Aging and People with Disabilities

Community Services and Supports Unit

OREGON DEPARTMENT OF
Human Services

Area Agencies on Aging (AAA) Onboarding Guide

April 2026

Contents

Purpose and Background

This guide is for Type A and Type B contract AAA offices who are requesting system access or updating system access for employees through the Office of Information Services (OIS) Service Desk portal.

The Individual Access Request (IAR) is also known as the 786 form. The IAR is where supervisors request new access, modify access or terminate access for staff. The IAR can only be submitted through the OIS Service Desk portal; the paper version of the 786 is being phased out and will be retired soon.

The IAR requires internet access and a secure connection to the state network. This is done through Citrix, on-site in a state office or through state issued VPN. AAA users will primarily use Citrix when accessing the state network for their work.

Please notify sua.email@odhs.oregon.gov with any suggestions or updates.

Multi-factor Authentication (MFA)

Multi-factor Authentication is a security system requiring more than one method of authentication to verify the users' identity to log into applications. MFA creates a layered defense, making it more difficult for an unauthorized person to access a computer, network or database.

All employees and partners are required to use MFA when accessing any Microsoft 365 app. This includes apps like OWL, Outlook, Teams, OneDrive, and SharePoint.

See Multi-Factor Authentication for Partners for additional information and set-up steps.

Getting Started

1. Connect to Citrix and log into the OIS Service Desk portal.
2. Click on "More"
3. Click on "Individual Access Request (IAR) MSC 0786"
4. Please read through the "Important Update" section for more information
5. Select one of the following requests:
    a. Identity Management Request (IMR) – For onboarding/offboarding of users and name/email address changes. Skip to New User – Identity Creation.
    b. Access Management Request (AMR) – For requesting access management actions for new/active users. An AMR can now be requested for up to 15 individuals in one request. Skip to New User: AMR

IMR versus AMR

The IMR is used for newly hired staff who do not have Partner numbers (P numbers) or access to any Oregon Department of Human Services (ODHS) systems. The IMR is specific to the individual user profile and once completed, only requires updates if the user changes their name, email address or they are no longer employed by the AAA. The IMR is specifically used to:

- Create a new network account (identity)
- Re-enable of a previously disabled network account
- Change personal identity attributes for a user (name, email address, etc.)
- Disable an account for an individual; usually because they are separating from employment

The AMR is used for newly hired and existing users to request access or changes to the ODHS systems that they use. The AMR is specifically used for:

- Shared folders
- ONE Oregon Eligibility
- MMIS (Medicaid Management Information System)
- Other Services

Identity Management Request

Managers can submit the IMR with a future effective date for new employees. The employee must have their unique agency email address created prior to submission of the IMR.

As you navigate the IMR, additional questions will generate depending on your responses. Please ensure that you complete all the required sections before proceeding.

New User: Identity Creation

1. It is important to verify that the user does not have an existing network account from another employer. This can happen if the employee was previously employed by another AAA, ODHS or Oregon Health Authority (OHA).
2. If the user has an existing profile, go to Existing User: Identity Update or Removal
3. If the user has no existing profile, select "Click here to create a new identity for this individual if you are unable to locate a current identity."
4. Action to Be Taken will auto populate with "Create a new identity for an individual using the attributes listed below."
5. Identity Attributes:
    a. Contract Type: Contractor/Partner
    b. State Email and Teams: AAAs should not request a state email account unless specifically instructed by the CSSU manager
    c. Partner/Contractor Organization Name: all supervisors who submit requests should use the same naming convention and avoid abbreviations. **Best practice – use the name listed on your contract.**
    d. External Email Address: this is the user's unique agency email address and not a shared email address. **Best practice – create AAA email for employee before submitting the IMR.**
    e. Sponsoring Agency: ODHS
    f. Sponsoring Department: APD
    g. Sponsoring Unit: CSSU

h. First Name: Please verify the correct spelling of the user’s first name

i. Last Name: Please verify the correct spelling of the user’s last name

j. Work Address: Agency address where user is located

k. Position/Title: What you enter here is how the user will appear in the system. **Best practice: Use your agency position description.**

l. Sponsoring Manager: Current CSSU manager. Search by name, Rodney Schroeder or OR0097055.

6. Effective Date and Manager Approval:

   a. The earliest effective date is the next business day. No same day requests are processed. **Best Practice: Submit the IMR up to one week before the employee start date.**

7. Summary: Review for accuracy and submit.

   a. The AMR can also be submitted at the same time by selecting Yes. Skip to New Employees - AMR.

Existing User: Identity Update or Removal

See Getting Started to log into the OIS Service Desk Portal.

1. To re-enable an account that was previously disabled:

   a. Search for user’s name by P number, name or email address

   b. Select “Re-enable this disabled identity”

   c. Follow steps for New User: Identity Creation

2. Changes to an account include the following:

   1. User’s name

2. Email address
3. Work address
4. Position or job title

a. Search for user's name by P number, name or email address
b. Select "Update attributes to this selected identity"
c. Follow steps for New User: Identity Creation

3. To disable an account:
    a. Search for user's name by P number, name or email address
    b. Select "Disable this selected identity"
    c. Enter effective date the action should take effect.

Note: The account will be disabled at 5:00 P.M. Pacific Standard Time on the selected date.

Access Management Request

Note: The user must have a completed IMR before an AMR can be processed. If the AMR is requested before the IMR, this will cause delays.

New User: AMR

1. Selected Identities: Search by name or P number. If the user is not displaying, verify that the IMR has been submitted.
2. Contract type: Contractor/Partner
3. Access Change Type: New Request
4. User Access Role (UAR): Defaults to "No"

5. Access Area Selection:
    a. Citrix Application Access
    b. MMIS (Medicaid Management Information System)
    c. ONE Oregon Eligibility
    d. SharePoint
    e. Other Services
6. Access Area Details:
    a. Citrix Application Access: Copy and paste the following into the text box.

MMIS, OWL, Oregon ACCESS, Mainframe, Oregon ACCESS training schoolhouse, ONE

    b. MMIS (Medicaid Management Information System): Copy and paste the following into the text box based on the user role. Select only one role for each user.

Case managers and supervisors (those entering the authorizations):

- D_I_P_Buy_In_Inquiry_SPD
- D_I_P_Claims_Inquiry_SPD_01
- D_I_P_Financial_Inquiry_SPD
- D_I_P_Financial_Premium_Data_Update_SPD_01
- D_I_P_Plan_of_Care_Update_SPD_Field
- D_I_P_Prior_Auth_Update_SPD
- D_I_P_Provider_Inquiry_SPD

- D_I_P_Recipient_Update_SPD_Field_01
- D_I_P_TPL_Inquiry_SPD

Support staff (those paying the authorizations):

- D_I_P_Buy_In_Inquiry_SPD
- D_I_P_Claims_Inquiry_SPD_01
- D_I_P_Financial_Inquiry_SPD
- D_I_P_Provider_Inquiry_SPD
- D_I_P_Recipient_Update_SPD_Field_01
- D_I_P_TPL_Inquiry_SPD

c. ONE Oregon Eligibility: Copy and paste the following into the text box:

Read only access

d. Other Services: Copy and paste the following into the text box.

Laserfiche - APD AAA Case Information Secured - Read (access to APD AAA Secured records)

Laserfiche - SSP APD AAA Case Records – Read (access SSP/APD/AAA general records)

7. Effective Date and Manager Approval

   a. The earliest effective date is the next business day. No same day requests are processed. Best Practice: Submit the AMR before the employee start date and select the effective date as the employee start date.

   b. Manager who normally approves these requests: Current CSSU manager. Search by name, Rodney Schroeder or OR0097055.

8. Summary: Review for accuracy and submit.

Existing User: AMR

See Getting Started to log into the OIS Service Desk Portal.

Existing users can modify or rebuild their access. This is usually done when users change job duties. Do not use the AMR for Oregon ACCESS or Mainframe requests, see Existing Users: 784 IUP.

Existing users who need Oregon ACCESS or Mainframe software installed on Citrix, see New User: AMR and request these under Access Area Details.

1. Modify - Select this option if you need to add access after the initial AMR is submitted.
   a. Select: Modify - Existing access will not be revoked or modified other than what is designated on this form.
   b. Access Area Selection: Choose the access needed. See New User: Identity Creation for access types and remaining steps.

2. Rebuild - Select this option if you don’t know what access the user has and need to start from the beginning.
   a. Select: Rebuild - All current access will be REVOKED and access will be replaced with what is designated on the form below.
   b. Access Area Selection: See New User: Identity Creation for access types and remaining steps.

APD Individual User Profile – 0784

Complete the 784 IUP after the IMR and AMR are completed. The users P number is required on the 784 IUP, do not submit the 784 IUP until the P number has been created. This form is not submitted through the OIS Service Desk portal.
Download newest version of the APD - Individual User Profile form.

New users: 784 IUP

A new user is someone who doesn't have an assigned RACF (Resource Access Control Facility) ID. A RACF ID is a unique identifier and is used to log into Oregon ACCESS and Mainframe systems.

1. Select Add a new user ID
2. Employed by:
    a. Select the appropriate AAA branch from the drop-down.
    b. Leave SDistXX blank unless indicated by a user role below.
    c. Contractor agency/business name: Best practice – use the name listed on your contract.
    d. Employment status: Select the appropriate status from the drop-down. Select Permanent or Temporary employment status.
3. Non-ODHS user Information:
    a. Enter user's name: Best practice – use the same information from the IMR.
    b. RACF ID: Leave RACF ID blank, one will be assigned after the 0784 IUP is submitted.

c. Effective Date: The date you want the user to have access to the systems.

d. Access Agreement (AA) Number: This number is included in the AAA base contract on the Third Party Information System Access Request form (MSC 0785).

e. Position/title: Best practice – use the same information from the IMR.

f. Email Address: This is the user's unique agency email address and not a shared email address.

g. Phone: User's direct phone number. This phone number will be pre-populated on forms.

h. Partner ID number: A P number is required before the form can be submitted.

i. Work address: Business address where the worker is located.

j. Manager Information: Include local office manager information.

    i. If manager submits the 784 IUP via email, signature is not required.

    ii. If someone other than the manager submits the 784 IUP, manager signature is required.

k. Users cannot submit requests on their own behalf. If directors require access to systems, the request must be approved and submitted by the CSSU manager.

4. AAA office mainframe user groups: Select one of the following user roles:

    a. Supervisors and those who can approve exceptions.

        i. SSUCSRCH

ii. CA/PS General Read

iii. CAPS 2 HR Exception T2

iv. CAPS 2 Assess. State Admin Act

v. CAPS 2 Update OPI Type

vi. OAA/OPI General Update

b. Case managers for OPI/OPI-M or those who authorize services

i. SSUCSRCH

ii. CA/PS General Read

iii. CAPS 2 Update OPI Type

iv. OAA/OPI General Update

v. SW-NAPIS/OAA Service Update

c. Support staff or those who enter payments for services.

Note: If your AAA covers multiple branches, please enter the appropriate APD district on page one. SDistXX is needed to PSET into the correct district branch for HCW voucher payments.

i. SSUCSRCH

ii. SSUHKOPI

iii. SSUHKINQ

iv. SW-NAPIS/OAA Service Update

5. AAA Office Roles: GetCare (RTZ)

a. Supervisors/lead workers

i. Caretool

   ii. I&R
   iii. Issue Manager
   iv. Reports (All)

b. Staff who enter client data including I&R/Options Counseling/OAA services:
   i. Caretool
   ii. I&R
c. Staff who do not enter client data:
   i. Caretool Read Only
   ii. I&R Read Only
   iii. Reports (All)
d. Contact CSSU GetCare Admin or AAA liaison for the following permissions:
   i. Listing Maintenance
   ii. OAAPS year-end reporting
   iii. Mental Health programs
   iv. Issue Manager
   v. Client file merge
e. Do not select the following boxes:
   i. Agency Information
   ii. System Administrator
   iii. OPI

iv. OPI Pilot

v. Digital Signature

vi. Medicaid Branches

6. CA View MF user access: Report repository for Mainframe. Select correct distribution ID for the AAA. See CA View Reports for ODHS Business User for additional information.
7. Other: Load code, this is required for users to take actions in OA or Mainframe. The local office manager must designate a unique 2-3 letter code for each user. **Best Practice: Use worker initials, include middle initial if load code is already being used.**

   Copy and paste the following in the User group:
   Action needed: Add load code
   Load Code: (Unique 2-3 letter code)

8. APD BI Center: Report Repository, access is granted by user role and is based on the user position/title that is entered on page one.
9. Other: PCC (PointClickCare)
   a. PCC is used to check on hospital admissions and discharges and is currently optional.
   b. PCC basic training is required before accessing the system. See PCC online training for additional information.
10. Signature:
    a. If manager submits the 784 IUP via email, signature is not required.

   b. If someone other than the manager submits the 784 IUP, manager signature is required.

11. Annual IUP/ISAA review: Leave blank for new user request. Manager annual reviews of the 784 IUP is required for all users
12. Save the completed 784 IUP locally for annual updates. Best Practice: Refer to local 784 IUPs to create templates.
13. Submit the completed 784 IUP directly to: apd.security-requests@odhs.oregon.gov.

Existing Users: 784 IUP

Existing users can request name changes, have their access terminated, revoked, or modified. An existing user is someone who already has an assigned RACF ID. See New users: 784 IUP if the user doesn't have a RACF ID.

Best practice: Save the original 784 IUP. When a user needs a modification, update the original 784 IUP with the new information and have management sign off on the annual review.

   a. Terminate a user ID – select this if the user is ending employment with your agency and not going to another AAA or APD agency (if known).
   b. Revoke a user ID – select this if the user is going on extended leave or they are leaving your agency and going to another AAA or APD agency (if known). If unsure, select terminate a user ID.
   c. Change name on user ID – select this if the user's legal name has changed.

d. Modify access – select this if job duties have changed and rights need to be adjusted.

e. Keep all previous roles – select this to keep all existing access when modifying access.

Additional Systems

Random Moment Sampling (RMS)

RMS is used to determine the administrative costs for each program which includes staff salaries, training, support and supplies. This is done by calculating the amount of effort and resources spent by a group of staff on various activities recorded at random intervals. The collective total of these individual surveys helps determine the proportion of funds that should be allocated between each program by looking at the activities carried out by staff at specific moments in time. See RMS Training Materials, User Guides, Form and Technical Assistance for additional information. The RMS Coordinator will notify you which group to select when requesting user access.

RMS can only be requested after a user has a P number. Do not request access until the IMR has been processed. See New User: Identity Creation for steps to request a P number.

1. Confirm that the user has a P number and Citrix access.
2. Email rmms@odhs.oregon.gov with the following information:

   Please add the following staff to RMS surveys for our agency.

   - P number
   - Primary branch
   - Main work group or ADRC/OMAC
3. Wait 48 hours for the security groups to be updated

4. RMS surveys will begin the following month

Provider Time Capture (OR PTC DCI)

OR PTC DCI is the system used for home care workers to record their time and is the approved electronic visit verification (EVV) system. Case management staff, supervisors and voucher clerks will need access to OR PTC DCI. Access requests are completed by PTC Support and do not go through the OIS Service Desk Portal.

OR PTC DCI – New User

Additional guidance can be found on the QRG - Profile Requests for OR PTC DCI.

1. Select "Add a new staff user"
2. Fill in all boxes under "User information part 1" and "User information part 2." **Best practice – use the same information from the IMR.**

   Note: The primary branch name and branch number refer to the home branch of the user.
3. Supervisor Role: The most common role for staff using OR PTC DCI is the supervisor role. This role is not limited to supervisors only. Select Supervisor Role if the user needs to:
   a. Edit, reject or create entries in OR PTC DCI;
   b. Make updated to profiles for consumers housed in their cost center;
   c. Make updates to provider profiles;
   d. View some authorization information;
   e. Run reports.

4. Auditor Role: The auditor role is view only and does not allow any action to be taken in OR PTC DCI. This role is rarely used for AAA staff. Select the Auditor Role if the user needs to:
   a. View entries in OR PTC DCI
   b. View profiles for consumers housed in their cost center;
   c. View provider profiles;
   d. View some authorization information;
   e. Run reports.
5. If access is needed for multiple branches, add all required branches here.
6. Change Email/Phone Report: Recipients of this report will receive a message in OR PTC DCI monthly. The report lists all consumer and provider email addresses and phone numbers that have been updated in the last month. Staff who receive this report should review, confirm the updates and update state systems as necessary.

Not all users will require this report. Identify the user in your office who will be responsible for managing this report.

7. Fill in “Manager Information” section
8. Manager emails the completed form to PTC support at ptc.support@odhs.oregon.gov

OR PTC DCI – Deactivating a Staff Profile

If the user is ending employment with your agency and previously had access to OR PTC DCI, a Staff Profile Maintenance form needs to be submitted to the PTC Support Team to deactivate the user profile.

1. Select “Deactivate a User”
2. Fill out “User information for part 1”
3. Fill out “Manager Information” section
4. Manager emails the completed form to PTC support at ptc.support@odhs.oregon.gov

OR PTC DCI – Modifying a Staff Profile

If a staff member moves from one team or branch to another, their role or cost center may need to be modified in OR PTC DCI.

1. Select “Modify Access.”
2. Fill out “User Information Part 1.”
3. Under “Staff User Roles,” fill out the roles that need to be added or removed.
    a. Tip: for requests that are more complex, use the Notes section on the 3rd page to provide details of your request.
4. Fill out “Manager Information” section.
5. Manager emails completed form to PTC Support at ptc.support@odhs.oregon.gov

OR PTC DCI - Reactivating a Staff Profile

If a staff member returns to a role that requires access to OR PTC DCI, their profile will need to be reactivated. On the Staff Profile Maintenance form:

1. Select “Reactivate Access.”
2. Fill out “User Information Part 1.”

3. Fill in the "Staff User Roles" section indicating which roles/cost centers to remove or add.
4. If additional explanation is needed, use the Notes section on page 2 to provide the details of your request.
5. Fill out "Manager Information" section.
6. Manager emails completed form to PTC Support at ptc.support@odhs.oregon.gov

Workday Learning

Workday Learning is the online learning management system used by ODHS. Partners need to create a Workday Learning account in order to take state-offered training. Partners are called Extended Enterprise Learners (EELearners) in Workday. See Workday Learning: Information for Partners and Providers for additional information.

Each AAA has a unique URL for enrollment. Please contact your local affiliation manager for account set-up.

ONE

Once you receive confirmation that ONE access has been granted, email CSSU manager the following information:

User Name:

P Number:

Rights requested: Choose an item.

You can get this document in other languages, large print, braille or a format you prefer free of charge. Contact Aging and People with Disabilities at apd.ltss@odhs.oregon.gov or 503-945-5600. We accept all relay calls.

OREGON DEPARTMENT OF
Human Services
Community Services and Supports Unit
SUA.Email@odhs.oregon.gov
ODHS Community Services and Support

To top of document