



Account Manager Role in IWDS 2.0

IWDS 2.0 TECHNICAL TRAINING DOCUMENTS



Purpose

This document explains the permissions available to an IWDS 2.0 user with the Account Manager role.



Audience

This document is designed to inform IWDS users about user roles.



How Access Works

Access is based on two simple things: where you work (Location) and what you're allowed to do (Role).



Location



Role



Access

Location defines where a user can do something — statewide, an LWIA, or a single office.

Role defines what a user can do — the functions and records they can reach.

The Account Manager role has access to add, edit or remove users, view roles and permissions, and accept pending users.

- The Account Manager role does not have access to customers, providers, grants, reports, or other management tools.



Permissions Granted

Controls user access and role assignments across the system. Approves new user registrations, assigns and updates roles, and manages security settings. Often paired with Super User or Data Steward.

Permission	Description	Scope
SECURITY & USER ADMINISTRATION		
Manage registrants <i>registration-admin-manage-registrants</i>	Allows a user to approve or deny new users.	None
Create user	Allows a user to create a new user in the system.	SecurityAdmin

[IWDS 2.0 Site](#)



Account Manager Role in IWDS 2.0

IWDS 2.0 TECHNICAL TRAINING DOCUMENTS

Permission	Description	Scope
<i>security-admin-user-create</i>		
View user <i>security-admin-user-read</i>	Allows a user to read the list of available system users.	SecurityAdmin
Update user <i>security-admin-user-update</i>	Allows a user to update a user's status in the system.	SecurityAdmin
Delete user <i>security-admin-user-delete</i>	Allows a user to delete a user in the system.	SecurityAdmin
View role <i>security-admin-role-read</i>	Allows a user to read the list of available system roles.	SecurityAdmin
Assign users to role <i>security-admin-role-modify-assigned-users</i>	Allows a user to assign users to roles.	SecurityRoleAssignment
Impersonate users <i>security-admin-impersonation</i>	Allows a user to impersonate another user's security settings.	SecurityAdmin
Security admin tools <i>security-management-tools</i>	Allows a user to access the Security Management section.	None



Granting Role Access

Account managers can grant and remove access to users.

- The Account Manager role can add, change or remove user access to other users in their location
- The Account Manager cannot change their own access.
- If the account manager's role needs to be added to an LWIA and there is no other account manager at the LWIA level, contact the state account manager for assistance.



Users

The Users section is where user access is changed, added, or removed.

- Navigate to Users by going to Management Tools, Security Management, Users.

[IWDS 2.0 Site](#)



Account Manager Role in IWDS 2.0

IWDS 2.0 TECHNICAL TRAINING DOCUMENTS

- The page contains:
 - Search bar – type start of name or email address to find users
 - Add New User button – used to create new user access
 - Action buttons – view, edit, impersonate

IWDSSTAGING

[Home](#)[Dashboard](#)[Management Tools](#)

Hi, Test Account Manager

Using impersonated permissions.

Manage User

[Add New User](#)

Email	First Name	Last Name	Status	Action
testaccountmanager@email.com	Test	Account Manager	Active	View Edit Impersonate

- View – shows the granted and denied permissions by user.
- Edit – the account manager to change the email, name, account status, roles, LWIA and assigned offices.
- Impersonate – allows the account manager to temporarily view and use the system from the user's perspective to help troubleshoot issues, verify access, or provide assistance without needing the user's login information.

[IWDS 2.0 Site](#)



Account Manager Role in IWDS 2.0

IWDS 2.0 TECHNICAL TRAINING DOCUMENTS



Roles

The Roles page shows the roles available in IWDS 2.0

- Navigate to Roles by going to Management Tools, Security Management, Roles.
- This page describes each role available and contains a way to search for roles.
- Use this page to assist in granting the correct roles for users.

Manage Roles			Search keyword
Name	Description	Actions	
Account Manager	Controls user access and role assignments across the system. Account Managers approve new user registrations, assign and update roles, and manage security settings. This role is critical to maintaining system access integrity.		
Auditor	Provides full read-only visibility across the system for monitoring and compliance purposes. Auditors can access all customer, application, service, grant, and provider data, as well as uploaded documents and logs. This function cannot modify any records.		
Career Planner	Supports direct service delivery to customers. Career Planners can create and maintain customer profiles, enter applications, assessments, and case notes, manage self-services, and track customer progress through program outcomes.		
Data Steward	Maintains data integrity and quality across the system. Data Stewards can edit restricted or sensitive fields, correct historical and post-exit data, and resolve data quality issues. This role carries elevated data editing authority and should only be assigned to staff responsible for data governance.		
Development Team	Full access to all permissions for development and testing purposes in the pre-production environments only.		
Entity Provider (special)	Provides limited, narrowly defined provider access for users who need to view or update specific provider information. This role has a restricted scope and is appropriate only when the Entity Provider Admin role is not warranted.		
Entity Provider Admin	Maintain provider entity data, manage provider user accounts, and control access at the provider level for a single provider.		
Front Line Support	View and create users, enter basic customer information, intake customers, and help with information-only services. They cannot enroll customers or view confidential case notes.		
Grant Administration	Manages grant records, funding sources, and grant-level administrative functions within the system. This function focuses on the financial and administrative infrastructure that supports service delivery, and does not include direct customer case management.		

Page 1 of 1 << 1 >> 1 15



Pending Users

Pending users show users who have requested access to IWDS 2.0.

- The account manager can view

WDST

LAST

Home

Customers

Dashboard

Reports

Management Tools

Manage Pending Registrations

Search keyword

Last Name	First Name	Email	Work Location	Role	Actions
[REDACTED]	[REDACTED]	[REDACTED]	07 - The Chicago Cook Workforce Partnership	Select a role	
[REDACTED]	[REDACTED]	[REDACTED]	07 - The Chicago Cook Workforce Partnership	Select a role	
[REDACTED]	[REDACTED]	[REDACTED]	07 - The Chicago Cook Workforce Partnership	Select a role	
[REDACTED]	[REDACTED]	[REDACTED]	07 - The Chicago Cook Workforce Partnership	Select a role	
[REDACTED]	[REDACTED]	[REDACTED]	19 - Workforce Investment Solutions	Career Planner	

IWDS 2.0 Site



Account Manager Role in IWDS 2.0

IWDS 2.0 TECHNICAL TRAINING DOCUMENTS

the pending registrations and approve or deny by using the action buttons.

- To add a user to your location from pending users, select the work location, role and click on the green check mark.

The Illinois workNet Center System, an American Job Center, is an equal opportunity employer/program. Auxiliary aids and services are available upon request to individuals with disabilities. All voice telephone numbers may be reached by persons using TTY/TDD equipment by calling TTY (800) 526-0844 or 711. This workforce product was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration.

[IWDS 2.0 Site](#)



Illinois
Department of Commerce
& Economic Opportunity



**Helpdesk.illinoisw
orknet.com**



www.illinoisworknet.com