é deslogado automaticamente do aplicativo, mas não deixa de ser confiável. Caso ele acesse novamente o aplicativo entrará sem solicitação de autorização.

ATENÇÃO (09): Caso o cliente sinta que seus acessos estão expostos, ele pode clicar em “**Trocar senha**” e assim trocar a senha de acesso ao aplicativo.

Dispositivo principal:



Dispositivo confiável:

12:30



Dispositivo confiável

Acessa as funcionalidades da conta com mais segurança e sem precisar de uma nova autorização a cada acesso.



Samsung Galaxy S20 Plus

Conectado

Último acesso: 04 jan, 2020 - 21:50

Bloquear dispositivo

Desconectar dispositivo

Caso o cliente selecione um dos dispositivos da listagem do histórico, visualizará detalhes do dispositivo (modelo, data e hora do último acesso e status do dispositivo). Ele poderá também bloquear ou desbloquear o dispositivo e desconectá-lo se a sessão se estiver ativa.

12:30



Detalhes do acesso

Este dispositivo foi autorizado a acessar sua conta uma única vez.



Samsung Galaxy S8+

Conectado

Último acesso: 04 jan, 2020 - 21:50

Chrome (71.8.3578.98)

Bloquear dispositivo

Desconectar dispositivo

12:30



Detalhes do acesso

Este dispositivo está bloqueado e não tem autorização pra acessar sua conta.



Samsung Galaxy S8+

Bloqueado

Último acesso: 04 jan, 2020 - 21:50

app Stone

Desbloquear dispositivo

ATENÇÃO (10): o dispositivo principal e os confiáveis aparecem novamente na listagem de histórico de acessos.

O que é possível fazer a partir do dispositivo confiável ou não cadastrado

Caso o cliente esteja visualizando o gerenciamento de dispositivos a partir de um dispositivo confiável ou em uma conta que não tenha dispositivo cadastrado, ele terá acesso apenas ao histórico de acessos. Esse dispositivo não possui autonomia para

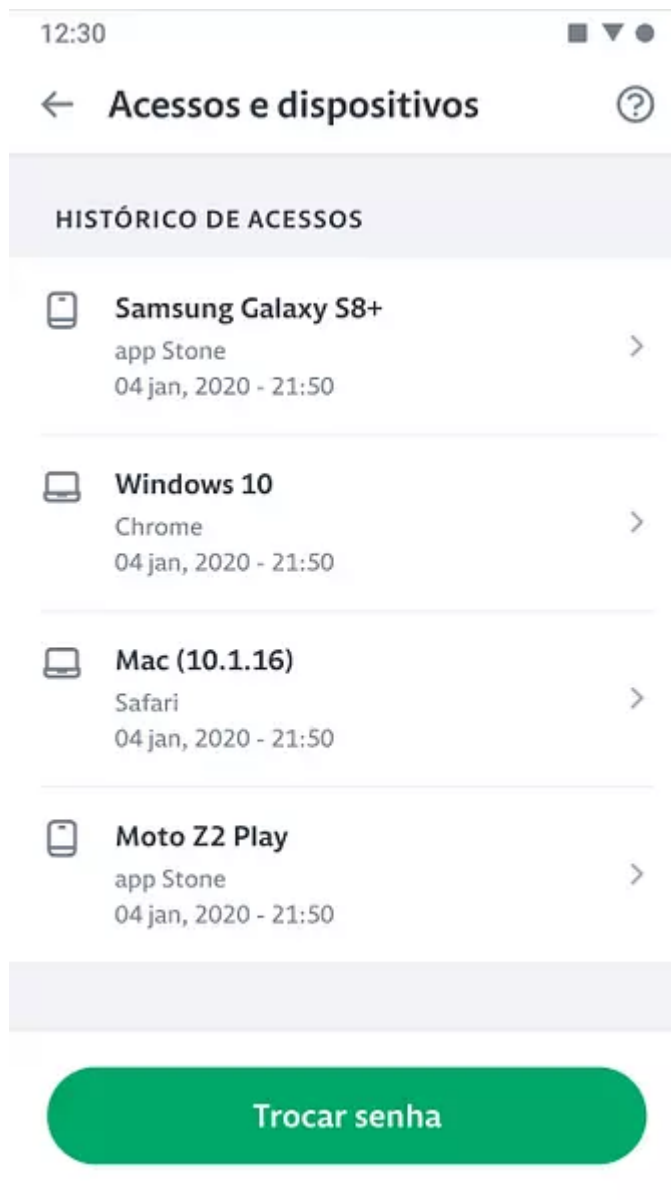
bloquear, desbloquear ou desconectar um dispositivo.

A visualização é ordenada do acesso mais recente para o mais antigo e inclui:

Tipo do dispositivo que fez o acesso (computador ou dispositivo móvel);
Sistema operacional;
Data do último acesso.

ATENÇÃO (11): o status do dispositivo (Conectado, Desconectado ou Bloqueado) não é visível para esse dispositivo.

ATENÇÃO (12): no histórico é possível visualizar apenas os acessos feitos nos últimos 60 dias.



12:30



Detalhes do acesso



Samsung Galaxy S8+

Último acesso: 04 jan, 2020 - 21:50

app Stone

Bloqueando, desbloqueando e desconectando dispositivos

Toda vez que o cliente for bloquear, desbloquear ou desconectar um dispositivo, será solicitado o PIN (senha de 6 dígitos).

Ao bloquear um dispositivo, esse dispositivo:

Não conseguirá mais fazer login na conta;

Caso seja confiável, deixará de ser;

Será desconectado caso sua sessão esteja ativa.

Ao desbloquear um dispositivo o acesso à conta poderá ser feito normalmente a

partir daquele dispositivo. Ao desbloquear o dispositivo, será necessário fornecer novamente e-mail/CPF e senha para logar, além de ser solicitada nova autorização ao dispositivo primário.

Ao desconectar o dispositivo, a sessão será encerrada e será necessário fornecer novamente e-mail/CPF e senha para logar, além de ser solicitada nova autorização ao dispositivo primário. Caso o dispositivo seja confiável não será necessária uma nova autorização.

ATENÇÃO (13): não é possível desbloquear pelo aplicativo dispositivos que foram bloqueados via Admin. Nesse caso o cliente visualizará uma tela de erro, e, para que esse dispositivo seja desbloqueado, será necessário entrar em contato com o RC.

FAQ

1. Quais os times envolvidos na aprovação do KYC?

Estão envolvidos os times de risco (Credenciamento e Risco-Banking) e alguns encantadores de Shield.

2. Qual diferença entre as telas: 30min, 6h e 2 dias úteis?

A tela de 2 dias úteis era um erro que já foi corrigido, visto que era uma tela com SLA antigo. Agora as telas de 30min e 6h estão certas e cada uma tem um significado:

- Tela de 30min: Caso o cliente tenha pedido uma recuperação de device ou tenha entrado no rollout.
- Tela de 6h: Caso o cliente não tenha concluído a abertura de conta ele vai cair na tela de 6h.

3. Porque alguns clientes não são aprovados em até 30min?

Na recuperação de device (dispositivo), é possível responder a maioria dos clientes dentro do SLA combinado. No entanto, no rollout, por ser um volume bem maior de clientes atrelado ao time pequeno, não é possível ter a mesma cadência. De todo modo, a entrega é sempre acima do esperado, de 70% SLA.

4. É possível alterar um dispositivo já cadastrado como confiável para primário?

Nesse caso, será necessário descadastrar o device (dispositivo) manualmente. Deve-se transferir o atendimento para o time de Shield seguir com a tratativa, como

"Problema de Cadastro de Dispositivo".

5. Quando a conta é controlada por um administrador, e não pelo titular do cadastro, existe algum fluxo onde seja possível prosseguir com o envio de uma procuração?

Não! Caso o titular queira que o responsável administre a conta, é necessário que o próprio administrador realize o fluxo de abertura de conta com uma procuração. Caso restem dúvidas sobre esse assunto, é recomendado revisar [o artigo de Abertura de Conta](#).

6. Caso cliente tenha o mesmo e-mail ou e-mail diferente de acesso no mesmo documento CNPJ, poderá cadastrar um único dispositivo como acesso primário?

Sim, quando o cliente tem CNPJ com numeração diferente e usa o mesmo e-mail ou e-mails diferentes, estes podem cadastrar um único dispositivo primário. Por exemplo: Stonildo, dono do CNPJ: 01.002.003/0001-04 e 01.003.004/0001-05, usa um único e-mail de acesso para os dois: stonildo@stone.com.br e deseja colocar o seu único dispositivo como acesso primário para os dois CNPJs, pode ser realizado este processo. Ou se fossem e-mails diferentes: stonildo@stone.com.br e stones@stone.com.br também poderia ser realizado o cadastro do dispositivo.

7. Quando um dispositivo confiável tenta fazer login na conta, o que ocorre?

Ele visualiza a home porque o dono da conta já autorizou o acesso, marcando a opção de tornar este dispositivo confiável.

8. Como vejo no Admin se um dispositivo que acessou é confiável ou não?

Na parte de histórico do Oráculo, clique em ver auditoria completa. Em seguida vá para dispositivos. Nessa parte é possível ver os status dos dispositivos.

Exemplo:

stone admin							
27/12/2022 09:00:55	E-mail	Enviado	Solicitado	Challenge de dispositivo	8c9f6caf-8293-45a9-aecc-7264c0ee8070	usuario2c3c4b-e5d2-4276-9f64-019f9501d128	
24/12/2022 15:22:26	E-mail	Enviado	Pedido expirado	Links de Pagamento	b1cd0951-8789-403f-845a-1aed8c759f22	usuario2c3c4b-e5d2-4276-9f64-019f9501d128	
24/12/2022 15:22:26	Notificação Push	Enviado	Pedido expirado	Links de Pagamento	1d9a91b6-d322-476f-be7b-362a79d30742	usuario2c3c4b-e5d2-4276-9f64-019f9501d128	
23/12/2022 15:21:33	E-mail	Enviado	Pedido criado	Links de Pagamento	54017334-5abe-4b31-b3a7-9c81ecabc43b	usuario2c3c4b-e5d2-4276-9f64-019f9501d128	
23/12/2022 15:18:33	E-mail	Enviado	Solicitado	Challenge de dispositivo	5863535e-4808-48f8-b3e6-74b6af9af1d8	usuario2c3c4b-e5d2-4276-9f64-019f9501d128	
Dispositivos							
Criado em	Detectado em	Aplicação	Versão	Sistema Operacional	Modelo	Tipo	Status
27/12/2022 09:00:55	27/12/2022 13:43:32			Windows	Não informado	desktop	Não cadastrado
01/11/2022 10:01:03	23/12/2022 16:00:51	banking	1.59.0-3	Android	motorola moto g31	smartphone	Dispositivo confiável
22/12/2022 14:22:30	22/12/2022 14:22:30			Windows	Não informado	desktop	Não cadastrado
26/10/2022 18:06:17	22/12/2022 11:08:28	banking prod	2.40.0	iOS	apple iphone 11	smartphone	Dispositivo primário
15/12/2022 17:57:33	15/12/2022 18:06:24			GNU/Linux	Não informado	desktop	Não cadastrado
28/11/2022 05:27:21	01/12/2022 17:25:22			Windows	Não informado	desktop	Não cadastrado
23/11/2022 09:37:40	23/11/2022 09:41:57			Windows	Não informado	desktop	Não cadastrado
12/04/2022 14:58:20	02/11/2022 22:44:37			Windows	Não informado	desktop	Não cadastrado

9. Autorizei o acesso de um dispositivo, mas não quero mais que ele acesse minha conta, como resolvo?

O dispositivo primário consegue desconectar ou bloquear o dispositivo indesejado. Ele precisa acessar a conta pelo aplicativo, ir em perfil, em acessos e dispositivos e desconectar ou bloquear o dispositivo que deseja. Para mais informações acesse o artigo de gestão de dispositivos. A árvore para registro desta demanda é: Dúvida > Segurança (D) > Cadastro de Dispositivo.

10. Quando um dispositivo bloqueado tenta fazer login na conta, o que ocorre?

Ele visualiza uma mensagem de erro pedindo para corrigir seus dados.

11. O cliente está tentando desbloquear um dispositivo, mas está visualizando tela de erro, o que pode ser?

Esse dispositivo pode ter sido bloqueado via Admin, nesse caso apenas a operação consegue desbloqueá-lo.

12. Cliente tem um dispositivo confiável cadastrado e quer transformá-lo em device primário. Como prosseguir?

Shield deve registrar com a árvore: Solicitação > Segurança (S) > Cadastro de Dispositivo | Picklist - Motivo: Troca de Confiável para Primário.