



Aranda Password Recovery

Este guia detalha as etapas necessárias para a instalação, configuração e uso do **Aranda PassRecovery V8 (APR)**, que permite a gestão e recuperação da palavra-passe de um utilizador registado, tendo em conta um processo de configuração e validação de questões de segurança, para o desbloqueio da conta de domínio.

Definindo um token de uso único

Durante os processos, o aplicativo envia um link exclusivo para os e-mails cadastrados do usuário (principal - alternativo). Este link contém um **Token de uso único**, que tem as seguintes características:

- O token é gerado e enviado pelo aplicativo como parte do link de acesso seguro.
- Cada token tem um tempo de validade limitado, que é previamente definido pelo administrador no **Configuração** no Admin Console.
- O token é considerado **Usado** Nos seguintes casos:
- Quando o usuário clica no ícone **Salvar** quando terminar de configurar as perguntas de segurança.
- Quando o usuário responde corretamente a todas as perguntas de segurança durante o processo de desbloqueio da conta, alteração de senha ou redefinição.
- Depois de usado ou expirado, o token não pode ser reutilizado. Em caso de tentar acessar novamente com um token inválido, o alerta será exibido: **Erro de validação de token**.

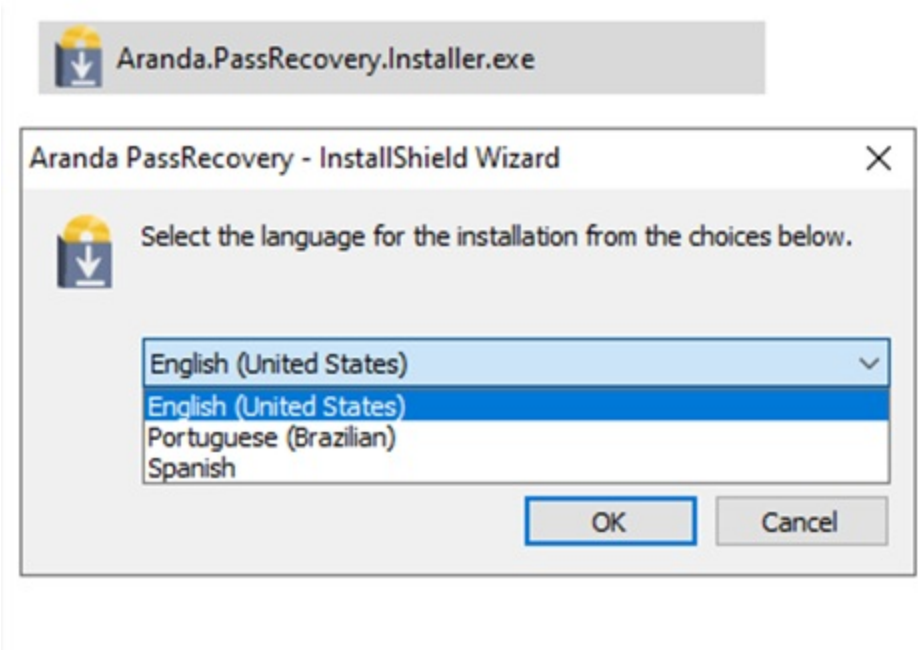
Instalação do Aranda PassRecovery

Instalação do Aranda PassRecovery

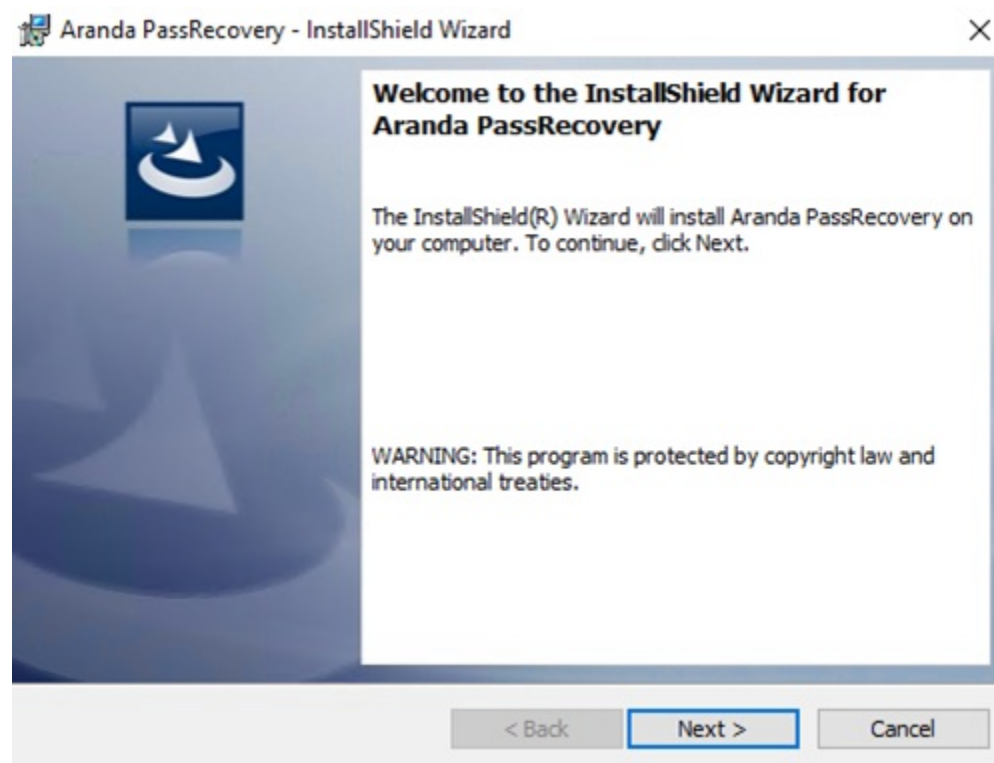
Para esta instalação, é importante que o banco de dados seja atualizado para a versão mais recente do Aranda, sendo a versão mínima necessária a versão 8.0.89.

Para instalar e configurar o aplicativo, siga estas etapas:

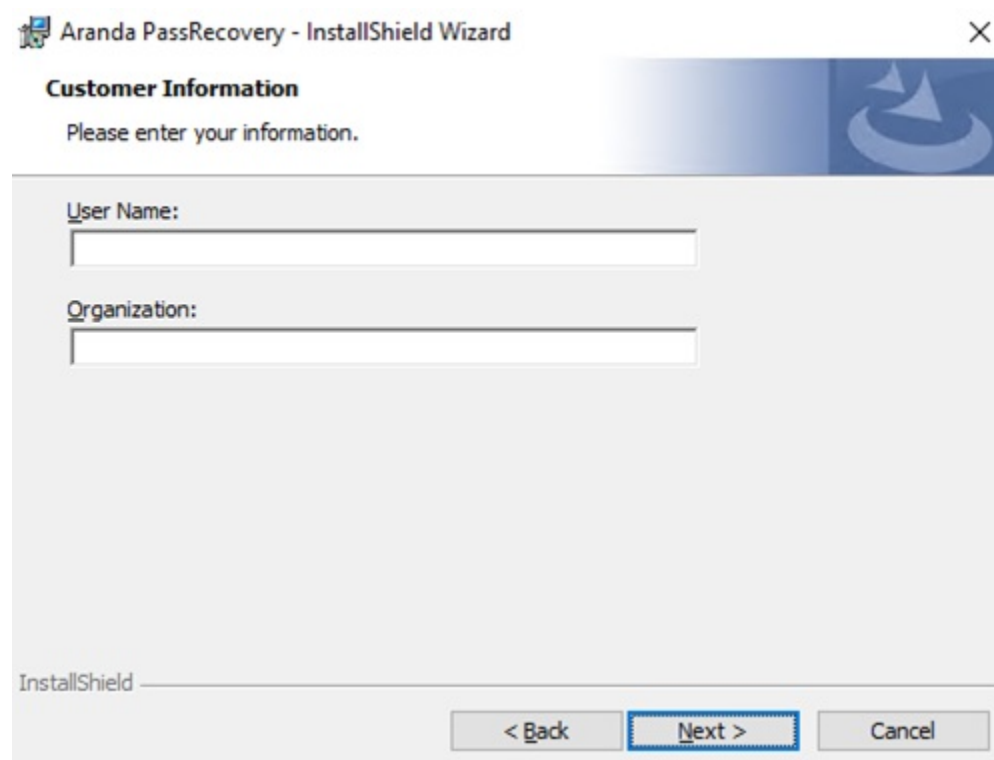
1. Execute o arquivo **Aranda.PassRecovery.Installer.exe**. O assistente de configuração lhe dará a opção de selecionar o idioma de instalação. Selecione o idioma desejado e clique no botão **OKEY**.



2. Na tela de boas-vindas, confirme a instalação clicando no botão **Seguinte**.



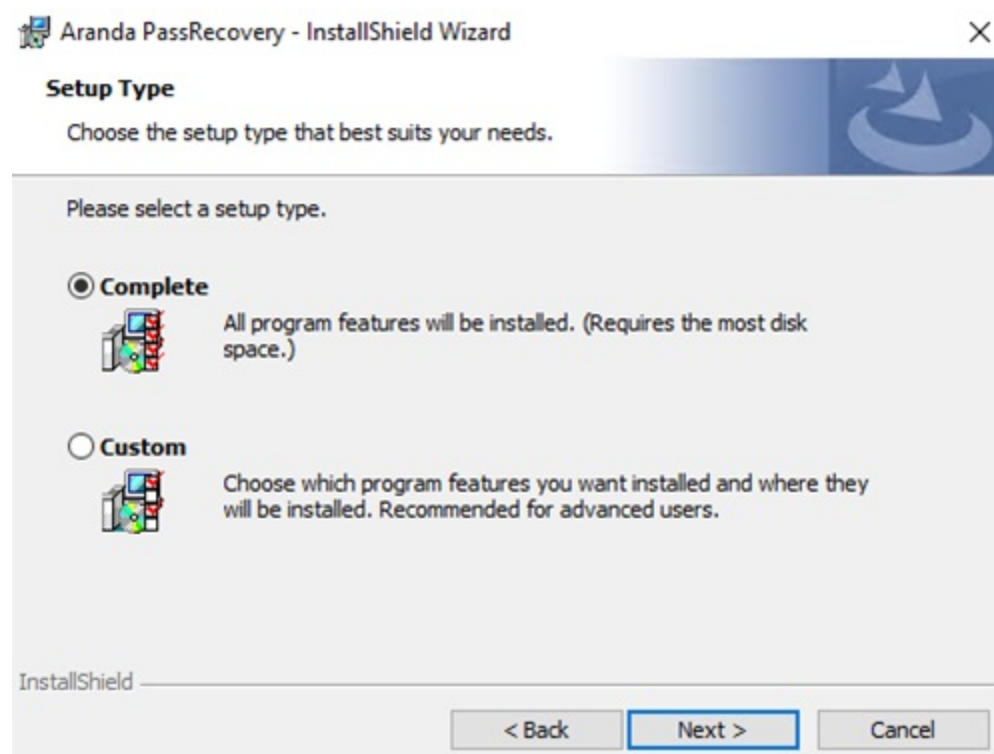
3. Na janela Informações do cliente, insira o nome de usuário, a organização e clique em Seguinte.

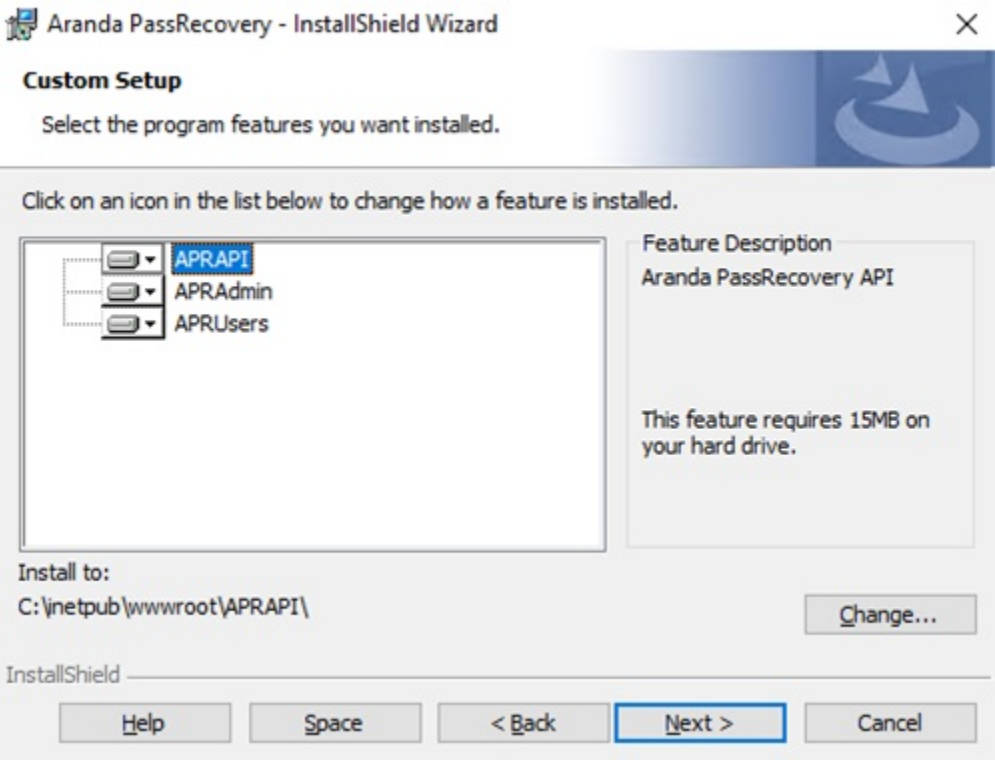


4. Na janela Tipo de instalação, você pode configurar as seguintes opções:

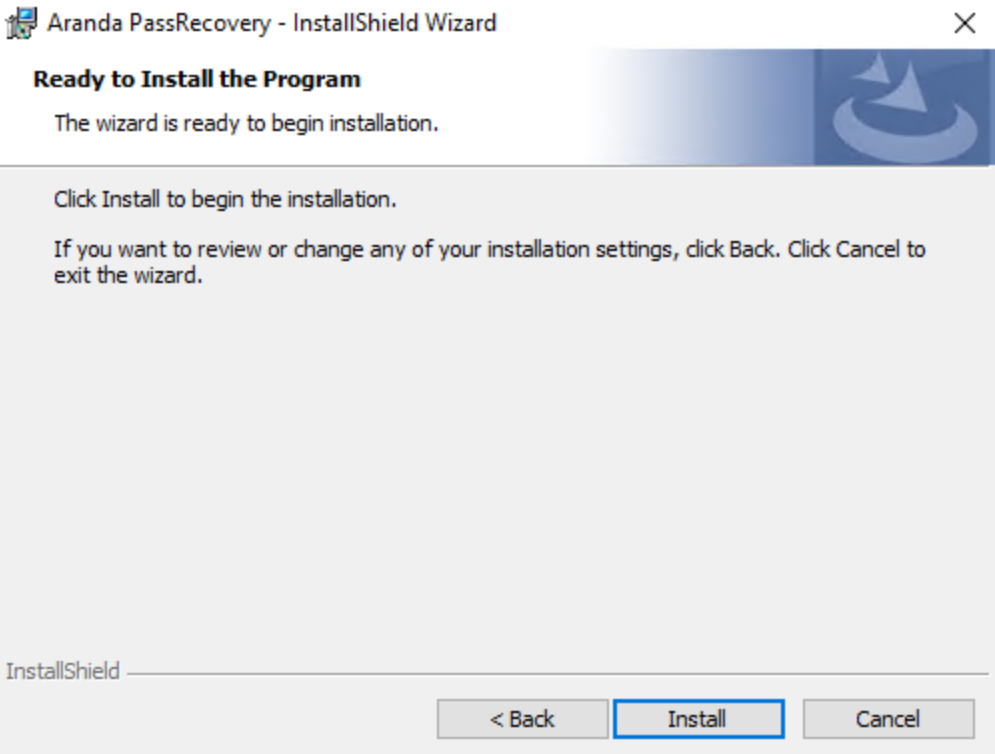
- **Completar**- Todos os sites e serviços serão instalados nas rotas padrão.
- **Costume**- Você pode selecionar os sites que deseja instalar ou alterar o caminho de instalação.

Selecione a opção e clique em Seguinte.





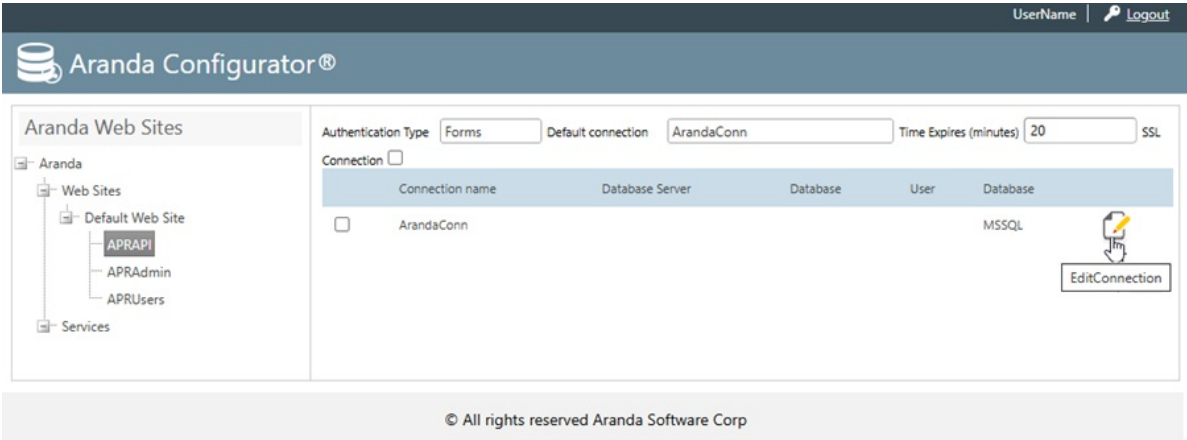
5. Para iniciar o processo de instalação, clique no botão Instalar.



6. Ao final do processo de instalação, clique no botão Fim. Três sites serão instalados no IIS: APRAdmin, APRAPI e APRUsers.

Configuração do banco de dados

7. Uma vez que a instalação do Passe de ArandaRecuperação, prossiga para configurar as strings de conexão para o banco de dados dos sites, inserindo o Configurador Aranda (AWCF). Na lista de tipos de árvore, selecione o(s) site(s) a ser configurado(s).



8. Faça a conexão com o banco de dados e, no AFW_SETTINGS, aplique os seguintes comandos de atualização (UPDATE):

```
UPDATE afw_settings SET default_value = 'https://{domain}/APRAPI/' WHERE id = 5;
UPDATE afw_settings SET default_value = 'https://{domain}/APRUsers/' WHERE id = 7;
```

📌 **Nota:** Lembre-se de substituir Domínio pelo nome ou IP do servidor de aplicativos.

```
UPDATE afw_settings SET default_value = 'https://domain/APRAPI/' WHERE id = 5;  
UPDATE afw_settings SET default_value = 'https://domain/APRUsers/' WHERE id = 7;
```

```
SELECT * FROM afw_settings WHERE id IN (5,7);
```

dos 1 X			
* FROM afw_settings WHERE id IN (5,7) Enter a SQL expression to filter results (use Ctrl+Space)			
123 id	A-Z description	123 setting_group_id	A-Z default_value
5	Url Api	1	☒ https://domain/APRAPI/
7	URL consola de usuario	1	☒ https://domain/APRUsers/

Habilitar funcionalidade e permissões

9. Para atribuir permissões a grupos e habilitar o acesso ao Console de ConfiguraçãoAranda PassRecuperação (APRAdmin), efetue login do servidor de aplicativos no console Perfil de Aranda. Selecione na lista de aplicativos ARANDA PassRecuperação e atribua a(s) permissão(ões) correspondente(s), de acordo com as regras de negócio.

Permissions/workgroups definition Users setup

Applications ARANDA PASS RECOVERY

- Aranda EventLog
- Aranda Software Metrix
- Aranda Software Delivery
- Aranda PCBrowser
- ARANDA SERVICE DESK BLOGIK
- Aranda Service Desk Front End
- Self Service KB
- ArandaMySoftware
- ArandaFAQ
- ARANDA DBImport
- ARANDA CMDB
- ARANDA WEB MANTENIMIENTO
- ARANDA SLM
- ARANDA SELF SERVICE
- ARANDA QUERY WEB
- ARANDA POWER MANAGEMENT
- ▶ ARANDA PASS RECOVERY

New workgroup Delete workgroup

Workgroups Administrator

- Administrator Administrator
- ▶ Administrator
- Administrator

Granted permissions

☒ Add permission to a workgroup ☒ Delete permission ☒ Select all ☒ Unselect all

Permissions	Audit
ACCESS THE CONFIGURATION MENU	☐
ACCESS THE DIRECTORY MENU	☐
ACCESS THE DOMAINS MENU	☐
▶ ACCESS THE TEMPLATES MENU	☐
EXECUTE APPLICATION	☐

10. No console de configuração da Web (BASDK), configure o caminho acessando Opções > Resumo, e no campo URL de PassRecovery Entrar 'https://{domain}/APRUsers/'. Lembre-se de substituir Domínio pelo nome ou IP do servidor de aplicativos.

Aranda SERVICE DESK  Configuración

Save

Options

Projects

Summary

Licenses

Actions

Status

Company

Survey

Provider

Chat

Setup

Scripts and help

Iti

Use Console

Change Password

Log Out

User Name in Session06/06/2025 7:45:41 p.m.

StartSummary

Service Desk ITService Desk IT

General parameters setup

Summary

Attach files to cases

File server address

Max. size of attached files (MB)

Send satisfaction survey link

Web server name

License time to expire

Time due for license to expire (mins)

Specific options

☐ Hide Aranda's Login

It allows hiding the Aranda Login in the consoles when you have SAML configuration.

☐ Allow using the same identifier in companies

☐ Enable password reminder for specialists

☐ Enable sending voting process MS Teams

☐ Enable sending survey MS Teams

☐ Enable push notification push

Push notification message. Max (200)

☐ Hide Aranda Assistant

Allows you to hide the Aranda assistant and the specialist chat in the user console.

☐ Hide send mail option

Allows you to hide the option Send mail in case management in the specialist console

Internationalization

Select the language for system notifications

☐ Spanish

☒ English

☐ Portuguese

Format for dates

Register Case

☐ Enable service filter case creation

☐ Enable filter customer - company in creating cases

Remote Control

URI Control Remote

Site of authorization

Survey API Address

URL console ASDK

REST Api Address

Remember to change the URL REST API must generate the QR code again.

URL push server, Aranda software

Chat Api Address

PassRecovery URL

https://domain/APRUsers/

Set the word for client

This configuration applies to the user console.

Record lock time

Time for record to be locked for edition (mins)

15

Default Record Type - Specialist Console

Service Requests

Mail

Problems

Mail

Incidents

Mail

Changes

Mail

Statistics

Number of existing actions : 0

Number of existing categories : 461

Number of existing rules : 31

11. Para ativar a recuperação de senha para usuários do domínio a partir do console da Web USDKV8entrar BASDK > Console do usuário > detalhes do cliente e habilite o Ativar lembrete de senha.

Aranda SERVICE DESK  Configuración

Save

Options

Setup

Scripts and help

Iti

Use Console

Case Creation

Record Closure

Client - Details

Procurar o caso

Links to redirect case

Access Options

Config Branding

Home Panels

Scheduled notifications Health Report

Change Password

Log Out

User Name in Session06/06/2025 8:08:38 p.m.

StartClient - Details

Service Desk ITService Desk IT

Client - Details

Client - Details

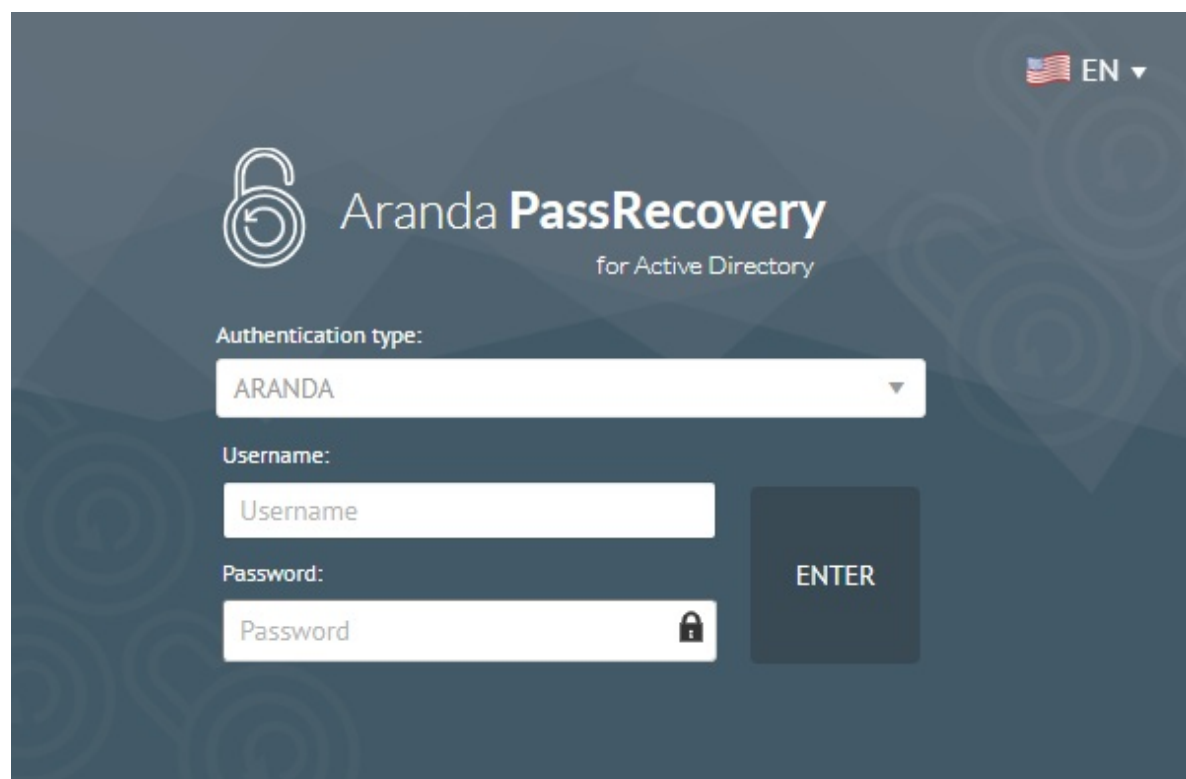
☐ Allow the client to edit its details

☒ Enable password reminder

Console de administração (APRAdmin)

Login

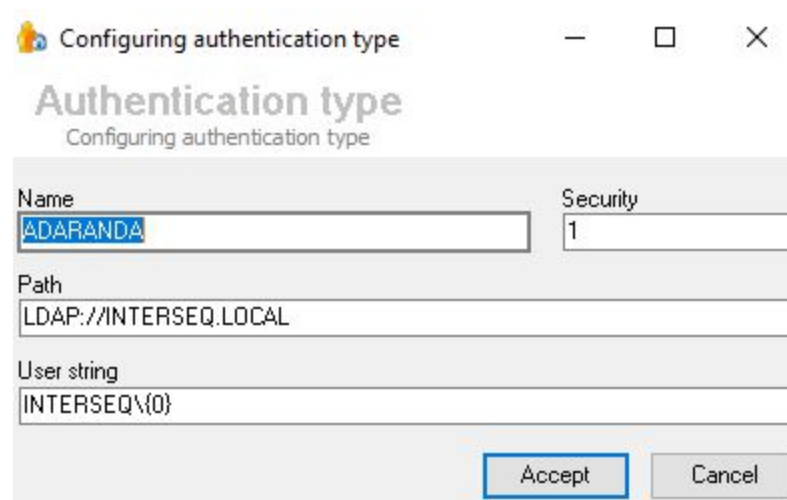
Para fazer login no Passe de ArandaRecuperação, o usuário deve pertencer a um grupo com permissões de acesso ao aplicativo. A URL de acesso é: 'https://{domain}/APRAdmin/'



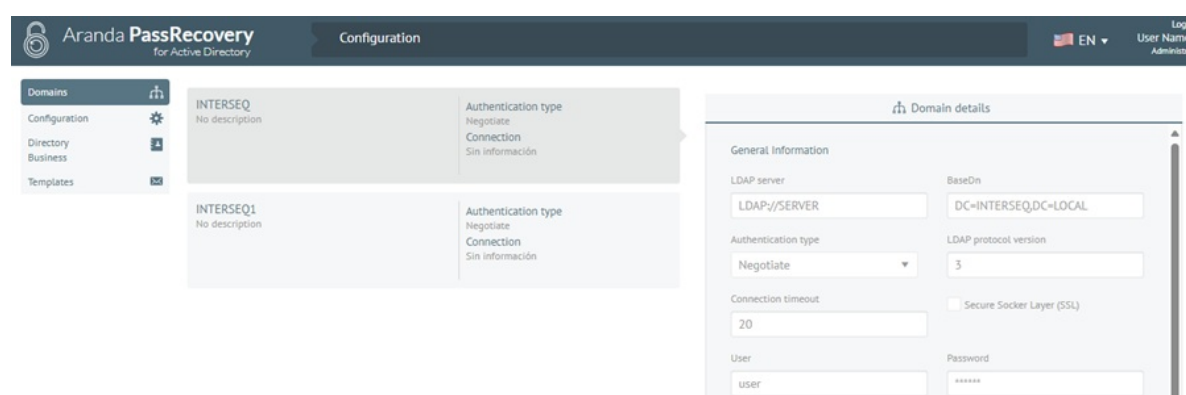
Domínios

Configurações de domínio

Os domínios presentes no Admin Console (APRAdmin) deve ser pré-configurado em Perfil de Aranda, no Configuração > tipo de autenticação.



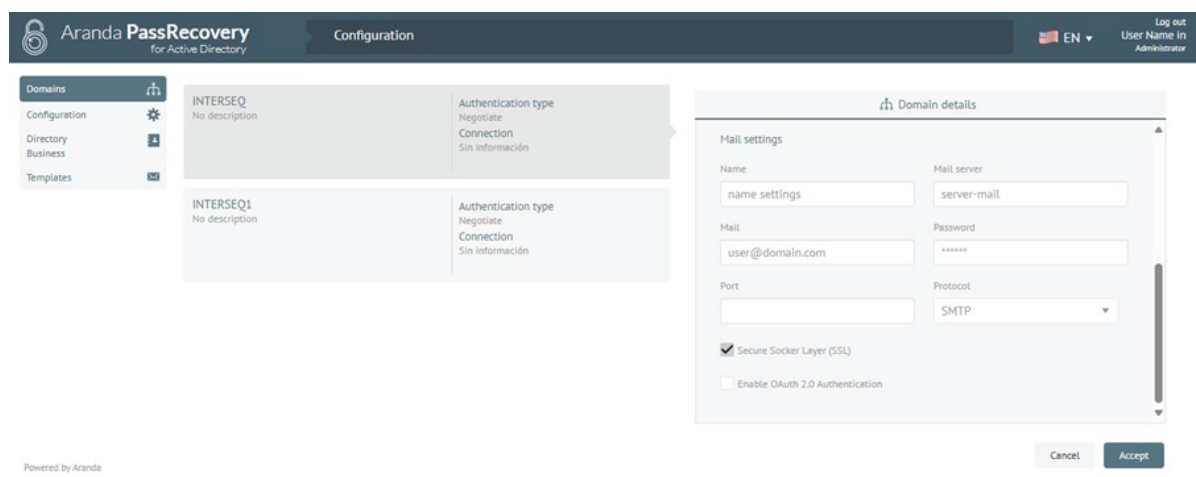
Quando você fizer login no Admin Console, os domínios pré-configurados serão listados automaticamente na página Domínios. No Visão geral, você pode preencher ou atualizar os detalhes do domínio conforme necessário.



✎ **Nota:** É importante configurar um usuário de domínio com privilégios suficientes, que tenha a permissão “Redefinir senhas de usuário e forçar alteração de senha” habilitada no nível do DÁ (Active Directory). Se esta condição não for atendida, as ações executadas não serão aplicadas.

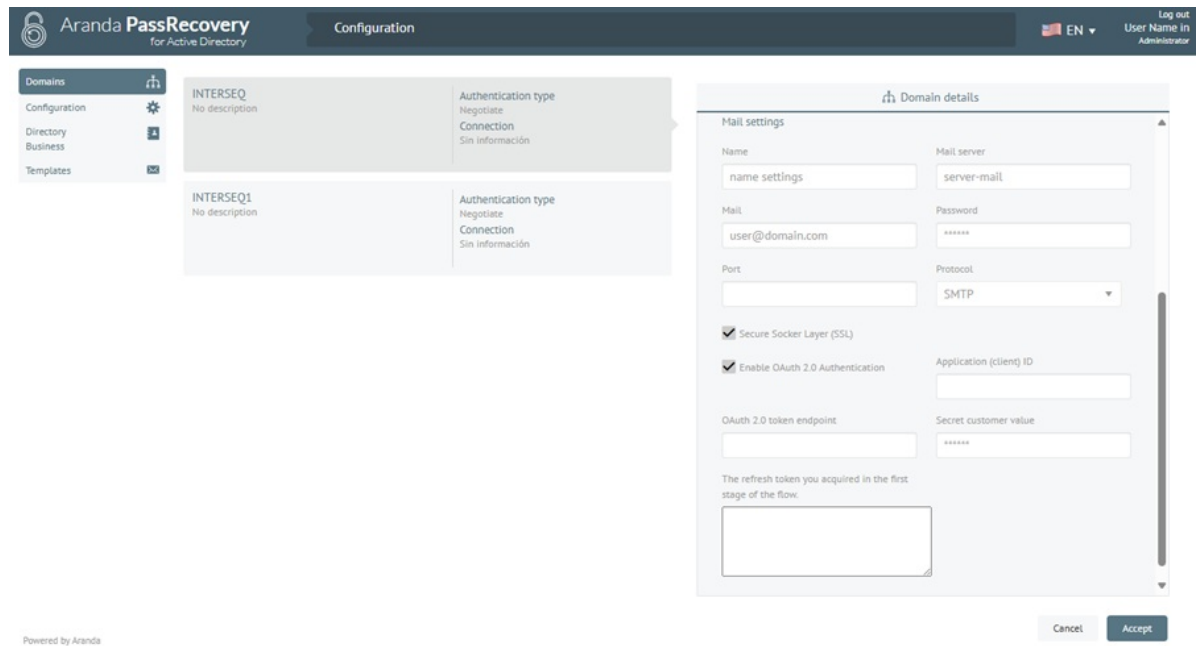
Configurações de e-mail

No Configurações de e-mail, você pode configurar dois tipos de autenticação (Básico e OAuth 2.0) para o envio de correspondência. Preencha as informações solicitadas de acordo com a configuração desejada.



Quando você ativa a verificação de campo **Habilitar a autenticação OAuth 2.0**, preencha os dados correspondentes, conforme indicado no seguinte documento:

[Configurações de autenticação moderna do OAuth](#)



Quando a configuração estiver concluída, clique no botão **Aceitar**. Se tudo tiver sido configurado corretamente, o alerta será exibido **Domínio atualizado**. Caso contrário, valide a configuração e tente novamente.

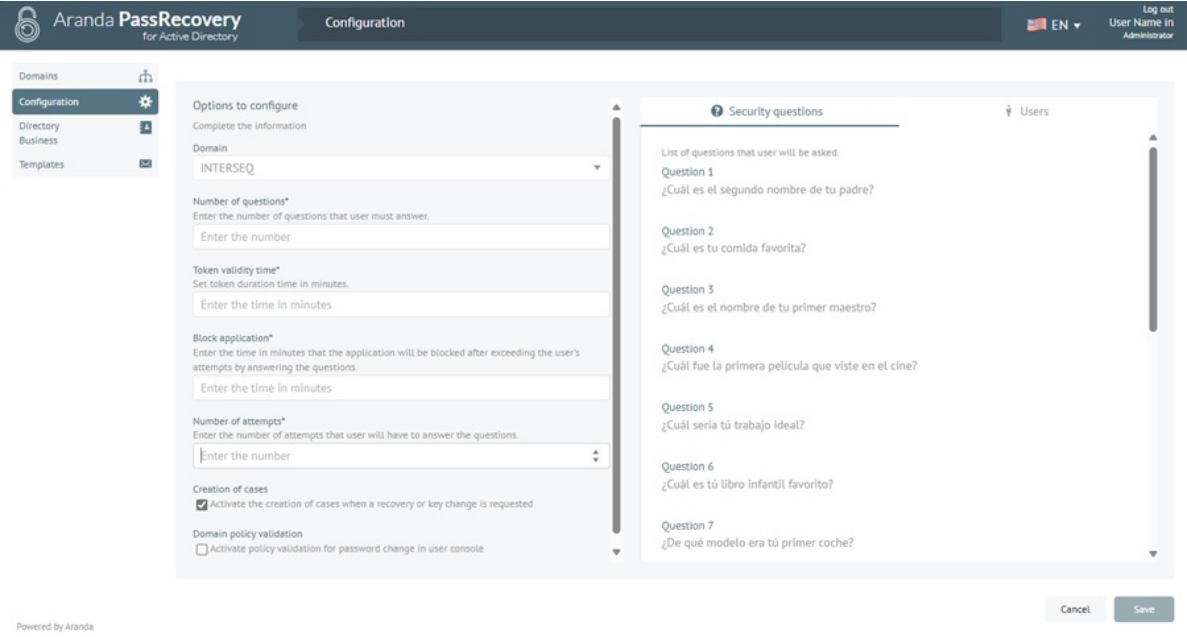
Configuração

Ao entrar no Admin Console (APRAdmin), no **Configuração**, o administrador poderá fazer as seguintes configurações:

Opções para configurar

Nesta seção, o administrador pode definir, para cada domínio configurado, as seguintes opções:

Campo	Descrição
Número de perguntas	Ele permite que você configure o número de perguntas que o usuário deve responder. O valor pode estar entre 1 e 15. As perguntas são predefinidas e podem ser visualizadas no Perguntas de segurança.
Tempo de validade do token	Ele permite que você defina o tempo de duração do token em minutos. Valor permitido entre 1 e 60.
Bloquear aplicativo	Ele permite que você configure o tempo em minutos durante o qual o aplicativo travará depois que o usuário exceder o número de tentativas para responder às perguntas. Valor permitido entre 1 e 60.
Número de tentativas	Ele permite que você defina o número de tentativas disponíveis para o usuário responder às perguntas. Valor permitido entre 1 e 10.
Criação de caso	Permite que a criação de casos seja acionada em ASDK quando uma recuperação ou alteração de senha é solicitada. Exibir configurações de criação de caso
Validação de política de domínio	Habilita validações de política de domínio para alteração de senha no Console do usuário.



📌 Anotações:

- Os campos marcados com (*) são obrigatórios.
- Para o campo **Número de perguntas**, se seu valor for alterado e houver usuários que já tenham P e R registrados no console (APRUsers), esses registros serão excluídos automaticamente quando o novo valor configurado for aplicado.
- Para que o bloqueio do aplicativo funcione corretamente, os servidores de aplicativos e banco de dados devem ter a data e a hora sincronizadas, bem como o computador do usuário que está acessando.

Usuários

Nesta seção, o administrador poderá definir os usuários que terão permissão para o autoatendimento (Desbloqueio de Conta, Alteração e Redefinição de Senha) no Diretório de Empresas. Você pode associar e desassociar usuários manualmente e também ativar o **Associar usuários automaticamente**, para que cada usuário no domínio que iniciar o aplicativo do usuário (APRUsers) solicite automaticamente que você configure as perguntas de segurança.

Security questions
Users

Associate the Users who will be allowed to self-service in the business directory.
☒ Associate users automatically

Users to add
Add

Associated users

Filter
☐ Select all
Disassociate

☐ Name
Juan Social
Alias
juan.social

☐ Name
Ramon Valdez
Alias
rvaldez

☐ Name
Test
Alias
test

☐ Name
Test CYS
Alias
testcys

☐ Name
Test CYS V8
Alias
testcysv8

Cancel
Save

Anotações:

- Se um usuário já tiver configurado suas perguntas de segurança e subsequentemente se desassociar desta seção, ele precisará repetir a configuração ao se associar novamente.
- Recomenda-se informar os usuários com antecedência sobre esse processo para evitar confusão ou relatos de acesso interrompido.
- As alterações aplicadas não são refletidas nas sessões ativas; Os usuários precisarão fechar e reabrir o aplicativo para aplicar corretamente as configurações.

O administrador pode **Limpar perguntas de segurança** registrado por um usuário quando necessário. Clique no ícone de três pontos do usuário associado e selecione a opção **Limpar perguntas**. Ao executar essa ação, o usuário será solicitado a reconfigurar suas perguntas de segurança no console APRUsers No seu próximo acesso, essa funcionalidade é útil em casos de suporte ou quando há suspeita de que as respostas foram comprometidas.

Security questions
Users

Associate the Users who will be allowed to self-service in the business directory.
☒ Associate users automatically

Users to add
Add

Associated users

Filter
☐ Select all
Disassociate

☐ Name
Juan Social
Alias
juan.social

Reset questions

☐ Name
Ramon Valdez
Alias
rvaldez

☐ Name
Test
Alias
test

☐ Name
Test CYS
Alias
testcys

☐ Name
Test CYS V8
Alias
testcysv8

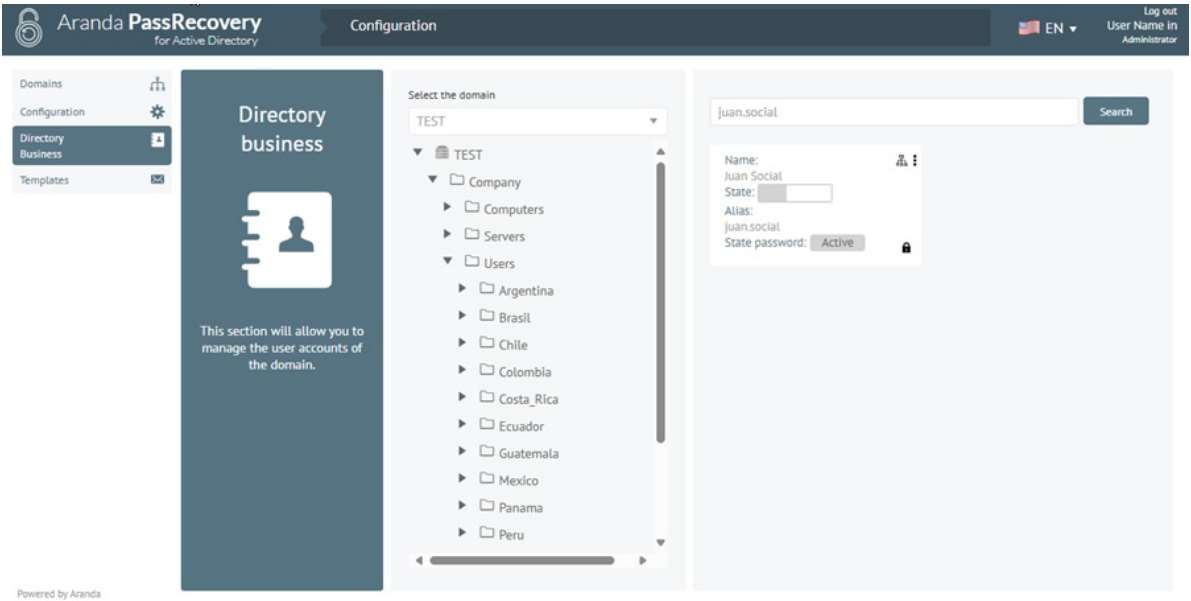
Cancel
Save

 **Aviso:** Essa ação excluirá permanentemente as respostas salvas do usuário. Certifique-se de notificar o usuário antes de executar este procedimento.

Quando a configuração estiver concluída, clique no botão **Salvar**. Se tudo tiver sido configurado corretamente, o alerta será exibido **Configurações atualizadas**. Caso contrário, valide a configuração e tente novamente.

Diretório de Negócios

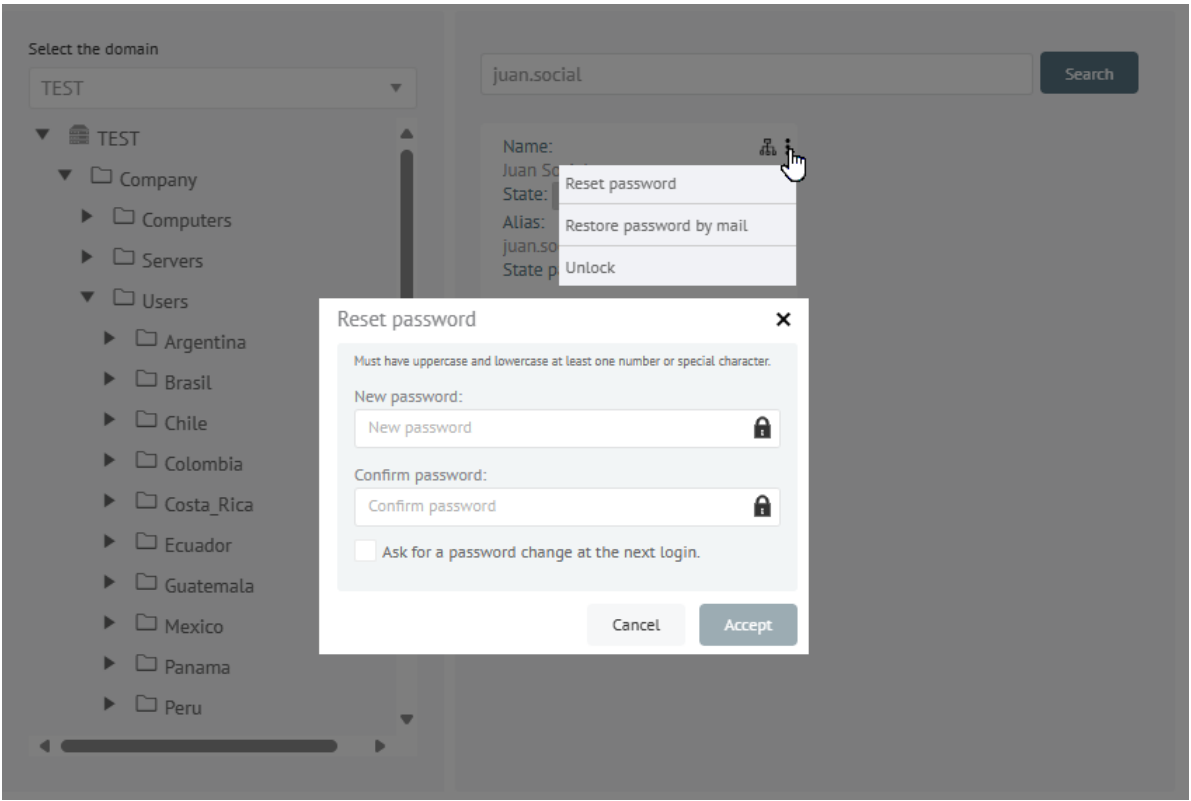
Ao entrar no Admin Console (APRAdmin), no **Diretório de Negócios**, o administrador poderá pesquisar usuários dentro do domínio selecionado, navegando na árvore ou usando o mecanismo de pesquisa preditiva.



Do Diretório de Negócios, o administrador pode realizar os seguintes procedimentos:

Redefinir senha

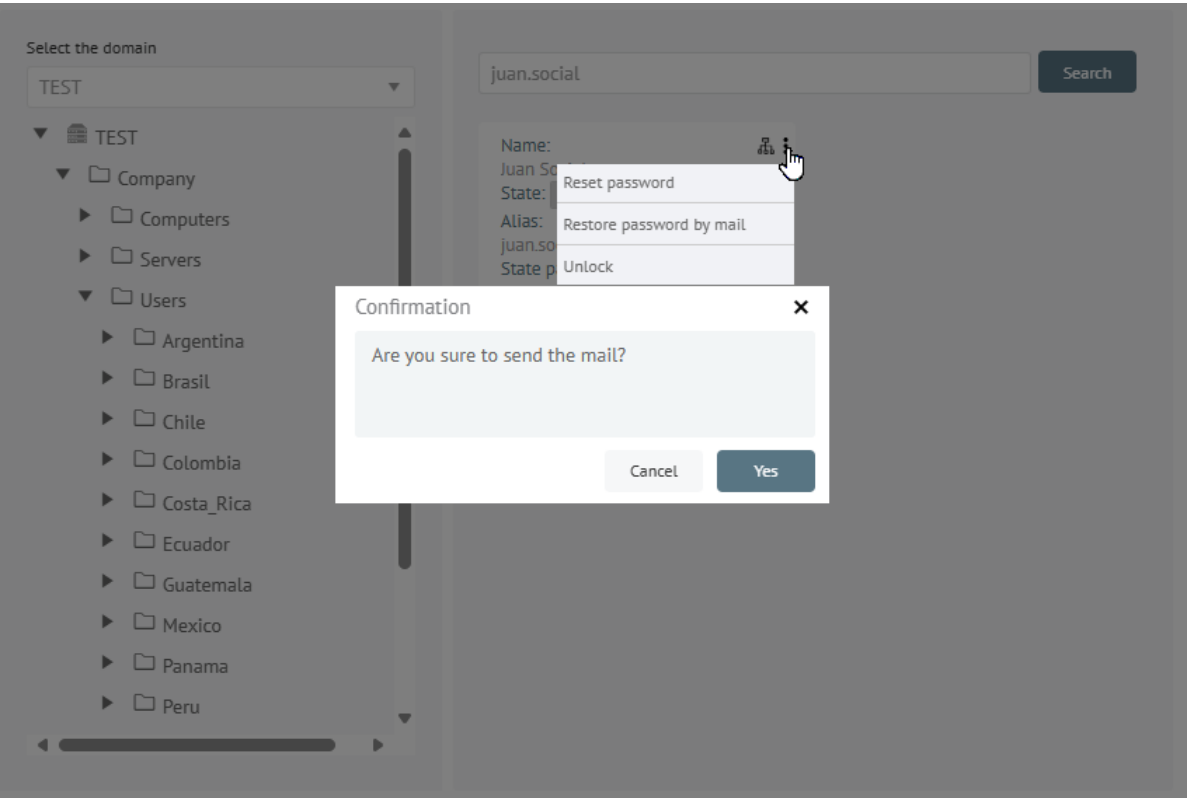
Para redefinir a senha, clique no ícone dos três pontinhos do usuário a ser gerenciado e selecione a opção **Redefinir senha**. Na janela **Redefinir senha**, preencha os campos solicitados. Quando você ativa a verificação **Peça a alteração da senha no próximo login**, você pode pedir ao usuário para alterar a senha no próximo login.



Após preencher os campos, clique no botão **Aceitar**. O alerta será exibido **Senha atualizada**. Se a opção estiver ativada **Criação de caso**, um caso será gerado automaticamente em **ASDK** de acordo com as configurações definidas.

Redefinir senha por e-mail

Para redefinir a senha por e-mail, clique no ícone dos três pontinhos do usuário a ser gerenciado e selecione a opção **Redefinir senha por e-mail**. Na janela **Confirmação**, clique no ícone **Sim**. O alerta será exibido **E-mail de redefinição de senha enviado**.



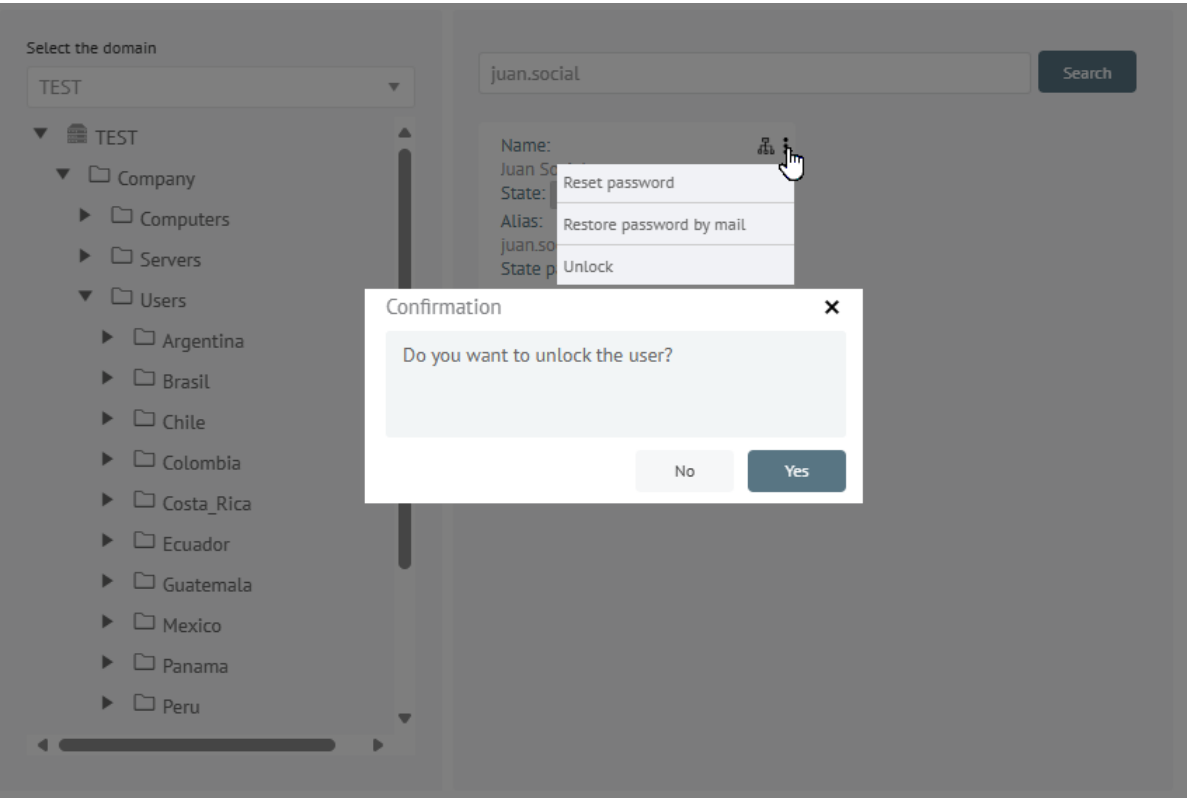
O aplicativo agendará o envio de um e-mail com um link que inclui um [Token de acesso único](#), isso permitirá que o usuário inicie o autogerenciamento de redefinição de senha. O e-mail será enviado para o endereço principal e para o endereço de correspondência alternativo registrado. Se a opção estiver ativada *Criação de caso*, um caso será gerado automaticamente em ASDK de acordo com as configurações definidas.

🚩 **Anotações:**

- Se o usuário já tiver perguntas configuradas, o aplicativo solicitará que ele preencha essas respostas.
- Se o usuário não tiver perguntas configuradas, o aplicativo solicitará que ele preencha as perguntas de segurança.
- Caso o usuário não se lembre das respostas, é recomendável limpar as perguntas da opção *Configuração* > *seção Usuários*.
- A função *Redefinir senha por e-mail* depende da configuração correta do servidor SMTP. Verifique se ele está ativado e acessível a partir do servidor de aplicativos.
- Se o usuário não receber o e-mail de restauração, verifique se ele tem um endereço principal ou alternativo válido.

Desbloqueio (quando aplicável)

Para desbloquear um usuário que está bloqueado no **Active Directory (AD)**, clique no ícone de três pontos do usuário bloqueado e selecione a opção *Desbloquear*. Na janela *Confirmação*, clique no ícone *Sim*. O alerta será exibido **O usuário está desbloqueado**.



🚩 **Nota:**

- Essa opção é habilitada somente quando o usuário está efetivamente bloqueado no Active

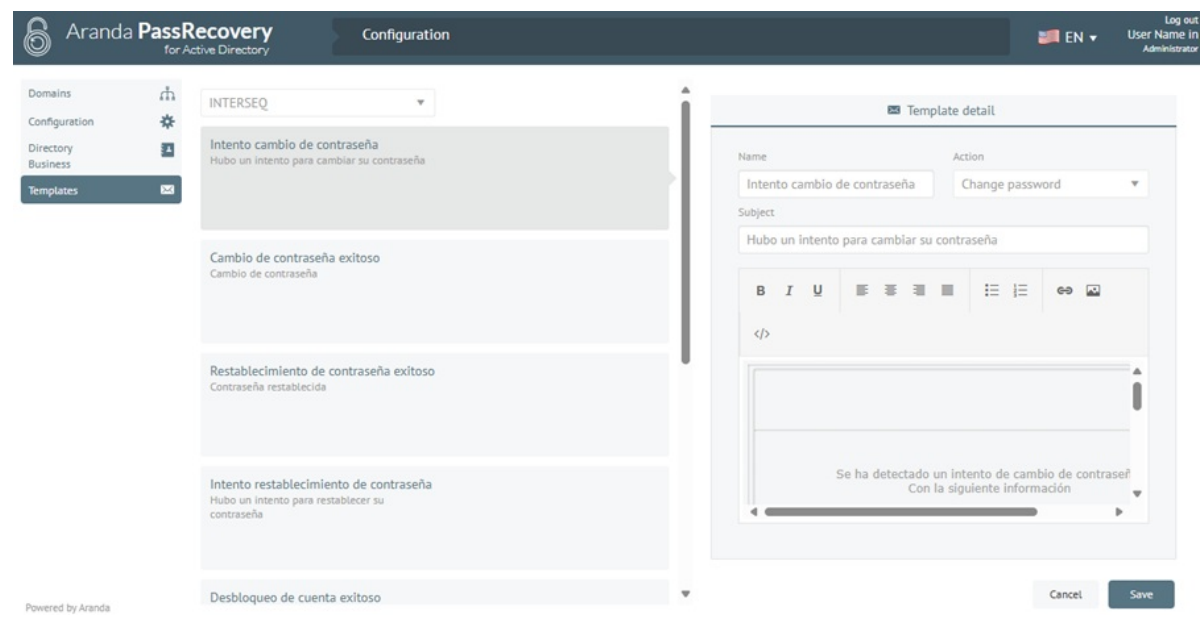
Modelos

Ao entrar no Admin Console (APRAdmin), no **Modelos**, o administrador poderá personalizar os modelos disponíveis para os diferentes comportamentos, de acordo com a necessidade de cada domínio configurado.

📌 **Anotações:**

- Não é possível adicionar ou remover modelos.
- Eles sempre serão exibidos em espanhol, só é possível personalizar o corpo da mensagem.

Uma vez feitas as modificações necessárias, clique no botão **Salvar** para aplicar as alterações.



Console do usuário (APRUsers)

Usar o console do usuário

Ao entrar no console do usuário (APRUsers) de **Passe de ArandaRecuperação**, o usuário poderá acessar três funcionalidades específicas, desde que previamente habilitadas no **Diretório ativo**:

1. [Desbloquear conta](#)
2. [Redefinir senha](#)
3. [Alterar senha](#)

Para aceder a estas funcionalidades, a aplicação utiliza um método de autenticação baseado na validação de [Perguntas de segurança](#). Essas perguntas devem ter sido configuradas anteriormente pelo usuário no mesmo console.

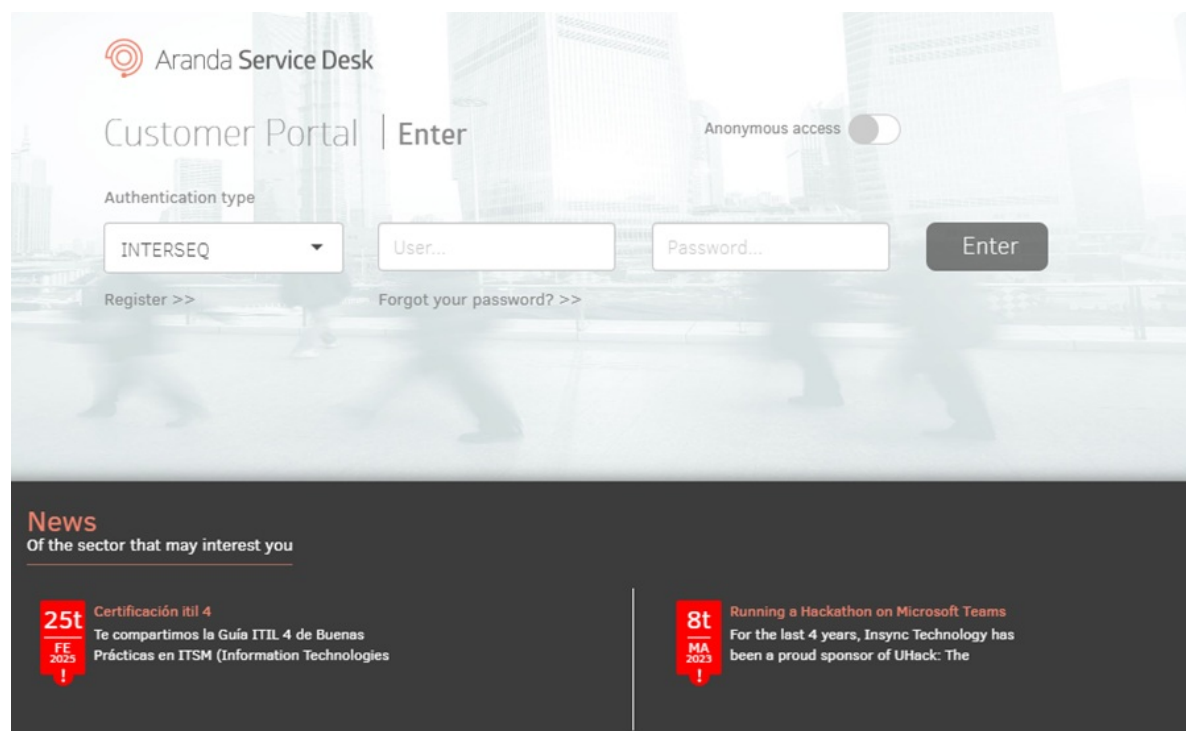
Configurando perguntas de segurança

Como parte do processo de configuração, o usuário final deve registrar as perguntas e respostas de segurança que deseja associar à sua identidade. O número mínimo de perguntas necessárias para autenticação é predefinido pelo administrador no console de administração.

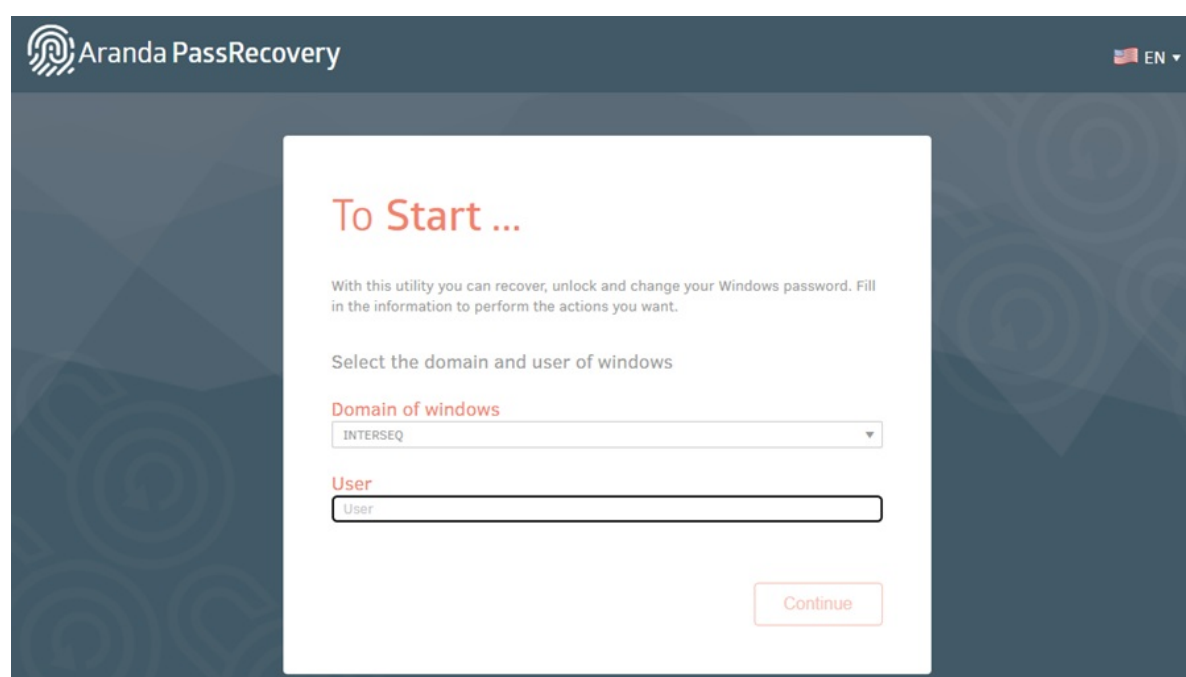
Essas perguntas serão configuradas apenas uma vez – ou novamente se o administrador as excluir ou modificar a quantidade necessária – e são solicitadas no primeiro login do usuário na ferramenta **Passe de ArandaRecuperação**.

Para realizar essa configuração, siga estas etapas:

1. Faça login no Console do Usuário do ASDK 'https://{domain}/USDKV8/', selecione o domínio com o qual deseja autenticar e clique no ícone **Esqueceu sua senha?**.

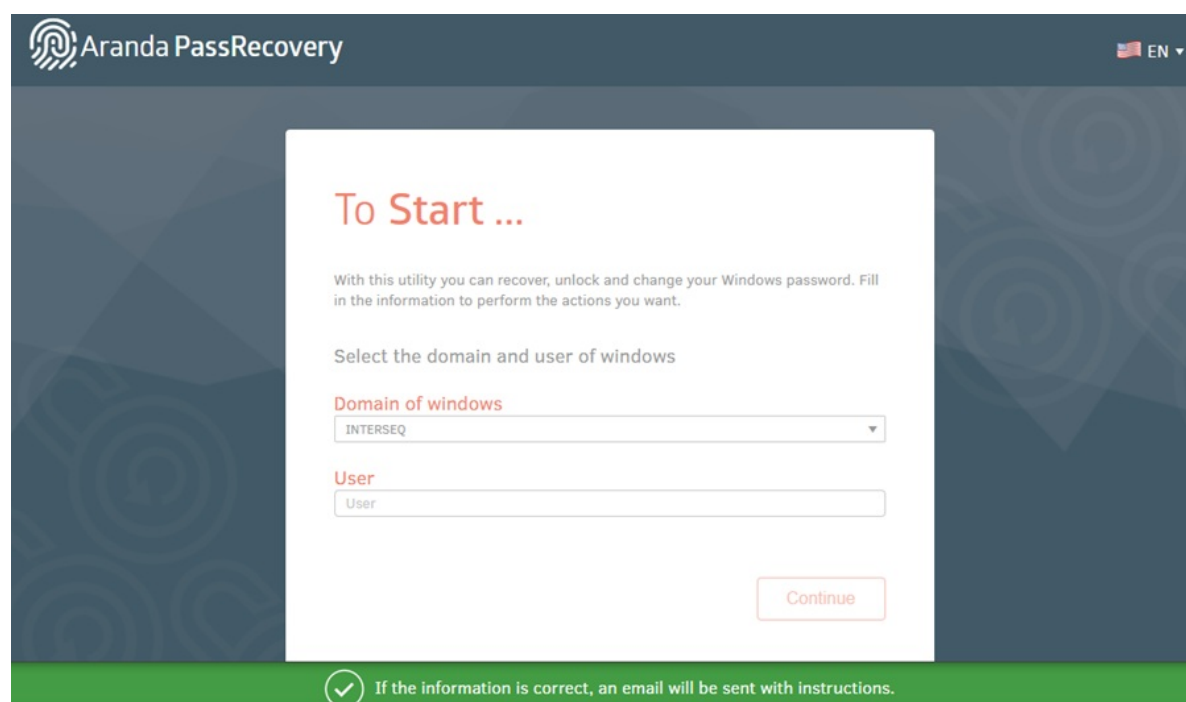


2. O Passe de ArandaRecuperação em uma nova guia. Digite seu nome de usuário e clique no botão Continuar.



3. Independentemente de o usuário estar ou não associado ao autoatendimento e de existir ou não no Active Directory, a seguinte mensagem será exibida:

“Se as informações estiverem corretas, um e-mail será enviado com instruções.”

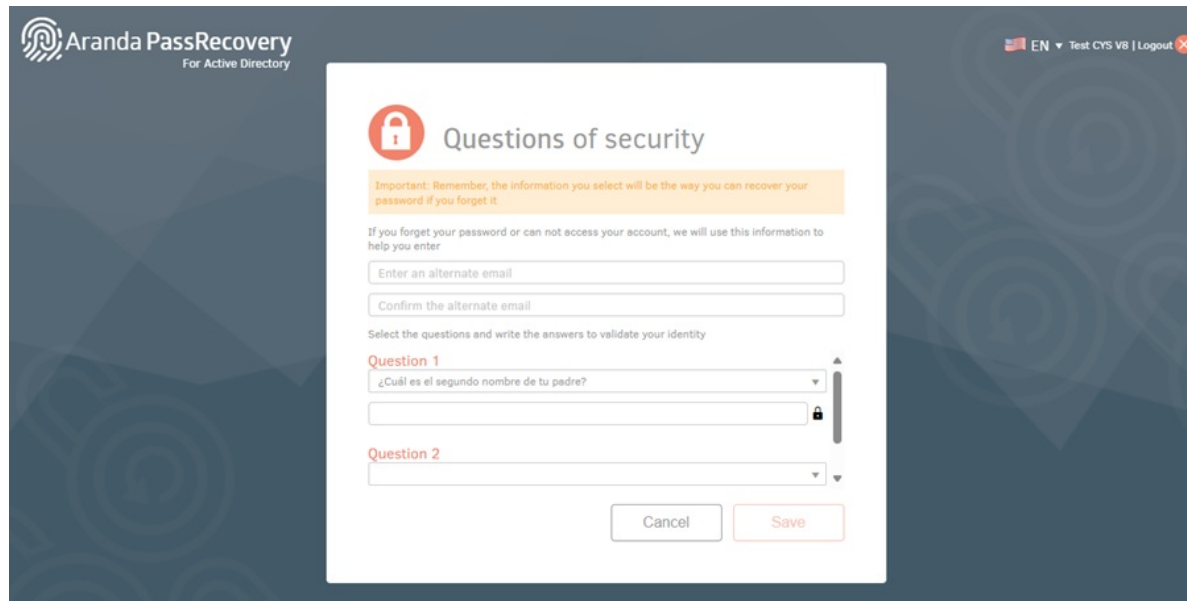


4. O aplicativo validará as configurações correspondentes e, se os critérios forem atendidos, agendará um e-mail para ser enviado usando o modelo **Redefinição de senha**. Este e-mail incluirá um link para um [Token de acesso único](#) o que permitirá ao usuário continuar com o gerenciamento. O email será enviado para o endereço principal ou alternativo registrado no banco de dados do ASDK.

📌 Anotações:

- O envio de e-mails depende da configuração correta do servidor SMTP. Verifique se ele está ativado e acessível a partir do servidor de aplicativos.
- Se o usuário não receber o e-mail, verifique se ele tem um endereço principal ou alternativo registrado e se ele está associado ao autoatendimento no Admin Console.
- O tempo de vida do token de acesso é definido no Admin Console, na página **Tempo de validade do token**, dentro do **Configuração**.

5. Assim que o usuário acessar o link recebido, ele será redirecionado para o formulário **Perguntas de segurança**, onde você pode registrar (ou atualizar) um e-mail alternativo e preencher as respostas às perguntas selecionadas.

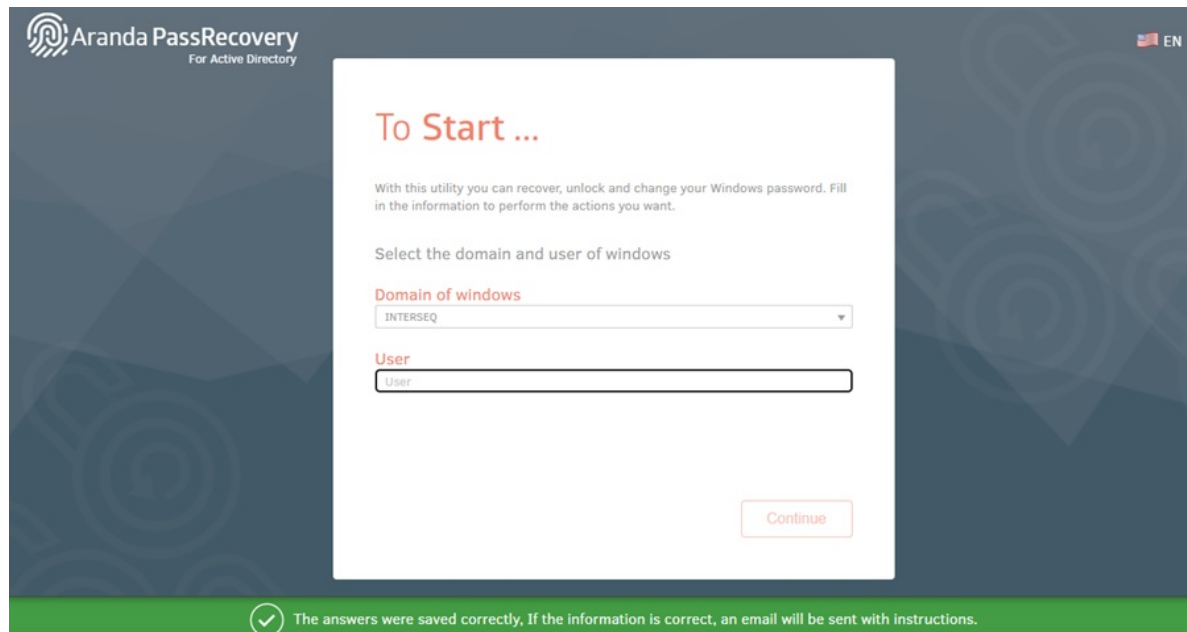


📌 Anotações:

- Caso o usuário já tenha dúvidas cadastradas, deverá respondê-las ao entrar no link. Se você quiser alterá-los, precisará solicitar ao administrador para removê-los do **Passe de ArandaRecuperação**.
- Se o usuário entrar com um token expirado ou já usado, o alerta será exibido: **Erro de validação de token**.

6. Depois de preencher as informações necessárias, clique no botão **Salvar**. O alerta será exibido: **“As respostas foram configuradas corretamente. Se as informações estiverem corretas, um e-mail será enviado com as instruções.”**

Caso contrário, valide a configuração e tente novamente.



📌 Nota:

- Configure um **Correio alternativo** Isso permitirá que o usuário recupere sua senha, mesmo que não consiga acessar seu e-mail principal.

7. O aplicativo agendará o envio de um novo e-mail usando o **Redefinição de senha**, com um link que inclui um [Token de acesso único](#). O e-mail será enviado para os endereços principal e alternativo registrados. 📌 **Nota:**

- Se ambos os endereços de e-mail (principal e alternativo) forem iguais, apenas um e-mail será enviado.

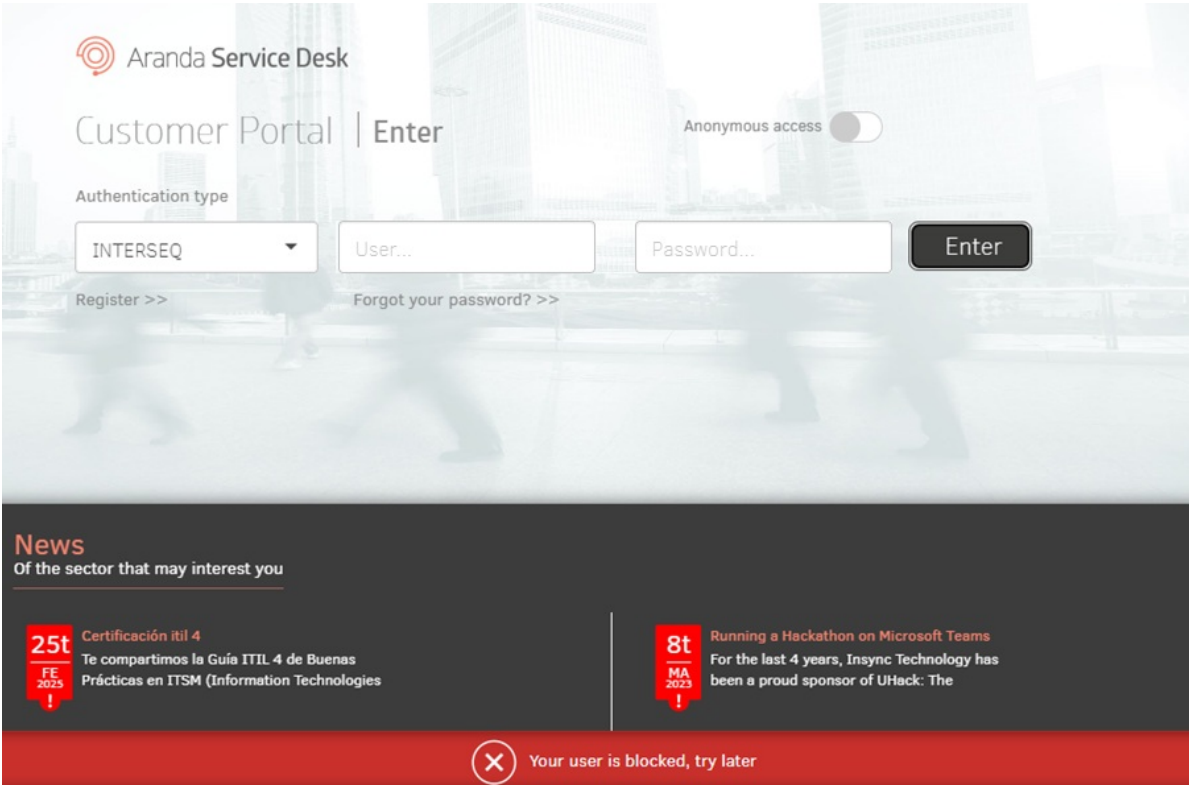
Desbloquear conta

Se o usuário bloquear sua conta depois de inserir uma senha inválida várias vezes, ele poderá executar o processo de desbloqueio no **Passe de ArandaRecuperação**.

⚠ **Aviso:** É obrigatório ter configurado previamente [Perguntas de segurança](#).

Etapas para desbloquear a conta

1. Faça login no Console do Usuário do ASDK 'https://{domain}/USDKV8/', selecione o domínio apropriado e clique no ícone **Esqueceu sua senha?**.



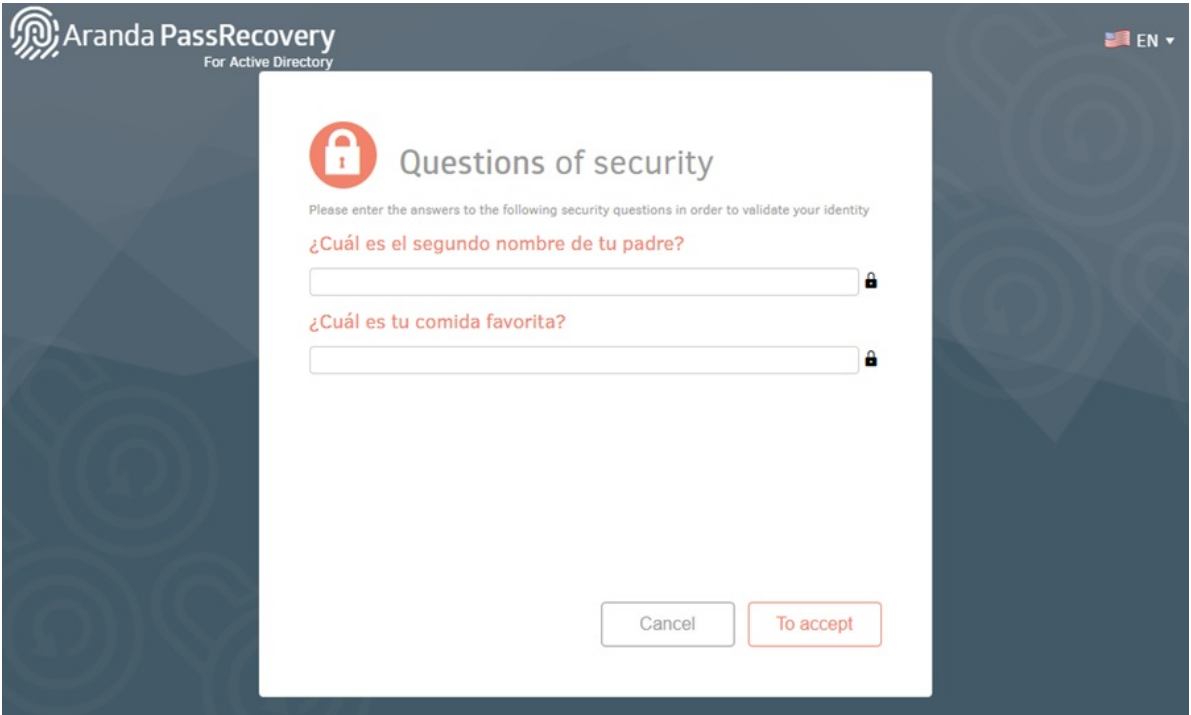
2. O **Passe de ArandaRecuperação** em uma nova guia. Digite seu nome de usuário e clique no botão **Continuar** para agendar o envio do e-mail que permitirá que você gerencie o desbloqueio de sua conta.

3. Digite o link recebido no e-mail. Você será redirecionado para o formulário **Perguntas de segurança**, onde você precisará responder às perguntas pré-configuradas.

📌 **Anotações:**

- Se o usuário entrar com um token expirado ou já usado, o alerta será exibido: **Erro de validação de token**.

4. Preencha as respostas e clique no botão **Aceitar**. O console validará as respostas inseridas e, se corretas, redirecionará o usuário para a janela **O que você quer fazer** onde permitirá que você desbloqueie a conta.

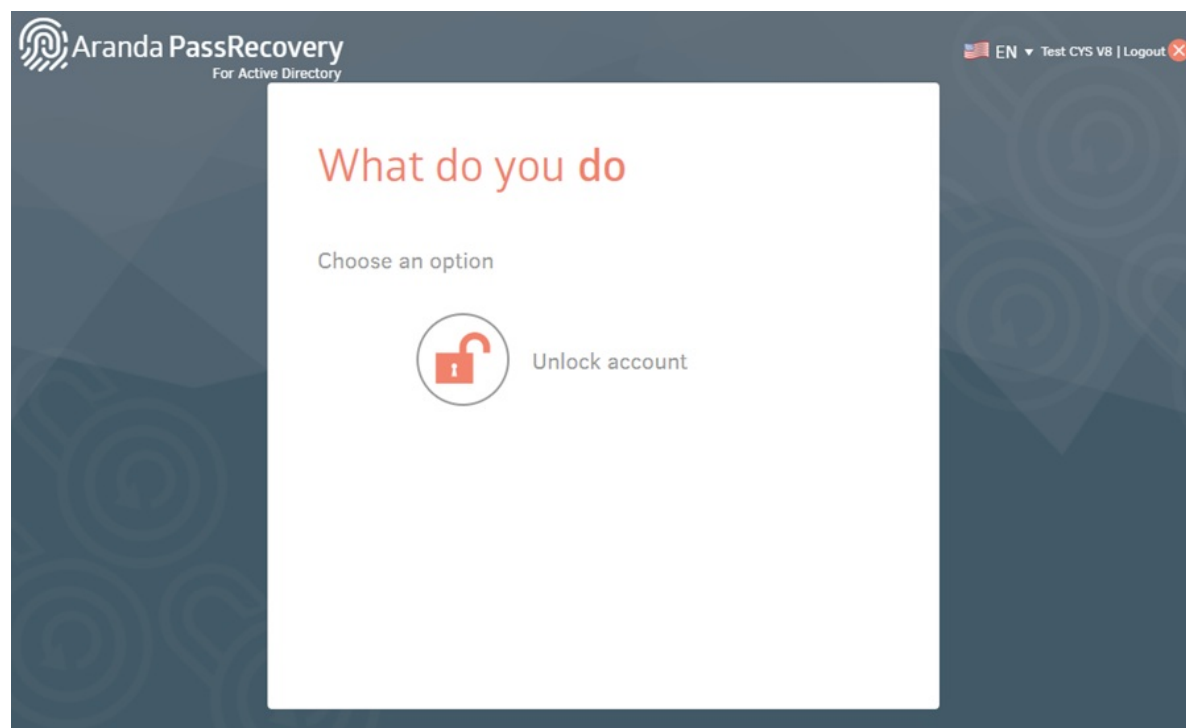


📌 **Anotações:**

- Se o usuário responder a uma ou mais perguntas incorretamente, o alerta será exibido: **Respostas incorretas**.
- Se o número de tentativas definido no campo Admin Console (**Número de tentativas**seção **Configuração**), o alerta será exibido: **Tentativas excedidas, tente novamente em X min**.

- Se um usuário bloqueado por tentativas fracassadas tentar fazer login com um token válido, o alerta será exibido: **Usuário bloqueado, tente novamente em X min.**

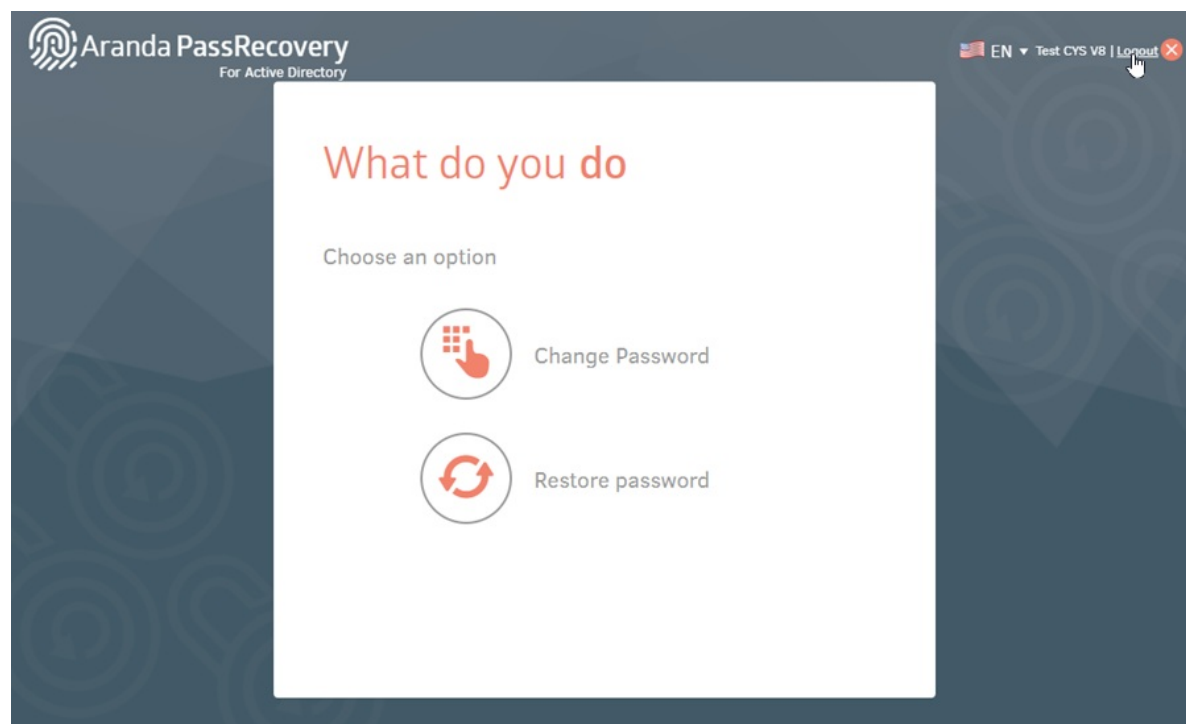
5. Clique no botão **Desbloquear conta**. O aplicativo enviará a solicitação ao Active Directory para remover o bloqueio da conta, exibindo a seguinte mensagem: **A conta foi desbloqueada**.



Após desbloquear a conta, o usuário poderá realizar as seguintes ações:

- [Redefinir senha](#)
- [Alterar senha](#), quando aplicável.

Se você não deseja realizar nenhuma ação adicional, faça logout clicando no botão **Fazer logoff**.



6. Se o **Criação de caso**, um caso ASDK será gerado automaticamente no nome do usuário que executou o desbloqueio.

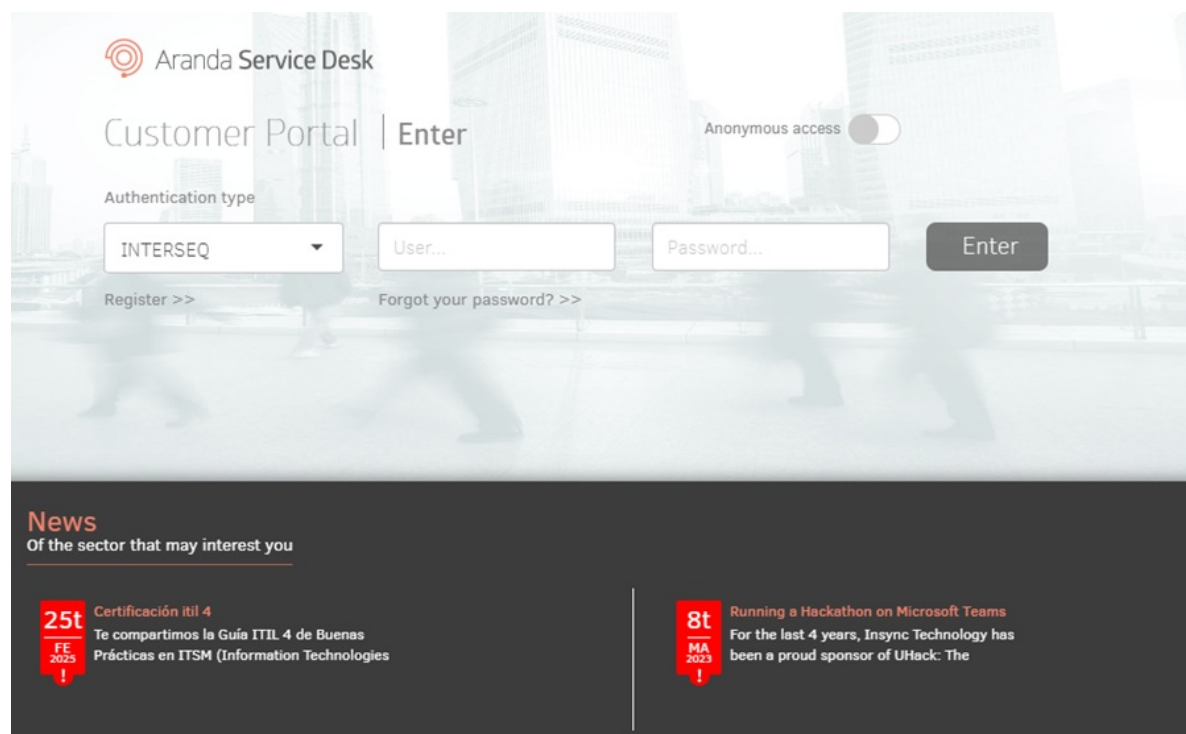
Redefinir senha

Se um usuário esquecer sua senha, ele poderá executar o processo de redefinição no console do usuário. **Passe de ArandaRecuperação**.

⚠ **Aviso:** É obrigatório ter configurado previamente [Perguntas de segurança](#).

Etapas para redefinir sua senha

1. Faça login no Console do Usuário do ASDK 'https://{domain}/USDKV8/', selecione o domínio apropriado e clique no ícone **Esqueceu sua senha?**.

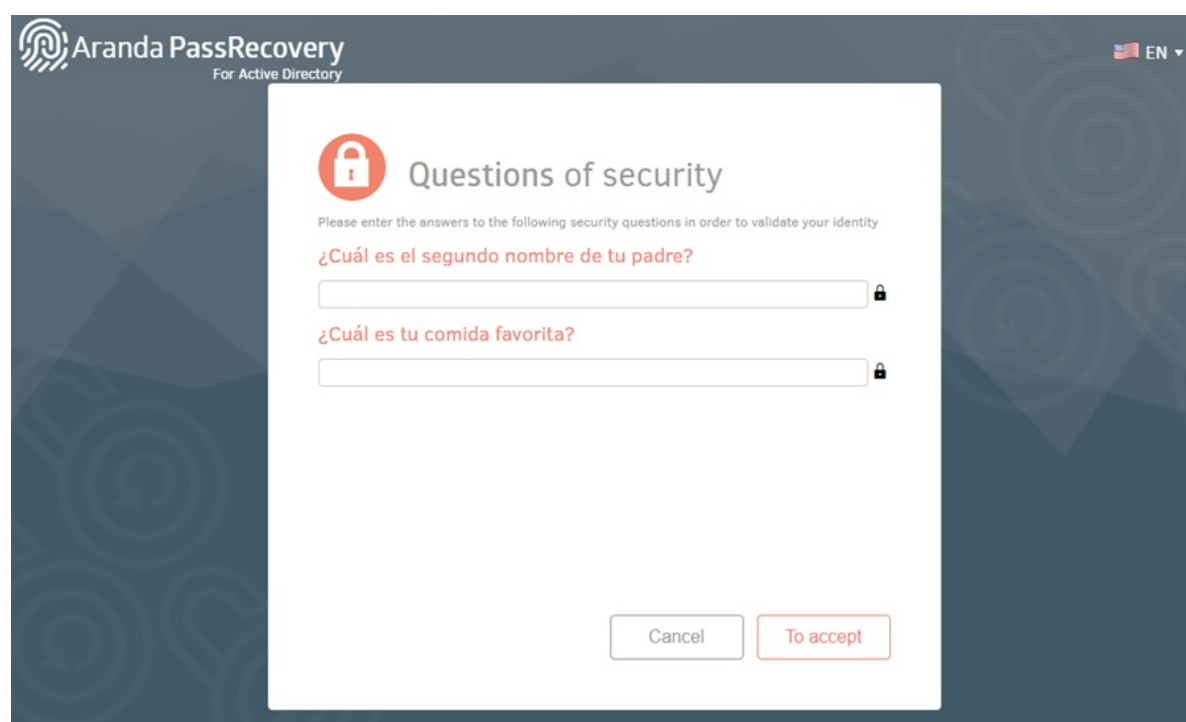


2. O **Passe de ArandaRecuperação** em uma nova guia. Digite seu nome de usuário e clique no botão **Continuar** para agendar o envio do e-mail que permitirá gerenciar a redefinição de senha.
3. Digite o link recebido no e-mail. Você será redirecionado para o formulário **Perguntas de segurança**, onde você precisará responder às perguntas pré-configuradas.

📌 **Anotações:**

- Se o usuário entrar com um token expirado ou já usado, o alerta será exibido: **Erro de validação de token**.

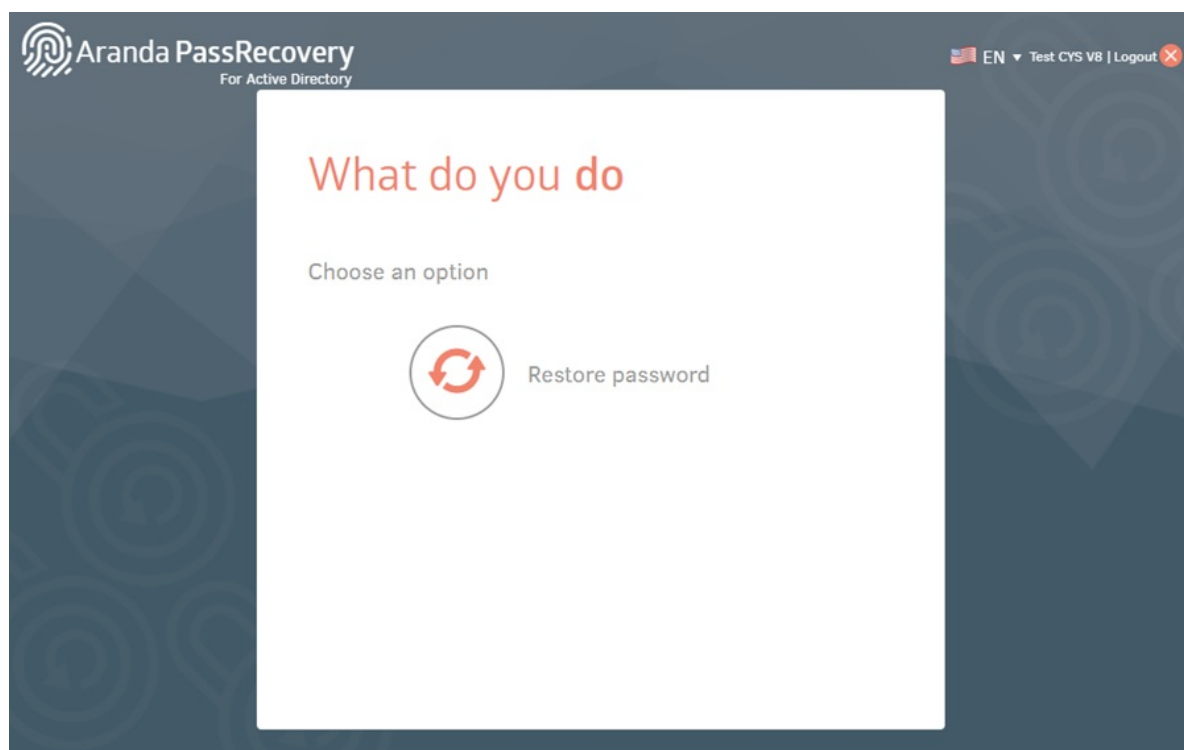
4. Preencha as respostas e clique no botão **Aceitar**. O aplicativo validará as respostas inseridas e, se estiverem corretas, redirecionará o usuário para a janela **O que você deseja fazer?**, onde você pode selecionar a opção para redefinir sua senha.



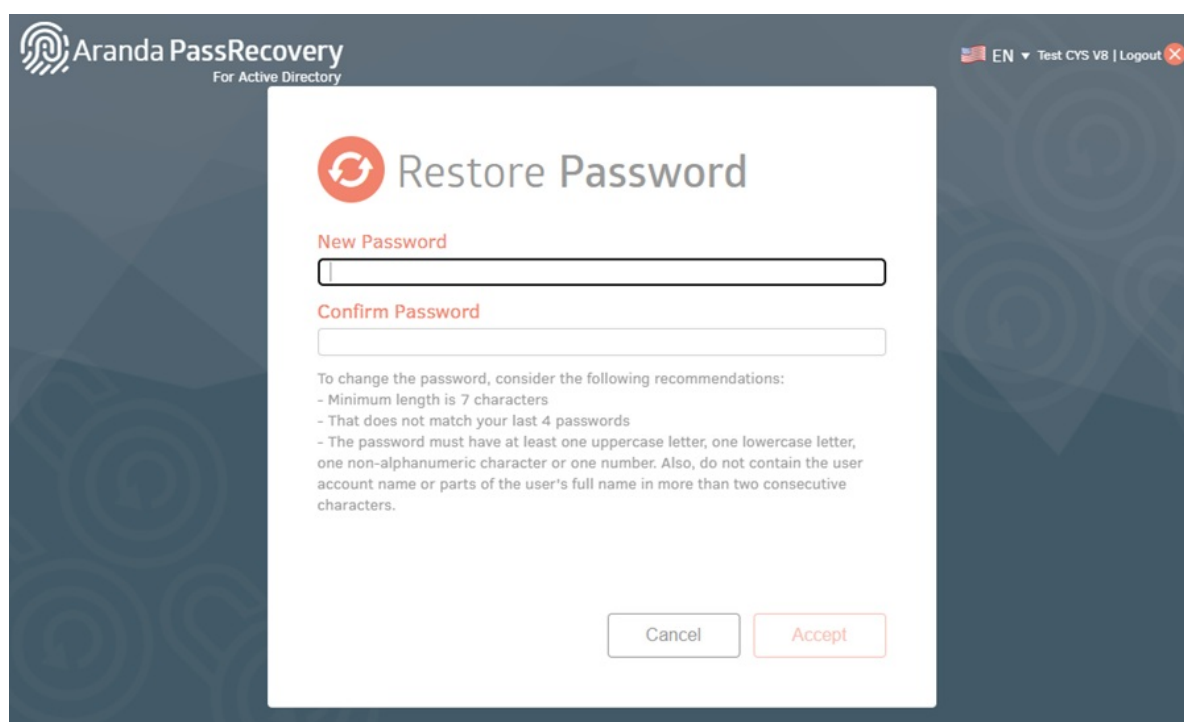
📌 **Anotações:**

- Se o usuário responder a uma ou mais perguntas incorretamente, o alerta será exibido: **Respostas incorretas**.
- Se o número de tentativas definido no campo Admin Console (**Número de tentativas** seção **Configuração**), o alerta será exibido: **Tentativas excedidas, tente novamente em X min**.
- Se um usuário bloqueado por tentativas fracassadas tentar fazer login com um token válido, o alerta será exibido: **Usuário bloqueado, tente novamente em X min**.

5. Na janela **O que você deseja fazer?**, clique no ícone **Redefinir senha** para iniciar o gerenciamento.



6. Na janela **Redefinir senha**, o console solicitará que você insira uma nova senha e confirme-a. Preencha os campos obrigatórios e clique no botão **Aceitar**. Na parte inferior, as políticas de senha definidas no Active Directory serão exibidas.



7. Se a ação for bem-sucedida, o aplicativo exibirá o alerta: **Senha atualizada**. Caso contrário, valide as informações inseridas e tente novamente.
8. Se o **Criação de caso**, um caso ASDK será gerado automaticamente no nome do usuário que executou a redefinição.

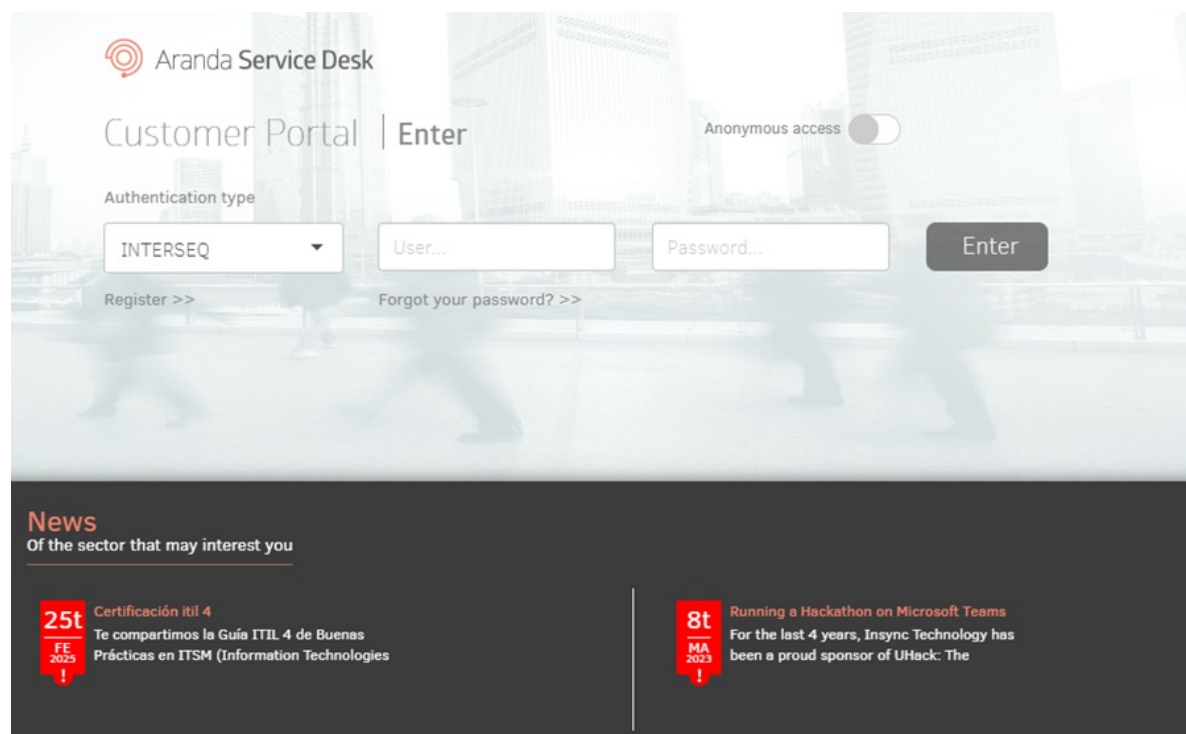
Alterar senha

Alterando sua senha no Console do Usuário **Passe de ArandaRecuperação** Ele estará disponível quando a senha estiver prestes a expirar. Se a senha foi alterada recentemente e o Active Directory (AD) tem políticas que definem um tempo mínimo para a alteração, o **Alterar senha** ele não será ativado.

⚠ **Aviso:** É obrigatório ter configurado previamente [Perguntas de segurança](#).

Etapas para alterar sua senha

1. Faça login no Console do Usuário do ASDK 'https://{domain}/USDKV8/', selecione o domínio apropriado e clique no ícone **Esqueceu sua senha?**.

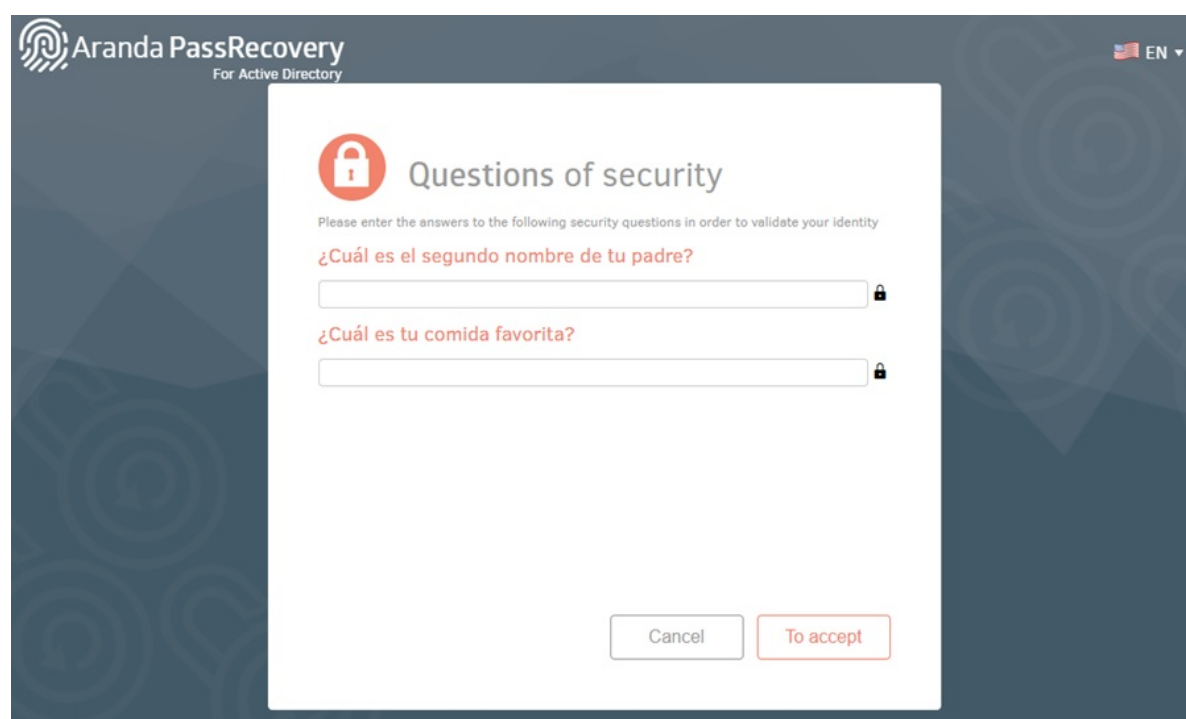


2. O **Passe de ArandaRecuperação** em uma nova guia. Digite seu nome de usuário e clique no botão **Continuar** para agendar o envio do e-mail que permitirá gerenciar a alteração da senha.
3. Digite o link recebido no e-mail. Você será redirecionado para o formulário **Perguntas de segurança**, onde você precisará responder às perguntas pré-configuradas.

📌 **Anotações:**

- Se o usuário entrar com um token expirado ou já usado, o alerta será exibido: **Erro de validação de token**.

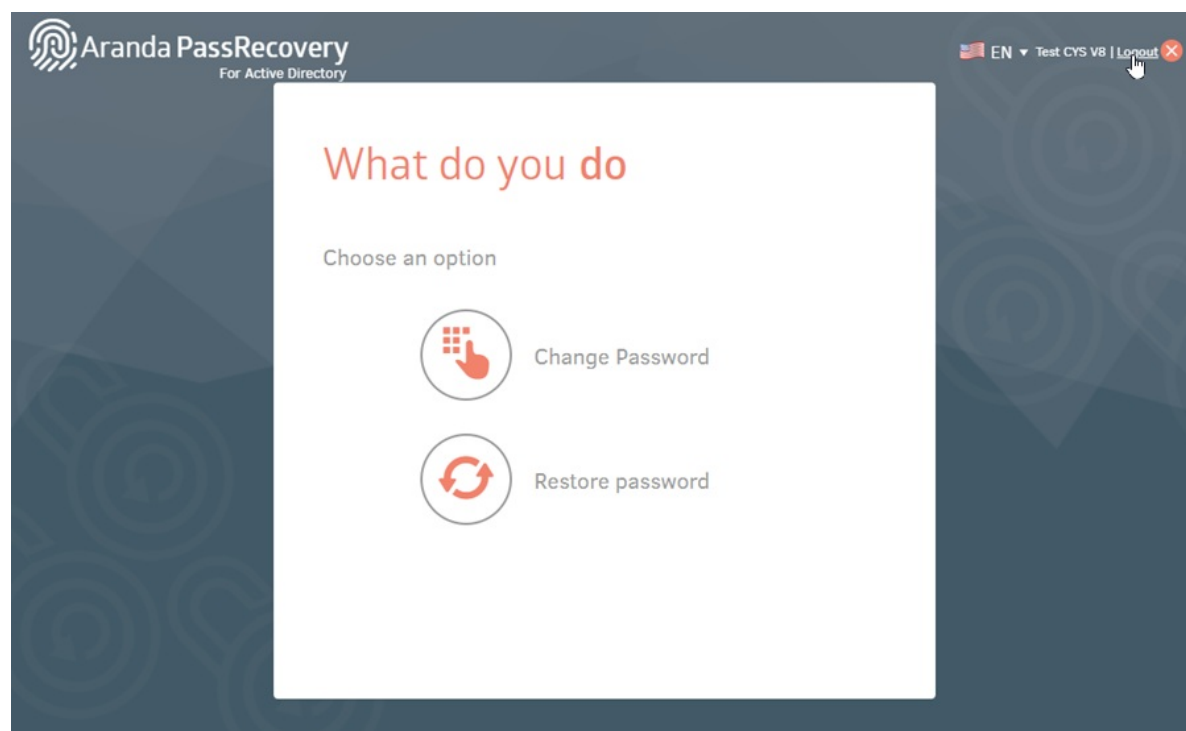
4. Preencha as respostas e clique no botão **Aceitar**. Se as respostas estiverem corretas, o aplicativo redirecionará o usuário para o **O que você deseja fazer?**, onde você pode selecionar a opção de alterar sua senha.



📌 **Anotações:**

- Se o usuário responder a uma ou mais perguntas incorretamente, o alerta será exibido: **Respostas incorretas**.
- Se o número de tentativas definido no campo Admin Console (**Número de tentativas** seção **Configuração**), o alerta será exibido: **Tentativas excedidas, tente novamente em X min**.
- Se um usuário bloqueado por tentativas fracassadas tentar fazer login com um token válido, o alerta será exibido: **Usuário bloqueado, tente novamente em X min**.

5. Na janela **O que você deseja fazer?**, clique no ícone **Alterar senha** para iniciar o processo.



6. Na janela **Alterar senha**, o console solicitará que você insira sua senha atual, nova senha e confirmação. Preencha os campos solicitados e clique no botão **Aceitar**. Na parte inferior, as políticas de senha definidas no Active Directory serão exibidas.

7. Se a ação for bem-sucedida, o aplicativo exibirá o alerta: **Senha atualizada**. Caso contrário, valide as informações inseridas e tente novamente.
8. Se o **Criação de caso**, um caso ASDK será gerado automaticamente no nome do usuário que fez a alteração.

Configuração de criação de caso

Este utilitário tem a função de criar casos automaticamente uma vez que qualquer uma das ações do aplicativo seja executada (Mudança de Chave, Restauração de Chave ou Desbloqueio de Conta). Para configurar a criação automática de casos a partir do utilitário, siga estas etapas:

- Os modelos devem ser criados para ações agendadas no BASDK em Configurações/Modelo, de acordo com os tipos de casos a serem criados.

- Adicionando ações em ações agendadas, uma vez configurados os modelos e a ação agendada, a ação deve ser adicionada, caso em que seria: **Tipo de Ação:** Criação de caso. **Modelo:** Seleccione o modelo que foi configurado para a criação de casos de utilitários. **Número de casos:** 1(Neste caso, deve ser um para que apenas um caso seja criado para cada ação).

Com essa configuração, quando você executa ações de **Passe de ArandaRecuperação** casos são criados automaticamente no ASDK.

Fluxograma Aranda PassRecovery

