



Login Rules.

All members of the staff at the Campus de excelencia UAM-CSIC (from here on, just “the Campus”) have the right to login in the CCC-UAM.

The application to login must be fulfilled at the CCC-UAM webpage.

Applicants are required to be in possession of an institutional e-mail address managed by the UAM or by one of the associated institutes. Otherwise, the applicant must provide the pertinent documentation to prove their affiliation to the Campus.

Documentation that proves vinculation to the Campus can be required from the users at any given time.

The validity status of the CCC-UAM account is subject to the user’s vinculation to the Campus.

Members of the staff responsible for interns, visitor professors and other temporal personnel are required to inform of the end of vinculation to the Campus if the situation arose before the expected date.

Any change in the following data must be communicated to the CCC-UAM administrators: affiliation, address, phone number and e-mail address.

Passwords must be changed at least once every six months. The first password, provided by the CCC-UAM administrators, must be changed within seven days of its reception.

In the event that the CCC-UAM has justified motive to suspect that a login has been compromised, they have the right to request a password change and temporally disable the login.

The login are to be used in the development of research projects. Users are prohibited to execute programs with goals not contemplated by the CCC-UAM.

All installed programs must be legal and in possession of a valid license.

The ownership of a login is restricted to a single user, being explicitly prohibited its usage by more of one person. The CCC-UAM will generate as many accounts as are needed to maintain functionality without the need to share login information.

The services of the CCC-UAM must be accessed only through the established servers. Access to any other server of the CCC-UAM is explicitly prohibited.

Connection to the CCC-UAM will only be available to systems with IP address granted by the Universidad Autónoma de Madrid, starting with 150.244. In the event that there is a need to connect from another IP address, the user may use the VPN service provided by the Information Technology department. This service is not provided or managed by the CCC-UAM.



The execution of jobs outside the queuing system is explicitly prohibited, with the exception of graphical jobs that, due to their nature, cannot be sent to the aforementioned system.

The usage of graphic programs will be limited by time and percentage of required CPU.

The maximum time of inactive connection is 4 hours. From that time on, the connection may be severed at any given moment.

The deletion of a login may be requested by an e-mail to the CCC-UAM administrators. Data belonging to the login will be exclusively given to the associated user, given that this user does not authorize a third party the access to the data.

Access to another user's data is prohibited if the owner of the data has not explicitly provided authorization.

Any malpractice or violation of these rules will entail the temporal or definitive block of the login and the involvement of the authorities in case of suspicion of criminal activity.