CRITICALL ONTARIO

CCIS
Critical Care Information System

Registration Guide

Version 14.0 | 10/01/2024

Prepared By:

CCIS Team

CritiCall Ontario

Table of Contents

INTRODUCTION

The purpose of this guide is to review the account management process for all stakeholders who access the Critical Care Information System (CCIS). For more information on how to use the online CCIS Account Management portal refer to the CCIS eLearning module. This information is located in the CCIS Resources/Registration Folder within the CCIS application.

This guide will provide information about the following:

- Identifying and Creating a Registration Authority (RA)

- Identifying and Creating a Delegate Registration Authority (DRA)

- Identifying and Creating a Local Registration Authority (LRA)

- Registering CCIS End-Users

- Changing roles and/or adding additional CCIS End Users

- End user password resets

- CCIS Role Combinations

1. Registration Authority (RA), Delegate Registration Authority, (DRA) & Local Registration Authorities (LRAS)

1.1 Responsibilities of the RA, DRA and LRA

In accordance with the CCIS Data Sharing Agreement, organizations who report data into the Ontario's Critical Care Information System (CCIS) are required to identify a Registration Authority (CEO or CIO) who assumes responsibility for all CCIS users within their organization.

The hospital CEO can appoint/revoke Delegate Registration Authorities who will assume the hospital's Registration Authority (RA) responsibilities on their behalf. Delegate Registration Authorities will have the ability to appoint/revoke CritiCall Ontario Local Registration Authorities (LRA's).

Hospital corporations cannot have more than two Delegate Registration Authorities at one time. The DRA's role can only be held by employers with hospital signing authority in a director role or above. The DRA role is not mandatory, but it can be used to facilitate coverage for the RA.

Local Registration Authorities (LRAs) are designated by each organization's Registration Authority (RA) or a Delegate Registration Authority (DRA). LRAs ensure the secure and appropriate registration of all CCIS end-users. This process ensures that each organization, in

accordance with the security and privacy policies of their organization, will securely manage CCIS end-user accounts.

2. Registration Authority (RA)/Delegate Registration Authority (DRA)

2.1 Completing the RA and DRA Registration Request/Change Online Form

To become a new Registration Authority (RA) or Delegate Registration Authority (DRA) complete the online form via the CCIS portal.

The following is a step-by-step outline of how the online form will be processed:

Step	Description
1	RA or DRA logs into the CCIS Portal and clicks on 'Request New Account'. Only one RA and 2 DRA accounts are allowed for one organization.
2	The RA and CCIS Helpdesk will receive the online form via email.
3	The RA will create/approve the new RA or DRA account LRA via CCIS Portal. If there is not an active RA, the CCIS Helpdesk will contact the requester.
4	The RA or DRA will receive an email with their new account information.

If a new RA or LRA is required for **non-hospital organizations** (e.g. Critical Care Services Ontario) contact the CCIS Help Desk at **CCISHelpdesk@CritiCall.org**

2.2 RA and DRA Attestation Responsibilities

RAs and DRAs must attest to their account within 30 days of account creation and on an annual basis.

Initial self-attestation must be completed within 30 days of initial sign in. Failure to do so will result in the deactivation of the RA/DRA account.

If annual attestation is not completed within one year, and 30-day grace period, the account will become inactive.

All other user account attestation is the responsibility of the LRAs. Refer to the LRA Attestation section for more information.
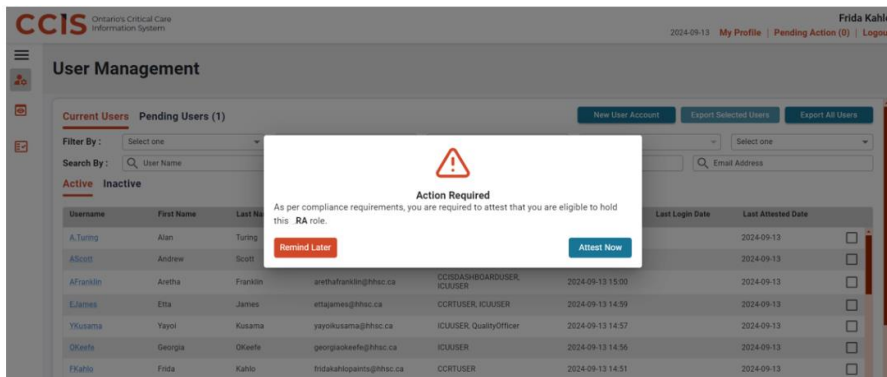
To attest your RA/DRA account follow the steps below.

Step 1

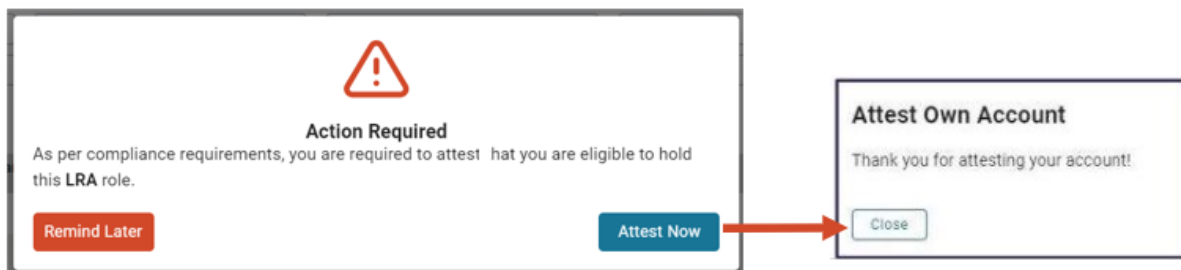A notification will pop up on initial sign in, and when the account is due for attestation.

If the user selects 'Remind Me Later', the pop up will disappear until next login

Note: if the user does not complete the attestation within 30 days, the account will be deactivated.

Step 2

Complete attestation by selecting 'Attest Now'.

The RA/DRA account is now attested for another year and will remain active, provided the user maintains their password change every 90 days.

3. Local Registration Authority

The LRA is a role assumed by individuals who have been delegated by the RA to perform the CCIS registration duties. **It is recommended that 3 - 5 individuals are assigned to the LRA role for hospitals, and 1-2 individuals for a Provincial/Region office**.

As an LRA, you are responsible for:

- Identifying prospective CCIS users.

- Adhering to the registration and/or identity management processes within your hospital or organization.

- Disabling accounts via the CCIS portal using your CCIS LRA account as soon as any user at your organization no longer requires CCIS access.

- Adhering to privacy and security policies and procedures within your hospital to ensure compliance with the Personal Health Information Protection Act (PHIPA).

- Validating that applicants are eligible to register for CCIS; please **consult with your organization's Privacy Officer or privacy expert if you have any questions regarding an access request**.

- Ensure end-users are aware of your organization's privacy policies with respect to securely accessing personal health information.

- Completing and authorizing CCIS online registration forms.

- Processing changes to registration information.

- Answering questions pertaining to the online registration process.

- Report registration issues to the CCIS Team.

3.1   Completing the Local Registration Authority Request/Change Online Form

The Registration Authority (RA) must complete and approve the online Local Registration Authority Request and Status Change Form via the CCIS portal.

It serves the purpose of identifying and/or changing the status of existing LRAs.

The following is a step-by-step outline of how the online form will be processed:

Step	Description
1	RA or DRA logs into the CCIS Portal using their accounts.
2	RA or DRA will create/approve the LRA request via CCIS Portal.
3	LRA will receive an email with their new account information.

3.2   Changes to LRA Status

Only an RA or DRA has the authority to change the status of the LRA. These changes include granting, suspending and revoking the LRA appointment that can be completed by logging into the CCIS Portal.

When an RA or DRA is *granting an individual LRA status*, they authorize the individual to collect, verify, and submit registration requests for CCIS users.

Deactivating an LRA is the removal of authority from the LRA by the RA or DRA. If the individual subsequently needs to become an LRA, the RA/DRA must reactivate the LRA request via the CCIS Portal. Possible reasons for LRA deactivation include:

- Individual no longer wishes to perform the role of LRA.

- Individual is no longer associated with the hospital.

- Inability to perform the LRA duties.

- Extended leave (such as maternity leave or sabbatical).

- Any other reason the RA deems appropriate.

3.3   LRA Attestation Responsibilities

New Account Attestation

LRAs must attest to their **own account** within 30 days of account creation. Failure to do so will result in the deactivation of your LRA account.

LRAs must attest to all **CCIS users within their organization** within 30 days of account creation. Failure to do so will result in CCIS user account deactivation.

Annual Attestation

LRAs must attest to their **own account** on an annual basis. Failure to do so will result in the deactivation of your LRA account.

LRAs must attest to all **CCIS users within their hospital or organization** on an annual basis. Failure to do so will result in the deactivation of CCIS user accounts.

Note: If annual attestation is not completed within one year, and 30-day grace period, accounts will become inactive.

Step 1

Sign in and identify users to attest. To filter for a specific site or unit, use the filter functions above the user list.

Step 2

User(s) who require attestation will have an exclamation mark in the column **Last Attestation Date**.
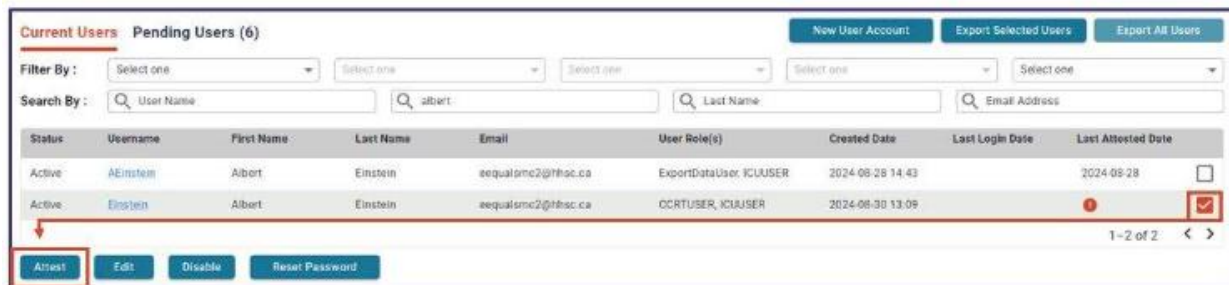
Only active users may be attested

Step 3

Select the user requiring attestation by clicking the check box.

Select **Attest**

Confirm that each user is authorized to hold their user account

Attestation is completed.

4.   Registering CCIS End-Users

There are two ways to register end users of CCIS:

1. *User requests access via CCIS Portal*:

    a)   User accesses CCIS portal **www.ccis-criticall.ca**

    b)   User clicks on *Request New Account* link on login screen of CCIS

    c)   User completes request for access and submits request for LRA approval

2. *LRA request User access via CCIS Portal*:

    a)   LRA accesses CCIS portal **www.ccis-criticall.ca**

    b)   LRA logs in to CCIS portal

    c)   LRA clicks on *New User Account* link

    d)   LRA completes form

    e)   LRA provides approval by clicking *Submit*

    f)   Account is created

Additional Important Notes

- Usernames/Passwords will not be communicated to LRA. The encrypted link to activate the account is sent to the end user automatically by the CCIS system when the account is created for the end user

- The details of First Login process can be found in *Login Guide*.

4.1 CCIS Users: Usernames, Roles and Access

The CCIS has multiple user roles, and what a user can do and see in the system depends upon that role. The table below lists the level of access, suggested role and corresponding CCIS role title. Please note that a single user can have more than one role, refer to the matrix in the Appendix for more information.

CCIS User ID (Username): In the CCIS Portal, the LRA will specify each end-user chosen CCIS username. These can be the same usernames as your hospital's information system, as long as the following criteria are met:

- Users cannot request IDs with special characters (examples: @, #, &, *, etc.). However, the underscore, period, and dash (_, ., -) are allowed in the **Username**

- Users cannot request IDs with language accents (examples: è, é, ç, á, â, etc.)

- User ID must be unique in CCIS system. If the provided User ID already exists in CCIS, LRA may create account by assigning another User ID. Prior to approving/creating an account it is the LRAs responsibility to verify if the user already has a CCIS account to fulfil their job responsibilities.

CCIS User Roles

User Role	Description	Suggested access for	User Access level	Entity
ICU USER	Enter Patient admissions, discharges and clinical data into CCIS	Nurse, Unit Clerk, ICU Manager	Site	1 Hospital
CCRT/PCCRT	Enter consults and monthly CCRT stats in the CCIS	Nurse, RT, DSS	Site	1 Hospital
Dashboard User	View the Bed Availability Dashboard and/or utilize the CCIS dashboard reports	CEO, CIO, ICU Manager, Quality, and DSS staff	Site or Corp	>=1 Hospital or Corp within own organization, Region or Province
Export Data User	Access to the Export Core Data reports	ICU Manager, and Director, DSS Staff	Site or Corp	>=1 Hospital or Corp within own organization, Region or Province
Quality Officer	Monitoring of CCIS patient census, Bed availability and clinical data entry and timeliness	ICU Director, Manager, Quality, Education	Site or Corp	>=1 Hospital or Corp within own organization
Privacy Officer	Monitoring of CCIS patient census, Bed availability and clinical data entry and timeliness	Hospital Privacy Department Staff	Site or Corp	>=1 Hospital or Corp within own organization
Registration Authority (RA)	Assumes responsibility for the CCIS users within their organization. Appoints LRAs to authorize user registration and maintenance. Authorize and disable LRA accounts	CEO, CIO, or equivalent	Corp	Corp within own organization
Delegate Registration Authority (DRA)	On behalf of the RA, Appoints LRAs to authorize user registration and maintenance. Authorize and disable LRA accounts	CIO, Director	Corp	Corp within own organization
Local Registration Authority (LRA)	LRAs authorize and disable CCIS user accounts and complete attestation process for all CCIS users	ICU Manager, Director, or delegate, IT Manager	Corp	Corp within own organization, region or province

CCIS User Access Level

CCIS User Access Level	Suggested Access for
SITE	Unit Nurse, Ward Clerk, Unit Clerk, Charge Nurse, Unit Manager, Quality
CORP	Hospital Manager, Quality, Decision Support or Analyst
REGION	Region Staff, Region eHealth Lead or Region CritiCall Care Lead
PROVINCE	This role is specific to MOH, CCSO and CritiCall users.

Additional Important Notes

- To add PHI access to Core Data Exports, approval is required from LRA

- Prior to approving/creating an account it is the LRAs responsibility to verify if the user already has a CCIS account to fulfil their job responsibilities. This is to avoid duplication of accounts within CCIS.

5. Changing roles and/or adding end-users to CCIS

An LRA will be able to request accounts for new end-users, facilitate password resets, and change/add roles to existing end-users. The following section outlines how these activities are accomplished.

5.1 Completing Registration Changes

The LRA will login to CCIS portal to complete any end-user registration changes.

The following notes regarding to additions, deletions and changes to roles for end-users:

- The LRA will log into the CCIS portal.

- The LRA will search for CCIS user accounts that requires change.

- In the CCIS user account LRA will be able to change the CCIS user's role, name, email address, and phone number. LRA will also be able to enable/disable account and complete a password reset.

5.2 End User Password Resets

In accordance with the CCIS privacy policy and considering the personal health information that is available with CCIS access, there is a strict procedure followed when end-users require their passwords reset.

End users should use the self-service feature to retrieve their forgotten password. If the end-user forgets the security questions and unable to retrieve their password, the following steps are followed:

Step	Title	Description
1	Self-Help	End Users use the **Forgot Password** functionality (defined in *Login Guide*) by entering the answers to Security Questions correctly and setting the new password
2	LRA – CCIS	- If the user does not remember the answers to security questions, the **Forgot Password** functionality cannot be used successfully - The end-user contacts one of their hospital's LRAs who will then use the CCIS Portal to reset password - LRA resets the password and CCIS system notifies the user with the instructions to set the new password

If there are any questions regarding the registration process, please do not hesitate to contact the CCIS helpdesk at **CCISHelpdesk@criticall.org** or, if the matter is urgent, page 1-866-740-3240 (available 24 hours per day; 7 days per week).

Additional Important Notes

- The account information of end user (passwords) is not shared with any person except the end user.

- After the LRA creates the account using the CCIS portal, the following activities are done by the user using the following self-service features. In this case, the end-user directly interacts with the CCIS:

  o First Login

  o Forgot Password

  o Update Personal Information

  o Change Password

  o Forgot Username

All these functionalities are described in *Login Guide*.

6. Appendix

The **Role Combination** is defined by the following table.

ROLES	ICUUSER	CCRT USER	PCCRT USER	DASHBOARD USER	EXPORT DATA USER	QUALITY OFFICER	PRIVACY OFFICER	RA	DRA	LRA
ICUUSER	X	X	X	X	X	X	X			
CCRT USER	X	X		X	X	X	X			
PCCRT USER	X		X	X	X	X	X			
DASHBOARD USER	X	X	X	X	X	X	X			
EXPORT DATA USER	X	X	X	X	X	X	X			
QUALITY OFFICER	X	X	X	X	X	X	X			
PRIVACY OFFICER	X	X	X	X	X	X	X			
RA								X		
DRA									X	
LRA										X

1. Additional rules regarding Role Combination are listed below:

   - If **ICUUSER** is selected, the user can select one of CCRTUSER or PCCRTUSER.

   - If **CCRTUSER** is selected, the user can select ICUUSER.

2. **RA**, **DRA** and **LRA** accounts cannot be combined with any other role.