
Newsletter CORE - Nouveautés pour la recherche - février 2025

À partir de Équipe CORE <informatique@centralesupelec.fr>

Date Mer 19/02/2025 17:59

À Margot Roussat <margot.roussat@centralesupelec.fr>

Newsletter CORE

Nouveautés pour la recherche

English version below

Mise en place d'une nouvelle passerelle SSH

Une nouvelle passerelle SSH, **sshgw.centralesupelec.fr**, est désormais disponible en remplacement de l'ancienne plateforme devenue obsolète (sshgw.ecp.fr).

Le service de passerelle SSH a pour fonction de vous donner accès aux ressources et réseaux internes de votre laboratoire, ainsi qu'aux centres de calcul nationaux.

Pour utiliser cette nouvelle passerelle, vous devez :

- Renseigner votre clé SSH publique dans l'espace "Mon accès SSH" sur **MySchool Research**
- Faire partie de l'équipe MyAdmin accordant l'autorisation de connexion à la passerelle SSH. Cet accès est géré par la ou le correspondant informatique de votre laboratoire, ou à défaut par le directeur ou la directrice.

Si vous utilisez déjà la passerelle SSH pour vous connecter aux centres de calcul nationaux via sshgw.ecp.fr (138.195.9.7), n'oubliez pas de mettre à jour vos informations pour utiliser la nouvelle adresse (138.195.193.14).

Mon accès SSH ⓘ

Aucune clé SSH enregistrée

[Ajouter une clé SSH](#)

Vous pourrez vous connecter à la passerelle SSH via :
██████████@sshgw.centralesupelec.fr

Pour toute question ou assistance sur ce sujet, envoyez un email à informatique@centralesupelec.fr.

Connexion au VPN



Pour accéder à certains services de CentraleSupélec ou ressources de votre laboratoire, vous pouvez avoir besoin du VPN OpenVPN (Windows) ou TunnelBlick (MacOS) fourni par la DISI.

Une fois le VPN configuré sur votre poste, vous devez utiliser **votre adresse email CentraleSupélec** et non votre login court pour vous connecter au service.

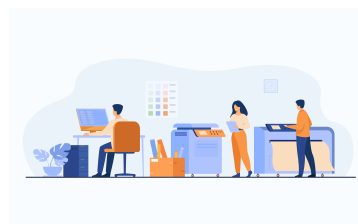
Pour plus d'informations sur le VPN à CentraleSupélec, rendez-vous sur MyCS.

[En savoir plus](#)

Imprimer depuis son navigateur web

Pour imprimer vos documents sans utiliser le système d'impression installé sur votre ordinateur, vous pouvez les envoyer sur le [webserveur Printweb](#) en suivant la procédure "Méthode 2 : utiliser le service Printweb" disponible sur [cette page MyCS](#).

N.B : les impressions à partir d'une clé USB ne sont pas autorisées.



[En savoir plus](#)

Rappel sur la double-authentification



A la suite de la cyberattaque des systèmes de Paris-Saclay, CentraleSupélec a mis en oeuvre des mesures pour prévenir tout impact similaire sur nos infrastructures, parmi lesquelles la mise en place de la **double authentification pour l'ensemble des comptes informatiques de CentraleSupélec**.

Si vous n'avez pas encore activé la double authentification sur vos comptes (SOG, Microsoft et NextCloud), **nous vous invitons à le faire dès que possible en suivant les procédures ci-dessous**.

Si vous ne souhaitez pas utiliser Microsoft Authenticator, vous pouvez opter pour d'autres solutions telles que :

- KeePassXC disponible sous Windows, MacOS et Linux
- FreeOTP disponible sur l'App Store et Google Play

Nous vous invitons à vous adresser à votre correspondant informatique afin de connaître la politique de sécurité appliquée dans votre laboratoire

Pour les personnes n'ayant pas encore activé la double authentification, notamment sur SOGo, celle-ci sera automatiquement mise en place sur leur compte dans les deux prochaines semaines. Nous vous recommandons d'anticiper cette activation en suivant les procédures dès maintenant, afin d'assurer une transition fluide et éviter tout problème de connexion imprévu.

Accéder aux procédures

Implementation of a new SSH gateway

A new SSH gateway, sshgw.centralesupelec.fr, is now available to replace the old platform, which has become obsolete (sshgw.ecp.fr).

The SSH gateway service allows you to access internal resources and networks of your laboratory, as well as national computing centers.

To use this new gateway, you must:

- Provide your public SSH key in the "My SSH Access" section on [MySchool Research](#).
- Be part of the MyAdmin team that grants permission to connect to the SSH gateway. This access is managed by your laboratory's IT correspondent or, if your laboratory don't have one, by its director.

If you are already using the SSH gateway to connect to national computing centers via sshgw.ecp.fr (138.195.9.7), make sure to update your information to use the new address (138.195.193.14).

For any questions or assistance regarding this subject, please send an email to informatique@centralesupelec.fr.

My SSH access ⓘ

No SSH key registered

[Add a SSH key](#)

You can connect to the SSH gateway with :
[redacted]@sshgw.centralesupelec.fr

VPN connection



To access some of CentraleSupélec services or your laboratory's resources, you may need to use the OpenVPN (Windows) or TunnelBlick (macOS) VPN provided by the DISI.

Once the VPN is set up on your device, you must use **your CentraleSupélec email address** instead of your short login to connect to the service.

For more information about the VPN at CentraleSupélec, visit MyCS.

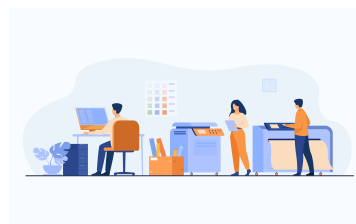
[Learn more](#)

Printing from your browser

Pour imprimer vos documents sans utiliser le système d'impression installé sur votre ordinateur, vous pouvez les envoyer sur le **webserveur Printweb** en suivant la procédure "Méthode 2 : utiliser le service Printweb" disponible sur **cette page MyCS**.

N.B : les impressions à partir d'une clé USB ne sont pas autorisées.

To print your documents without using the printing system installed on your computer, you can upload them to the **Printweb web server** by following the procedure "Méthode 2 : utiliser le service Printweb" available on **MyCS**.



Note: Printing from a USB drive is not allowed.

[Learn more](#)

Reminder about two-factor authentication



Following the cyberattack on the Paris-Saclay systems, CentraleSupélec has implemented measures to prevent any similar impact on our infrastructure, including the **implementation of two-factor authentication for all CentraleSupélec accounts**.

If you have not yet activated two-factor authentication on your accounts (SOG, Microsoft and Nextcloud), **we encourage you to do so as soon as possible by following the procedures below**.

If you prefer not to use Microsoft Authenticator, you can use the following alternatives:

- KeePassXC, available on Windows, MacOS, and Linux
- FreeOTP, available on the App Store and Google Play.

We invite you to reach out to your IT referent to learn about the security policy in place in your laboratory.

For those who have not yet activated two-factor authentication, especially on SOGo, it will be automatically set up on their accounts in the 2 next weeks. We recommend you to anticipate this activation by following the procedures now to ensure a smooth transition and avoid any unexpected connection issues.

Access the procedures

Cordialement, l'équipe DISI

Pour toute question ou suggestion, contactez : informatique@centralesupelec.fr
