

Deliverable Administration Review and Repository Tool (DARRT)

The Deliverable Administration Review and Repository Tool (DARRT) is a cloud-based solution providing a program management tool for CMS and Quality Improvement Organization (QIO) users. It provides the following functions:

- **Deliverables** - CMS CCSQ contractors, CCSQ Central Office staff, and CMS Regional Office staff with a central location for the submission, review, and storage of Quality Improvement contractor-related artifacts including, but not limited to, Contract Deliverables and Quality Measure Reports.
- **Quality Improvement Initiative (QII)** – Initiation and tracking.

Quick Start Guide

Step 1: If you do not yet have a HARP account or an EIDM or EUA account, register for a HARP ID. For instructions on the process, refer to the HARP handout.

Step 2: Once the HARP account has been created, log in to DARRT (<https://darrt.cms.gov>) to submit your role request.

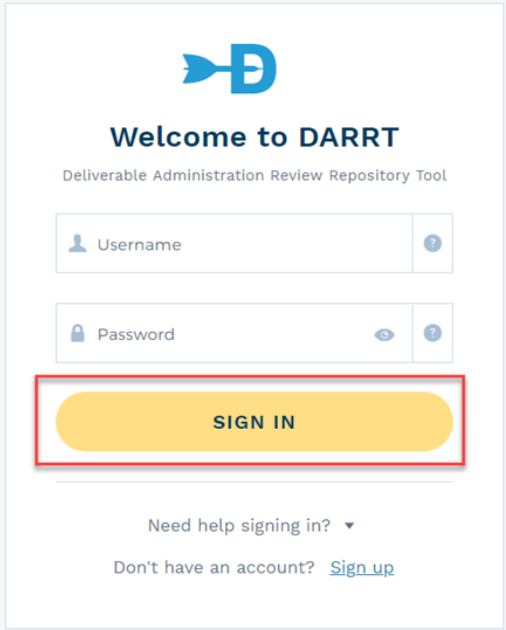
Which Role Do I Choose?

Each contractor **must** have at least one Security Official designated to process user requests or additional Security Official role requests.

Capability	Role
<p>This role should be given to the person at your organization who is responsible for approving, deleting, rejecting, deactivating role requests within your organization for Submitter and Support Contractor roles; generally, the Security Official. Users with this role will be able to:</p> <ul style="list-style-type: none"> • View users • Modify users (approve roles, delete role requests, reject role requests, and deactivate roles) 	User Admin

Capability	Role
<p>Users with this role will be able to:</p> <ul style="list-style-type: none"> • Submit deliverable documentation for assigned deliverables • View deliverable instances for assigned deliverables • Create QII referrals • Modify QII referrals • View QII details • Download QII documentation • View reports 	Submitter
<p>This role is for the CMS COR who is responsible for approving, rejecting, and acknowledging deliverables that are ready for review. Users with this role will be able to:</p> <ul style="list-style-type: none"> • View deliverable instances for assigned deliverables • Download deliverable documentation • Review deliverable instances (approve, reject, acknowledge) • Create QII referrals • View QII details • Download QII documentation • View reports 	Reviewer (COR)
<p>* CMS SMEs should request a SME role in DARRT. Users with this role will be able to:</p> <ul style="list-style-type: none"> • View deliverable instances for assigned deliverables • Download deliverable documentation • Create QII referrals • Delete QII referrals • Modify QII referrals • View QII details • Download QII documentation • View reports 	*SME
<p>This role is reserved for the Application Development Organization (ADO). Do not request this role.</p>	Application Admin
<p>This role is reserved for CMS. Users with this role can create and modify deliverables. Do not request this role.</p>	Admin (Deliverable)
<p>This role is for users accessing DARRT for read-only purposes.</p>	Support Contractor

Step 3: Sign in to DARRT.



1. Navigate to the DARRT URL darrt.cms.gov
2. On the sign-in form, enter your existing HARP Username and Password
3. Click **Sign In**
4. You will be prompted to provide your Multifactor Authentication (MFA) information. If you did not set up your MFA during your HARP account registration, you will be prompted to set up your (MFA) method before logging in. See Step 2.

Step 4: If you set up MFA in HARP, skip to Step 5.

If you did not previously set up MFA during your HARP account set up or profile update for existing users, you will be prompted to set up MFA before logging into DARRT.

HARP will present you with five multifactor authentication methods during your account registration process.

Refer to [HARP Help and FAQ](#) for more information.

SMS and Voice Authentication: Will require that you enter a single-use security code that is sent to your designated device when prompted.

<p>SMS</p> <p>Please enter your phone number to receive a text with a security code.</p> <p>Phone Number *</p> <input type="text"/> <p>Send Code</p>	<p>Voice</p> <p>Please enter your phone number to receive a call with a security code.</p> <p>Phone Number *</p> <input type="text"/> <p>Send Code</p>
---	---

Okta Verify: Will require that you download and install the Okta Verify app on your designated device. You will be requested to verify your identity by approving a push notification or by entering a one-time code during login the process.

<p>Okta Verify</p> <p>Please download the Okta Verify app to your mobile device and click the button below to initiate setup. The Okta Verify app generates two-factor authentication codes on your mobile device.</p> <p>Configure Okta Verify</p>	<p>Okta Verify Push</p> <p>Please download the Okta Verify Push app to your mobile device and click the button below to initiate setup. The Okta Verify Push app generates two-factor authentication codes on your mobile device.</p> <p>Configure Okta Verify Push</p>
---	---

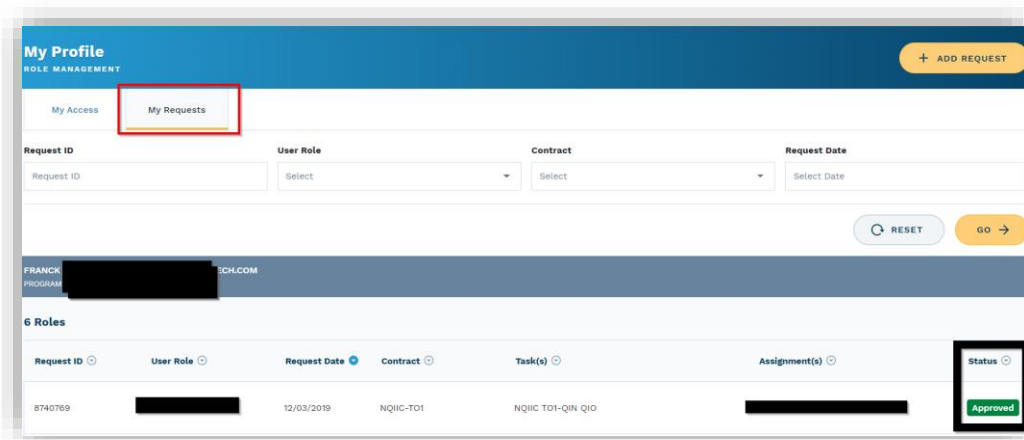
Google Authenticator: Will require that you download and install the Google Authenticator app on your designated device. You will be requested to verify your identity by entering a one-time code during the login process.

<p>Google Authenticator</p> <p>Please download the Google Authenticator app to your mobile device and click the button below to initiate setup. The Google Authenticator app generates two-factor authentication codes on your mobile device.</p> <p>Configure Google Authenticator</p>

After configuring your MFA, follow the instructions for your selected MFA method to gain access to DARRT.

Note: The OKTA Verify and Google Authenticator options require an application to be downloaded for push notifications and single-use code to your mobile device.

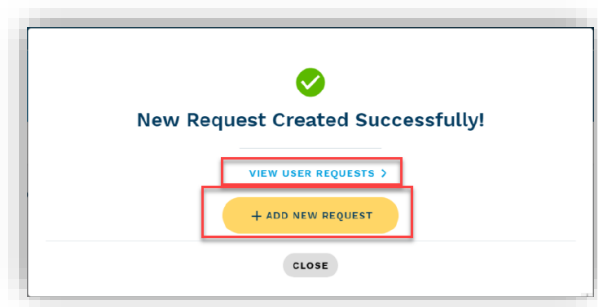
Step 5: Select the **ADD REQUEST** button on the User Role Management screen. On the Add New Request modal, select the Contract, Task, User Role, and Assignment(s) you require, then click Submit.



Note that a separate role request must be selected for each contract for users such as Reviewers (CORs) who are responsible for multiple contracts.

For descriptions on DARRT roles, click [DARRT Roles](#) to review roles before selecting a role.

Step 6: After submitting your request, DARRT will present you with a role request confirmation.



Once you have completed your role selection, you will be redirected to the User Requests page where you can review your pending requests. A notification email regarding your request will be sent by DARRT.

Step 7: The submitted role request will be reviewed for approval or rejection by your designated Security Official.

Need Help?

Please contact the QualityNet Help Desk with questions regarding registering, access, or general questions about DARRT via email at gnetssupport@hcqis.org or phone at 1-866-288-8912 (TTY: 1-877-715-6222). Monday – Friday, 8 am – 8 pm EST.