

2FA User Manual

SGND 7.18



Version 1.0

ÍNDICE

1. SGND ACCESS	3
1.1. How to recover the password?	4
2. TWO FACTOR AUTHENTICATION ACCESS (2FA).....	7
2.1. Two Factor Authentication by Email	7
2.2. Two Factor Authentication by App	8
3. TROUBLESHOOTING	9
3.1. How to configure the Application?	9
3.2. How to change the Two Factor Authentication method?	10
3.3. How to reset the QR code for Application?	11
3.4. What to do if you lose the QR code for the Application?	11
3.5. How to change the email address?	11
3.6. Management of certificates for login	13
3.6.1. Associate Certificates.....	15
3.6.2. Disassociate Certificates	15

1. SGND ACCESS

Access to the application is through the validation screen, which as a security measure requires an identifier and a password. If you have not registered in the application and you do not have this information, you must first register on the dominios.es website.

Once entered, a screen will appear to enter the Two Factor Authentication security code. By default, the double factor method is to send the security code by email (this method can be changed to "by application" once you access the page).

Login

WARNING: In order to comply with the new National Security Scheme (ENS), published in the Royal Decree 311/2022 of 3rd May, the ".es" Domain Names Registry has established a **two-factor authentication (2FA)** to be able to access the management of your domain. By default, the 2FA code **will be sent to the email address associated with your user**, but once you are logged into your account, you can also set it up through any application that generates 2FA codes, e.g. Google Authenticator. [\(2FA User Manual\)](#)

It is necessary that your **email address is operational and updated** in the Registry database. We remind you of your obligation to keep all data associated with your domain name up to date ([Terms and conditions](#)).

To access the system you can:

- 1- Enter the **ID and password**, which was assigned to register through Dominios.es.

Please enter them below:

Authentication form

ID: E.g.: AAAA0-ESNIC-F0

Password:

[Retrieve password](#) **Authenticate**

- 2- **Authenticate** using your eID or certificate.

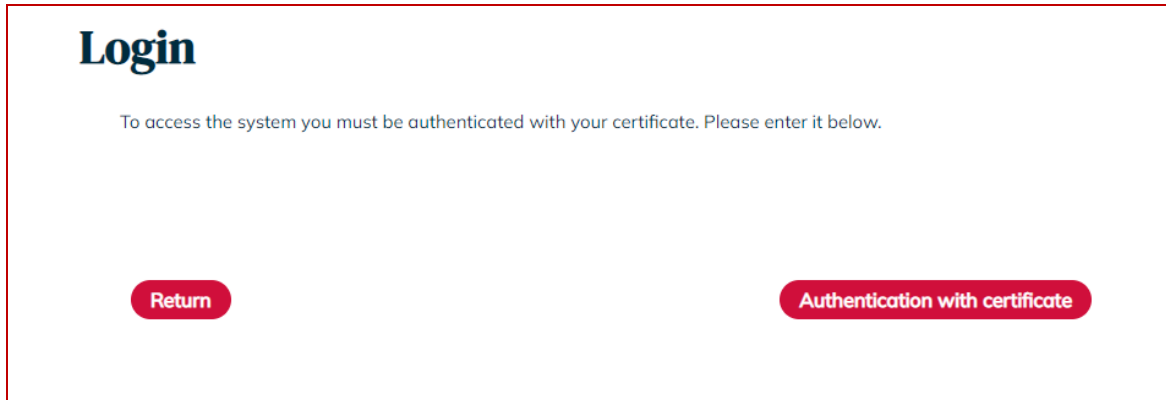
Please enter your eID in the card reader. [Authentication with certificate](#)

If you wish to change the email: [Change email](#)

If you are not registered, you can do it in Dominios.es: [Register in Dominios.es](#)

It is also possible to access the application from a **valid digital certificate** (DNIe, FNTM certificate,...). This certificate must be valid at the time of trying to access the application, so certificates that are expired, revoked or whose validity cannot be verified are not valid. To use this option, the user must have a valid certificate associated to their identifier.

Users who have only one user in the system, with the ID number correctly stored, will be able to access the application with DNIe/Certificate without having to make a previous association.



Login

To access the system you must be authenticated with your certificate. Please enter it below.

[Return](#) [Authentication with certificate](#)

1.1. How to recover the password?

If you enter the wrong ID or password, the system will inform you that you have ten attempts. In case you spend all the allowed attempts, you will be blocked for one day.

If the identifier is known but the password has been forgotten, there is the option to recover it by clicking on the "Recover password" button as shown in the image:

Login

WARNING: In order to comply with the new National Security Scheme (ENS), published in the Royal Decree 311/2022 of 3rd May, the ".es" Domain Names Registry has established a **two-factor authentication (2FA)** to be able to access the management of your domain. By default, the 2FA code **will be sent to the email address associated with your user**, but once you are logged into your account, you can also set it up through any application that generates 2FA codes, e.g. Google Authenticator. **(2FA User Manual)**

It is necessary that your **email address** is **operational** and **updated** in the Registry database. We remind you of your obligation to keep all data associated with your domain name up to date ([Terms and conditions](#)).

To access the system you can:

1- Enter the **ID and password**, which was assigned to register through Dominios.es.

Please enter them below:

Authentication form

ID: E.g.: AAAA0-ESNIC-F0

Password:

[Retrieve password](#)

[Authenticate](#)

2- **Authenticate** using your eID or certificate.

Please enter your eID in the card reader. [Authentication with certificate](#)

If you wish to change the email:

[Change email](#)

If you are not registered, you can do it in Dominios.es:

[Register in Dominios.es](#)

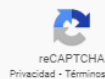
This option displays a screen with a form where you must indicate the identifier, fill in the Captcha and click on the "Continue" button.

Renew password

If you forgot your password, you can request to have emailed the link to the form where you set the new password. To do this, enter the identifier.

Identifier :

No soy un robot



[Return](#)

[Continue](#)

At that moment you will receive an email with a link to update your password.

Renew password

Will be sent an email to the account with a link to renew the password, you will need the ID 54830-ESNIC-F5 for activation

[Continue](#)

Dear Sir/Madam,

In this message indicate the link where you must go to renew your user password DOMINIOS.ES
[Renew password](#).

Sincerely,

DOMINIOS.ES
Public Business Entity Red.es

2. TWO FACTOR AUTHENTICATION ACCESS (2FA)

2.1. Two Factor Authentication by Email

You will receive an email containing the security code that you must use to verify the user to access the system.

Estimado Sr./Sra.,

Recientemente ha intentado acceder al portal de DOMINIOS.ES.

Complete el acceso con el código de seguridad indicado abajo:

299269

Este código expirará en **15 minutos** desde la recepción de este correo.

Atentamente,

DOMINIOS.ES
Entidad pública empresarial Red.es

Dear Sir/Madam,

You recently tried to log in to DOMINIOS.ES portal.

Complete your login with the security code below:

299269

This code will expire in **15 minutes** after you receive this email.

Yours faithfully,

DOMINIOS.ES
Public Business Entity Red.es

Once you enter it, you should click on "Verify".

Login

An email with the security code has been sent.

Enter the 2-Factor code:

[Back](#) [Verify](#)

2.2. Two Factor Authentication by App

You must open the application where you have the QR code saved and enter the indicated code.

Login

Check the code in the app.

Enter the 2-Factor code:

[Back](#) [Reset to "by mail"](#) [Verify](#)

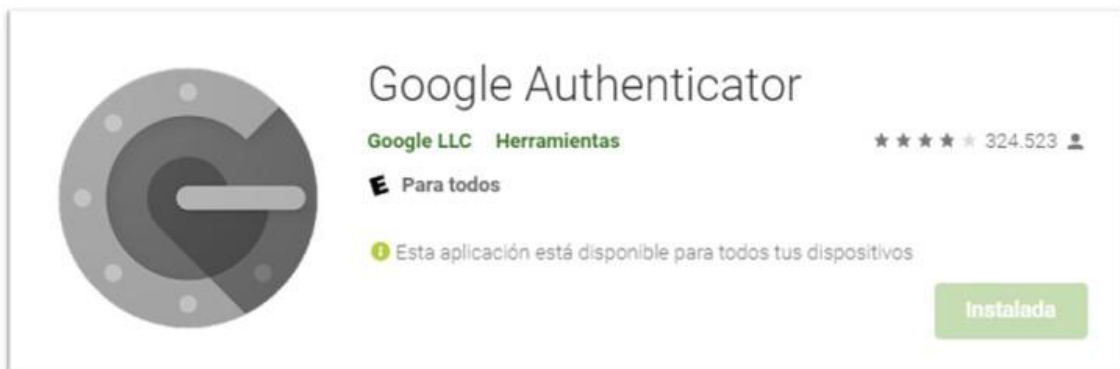
3. TROUBLESHOOTING

3.1. How to configure the Application?

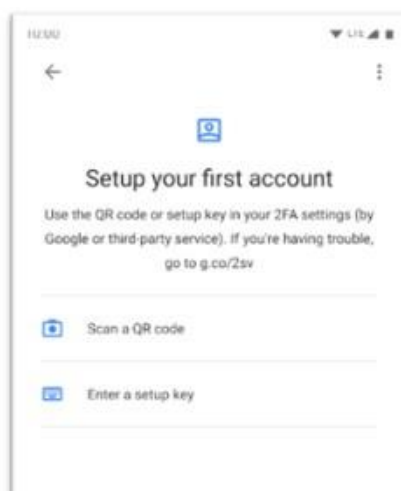
Recommendation: It is advisable that the mobile device has the date/time automatically configured, since in case it has been manually stored there could be an error.

In this case, the steps to configure the Google Authenticator application are indicated as it is the recommended one and is available in both the Play Store (Android) and App Store (iOS), but any other similar App can be configured for 2FA:

- 1) Download and install the Google Authenticator app



- 2) The application will open, and two options to enter an account will appear on the screen:



- 3) On the system page, both the QR code and the Setup Key will appear. It is recommended to use the QR code scan to avoid transcription errors when entering the Setup Key.



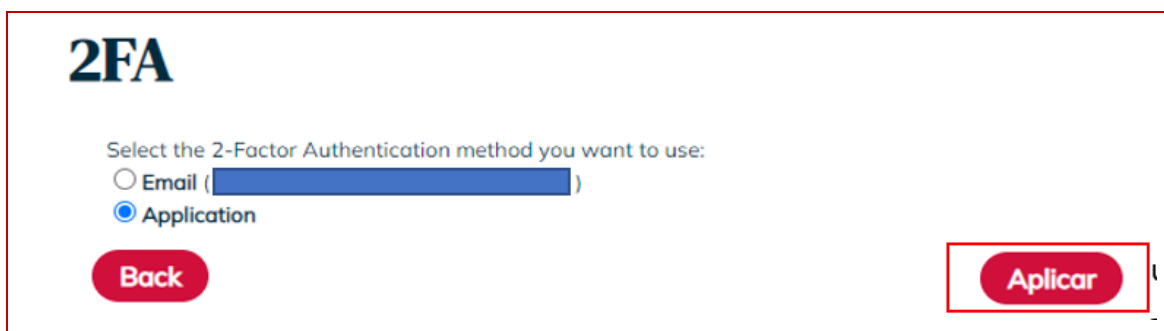
At the next login, the method will already be by Application and it will just be necessary to enter the number that appears in the Application.

3.2. How to change the Two Factor Authentication method?

To change the way by which you want to get the Two Factor Authentication security code, you should click on the "2FA" button in the header.

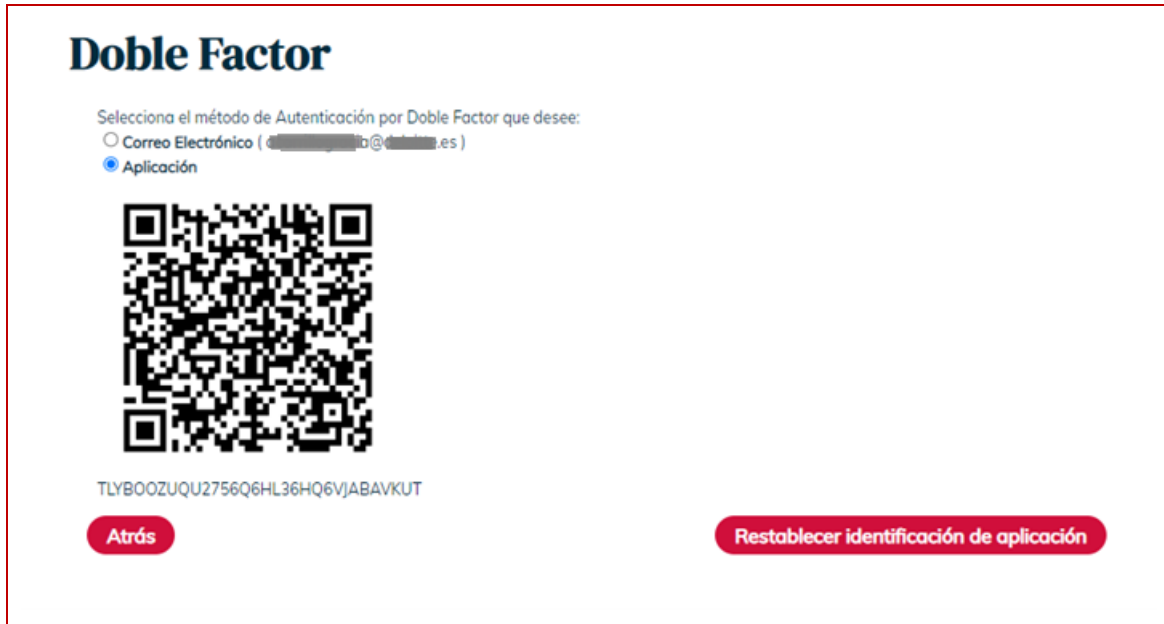


By default, the method will be by email, but it is possible to change it to by Application and click "Apply".



3.3. How to reset the QR code for Application?

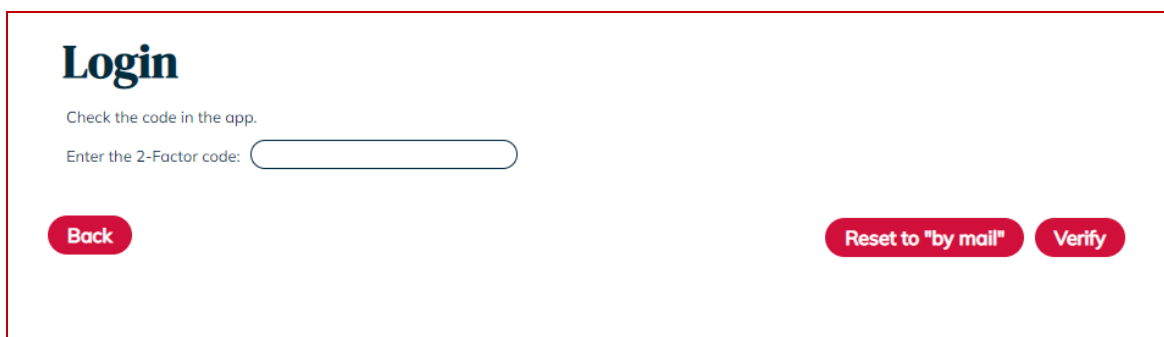
If you want to reset the QR code for any reason (loss, security, device change, etc), you only need to click on "Reset App code".



Warning: We recommend scanning the QR code instead of writing it, to avoid any transcription errors.

3.4. What to do if you lose the QR code for the Application?

In the event that the user has lost the QR code, it is possible to reset the Two Factor Authentication method to email by clicking on "Reset to by email".



3.5. How to change the email address?

In the event that the user does not have an access password or an email address to receive the password through the access password recovery process, a public email

change service is available, accessible from the login screen through the "Change email" option.

Login

WARNING: In order to comply with the new National Security Scheme (ENS), published in the Royal Decree 311/2022 of 3rd May, the ".es" Domain Names Registry has established a **two-factor authentication (2FA)** to be able to access the management of your domain. By default, the 2FA code **will be sent to the email address associated with your user**, but once you are logged into your account, you can also set it up through any application that generates 2FA codes, e.g. Google Authenticator. [\(2FA User Manual\)](#)

It is necessary that your **email address** is **operational** and **updated** in the Registry database. We remind you of your obligation to keep all data associated with your domain name up to date ([Terms and conditions](#)).

To access the system you can:

- 1- Enter the **ID and password**, which was assigned to register through Dominios.es.

Please enter them below:

Authentication form

ID: E.g.: AAAA0-ESNIC-F0

Password:

[Retrieve password](#)

[Authenticate](#)

- 2- **Authenticate** using your eID or certificate.

Please enter your eID in the card reader. [Authentication with certificate](#)

If you wish to change the email: [Change email](#)

If you are not registered, you can do it in Dominios.es: [Register in Dominios.es](#)

Once "Change email" is clicked, the following screen will appear:

Your domains

Email not accessible

Process

[Request email address change](#) The contact must be identified through one of the following ways:

- ID/Electronic certificate, the email change will be online.
- ID card photocopy, the email change will have to be checked and approved by our network operators.

[Return](#)

To continue with the process, you must click on "Request email address change" through which you access the screen of the email update process:

E-mail update process

Identifier :
New email :
New email confirmation

To modify a legal person must attach the Identification ID and the corresponding powers.

* Tamaño máximo de archivo 4MB :

Ninguno archivo selec.

Ninguno archivo selec.

* Allowed formats: .pdf, .doc, .txt, .jpg, .png, .tif, .rar, .zip y .br2

(Attach photocopy of the ID card)

You must enter the user identifier on which you want to make the change made and the new email address. Once these fields are completed, you must choose the method of processing the email change request:

- **Legal Entities:** they must attach documentation that proves the change of email in a single file through the processing option without eID/Certificate. The request will be pending of approval by a Red.es network operator.
- **Individuals:** they can choose to attach an image of their identity document or sign the request using a certificate. In the case of processing by means of a copy of the national identity document or the signature through a certificate that does not correspond to the user's identification, the request will be pending of approval by a Red.es network operator. In the case of signing the request using a certificate that corresponds to the user's identification, the change will be made automatically.

Once the data has been entered and a form of processing has been selected, click on "Finish request" and an email will be received later to confirm or deny (depending on the case) the requested modification.

3.6. Management of certificates for login

If the registered user has a unique ID number and the certificate contains that same ID number, the user will be able to login without the need to associate a certificate.

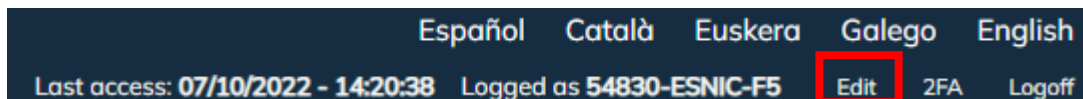
The user will be able to assign/unassign certificates in order to log in to the application with them.

A contact can only have one associated certificate, and said certificate must contain the same identification as the user.

The same certificate can be assigned to more than one contact at the same time. If this circumstance occurs, when logging in you can select the user with which you want to log in.

The certificates that will appear in the list for their possible association will be those that the user has previously loaded in their browser and are admitted by Red.es, and these may lose their validity even when associated (expiry, revocation...).

To modify the End User profile, you must access "Edit" in the menu displayed at the top of the application, and then access the "Login certificate management" button:



Edit contact details

Identifier: 54830-ESNIC-F5
 Contact Type: Persona Física
 Name:
 Identification (ID): NIF/DNI (spanish) - 0:
 E-mail:
 Voice: - (i.e.: +34 - 911234567)
Address
 Select country:
 Postal code:
 Postal Address:
 Change password:

Personal data provided through the following form will be registered in a file from the Public Company RED.ES (hereinafter RED.ES), settled at Edificio Bronce, Plaza Manuel Gómez Moreno, s/n, (28080) Madrid, to manage the condition of user of this service. You have the right to access, modify, object and cancel this data by addressing the Legal Advice RED.ES, at Edificio Bronce, Plaza Manuel Gómez Moreno, s/n, (28080) Madrid.

* Required fields

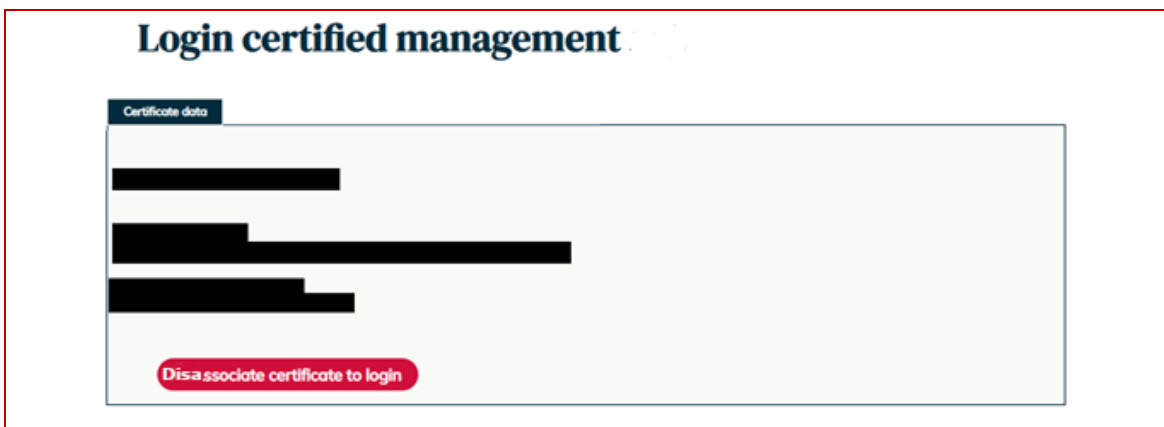
3.6.1. Associate Certificates

In this screen the user can assign a new certificate. When pressing Associate certificate for login, a screen will appear showing the list of certificates, in which the user can select the certificate they want to associate it with their contact.



3.6.2. Disassociate Certificates

On this screen there will be a button with which the user can unassign the previously associated certificate.



***Note:** For more detailed information on the procedures in the System, please check the corresponding End User or Accredited Registrar User Manual.