

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** - provides CMS CCSQ contractors, CCSQ Central Office staff and CMS Regional Office staff a central location for the submission, review and storage of Quality Improvement contractor related artifacts and 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.hcqis.org/>) to submit your role request.

Which Role Do I Choose?

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

Role	Capability
Reviewer (COR)	<p>This role should be given to the CMS COR who is responsible for approving, rejecting and acknowledging deliverable 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
SME	<p> CMS SMEs and Support Contractors such as National Strategic Leadership (NSL), National Administration Support (NAS) and Improvement Evaluation Contractor (IEC) 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 • View QII details • Download QII documentation • View reports
Application Admin	This role is reserved for the Application Development Organization (ADO). Do not request this role.
Admin (Deliverable)	This role is reserved for CMS. Users with this role can create and modify deliverables. Do not request this role.
Support Contractor (Help Desk)	This role is reserved for the Help Desk.

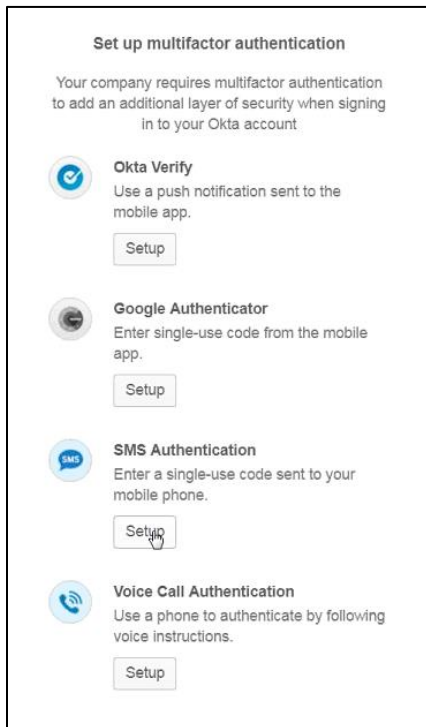
Step 3: Sign in to DARRT

1. Navigate to the DARRT URL darrrt.hcgis.org
2. On the Sign in form, enter your existing EIDM or EUA Username and Password or your HARP Account credentials
3. Click Sign In
4. You will then be prompted to set up your Multifactor Authentication (MFA) method if you did not previously select an MFA method in HARP.

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.

OKTA will present you with multifactor authentication methods. You may elect to set up one or more. Upon selecting your preferred method by clicking Setup, OKTA will walk you through the setup process.



OKTA Verify

Allows you to receive push notifications from the app and just select “Approve” or “Deny” when prompted for multifactor authentication.

Google Authenticator

Will require that you enter a single-use security code when prompted.

SMS Authentication

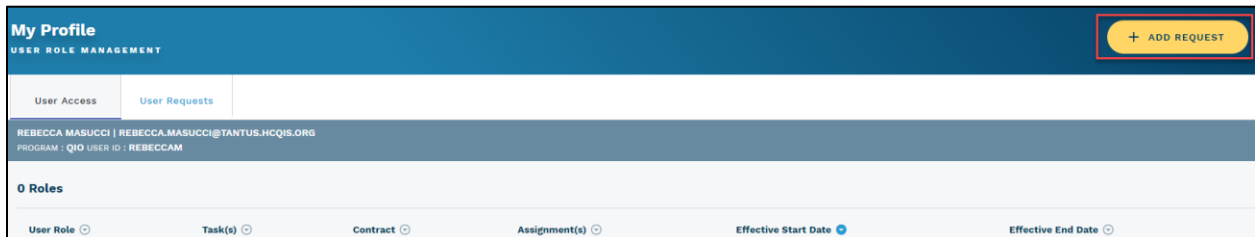
Will require that you enter a single-use security code that is sent to your designated device when prompted.

Voice Call Authentication

Will require that you use a phone to authenticate by following voice instructions.

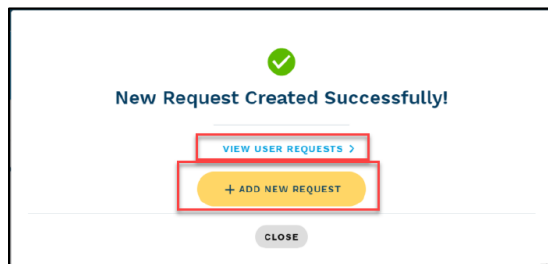
Note: that the OKTA Verify and Google Authenticator options require an application to be downloaded for push notifications and single-use code to your mobile device.

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, and 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.

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 Service Center with questions regarding registering, access, or general questions about DARRT via email at qnetssupport@hccjis.org or phone at 1-866-288-8914 (711 for Telecommunications Relay Service).