

Two-Factor Authentication (2FA)

Since now, access to the computing resources with **2FA** is required.

All the computing services where the access with IPA is needed such as **HPC login system, Nextcloud, Confluence, Indico or the OpenStack Dashboard** need to access with the "**Password+OTP code**" (all in a row, without the "+" symbol).

The OTP code is a one-time password, also known as a dynamic password, used as a second authentication factor in addition to the commonly used username and password. It is only valid once, so even if an attacker manages to get hold of it, he/she cannot reuse it.

To enable this method in freeipa, must follow the next steps:

1. Install an App such as Authy or similar app for OTP generator (Google Authenticator or Microsoft Authenticator, FreeOTP, ... [alternative apps page](#)), to your **Mobile Device**.



Authy



Microsoft Authenticator

[blocked URL](#)

[blocked URL](#)

[blocked URL](#)

[blocked URL](#)

[blocked URL](#)

This application will give us the OTP codes generated through the token created, this code will change every 30sg and will be valid only once.

Note: RSA authenticator (SecurID) application gives some problems.

2. Login as usual at IFCA Auth System (<https://auth01.ifca.es> or <https://auth02.ifca.es>) using your credentials (User / Password)

2. This is your user area

freelPA

Users | OTP Tokens

User: [Name]

[Refresh] [Revert] [Save]

Identity Settings

Job Title: [Text]

First name *: [Text]

Last name *: [Text]

Full name *: [Text]

Display name: [Text]

Initials: [Text]

Car License: [Text]

Contact

Email address: [Text]

Telephone Number: 942200969

Pager Number: [Text]

Mobile Telephone Number: [Text]

Fax Number: [Text]

3. As a user, access to the token area

freelPA

Users | **OTP Tokens**

User: [Name]

[Refresh] [Revert] [Save]

Identity Settings

Job Title: [Text]

First name *: [Text]

4. As a user, add the OTP token.

freelPA

Users | OTP Tokens

OTP Tokens

Search [Input]

[Refresh] [Delete] **[Add]** [Disable] [Enable]

<input type="checkbox"/>	Unique ID	Owner	Status	Description
<input type="checkbox"/>				

5. Add the new token and you will generate the QR code that you will have to scan with your chosen mobile device App (Section 1 - Install an App)

Add OTP Token ✕

Type Time-based (TOTP) Counter-based (HOTP)

Description

* Required field

Add
Add and Add Another
Add and Edit
Cancel

6. You will see the QR code or token that you need to enter in your mobile app (Installed in step 1 - Authy, Google Authenticator, Microsoft Authenticator, FreeOTP, ...).

7. Now you will see your token created and enable in your user area

freeIPA

Users | **OTP Tokens**

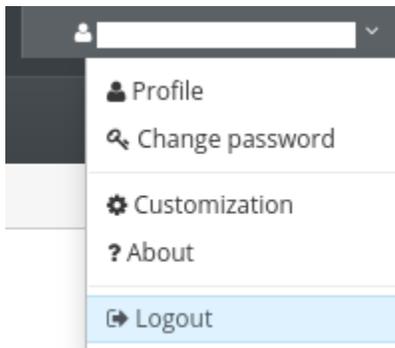
OTP Tokens

Search

Unique ID	Owner	Status	Description
<input type="checkbox"/>		▼ Enabled	OTP token for IFCA services

Showing 1 to 1 of 1 entries.

8. Logout freeipa



9. OTP Token Synchronization

Before you can log in with 2FA for the first time, you must **synchronize the OTP token**. For this purpose, in the login window to the IPA server, select the Sync OTP Token option .

freelPA
Open Source Identity Management Solution

Username *

Password *

Login Using Certificate Sync OTP Token Login

10. Fill in the username and your password, then enter the first code that appears in the Authy/OTP App in the First OTP field and the next code (appearing after 30sg) in the Second OTP field.

freelPA

Username *

Password *

First OTP *

Second OTP *

Token ID

One-Time-Password(OTP): Generate new OTP code for each OTP field.

Cancel Sync OTP Token

11. How to use OTP Token Synchronization

Now when you try to access to IFCA systems you must enter your passwd followed by the OTP code showed in the **Authy/OTP app**.

freelPA

Username *

Password *

Passwd TOTP

Login Using Certificate Sync OTP Token Login

If you have any questions, please contact us at [computing.support@ifca.unican.es]