Reference Guide

Access Control List

ACL Definition

Access Control List Definition

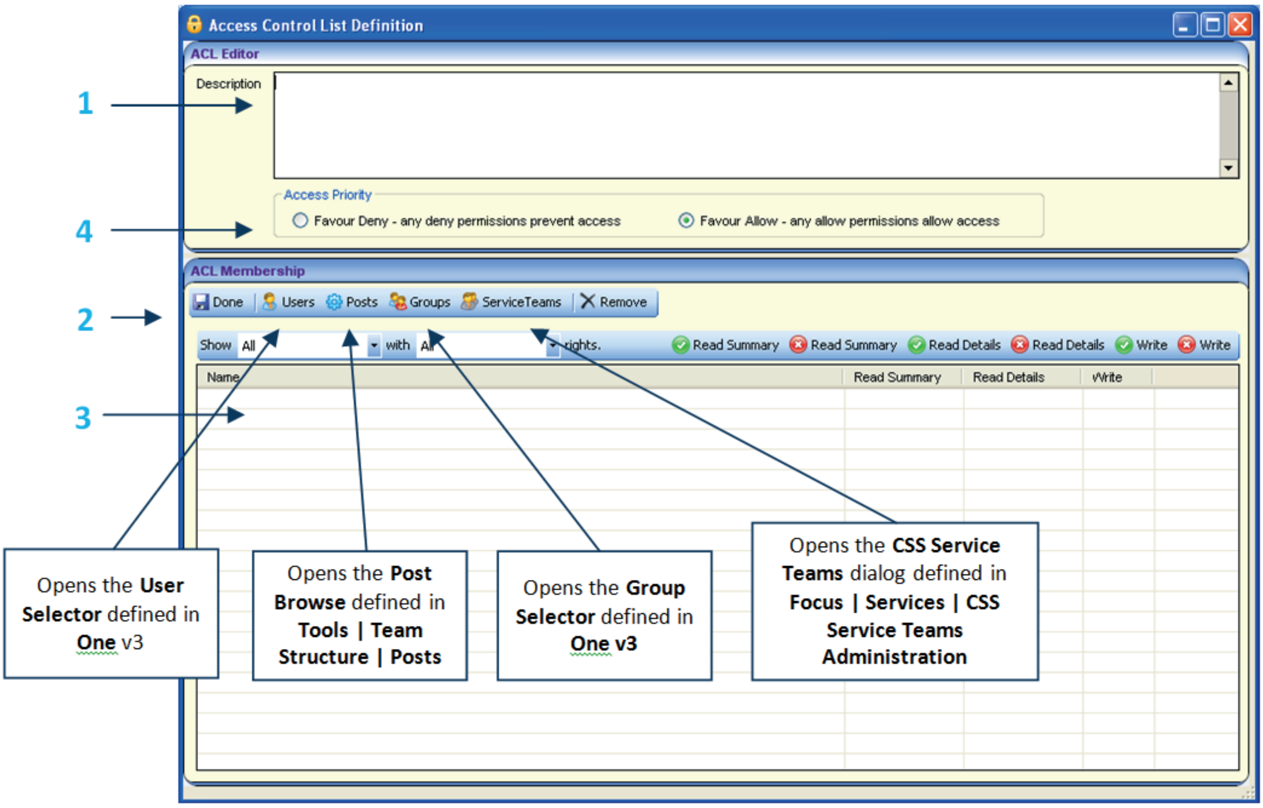
ACLs can be set for **B2B: Student**, **Person Details**, **Communication Log**, **Activities**, **Provision**, **Equipment**, **Exclusions**, **Involvements**, **Risks**, **Early Years Maintain Provider**, **SEN2 Returns**, **Service Level Agreements**, **Adoption**, **Fostering**, **Case Notes** and **Service Provision**.

Default ACLs can also be applied to **Service Teams** via **Focus | Services | Service Team Administration**. ACLs defined for a service team are inherited by all associated entities (e.g. Involvements). If a service team's default ACL is updated, then the new ACL cascades to all involvements and related communication log items, unless the ACL has been customised locally at record level.

NOTE: If an ACL is defined, users not included in the ACL are denied access.

To set an ACL for a record:

1. Click the **Set ACL** button to display the **Access Control List Definition** dialog.



Opens the **User Selector** defined in **One** v3

Opens the **Post Browse** defined in **Tools | Team Structure | Posts**

Opens the **Group Selector** defined in **One v3**

Opens the **CSS Service Teams** dialog defined in **Focus | Services | CSS Service Teams Administration**

2. Enter a **Description** for the ACL. (**1**)
3. On the **ACL Membership** panel, use the buttons to select your membership. The available options are **Users, Posts, Groups and Service Teams**. (**2**)
4. Assign levels of access to the group's members. If required, you can assign levels for all members in a continuous block by using the **Shift** key, or use the **Ctrl** key to select several non-adjacent members. Alternatively, you can assign levels individually. (**3**)
5. Set the **Access Priority** to **Favour Allow** (default) or **Favour Deny**. (**4**)
6. Click the **Done** button to save your changes.

Reference Guide

Access Control List

ACL Definition

Access Levels

There are three levels of access which can be applied to users. These are: **Read Summary**, **Read Details** and **Write**. When ACL members are selected, **Allow** is the default setting.

To apply access levels, select the row or rows to be defined and click **Allow** or **Deny** for the relevant level.

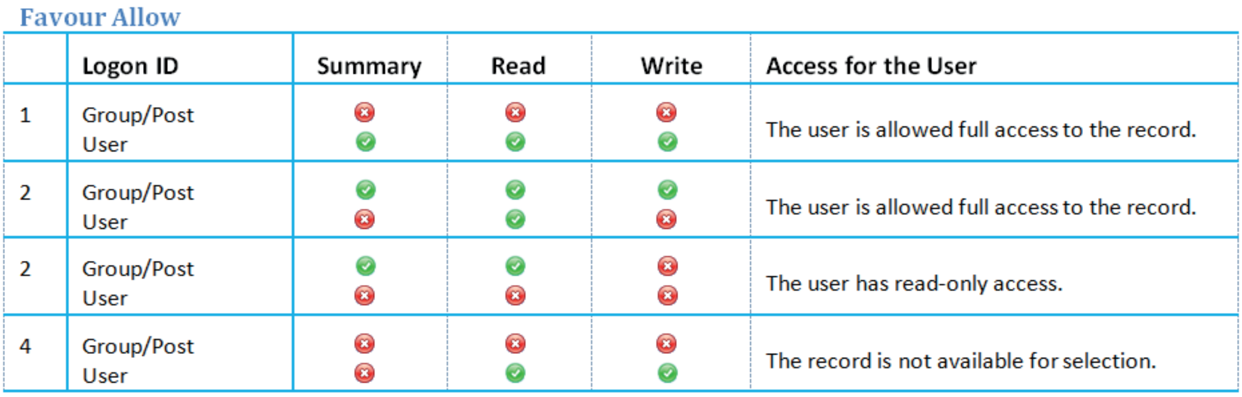
- To **Allow** access to **Read Summary**, **Read Details** and **Write** gives full access to the data.
- To **Allow Read Summary** and **Read Details** access but **Deny Write** access gives read-only access to the data to which it is applied - the user will not be allowed to edit the data.
- To **Deny Read Summary** refuses access to summary pages (e.g. Involvements and Provision). It would therefore not make sense to allow **Read Details**.

NOTE: The **CSS** and **SEN** Summary reports do not display records where **Read Summary** access is denied.

- To **Deny Summary** and **Read Details** access but **Allow Write** access denies the user access to see the data but allows the data to be updated at system level (e.g. when the system is being updated from an external source).

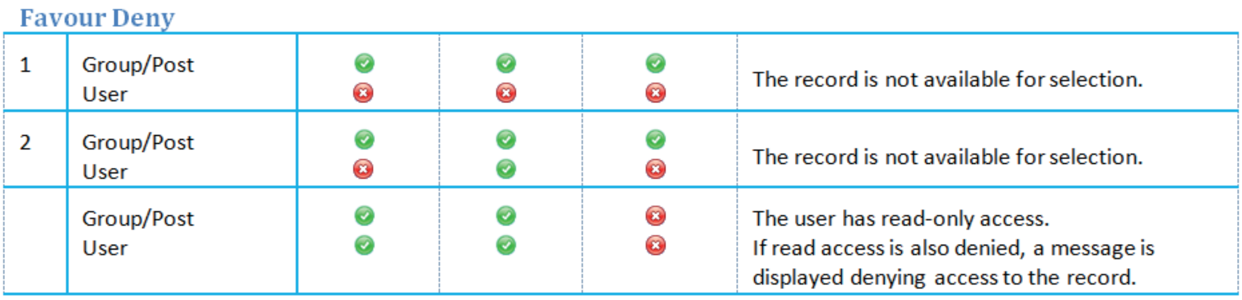
Access Priority

The Access Priority an be set to **Favour Deny** or **Favour Allow**. These settings dictate access rights, either downgrading or upgrading a user’s permissions, depending upon which Group or Post the user is logging on as. **Favour Allow** is the default selection. The following scenarios are based on access to a Person record.



Favour Allow

	Logon ID	Summary	Read	Write	Access for the User
1	Group/Post User	✗ ✓	✗ ✓	✗ ✓	The user is allowed full access to the record.
2	Group/Post User	✓ ✗	✓ ✓	✓ ✗	The user is allowed full access to the record.
2	Group/Post User	✓ ✗	✓ ✗	✗ ✗	The user has read-only access.
4	Group/Post User	✗ ✗	✗ ✓	✗ ✓	The record is not available for selection.



Favour Deny

1	Group/Post User	✓ ✗	✓ ✗	✓ ✗	The record is not available for selection.
2	Group/Post User	✓ ✗	✓ ✓	✓ ✗	The record is not available for selection.
	Group/Post User	✓ ✓	✓ ✓	✗ ✗	The user has read-only access. If read access is also denied, a message is displayed denying access to the record.

CAPITA

Capita One. Tel: 01234 838080. Email: info@capita-one.co.uk. Web: www.capita-one.co.uk.

For more detailed instructions refer to the online help file or handbook. You can contact the Service Desk via My Account. This guide is based on the version of the software (Autumn 2014, 3.55) in use at the time of publication.