



Aranda Password Recovery

This guide details the steps required for the installation, configuration, and use of **Aranda PassRecovery V8 (APR)**, which allows the management and recovery of the password of a registered user, taking into account a process of configuration and validation of security questions, for the unlocking of the domain account.

Defining a one-time token

During the processes, the application sends a unique link to the user’s registered emails (main - alternate). This link contains a **One-time token**, which has the following characteristics:

- The token is generated and sent by the application as part of the secure access link.
- Each token has a limited validity time, which is previously defined by the administrator in the **Configuration** in the Admin console.
- The token is considered **Used** in the following cases:
 - When the user clicks the **Save** when you finish setting up the security questions.
 - When the user correctly answers all security questions during the account unlocking, password change, or reset process.
- Once used or expired, the token cannot be reused. In case of trying to access again with an invalid token, the alert will be displayed: **Token validation error**.

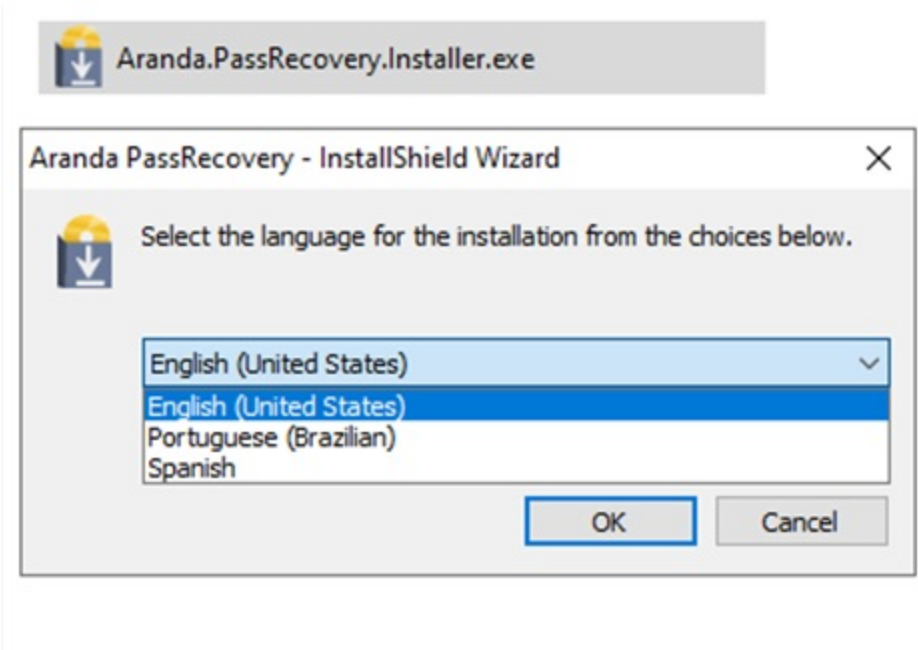
Aranda PassRecovery Installation

Aranda PassRecovery Installation

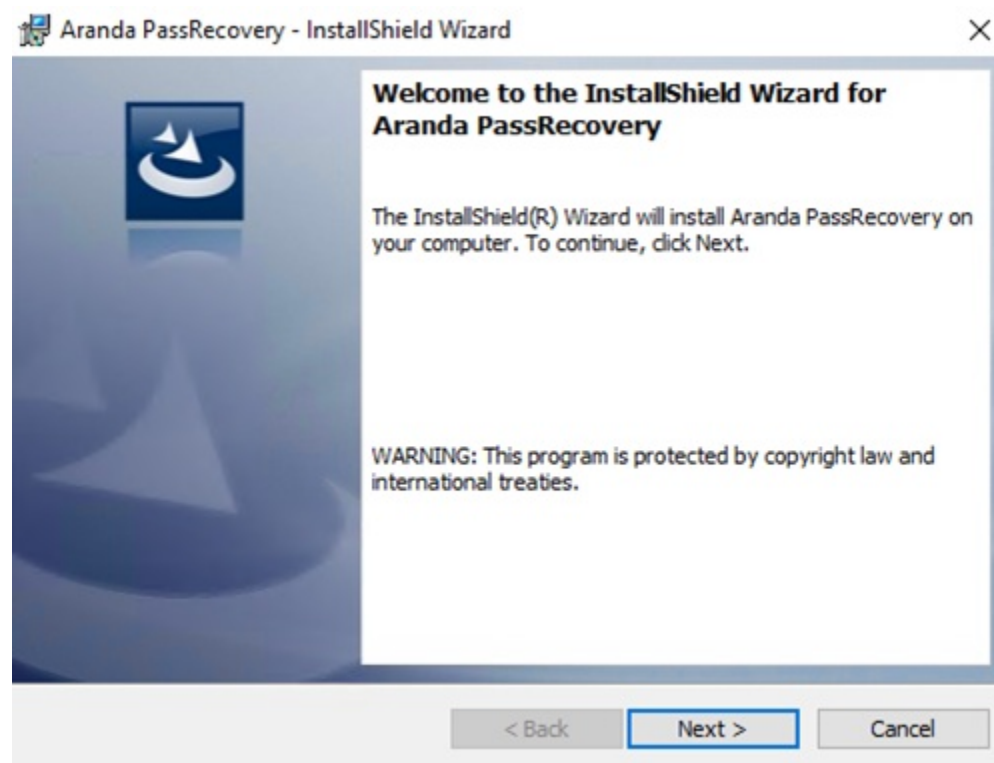
For this installation, it is important that the database is updated to the latest version of Aranda, with the minimum required version being the 8.0.89.

To install and configure the app, follow these steps:

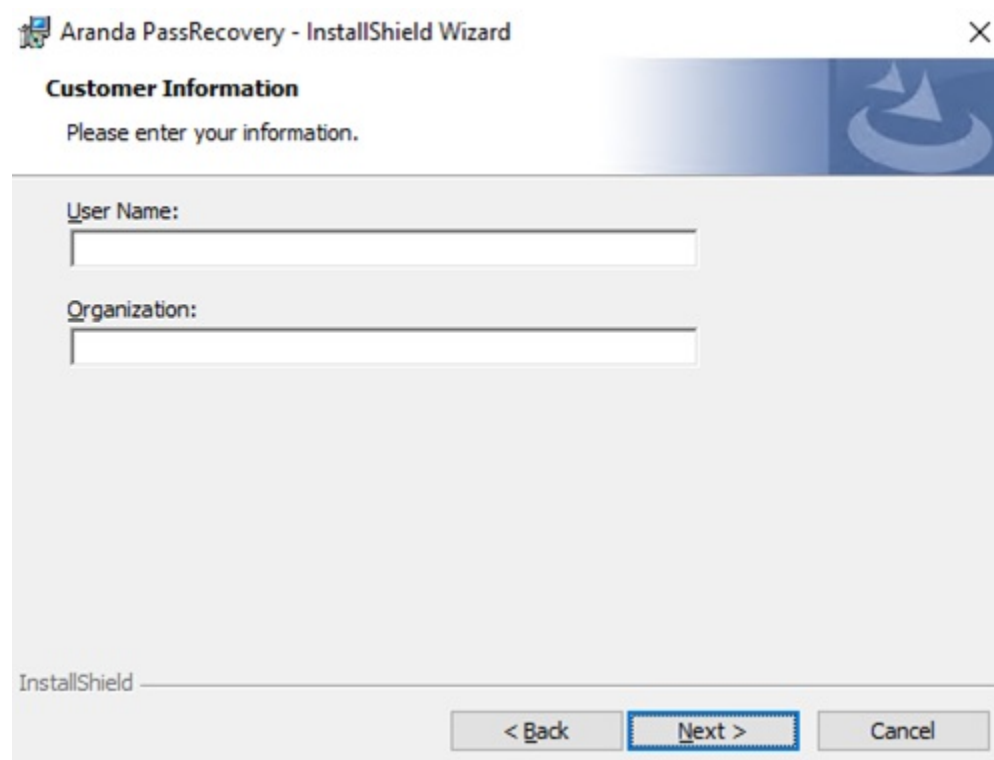
1. Run the file **Aranda.PassRecovery.Installer.exe**. The setup wizard will give you the option to select the installation language. Select the desired language and click the OK.



2. On the welcome screen, confirm the installation by clicking the **Following**.



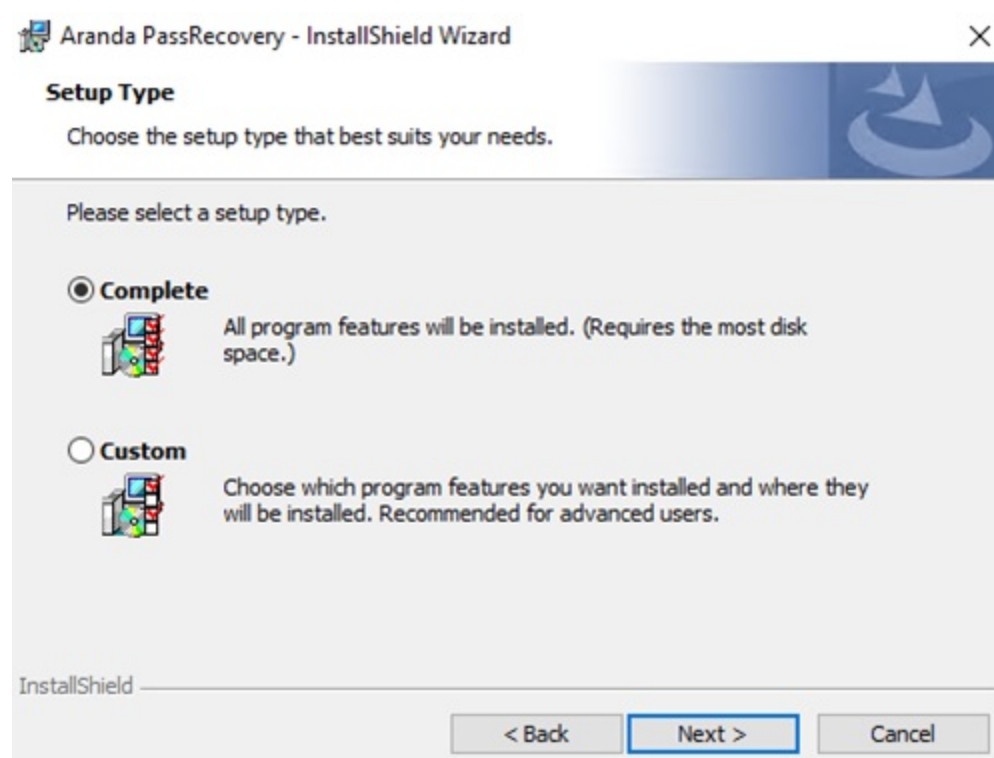
3. In the window Customer Information, enter the user name, organization, and click Following.

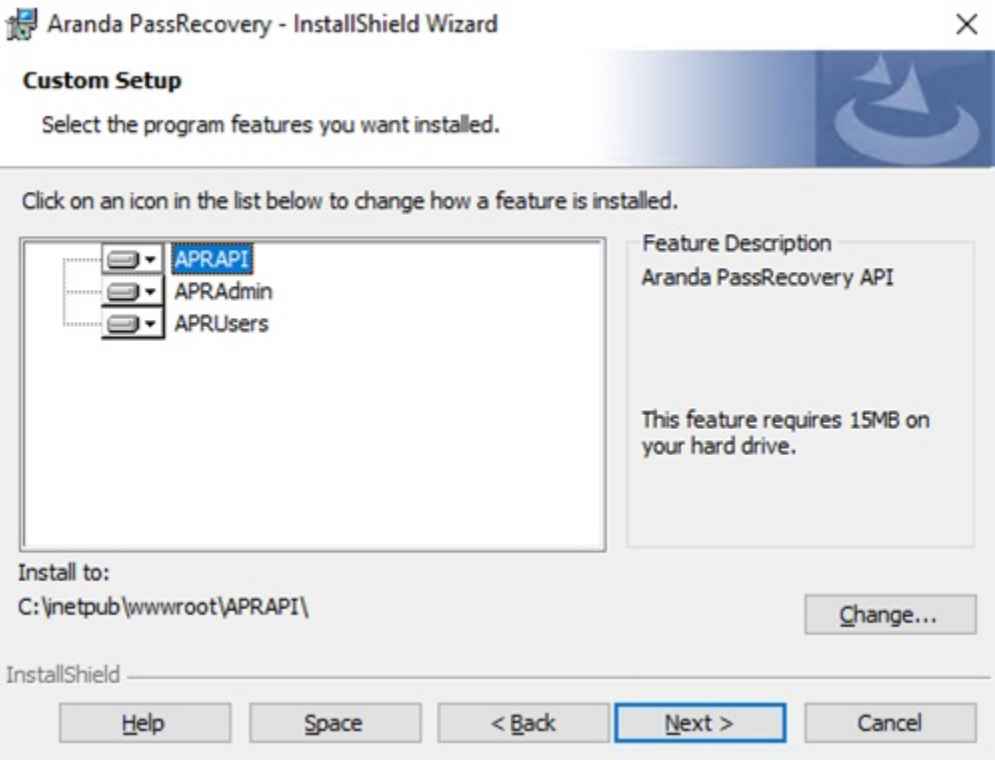


4. In the window Type of installation, you can configure the following options:

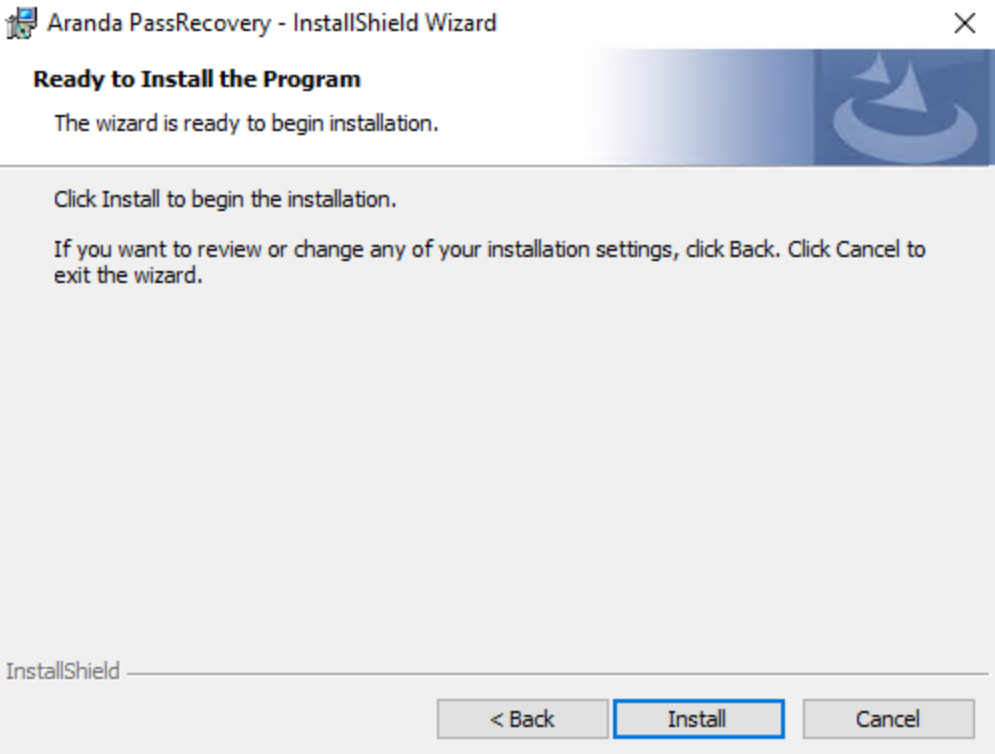
- **Complete**- All sites and services will be installed on the default routes.
- **Custom**- You can select the sites you want to install or change the installation path.

Select the option and click Following.





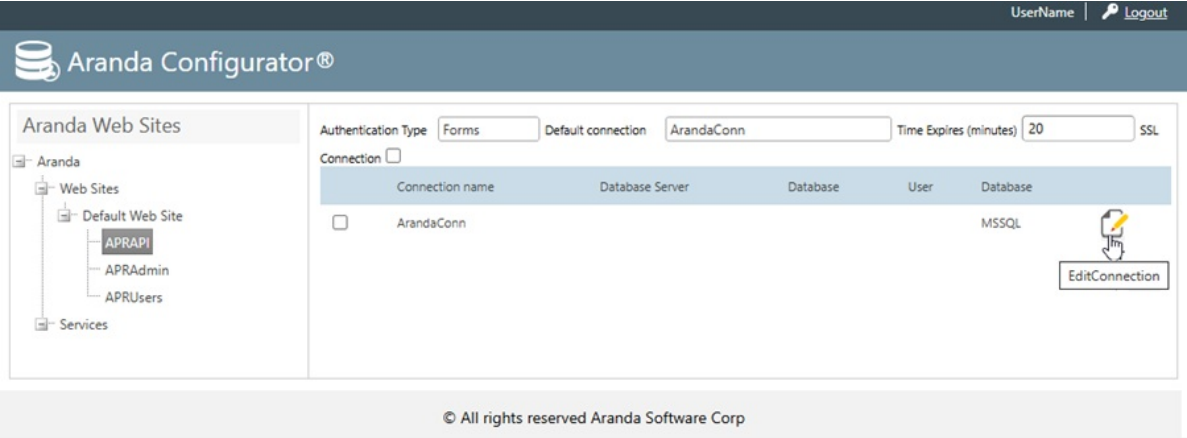
5. To start the installation process, click the Install.



6. At the end of the installation process, click on theEnd. Three websites will be installed in the IIS:APRAdmin, APRAPI and APRUsers.

Database configuration

7. Once the installation of Aranda PassRecovery, proceed to configure the connection strings to the database of the sites, entering the Aranda Configurator(AWCF). From the tree-type list, select the website(s) to configure.



8. Make the connection to the database and, in theAFW_SETTINGS, apply the following update commands (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;
```

📌 **Note:** Remember to replace Domain by the name or IP of your application server.

```
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	<input checked="" type="checkbox"/> https://domain/APRAPI/
7	URL consola de usuario	1	<input checked="" type="checkbox"/> https://domain/APRUsers/

Enable functionality and permissions

9. To assign permissions to groups and enable access to the Configuration ConsoleAranda PassRecovery (APRAAdmin), log in from the application server to the consoleAranda Profile. Select from the list of applications ARANDA PassRecovery and assign the corresponding permission(s), according to the business rules.

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	<input type="checkbox"/>
ACCESS THE DIRECTORY MENU	<input type="checkbox"/>
ACCESS THE DOMAINS MENU	<input type="checkbox"/>
ACCESS THE TEMPLATES MENU	<input type="checkbox"/>
EXECUTE APPLICATION	<input type="checkbox"/>

10. In the Web Configuration Console (BASDK), configure the path by going to Options > Summary, and in the field URL de PassRecovery Enter 'https://{domain}/APRUsers/'. Remember to replace Domain by the name or IP of your application server.

Aranda SERVICE DESK Configuración

User Name in Session 06/06/2025 7:45:41 p.m. Start Summary

Service Desk IT Service Desk IT

General parameters setup

Summary

Attach files to cases

File server address

Max. size of attached files (MB)

Internationalization

Select the language for system notifications

Spanish English Portuguese

Format for dates

Send satisfaction survey link

Web server name

Register Case

Enable service filter case creation

Enable filter customer-company in creating cases

License time to expire

Time due for license to expire (mins)

Remote Control

Uri Control Remote

Specific options

Hide Aranda's Login

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

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

Hide send mail option

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

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

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

Statistics

Number of existing actions : 0

Number of existing categories : 461

Number of existing rules : 31

Default Record Type - Specialist Console

Service Requests

Mail

Problems

Mail

Incidents

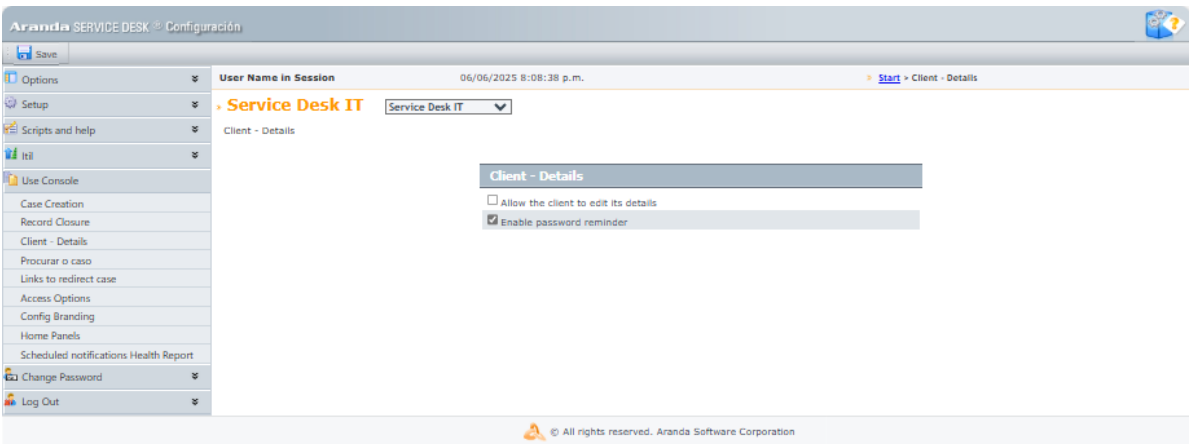
Mail

Changes

Mail

© All rights reserved. Aranda Software Corporation

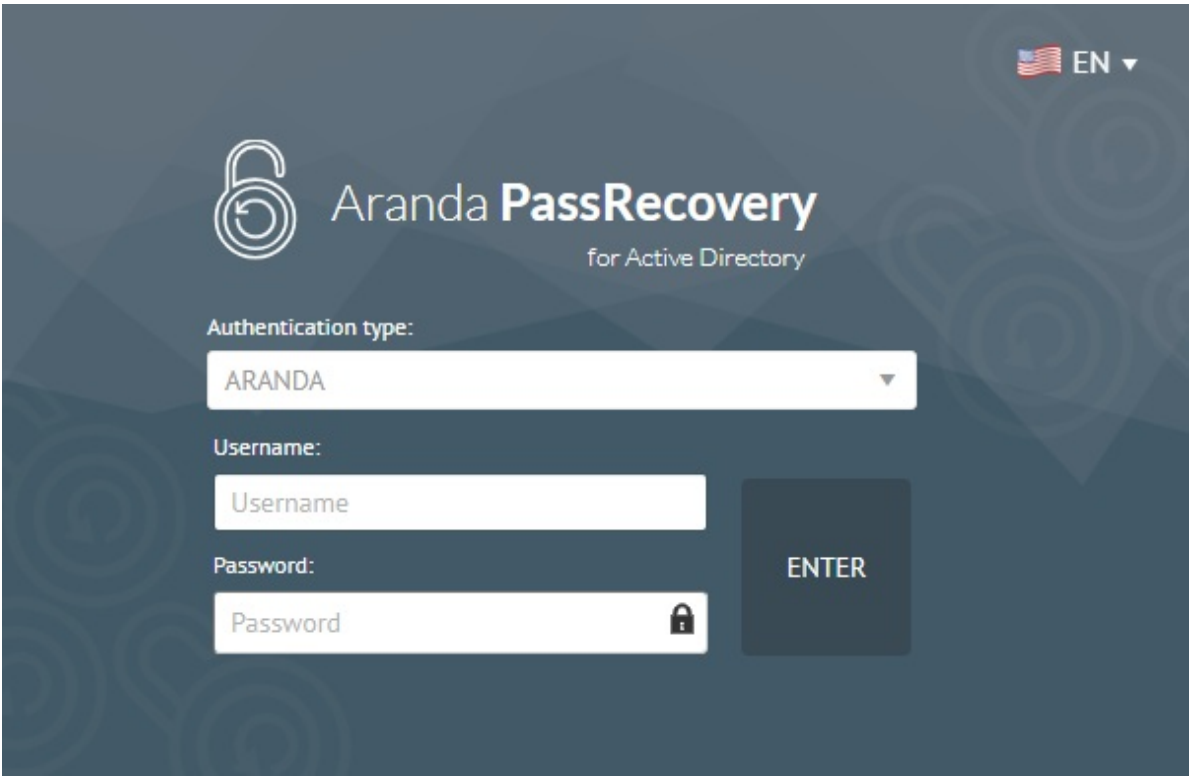
11. To enable password recovery for domain users from the web console USDKV8, enter BASDK > User Console > Client Details and enable the Enable password reminder.



Admin Console (APRAdmin)

Login

To log in to the Aranda PassRecovery, the user must belong to a group with access permissions to the app. The access URL is: 'https://{domain}/APRAdmin/'



Domains

Domain Settings

Domains present in the Admin console (APRAdmin) must be pre-configured in Aranda Profile, in the Configuration > Authentication Type.

When you log in to the Admin console, the preconfigured domains will automatically be listed in the **Domains**. In the **Overview**, you can complete or update the domain details as needed.

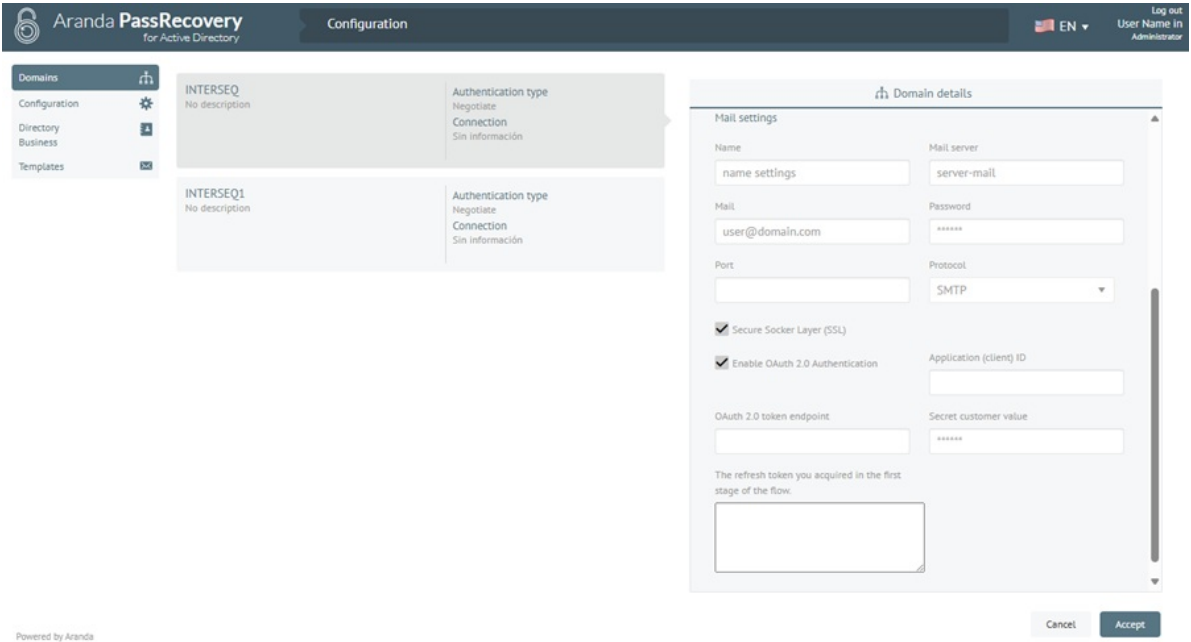
ⓘ **Note:** It is important to configure a domain user with sufficient privileges, who has the “Reset user passwords and force password change” permission enabled at the level of the GIVES (Active Directory). If this condition is not met, the actions executed will not be applied.

Mail Settings

In the **Mail Settings**, you can set up two types of authentication (**Basic** and **OAuth 2.0**) for sending mail. Fill in the requested information according to the desired configuration.

When you enable field check **Enable OAuth 2.0 authentication**, fill in the corresponding data, as indicated in the following document:

[OAuth Modern Authentication Settings](#)



When the setup is complete, click the **Accept**. If everything has been set up correctly, the alert will be displayed **Updated domain**. If not, validate the configuration and try again.

Configuration

When entering the Admin console (APRAdmin), in the **Configuration**, the administrator will be able to make the following settings:

Options to configure

In this section, the administrator can define, for each configured domain, the following options:

Field	Description
Number of questions	It allows you to configure the number of questions that the user must answer. The value can be between 1 and 15. The questions are predefined and can be viewed in the Security Questions .
Token validity time	It allows you to set the token duration time in minutes. Allowed value between 1 and 60.
Block app	It allows you to configure the time in minutes during which the application will crash after the user exceeds the number of attempts to answer the questions. Allowed value between 1 and 60.
Number of attempts	It allows you to define the number of attempts available for the user to answer the questions. Allowed value between 1 and 10.
Case creation	Enables case creation to be triggered in ASDK when a password recovery or change is requested. View Case Creation Settings
Domain Policy Validation	Enables domain policy validations for password change in the User Console.

The screenshot shows the 'Configuration' page for 'Aranda PassRecovery for Active Directory'. The left sidebar has 'Configuration' selected. The main area is divided into two panes. The left pane, 'Options to configure', contains fields for 'Domain' (INTERSEQ), 'Number of questions*' (with a description and input field), 'Token validity time*' (with a description and input field), 'Block application*' (with a description and input field), 'Number of attempts*' (with a description and input field), 'Creation of cases' (with a checked checkbox and description), and 'Domain policy validation' (with an unchecked checkbox and description). The right pane, 'Security questions', shows a list of 7 questions in Spanish. At the bottom right are 'Cancel' and 'Save' buttons.

Notes:

- Fields marked with (*) are mandatory.
- For the countryside **Number of questions**, if its value is changed and there are users who already have Q&A registered in the console (APRUsers), these records will be automatically deleted when the new configured value is applied.
- For application lock to work properly, the application and database servers must have the date and time synchronized, as well as the accessing user's computer.

Users

In this section, the administrator will be able to define the users who will be allowed to self-service (Account Unlock, Change, and Password Reset) in the Business Directory. You can manually associate and disassociate users and also enable the **Associate users automatically**, so each user in the domain who starts the user application (APRUsers), will automatically prompt you to configure the security questions.

The screenshot shows the 'Security questions' and 'Users' section. The 'Security questions' tab is active, showing the instruction 'Associate the Users who will be allowed to self-service in the business directory.' and a checked checkbox for 'Associate users automatically'. Below is a 'Users to add' input field with 'Add' and 'Import' buttons. The 'Users' tab is also visible, showing a list of associated users with a 'Filter' input, a 'Select all' checkbox, and a 'Disassociate' button. The list of users includes: Juan Social (Alias: juan.social), Ramon Valdez (Alias: rvaldez), Test (Alias: test), Test CYS (Alias: testcys), and Test CYS V8 (Alias: testcysv8). At the bottom right are 'Cancel' and 'Save' buttons.

Notes:

- If a user has already configured their security questions and subsequently disassociates from this section, they will need to repeat the configuration when re-associating.

- It is recommended to inform users in advance about this process to avoid confusion or reports of interrupted access.
- Applied changes are not reflected in active sessions; Users will need to close and reopen the app to properly apply the settings.

The administrator may **Clean up security questions** registered by a user when necessary. Click on the three dots icon of the associated user and select the option **Clean up questions**. When performing this action, the user will be prompted to reconfigure their security questions from the console **APRUsers** On your next access, this functionality is useful in support cases or when responses are suspected to have been compromised.

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 V8
Alias
testcysv8

☐ Name
Test CYS
Alias
testcys

Cancel

Save

Warning: This action will permanently delete the user’s saved replies. Be sure to notify the user before running this procedure.

When the setup is complete, click the **Save**. If everything has been set up correctly, the alert will be displayed **Updated Settings**. If not, validate the configuration and try again.

Business Directory

When entering the Admin console (APRAdmin), in the **Business Directory**, the administrator will be able to search for users within the selected domain, either by browsing the tree or by using the predictive search engine.

Aranda PassRecovery
for Active Directory

Configuration

EN

Log out
User Name In
Administrator

Domains

Configuration

Directory Business

Templates

Directory business

This section will allow you to manage the user accounts of the domain.

Select the domain

TEST

TEST

Company

Computers

Servers

Users

Argentina

Brasil

Chile

Colombia

Costa Rica

Ecuador

Guatemala

Mexico

Panama

Peru

Search

Search

Name: Juan Social

State:

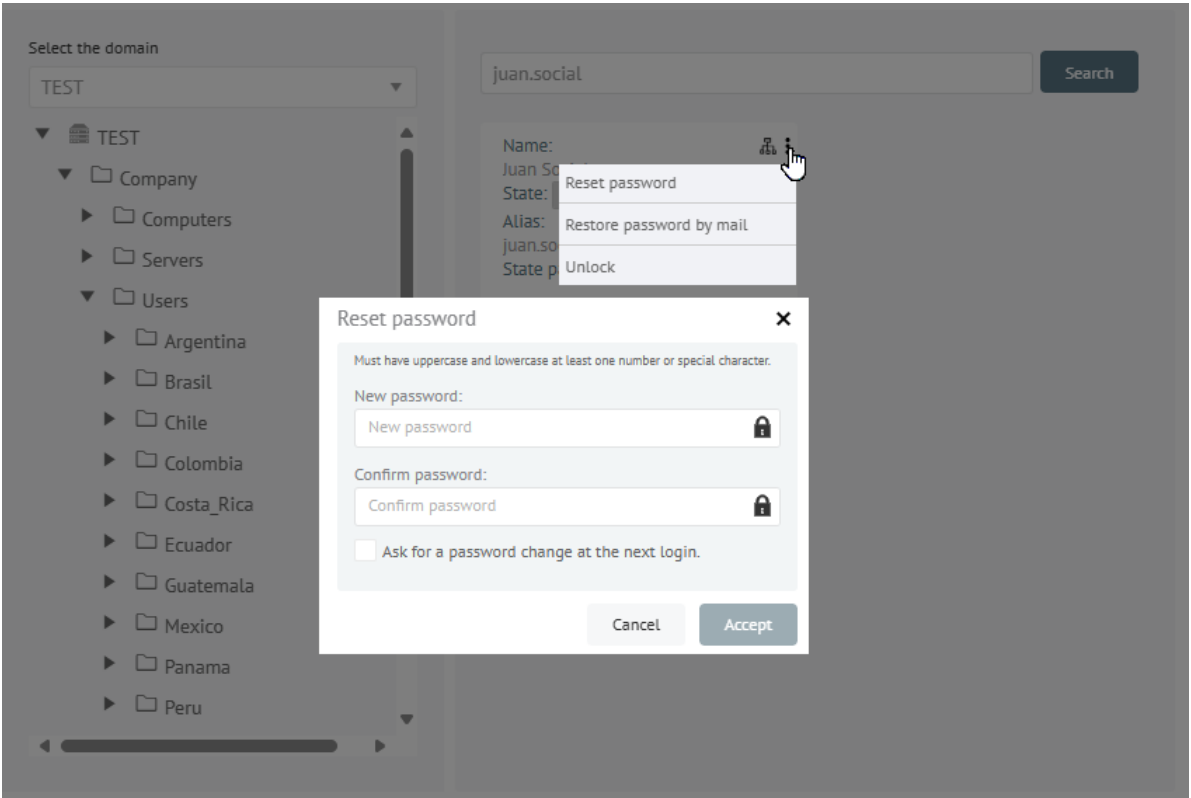
Alias: juan.social

State password: Active

From the Business Directory, the administrator may carry out the following procedures:

Reset password

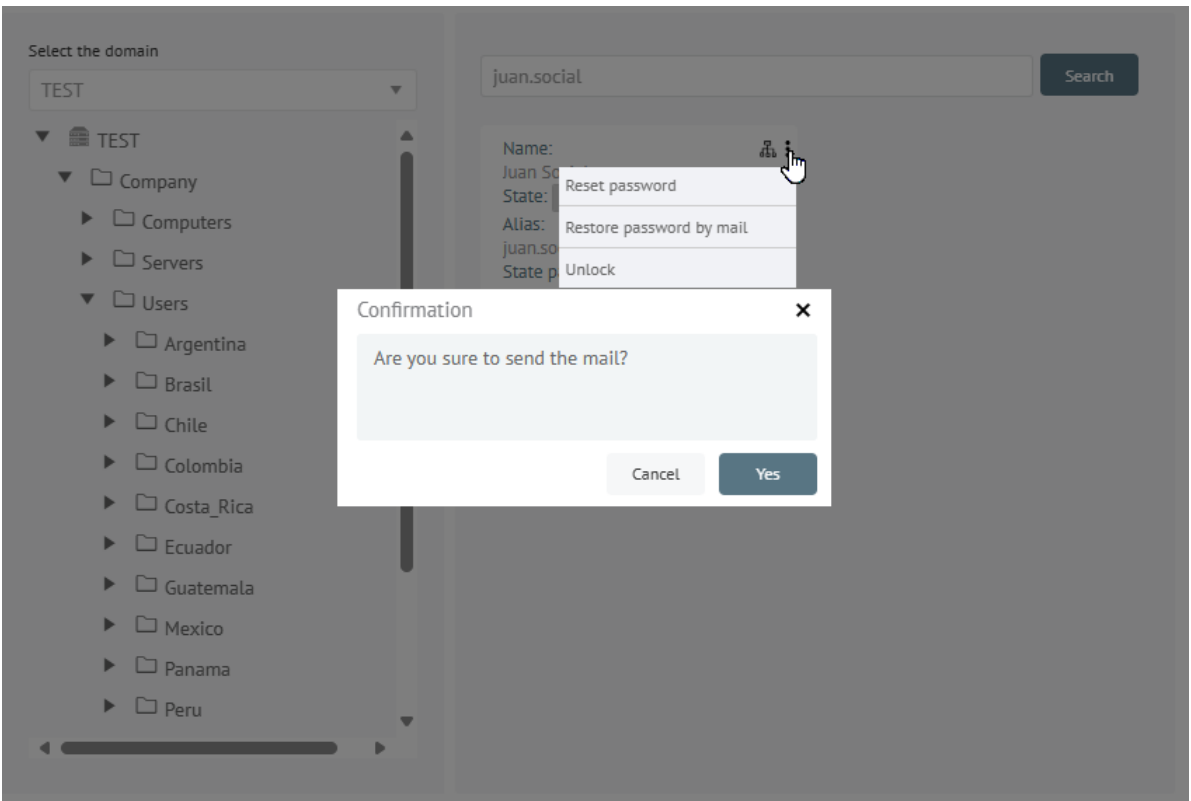
To reset the password, click on the icon of the three dots of the user to be managed and select the option **Reset password**. In the window **Reset password**, fill in the requested fields. When you activate the check **Ask for password change at next login**, you can ask the user to change the password on their next login.



After filling out the fields, click the **Accept**. The alert will be displayed **Password updated**. If the option is enabled **Case creation**, a case will be automatically generated in **ASDK** according to the configured settings.

Reset password by email

To reset the password by email, click on the icon of the three dots of the user to be managed and select the option **Reset password by email**. In the window **Confirmation**, click the **Yes**. The alert will be displayed **Password Reset Email Sent**.



The application will schedule the sending of an email with a link that includes a [One-time access token](#), this will allow the user to initiate password reset self-management. The mail will be sent to both the primary address and the alternate mailing address on file. If the option is enabled **Case creation**, a case will be automatically generated in **ASDK** according to the configured settings.

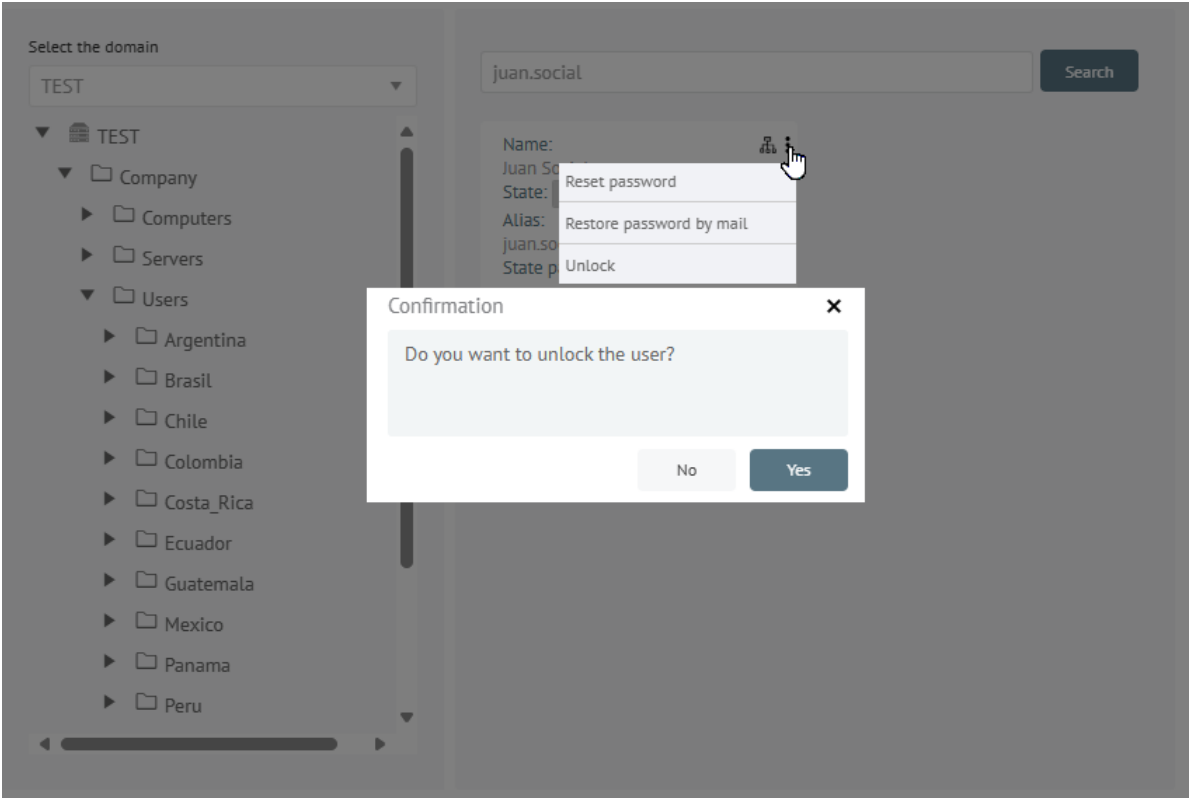
Notes:

- If the user already has questions configured, the application will ask them to fill out these answers.
- If the user does not have questions configured, the application will ask them to fill out the security questions.
- In case the user does not remember the answers, it is recommended to clean the questions from the option **Configuration** section **Users**.
- The function **Reset password by email** it depends on the correct configuration of the SMTP server.

- Verify that it is enabled and accessible from the application server.
- If the user does not receive the restore email, verify that they have a valid primary or alternate address.

Unlock (when applicable)

To unblock a user who is locked out of the **Active Directory (AD)** icon, click the blocked user’s three dots icon, and select the option **Unlock**. In the window **Confirmation**, click the **Yes**. The alert will be displayed **The user is unlocked**.



📌 **Note:**

- This option is enabled only when the user is effectively locked out of the active directory.

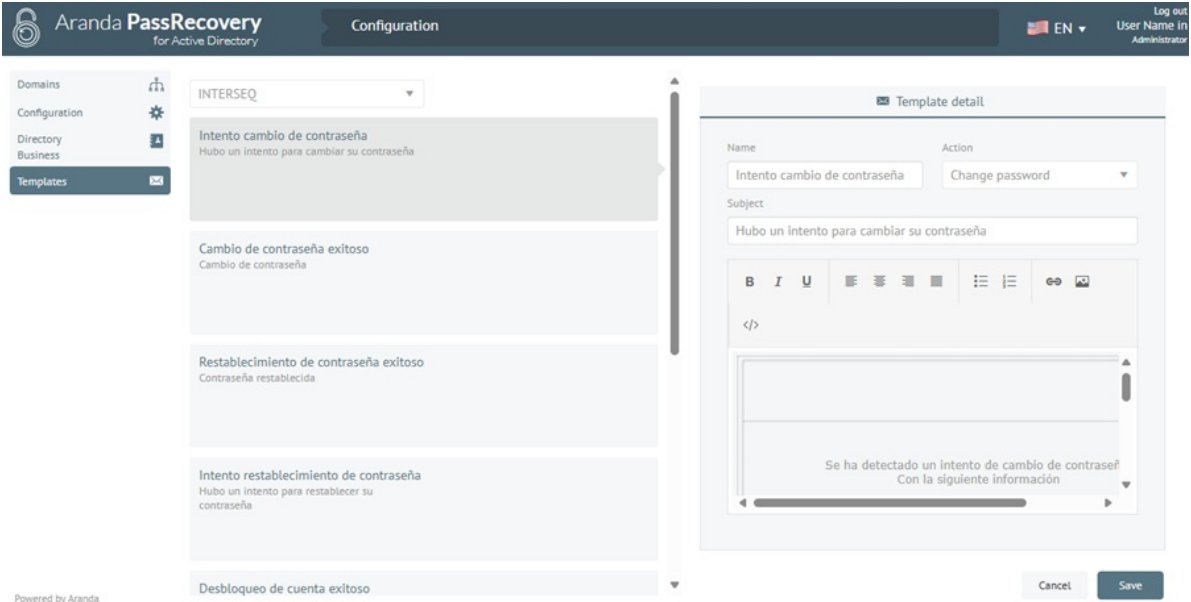
Templates

When entering the Admin console (**APRAdmin**), in the **Templates**, the administrator will be able to customize the templates available for the different behaviors, according to the need of each configured domain.

📌 **Notes:**

- It is not possible to add or remove templates.
- They will always be displayed in Spanish, it is only possible to customize the body of the message.

Once the necessary modifications have been made, click on the **Save** to apply the changes.



User Console (APRUsers)

Use user console

When entering the user console (APRUsers) of **Aranda PassRecovery**, the user will be able to access three specific functionalities, provided that these are previously enabled in the **Active Directory**:

1. [Unlock account](#)
2. [Reset password](#)
3. [Change password](#)

To access these functionalities, the application uses an authentication method based on the validation of [Security Questions](#). These questions must have been previously configured by the user from the same console.

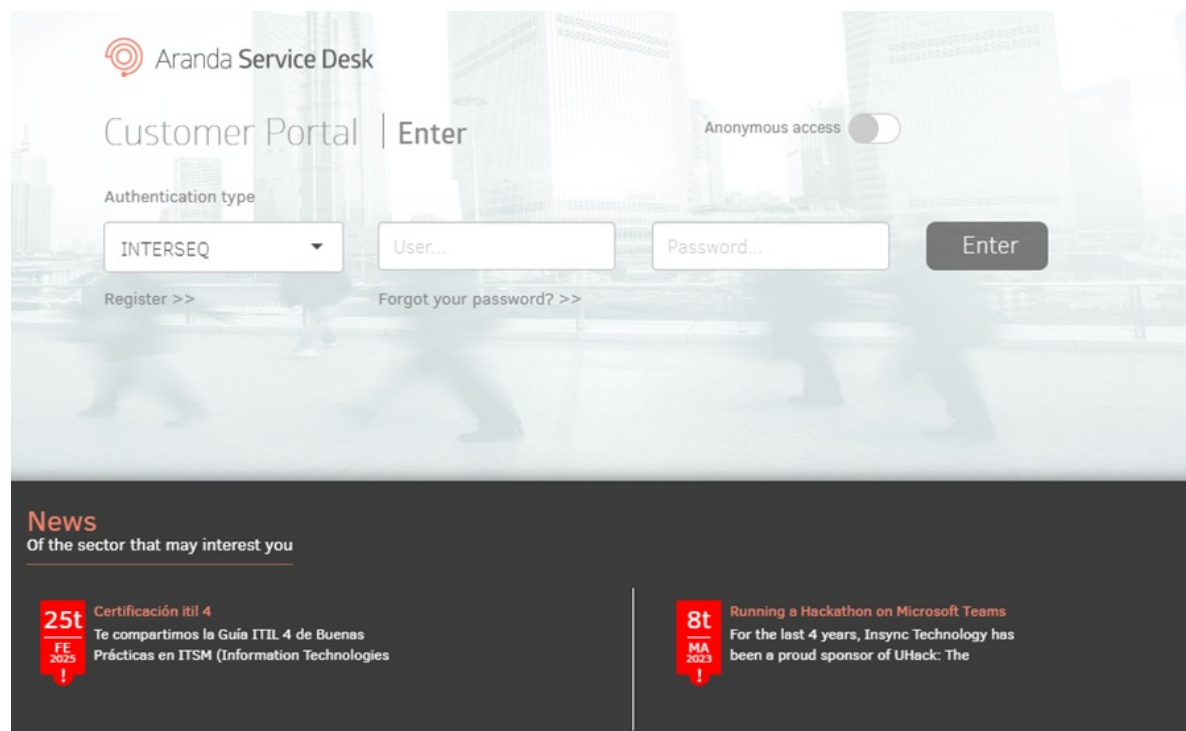
Setting up security questions

As part of the setup process, the end user must record the security questions and answers that they want to associate with their identity. The minimum number of questions required for authentication is predefined by the administrator from the admin console.

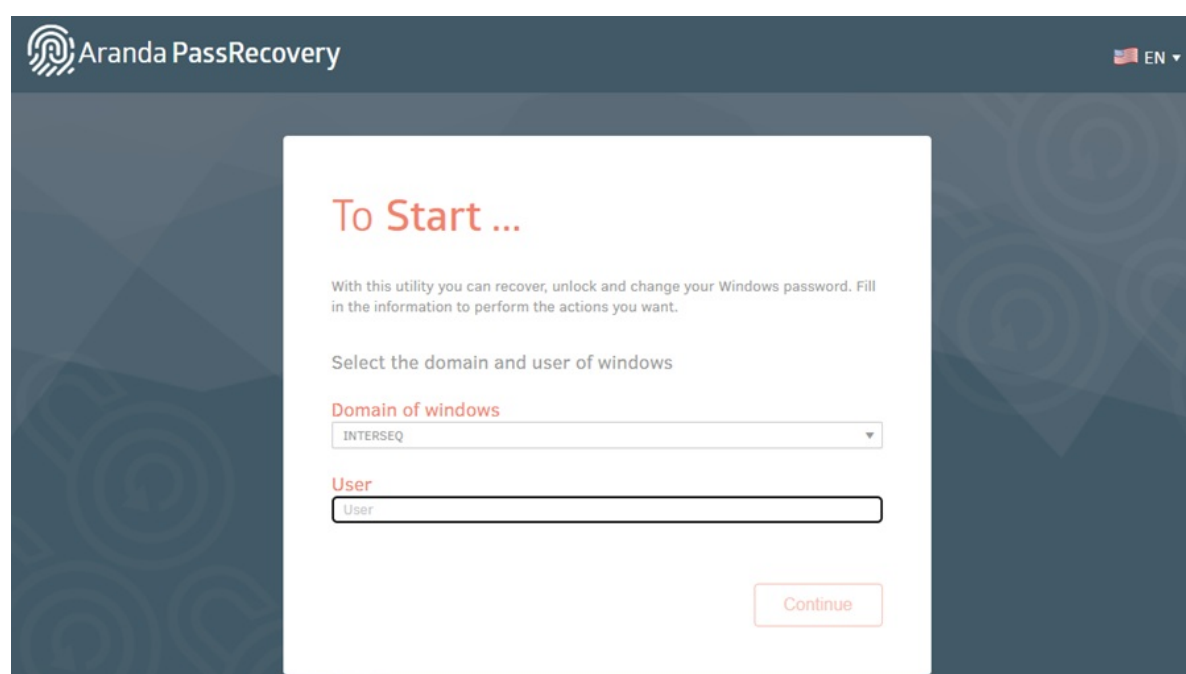
These questions will be configured only once – or again if the administrator deletes them or modifies the required amount – and are requested at the user's first login to the tool **Aranda PassRecovery**.

To perform this configuration, follow these steps:

1. Log in to the ASDK User Console 'https://{domain}/USDKV8/', select the domain you want to authenticate with, and click the **Forgot your password?**.

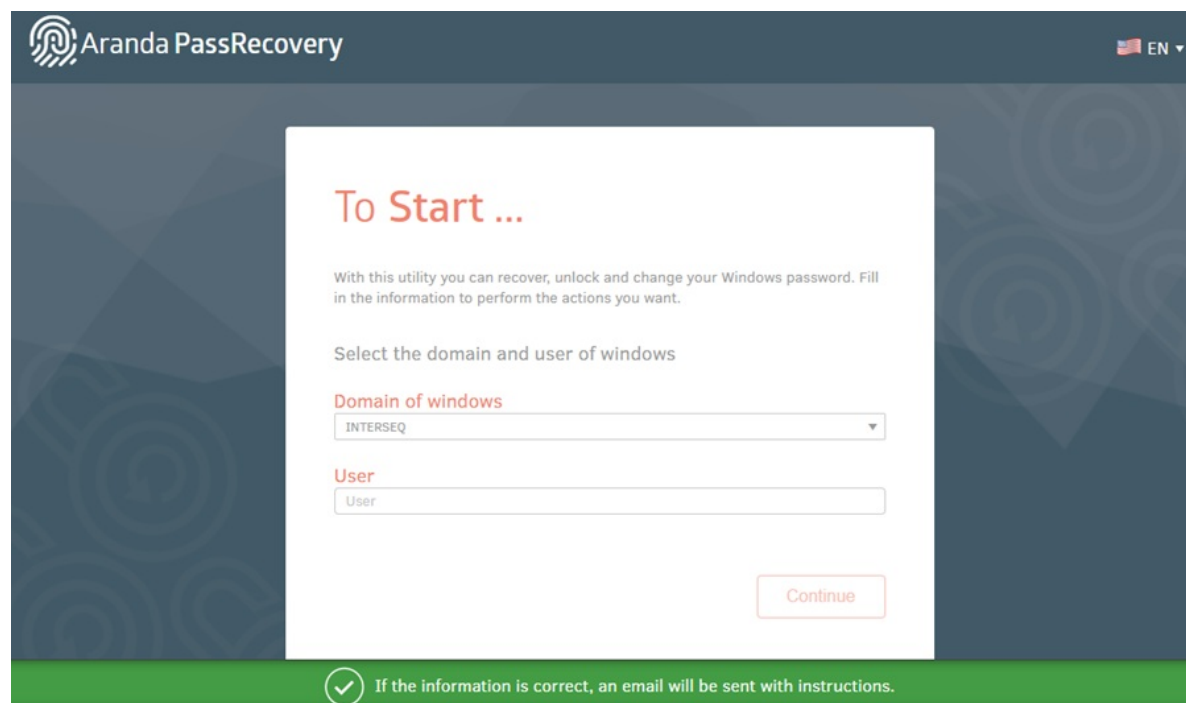


2. The **Aranda PassRecovery** in a new tab. Enter your username and click the **Continue**.



3. Regardless of whether or not the user is associated with self-service, and whether or not they exist in Active Directory, the following message will be displayed:

“If the information is correct, an email will be sent with instructions.”

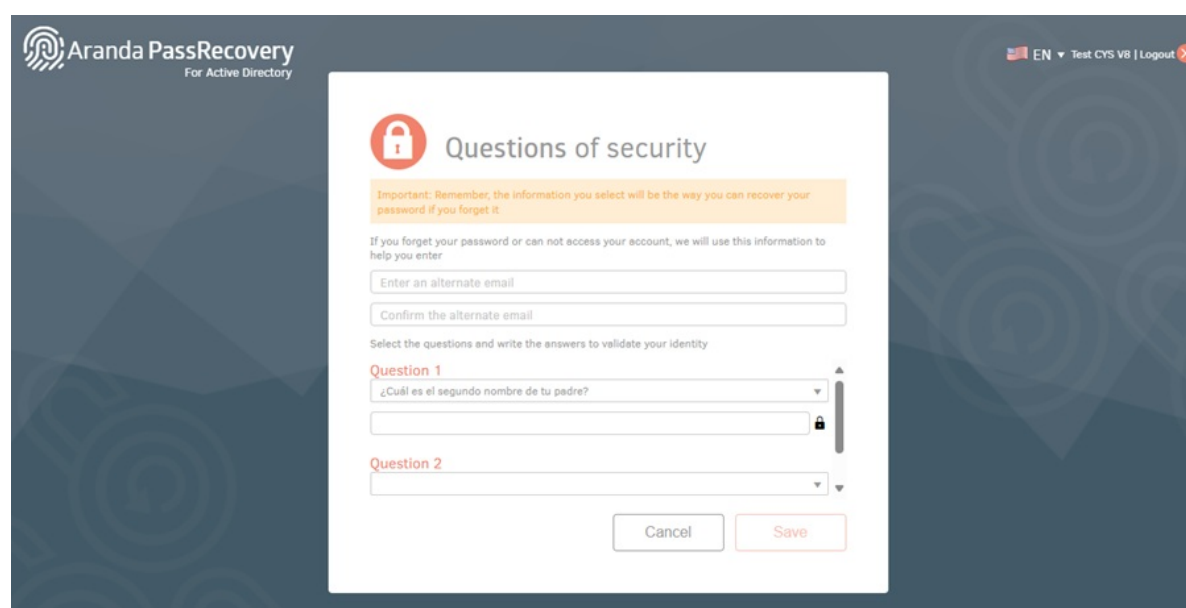
The screenshot shows the 'To Start ...' screen of the Aranda PassRecovery application. The header includes the logo and 'Aranda PassRecovery' text, with a language dropdown set to 'EN'. The main content area has a title 'To Start ...' in red, followed by a brief description: 'With this utility you can recover, unlock and change your Windows password. Fill in the information to perform the actions you want.' Below this, it says 'Select the domain and user of windows'. There are two input fields: 'Domain of windows' with a dropdown menu showing 'INTERSEQ', and 'User' with a text input field containing 'User'. A 'Continue' button is at the bottom right. A green banner at the bottom contains a checkmark icon and the text: 'If the information is correct, an email will be sent with instructions.'

4. The application will validate the corresponding configurations and, if the criteria are met, will schedule an email to be sent using the template **Password reset**. This email will include a link to a [One-time access token](#) which will allow the user to continue with the management. The mail will be sent to the primary or alternate address registered in the ASDK database.

📌 Notes:

- Sending emails depends on the correct configuration of the SMTP server. Verify that it is enabled and accessible from the application server.
- If the user doesn't receive the email, verify that they have a primary or alternate address registered and that it's associated with self-service in the Admin console.
- The lifetime of the access token is defined from the Admin console, in the **Token validity time**, within the **Configuration**.

5. Once the user accesses the link received, they will be redirected to the form **Security Questions**, where you can register (or update) an alternate email and fill out the answers to the selected questions.

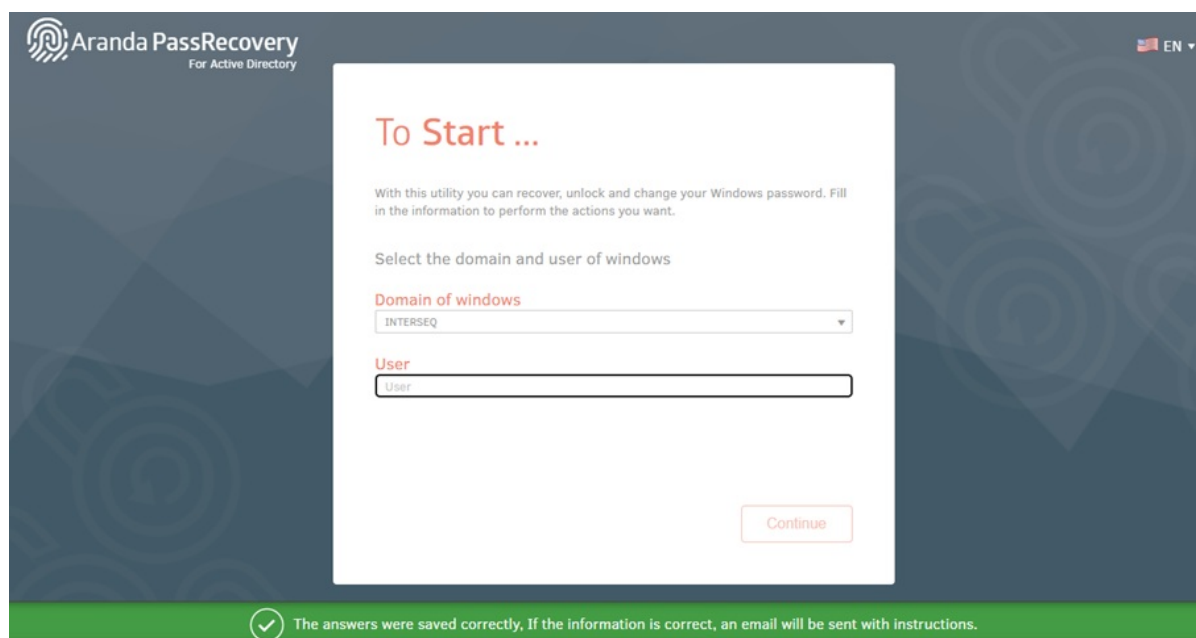
The screenshot shows the 'Questions of security' screen of the Aranda PassRecovery application. The header includes the logo and 'Aranda PassRecovery For Active Directory' text, with a language dropdown set to 'EN' and links for 'Test CYS V8' and 'Logout'. The main content area has a title 'Questions of security' with a lock icon. Below the title is an important note: 'Important: Remember, the information you select will be the way you can recover your password if you forget it.' This is followed by instructions: 'If you forget your password or can not access your account, we will use this information to help you enter'. There are two input fields: 'Enter an alternate email' and 'Confirm the alternate email'. Below these, it says 'Select the questions and write the answers to validate your identity'. There are two question sections: 'Question 1' with a dropdown menu showing '¿Cuál es el segundo nombre de tu padre?' and a text input field, and 'Question 2' with a dropdown menu. At the bottom, there are 'Cancel' and 'Save' buttons.

📌 Notes:

- If the user already has registered questions, they must answer them when entering from the link. If you want to change them, you will need to request your administrator to remove them from the **Aranda PassRecovery**.
- If the user signs in with an expired or already used token, the alert will be displayed: **Token validation error**.

6. Once you have filled out the required information, click on the **Save**. The alert will be displayed: “The answers were set up correctly. If the information is correct, an email will be sent with the instructions.”

If not, validate the configuration and try again.



🚩 **Note:**

- Set up a **Alternate mail** It will allow the user to recover their password even if they cannot access their main mail.

7. The application will schedule the sending of a new email using the **Password reset**, with a link that includes a [One-time access token](#). The mail will be sent to the main and alternate addresses on file. 🚩 **Note:**

- If both email addresses (primary and alternate) are the same, only one email will be sent.

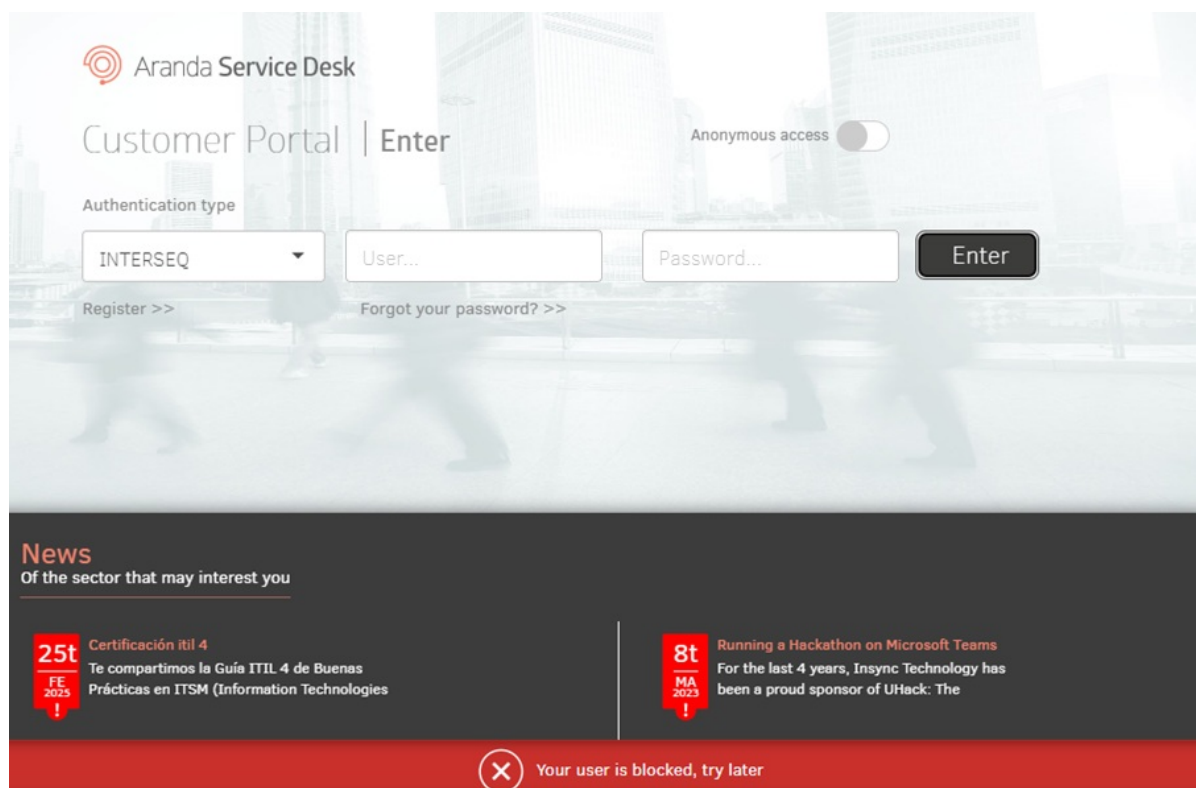
Unlock account

If the user locks out their account after entering an invalid password several times, they can perform the unlocking process from the **Aranda PassRecovery**.

⚠ **Warning:** It is mandatory to have previously configured [Security questions](#).

Steps to unlock the account

1. Log in to the ASDK User Console 'https://{domain}/USDKV8/', select the appropriate domain, and click the **Forgot your password?**.



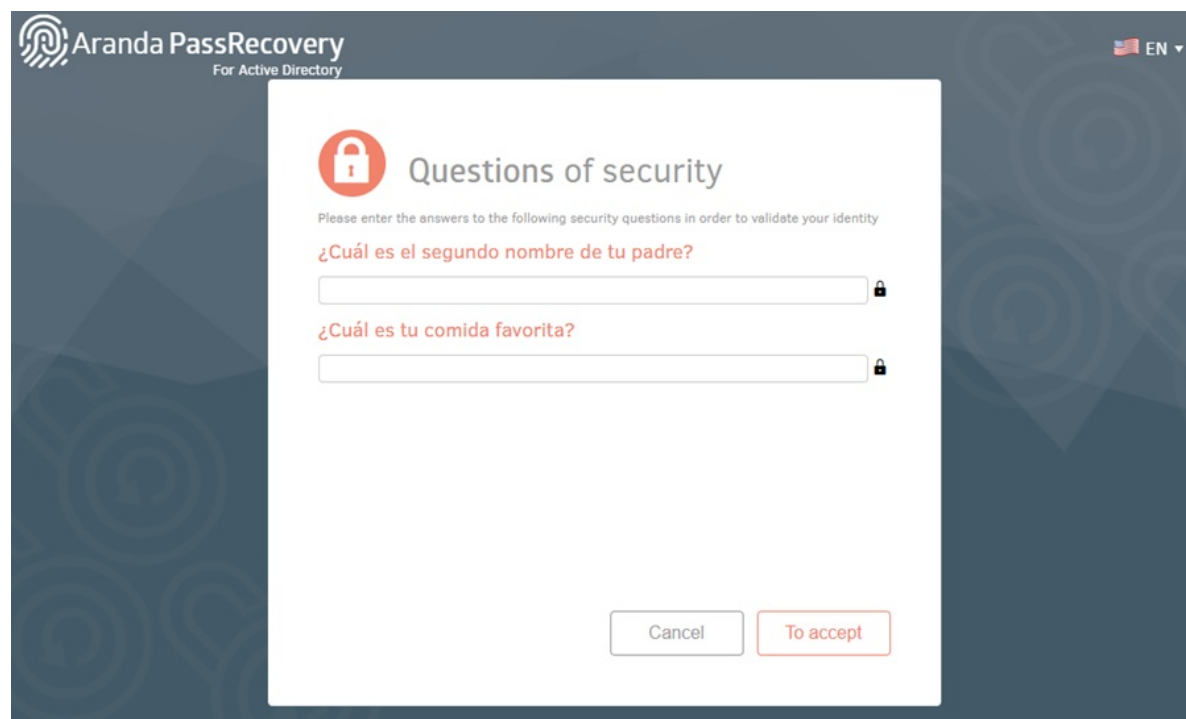
2. The **Aranda PassRecovery** in a new tab. Enter your username and click the **Continue** to schedule the sending of the email that will allow you to manage the unlocking of your account.

3. Enter the link received in the email. You will be redirected to the form **Security Questions**, where you will need to answer the pre-configured questions.

🚩 **Notes:**

- If the user signs in with an expired or already used token, the alert will be displayed: **Token validation error**.

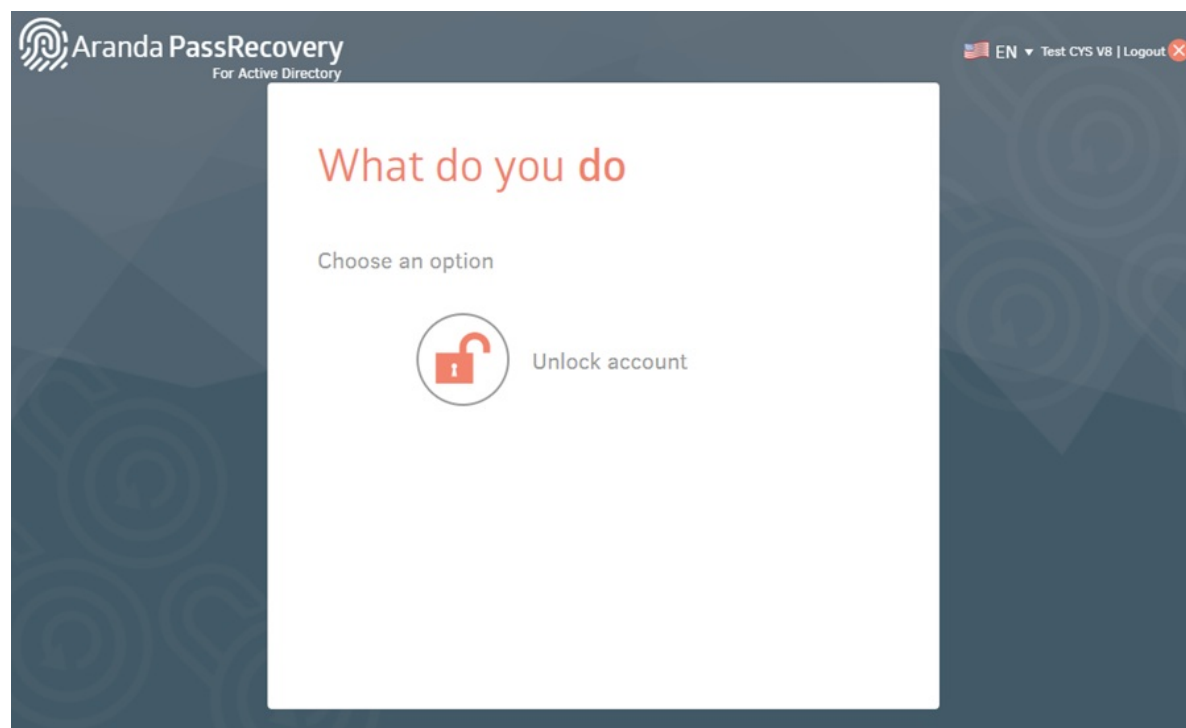
4. Fill in the answers and click the **Accept**. The console will validate the answers entered and, if correct, redirect the user to the window **What you want to do** where it will allow you to unlock the account.

A screenshot of the Aranda PassRecovery application interface. The title bar shows 'Aranda PassRecovery For Active Directory' and a language dropdown set to 'EN'. The main window is titled 'Questions of security' with a red padlock icon. Below the title, it says 'Please enter the answers to the following security questions in order to validate your identity'. There are two questions in Spanish: '¿Cuál es el segundo nombre de tu padre?' and '¿Cuál es tu comida favorita?'. Each question has a text input field with a small lock icon on the right. At the bottom, there are two buttons: 'Cancel' and 'To accept'.

Notes:

- If the user answers one or more questions incorrectly, the alert will be displayed: **Incorrect answers**.
- If the number of attempts defined in the Admin console (field **Number of attempts** section **Configuration**), the alert will be displayed: **Attempts exceeded, retry in X min**.
- If a user blocked by failed attempts tries to log in with a valid token, the alert will be displayed: **Blocked user, please try again in X min**.

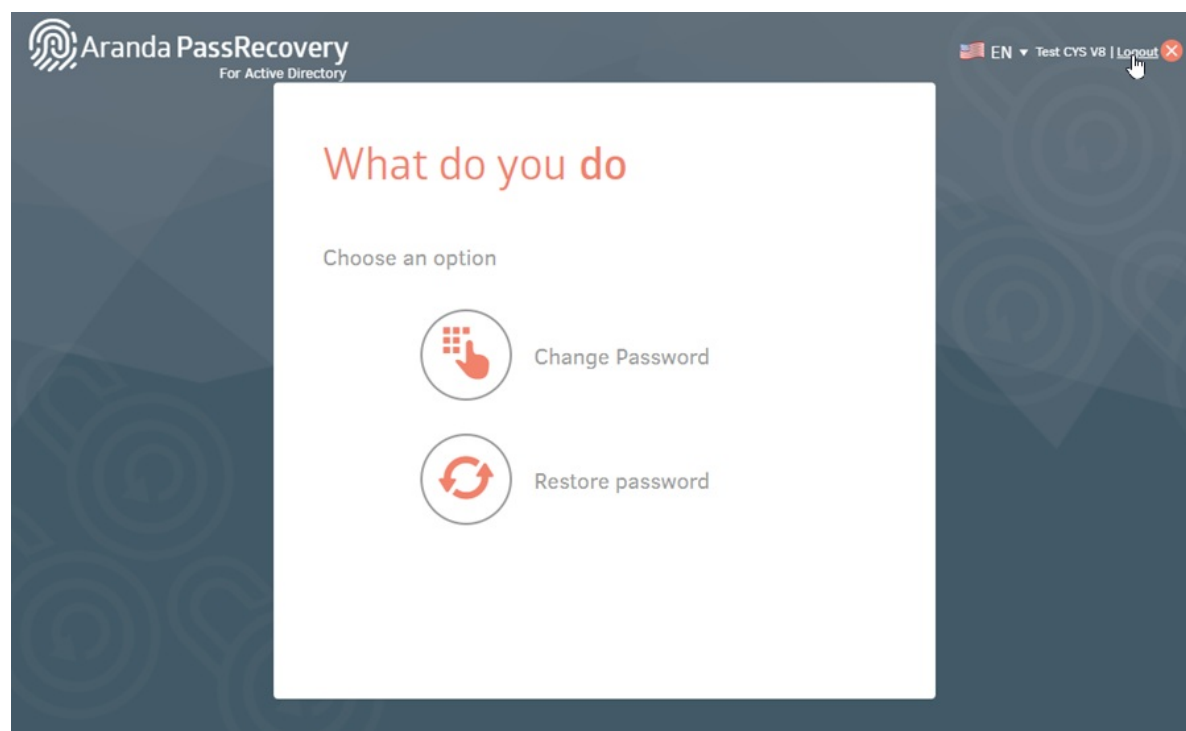
5. Click the **Unlock account**. The application will send the request to the Active Directory to remove the account lock, displaying the following message: **The account has been unlocked**.

A screenshot of the Aranda PassRecovery application interface. The title bar shows 'Aranda PassRecovery For Active Directory' and a language dropdown set to 'EN'. The main window is titled 'What do you do' in red. Below the title, it says 'Choose an option'. There is a single option with a red padlock icon and the text 'Unlock account'. In the top right corner of the window, there is a status bar with 'EN', 'Test CYS V8', and a 'Logout' button with a red 'X' icon.

After unlocking the account, the user will be able to perform the following actions:

- [Reset password](#)
- [Change password](#), when applicable.

If you do not wish to take any further action, log out by clicking the **Log off**.



6. If the **Case** creation, an ASDK case will be automatically generated in the name of the user who performed the unlock.

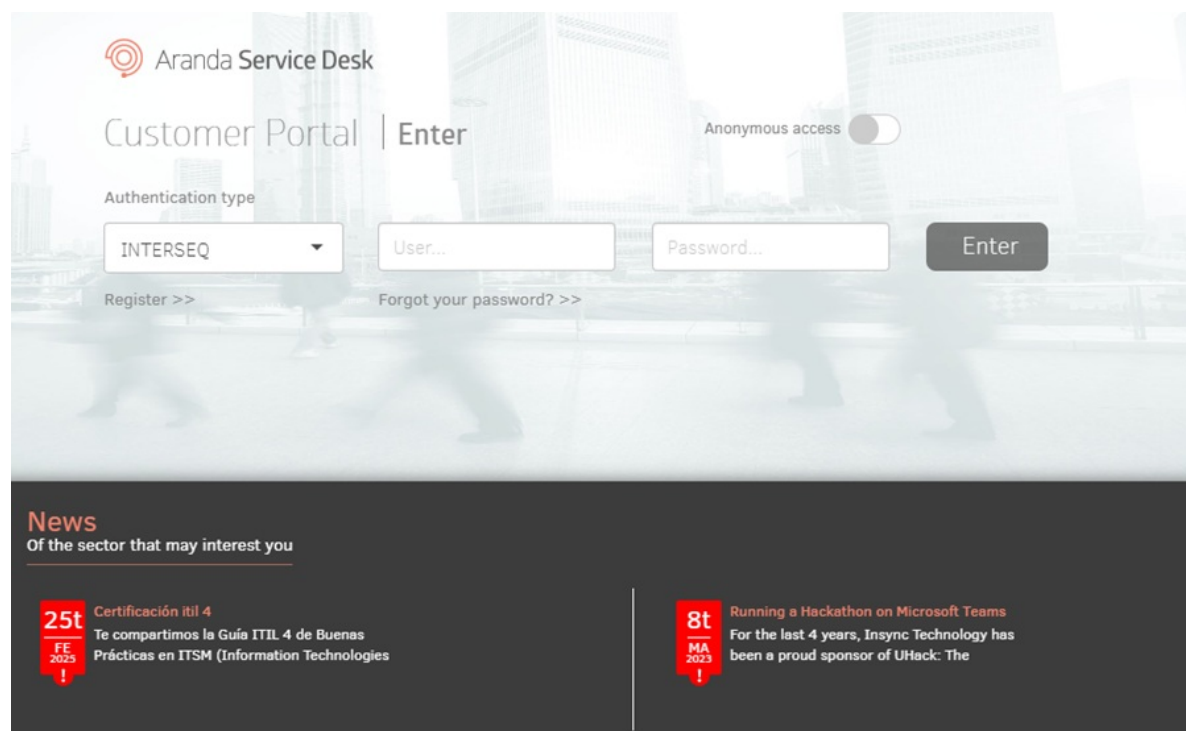
Reset password

If a user forgets their password, they can perform the reset process from the User's console. **Aranda PassRecovery**.

⚠ **Warning:** It is mandatory to have previously configured [Security questions](#).

Steps to reset your password

1. Log in to the ASDK User Console 'https://{domain}/USDKV8/', select the appropriate domain, and click the **Forgot your password?**.




2. The **Aranda PassRecovery** in a new tab. Enter your username and click the **Continue** to schedule the sending of the email that will allow you to manage the password reset.

3. Enter the link received in the email. You will be redirected to the form **Security Questions**, where you will need to answer the pre-configured questions.

📌 Notes:

- If the user signs in with an expired or already used token, the alert will be displayed: **Token validation error**.

4. Fill in the answers and click the **Accept**. The application will validate the answers entered and, if they are correct, redirect the user to the window **What do you want to do?**, where you can select the option to reset your password.



EN

Questions of security

Please enter the answers to the following security questions in order to validate your identity

¿Cuál es el segundo nombre de tu padre?

¿Cuál es tu comida favorita?


Cancel

To accept

Notes:

- If the user answers one or more questions incorrectly, the alert will be displayed: **Incorrect answers.**
- If the number of attempts defined in the Admin console (field **Number of attempts** section **Configuration**), the alert will be displayed: **Attempts exceeded, retry in X min.**
- If a user blocked by failed attempts tries to log in with a valid token, the alert will be displayed: **Blocked user, please try again in X min.**

5. In the window **What do you want to do?**, click the **Reset password** to start the management.




EN Test CYS V8 | Logout

What do you do

Choose an option

Restore password

6. In the window **Reset Password**, the console will prompt you to enter a new password and confirm it. Fill in the required fields and click on the **Accept**. At the bottom, the password policies defined in the Active Directory will be displayed.



EN Test CYS V8 | Logout

Restore Password

New Password

Confirm Password

To change the password, consider the following recommendations:

- Minimum length is 7 characters
- That does not match your last 4 passwords
- The password must have at least one uppercase letter, one lowercase letter, one non-alphanumeric character or one number. Also, do not contain the user account name or parts of the user's full name in more than two consecutive characters.

Cancel

Accept

7. If the action is successful, the application will display the alert: **Updated password**. If not, validate the information entered and try again.
8. If the **Case creation**, an ASDK case will be automatically generated in the name of the user who performed the reset.

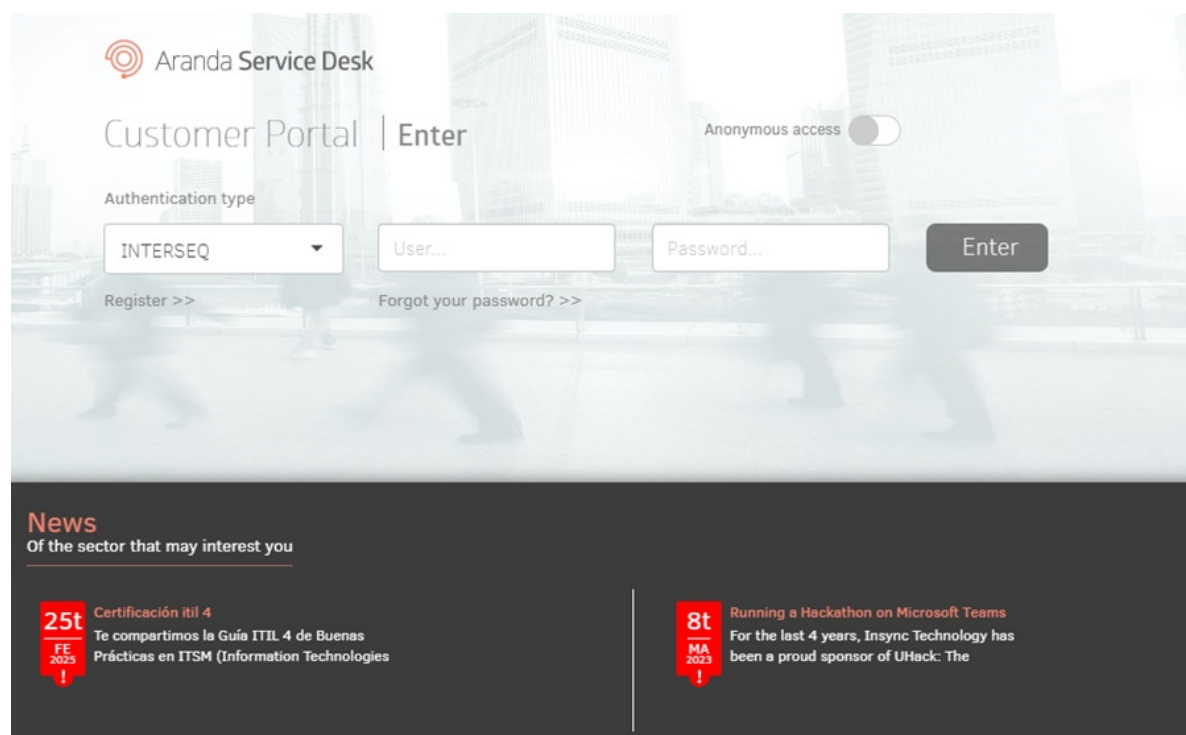
Change password

Changing your password from the User's Console **Aranda PassRecovery** It will be available when the password is about to expire. If the password was recently changed and the Active Directory (AD) has policies that set a minimum time for the change, the **Change Password** it will not be enabled.

⚠ **Warning:** It is mandatory to have previously configured [Security questions](#).

Steps to change your password

1. Log in to the ASDK User Console 'https://{domain}/USDKV8/', select the appropriate domain, and click the **Forgot your password?**.

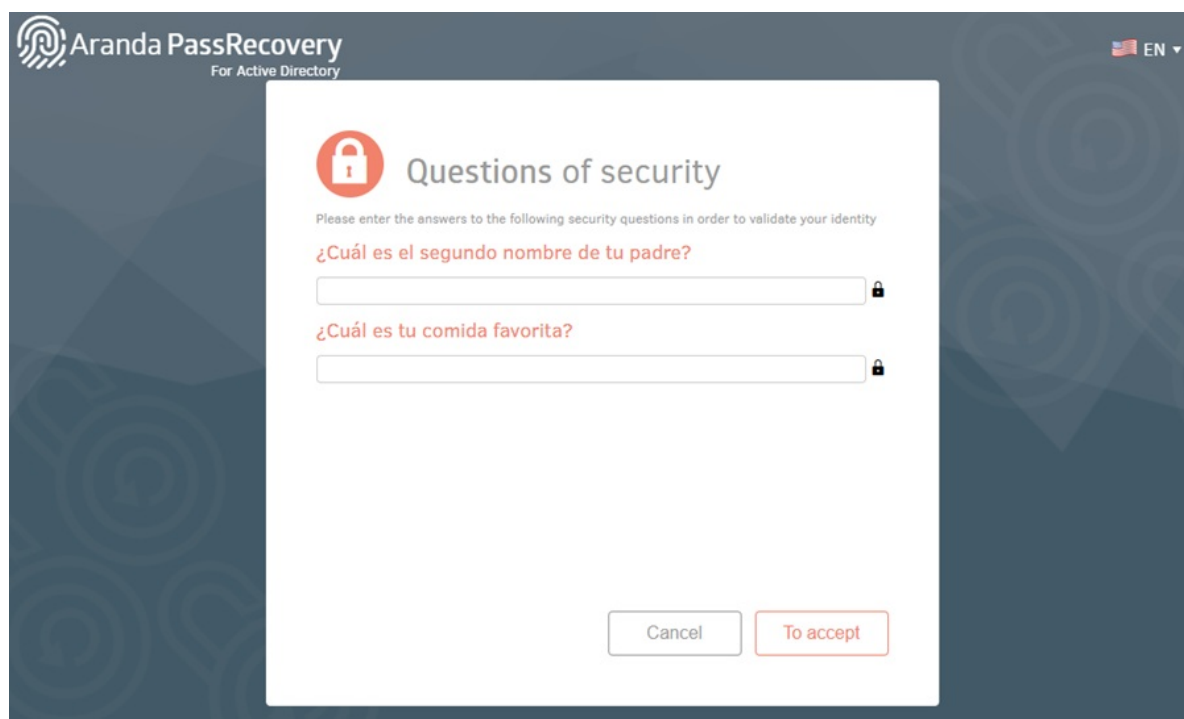


2. The **Aranda PassRecovery** in a new tab. Enter your username and click the **Continue** to schedule the sending of the email that will allow you to manage the password change.
3. Enter the link received in the email. You will be redirected to the form **Security Questions**, where you will need to answer the pre-configured questions.

📌 Notes:

- If the user signs in with an expired or already used token, the alert will be displayed: **Token validation error**.

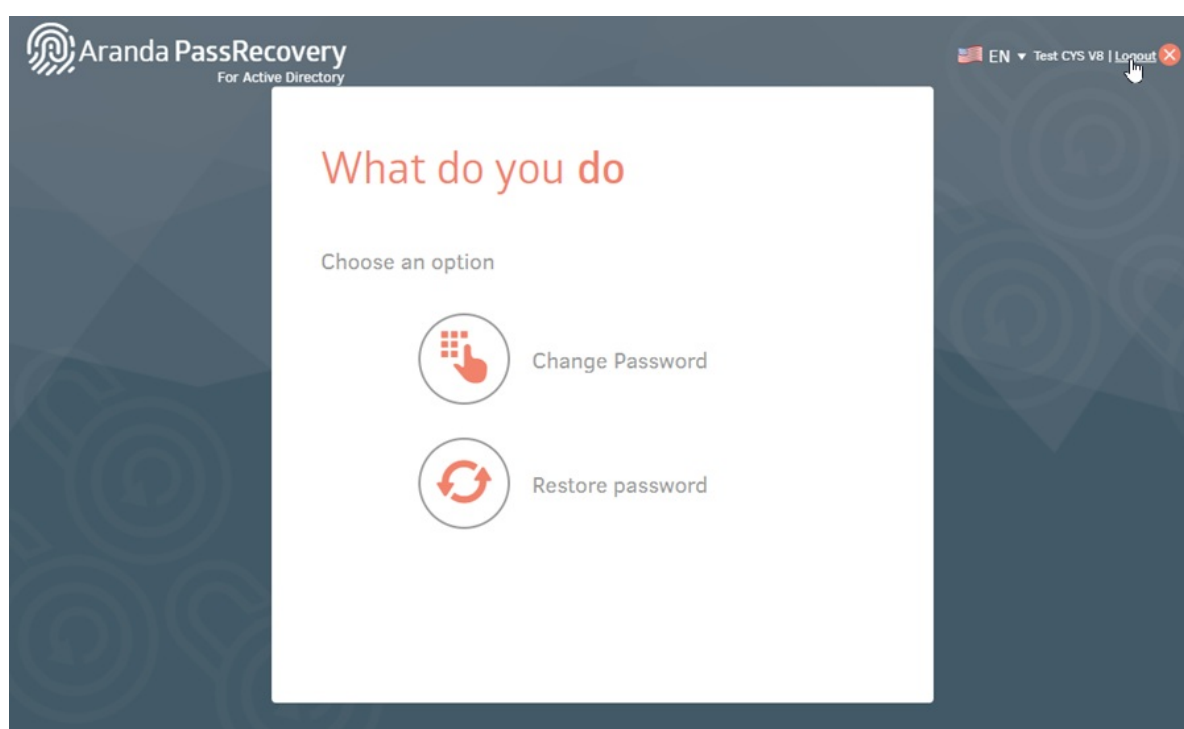
4. Fill in the answers and click the **Accept**. If the answers are correct, the application will redirect the user to the **What do you want to do?**, where you can select the option to change your password.



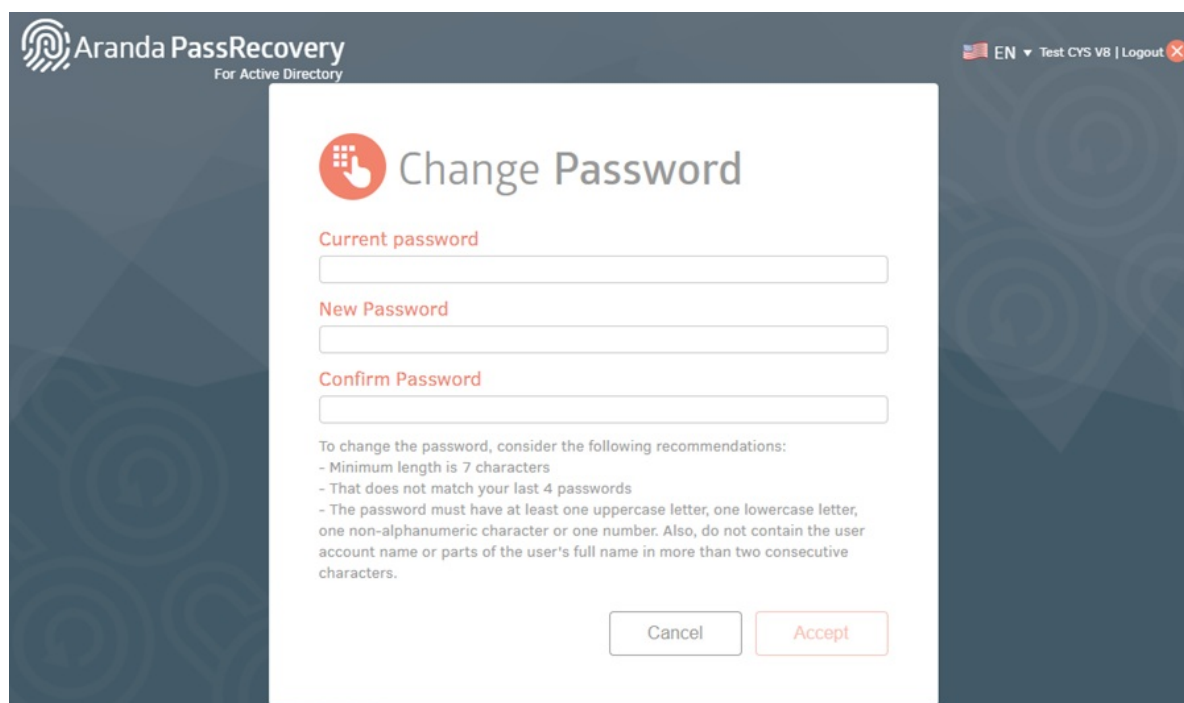
Notes:

- If the user answers one or more questions incorrectly, the alert will be displayed: **Incorrect answers.**
- If the number of attempts defined in the Admin console (field **Number of attempts** section **Configuration**), the alert will be displayed: **Attempts exceeded, retry in X min.**
- If a user blocked by failed attempts tries to log in with a valid token, the alert will be displayed: **Blocked user, please try again in X min.**

5. In the window **What do you want to do?**, click the **Change Password** to start the process.



6. In the window **Change Password**, the console will prompt you to enter your current password, new password, and confirmation. Fill in the requested fields and click on the **Accept**. At the bottom, the password policies defined in the Active Directory will be displayed.



7. If the action is successful, the application will display the alert: **Updated password**. If not, validate the information entered and try again.

8. If the **Case creation**, an ASDK case will be automatically generated in the name of the user who made the change.

Case Creation Configuration

This utility has the function of creating cases automatically once any of the application's actions are executed (Key Change, Key Restoration or Account Unlock). To configure the automatic creation of cases from the utilitarian follow these steps:

- Templates must be created for scheduled actions in BASDK in Settings/Template, according to the types of cases to be created.

Editar / Plantilla	
<input checked="" type="checkbox"/>	Plantilla para acciones programadas
Nombre	CambioClaveAD
Impacto	BAJO
Urgencia	BAJA
Prioridad	BAJA
Tipo de Registro	Requerimientos de Servi
Categoría	Cuentas de Dominio
Servicio	Administración de Cuel
Grupo de Especialistas	Mesa de Servicio Nivel
Especialista	APPLICATION ADMINIST
ANS	Bajo
Cliente	APPLICATION ADMINIST
Compañía	
Ci	
Asunto	Creación de Caso por cambio de clave AD
Descripción	
<p>Creación de caso por cambio de Clave de AD por medio del utilitario.</p>	

- In the **Configuration/Scheduled Actions**, create the scheduled actions according to the created templates. Note that the scheduled action is executed based on the following wildcards, these must be set in the name of the scheduled action.

Wild cards

- SetPassword Actions related to Reset the domain key.
- ChangePassword Actions related to Domain Key Change.
- ActiveUser Actions related to unlocking a domain account.

Scheduled action configuration fields:

Name: Name of the scheduled action with the corresponding wildcard. Ex: changeKey - SetPassword.**Guy:** Only once. **Execution Time:**Any. **Run From, To:** It must be an expired date for the database to execute the creation of the case only once.

Example of scheduled action configuration:

Acciones programadas			
Identificador	Nombre	Fecha de inicio	Fecha Fin
14	cambio-SetPassword-ChangePasword	01/04/2018 06:00:00 a.m.	02/04/2018 12:00:00 a.m.
15	activacion-ActiveUser	01/04/2018 06:00:00 a.m.	02/04/2018 12:00:00 a.m.

Configuración General

Nombre: cambio-SetPassword-ChangePasword

Tipo: Una sola vez

Hora de ejecución: 08:00:00 a.m.

Ejecutar desde: 01/04/2018 Hasta: 02/04/2018

Acciones

Nueva acción

Nombre	Plantilla	Cant. de casos
Crear caso	CambioClaveAD	1

Total registros 1

Cambiar página: 1 Registros por página: 100

Cancelar Guardar

- Adding actions in scheduled actions, once the templates and the scheduled action are configured, the action must be added, in which case it would be: **Type of Action:** Case Creation. **Template:** Select the template that was configured for the creation of utility cases. **Number of cases:** 1(In this case it must be one so that only one case is created for each action).

With this setting when you run actions from **Aranda PassRecovery** cases are automatically created in ASDK.

Aranda PassRecovery Flowchart

