

TWO FACTOR AUTHENTICATOR

USER GUIDE

BNP PARIBAS SECURITIES SERVICES

NEOLINK

April 2021



BNP PARIBAS

The bank for a changing world

TWO FACTOR AUTHENTICATOR (2FA)

Smartphone Set-Up

You will need to go to the App Store on your smartphone and download an authenticator application which supports time-based **one time passwords (OTP)**.

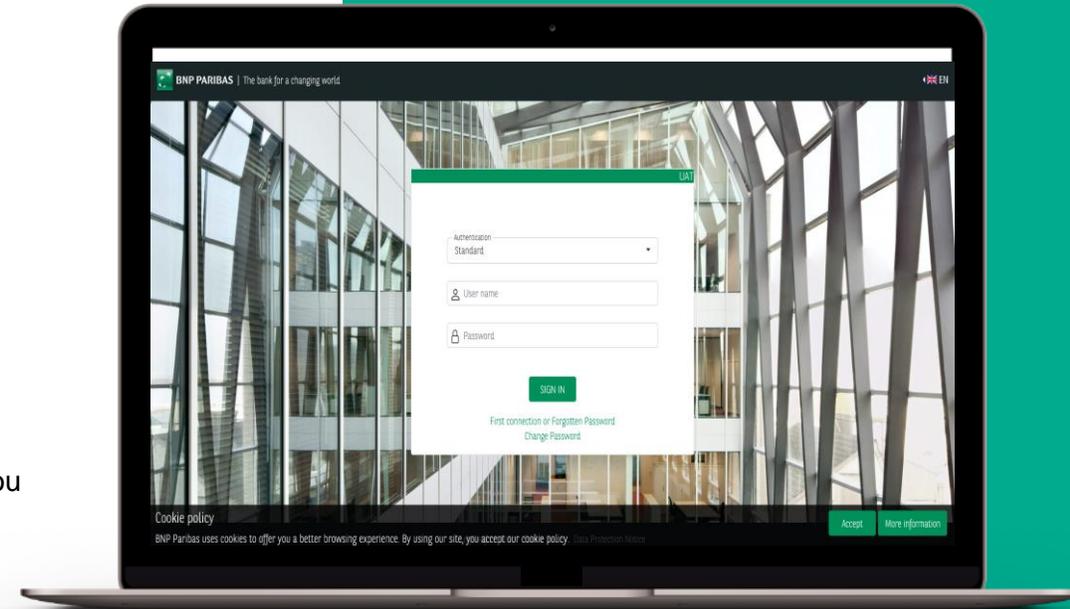
Listed below are a sample of authenticator applications available for both Android and iPhone smartphone users:

- Authy 2-Factor Authentication
- Duo Mobile
- Google Authenticator
- IBM Authenticator

On opening the app you will be required to scan the QR code or manually enter the secret key provided (you will have 90 seconds to enter the 32 characters).

You will only be required to do this once for the initial set-up of 2FA.

On entering the **one time password** provided by your application, click to submit and complete your registration.



This does not replace in any way the password and hard token offering - our clients will be able to decide going forward how the users should authenticate:

- **Password** – Recommended for users with read-only access.
- **Secure ID (hard token)** – Required for user with instruction access and clients who are not ready to migrate to soft token.
- **Soft Token** – New offering to use Two Factor Authenticator, it works for both read-only and instruction access.

“Two-factor authentication works as a second security layer, that will re-confirm your identity helping to reduce hacking and risks of fraud”



TWO FACTOR AUTHENTICATOR (2FA) – One-time password enrollment

UAT

Authentication
Standard

User name

Password

3 **SIGN IN**

First connection or Forgotten Password
Change Password

This screenshot shows the initial login interface. A dropdown menu is set to 'Standard'. The 'User name' and 'Password' fields are highlighted with a green box and labeled '2'. A green arrow labeled '3' points to the 'SIGN IN' button. Below the button, there are links for 'First connection or Forgotten Password' and 'Change Password'.

For this process you should have already downloaded the authenticator application of your choice on your device (smartphone).

1 Select **Standard** as the authentication method

2 Input the **User ID and Password** provided in the First Authentication email sent by BNP Paribas.

4 In the next screen the system will display a QR Code – open the authenticator app on your device and **Add the account**, the application will request to access your camera

One Time Password Enrolment

An authenticator app generates the code automatically on your smartphone. If you don't already have one, look for an app that supports time-based one-time passwords (TOTP). Open the application and scan the QR code.

If you can't scan the code, [enter your secret key manually](#)

Enter the one-time code provided by your application and click Submit to complete registration.

Token

Submit

This screenshot shows the 'One Time Password Enrolment' page. It contains a QR code for scanning. Below the QR code, there is a link to 'enter your secret key manually' and a text prompt to 'Enter the one-time code provided by your application and click Submit to complete registration.' A 'Token' input field with a password icon and a 'Submit' button are at the bottom.

5 Place the phone in front of your monitor so the QR code is scanned. Once registered, the application on your phone will display a 6-digit code.

6 Input the **6-digit code** in the Token section and click on **Submit**

BNP PARIBAS
SECURITIES SERVICES

soft.token@test.com token is:

111 093

Your token expires in **24**

This screenshot shows the authenticator app interface. It displays the BNP Paribas Securities Services logo, the email address 'soft.token@test.com', and a 6-digit token '111 093'. Below the token, it indicates 'Your token expires in 24'.



TWO FACTOR AUTHENTICATOR (2FA) – One-time password use

For all subsequent logins you will need to open the authenticator application on your smartphone or desktop and follow these steps:

UAT

Authentication
Standard

User name

Password

3 → SIGN IN

First connection or Forgotten Password
Change Password

1 Select **Standard** in the authentication method

2 Input the **User ID and Password** provided in the First Authentication email sent by BNP Paribas.

UAT

One Time Password

Token

Reset OTP ?

OK Cancel

4 Open your authenticator app, input the 6 digits code in the Token field and click on **Submit**



HOW TO REQUEST 2FA FOR YOUR NEW USERS?

Reminder: please make sure you have validated with your IT security services that you are authorised to use authentication applications on your devices.



Home > Solutions > Admin > Client set up > Manage users > Users list

USERS LIST

Go to Manage Users' screen and click on **Create a request** as usual

SEARCH
Not active

0 results

Export Modify Copy Reactivate Deactivate

Select the number of users to create

1

CREATION TYPE

Free

From a user copy

Search and select a user to copy.
Start typing 3 characters to get a list of possible matches

CODE	LAST NAME	FIRST NAME
090020	TESTS LOADRN 21	Frenon

AUTHENTICATION

Strong authentication

SecurID Soft Token

Once in the form, make sure to select the strong authentication option to have the options displayed – continue the request process as usual by adding subscription, rights, perimeter, etc.

New option when selecting **Strong Authentication** – select **SecurID for physical token** to be sent to the user's address or **Soft Token (for 2FA)**



HOW TO REQUEST 2FA FOR EXISTING USERS?

Go to Manage users screen, look for the user and click on **Modify** as usual



Reminder: please make sure you have validated with your IT security services that you are authorised to use authentication applications on your devices.

500 results

Export + Modify Copy Reactivate Deactivate

Multi-column sorting ^ Status X ^ User code X

<input type="checkbox"/>	REQUEST	USER CODE	LAST NAME	FIRST NAME	EMAIL
--------------------------	---------	-----------	-----------	------------	-------

User Prenom TESTS LOADRN 21 Identifier: 090020

Email *

none@bnpparibas.com

Confirm email

none@bnpparibas.com

Last name *

TESTS LOADRN 21

Phone number *

00001

Time zone *

Europe/Liban

Strong authentication

SecurID Soft Token

2

Once in the form, in the tab **Information** make sure to select the strong authentication option to have the options displayed as below

Select **Soft Token** and click on save. This will create a new request and the user profile will be updated. You will receive a notification and the user will receive an email with further instructions for first authentication.



YOUR CONTACTS FOR MORE INFORMATION

Neolink Support EMEA (UK/Germany/Channel Islands)

bp2s_neolinksupport_emea@bnpparibas.com

+44 (0) 207 410 1026 (English)

+49 (0) 69 1520 5751 (German)

Neolink Support Luxembourg

neolink_support_lux@bnpparibas.com

+352 2696 2500

Neolink Support Spain

bp2s_neolink_spain@bnpparibas.com

+34 91762 5149 / +34 91762 5242 / +34 91762 5133

Neolink Support Italy

bp2s_neolink_italy@bnpparibas.com

+39 02 7247 4254 / +39 02 7247 4135

Neolink Support France

neolink.support.fr@bnpparibas.com

+39 02 7247 4254 / +39 02 7247 4135

Neolink Support Asia

bp2s_neolinksupport_asia@bnpparibas.com

+91 44 71 1234 56

Neolink Support Australia and New Zealand

bp2s_neolink_ausnz@bnpparibas.com

Australia: +61 2 8116 0500

New Zealand: +64 4 439 2198

Neolink Support Americas

bp2s_neolink_americas@bnpparibas.com

US: +1 201-850-5060

LatAM: +571 651 6440

