Introduction to two-factor authentication (2fa) on CINECA HPC clusters

June 7th, 2023
Francesco Talpo – f.talpo@cineca.it
Summary

- How to activate 2FA for HPC access and configure the mobile authenticator
- How to connect to the HPC clusters with SSH certificates using Smallstep
- How to recover HPC password and OTP generator
- FAQs and common problems
Registering to the Identity Provider

Three possible scenarios:

1 – You have a valid CINECA HPC username and password

2 – You have a valid HPC username, but your password is expired, or you forgot it

3 – You are registering as a new HPC user
1 – Registering to the Identity Provider with a valid CINECA HPC password

Authenticate on our new Identity Provider at:  https://sso.hpc.cineca.it

using username and password you use to connect to CINECA clusters
At the first login you will be forced to:

- verify your email
- change the password
- configure your One-Time Password (OTP) code

An e-mail containing a link will be sent to the e-mail address indicated into the UserDB site:

Subject "CINECA HPC Single Sign On: verify your email"
2 – Registering to the Identity Provider WITHOUT a valid CINECA HPC password

Write to superc@cineca.it, and we will send you the link (with a validity of 12 hours) to verify your e-mail address and register to the Identity Provider

3 – Registering to the Identity Provider as a new CINECA HPC user

You can register following the procedure reported on the User Guide, and you will receive, in two separate e-mails, the username and the link for e-mail verification and for registering to the Identity Provider
How to activate 2FA and configure the OTP

Following the link received in the e-mail you will be forced to change the password:

The new defined password will replace the password used to login to CINECA cluster
How to activate 2FA and configure the OTP

Please refer to the policy for password definition on our User Guide; specifically:

• The new password must be 10 characters long and contains at least 1 capital letter, 1 number, and 1 special character ("#$%&'()*+,-./;:<=>?@[\]^_`{|}~)

• The password has a validity of 3 months. You will receive a reminder 10 days before the expiration when you login.

• The new password must be different from the previous 5 ones.

• Any password change will be notified to the user by email.

WARNING: in this case the process will fail silently without any error.
How to activate 2FA and configure the OTP

Next step after the definition of the new password is the activation of the 2FA via OTP following these simple steps:
How to activate 2FA and configure the OTP

First step: install on your mobile an App to generate authentication codes:
- FreeOTP
- Google Authenticator
- other

Second step: once the app is installed, you can use your authenticator to scan the QR code shown in the page. The OTP will be automatically configured on your authenticator.

Third step: you will be asked to insert the 6 digits code that appears on the App to verify the correct configuration. If you have multiple OTP defined in the App, the correct one has the name "CINECA HPC: <your username>".

If you have problems in configuring the 2FA on your smartphone, contact us at: superc@cineca.it
Once the configuration is complete the subsequent page will show you the **Recovery codes**.

Please **save these codes somewhere** by downloading, printing or copying them in a text file.

These codes are requested to the user in case of problems in the OTP configuration (issue with the app or smartphone lost) so they are very important (**ALL** of them).

They are **one-shot** codes, and more can be generated.

**Now 2FA and OTP are enabled and configured.**
Summary

- How to activate 2FA for HPC access and configure the mobile authenticator
- How to connect to the HPC clusters with SSH certificates using Smallstep
- How to recover HPC password and OTP generator
- FAQs and common problems
How to configure SSH access to the HPC Clusters

HPC clusters can be accessed through SSH with a temporary certificate obtained via the smallstep software. You can setup the smallstep client in several ways:

- Either follow the instructions on the Smallstep website
- Or download an executable from the official GitHub repository

!! WARNING !!

Some Linux distributions (Ubuntu ...) may have a completely different "step" package available in the distribution's official repositories;

DO NOT INSTALL IT UNLESS SURE THAT IT'S THE SAME SOFTWARE, OTHERWISE IT MAY LEAD TO ERRORS
How to configure SSH access to the HPC Clusters – Linux/MacOS

Configure the smallstep client for SSH access with the following commands:

- Get the CA certificate:
  
  ```
  $ step ca bootstrap --ca-url=https://sshproxy.hpc.cineca.it --fingerprint 2ae1543202304d3f434bd1a2c92eff2cd2b02110206ef06317e70c1c1735ecd
  ```

- Activate the ssh-agent:
  
  ```
  $ eval $(ssh-agent)
  ```

- Get the temporary certificate:
  
  ```
  $ step ssh login '<user-email>' --provisioner cineca-hpc
  
  <user-email> IS THE USERDB MAIL ADDRESS
  ```
How to configure SSH access to the HPC Clusters – Linux/MacOS

You will be redirected to a web page asking for your **HPC credentials** (username, password) and OTP:

At this point, the temporary certificate will be passed to the ssh-agent, and you will be able to connect to the cluster via SSH.
How to configure SSH access to the HPC Clusters – SSH keys

Alternatively, the command:

$ step ssh certificate 'user-email' --provisioner cineca-hpc my_key

Followed by the same login procedure on the Identity Provider page

Will download to your system a pair of public/private ssh keys with a limited validity of 12 hours.
How to configure SSH access to the HPC Clusters – SSH keys

If you passed "my_key" as the last argument to the previous command, you will find the files "my_key", "my_key.pub" and "my_key-cert.pub" in your current directory.

Only "my_key" and "my_key-cert.pub" are needed to access the cluster, which can be done:

With the command: `ssh -i my_key <user>@login.<cluster>.cineca.it`

passing the correct identity directly to the ssh command

Or with the commands:

`ssh-add my_key`

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

which will add the key to the ssh agent before connecting to the cluster
How to configure SSH access to the HPC Clusters – Windows

For Windows some of the commands are slightly different:

1. Get the CA certificate:
   ```
   > step ca bootstrap --ca-url=https://sshproxy.hpc.cineca.it --fingerprint 2ae1543202304d3f434bdc1a2c92eff2cd2b02110206ef06317e70c1c1735ecd
   ```

2. Activate the ssh-agent:
   ```
   > Get-Service -Name ssh-agent
   > Start-Service -Name ssh-agent
   ```

3. Get the temporary certificate:
   ```
   > step ssh login '<user-email>' --provisioner cineca-hpc
   ```
How to configure SSH access to the HPC Clusters – Windows

If, when activating the ssh agent, these commands don't work:

> Get-Service -Name ssh-agent
> Start-Service -Name ssh-agent

the following commands need to be executed in a Powershell instance with admin rights:

> Set-Service -Name ssh-agent -StartupType Auto
> Start-Service ssh-agent
How to configure SSH access to the HPC Clusters – Windows

Alternatively on Windows it is possible to install WSL2 ([https://learn.microsoft.com/en-us/windows/wsl/install](https://learn.microsoft.com/en-us/windows/wsl/install)) and configure the subsystem following the instructions for Linux.

In this case, to share the certificate between WSL tabs, the following lines can be added to `.bashrc`:

```bash
if [ -f ~/.bash_agent ]; then
  . ~/.bash_agent
fi
steptest=$(step ssh list --raw '<user-email>'| step ssh inspect | grep "Valid")
if [ -z "$steptest" ]
then
  eval $(ssh-agent)
  echo "export SSH_AUTH_SOCK=$SSH_AUTH_SOCK" > ~/.bash_agent
  echo "export SSH_AGENT_PID=$SSH_AGENT_PID" >> ~/.bash_agent
  step ssh login '<user-email>' --provisioner cineca-hpc
fi
```
How to configure SSH access to the HPC Clusters – Useful commands

- You can check for the presence of a valid certificate, in both Linux/MacOS and Windows systems, with the commands:
  ```
  > ssh-add -L
  > step ssh list
  ```

- And, to display the validity of the certificate, you may run the command:
  ```
  > step ssh list --raw '<user_email>' | step ssh inspect
  ```

- If you want to "clean" the ssh-agent memory from any memorized key and certificate you can do so with the command:
  ```
  > ssh-add -D
  ```
Summary

- How to activate 2FA for HPC access and configure the mobile authenticator
- How to connect to the HPC clusters with SSH certificates using Smallstep
- How to recover HPC password and OTP generator
- FAQs and common problems
How to reset the HPC password – ONLY IF ALREADY REGISTERED ON "sso.hpc.cineca.it"

The new Identity Provider system allows users to recover their HPC password: you can do so by clicking **Forgot Password?** on the Identity Provider login webpage.

You will then receive an e-mail with a **temporary link** for password reset.
How to reset the HPC password – ONLY IF ALREADY REGISTERED ON "sso.hpc.cineca.it"

If you just need to change your password, you can do it by clicking on the My Password - Update button in the Account Security section of your Identity Provider page at https://sso.hpc.cineca.it

NOTE: the passwd command has been disabled on the clusters
How to recover the OTP generator

If you lose your OTP generator, you can reset it by clicking on **Forgot Password?** in the **Identity Provider login** page, then following the link received via e-mail and then clicking on **Try Another Way** when prompted for the OTP code.

If you have any issues with these procedures, you can contact us at: **superc@cineca.it**
How to recover the OTP generator

You will then be asked to insert a specific code from the Recovery codes that you were provided with during the registration with the Identity Provider (https://sso.hpc.cineca.it)
Summary

- How to activate 2FA for HPC access and configure the mobile authenticator
- How to connect to the HPC clusters with SSH certificates using Smallstep
- How to recover HPC password and OTP generator
- FAQs and common problems
FAQs and common problems

Q: I forgot my password, or it is expired, but "Forgot your password?" takes me to this page ->

A: you can see the "Forgot password?" link even if you're not registered to the Identity Provider, but it will be broken like this.
Write to superc@cineca.it to get your registration link.
Q: Trying to install smallstep through scoop on Windows, but the commands
scoop bucket add smallstep https://github.com/smallstep/scoop-bucket.git
scoop install smallstep/step
don't seem to install "step.exe" in my PATH?

A: make sure that you're launching the two commands separately.
Look for the "step.exe" file and if you find it, make sure that its directory is in the system's PATH.
Q: How can I connect to CINECA HPC clusters from a machine on which Network access has been restricted and a web browser is not available?

A: You can refer to the How to configure SSH access to the HPC Clusters – SSH keys section of the presentation; You can generate a pair of public/private keys on a computer with an available browser and transfer them to the machine from which you intend to connect to CINECA's clusters.
FAQs and common problems

Q: I have too many ssh keys memorized in the ssh agent and the ssh connection does not work?

A: having more than 5 ssh keys in a single ssh agent may lead to connection problems. Common workaround is to pass the identity to the ssh command through the –i flag.

It is not possible to do so while using the agent-embedded certificate; you will need to download the public/private keys as described in the How to configure SSH access to the HPC Clusters – SSH keys section of the presentation.