

# CoCoA for the MFA Cohortium

## CoCoA for the MFA Cohortium

The MFA Cohortium will be utilizing a CoCoA-based platform for its Sympa electronic mail lists and Confluence wiki spaces, with other collaboration services to be added in the future. CoCoA enables administration of users and groups using these services from a single interface, as well as allowing for delegation of administration of subgroups within the larger Cohortium project. See [Background on CoCoA](#) below, for more information.

The Cohortium's current services are:

- MFA Cohortium Wiki: <https://wiki.cohortium.internet2.edu>
- MFA Cohortium Registry: <https://registry.cohortium.internet2.edu/registry>

To register to use the CoCoA platform, click [<here>](#) and you will be guided through the process.

Both the Registry and the Wiki have a federated login interface, that is, you need an account with an [InCommon Identity Provider](#) to log into each of the applications. If you don't have such an account, you can use a Google account (if you have one).

To access either the MFA Cohortium Registry or the MFA Cohortium Wiki, your Identity Provider (IdP) must release the eduPersonPrincipleName (ePPN) attribute. Contact your site's help desk or technical support unit and point them to a technical resource that shows them [how to configure an IdP to release attributes to Cohortium SPs](#). If you use Google to access Cohortium resources, the necessary attributes will be automatically provided.

## Background on CoCoA

Collaboration is at the very center of the R&E mission, with inter-institutional and international engagements a very common characteristic. To make such collaborations effective both technically and from a user perspective requires three components:

1. A set of collaboration apps such as wikis, lists, calendaring (ad hoc and event), and conferencing, etc. These applications should have their identity and access needs met through open interfaces (API's, SAML assertions, LDAP, etc.). The use of open protocols allows the focus to be on the community groups and access control that are the payloads of those protocols, and on growing an ever more comprehensive set of domesticated applications. A consistent UI, for the user both as user and as collaboration manager, is also essential.
2. A set of domain tools (computation systems, storage, common scientific analytic tools, databases and data sets, etc.) that also have their identity and access control needs met with open community-standard interfaces. These tools are noteworthy not only for their users - relatively small in number but consequential in importance - but also their requirements: command line applications, process authentication, delegation of authorization needs, etc.
3. A collaboration-centric identity management and access control mechanism that leverages the growing R&E federation infrastructure, gives the collaborators the ability to mingle institutional and collaboration attributes and permissions in order to manage access to collaboration resources, and provides consistent user experiences. While the sciences and domains may be different, and the desired collaboration apps vary (though a core seems to be common to all collaborations) the need to identify participants, to have scalable authentication and authorization across the tools and apps, and to have reliable reporting are the same.

CoCoA (Comanage + Conext + Applications) is a blending of two collaboration management platforms, one that focuses on the entire identity life cycle process and the Registry that feeds identity information to applications, and the other that focuses on the user experience. CManage and OpenConext are working together to provide a complete, feature-rich identity management service and collaboration platform for VOs.

The CManage Project, funded by the National Science Foundation and Internet2, is developing tools and resources that allow virtual organizations to meet their research objectives without building their own stand-alone identity management infrastructures. By leveraging external (federated) identity management services and standard group and registry tools, authentication and authorization are handled in a single, efficient process that integrates a mix of collaboration attributes and each member's home organization attributes into all of the various applications that serve a collaboration community. It allows a collaboration to seamlessly use a variety of tools instead of being locked into a proprietary suite. It also allows collaborators to focus on what they do best — advancing scholarship and research in their field of expertise — rather than the complexities of identity management.

OpenConext was developed by SURFnet as part of the SURFworks and GigaPort3 programme. It is an opensource technology stack for creating and running collaboration platforms and creates a powerful front end for users to choose for themselves and their workgroups the right applications for their collaborations. When combined with the CManage Registry service, collaborations have a complete solution from front to back for identity management and collaboration needs.

CManage can be thought of as a specialized identity management system for supporting a Virtual Organization (VO). The needs of VO's are unique in the identity management world, and while there is some overlap with enterprise identity management, a few specialized requirements come in to play:

- A VO will have very specialized attributes and permissions not replicated anywhere else.
- For reasons of sustainability and freshness of data, VO's also want to leverage enterprise attributes.
- A VO will have business processes for participation that feed their onboarding and enrollment that are specific to their collaboration; they have no systems of record to build on, as enterprises do.
- The lifecycle of identities within the collaboration go beyond the lifecycle of identity within a single institution.
- There is no identity management staff to run the systems; there are, at best, general IT architects for the VO who may be uninformed of the modern federated world.

For organizations that want to replace an ad hoc (or largely absent) set of identity management tools within their own cyberinfrastructure, there is the CManage toolkit. The toolkit can provide a coordinated, federated access control layer to a VO's wiki, list processing, audio conferencing, etc. as well as potentially their specific domain applications. The CManage toolkit provides a rich set of critical components to a VO, including: an identity registry, automatable processes for enrollment, collaboration identity lifecycle maintenance, group attribute management, and provisioning that developers can connect to the domain science applications in use by the VO. From an end user's perspective, having the CManage toolkit working behind the scenes allows individuals to create personal groups as well as manage organizational groups that they have permissions for, and allows the user more control over the information they might share within the VO.

Poorly done IdM, with its gaps, frustrations, and spills, takes more time than IdM done structurally. Students enrolled in classes wait for weeks to get to scientific resources. Researchers long gone still have active permissions, creating serious security concerns. Ad hoc agency reporting requirements generate chaotic weeks-long multi-institutional fire. With a platform like CoCoA, these pain points and many others are addressed for VOs and their associated institutions.

More information is available online:

COmanage = <http://www.internet2.edu/comanage>

OpenConext = <https://wiki.surfnetlabs.nl/display/OpenConext>