B2ACCESS Management

About

Document that describes how a service manager can use the B2ACCESS portal to manage the users and groups that are allowed to perform certain actions in B2ACCESS-enabled services.

Service: B2ACCESS

Modified: 04 May 2016

Synopsis

B2ACCESS is the EUDAT federated cross-infrastructure authorisation and authentication framework for user identification and community-defined access control enforcement. The B2ACCESS service managers are responsible for managing users and their assignments to groups for their specific service. They can also manage (edit, delete and modify) groups of their service. This document describes how to perform these actions on the B2ACCESS administrative interface.

Introduction

B2ACCESS allows EUDAT users to authenticate themselves using a variety of credentials.Users then get access to the EUDAT services, with varying levels of privileges in these services. The process of handling user registration and giving them access to services is carried out on the B2ACCESS administration portal. There are two important aspects that run through the B2ACCESS process: attributes and groups.

Attributes

Attributes are typically key-value pairs, where the key is the "name" of the attribute, for example, "givenName=Joe" and "surname=Bloggs". These attributes tend to have common names that are understood by many different kinds of services and they follow well-defined *schemas* that define the names and semantics of the attributes.

EUDAT keeps attributes for each user, associated with the user account, and these can be common ones like "email=..." or they could be Uniform Resource Names (RFC 1630) like, say, "urn:eu:eudat:b2safe:role=admin". They can also be specialised ones such as "urn:oid:2.5.4.49"; while not very human readable, these make sense to a machine looking for (in this case) the distinguishedName attribute (which is a globally unique name for the user). EUDAT also uses attributes that should have been encoded as URNs but use a "short-hand" naming convention, e.g. "unity:persistent" instead of the proper "urn:eu:eudat:b2access:unity:persistent".

Attributes are thus used not only as a part of the authentication process by providing user names in different forms, but also to provide attributes that can be used for authorisation purposes, such as the role of a user, or membership of communities.

The following attributes can be used by a back-end service to authorise a user to perform certain actions:

- Group membership: contains a multi-valued list of groups this user is a member of.
- (Not supported currently) Community membership: contains a multi-valued list of communities this user is a member of. In EUDAT, these are published as multi-valued attributes with the name "memberOf".

EUDAT receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 654065.

- Level of assurance (not included in release 1.0 of B2ACCESS): indication of the level of assurance of the provided attributes, based on the method of authentication. B2ACCESS username/password and social identities have a low level of assurance, while authentication via a national federation will result in a higher level of assurance
- Identity: this is the unique identifier for the user. This can be the principal identity coming from the identity provider used to log in and/or the unique EUDAT identifier generated for each user, as with the distinguishedName above. Each user or user-agent can have multiple identities; they are equivalent to each other and they provide flexibility to support various authentication systems.

What groups are available depends on the service in question. Assigning a user to one or more groups changes the user's group membership and therefore the resources and services the user can access and the actions the user can perform.

The other attributes relevant for authorisation are controlled by other factors and cannot be set by a B2ACCESS service manager. For example, the level of assurance (LoA) is based on the method used to authenticate: authentication via a national identity federation or a government id will have a high LoA, users who used social media id (where the name is likely to be right but anyone can create an account, and the policies governing use is more lax) have a lower LoA, and users who have registered only with B2ACCESS, providing little more than an email address, have a lower LoA still. A service may require a higher LoA for certain types of privileged actions.

B2ACCESS uses the UNITY IDM technology. The Unity user documentation provides more in-depth instructions on how to use this user interface. The B2ACCESS integration page provides more technical documentation regarding the attributes currently available in EUDAT.

Groups

Contents Management allows the manipulation of groups. Each EUDAT service has its own set of groups, organised in namespaces. Membership of a service-specific group implies certain privileges for that service. The following table specifies the main namespaces for each available service; more will be added as more services are integrated.

Table 1. B2ACCESS groups and services that use them

Group	Service
eudat:b2drop	B2DROP
eudat:b2safe	B2SAFE
eudat:b2share	B2SHARE
eudat:creg	CREG

The idea is that attributes whose *name* begins with "eudat:b2drop" are specific to the B2DROP service - any B2DROP service instance, wherever in the EUDAT infrastructure it appears. So, if it makes sense to have an "admin" role for B2DROP specifically, we can add attributes like "eudat:b2drop:role=admin" for users who have this role; if the attribute is absent or has a different value, B2DROP will give users normal access and if it has the value "admin", they will get privileged access.

Administration interface

The B2ACCESS administration endpoint is available online. The following figure shows the web-page as it appears after successful log in.

EUDAT receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 654065.

Figure 1. Service managers can use a web interface to access B2ACCESS management

Please see the B2ACCESS Usage document for instructions about registering to B2ACCESS.

The main B2ACCESS interface provides a menu bar with the following options, available as tabs:

1. Contents Management
2. Registrations Management
3. Schema Management
4. Server Management

The Contents Management screen is used in order to manage groups and users. To manage user registration refer to the Registrations Management. Schema and Server Management are intended for the B2ACCESS administrators and therefore beyond the scope of this document.

Structure of this document

The rest of this document discusses how to manage groups and registrations on the B2ACCESS portal.

Contents Management

In order to give a user access to specific services, the user must be a member of the corresponding service group. This section will describe how to manage the groups under a service namespace and how to manage users in these groups.

Group membership management

Assign users to a group:

- Select the 'Root (/)' group. All entities (i.e. users, or user-agents) are now shown in the right UI pane
- Find the entity for the user you want to assign to the group (a single entity can have multiple entries per authorisation type; enable *Group by entities* to easily see them all)
- Drag the user from the right pane and drop it onto the desired group in the left pane

View users in a group:

- Select a group in the top left pane of the UI. You will now see all members of this group in the right pane, as in the (anonymised) figure below

Figure 2. Service managers can see all members of their group

- Use the *Group by entities* checkbox to group all members by entity

Remove a user from a group:

- Select a group in the top left pane of the UI
- Select the user's entity (make sure *Group by entities* is enabled)
- Click the *Remove from the group* button in the toolbar above the right pane

EUDAT receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 654065.

- Confirm to apply the changes

Manage groups

Service managers have B2ACCESS privileges to create and delete subgroups within their service.

Create a new subgroup:

- Select a group in the top left pane of the UI, as shown on the following figure.

Figure 3. Group selection

- Click the *Add subgroup* button on the top left pane icon bar
- Supply:
    - Name: the name of the group as used in attribute values (this is what is exposed to service providers). Names cannot include the '/' character nor be empty.
    - Display name: a string used to display this group in the user interface. Display names cannot include the '/' character nor be empty.
    - Description
- Click the *OK* button to add the new group
- Follow the steps from the next section to manage users in this new group

Delete a subgroup:

- Select a group in the top left pane of the UI
- Click the *Remove group* button on the top left pane icon bar
- Confirm to remove the group

Note: There is no undo action in the Unity IDM used by B2ACCESS behind the scenes. If you want to revert a change, you have to manually perform the steps to re-introduce it.

User actions

Service managers can also perform global actions on users, using the following workflow:

- Select a group in the top left pane of the UI
- Select a user in the right pane, as in the following (anonymised) picture.

Figure 4. User selection

The following options are then available:

- Delete a user:
    - Select the user's entity (make sure 'group by entities' is enabled)
    - Click the *Remove entity* button in the toolbar above the right pane
- Block a user:
    - Select the users entity (make sure 'group by entities' is enabled)
    - Click the *Change status* button in the toolbar above the right pane

EUDAT receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 654065.

- Select the *Disabled* status
- Save the changes
- Note: this menu can also be used to have users accounts expire after a set date

- Update user credentials:
  - Select the user's entity (make sure 'group by entities' is enabled)
  - Click the *Change status* button in the toolbar above the right pane
  - Provide a new password
  - Save the change

Registrations Management

The following section only applies to B2ACCESS administrators.

When a user applies to register with B2ACCESS, a registration request is generated. A user can be an end-user but also OAuth2 clients are associated with a user within B2ACCESS. The registration request is generated on the "pending" state, from which it can be "accepted" or "declined". The registration management screen also provides an overview of all registrations and the ability to view details of a registration.

Registrations overview

- Click on *Registrations Management* in the top menu bar.
- Click on *Registration Requests* (default).

You should now see a window as shown in the following figure.

Figure 5. The administration interface allows registration requests to be reviewed

- You can click on the column headers to sort.
- You can click on any entry to manage that request.

Manage a registration

- After a registration is selected, you should see a screen as in the figure below.

Figure 6. Reviewing and managing a registration request

This window provides an overview of the registration request and all associated attributes

- For a pending registration you can use the *Accept*, *Reject* and *Delete* buttons
- For an accepted registration you can use the *Delete* button

Support

Support for B2ACCESS is available via the EUDAT ticketing system through the webform.

If you have comments on this page, please submit them though the EUDAT ticketing system.

EUDAT receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 654065.

Document Data

Version: 1.0

Authors:

Willem Elbers, willem@clarin.eu

Jens Jenssen, jens.jensen@stfc.ac.uk

Editors:

Hans van Piggelen, hans.vanpiggelen@surfsara.nl

Kostas Kavoussanakis, kavousan@epcc.ed.ac.uk

Read more

EUDAT receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 654065.