User Rights Management

Access Groups and Roles

Prerequisites

- Veritas eDiscovery application version 8.2 or higher.
- **Access Groups** now includes cases and locations. This affects workflow. Meet with stakeholders and decide whether and how to use **Access Groups.**
- If you decide to use **Access Groups**, create them and make all needed group and role assignments immediately after installation or upgrade.
- If you are already using **Access Groups** and are upgrading, understand how users will be affected.
  - There is a new role: **Group Admin**.
  - Custom roles will not change as a result of an upgrade.
  - Users assigned to groups with case authorization will retain case authorizations but lose group assignments. The Access Group Change Report will record results of remapping.
  - You cannot give a user both group access and case authorization.
- You need at least one **System Manager**. Only the **System Manager** role can create **Access Groups** and **Group Administrators**. Once created, the **Group Administrator** can create users and assign them to a group, **or** to specific cases.

Overview of Roles

Determine if one of these predefined roles fits your needs. Create additional roles only if needed; then test the new role.

- System Manager — Allows rights to all system, case, search, reporting functions.
- Group Admin — Add and remove users, cases, and other items from the group, and to perform other administrative tasks
- eDiscovery Admin — Manage Identification Data Map, perform Collections, Process, Analyze, Review.
- Case Admin — Admin-level access to one or more cases, search, tagging, export, and reporting functions.
- Case Manager — As with Case Admin, but no source setup.
- Case User — Search, tagging, export, reporting rights for a case(s).
- Collection Admin — Manage Identification Data Map, perform Collections.
- Legal Hold Admin — Administrator-level legal hold management.

Initial Workflow

1. Create the User

Create users and assign them to roles, or re-assign roles to existing users, from **System > Users**.

Note: Only **System Managers**, **Group Administrators,** or **Case Administrators** (with some restrictions) can do this.

2. Decide on **Group Access** OR **Case Authorization.**

You have a choice in how a user accesses cases. Either option will permit you to further restrict user access to cases.

- **Group Access**, in which all users assigned to an Access Group can interact with all cases in that Access Group. See step 3A.
- **Case Authorization**, in which users not assigned to an Access Group interact only with cases assigned to them. See step 3B.

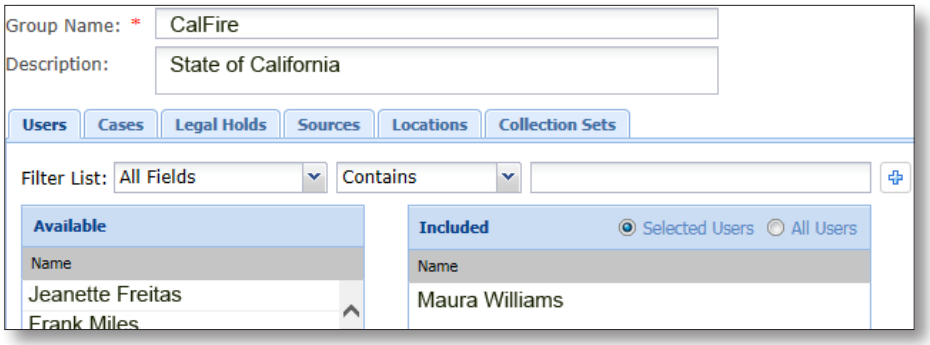
When creating a user, the group access comes up by default, but case access can be selected via a radio button. It can be changed later as well.

Tip: Make sure the person(s) in charge of adding Access Groups or adding Users has the correct role assigned to them.

3. **Create Access Group** OR **Assign Authorized Case**

3A.) Create Access Group

For Group Access: Create an **Access Group** for each independent section of your organization. From **System > Users**, click the **Access Groups** tab, then **Add**, and enter the group name and description. Specify the Users, Cases, and other assets assigned to that group.



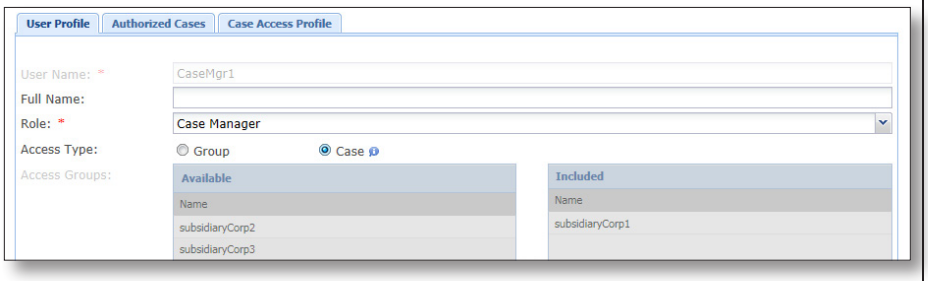
Create at least one **Group Administrator** for each Access Group. From **System > Users**, you can either add a new user with the **Group Administrator** role, or change the role of an existing user.

3b.) Assign Authorized Case

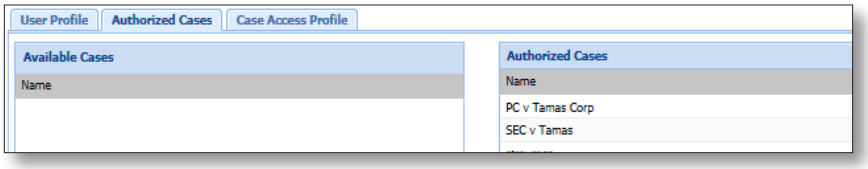
Case Authorization: For Case Authorized users, assign them to their authorized cases and give them roles when you create them.

Note: *you cannot give a user both group access and case authorization.*

A **User Profile** for a user who is assigned to a group will show the **Authorized Cases** tab grayed out.

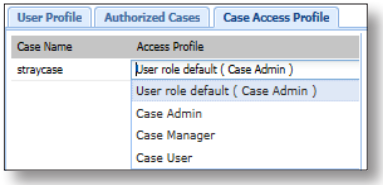


Click the **Authorized Cases** tab to specify which cases are authorized.



4. Optional: change Case Access Profile

By default, a user is given the Case Access profile of their role for the cases they can access. To change it, select a user, choose a case name, and select a different role from the pulldown. A case access profile is case specific.



5. Save the User

6. Passwords

Set the Password Length, Expiration Policy, and related login-security items. From **System > Settings**, click the **Security** tab and update the values. These are system-wide.

7. Notify the user

Inform the user of their new (or revised) Veritas eDiscovery user account.

FAQs

Why make more changes to the Access Groups feature?

This release completes the group access feature begun in release 8.0, which allowed organizing users collectively for ease of maintenance. Users, Legal Holds, Sources, and Collections Destinations were the original areas under Group Access control. Cases and Locations have been added.

What is Group Access?

Access groups can be used to segregate groups of users according to the functional units within an organization throughout the case's workflow.

Access groups are created by the **System Manager** role. Within each Access Group there are one or more **Group Admins**, who handle many of the tasks formerly handled by **Case Admins**, but who have access to all cases within a group. There are still **Case Admins**, **Case Managers**, and **Case Users**, as before.

For more information on groups, refer to the *Case Administration Guide*.

Do you still support pre-8.0 behavior, "pre-groups"?

Yes. If you do not create any **Access Groups**, the system still works. This is called **Case Authorized** behavior.

- A user who is not assigned to an access group can see authorized cases only if an administrator specifically assigns some cases but not others.
- When a user is not assigned to any access group, all cases, legal holds, sources, locations, and collection sets **that are not assigned to any access group** are accessible and able to be authorized.
- User access can be further restricted for specific cases by changing the user's case access profile for each case. Otherwise the user gets the default for the assigned role.

Note: After upgrading the eDiscovery platform to version 8.2 or higher, all cases, users, legal holds, sources, locations, and collection sets that are not part of an access group are accessible to all users, whether those users are assigned to Access Groups or not.

What about new users?

If you create a new user but do not specify or assign either an **Access Group** or specific cases, the new user will have access to everything accessible by the user who created the new user.

Note: If a **System Manager** creates a new user and does not assign either specific cases or **Access Groups**, that new user has access to everything.

What happens to a user who is both part of a group and assigned to a case when the system is upgraded?

- The user will lose group access: only previously authorized cases will be preserved.
- If you had users with both **Case Authorization** and **Group Access**, you must create new groups and assign users to them such that only the correct users will be able to access cases.

Tip: Plan the new groups prior to upgrade. To prevent users from seeing cases that they shouldn't, user reassignment must happen as part of the upgrade.

Which roles can add users?

Users can be added by the **System Manager, Group Administrator**, or **Case Administrator**.

- **System Manager** can create and assign users to any role, to as many **Access Groups** as desired, or to specific cases.
- **Group Admin** can create users for the that admin's group.
- **Case Admin** can create users for each of their authorized cases. A user added by the **Case Admin** belongs to that case only.
- **System Manager** can explicitly grant role and group management rights.

How do I give users access to the appropriate items with the correct privileges?

User **permissions** and **access** (or **authorization**) are defined by:

- The **role** you give the user grants default **permissions**. Permissions set by a role extend to all cases to which a user has access.
- Assigning the user to an **access group**, or **authorizing** the user for specific **cases**: both of these control which cases a user can access.

Note: If you assign a User to an **Access Group**, they can see all cases within that access group, subject to their role.

- Choosing an optional per-case **Access Profile** for that user is similar to giving the user a different role on a case-by-case basis.

What is an Access Profile?

If a user's permissions are not the same for every case, choose an **Access Profile** to further restrict which documents, folders, and tags a user can see within a case. **Access Profiles** have predefined rights and are case-specific. Refer to the *System Administration Guide: Managing User Accounts For a Specific Case* for details.

Why is there a new Group Admin role?

There is a new role: **Group Admin**. A Group Admin works with all cases in the same group.

Only the **System Manager**, the **Group Admin**, and the **Case Admin** can add users and assign them to roles.

The **System Manager** has the broadest administration powers, and they extend across groups: for example, creating access groups, assigning users to mulitple access groups or cases.

Like a **Case Admin**, a **Group Admin** has access to all case administration, search, tagging, export, and reporting functions **within a group**. **Group Admin** powers are broader than the Case Admin powers.

The **Case Admin** has access to all case administration, search, tagging, export, and reporting functions **for a case**. The **Case Admin** role is for users who need to be restricted to these functions within a case.

In most cases, you will want to assign some users who are currently **Case Administrators** to be **Group Administrators** or **System Managers**, depending on if they need to see users or workflow outside of their own case or group.

What if none of the existing roles work for my user?

If none of the seven pre-defined roles can replace any custom roles, the **System Manager** can create a custom role. Refer to the *System Administration Guide*: *Managing User Accounts: Defining User Roles* for details.

For More Role and Privilege Information

See the *System Administration Guide*: *Defining User Accounts,* and *Access Groups and User Creation.*

For More Information on Case Administration

See the *Case Administration Guide: Defining New Cases* and *About Access Groups and Roles*

For More Information on Source Groups Setup

See the *Identification and Collection Guide: Setting Up Data Sources*.

For More Information on Legal Hold Groups

See the *Legal Hold Guide: About Legal Hold User Privileges,* and the *Managing Access Groups section of the Identification and Collection Guide*.

For More Information on Upgrade

See the *Upgrade Guide* and *Upgrade Overview.*

