

# User Reports

	Search
--	--------

**User accounts** give programs the ability to grant and prevent system access. Each account contains a user's personal and system-related information, such as a user ID and email address.

All user accounts are initially assigned to the lowest-level parent organization in which they are created. This organization defines the data that he or she can view and manage. Each user account is associated with a user role(s) and a set of permissions. A user can access data only for their assigned organization(s) and organizations lower in the hierarchy.

To learn how to manage users, see [Manage Users](#).

Report Name	Report displays...	Report Parameters	Field Names
Users With Org Access	Selected organization's users (active or inactive)	<ul style="list-style-type: none"> <li>Organization</li> <li>Disabled and Deleted Filter: Exclude Disabled and Deleted; Include disabled and Deleted</li> </ul>	<ul style="list-style-type: none"> <li>Username</li> <li>Last Name</li> <li>First Name</li> <li>Email Address</li> <li>Active Begin Date</li> <li>Active End Date</li> <li>Disabled Date</li> <li>Delete Date</li> <li>Last Login Date</li> </ul>
Users With Role Access	All users with the selected role	<ul style="list-style-type: none"> <li>Role</li> <li>Disabled and Deleted Filter: Exclude Disabled and Deleted; Include disabled and Deleted</li> </ul>	<ul style="list-style-type: none"> <li>Username</li> <li>Last Name</li> <li>First Name</li> <li>Email Address</li> <li>Active Begin Date</li> <li>Active End Date</li> <li>Disabled Date</li> <li>Delete Date</li> <li>Last Login Date</li> </ul>

[Back to the top](#)