How to connect via 2FA

Two-factor authentication (2FA) refers to an **authentication method** in which a user is granted access to the CINECA HPC systems only after successfully **presenting two pieces of evidence** (or factors). Verifying your identity, using an independent second factor, prevents other users from logging in with your identity, even if they have the password. Therefore, two factor authentication (hereafter 2FA) adds a **further level of security** to the authentication for access to services based on the Identity Provider.

The new access mode proposed is entirely transparent to the user, who continues to use the ssh client as usual. Before connecting to the cluster you have to **request the ssh certificate** to our Identity Provider (IP) via the smallstep client. A web page will be automatically opened on the browser and you will be asked to **authenticate to our IP by inserting an OTP**. Once the authentication has taken place, the server will issue a time-limited **certificate valid for 12 hours** through which you can connect to CINECA systems via SSH client (just ssh to the cluster login). After 12 hours a new certificate needs to be generated using smallstep client.

First access

If this is the **first access** and you need to **activate the 2FA** following the steps below:

- register on our Identity Provider and configure the OTP
- Install and configure the smallstep client on your local PC

Warning: For services which authentication is done via web, such as **Adacloud,** there is **no need** to install and configure smallstep. At login time the website will ask the password and the OTP to access.

After your first access, you can manage from our Identity Provider website (https://sso.hpc.cineca.it) all the issues related to the authentication to our CINECA clusters. For example:

- reset password
- re-configure the OTP on your smartphone
- generate new Recovery Authentications codes

Access to the systems

If you have already activated the 2FA and configured the smallstep client, and you have **downloaded the temporary certificate** you can login to the CINECA cluster via the usual ssh protocol

```
ssh <username>@login.<cluster>.cineca.it
```

You will be directly logged into the cluster **without having to insert the password**.

If you would like to connect via Remote Connection Manager (RCM) once downloaded the temporary certificate, as for the ssh login, you can login following the same instructions as before with the exception that you don't have to insert the password in the login page.

Table of contents: