HOW-TO: SELF-SERVICE REPORTING TOOLS FOR ADMINISTRATORS

March 22, 2018 12:04

Follow

You and your faculty may already be familiar with Activity Insight's Customizable CV tool, which allows users to create and edit formatted reports using their own data. These reports are completely flexible, allowing users to add and re-order sections and maintain complete control over the formatting, filtering, and grouping of activities within that report template — all without any work request processing by the Digital Measures development team!

Once you are familiar with these self-service tools as they relate to self-scoped reports (i.e., reports that are generated with *your own* activity data), you will find it useful to explore the self-service reporting features that are specifically designed for those who run reports on *other users' data*.

You can use these tools for a variety of purposes:

- Annual activity reports
- Promotion and tenure documents
- Standard university CVs
- Discipline-specific report remplates
- Standardized reporting to specific audiences, like accreditors, your university's marketing department, etc.
- Responding to requests for specific information
- Reviewing data for missing or inaccurate information

"PREVIEW" REPORT AS ANOTHER USER

As you're building a new report, you may want to see at-a-glance how the report would look for various users based on the data they have in Manage Activities. For instance, users in your College of Fine Arts may have very unique data as compared to users in the College of Natural Sciences. The "Preview As" icon in the report Options tab allows you to do just that.

This is especially useful when building and proofing a report that needs to run well across users who capture data with very different structures.

RECENTLY VIEWED ARTICLES

Activity Insight Roadmap

New System Navigation

RELATED ARTICLES

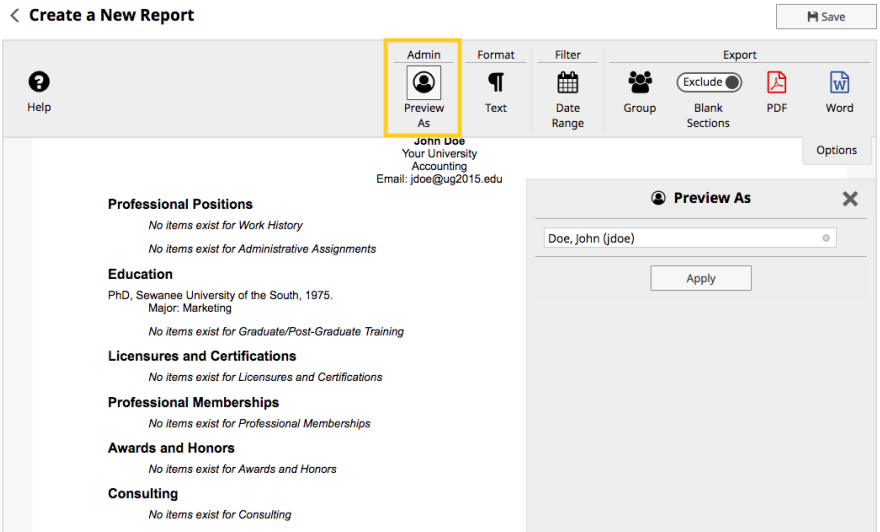
Activity Insight Roadmap

Reports Menu

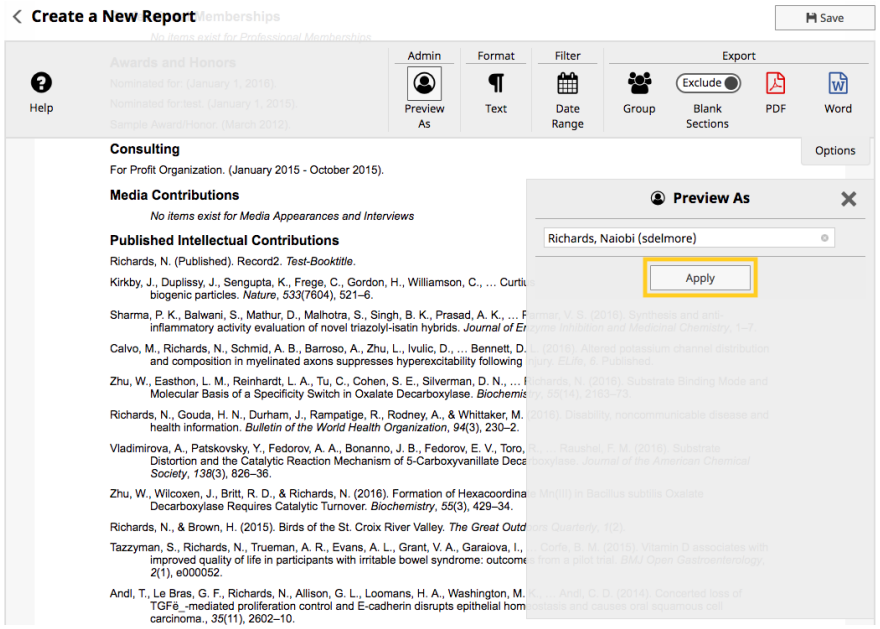
How to Customize a CV in Activity Insight

Best Practices for Building and Testing Custom Reports

Self-Service Reporting Updates



In the image above, we can see that the user John Doe has very few records that meet our report criteria. If we choose another user under "Preview As", we can preview the report as a user with more robust data to get a better picture of the report output.

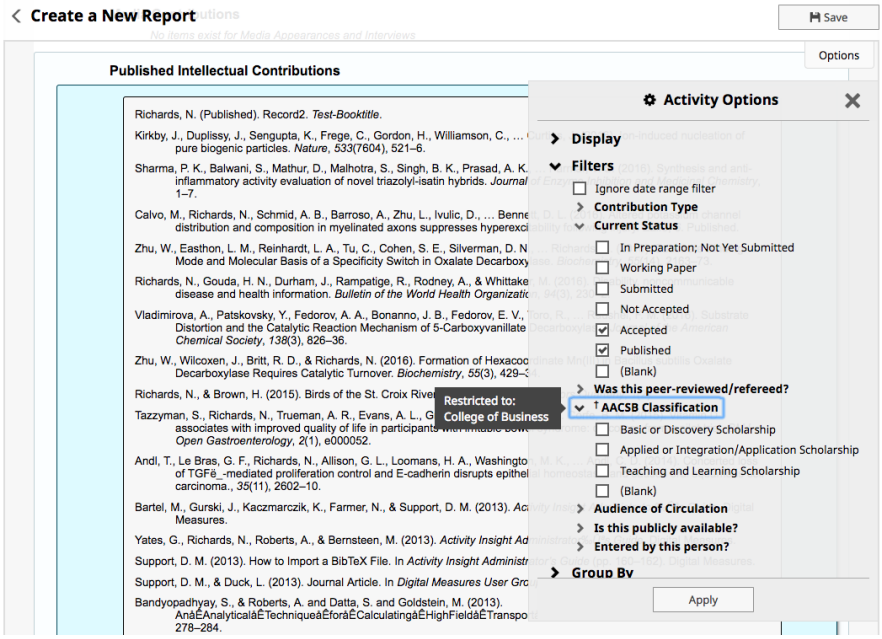


MAINTAIN AWARENESS OF RESTRICTIONS

Your data collection instrument may have screens or fields that are only available to certain areas. For instance, users in the College of Business must select an "AACSB Classification" for their publication records for those records to appear in certain AACSB tables. In most instances, those AACSB-specific fields will be restricted to users in the College of Business.

Read more about screen and field restrictions

Rather than having to refer to your Configuration Report to identify these restricted fields while building a report, we have introduced the "dagger" character to denote fields or screens that have access restrictions. If you hover over any field or screen with this character, a note will appear to identify that restriction.



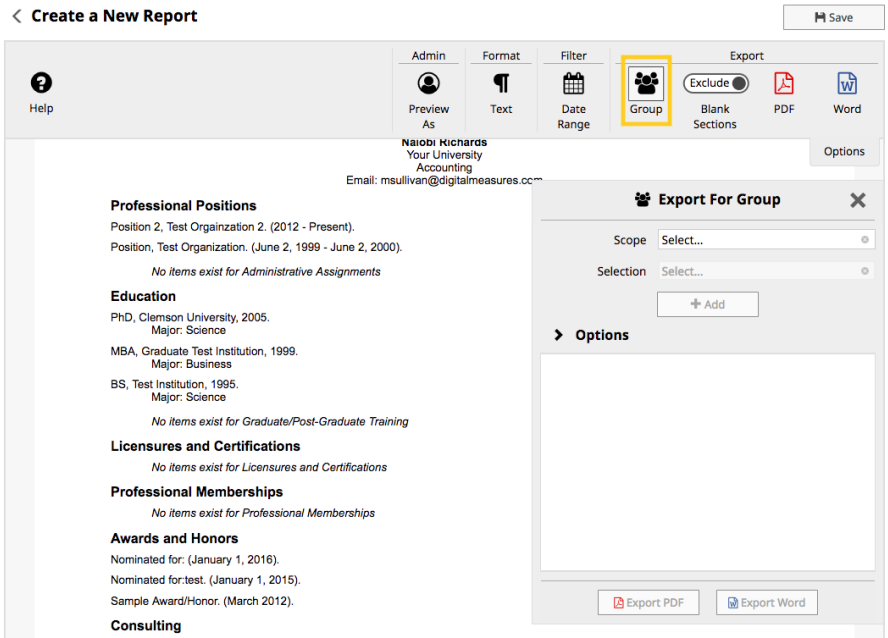
It is completely possible and recommended to build reports that include restricted screens and fields. You may take more time to ensure that everything shows up the right way for each group you intend to run the report on. As a rule of thumb, when including a screen or field with restrictions, use "Preview As" to ensure everything shows up correctly for users with, and without, access to that screen or field.

We also recommend...

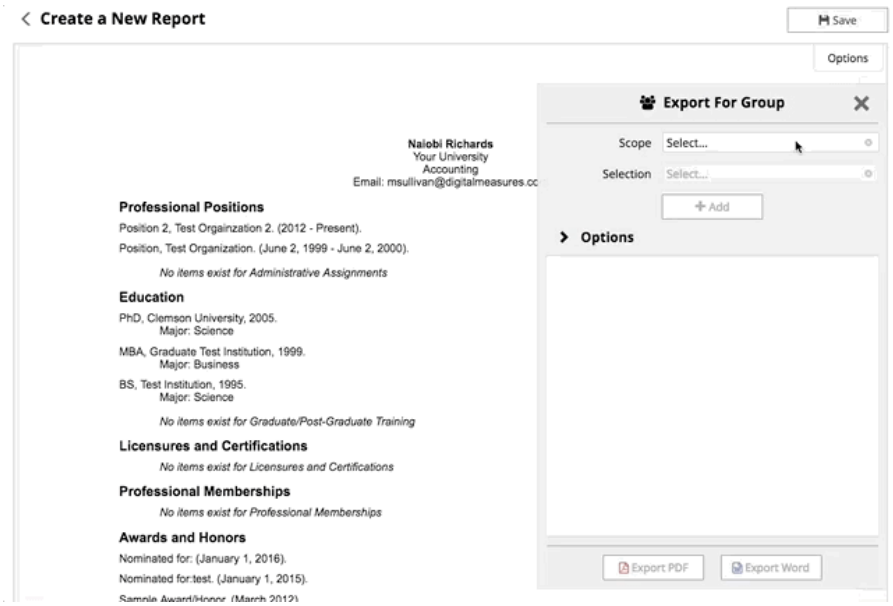
- Avoiding grouping and filtering by restricted fields
- Excluding blank sections when running (exporting) the report so that users without access to the restricted screens you've included in your report won't end up with headers for blank sections

EXPORT YOUR REPORT FOR A GROUP OF USERS

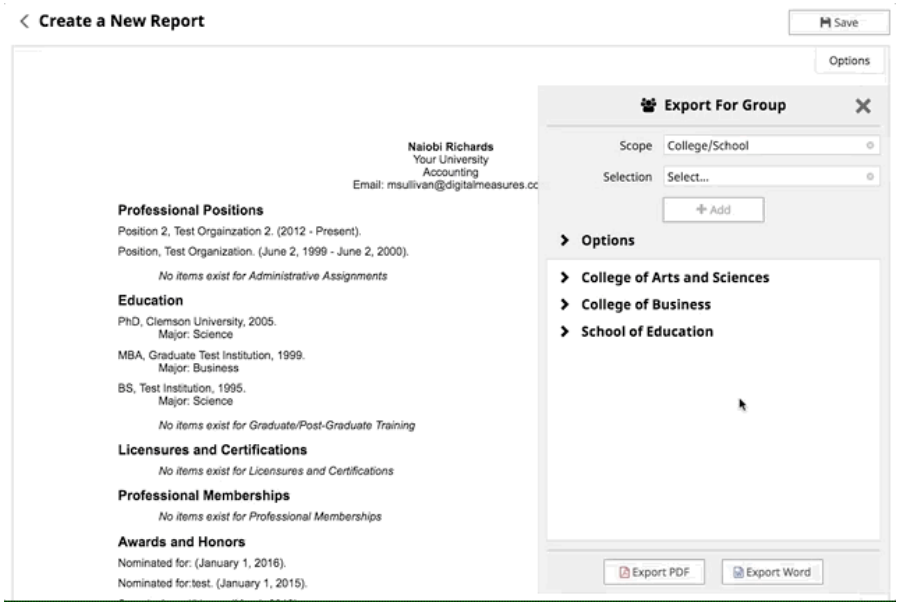
Suppose you've just built an annual activity report, and you want to share that formatted data with an external audience. The "Export For Group" feature allows you to do that.



To select users for whom to export your report, first select the scope, then select an option within that scope, and click "Add". Each time you add a selection, it will appear in the list below.



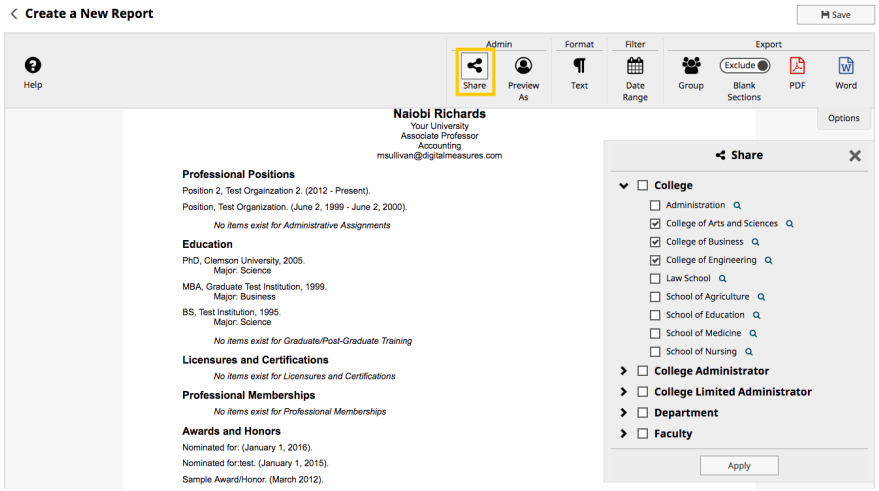
You can also remove selections, or individuals within a selection, using the trash can icon.



Once you have finalized your selections, you can export using PDF or Word format. When exporting reports for multiple users, Activity Insight will generate a .zip file containing one PDF or Word document for each individual user, based on your selections.

SHARE SELF-SERVICE REPORTS WITH OTHER USERS

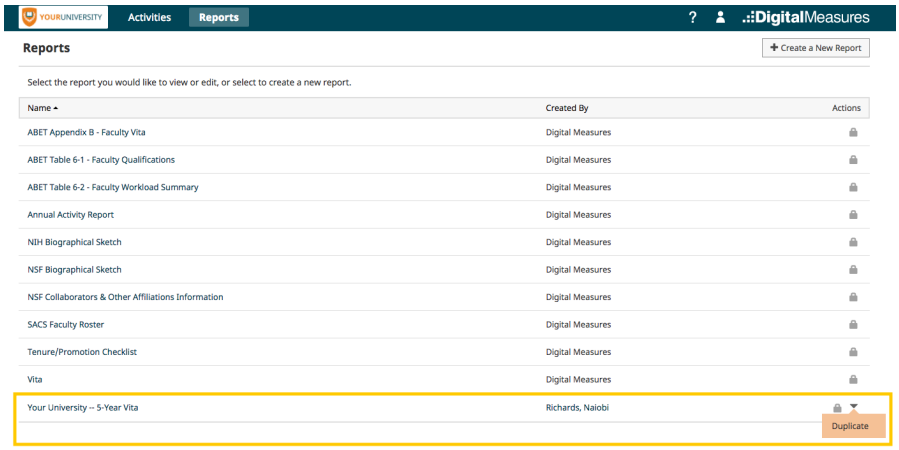
Once you have built a Self-Service report, you can share that report with individual users or specific groups of users to allow them to run that report themselves. In some cases, this functionality may reduce the need for custom reports built by the Digital Measures team, allowing administrators to make immediate updates to reports they have built themselves.



The Share panel allows the university administrator to choose segments of users with whom to share self-service reports.

Administrators can share Self-Service Reports with individual users or with groups of users based on the security roles assigned to them. Note the magnifying glass icon, which when selected will show you a list of users assigned to that particular security role.

Users with whom you share a given report can open the report, view the criteria and different options selected by the user who created the report, but none of these options are editable (except the date range). If the user wanted to duplicate the shared report and make adjustments to their own personal copy of the report, they can do so from the Reports menu:



If a user who has access to a shared report wants to contact the user who originally created and shared the report, selecting the name under "Created By" on the Reports menu will launch the user's email application with a new email addressed to the report's creator.

The sharing functionality is available to users who meet the following criteria:

- Have the Self-Service Reporting: Formatted permission in their security role. (By default, the top-level administrator has access to this permission. If you would like to expand this to others, please submit a work request with the names of the security roles who should have access.)
- Have a security role scope that is not “self”

COMMENTS