Best Practice

Reporting to Multiple Identities

Publication 28 April 2026

Background

Publishers offer many different authentication methods to end users. This is great in terms of allowing a user to access content seamlessly, but having lots of ways to authenticate means a single user could be linked to lots of institutions at the same time. For example, Sam may be affiliated with institution A through IP recognition, institution B through Shibboleth / Open Athens authentication, and Institution C through role-based access (i.e. a personal log-in for an editor).

This guidance applies to Release 5.1 of the COUNTER Code of Practice (R5.1).

COUNTER has not previously specified how report providers should manage reporting where a user's activities may be attributed to multiple institutions. This best practice reflects the majority of current reporting mechanisms. Introducing a formal requirement for how report providers should report multi-identity usage represents a breaking change to the Code of Practice. Such changes cannot be introduced before a future Release 5.2. Our goal in publishing this best practice is simply to introduce transparency into a previously opaque part of COUNTER reporting.

Relevant parts of the Code

Conventions

Per the Code of Practice, this best practice guidance uses the following convention:

The keywords MUST (or REQUIRED), MUST NOT, SHOULD (or RECOMMENDED), SHOULD NOT (or NOT RECOMMENDED), and OPTIONAL in this document are to be interpreted as described in RFC 2119.

User sessions

Section 7 of the Code of Practice defines user sessions as follows

> A user session is defined any of the following ways: by a logged session ID + transaction date, by a logged user ID (if users log in with personal accounts) + transaction date + hour of day (day is divided into 24 one-hour slices), by a logged user cookie + transaction date + hour of day, or by a combination of IP address + user agent + transaction date + hour of day.
>
> To allow for simplicity in calculating session IDs, when a session ID is not explicitly tracked, the day will be divided into 24 one-hour slices and a surrogate session ID will be generated

by combining the transaction date + hour time slice + one of the following: user ID, cookie ID, or IP address + user agent. For example, consider the following transaction:

- Transaction date/time: 2024-06-15 13:35
- IP address: 192.1.1.168
- User agent: Mozilla/5.0
- Generated session ID: 192.1.1.168|Mozilla/5.0|2024-06-15|13

The above replacement for a session ID does not provide an exact analogy to a session. However, statistical studies show that the result of using such a surrogate for a session ID results in unique counts within 1-2 % of unique counts generated with actual sessions.

Overlapping institutions

Section 10.3 of the Code includes an acknowledgement that for consortial reporting,

> The totals on the summary report may differ from the sum of the totals on individual member reports for the same items if an authentication method used identifies to multiple member sites and usage is attributed to each such site (e.g. overlapping IP ranges).

Best practice

Reporting where a user session is linked with multiple institutions

Report providers SHOULD attribute single user sessions to multiple institutions where the session can be clearly tied to more than one institution. Attribution to multiple institutions could be through

- Overlapping IP ranges, per Section 10.3 of the Code.
- Multiple authentications via Google Scholar's Campus Activated Subscriber Access (CASA), a remote access extension of Google Scholar's Subscriber Link Program.
- Stacked logins (e.g. IP plus federated authentication).

Where a user session is attributed to multiple institutions, all COUNTER metrics generated during the user session MUST be reported to all of the institutions.

This configuration has the benefit of maximising users' access to content.

This configuration has the drawback that it could result in institutions seeing Requests for content they have not licensed.

Reporting where a user session is linked with one institution

Report providers MAY restrict attribution to a single institution per user session.

Where a user session is only attributed to a single institution, all COUNTER metrics generated during the user session MUST be reported to that institution.

This configuration has the benefit of simplifying reporting, as it is only ever possible to attribute usage, search and denial metrics to a single institution within a single user session.

This configuration has the drawback of presenting user experience challenges. Users who are entitled to content by virtue of being affiliated with multiple institutions may find their access curtailed when they are only able to use one affiliation for authorization purposes.

Transparency

COUNTER will be investing in Registry developments in late 2026. As part of this work, we will add a flag to indicate whether user sessions can be attributed to more than one institutional identity. When the Registry project is complete we will update this best practice guidance to require that report providers add the information to the Registry.