DSOnly Access Management

Creating and maintaining DSOnly Users

Purpose
Decision Support provides the ability to grant limited access to faculty and staff who do not have a daily business need for DaFIS. Access is granted by approved access managers, and is limited on an organizational, account, sub account and/or project basis.

In this manual, we will examine the tool that provides this limited access, discuss the methods of requesting status as an access manager, and outline the process for granting access to users and other managers.

Contents

- What is Access Management?, p. 1
  - Access Restrictions, p. 3
  - The Audit Trail, p. 4
  - Removing Access Managers, p. 4
- Becoming an Access Manager, p. 4
  - Requesting Authorization, p. 4
  - Once You Are Approved, p. 4
  - Viewing Your Authority and Delegations, p. 5
- Managing DSOnly Users, p. 6
  - Restricting Access, p. 6
  - Restricted Queries, p. 7
- Setting Up New Users, p. 8
- Editing User Access Rights, p. 9
- Revoking User Access, p. 11
Managing Subordinate Managers, p. 11
  - Delegating Organizations, p. 12
  - Granting Delegation Authority, p. 12

Setting Up New Access Managers, p. 12

Editing Manager Delegation Authority, p. 13

Revoking Delegations, p. 14
  - Transfer Delegations to a New Access Manager, p. 15
  - Transfer Delegations to an Existing Access Manager, p. 16
  - Transfer Delegations to the Revoking Manager, p. 17
  - Revoke All Delegations, p. 18
What is Access Management?
Access to DaFIS Transaction Processing (TP) and Decision Support (DS) is currently limited to individuals with a business need to access the information contained in both systems. This includes those who create the financial transactions, and those individuals who have the approval authority. However, there are faculty and staff who are not directly involved with transactions, but have a need for access to limited sets of information.

Access managers are selected users within each college/division. They must be current DaFIS Users with normal access to both TP and DS. Once authorized, they are able to grant non-TP users limited access to Decision Support. In some cases, they are also given the authority to delegate access manager rights to other TP users.

The DSOnly User Access Management system allows access managers, and their delegates, to grant restricted Decision Support access to non-TP users. There is also a maintenance function that allows access managers to modify or revoke access as needed.

Access Restrictions
DSOnly user access can be limited based on:

- **Organization** – all accounts within the specified organization(s) would be accessible by the user
- **Account(s)** – the user could only see information pertaining to the specified account(s)
- **Sub-account(s)** – the user could only see information pertaining to the specified sub-account(s)
- **Project(s)** – the user could only see information pertaining to the specified project(s)
- **Report Type(s)** – the user will only have access to query types authorized by the access manager

Access can only be provided within an access manager’s delegated organization and any organizations subordinate to it.
The Audit Trail
The system provides a full history of all the rights granted and revoked. Records of the accounts and organizations a user has been granted access to are never deleted from the system. When access is removed, the records are simply marked as invalid. With the information stored, it is possible to recreate the exact time periods an individual had access to a particular item and who granted it to them. This information will only be used to resolve issues of possible misuse of university financial information.

Removing Access Managers
An access manager who delegates authority to another manager can also revoke it. When a subordinate manager is removed, all permissions that manager has made must be either revoked or transferred to another access manager. This includes user access and delegations to managers.

Becoming an Access Manager
Before you can grant DS Only access to non-TP users, you must become an access manager. Top-level access managers have been chosen from Dean’s/Vice Chancellor’s Offices. These users have been given the ability to delegate authority to users at the departmental level.

Requesting Authorization
A list of the top-level access managers, and the organizations over which they have authority, can be found on DaFIS web site. You will need to send a request to one of these people, or ask them who the appropriate access manager is at your level:

1. Go to http://dafis.ucdavis.edu/;
2. Click on DS Only Access Information;
3. Locate the top level manager appropriate to your college or division;
4. Scroll down the page and locate the e-mail link to send an inquiry/request to that access manager.

That access manager should contact you when you have been established as an access manager or to direct you to the appropriate person.

Once You Are Approved . . .
Once you are approved as an access manager, a new link, Administer DS Only User Access, will appear at the top of the DS home page.
Clicking on this selection will take you to a screen with options for:

- Viewing your authority and delegations
- Managing or adding DSOnly users
- Managing subordinate access managers

**DSOnly User Access Management**

You may use this interface to manage non-DP user access rights within Decision Support. To grant a new user rights within DS, click on the “Manage New User” link below. To edit or revoke a user’s access abilities, click on the appropriate link next to their name.

The remainder of this document will detail the use of each of these options.
For each manager you have set up, you may also examine any access they have delegated by clicking on the appropriate View User's Delegations link.

Managing DSONly Users

Once you are given access manager privileges, you can begin to set up DSONly users. Any users you wish to set up will first have to establish a UCD Login ID. (Instructions can be found at https://computingaccounts.ucdavis.edu/cgi-bin/services/index.cgi) You will need to know the users login IDs before you can establish their access. If you do not know whether they have established their UCD Login ID, or what it is, you can lookup them up in the campus database at http://www.ucdavis.edu/directory.html. It is also advisable to run the FIS User Lookup (86) in Decision Support to confirm that the person is not already a TP User.

Each Login ID will be checked against the DaFIS Universal User table. The Universal User table contains all users with UCD Login IDs who are employees of UC Davis. Employee status is loaded from the payroll system, which can take a few weeks to be updated. Each ID will also be checked against the DaFIS User table to confirm that the ID does not belong to an active DaFIS TP user. If an entered ID is found not to meet the above criteria, you will receive an error message.

Restricting Access

Organizations, accounts, sub-accounts and/or projects may be specified. If an organization alone is specified, the DSONly user may access information about any account in that organization. However, accounts in subordinate organizations will not be included. If subordinate organizations are to be included, they each must be specified individually. Additional accounts can also be specified, and do not have to be within any organizations that may be listed.
Organizations and accounts are used in an “or” fashion: The account being accessed either has to be in one of the listed organizations or has to be one of the listed accounts. This way a manager can specify that a user has access to all accounts in **ORG1**, but only to **ACCTONE** and **ACCTTWO** from **ORG2**.

Sub-accounts and projects may also be specified. If you want to specify a sub-account or project, you must also enter an organization, or account, to be associated with them.

**Restricted Queries**

An access manager can specify the Decision Support categories that the DSOnly user should be able to access. Queries that match any of the criteria specified will be displayed on the lists of available queries. Access managers may only allow access to those areas that they have access to themselves. Areas from which a manager is restricted are automatically restricted to the users they setup.
Setting Up New Users

On the DSOnly User Access Management page is a table with all of the users that you manage directly. There is also a link to establish new DSOnly users.

To set up a new DSOnly user:

1. Click on the Manage New Users link.

2. This will bring up a form where you enter the UCD Login ID of the new user.

3. Once entered, click the Verify Login ID button. If the user to whom you are granting access is already a TP user, you will receive the following screen:

4. If the user has been verified, you will be taken to the screen where you set up access rights as outlined below.

Each non-TP user must have a UCD Login ID before being granted DSOnly User access.

If the login ID was mis-typed, return to the Manage New User screen and re-enter the ID.
Editing User Access Rights

Once you have setup a DSOnly user, you have to establish their access rights. You can also edit the access rights for any users you have already setup. Clicking the Edit link next to a user name on the DSOnly User Access Management page will take you to the Edit User Access Permissions page. This page allows you to specify what information a user is allowed to view.

As an access manager, you can grant access to any organization, account, sub-account, or project at or below your delegated authority. In addition, you can restrict the areas of Decision Support to which the user has access.

To view or modify the access rights for a user:

1. Click on the Edit link next to the user’s name. That will open the Edit User Access Permissions screen for that user. (If you have just setup a new DSOnly user, you will be taken to this page automatically);

2. Mark all the query categories, in the Report Types section, to which the user should have access;

3. In the Access Rights section enter an organization to which the user should have access. Include any associated sub-accounts or projects, if applicable;

4. Click the button after each entry to add it to the list. Repeat steps 3 and 4 as needed;
5. Enter any accounts, not within the previously specified organizations, to which the user should have access. Include any associated sub-accounts or projects, if applicable;

6. Click the **Add To Access List** button after each entry to add it to the list. Repeat steps 5 and 6 as needed;

7. Click the **Update User Access Rights** button to submit the changes for verification.

When the changes are submitted, the system performs edit checks against the entered information. Every account and organization listed is checked for validity and whether they are within the access manager’s organization hierarchy. The manager will then receive a confirmation screen detailing the changes they are about to make, as seen below. If any information entered on the authorization screen is found to be invalid, it will be noted on this screen (as seen below).

8. If all changes are valid, click on the **Process Changes** link to put them into effect.

After processing for a moment, the system will display a result page (which looks almost exactly like the conformation page) detailing what was just done.

9. Click on the **Return to Access Manager Page** link to return to the Access Manager main menu.
Revoking User Access Rights

To revoke a DSOnly user's access, click on the **Revoke All** link next to their name. You will be presented with a screen verifying the action you are about to take. If you are sure, click on the **Process Changes** link. Alternatively, you could edit the user's access rights and revoke their account and organization access rights individually. If the system detects that you no longer grant them *any* rights, it will automatically remove them from your user list.

If an access manager removes a DSOnly user from their list of managed users, all access rights granted by that access manager will be revoked. Access rights granted by any other access manager will be retained. However, if the access manager is the *only* manager for a DSOnly User, then removing that user will disable their Decision Support account.

Managing Subordinate Managers

When you are granted access manager status, your grantor may also give you the ability to re-delegate your authority to lower levels. If you have been granted delegation rights by at least one manager, another section will appear at the bottom of the **DSOnly User Access Management** screen. The lower section of the screen has a table that lists the subordinate managers to which you have delegated authority.

If an access manager has been granted the ability to delegate their authority, they may delegate part or all of their access manager rights to another person. That person, in turn, then becomes an access manager. This is not a *transfer* of authority, as the granting manager maintains the ability to grant access to DSOnly users and to other managers. The subordinate manager then has the ability to grant DSOnly user’s access within whatever authority the granting manager specifies. The subordinate manager may also be given delegation authority to create subordinate managers.
Delegating Organizations

Only organizations completely within your delegated authority may be delegated, in turn, by you. Overlapping organizations will be ignored. In other words, you if specify an organization, and then an organization subordinate to it, the lower level organization will be ignored.

Granting Delegation Authority

An access manager must allow all of the authority given to a subordinate manager to be delegated, or allow none of it. It is not possible to specify that they have the ability to grant DSOnly users access to an organization, but only have delegation authority within part of that organization.

Setting Up New Access Managers

If you have been given delegation authority, then you can begin setting up subordinate managers who have the rights to setup DSOnly users within the limits that you specify.

To set up a new access manager:

1. Click on the Delegate Authority to a New Person link in the lower section of the screen.

2. This will bring up a form where you enter the UCD Login ID of the new manager.

3. Once entered, click on the Verify Login ID button.

If the user you selected is not an active DaFIS User, with normal status, you will receive the following message:
4. If the user has been verified, you will be taken to the screen where you set up delegation authority as outlined below.

**Editing Manager Delegation Authority**

Once you have setup a subordinate access manager, you have to establish their authority and delegation rights. Clicking on the Edit link next to the user name of a subordinate access manager will bring up the Update Manager Authority page where you specify the organization hierarchies the subordinate manager has authority over, and whether they can delegate that authority to others.

To modify a subordinate access manager’s access:

1. Click the Edit link next to the name of the manager whose access you wish to edit. This will take you to the Update Manager Authority page. (If you have just setup a new manager, you will be taken to this page automatically);

2. Select whether this manager should be able to re-delegate their authority. If this checkbox is selected, then all organizations you grant to this new manager may be re-delegated by them;

3. Enter all organizations to which the manager should have authority. This list specifies the organization hierarchies that the manager will have authority over;
4. Click on the **Update Manager Information** button to submit the changes; When the changes are submitted, the system performs edit checks against the entered information. Every organization entered is checked for validity and whether they are within your re-delegation authority. You will then receive the confirmation page like the one shown below, detailing the changes they are about to make. If any information entered on the authorization screen is found to be invalid, it will be noted on this screen (as seen here).

<table>
<thead>
<tr>
<th>Manager: HENNESSY, MOLLY C</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID: HCH</td>
</tr>
</tbody>
</table>

**Pending Actions**

- Add user to your subordinate manager list.
- 3-ACCT is not within your delegated authority. It will not be processed.
- Grant user authority to manage the following organization(s):
  - 5-ACDF

**Process Changes**

5. If all changes are valid, click on the **Process Changes** link to put them into effect.

After processing for a moment, the system will display a result page (looking almost exactly like the confirmation page) detailing what was just done.

6. Click on the **Return to Access Manager Page** link to return to the Access Manager main menu.

**Removing a Manager’s Authority**

Partial revocation of authority can be made at any time by editing the subordinate manager’s settings (see page 13). However, the system also provides a utility to revoke all of a subordinate manager’s authority. When revoking a manager’s authority, there are four options available:

- Transfer delegations to a new access manager;
- Transfer delegations to an existing access manager;
- Transfer delegations to revoking manager;
- Revoke all delegations.

The first three options are designed so that if an access manager leaves the university or changes responsibilities, the delegations need not be re-created.

To remove all of an access manager’s authority, click on the **Revoke all delegations and user rights** radio button. You will be taken to the **Revoke Manager Authority** page.
Here you are presented with the four options. Each option is covered below, along with its implications and instructions.

**Transfer Delegations to a New Access Manager**

This option will transfer all of the rights you are revoking to a specified user, who will thus become an access manager. As when creating a new subordinate manager, the user ID entered will be checked for validity and that it is not one of the manager’s existing subordinate managers.

1. Click on the **Revoke All** link to the right of the manager whose authority you wish to remove;

2. Select the **Assign delegations and users to a new manager** option by clicking on the radio button;

3. Enter the login ID for the person to whom you wish to transfer this authority. Remember, as when setting up a new manager, this person must already be an active DaFIS user;

4. Click **Revoke Manager Authority** to submit your change.

If the login ID is for someone who is already one of your subordinate managers, you will receive the following message:

---

**Pending Actions**

- **HEWLETT.JAMES G (JIM3082)** is already one of your subordinate managers. To assign delegations to this user, please use Rev B Revoke Manager Authority page.
If the login ID you entered is not that of an active DaFIS user, you will receive the following message:

**Manager:** HENNESSY, HOLLY C  
**User ID:** HCH

**Pending Actions**
- OKHREMCHOUK, IRINA STEFANO (BOOK) is not an active TP user. Only active TP users may be access managers.

5. Once you have entered an appropriate login ID, you will receive a confirmation notice indicating all of implications of the requested change. Review this screen carefully to make sure you want all of the indicated changes made. Remember, this is an all or nothing situation;

**Manager:** HENNESSY, HOLLY C  
**User ID:** HCH

**Pending Actions**
- Add KCLUDWIG to your subordinate manager list.  
- Add 3-ACDP to authority for KCLUDWIG.  
- Remove delegation authority from HCH.  
- Remove HCH from your delegate list.  
- Disable HCH as an access manager.

**Process Changes**

6. If all changes are valid, click on the **Process Changes** link to put them into effect.

After processing for a moment, the system will display a result page (looking almost exactly like the confirmation page) detailing what was just done.

7. Click on the **Return to Access Manager Page** link to return to the Access Manager main menu.

**Transfer Delegations to an Existing Access Manager**

This option will transfer all of the revoked authority to another of your subordinate managers. The selected user must have sufficient authority to completely cover the delegations and users of the manager whose access is being revoked. The system will give a warning if the new manager’s authority is not sufficient.

1. Click on the **Revoke All** link to the right of the manager whose authority you wish to remove;

2. Select the **Assign delegations and users to an existing manager** option by clicking on that radio button;
3. Select the person to whom you wish to transfer this authority. The list to
the right of this option will list all of your subordinate managers. Someone
from this list must be selected to receive the transfer of the delegations;

4. Click **Revoke Manager Authority** to submit your change;

If the manager you selected does not have sufficient authority to assume the
new delegations, you will receive a message asking you to first grant additional
authority to the new manager you are creating to cover proposed authorities.

5. Once you have selected a manager with sufficient authority, you will
receive a confirmation notice indicating all of implications of the requested
change. Review this screen carefully to make sure you want all of the
indicated changes made. Remember, this is an all or nothing situation;

6. If all changes are valid, click on the **Process Changes** link to put them into
effect.

After processing for a moment, the system will display a result page (looking almost
exactly like the conformation page) detailing what was just done.

7. Click on the **Return to Access Manager Page** link to return to the Access
Manager main menu.

**Transfer Delegations to Revoking Manager**

A manager can also assume direct control of all delegations that the subordinate
manager made. **Note:** there is no way to selectively transfer delegations. Before
making this selection, you should be sure that you want to take on all of the
delegations.

1. Click on the **Revoke All** link to the right of the manager whose authority you
wish to remove;
2. Select the *Assign delegations and users to yourself* option by clicking on that radio button;

3. Click the *Are You Sure?* checkbox. If you do not mark this box, you will receive the following message when you try to submit the change:

![JavaScript Application]

*You must select the checkbox to verify this action.*

OK

4. Click *Revoke Manager Authority* to submit your change;

5. You will receive a confirmation notice indicating all of implications of the requested change. Review this screen *carefully* to make sure you want *all* of the indicated changes made. Remember, this is an all or nothing situation;

Manager: HENNESSY, HOLLY C
User ID: HCH

**Pending Actions**
- Remove delegation authority from HCH.
- Remove HCH from your delegate list.
- Disable HCH as an access manager.

Process Changes

6. If all changes are valid, click on the *Process Changes* link to put them into effect.

After processing for a moment, the system will display a result page (looking almost exactly like the confirmation page) detailing what was just done.

7. Click on the *Return to Access Manager Page* link to return to the Access Manager main menu.

**Revoke All Delegations**

Finally, a manager can simply revoke all delegations the subordinate manager has made. It is important to realize the effects that revoking authority has on a subordinate manager and all of the DSOOnly users they setup.
When access manager authority is revoked, the system searches down the manager's hierarchy of users and subordinate managers. Any access or delegations granted by this access manager will be revoked. If the users involved have access or delegations granted by another access manager, they will retain those. However, if any of the DSOnly users do not have additional access rights, then revoking the manager's authority will disable the DSOnly users' Decision Support accounts.

To revoke an access manager's access:

1. Click on the **Revoke All** link to the right of the manager whose authority you wish to remove;

2. Select the **Revoke all delegations and user rights** option by clicking on that radio button;

3. Click the **Are You Sure?** checkbox. If you do not mark this box, you will receive the following message when you try to submit the change:

   ![JavaScript Application]

   You must select the checkbox to verify this action.

   OK

4. Click **Revoke Manager Authority** to submit your change;

5. You will receive a confirmation notice indicating all of implications of the requested change. Review this screen **carefully** to make sure you want **all** of the indicated changes made. Remember, this is an all or nothing situation;

### Pending Actions

- Revoke management authority from user on the following organizations:
  - 3-ACDF
- The above revocations had the following affects on these subordinate managers and users:
  - Manager **REINDROP** will have their authority to delegate 3-ACDF revoked
  - Manager **KCLUGWIG** will have their authority to delegate 3-ACDF revoked
  - DSOnly User **DOCX** will have their right to view 3-ACDF revoked
  - Remove delegation authority from **KMCARPEN**
  - Remove **KMCARPEN** from your delegate list
  - Disable **KMCARPEN** as an access manager.

### Process Changes
6. If all changes are valid, click on the Process Changes link to put them into effect.

After processing for a moment, the system will display a result page (looking almost exactly like the confirmation page) detailing what was just done.