ONE® ID Local Registration Authorities Procedures Manual

ONE® ID Business Support | 2026-07-10

Ontario Health

Document Information

Copyright Notice

All rights reserved

Trademarks

Document Control

The electronic version of this document is recognized as the only valid version.

Document Sensitivity Level

Medium

Table of Contents

Ontario Health

Appendices

Ontario Health

About this Document

This document for Local Registration Agents (LRAs) describes the various roles, responsibilities, and functions of an LRA for supporting ONE® ID processes within their organization on behalf of Ontario Health.

Audience

This document is intended for LRAs that have been authorized to execute ONE® ID processes on behalf of Ontario Health and their organization(s). An LRA should have an intermediate level of understanding of registration, service enrolment, and change management concepts.

Reference Material

This manual provides the necessary instruction and background information for LRAs to fulfill their duties. The documents listed below provide additional information:

- ONE® ID Policy and Standards: These documents provide the conditions and requirements of ONE® ID pertaining to registering, enrolling and authenticating individuals, in which an organization is bound to as part of an Agreement with the Agency.
- ONE® ID Implementation Package: This document serves as an overview and guide to implement ONE® ID within an organization.
- ONE® ID Registrant Reference Guide: This document provides the registrant with detailed step-by- step procedures to self-manage their ONE® ID account.
- ONE® ID Acceptable Use Policy: This document must be agreed to by all ONE® ID registrants (including LRAs).

Additional supplemental material can be found on the ONE ID section of the Ontario Health website.

Introduction

ONE® ID is a set of systems and business processes that provide secure and trusted access to health care applications and services to healthcare providers in Ontario. ONE® ID enables registration, authentication, and authorization for access to digital health services offered by Ontario Health and its partners.

The purpose of the ONE® ID System is to ensure that individuals who are authorized to electronically access personal health information (PHI) under the control of Ontario Health are permitted to do so.

ONE® ID leverages employees at health care organizations to perform registration and enrolment duties on behalf of Ontario Health. These individuals are known as Local Registration Authorities (LRAs) and are registered, sponsored and trained on the ONE® ID processes, policies and system.

Prior to leveraging ONE® ID services, organizations must enter a legal agreement with Ontario Health for the provisioning of services, products or technologies as well as nominate individuals to fulfill the Authorized Representative, Sponsor, and LRA roles. These roles and the ONE® ID business processes are described in detail in this manual.

LRAs are the primary ONE® ID support contact for individuals within their organization and must have an understanding of ONE® ID policy and processes to fulfill their role. This includes:

- Validating identities and registering and enrolling individuals in the ONE® ID system
- Ensuring that individuals receive appropriate authorization prior to granting them access to any services
- Protecting the privacy and security of the personal information they must access in the course of their duties
- Communicating with staff in their organization and liaising with Ontario Health
- Fulfilling and/or submitting ONE® ID requests made by their organization to Ontario Health

NOTE: Ontario Health has Registration Agents (RAs) who are experts on ONE® ID services. LRAs can contact ONEIDRegistrationAgents@ontariohealth.ca for additional support in any ONE® ID registration activity.

The LRA Role

The Local Registration Authority (LRA) role is assumed by individuals who have been nominated by their organization(s) and approved by Ontario Health to perform ONE® ID registrations, enrolments, changes, and to support requests on behalf of their organization(s).

LRAs support authentication, authorization, user management, and compliance with auditing requirements established by the provincial government, their organization, and Ontario Health.

Qualifications

The following qualifications must be met to become a ONE® ID LRA:

- Willing to fulfil all duties described in this manual
- Familiar with their organization's onboarding practices, accountability structure, and local record keeping
- Familiar with Privacy & Security principles and best practices as they pertain to handling personal information
- Registered by Ontario Health at Assurance Level 2
- Nominated by their organization's Authorized Representative
- Approved by the Ontario Health Registration Authority

Duties and Responsibilities

The following list summarizes the responsibilities of an LRA. Additional details can be found throughout the LRA Procedures Manual.

- Providing guidance to other LRAs and registrants within their organization
- Communicating and maintaining a list of sponsors and registered users for their organization
- Validating the identity of individuals and sponsors
- Registering individuals and adding service enrolments to authorized accounts
- Liaising with Ontario Health on registration issues
- Responding to Ontario Health requests to validate the identity of individuals

Sponsorship

Sponsorship is the first step in the registration and enrolment process. It is how organizations identify an individual's authorization to access services and their privileges within those services under that organization’s authority. While organizations are accountable for this authorization, they are represented by individuals fulfilling the Authorized Representative and/or Sponsor roles.

Authorized Representative Role

The Authorized Representative (AR) is identified during the Agreements process when an organization first engages with ONE® ID and/or when an established AR submits an Authorized Representative Delegation Form. An Authorized Representative will be accountable for the registration and enrolment processes for their organization.

The AR is authorized to:

- Engage Ontario Health for access to eligible services (such as ConnectingOntario)
- Engage Ontario Health regarding changes to their ONE® ID implementation (e.g. evaluating their internal identity validation process)
- Nominate new LRAs via submission of a Local Registration Authority Nomination Form.
- Identify new Sponsors (see below)
- Fulfill the Sponsor and/or LRA roles as required (i.e. If no other LRA or Sponsor is nominated, then the Authorized Representative must fulfill these responsibilities)

Sponsor Role

The Sponsor’s role is to authorize individuals to be enrolled for services under the authority of their organization. This role is managed internally within their organization and Sponsors should be familiar with the service(s) for which they are authorizing users.

Sponsors are responsible for:

- Confirming that registrants have a legitimate reason to access the service(s) in support of the organization
- Confirming that registrants have met the specific access criteria for the respective service(s).

- Confirming that additional approvals/pre-requisites imposed by their organization are received/met
- Identifying the role(s) (access privileges) that registrants should receive in a given service
- Updating and/or rescinding authorization as warranted by changing circumstances
- Communicating sponsorship information to their organization's LRAs for entry into ONE® ID

Obtaining and Tracking Sponsorship

LRAs should follow their organization's internal request and approval process for obtaining and tracking sponsorships. If there is no such process, the LRA should develop a system with the organization's management. Refer to General Guidelines for more information.

Sponsors and LRAs

Best practices require separation of duties with respect to Identity and Access Management, i.e. the individual authorizing users should not be the same individual that captures the authorization in the system. That being said, resource constraints may require that the same individual fulfill both the Sponsor and LRA roles for their organization.

The key difference between Sponsors and LRAs is that Sponsors authorize user access, whereas LRAs complete and execute ONE® ID support processes and serve as the main point of contact for staff requiring additional support.

A Sponsor or an LRA cannot authorize or make legal changes to their own account. It must be approved by the Authorized Representative, another Sponsor, or LRA.

The responsibilities of each role are depicted in the table below.

Roles and Responsibilities	Sponsor	LRA
Identifies prospective registrants	✓	
Documents the user’s entitlement to access a service	✓	
Responsible for the registration processes		✓
Responsible for adhering to the ONE® ID policies	✓	✓
Maintains list of sponsors per service and assists other LRAs		✓

Conducts identity validation and processes the Registration & Service Enrolment Requests		✓
Processes changes to service enrolments		✓
Processes changes to registration information		✓
Answers registration and service enrolment questions from registrants		✓
Liaises with Ontario Health on Identity and Access issues		✓

Identity Validation

The ONE® ID's Registration Process relies on an individual's real-world identity to create a digital identity, which is then used to authenticate their access to applications. "Real world identity" is reflected in ONE® ID by capturing the user's **core identity information** (legal name and date of birth) and validating this information to a prescribed level of assurance.

Granting an account online access to personal health information requires a minimum Assurance Level of 2 (**AL2**). Individuals must present one piece of government issued photo ID and one piece of corroborating evidence in a face-to-face (in person or video conference) meeting. This may occur prior to (Identity Validation by Organization) or during (Identity Validation by ONE® ID Process) the Registration and Enrolment process.

NOTE: As an LRA, you must be satisfied with the legitimacy of the means used to validate the individual's identity. If you have any cause to doubt the veracity of an individual's identity, you may request to review an additional identity document or reject the registration.

Identity Validation by Organization

Identity validations performed by your organization (typically as part of employee onboarding) may be relied upon to create ONE® ID accounts at AL2. Your organization's processes must be confirmed to meet ONE® ID requirements before they can be used for this purpose, contact OneIDBusinessSupport@ontariohealth.ca to initiate the evaluation process.

As an LRA, you are responsible for confirming that Registrants have completed your organization's identity validation process and that the information entered in ONE® ID aligns with what is captured in your system. How this information is shared varies between organizations, but may include any or all of:

- Participating in the employee onboarding process
- Referring to company directory
- Referring to a Human Resources Information System
- Review of the Registrant's Employee ID Badge

Self-Complete Invitations

After entering identity information, select the appropriate service(s) and issue a registration invitation. The system will send an email with a unique link to the registrant. The Registrant will enter the remaining account information when completing the invitation.

Federated Identities

ONE® ID integrates with other identity providers (Local IDPs) to provide a single-sign-on experience between local (e.g. an HIS [Health Information System]) and Provincial (e.g. a Clinical Viewer) applications. In this scenario, the local IDP performs the identity management function for end users while ONE® ID identifies the IDP system. Please see Appendix C for more information.

Identity Validation by ONE® ID Process

To expedite the user's onboarding process and reduce the administrative workload, it is recommended that users be validated internally within your own organization. If your organization's processes do not meet the requirements for AL2, identity validation must be completed via review of acceptable evidence in a face-to-face meeting (in person or video conference) with an LRA.

Acceptable Identity Documents

Identity documents must include at least one document from the Primary Identity Document list and one form of corroborating evidence. The Primary Identity Document serves to confirm the user's core identity information while the corroborating evidence may be an additional document and/or circumstantial evidence that serves to increase assurance that the Primary Document is genuine.

REVIEWING DOCUMENTARY EVIDENCE

At least one document presented must be on the Primary Identity Document list. Secondary documents may be reviewed in conjunction with a Primary Document as a form or corroboration. See Appendix A for a complete list of acceptable documents.

When reviewing Identity Documents, the following requirements apply:

- Document must be original; photocopies are not accepted.
- Document must be current, i.e. not expired.

- The document must contain a photo or be reviewed in conjunction with another approved document that contains a photo.
    - E.g., if birth certificate is used, secondary piece of evidence must include photo.
- The document, on its own or combined with a second identity document, must confirm the individual's legal name and date of birth.

REVIEWING CONTEXTUAL EVIDENCE

The context of a registration can corroborate the identity of an individual when used in conjunction with a Primary Identity Document. The following contexts are considered acceptable to support the identity of a Registrant:

- **Prior Professional Relationship:** If the LRA has known the individual professionally for more than 12 months, they may rely on this relationship as a form of identity validation. Professional Relationship includes those with coworkers, colleagues, and patients.
- **Employment by the Sponsoring Organization:** Employment may be confirmed by reference to an employee directory or as advised by organization leadership.
- **Registration at Practice Location:** Meeting the Registrant and their medical practice location can serve to corroborate their identity. This form of evidence is only applicable for LRAs registering individuals outside of their own organization.

The means of supplemental identity validation used must be recorded in the ONE® ID System.

PROFESSIONAL LICENSE VALIDATION

When presented, medical professional credentials qualify as a secondary form of documentary evidence of identity. If not presented, credentials may still serve as a form or corroborating evidence when validated by an LRA against an authoritative source. Professional License credentials may be inputted into the system during the identity validation process, self-registration, or any time after the ONE® ID account has been created and set up.

The ONE® ID System automatically validates credentials for Physicians, Nurses, and Dieticians. To validate other credentials, refer to the issuing Regulatory College website to confirm that the registrant's identity aligns with their license number.

CAPTURING IDENTITY INFORMATION

It is recommended that you capture identity information in ONE® ID as you conduct identity validation. In the event that you record identity information outside the system (e.g. on a registration form), such records should be destroyed or archived in accordance with your organization's document retention policies after being entered into ONE® ID.

Within the ONE® ID system, you must record the registrant's:

- Legal First and Last Names
- Preferred First and Last Names
- Date of Birth
- The Evidence presented to validate identity including the type and number of documentary evidence
- Healthcare Professional License Information

CONTACT INFORMATION

Contact Information (**Email** and **Contact Phone Number**) may be used by Ontario Health to alert users regarding changes to their account, help resolve technical issues with the account and/or in the event that the account is involved in a suspected security breach.

MOBILE NUMBER FOR AUTHENTICATION

Distinct from a '**Contact Phone Number'**, the mobile number designated for authentication (referred to as the **Mobile Number** within the ONE® ID user interface) is used to support user login session authentication. It is strongly recommended that ONE® ID users, especially Local Registration Authorities (LRAs) configure a Mobile Number within their contact information, as this enables authentication without reliance on an RSA token. If your **Contact Phone Number** is a mobile phone, you can add the same number for your **Mobile Number.** For additional guidance, refer to the ONE® ID Registrant Reference Guide for detailed instructions.

SECURITY QUESTIONS

These are questions to which only individuals know the answers and are collected for the purposes of verifying their identity via phone or internet, to safeguard the integrity of the system. **Service Desk Questions** may be asked when registrants call Ontario Health Service Centre (e.g., cannot reset their password online or forget their Login ID and password) to verify their identity. The **Online Authentication Questions** are used by the ONE® ID system for self-recovery (e.g., Forgot Login ID, Forgot Password) and for knowledge-based authentication (KBA).

During the registration process, individuals will be asked to provide answers to **two (2) Service Desk Questions** collected for support purposes during the registration process. If the individual provides a mobile phone number during the registration process, the two service desk questions become optional and do not need to be completed.

During the self-completion process, individuals are required to provide answers to five (5) challenge questions. They are required to select and answer **two (2) Service Desk Questions** and **three (3) Online Authentication Questions**.

ENROLMENT INFORMATION

Enrolment information (e.g., roles and attributes) may need to be collected for select services. As this information may determine the registrant's level of access within a service, it must be provided or confirmed by the authorized sponsor.

Identity Validation for Previously Registered ONE® ID Users

Users who have an existing ONE® ID account have had their identity previously validated and do not need another validation for the purpose of enrolment. Other account modification requests may require identity validation as follows:

Modifying Identity Information

If there are legal changes that need to be made to the account (e.g., Legal name change), specific documentary evidence is needed to confirm the validity of the change. If it is a non-legal change (e.g., email, change in phone number), the user should be directed to modify their own account via self-management.

Correcting Identity Information

Cases where identity information was previously captured incorrectly are distinct from changes to identity information, e.g., a typo in a legal name vs assuming a married name. Correcting errors in identity information can be based on previously reviewed documentary evidence and/or your professional relationship with the user. If neither of these are sufficient to confirm the correct information, you must review a piece of documentary evidence.

Modifying Security Information

Users that are locked out of their ONE® ID account and are unable to authenticate over the phone may require LRA assistance to update their Service Desk Questions or reset the password for their ONE® ID account. To mitigate the risk of identity fraud, you must validate the requestor as follows:

ESTABLISHED PROFESSIONAL RELATIONSHIP

If you have a professional relationship with the user for at least 1 year, you may use this contextual evidence to make the required changes.

DOCUMENTARY EVIDENCE

The user's identity information (legal name and date of birth) must be validated using the documentary evidence that matches what is listed in the account before modifying challenge information.

Missing Security Information

In some cases, previous ONE® ID accounts may not have had Security Questions captured. After verifying the user's identity (same process as above), the user has the opportunity to input this information during self-complete process.

The user will call Service Desk at **1-866-250-1554** and be verified using the service desk questions. The user will then be permitted to receive a registration email to reset their account and input their own Security Questions.

General Guidelines

This section provides high level guidance on how to perform your duties as an LRA and is intended to help you establish practices to support these duties when they do not already exist within your organization. You are encouraged to leverage all or your organization's internal polices, processes, tools, etc. where applicable. If you believe that these guidelines (or any of the content of this manual) conflicts with your organization's practices, please contact ONEIDRegistrationAgents@ontariohealth.ca

As part of the ongoing support and maintenance of ONE® ID, you should periodically review how these practices are working for your organizations and refine as needed.

Information Management

You are responsible for communicating the information management practices outlined in this guide to registered individuals within your organization. Components of information management include:

- Information collection
- Information storage and retention

NOTE: These practices are necessary to safeguard the privacy of personal information (PI) (including PHI) that is collected, transmitted, stored, or exchanged by and through the information infrastructure to ensure the privacy and security of that information.
If you have any questions or require further information about the collection described above, you can reach out to Ontario Health's Privacy Team by filling out the contact form on this page.

Information collection

Information collected in the course of your duties as an LRA is necessary for the creation and/or maintenance of ONE® ID accounts and enrolments and **must not be used for any other purpose**. You must advise users of this fact when collecting their information.

When collecting information, you must:

- Ensure the privacy of the collection process, i.e., it is limited to you and the Registrant and relies on a secure channel

- Obtain it directly from the source (the registrant and/or your organization's records) and not via an intermediary
- Ensure the accuracy of the information you record as compared to the source

See [**Compliance and Assurance**] **for more information** on Privacy and Security Practices.

Information Storage and Retention

Any user registration information **must not be kept or recorded anywhere outside of the ONE® ID system**. If this information is captured outside of the system, these records should be properly retained and/or disposed of in accordance with your organization's Privacy, Security, and Data Retention policies.

Transient records (e.g., paper forms) used to support your organization's internal process **must be stored in a secure location** (e.g., locked file cabinet) until the information has been entered into the ONE® ID System. Thereafter, these documents should be handled in accordance with your organization's Data Retention, Privacy, and Security Policies.

Incident Management

Incident management addresses what needs to be done in the event that an individual's Personal Information (PI) is compromised or used in a manner that is unrelated to registering or enrolling individuals into Ontario Health services.

Examples of incidents include but are not limited to:

- Personal Information is stolen or misplaced
- Personal Information is used to perpetrate identity theft
- Personal Information is used for purposes other than registration, such as updating an HR contact database

Reporting an incident

In the event of an actual or suspected privacy incident, please contact the Ontario Health Service Desk at **1-866-250-1554** immediately so that it will be actioned as soon as possible. Please ensure that you recount the incident in detail, which may include the time the incident occurred, and the parties involved. For more information on the practices for incident management, refer to **Compliance and Assurance**. You are responsible for ensuring your organization complies with these practices.

Communications and Training within the Organization

As an LRA, you will be interacting with different groups and are responsible for the following:

- **New LRAs**: Training and support for other LRAs within your organization
- **Individuals and Registrants**: Ensuring that all registrants understand the Ontario Health Acceptable Use Policy and Notice of Collection
- **Sponsors**: Understanding who the Sponsors and Authorized Representatives are
- **Staff within your organization**: Communicating how the registration and enrolment processes will work within your organization or care team
- **ONE® ID staff**: Communicating changes to delegates or users

Interacting with New LRAs

You are responsible for registering, training and monitoring the activities of new LRAs within your organization. This includes:

- Ensuring that the nomination has come from the Authorized Representative (**AR**)
- Submitting the LRA Nomination Form to ONEIDBusinessSupport@ontariohealth.ca

NEW LRA TRAINING PLAN

The types of questions you may want to address as you develop the LRA training plan include:

- Has the LRA read and understood the LRA Procedures Manual?
- Do you want the new LRA to shadow an experienced LRA for a certain period? If so, how long?
- How will you note that the LRA has been trained?
- How will you ensure that the LRA is fulfilling the duties and responsibilities of the position, especially within the first few weeks, and provide feedback?

When enrolling new LRAs, direct them to the ONE ID Section of the Ontario Health Website to complete the necessary training. You will be responsible for documenting the answers to these questions and communicating them within your organization and to Ontario Health if required (such as, in support of an audit), and for ensuring that your organization is in compliance. See Compliance and Assurance for more information.

As part of the ongoing support and maintenance, you may also want to revisit how the process is working for your organizations and refine as needed.

Interacting with Individuals and Registrants

When and how LRAs interact with users is heavily dependent on your organization's structure and request management protocols. Questions you may want to consider include:

- Which individuals/groups will require access?
- Does your organization have multiple ONE® ID protected services? What is the overlap between the user groups?
- How high is the turnover in your user group(s)? How many registrations/revokes/suspends/reinstates will need to be processed on a monthly basis?

NOTE: Identity confirmation is a key component of all interactions with users, not just registration. **Always confirm a registrant's identity before updating their account information or providing information regarding it.** If you previously registered or otherwise know the registrant, you may rely on this knowledge as confirmation of their identity. You may also, at your discretion, request to review an identity document to confirm their identity.

Interacting with Sponsors

How LRAs interact with Sponsors is heavily dependent on your organization's structure and request management protocols. At a minimum, all LRAs should be aware of who in their organization fulfills the Sponsor and Authorized Representative roles. More specific questions to consider include:

- Has a process been established for your organization as to how you will be notified of new sponsors?
- How will the list of sponsors be communicated amongst the LRAs within your organization; how will the list be updated?
- Will an email from a sponsor or memo be acceptable as proof of sponsorship?
- Is there an established authorization process that can/should be leveraged for ONE® ID sponsorship?

You will be responsible for documenting the answers to these questions and communicating them within your organization, and to Ontario Health if required (such as, in support of an audit), and for ensuring that your organization is compliant. See section Compliance and Assurance for more information.

Interacting with "Staff"

Depending on your organization, there may be other departments you can work with to ensure that the processes and policies that you are developing are in keeping with federal or provincial legislation and your organization's operations. For example, if your organization has a Human Resources division, you may want to exchange information when individuals have been hired or left the organization.

Interacting with ONE® ID

ONEIDRegistrationAgents@ontariohealth.ca should be your primary communication channel for ONE® ID related matters, including submitting requests for action, reporting errors in the ONE® ID system, and asking for guidance on process/policy interpretation.

ONEIDBusinessSupport@ontariohealth.ca is the appropriate communication channel regarding any changes to AR/LRA delegates and user statuses, sponsorship attestation requests, and changes to ONE® ID process/policies/systems.

Communications Plan

The types of questions you may want to address as you develop an effective communications plan for your organization include:

- Will you use posters or send emails to educate the organization about the framework and process?
- How will you communicate the process(es) the sponsor or applicants need to follow
- What information will be requested of them, why is the information required, and how will the information be used?
- How will you communicate changes to the processes?

Record Keeping

All LRAs are accountable for recording their own and other LRAs transactions within the organization. Upon request, the ONE® ID Program can provide you with a report of registrants sponsored by your organization and transactions performed by the LRAs. However, it is recommended that you maintain your own records as a point of comparison.

The following are records to maintain by the organization's LRAs:

- Registrations performed

- Service enrolments
- Updates performed
- Sponsorship requests (electronic or hard copy) received

Your internal request management tools/processes may already incorporate sufficient record keeping. If this is not the case, it is recommended that the LRA develop an internal record keeping process to maintain this information.

NOTE: Do not keep any personal identity information other than the name of the person for whom the transaction was performed, the transaction date, and the transaction type.

Communication Guidelines

While fulfilling your responsibilities as an LRA, you will need to communicate with end users, Ontario Health, and other stakeholders. It is assumed that communication will be via email, though these guidelines can be applied to any communication method. Note that your organization's communication and privacy/security standards may provide additional guidance.

Privacy Considerations

Transmission of any PI via email is against Ontario Health's policy and will result in a security incident being raised. **Do not submit any PI about users via email, including Gender, Date of Birth, and Identity Document Information**. Registrants should be identified in email only by their name, Login ID, and Professional Designation number (if applicable).

General Guidelines

Consider the nature of the request when sending communications. Ontario Health will always make efforts to engage the appropriate support teams, but starting with the appropriate communication channel will ensure faster service. Specific guidelines for submitting ONE® ID account management requests are provided below. Other communication can be directed as follows:

- Incident reporting and general inquiries regarding Ontario Health services should be directed to OH-servicedesk@ontariohealth.ca or, for immediate assistance, you can call 1-866-250-1554 (Ontario Health help desk).
- For assistance with ONE® ID processes, policies, or system, please email ONEIDRegistrationAgents@ontariohealth.ca.
- For inquiries regarding adopting a new Ontario Heath service, please go to this page and complete the appropriate webform.

Submitting ONE® ID Requests to Ontario Health via Email

The ONE® ID System is the primary method for executing all Registration, Enrolment, and Account Maintenance requests. However, requests related to select services cannot be processed directly in the online system and require the intervention of Ontario Health. In such cases, LRAs can submit requests via email.

NOTE: Submitting requests via email creates delays in the process and increases the risk of errors due to miscommunication. For these reasons, Ontario Health may reject email requests that could be completed using the ONE® ID Online system.

Sender's Email

Email requests must clearly identify you as the LRA (either in the body of the email or your signature) and be sent from the email account entered in your ONE® ID Account. Ensure that the contact information in your ONE® ID profile is current.

Subject

The subject line of your email should indicate the type of request (Enroll / Suspend / Reinstate / Revoke), the relevant service, and the Login ID (FIRSTNAME.LASTNAME@ONEID.ON.CA) of the relevant user, e.g.: "HSI Enrolment Request for JOHN.SMITH@ONEID.ON.CA."

Request Statement

The body of your email should contain an explicit statement of the request being made, including:

- **Type of request** (Enroll/Revoke for a Service or Revoke/Suspend user registration)
- **Login ID of the Registrant** (FIRSTNAME.LASTNAME@ONEID.ON.CA)
- **Requested Service** (Connecting Ontario User, ONE Labs Clinician, etc.)
- **Enrolment Attributes** (as applicable per service)
- **Expected Return Date** (only applicable for suspend user requests)
- **Reason** (only applicable for revoke and suspend requests), select from:
    - The registrant no longer requires access to the service
    - The registrant's level of assurance no longer meets the minimum required for the service
    - The registrant is no longer associated with the sponsoring organization

Example Email

"Hi,

As LRA under the authority of Kingston Health Sciences Centre, please REVOKE the Connecting Ontario Service from the account of JOHN.SMITH@ONEID.ON.CA as they are no longer associated with the sponsoring organization."

In lieu of including these details in the body of your email, you may instead complete one of the email enrolment form templates located at the ONE ID Section of the Ontario Health Website.

Sponsorship Assertion

The LRA must include an explicit statement of sponsorship, indicating that the request has received proper authorization, e.g. "This request has been authorized under (insert Sponsoring Organization name)."

The organization must be one for which the LRA has been authorized to act on behalf of, and the individual sponsor must have appropriate authority therein.

Federated Authorization Request

Once IDs are setup for access at your organization, they need to be submitted to us at OneIDBusinessSupport@ontariohealth.ca by an LRA. Individual Federated Authorization Requests (requests for local IDPs rather than ONE® ID accounts) should follow the same format as ONE® ID Requests. Federated Authorization requests may be submitted in bulk using the request template. Email requests should include the following information:

- LRA Submitting request
- Organization the request is for; e.g West Parry Sound Health Centre
- Type of Request; Add or Revoke
- Environment e.g. PROD, PST

See Appendix C for more information on Federated Authorizations.

ONE® ID Registration & Enrolment Process

This process details the steps required to Register and Enroll end users for access to ONE® ID protected applications.

This process may be initiated as part of a broader service implementation process or independently.

Preconditions

- The ONE® ID Organization Setup process has been completed for the organization, and it is authorized to sponsor end users for access to the respective service(s).
- An LRA must be authorized by the sponsoring organization before registering and enrolling registrants.

Triggers

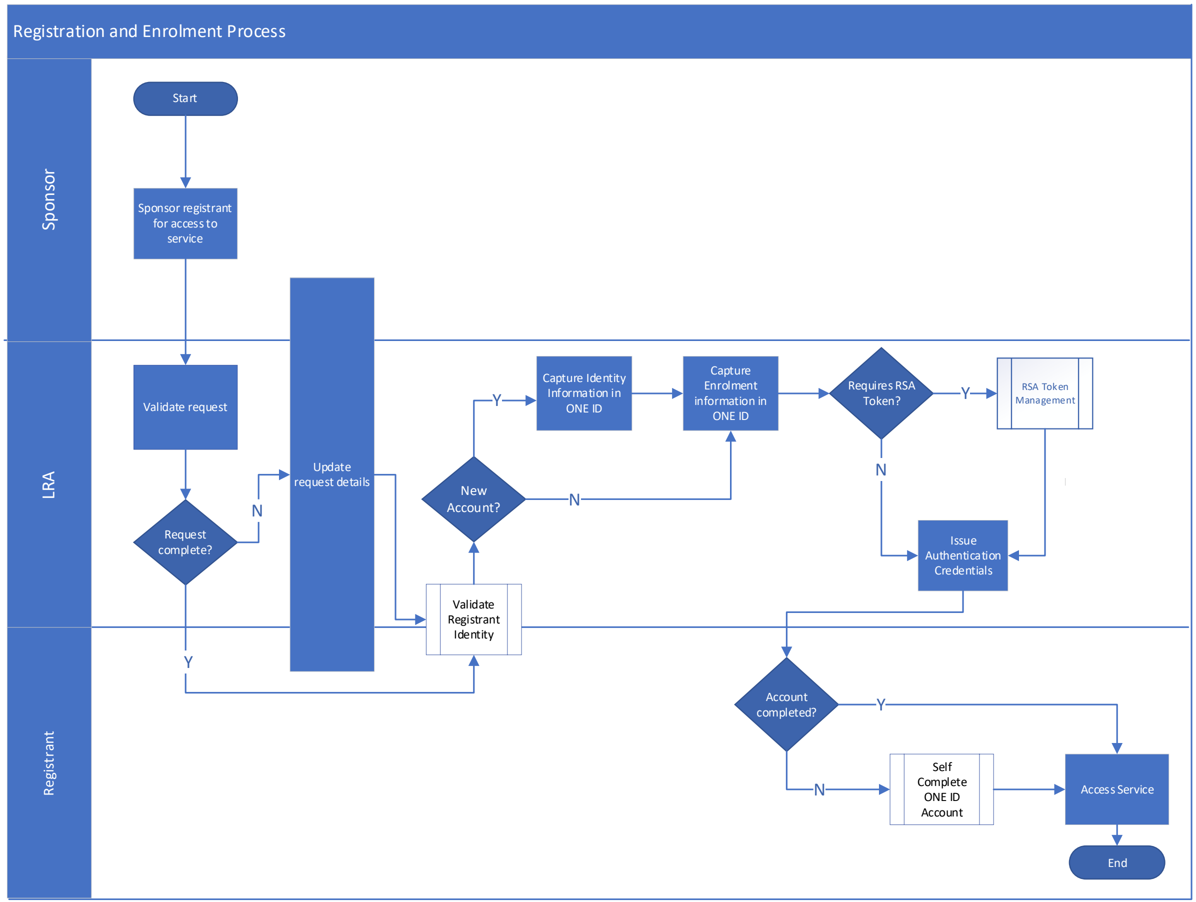
This process may be triggered in any of the following circumstances.

- A new staff member has joined the organization with or without an existing ONE® ID account, and requires access to services protected by ONE® ID.
- A current staff member with or without a ONE® ID Account has assumed a new role and requires access to services protected by ONE® ID.
- A new service has become available via ONE® ID and must be enabled for end users.

Post-Conditions

- User's ONE® ID account can be used to access requisite services.

Workflow



Process Steps

#	Name	Description	Role
1	Sponsor registrant for access to service	Sponsor validates that the Registrant meets the criteria for accessing the service and is authorized to do so under the authority of the Sponsor's organization. ***NOTE***: Access criteria vary depending on service, refer to service-specific documentation for details.	Sponsor
2	Validate Request	Review the request to ensure that the organization's internal authorization process has been followed and that requisite data elements (e.g. service role) have been included.	LRA

Ontario Health

		If the request is incomplete or inaccurate, go to step 3. If the request is complete/accurate, go to step 4. ***NOTE***: Requisite data varies depending on type of service; refer to service documentation for details.	
3	Update Request Details	Coordinate with Sponsor and/or Registrant to complete the request.	Sponsor, LRA, Registrant
4	Validate registrant identity	Complete the identity validation process as prescribed by your organization and ONE® ID. Process details may vary depending on circumstances, refer to Identity Validation for details.	LRA, Registrant
5	Capture identity information in ONE® ID	Enter the registrant's identity information into the ONE® ID system. Information requirements are determined by the identity validation method used.	LRA
6	Capture Enrolment information in ONE® ID	Add enrolments/roles as per sponsorship request. If enrolment service requires RSA token, go to step 7 If the service does not require an RSA token, go to step 8	LRA
7	RSA Token Management	Assign an RSA token to the registrant using the RSA console. Refer to the RSA Quick Reference Guide or the RSA Token Management Process for more details.	LRA
8	Self-complete ONE® ID account	The Registrant completes an online process to activate their account. Refer to the ONE® ID Registrant Reference Guide for further information on this functionality.	Registrant
9	Access service	The registrant verifies access to the respective service(s) by logging in for the first time.	Registrant

Ontario Health

RSA Token Management Process

This process details the steps required when assigning, enabling/disabling/replacing/revoking tokens, and resetting token pins. Please see the RSA Quick Reference Guide and the Registration and Enrolment Process for more details.

If you must assign a token and do not have one available, please contact the Registration Agents.

Preconditions

- LRA has an RSA Token and has access to the RSA console.
- Registrant has a ONE® ID account and has been sponsored and enrolled in a service that requires a token.

Triggers

This process may be triggered in any of the following circumstances.

- Registrant needs a token to access a service enrolment.
- Registrant's token needs to be enabled/disabled/replaced or needs a pin reset.
- The Registrant no longer requires an RSA Token

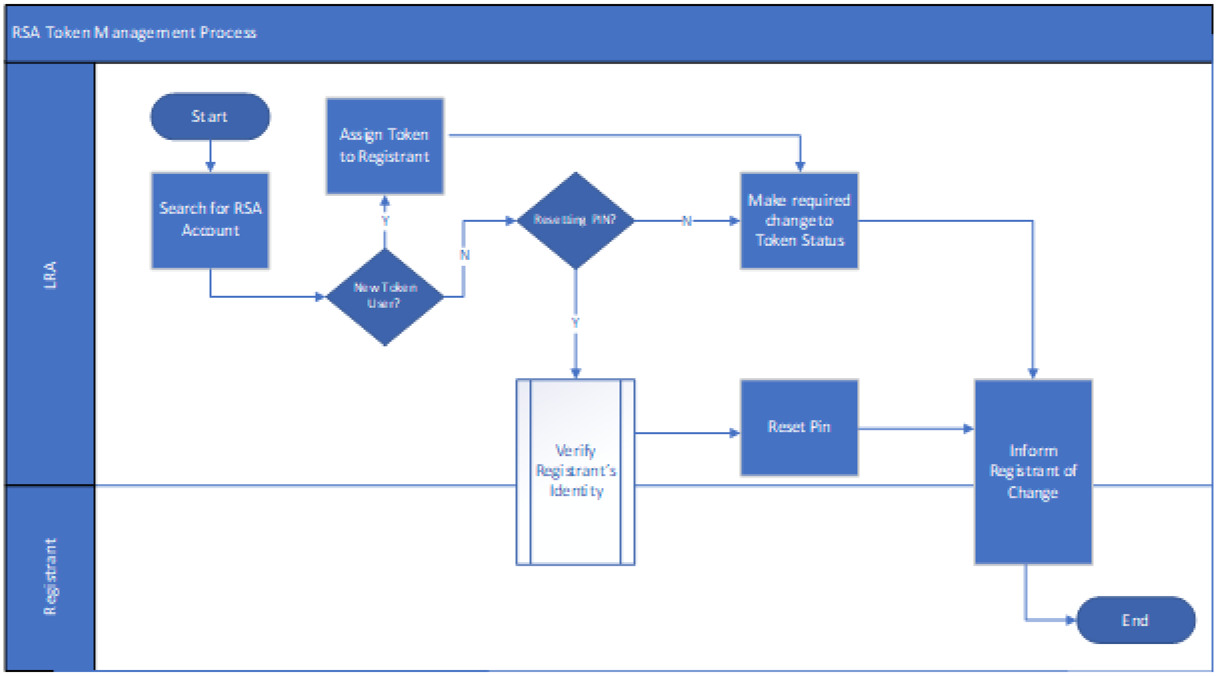
Post-Conditions

- Registrant has an active RSA Token and has access to the service enrolment.

Or

- The Registrant's RSA Token has been revoked

Workflow



Process Steps

#	Name	Description	Role
1	Search for RSA Account	Search the [RSA Console](#) for the user's ONE® ID account. • If the user requires a new token to access a service, proceed to step 2. • If the user has an existing token that requires a PIN Reset, proceed to step 3. • If other changes are required, proceed to step 5.	LRA
2	Assign Token to Registrant	Assign Hardware Token you have on hand to the Registrant. Proceed to step 5 to enable the token. ***NOTE:*** For a user to set a new PIN, advise them to login to ONE® ID and leave the PIN section blank.	LRA

		The system will then prompt them to create a new PIN.	
3	Verify Registrants identity	Verify the Registrant's identity using the ONE® ID Challenge Questions or by reviewing the employee ID. For more details, refer to Identity Validation.	LRA, Registrant
4	Reset Pin	To set new pin, advise the user to login to ONE® ID as per their standard instructions and leave the PIN section blank. For additional assistance, the user may contact Ontario Health Service Desk.	LRA
5	Make Required Change to Token Status	Enable/Disable or replace token as required.	LRA
6	Inform Registrant of Change	Inform registrant that the request has been completed. This may involve an update of internal records.	LRA, Registrant

ONE® ID Enrolment Management Process

This process details the steps required when revoking users' service enrolments to ONE® ID protected applications. To add a service enrolment, please see the Registration and Enrolment Process for more details.

- To **REVOKE** is to permanently rescind the registrant's access to the service. A registrant will still have access to their remaining services even if one of those services are revoked

NOTE: In the event that a Registrant is deceased or retired, please notify Ontario Health. Registration Agents will permanently revoke the registration and all associated service enrolments.

NOTE: ONE® ID does not allow the suspension of enrolements. Only ONE® ID accounts can be suspended.

Preconditions

- The registrant has left the organization or no longer requires access to the service.

Triggers

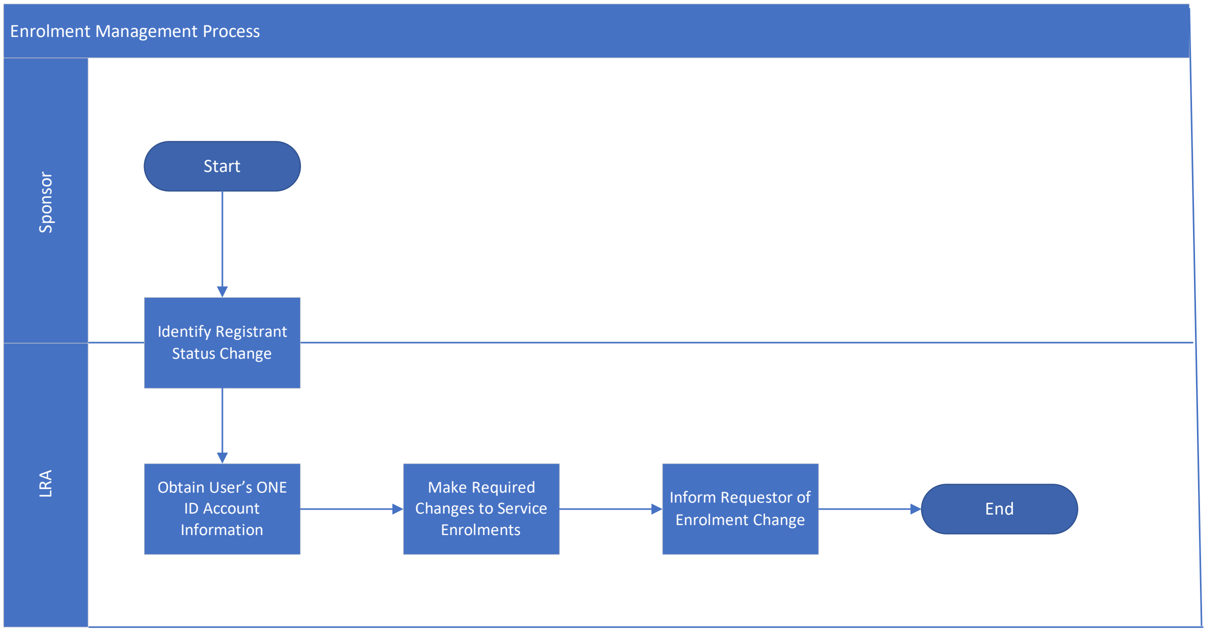
This process may be triggered in any of the following circumstances.

- The sponsor advises that the enrolment should be revoked
- The LRA becomes aware of the employee status change through organizational processes.

Post-Conditions

- Revocation to the user's service enrolments have been made.

Workflow



Process Steps

#	Name	Description	Role
1	Identify Registrant Status Change	The LRA is made aware of a change to the registrant's status. This may be communicated by the Sponsor or raised via internal processes.	Sponsor LRA
2	Obtain User's ONE® ID Account Information	Obtain ONE® ID login from the Registrant, internal records, or by searching for it on ONE® ID.	LRA
3	Make Required Changes to Service Enrolments	Revoke the service enrolments in the user's ONE® ID account as required	LRA
4	Inform Requestor of Enrolment Change	Inform the requestor that the request has been completed. This may involve notification to the Sponsor and/or update of internal records	LRA

User Information Management Process

This process details the steps required when making changes to a user's ONE® ID account information. These include changes to a registrant's preferred name or date of birth.

When modifications or updates are made to a registrant's account, the ONE® ID System will send an automated notification email outlining the changes that were made.

NOTE: Other changes to the user's account profile (contact information, password, challenge questions, etc.) can be self-completed by the registrant. Refer to the ONE® ID Registrant Reference Guide for more information.

Preconditions

- The registrant's Date of Birth was entered incorrectly in the registration system.
- The registrant's preferred name has changed or is entered incorrectly

Triggers

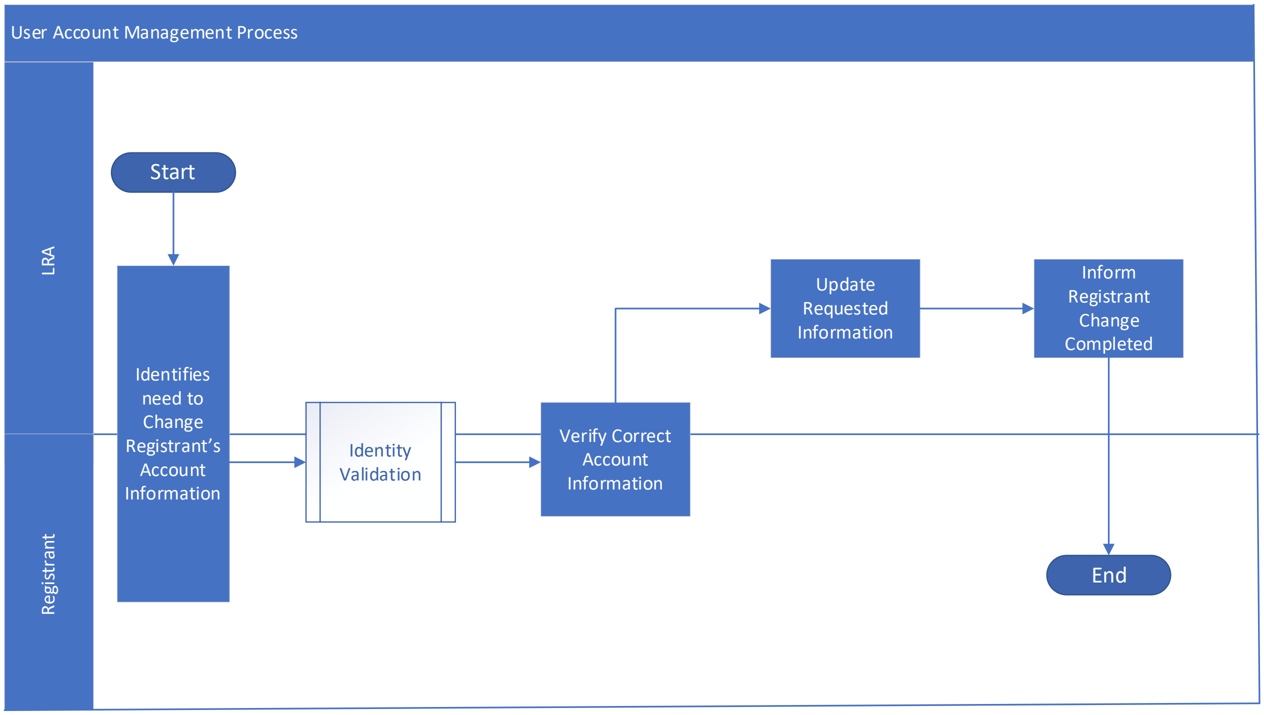
This process may be triggered in any of the following circumstances.

- The LRA becomes aware of an error in the user's identity information.
- The Ontario Health Service Desk redirects a user to their LRA after their identity cannot be validated over the phone.

Post-Conditions

- Date of Birth or Preferred Name changes to the user's ONE® ID account information have been made.

Workflow



#	Name	Description	Role
1	Identifies need to Change Registrant's Account Information	LRA identifies a need to change Registrants account information regarding their Date of Birth. This is likely to be raised by the Registrant themselves, but not necessarily.	LRA, Registrant
2	Identity Validation	Confirm the registrant's identity. If the LRA has previously validated the registrant's identity and/or has an established (>1 year) working relationship with them, they may rely on this knowledge as confirmation of identity. To the discretion of the LRA, they may also ask to review a valid identity document from the registrant. Please refer to Identity Validation for more details.	LRA, Registrant

3	Verify Correct Account Information	Verify the correct information to be entered into ONE® ID. Verification requirements depend on the nature of the change, refer to Account Change Documentation Requirements (below) for details.	LRA, Registrant
4	Update Requested Information	Update the date of birth in the user's account.	LRA
5	Inform Registrant Change Completed	Inform Registrant that the request has been completed	LRA

Account Change Documentation Evidence Requirements

Types of Account Change	Evidence Requirements
Legally Changed Name	Must reach out to ONE® ID Business Support. Primary/Secondary Evidence Document (e.g. Identity document with new name, change of name certificate)
Service Desk Challenge Questions	No documents needed, Registrant can self-manage in account. For more details, please see the ONE® ID Registrant Reference Guide.
Contact Information: (e.g. phone number, email)	
Professional Registration	
Error Corrections for Date of Birth	Identity not previously validated: • Review Primary/Secondary identity evidence documents Previously validated identity/professional relationship: • No evidence document needed

Compliance and Assurance

Ontario Health delegates the responsibilities for identity validation, registration and enrolment to the Sponsoring Organization's LRA(s). LRAs are responsible for adhering to the practices outlined in the LRA Procedures Manual, and Ontario Health may request the LRA to assure they comply with these practices.

Upon request, the LRA should be prepared to confirm the names of all Sponsors, LRAs, and authorized registrants within their organization and to provide documentation regarding their organization's established processes. Please refer to General Guidelines for more information.

A record of all requests must be stored and maintained for reference in the event of an audit. At minimum, records must identify:

- The Registrant
- The LRA
- The Sponsor
- The service(s) being enrolled/revoked

Such records can be maintained in your organization's request management system or an email archive.

Information Collection

The LRA is responsible for adhering to the Privacy and Security practices outlined in this guide regarding information collection and communicating the Privacy and Security practices, such as:

- Advising the individual what information will be requested of them, why the information is required, and how the information will be used.
- Adhering to privacy legislation (Freedom of Information and Protection of Privacy Act).

The LRA must NOT:

- Retain any of the identity documents presented during the registration process.
- Record PHI (such as the state of the individual's health).
- Use any of the PI provided by individuals for any other purpose than to register and enrol them in Ontario Health services.

For questions or concerns about the collection described above, you can reach out to Ontario Health's Privacy Team by filling out the contact form on this page.

Information Storage and Retention

Personal Information (PI) physically documented outside of the ONE® ID System as part of the organization's internal process must be stored in a secure location (i.e. locked file cabinet) until the information has been entered into the ONE® ID System.

Hereafter, these documents should be handled in accordance to your organization's Document Management, Privacy and Security Policies.

Incident Management

If the LRA or individuals within the organization suspects a security or privacy breach**, immediately report the incident to Ontario Health's Service Centre at 1-866-250-1554**.

Ontario Health will be responsible for investigating the incident and following its lifecycle. Security or privacy breaches includes:

- PI recorded during the registration process is stolen or misplaced.
- PI is stolen and used to perpetrate identity theft.
- Someone other than the LRA accesses registrant identity information.
- Information collected during the registration process is used for other purposes, such as updating an HR contact database.

Training of LRA's

As an LRA, you are responsible for ensuring that an LRA training plan has been established for new LRAs. Organizations should have their own internal processes related to onboarding and authorizing staff and how they connect to ONE® ID.

- The LRA should be directed to read the documentation regarding the processes around registration, especially those regarding privacy and security. All relevant documentation can be found on the ONE ID Section of the Ontario Health Website.
- Have the LRA shadow an experienced LRA through a few user registrations.
- Allow yourself some time to review the registrations and enrolments processed by the LRA within the first couple of weeks to ensure that the LRA is fulfilling the duties and responsibilities of the position and vis-versa.

Auditing of LRAs

All LRAs are responsible for tracking their own activities within their organization and ensuring they are in compliance with the LRA Procedures Manual.

It is recommended that the Authorized Representative conduct an internal audit of the LRAs on a yearly basis to ensure their continued compliance.

Ontario Health may request proof of compliance with the procedures and practices outlined in this document.

For auditing purposes, the Authorized Representative may be required to provide evidence that LRAs are trained and complying with the processes defined in this document for ONE® ID Registrations and Service Enrolments.

An LRA may be asked to show compliance with the Privacy and Security practices outlined in this procedures guide regarding:

- Information collection
- Information storage and retention
- Incident management

Verifying Registrant Information

Ontario Health may request the assistance of the LRA to confirm the identity of existing registrants in ONE® ID due to:

- A Security Incident
- An apparent duplicate account
- Any account information that appears to be incorrect

Appendices

Ontario Health

Appendix A – Identity Documents

Identity documents are the standard means of validating identity during the ONE® ID registration and service enrolment of individuals. They are also used to validate any changes to registration information (such as legal name, date of birth and gender) after the applicant has been registered.

During identity validation, perform a visual inspection of the document for signs of tampering or forgery. If the document appears to be altered, the LRA may reject it at their own discretion.

Primary Identity Documents

#	**Acceptable Primary Identity Documents**
1	Birth Certificate issued by a Canadian Province or Territory
2	Canadian Certificate of Birth Abroad
3	Canadian Certificate of Indian or Metis Status
4	Canadian Permanent Resident Card
5	Certificate of Canadian Citizenship (paper document or plastic card, excluding commemorative issue)
6	Certification of Naturalization (paper document or plastic card, excluding commemorative issue)
7	Citizenship Identification Card issued by a foreign jurisdiction where these exist (e.g., Mexico, Europe)
8	Confirmation of Permanent Resident (IMM 5292)
9	CANPASS (A Remote Area Border Crossing permit allowing the bearer to cross into Canada at certain remote areas without reporting to a port of
10	Nexus (A cross-border express pass available to low-risk individuals who have passed a stringent Canadian and American security check, including a fingerprint biometric, photograph, and personal interview with immigration
11	Firearm Registration License
12	Permanent Resident Card (i.e., Maple Leaf Card)
13	Driver’s License (including graduated driver’s license)
14	Canadian Passport (currently valid)

15	A valid Passport issued by a foreign jurisdiction
16	Statement of Live Birth from Canadian Province (Certified Copy)
17	Immigration Canada – Refugee Claimant ID Document
18	Ontario Photo Card

Secondary Identity Documents

#	Acceptable Secondary Identity Documents
1	Any document listed as an Acceptable Primary Identity Document except for the Primary
2	Old Age Security Card
3	Certificate issued by a government ministry or agency (e.g., Marriage, Divorce,
4	Canadian Convention Refugee Determination Division Letter
5	Canadian Employment Authorization
6	Canadian Minister's Permit
7	Canadian Immigrant Visa Card
8	Canadian Student Authorization
9	Record of Landing (IMM 1000)
10	Document showing the registration of a legal change of name accompanied by evidence of use of prior name for the preceding 12 months.
11	Current Registration Document from the College of a Health Profession under the Regulated Health Professions Act, 1991. (Audiology and Speech-Language Pathology, Chiropody and Podiatry, Chiropractic, Dental Hygiene, Dental Technology, Dentistry, Denturism, Dietetics, Homeopathy, Kinesiology, Massage Therapy, Medical Laboratory Technology, Medical Radiation

12	Current Professional Association License/Membership Card (for any Regulated Health Profession, including the following: Association of Ontario Midwives, Denturist Association of Ontario, Nurse Practitioner Association of Ontario, Ontario Association of Medical Radiation Technologists, Ontario Association of Naturopathic Doctors, Ontario Association of Orthodontists, Ontario Association of Speech Language Pathologists and Audiologists, Ontario Chiropractic Association, Ontario Dental Association, Ontario Medical Association, Ontario Nurses Association, Ontario Opticians Association, Ontario Pharmacists" Association, Ontario Physiotherapy Association, Ontario Podiatric Medical Association, Ontario Society of Chiropodists, Ontario Society of Medical Technologists, Registered Nurses Association of Ontario, Registered Practical Nurses Association of Ontario, or Respiratory Therapy Society of Ontario)
13	Federal, Provincial, or Municipal Employee Card
14	Current Employee Identification or Identifier from a Sponsoring Organization
15	Union Card
16	Other Federal ID Card, including Military
17	Ontario Ministry of Natural Resources Outdoors Card
18	Judicial ID Card
20	BYID Card (Formerly Age of Majority Card)
21	CNIB Photo Registration Card
22	Canadian Police Force Identification Card
23	Identification Card issued under the *Blind Persons Rights Act*

Appendix B – LRA Acknowledgement

This form is intended for your review only. Acknowledgement is made via the ONE® ID Online System.

Form of LRA acknowledgement

I, _______________, understand that I will be registered in Ontario Health ("Ontario Health") ONE® ID and appointed as a Local Registration Authority ("LRA"). Local Registration Authority means an individual that has been delegated responsibility by a Client Organization or the Ontario Health Identity Authority for the performance of tasks associated with identifying, authenticating, registering, enrolling, and managing registrants who are within the scope of his or her authority as delegated by a Client Organization or the Ontario Health Identity Authority. "Identity Authority" or "IA" means an individual or group of individuals designated by Ontario Health that are responsible for the registration, service enrolment, and authentication services provided by Ontario Health to clients.

As an LRA I will be obligated to:

1) Read and adhere to Ontario Health's LRA Procedures Manual as amended from time to time.
2) Complete such training, including security and privacy training, related to Ontario Health's registration and appointment processes and technologies used for authentication as Ontario Health may reasonably require and provide from time to time.
3) Take reasonable steps to keep my ONE® ID Credential provided by Ontario Health secure and confidential at all times. "ONE® ID Credential" means the ONE® ID authentication credential, including a user identification, password, token, public key infrastructure certificate (PKI certificate), or any combination of these issued by Ontario Health to an End User to access a Sponsored Service. I understand that I am responsible for any unauthorized or inappropriate use of my ONE® ID Credential. Should I suspect or become aware that my ONE® ID Credential has been compromised, or unauthorized access has been made of any computer terminal or other device connected to Ontario Health's infrastructure, I will immediately notify Ontario Health by calling the support number

provided by Ontario Health in the LRA Procedures Manual or by any other method set out in LRA Procedures Manual.

4) Read and abide by Ontario Health's Acceptable Use Policy, as amended from time to time. A copy of Ontario Health's current Acceptable Use Policy can be found at www.ehealthontario.on.ca.
5) Not exceed the scope of authority delegated to me by Ontario Health including but not limited to registering and enrolling only individuals and Computer Applications (as defined in the LRA Procedures Manual) that have been sponsored and the identity of the individual or validity of the Computer Application, has been verified as set out in the LRA Procedures Manual.
6) Obtain any necessary consents required before collecting, using, or disclosing personal information as set out in the LRA Procedures Manual.
7) Safeguard confidential and personal information collected or received by me in connection with my duties as an LRA and meet privacy requirements as set out in the LRA Procedures Manual.
8) Perform my duties as an LRA fully, responsibly, and diligently, in a professional and competent manner.
9) Immediately notify a Local Registration Authority within my organization or Ontario Health when the organization identified below no longer requires me to act as an LRA or I no longer wish to act as an LRA for any reason.

I understand that:

- My appointment as an LRA is not approved unless Ontario Health provides me with ONE® ID Credential signifying Ontario Health's acceptance of me as an LRA;
- Ontario Health may suspend me from acting as an LRA or terminate my designation as an LRA for any reason, including but not limited to, my failure to comply with the obligations set out above;
- My actions as an LRA may be subject to an audit from time to time to ensure compliance with the obligations set out above; and
- My appointment as an LRA is subject to the obligations set out above and by accepting below, I acknowledge that I have read and understand these obligations and commit to adhere to the same.

Appendix C – Ontario Health Identity Federation

The Ontario Health Identity Federation is a business and technology framework which establishes trust amongst member organizations with respect to end user identity validation, authentication, and access. Common agreements, policies, and technology standards enable secure access to provincial services via local credentials.

The Ontario Health Identity Federation allows organizations to authenticate users locally and send the requisite information to federated services which, in turn, allow access. The established trust within the Federation ensures confidence that the information shared is both valid and secure and enables a “Single Sign-On” (SSO) experience for end users such that they can use a single Login ID & password to access both local and provincial services.

NOTE: Not all services rely on Federation infrastructure, however alignment with its Identity Standard is a pre-requisite for accessing all services managed by Ontario Health, i.e. requirements for identity assurance and authentication must be met before Personal Health Information can be accessed online, regardless of the technical specifics.

Entitlement Prerequisites

Before an individual can be authorized to access a service their identity must first be verified with sufficient assurance to meet the requirements of the respective Application Provider; i.e. only valid credentials may be authorized for access. Identity Providers establish an identity assurance level for all registered individuals and issue credentials that may be relied on to authenticate an individual’s identity. Such credentials are a pre-requisite for entitlement to access a service.

The User Registration Process is defined by the respective IDP and may or may not be executed by the same resource that manages entitlements. Regardless, the process must be completed prior to user entitlements being granted, and the LRA must be able to confirm that the credential being granted access belongs to the individual being authorized.

Identity Provider

Organizations with the Identity Provider (IDP) role create and maintain credentials for end users based on their real-world identities and authenticate them for access to Federated Services. IDPs must comply with Federation business and technology standards with respect to user identity management and authentication and complete technical integration such that they can pass validated data to the Federation Hub. An organization must assume this role in order to enable an SSO experience for its users.

Health Information Custodians

HICs leverage Federation infrastructure to access Digital Health services. They are likely to have relationships with Application Providers independent of their use of Federation (e.g. they may be required to sign a service agreement) as their role is to authorize users for access as per The Sponsorship Model. This role does not require technical integration with the Federation Hub, but an Organization would also have to assume the role of IDP to enable an SSO experience for its users.

Appendix D – Panorama Service

The purpose of this document is to outline the steps to provide user access to the Panorama service in ONE® ID with a focus on the steps unique to Panorama roles

Sponsorship

The following organizational units are currently the only sponsors for the Panorama service:

- Public Health Units (PHUs)
- Ministry of Health and Long-Term Care – Health Services Cluster

Registration

For users that do not already have a ONE® ID account, validation of identity information is a prerequisite for account creation and enrolment of users into the Panorama service. The identity validation method can vary depending on your organization. Refer to section Identity Validation for detailed options.

Enrolment

To add the Panorama enrolment and applicable role(s), follow the enrolment steps summarized below.

- From the ONE® ID home page, select **My workspace** -> **Create / modify ONE® ID account**
- In the Login tab, type in full or partial ONE® ID account to search, press Search button

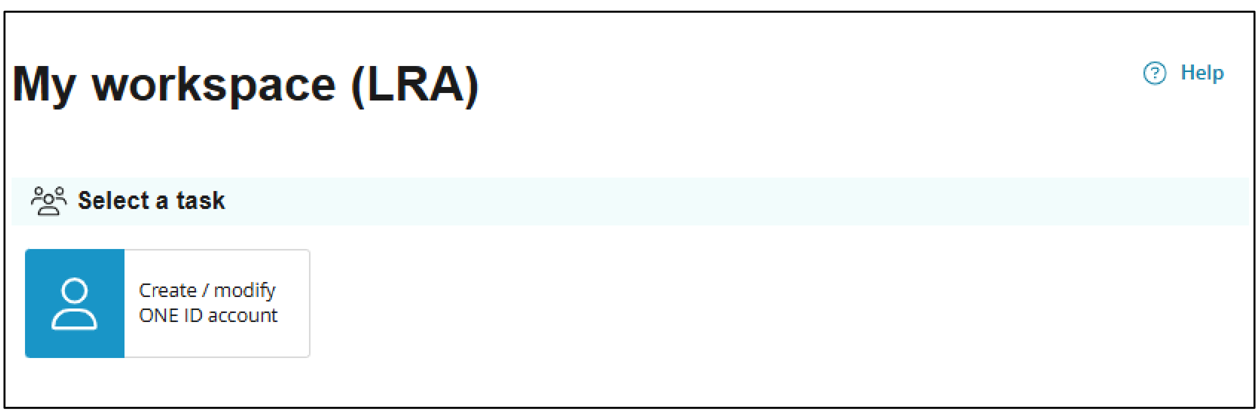


Figure 1 - My Workspace

- Click on the profile that appears in the search result to proceed with modification:

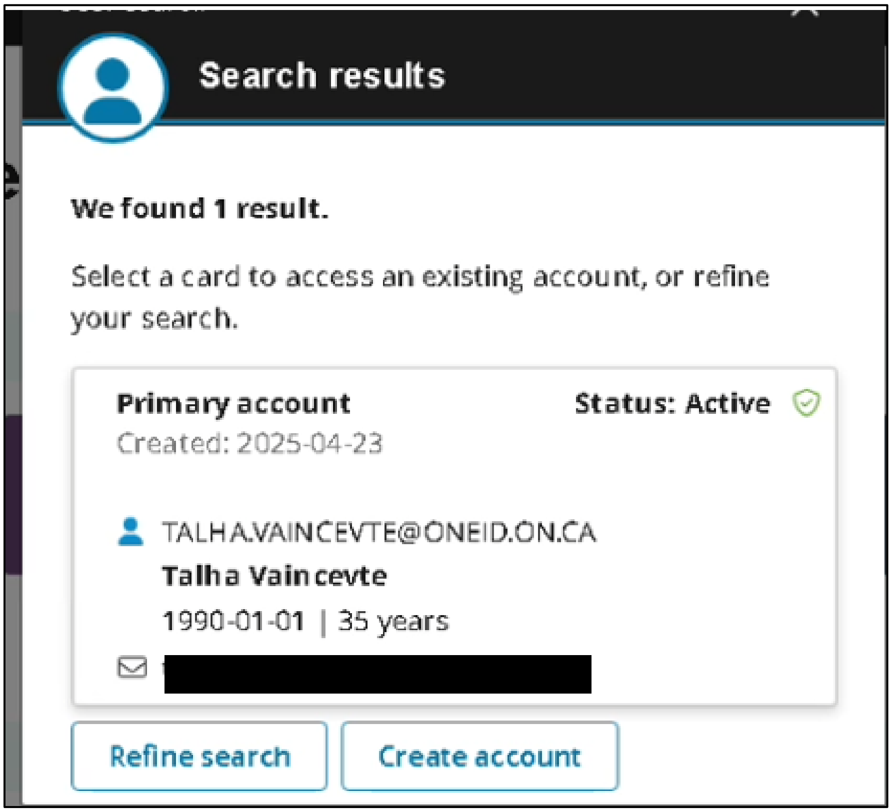


Figure 2 - Search by LOGIN ID Results

- The next page will ask upon whose authority you are requesting to change the account, select **Myself** as account requester, and press continue. You will now be at the user's profile screen: Select the **Services** tab and click **Add a Service**
- Select the **Services** tab and click **Add a service**
- Select **Sponsoring organization** (type to search) and **Service or role** (select the Panorama enrolment and applicable role(s) that have been authorized for the registrant and click **Next**)
    - There are three Panorama Services to enrol for:
        - Panorama User
        - Panorama CCM-BI
        - Panorama Inventory
        - Panorama Verification
- Fill in the enrolment attributes for Panorama enrolment; these are the user's Health Unit organization, role(s), and services delivery location(s).

- Multiple roles may be assigned in the **Panorama Roles** field based on provisioning requirements and the intended user access. While the applicable roles are listed below, a complete reference can be found in the [Panorama Individual Service Enrolment Form]:
    - Immunization View Only
    - Immunization Management
    - Immunization Full Clinical
    - Immunization Provider
    - Immunization Full Administrative
    - Immunization Reminder/Recall
    - Immunization Data Entry
    - Immunization Data Import/Export
    - Immunization Duplicate Management
    - Immunization PHU Superuser
    - Inventory PHU Clerk 1
    - Inventory PHU Clerk 2
    - INVENTORY Customer Service Clerk 1
    - INVENTORY Customer Service Clerk 2
    - INVENTORY Warehouse Service Clerk 1
    - INVENTORY Warehouse Service Clerk 2
    - INVENTORY Procurement Clerk 1
    - INVENTORY Procurement Clerk 2
    - INVENTORY Superuser Role
- ***NOTE***: Role(s) indicated on the **Panorama Role** field is used by the administrator to create the user account directly in the Panorama application. If a modification is required for these attributes, please contact the Panorama Administrator directly at the Ministry of Health.

- Click **Add**

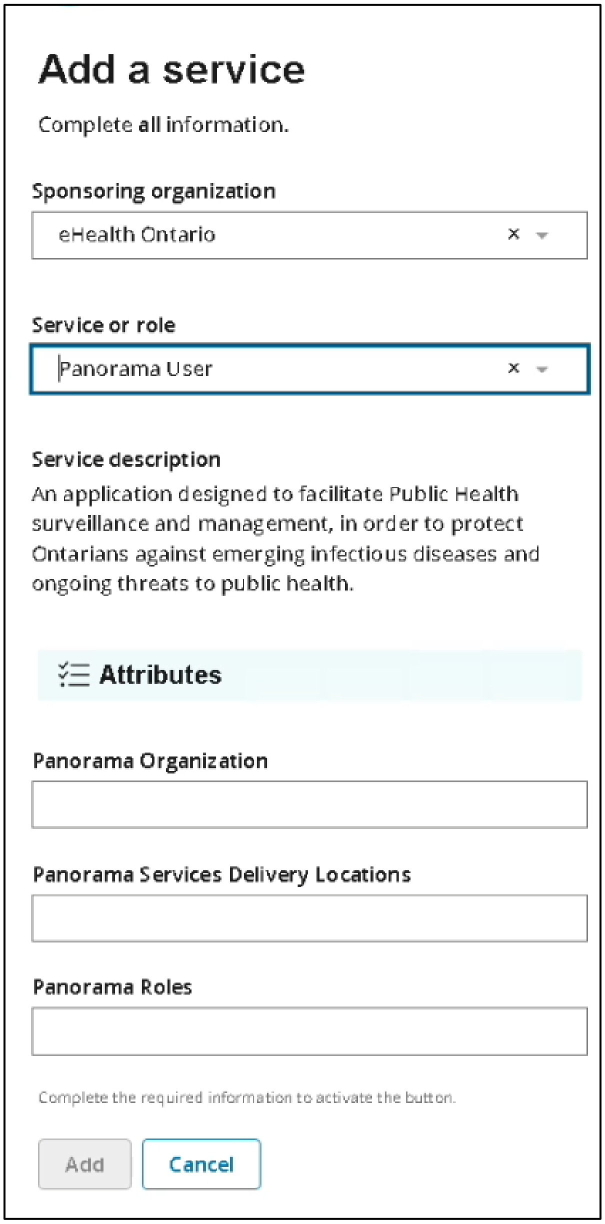


Figure 3 - Add a Service

- Proceed to the RSA console to assign a physical token to the user by entering, the token serial number in the user's RSA profile. Refer to Appendix F for guidance on how to assign RSA tokens.
    - If you have run out of tokens, contact the Ontario Health Service Desk to request spare tokens for future enrolment.
    - If the registrant already has an RSA token for one or more of their other services e.g. the Integrated Public Health Information System (IPHIS), you will not need to add a token as the user can use their existing ONE® ID token.

Ontario Health

NOTE: LRAs cannot add a service to their own account or another LRA account, however they are able to modify PI for their own account, like email, phone #, password, etc), or other LRA accounts.

Panorama Application Roles

When a user is enrolled into Panorama or their Service enrolment is modified in ONE® ID, the Panorama Administrator will receive a system generated email notification with the enrolment information. This information is used by the authorized Panorama Administrator to create user accounts and configure role-based access permissions within the Panorama application itself.

An email notification will be generated for the following Panorama enrolment/role modifications:

- Panorama enrolment is added to a new or existing Registrant.
- Additional Panorama role is added to an existing registrant.
- Panorama enrolment is revoked.
- Panorama role is deleted.

Panorama Inventory Role

Ministry of Health and Long-Term Care - OGPMSS was the initial organization sponsoring users for Panorama inventory role. However, all PHUs can now sponsor eligible users for the service. The appropriate organization must be selected in ONE® ID for enrolment purposes.

Enrolling a User in Panorama with Training Role

If a user has been authorized to access the Panorama Training Environment, a subsidiary account will have to be created for the user. The registration information from the parent ONE® ID account (i.e. personal information) will be automatically pre-populated over to create the subsidiary account. The Login ID that must be created for the Panorama training ONE® ID subsidiary account is FirstName.LastNameTR@oneid.on.ca, so it can be easily identified.

For instructions on creating the subsidiary account for training, please read subsection: Making a Subsidiary Account for Panorama Training or Panorama Guided Workflow Training. Alternatively, you may request that the Ontario Health Registration Agents create the subsidiary account on your behalf by sending them an email.

NOTE: Only the Panorama Training role can be added to the FirstName.LastNameTR@ONEID.ON.CA account. If any other service enrolment or Panorama role is added to this account, access to the service will be denied.

Requesting multiple Panorama enrolments

Panorama is a single sponsor enrolment; This is due to a Panorama Application restriction that allows only one Panorama enrolment to be associated with a user's ONE® ID account, regardless of sponsoring organization. Once a Panorama enrolment has been added to a registrant's profile, it will not be available for selection again in their ONE® ID profile due to this Panorama restriction.

To add a Panorama enrolment under the sponsorship of an additional PHU, a subsidiary account will need to be made. Existing ONE® ID user ID format of **firstname.lastname@oneid.on.ca** from the parent account will be replicated for the subsidiary account; however, a number will be added to the prefix to create a new unique user ID.

As an example:

- if the user operates at two PHUs – Peel and Toronto, with Peel being the primary location of operation, the user's parent ONE® ID account will contain the Panorama enrolment sponsored by Peel while the subsidiary account will contain the second enrolment sponsored by Toronto.
- The administrator will configure each of the two user accounts to have access to the data for only Peel or Toronto respectively so that the user cannot view both sets of data at the same time in any location, in other words the user cannot view Toronto's data when they are located at Peel and vice versa.
- The user will have to manage multiple accounts, and each account will have its own RSA token.

If the user requires Panorama access at multiple locations like the above example, refer to the steps contained in the subsection Making a Subsidiary Account for Additional Panorama/PGW Locations. Alternatively, you may request that the Ontario Health Registration Agents create the subsidiary account on your behalf by sending them an email.

Ontario Health

Appendix E – Panorama Subsidiary Accounts

This appendix will cover steps on how to create subsidiary accounts for multiple Panorama and Panorama Guided Workflow Locations, as well as how to make subsidiary accounts for the purposes of Panorama Training & Panorama Guided Workflow Training.

While creating subsidiary accounts follows a common process, the subsections below distinguish the unique steps required to make a sub account for training purposes vs creating a sub account for additional Panorama locations (ie; multiple PHUs or multiple pharmacies)

Panorama Subsidiary Account Structure

To represent the parent vs subsidiary account(s) structure for a user, it will look like the following:

User's Name	**Master Account - Primary Organization**	**Second Account – Training**	**Third Account - 2nd Organization**	**Fourth Account - 4th Organization**
Jane Doe	jane.doe@oneid.on.ca	Jane.doeTR@oneid.on.ca	jane.doe**1**@oneid.on.ca	jane.doe**2**@oneid.on.ca

If there is an existing name with an exact match, the second Jane Doe will get the following user IDs:

User's Name	**Master Account - Primary Organization**	**Second Account – Training**	**Second Account - 2nd Organization**	**Third Account - 3rd Organization**
Jane Doe	jane.doe3@oneid.on.ca	Jane.doeTR1@oneid.on.ca	jane.doe**4**@oneid.on.ca	jane.doe**5**@oneid.on.ca

And so forth.

Making a Subsidiary Account for Panorama Training or Panorama Guided Workflow Training

This sub-section explains how to create a subsidiary account for Panorama or Panorama Guided Workflow Training.

NOTE: For Panorama Training, the service is named **'Panorama – Training',** and for Panorama Guided Workflow (PGW) training, the service is named '**Panorama - Guided Workflow - Training'.** Please ensure you are provisioning for the correct training role upon making the subsidiary account.

Please follow the steps below to create a subsidiary account for training purposes:

- From the ONE® ID home page, select **My workspace (LRA)**, **Create / modify ONE® ID account**
- Look up the user you would like to make a training sub account for, and select their profile (through either name, email or login)
- Select their profile that appears in the search result, select **myself** as account requester, and press continue. You will now be at the user's profile screen:

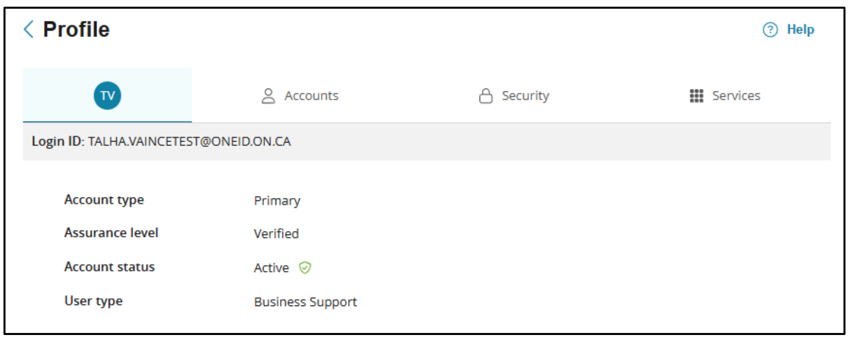


Figure 4 - Profile Page

- Select the **Accounts** tab of the User Profile and in the dropdown select **create sub account**:

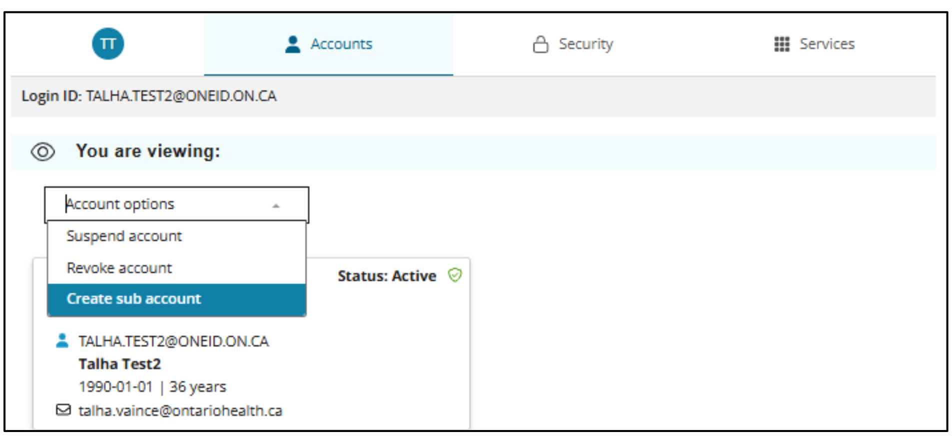


Figure 5 - Create Sub Account Button

- A screen will appear asking you to confirm preferred first and last name for the sub-account. At this point you *must* add **TR** at the end of the preferred last name (highlighted in the screenshot), as this will give the distinction that the sub-account is for training purposes only:

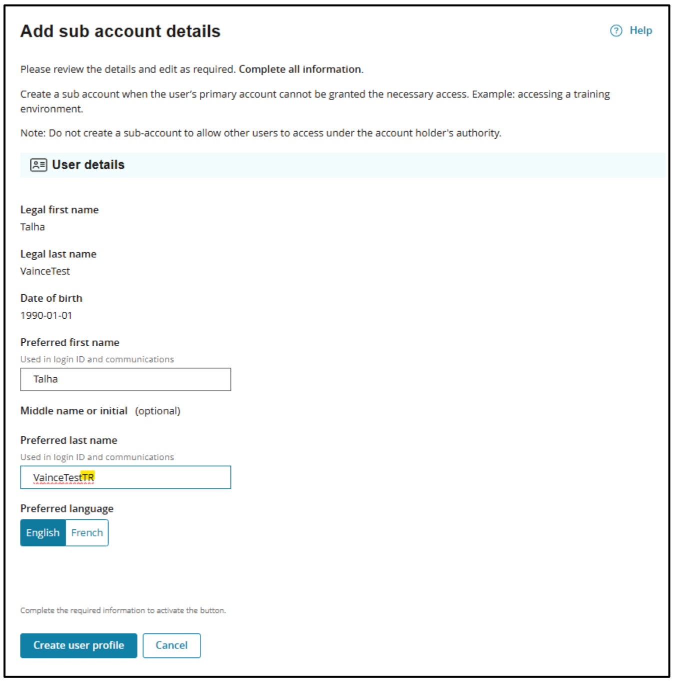


Figure 6 - Modify Sub Account Details

- Once you have added this amendment select **Create User Profile**
- The next page will have you confirm the user's contact info, in particular email, mobile phone and configuration of new Service Desk Challenge Questions. Once these details are filled out click **Save and Continue**
- Now you will be in the **Add services** step of the account creation process. To add the '**Panorama Training**' or **'Panorama - Guided Workflow – Training'** role, select '**Add Services**', select the sponsor the user is to be enrolled under and then fill in the enrolment attributes for the enrolment; these are the user's Health Unit organization, role(s), and services delivery location(s). Once you have inputted the required information, click **Add**

NOTE: While other roles are available for selection, only the training role must be added to the account since it is exclusively for access to the training environment; Other service roles <u>**will not**</u> work with this subsidiary account.

- Now click **complete registration**, upon which an email is sent to the user with their TR ONE® ID Login ID and instructions on how to self complete their registration.

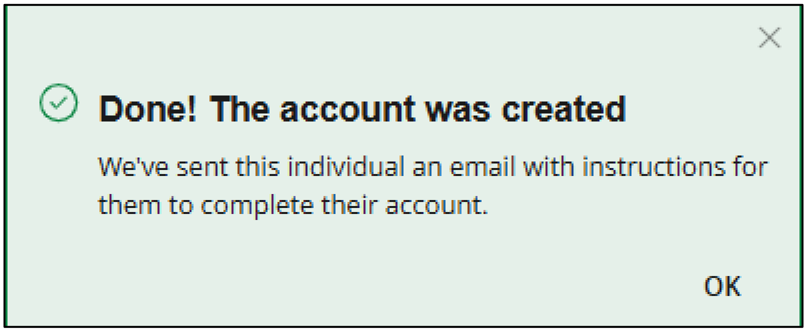


Figure 7 - Sub Account Creation Complete

- Once the user has self completed their registration through the email link, they will be able to access Training with their sub account login details.

Making a Subsidiary Account for Additional Panorama/PGW Locations

This sub-section explains how to create a subsidiary account for Panorama Service or Panorama Guided Workflow, in the case where the user needs to access the services from multiple locations.

- From the ONE® ID home page, select **My workspace (LRA)**, **Create / modify ONE® ID account**
- Look up the user you would like to make a sub account for, and select their profile (through either name, email or login)
- Select their profile that appears in the search result, select 'myself' as account requester, and press continue. You will now be at the user's profile screen:

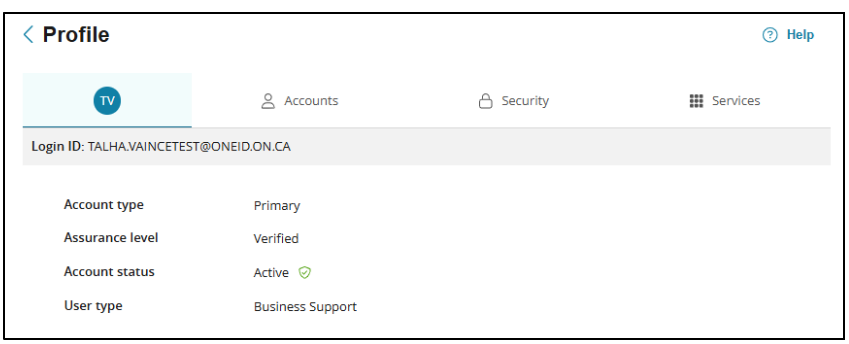


Figure 8 - Profile Page

- Select the **Accounts** tab and in the dropdown select **Create Sub Account**:

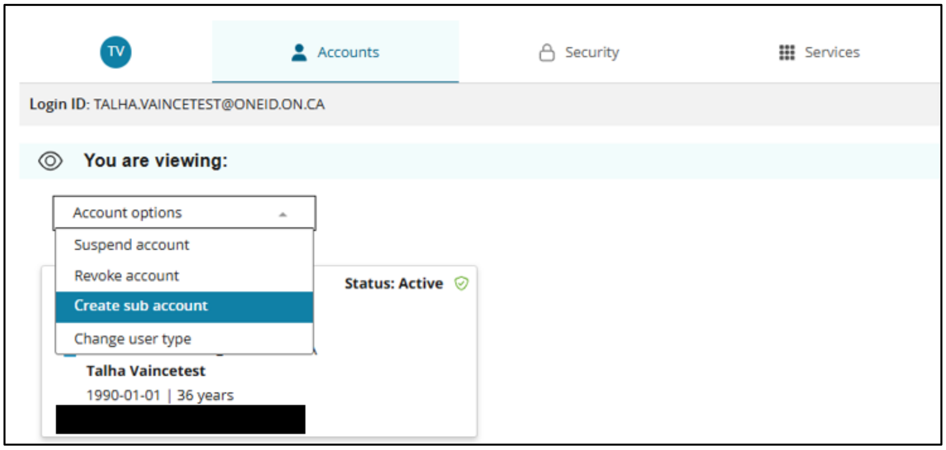


Figure 9 - Create Sub Account Button

- A screen will appear asking you to confirm preferred first and last name for the sub-account. Do not edit any of these details and simply click **Create User Profile**.
- Now confirm the security info on the next screen for the user and click **Save and Continue**.
- Click **Add Services** and enrol the user for the Panorama or PGW Service Role under the desired sponsor of choice and then fill in the enrolment attributes for the service; these are the user's Health Unit organization, role(s), and services delivery location(s). Once you have inputted the required information, click **Add**.
- Click **Complete Registration**, upon which an email is sent to the user with their sub account ONE® ID Login ID and instructions on how to self complete their registration. Once the user has self completed their registration through the email link, they will be able to access Panaroma under the second sponsor with their sub account login details.

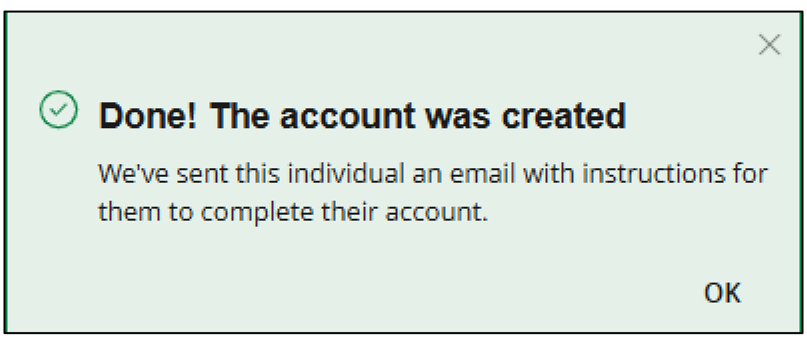


Figure 10 - Sub Account Creation Complete

Requesting Ontario Health to create Subsidiary Accounts for Panorama/PGW Access for multiple locations or training

Alternatively, LRAs can request Ontario Health Registration Agents to create user subsidiary accounts in their stead.

To request additional ONE ID subsidiary accounts for a user who requires multiple access or a training account, send e-mail with the information listed below to Ontario Health Registration Agents at oneidregistrationagents@ontariohealth.ca

Please specify the user's existing ONE® ID account (primary account) and the name of the organization the user is currently enrolled under.

For the new additional account being requested, specify the following:

a) User's First Name
b) User's Last Name
c) Requesting Organization Name (sponsoring organization)
d) Sponsor's Name and Designation
e) LRA Name
f) Type of enrolment/role
g) List attributes (Health Unit organization, role(s) and service delivery location(s))

Appendix F – RSA Quick Reference Guide

This quick reference guide will walk through basic functions of the RSA Console which LRAs can use to manage their users' RSA tokens.

Overview

The RSA Console is an application used to manage RSAs assigned to ONE® ID users. LRAs can troubleshoot potential RSA issues using the consoles, as well as reuse tokens by reassigning them to new users.

This quick reference guide will teach LRAs how to:

- Log in
- Navigate the Home Menu
- Assign a Token to a User
- Reset the PIN of a Token
- Resynchronize Tokens
- Reusing a Token
- Order Additional Tokens
- Reach out for general RSA inquiries

How to Access the Console

LRAs can access the console through this link: https://prds.ontariohealth.ca/ .

You will be asked for your ONE® ID Login ID and passcode (Token PIN + 6-digit code currently on token):

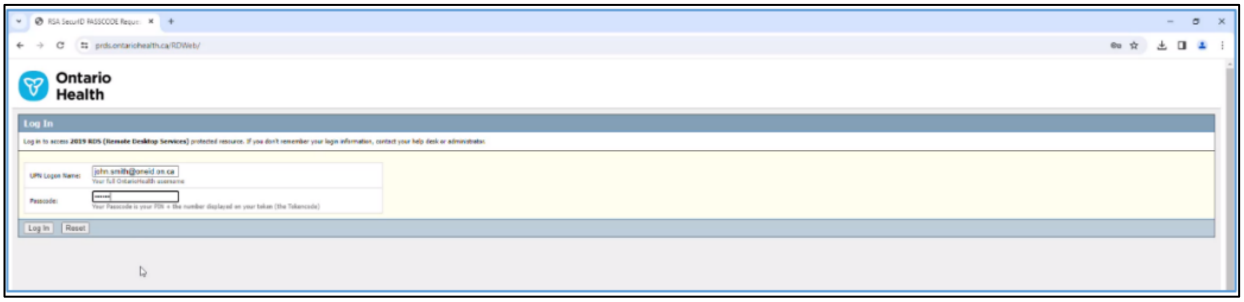


Figure 11 - MFA Screen

After entering your details, click 'Log In'. Note that you will be navigated to a subsequent 'Log In' screen after submitting your login credentials for the initial screen noted above. Now on the next screen, log in with your ONE® ID Login ID and Password:

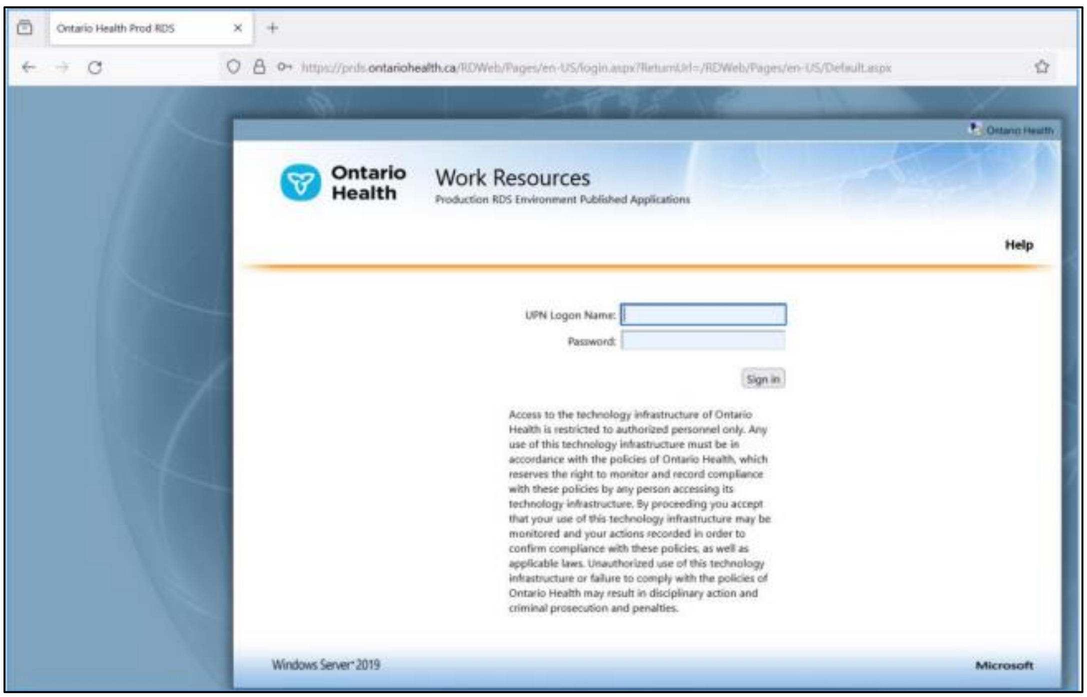


Figure 12 - RDS Login Screen

Upon logging in, you will be brought to this menu screen.

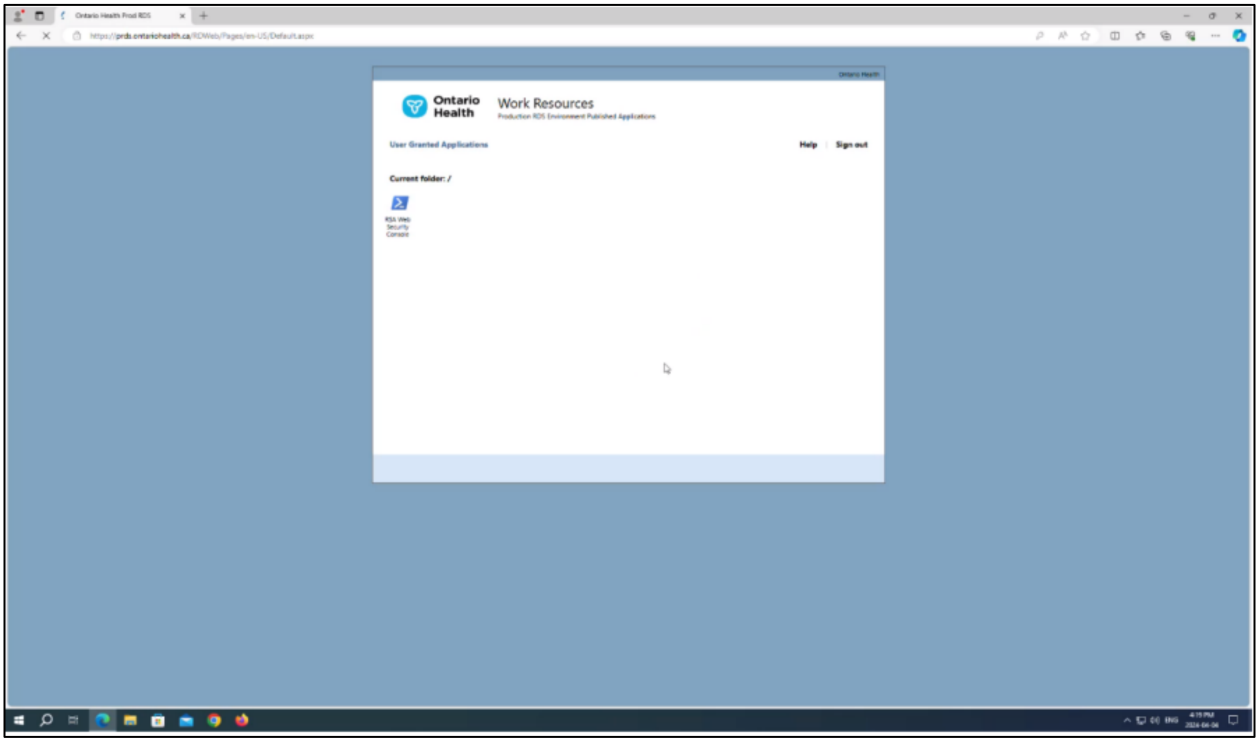


Figure 13 - RDS Work Resources Menu

Select the RSA Console Application.

Now the file for the Console will be downloaded to your computer:

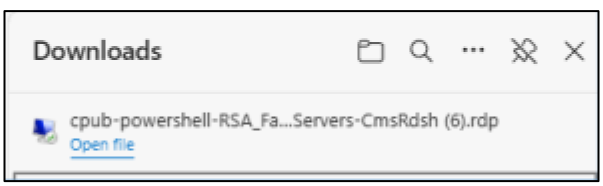


Figure 14 - Browser Download Pop-Up

Open this downloaded file to launch the application.

Upon launching, you will be asked to provide your ONE Login ID and Password again. Click **OK**:

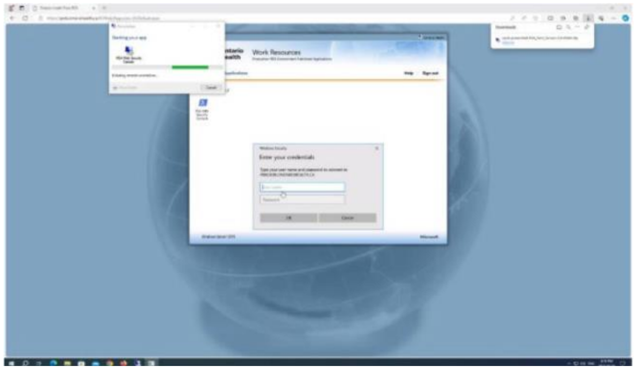


Figure 15 - Additional Authentication Screen for First Login

You will now be taken to the secure login screen. Enter your ONE® ID Login ID again and click **OK**:

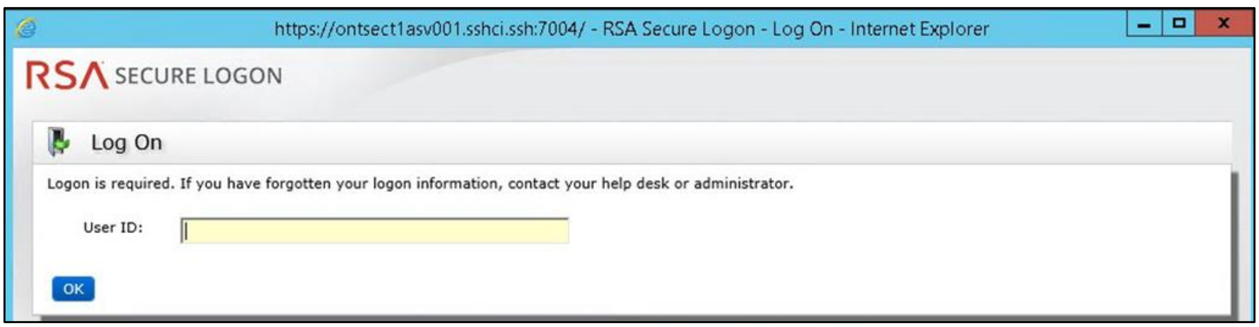


Figure 16 - RSA Secure Log on Screen

Choose whether you would prefer to enter your ONE® ID password (Password) or ONE® ID Passcode (Passcode) and click **Log On**:

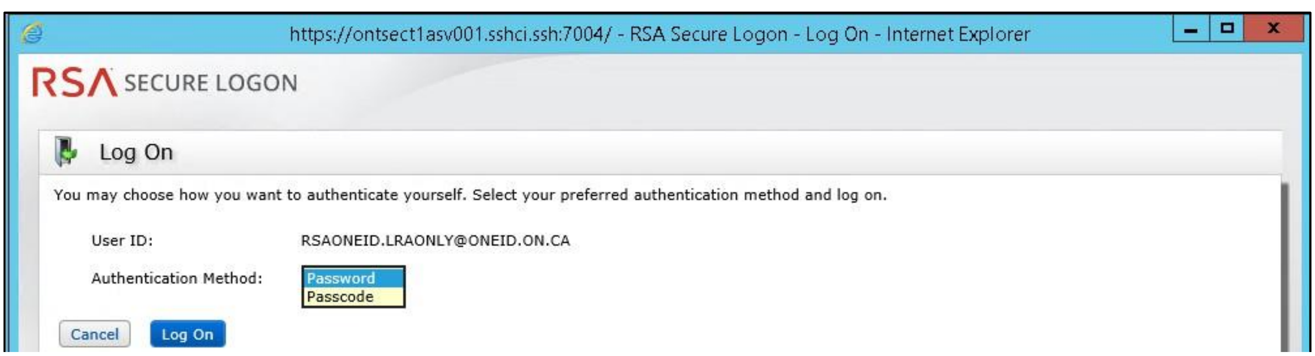


Figure 17 - RSA Secure Logon Authentication Options

NOTE: Your **Passcode** is your RSA PIN followed by the six-digit token code currently displayed on your token

Upon successful authentication, the **Home Menu** Opens.

Ontario Health

RSA Console Functions

Home Menu

The home menu serves as a starting point for multiple functions. Press the **Home** button on the top left at any time to return to this screen.

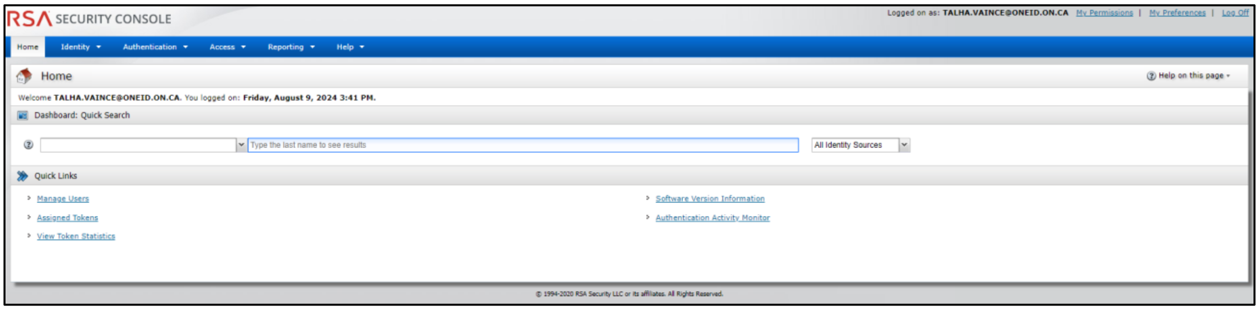


Figure 18 - RSA Console Dashboard

Dashboard

The dashboard is a search box located on the home menu. It is used to search for user profiles associated with RSA tokens. It has multiple filters you can search for by:

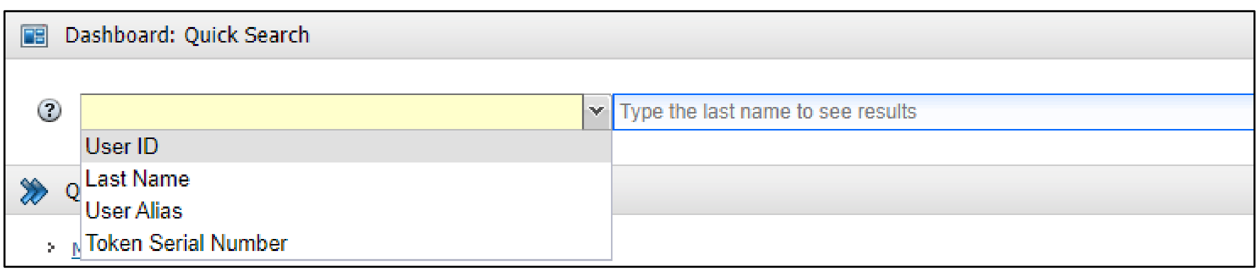


Figure 19 - RSA Dashboard Filters

- User ID – search by user's ONE® ID Login ID
- Last name – search by user's last name
- User Alias – search by a user's associated nickname
    - This filter is not too commonly used, as there are few aliases on the console
- Token Serial Number – search by an RSA's serial #

For the User ID, Last name & User Alias filter, there are also identity source filters:

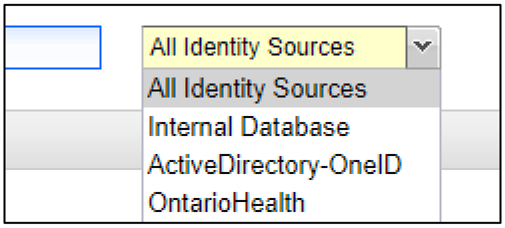


Figure 20 - Identity Source Filters

For purposes of LRA management, the main filter LRAs will work with is accounts under 'ActiveDirectory-OneID'. The other two filters only pertain to Ontario Health Employees.

Assigning a Token

To assign a token to a ONE® ID account, first search up the user's ONE® ID login on the home dashboard:

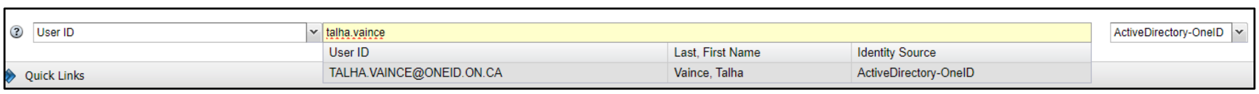


Figure 21 - Select User Search Menu

Click on the username and their profile will appear:

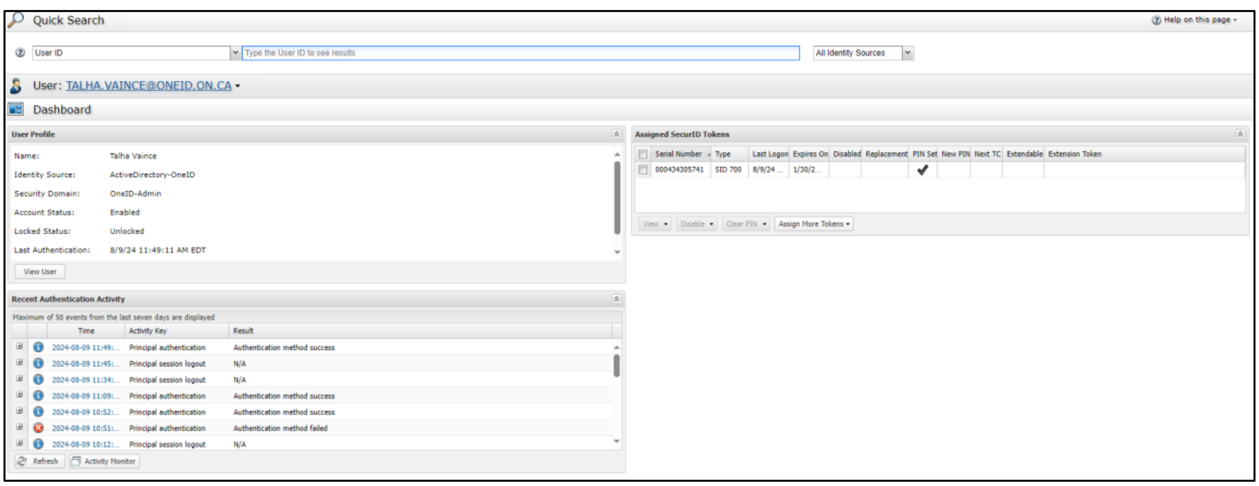


Figure 22 - RSA User Profile

Please note that users must already be enrolled to the enrolement which requires an RSA on ONE® ID, or else their username will not show up on the console.

To assign a token select the **Assign More Tokens** button under the **Assigned SecurID Tokens** tab:

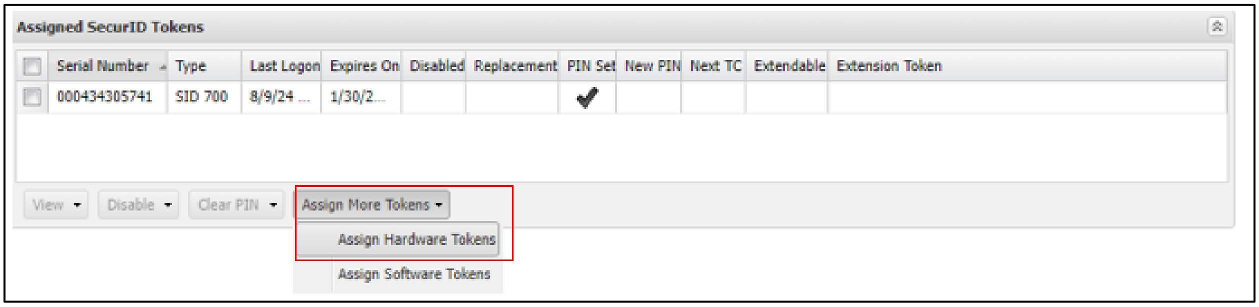


Figure 23 - Assign Hardware Tokens

Now select the desired token by entering its serial # and check it off. Then click **Assign Token(s):**

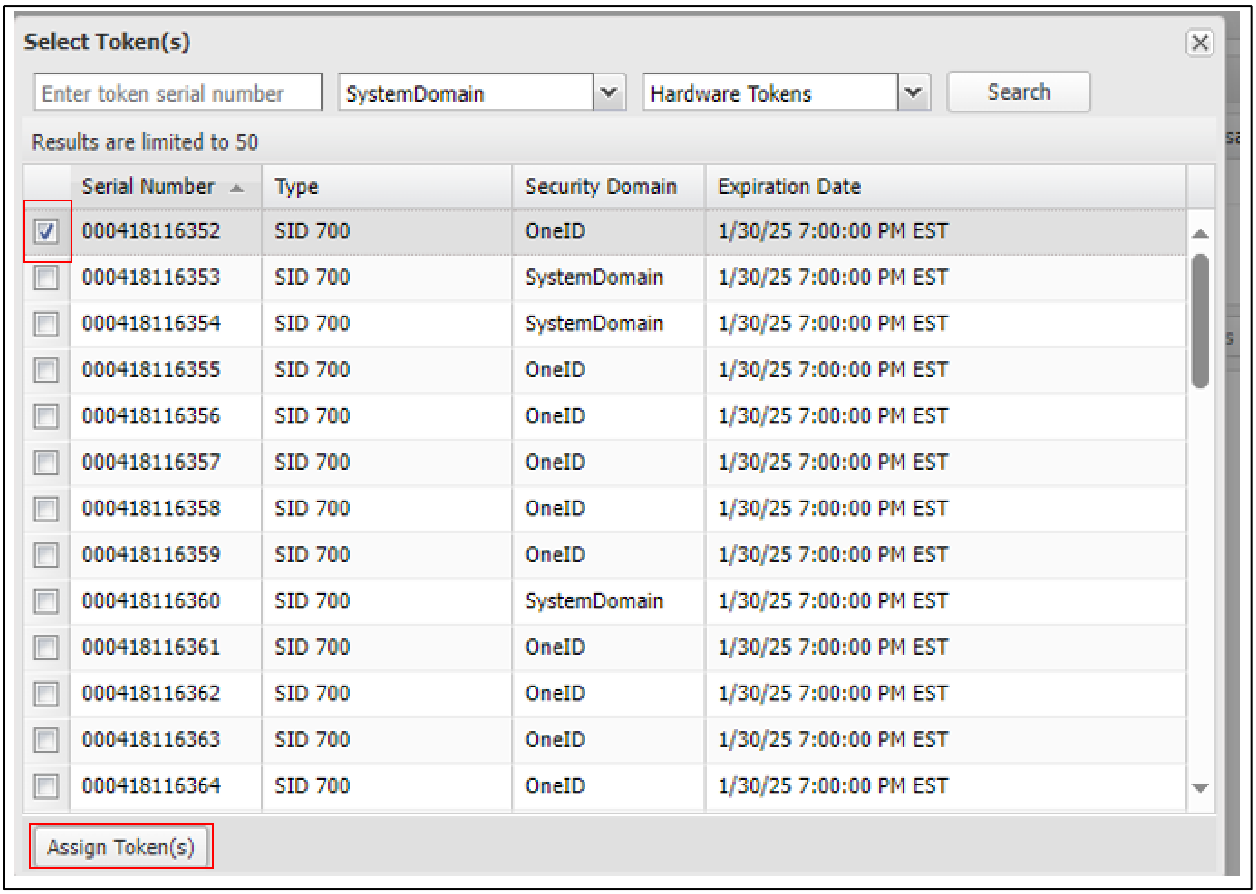


Figure 24 - Token Assignment Screen

There will be a notification indicating that you have successfully assigned the token to the user:

Figure 25 - Token Assignment Confirmation Screen

The token will remain at having **New PIN** checked off until they configure their RSA with their own PIN. Then this will change to **PIN Set**.

Tokens are assigned in Enabled (Active) status, if you are shipping the token to the user or will not be directly handing it to them, please disable the token straight after assignment. You can activate the token for the user when they have the token in their possession, or they can contact the Ontario Health Digital Service Desk to request activation.

RSA Troubleshooting

There are a few common issues with RSA tokens which can be resolved through the usage of the RSA console.

PIN Reset

When a user forgets the PIN they had set for their RSA token, it can easily be reset within the console. First, go to the user's profile and press **Clear PIN**:

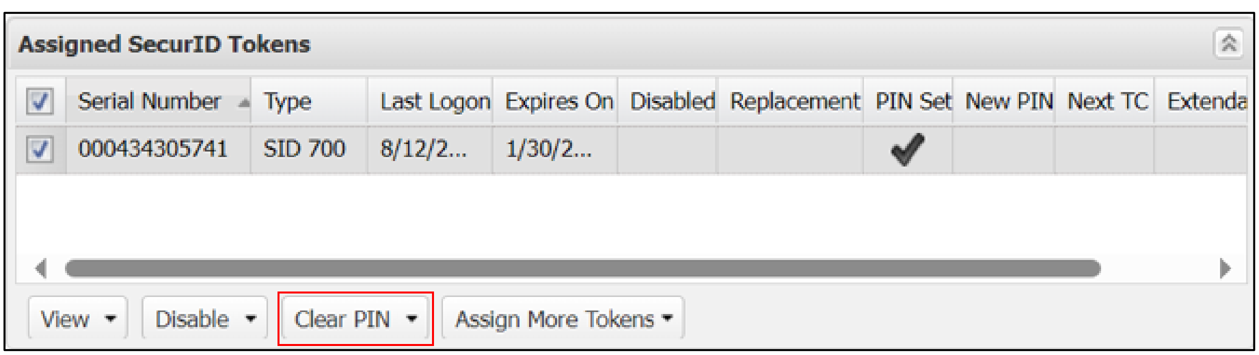


Figure 26 - Clear PIN Selection

The console will then ask you to confirm if you want to clear this token's PIN

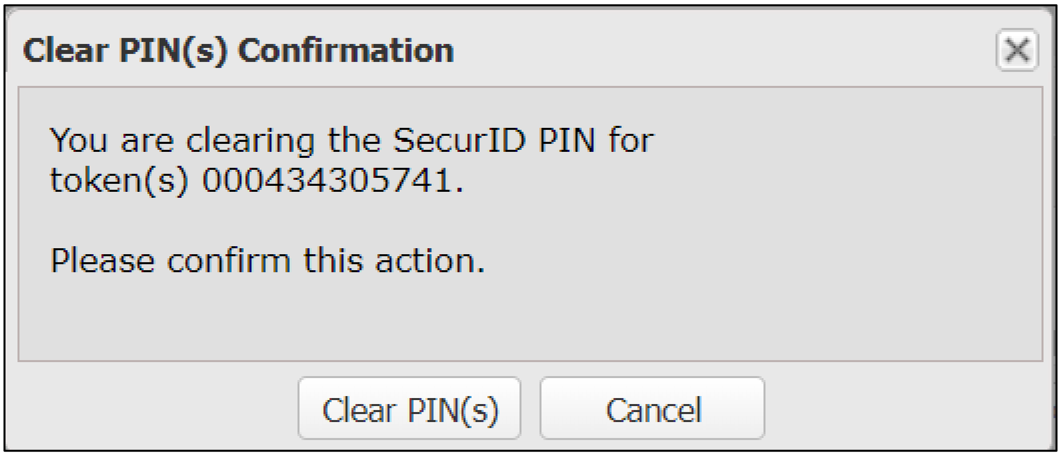


Figure 27 - Clear PIN Confirmation

Once the PIN has been cleared, the token will have changed to new PIN mode. Have the user log into ONE® ID and get to the RSA authentication screen. Just like any PIN setup, have the user only enter in their 6-digit code while leaving the PIN section blank. Then the screen to configure a new PIN will appear.

Next TC

If your token or another user's token is displaying the **Next TC** column checked off in the RSA Security Console, this means it requires resynchronization.

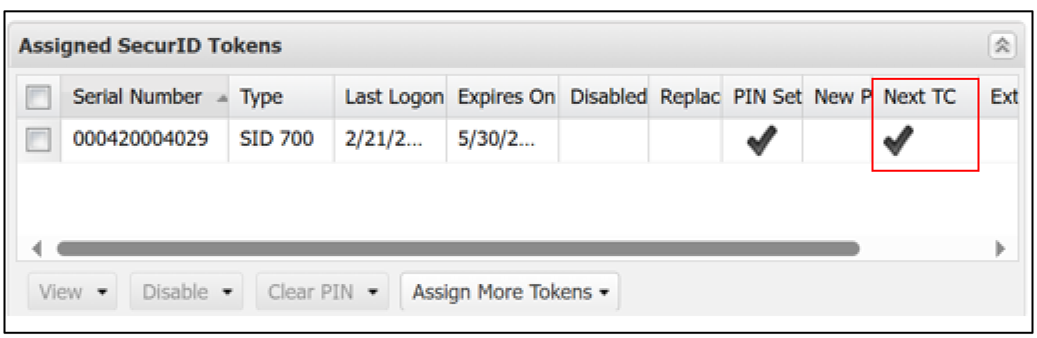


Figure 28 - Next TC Checkbox

To amend this, simply have them sign into their service where they use their RSA token, and have them authenticate as normal. They will be self-prompted to resynchronize their token.

If the user does not get self-prompted, they should reach out to OH Service Desk for further assistance.

Token Replacement

If a token has been lost or is faulty, LRAs have the power to assign a replacement token. Go to the user's profile, check off the desired token **Assigned SecurID Token** tab then select **Replace** under the **View** drop down menu:

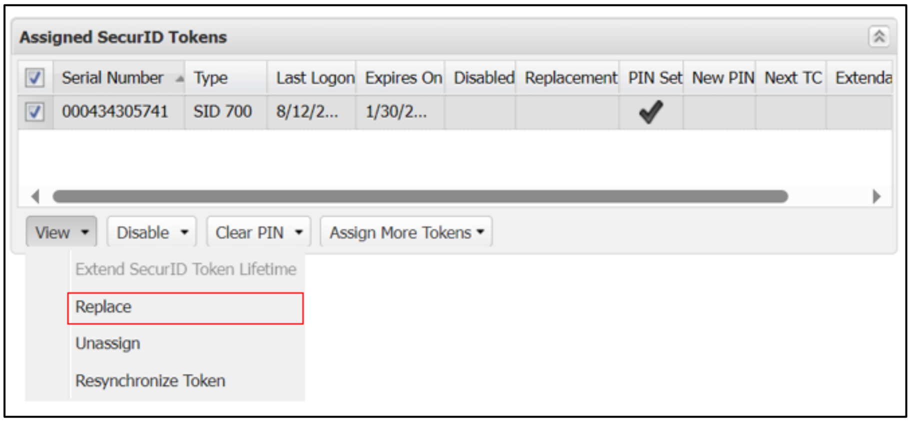


Figure 29 - Replace Token Option

Then the **Select a Replacement Token** pop up window will appear, enter the serial # of the token you are going to replace the older token with.

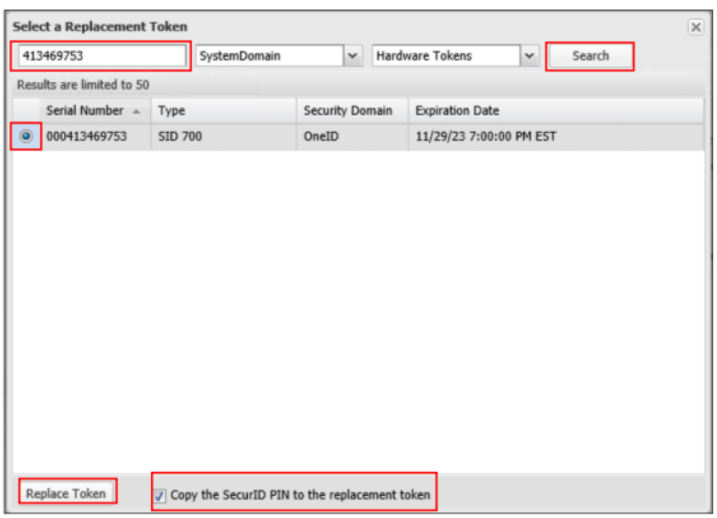


Figure 30 - Selecting a Replacement Token

Check it off and check off the **Copy the SecureID PIN to the Replacement Token** to have the old PIN carry over to the new token. Then click **Replace Token**. You will get a notification that the token has been replaced.

Reusing Tokens

There are instances where users no longer require their RSA token. LRAs can reuse these tokens and assign them to another user who may need it if the token has not expired. Once the user's RSA-dependent enrolment has been revoked in ONE® ID (ie; LRA, Panorama), the token will be automatically unassigned from the account within 24 hours. Then LRAs will have the freedom to reassign it to another employee who requires the RSA.

Ordering Tokens & Support

If LRAs wish to order extra tokens for their clients or have any general RSA inquiries send an email to OH-DS_Servicedesk@ontariohealth.ca or call 1-866-250-1554 with your inquiry.

Appendix G – How to View a User Account

Local Registration Authorities (LRAs) can view the profiles of end users sponsored by their organization. They can also register new users, update profile details, including resetting passwords, changing personal information, and adding or revoking services. This guide provides step-by-step instructions for searching and viewing ONE® ID accounts.

Searching for a User

To access a user profile, first open the '**Menu**' on the top right hand of the screen and press '**My Workspace**'

Figure 31 - Press 'Menu'

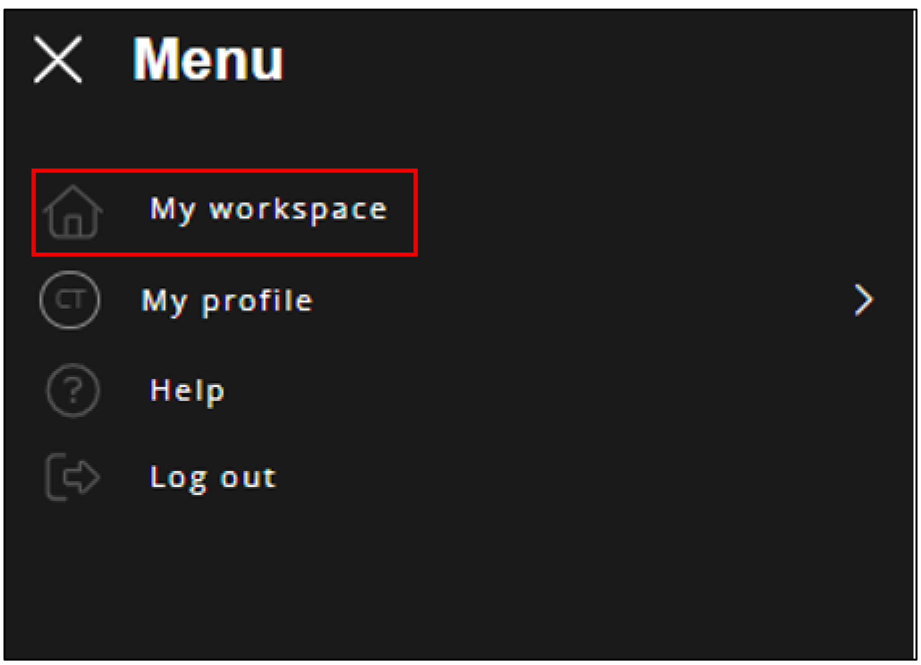


Figure 32 - Press 'My Workspace'

Then select **Create/Modify ONE® ID Account** and then enter the details of the user you would like to view. You can look them up by **Legal Name**, **Email Address**, or **Login ID**:

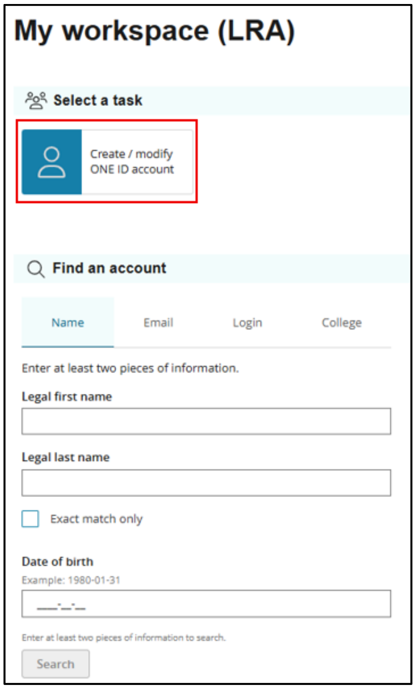
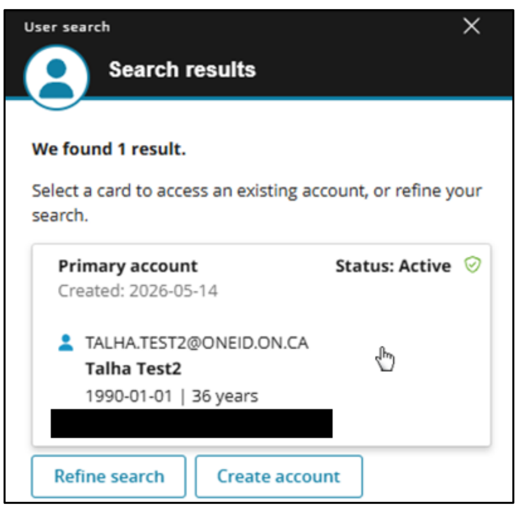


Figure 33 - Create/Modify ONE® ID Account

Once you entered in the desired user's information, select '**Search',** profiles with matching results will appear, simply press on the tile of the user profile you wish to view:



NOTE: At this point you also have the option of creating a new account by selecting the **Create Account** Button. Refer to the [Appendix L - *Register/Enrol a New User to ONE® ID*] for more details

Figure 34 - Search Results

You have now arrived at the user's account screen:

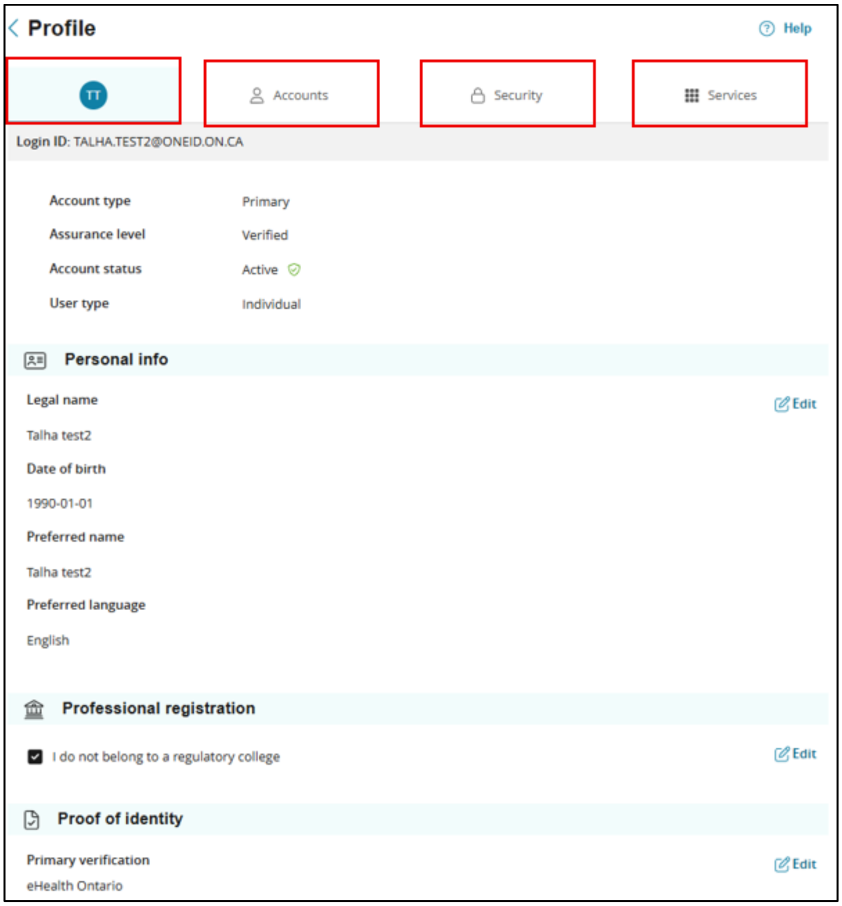


Figure 35 - User Account Screen

From here, you can press any of the four panes highlighted above to conduct a differing array of actions for the user profile.

Appendix H - How to Modify Profile Information

Local Registration Authorities (LRAs) can view the profiles of end users sponsored by their organization. They can also register new users, update profile details, including resetting passwords, changing personal information, and adding or revoking services. This guide provides step-by-step instructions for modifying personal information in ONE® ID accounts.

The ‘**Profile**’ page is the default screen you will land on when you enter. A user profile is always denoted by the user’s initials. Personal information for the user, including Legal Name, Preferred Name, Date of Birth, Professional Registration and Proof of ID is displayed here.

Changing a User’s Legal Name, Preferred Name, Date of Birth and Preferred Language

To change legal name, preferred name, date of birth or preferred language, press the ‘**Edit**’ button in the ‘**Personal Information**’ category. Remember to press Save on the next screen when you are satisfied with your changes.

Figure 36 - Personal Info

NOTE: If you do decide to change a user’s preferred name, ONE® ID will ask you if you wish to change their LOGIN ID to match this new preferred name, or to keep it the same. Please continue with your preference.

Changing A User's Professional Registration

LRAs cannot add, modify or remove a professional registration to a user's profile themselves. Rather, the user must do so themselves, for more information, please refer to the ONE® ID Registrant Reference Guide, section How to Update your Personal Information or Professional Registration

Adding/Changing a User's Identity Documents

If identity documents were not added during a user's initial registration, LRAs can edit them in the Proof of Identity section by selecting Edit and adding or changing the required documents.

NOTE: If the user has had their identity documents already successfully validated at a former point, the LRA will not be able to modify their identity documentation. If identity documentation for a user needs to be updated, please contact the Ontario Health Service Desk at 1-866-250-1554 or OH-servicedesk@ontariohealth.ca.

Appendix I - How to Modify Account Security

Local Registration Authorities (LRAs) can view the profiles of end users sponsored by their organization. They can also register new users, update profile details, including resetting passwords, changing personal information, and adding or revoking services. This guide provides step-by-step instructions for modifying account security information in ONE® ID accounts.

The **'Security'** page will display security information for the user, including their service desk challenge questions, days until password expiry, email, mobile phone number, and the modification event log on the user's profile.

Supporting Locked and Unlocked Users with Password Reset

Password resets conducted by LRAs follow a consistent process for both locked and unlocked ONE® ID accounts. LRAs can reset user passwords at any time through the user's **Security** page. To access the **Security** page, refer to Appendix G - *How to View a User Account*.

***NOTE*:** If a user account is not **locked**, users may reset their own password by selecting **Forgot Password** on the ONE® ID login screen.

When an account becomes **locked**, password resets must be performed by an LRA. In these cases, the account status will display **Reset Required**:

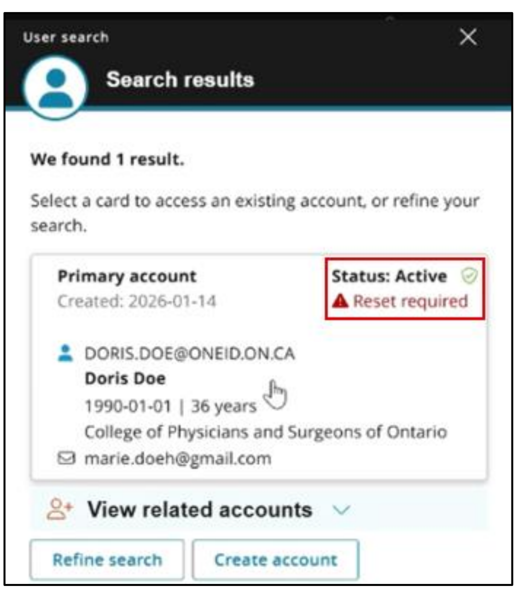


Figure 37 - Reset Required Profile

On the **Security** page, scroll down to the **'Password'** category and simply press **'Reset Password'**:

Figure 38 - Reset Password Button

An email will now be sent to the user with instructions to configure a new password, upon which they will be able to regain their ONE® ID access.

How to Change a User's Security Questions

The **Service Desk questions** section of the **Security** page allows you to manage the challenge questions used to verify over the phone with the Ontario Health Service Desk.

To edit the service desk challenge questions of a user, simply press **Edit** in the **Service Desk Questions** Category. Press **Save** in the next screen when you are satisfied with your edits.

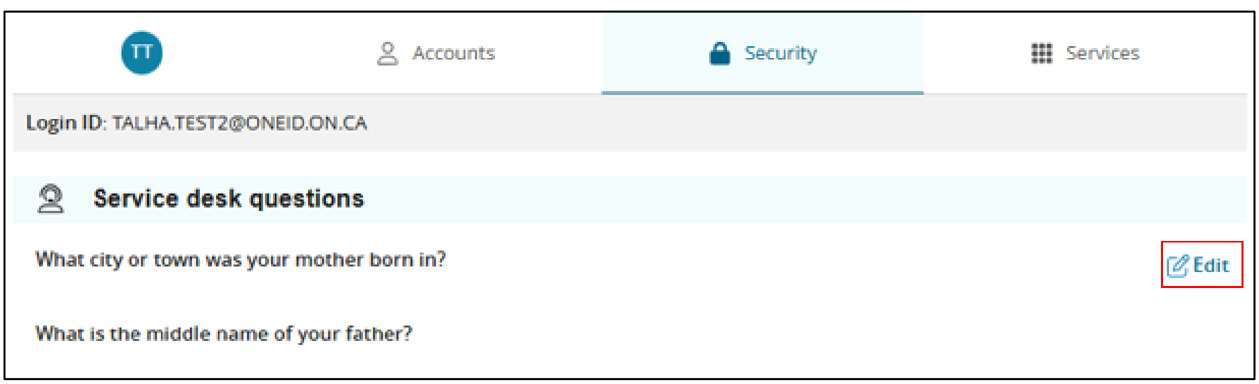


Figure 39 - Edit Service Desk Questions

NOTE: LRAs are only able to modify service desk challenge questions for a user, not online challenge questions. If the user wants to modify their online challenge, they will have to do so in their profile themselves. Please refer to the ONE® ID Registrant Reference Guide, section *How to Change Your Security Questions* for more information.

How to Change a User's Email, Contact Phone & Mobile Phone

The LRA can update a user's **email address**, **contact phone number** (used by Ontario Health to contact the client), and **mobile phone number** (used for SMS verification, if enabled by the client) by selecting **Edit** in the **Security Information** section. Once the changes are complete, select **Save** on the next screen.

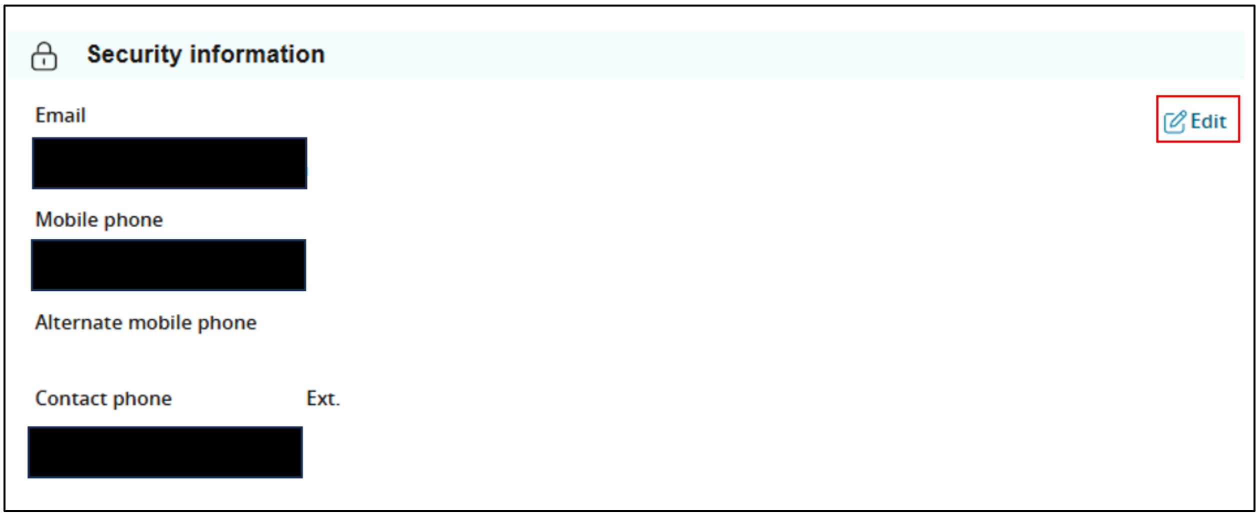


Figure 40 - Change Security Information

How to View a User's Event Log

LRAs can view a user account's provisioning history. The event log displays all enrolments that have been provisioned or revoked, along with any updates made to the account, including changes to personal information, passwords, and security details such as challenge questions and phone numbers.

To access it, scroll to the bottom of the **Security** page and select **View Event Log** in the **View Event Log** section:

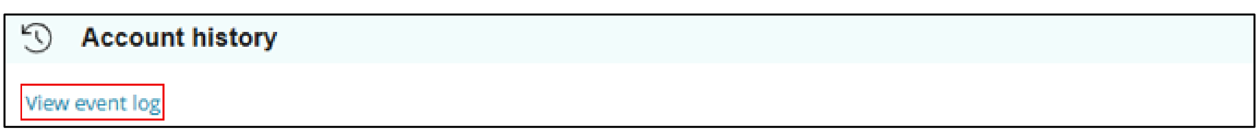


Figure 41 - View Event Log

You will then be taken to the user's event log. To exit, select **Close** in the bottom-right corner of the screen.

Ontario Health

Appendix J - How to Manage User Accounts

Local Registration Authorities (LRAs) can view the profiles of end users sponsored by their organization. They can also register new users, update profile details, including resetting passwords, changing personal information, and adding or revoking services. This guide provides step-by-step instructions for managing ONE® ID accounts.

The '**Accounts**' page will show you all the active accounts under the user. The LRA is also able to suspend, reinstate, or revoke the user account on this screen. Further, they can also create a subsidiary account for the user. To access the **Accounts** page, refer to Appendix G - *How to View a User Account*.

How to Suspend, Reinstate or Revoke A User Account

LRAs do not have the ability to suspend an active account nor reinstate it. Please reach out to Ontario Health Service Desk at 1-866-250-1554 or OH-servicedesk@ontariohealth.ca to have them conduct this task.

Accounts cannot be revoked by the LRA as well. Rather, it is encouraged that the LRA revokes the services of the user instead. Please refer to Appendix K – How to Enroll and Revoke Services for more details. If the user is no longer practicing in Ontario, then you can reach out to Ontario Health Service Desk to request account revocation.

How to Create a Subsidiary Account

An LRA can create a subsidiary account for a user in certain situations where services cannot be provisioned under the same account across multiple sponsorships. This applies to the following service roles:

- OHISS
- eNLB

NOTE: Panorama also uses this account model. However, a separate appendix is available that provides detailed instructions for creating Panorama subsidiary accounts.

To create a subsidiary account, select the **Account Options** drop-down and press Create **Sub Account.**

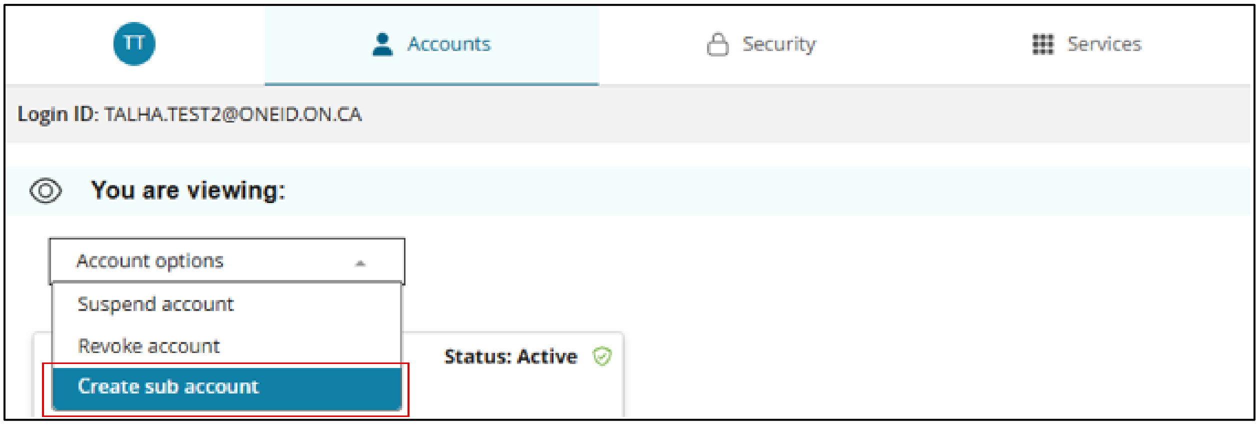


Figure 42 - Press Create Sub Account

The next screen will ask you to confirm preferred name details for the desired sub account:

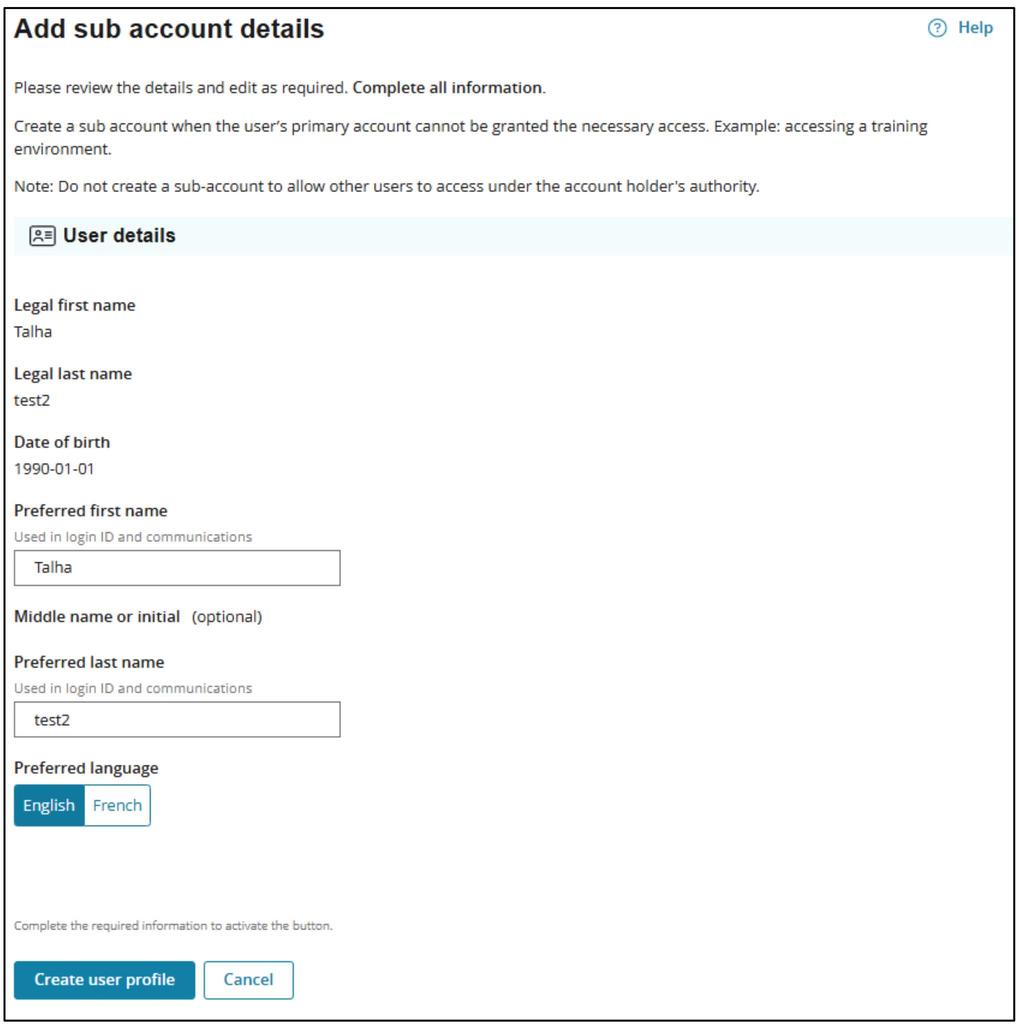


Figure 43 - Add Sub Account Details

If these inputs are not modified, the login for the subsidiary account will name itself by adding a number at the end of the original account name. For example, if your ONE® ID account is Joe.Singh@oneid.on.ca, the subsidiary account will be called Joe.Singh1@oneid.on.ca. If Joe.Singh1 is taken, it will go to Joe.Singh2, and so forth. Click **Create User Profile** once you are satisfied with these changes.

The next screen asks the LRA to confirm security details, including email, mobile phone, contact phone and security question. Once you have confirmed these details, select **Save and Continue**.

The last screen will give you the option to Add a Service to the subsidiary account. For more details on how to specifically add a service, refer to Appendix K - How to Enroll and Revoke Services. Once you are satisfied with the service enrolments or wish to add them later, select **Complete Registration**. An email will be sent to the user with instructions to self-complete their profile, after which they can access their new subsidiary account.

NOTE: Adding a subsidiary account for the purposes of Panorama training follows the same above process, save for the 'TR' you must add to the end of the preferred last name. For more information on making a subsidiary account for Panorama training, please refer to Appendix E.

Appendix K – How to Enroll and Revoke Services

Local Registration Authorities (LRAs) can view the profiles of end users sponsored by their organization. They can also register new users, update profile details, including resetting passwords, changing personal information, and adding or revoking services. This guide provides step-by-step instructions for enrolling and revoking services in ONE® ID accounts.

The '**Services'** page will display the current services the user is enrolled to, as well as under whose sponsorship they are enrolled under. The LRA can view, enroll, and revoke enrollment for the user on this page. To access the **Services** page, refer to [Appendix G - *How to View a User Account*.]

How to view a User's Services

All services that the user is enrolled under will be displayed in pages below the '**Add a Service'** button. In this screenshot, we see that the user is enrolled for two services, ConnectingOntario User and ONE Meds Conformance PST:

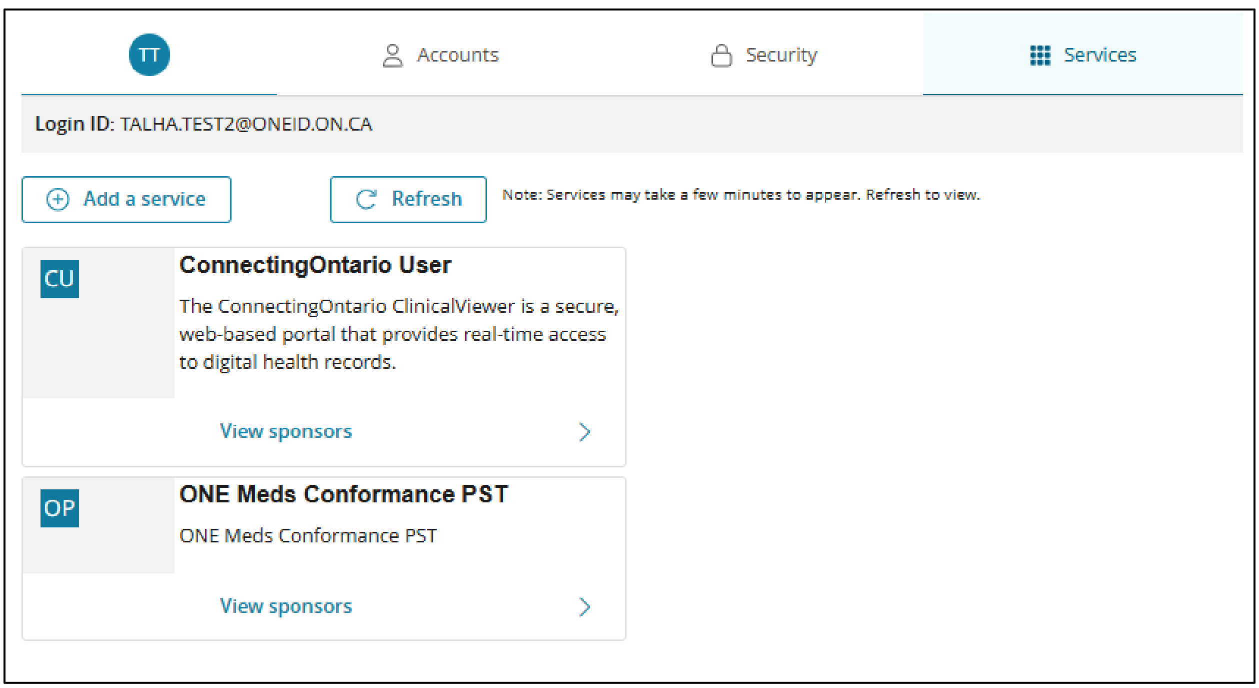


Figure 44 - User Services

To view the sponsor of which the user is enrolled under, simply select **View Sponsors.** You will see in the screenshot that both services are enrolled under the sponsorship of eHealth Ontario:

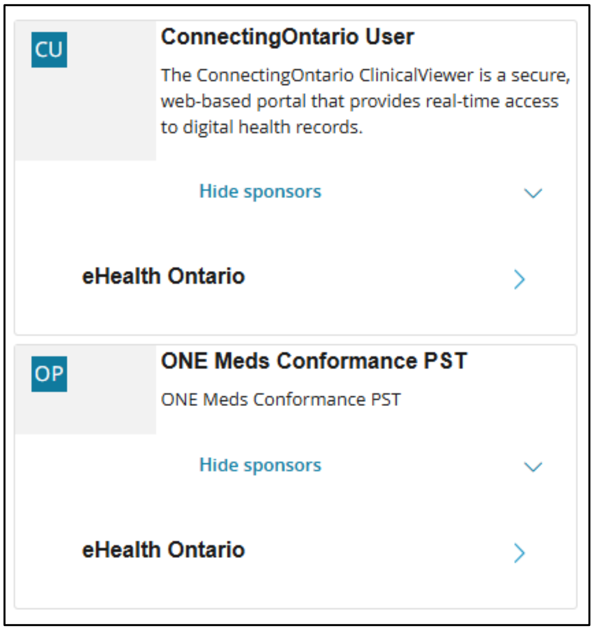


Figure 45 - Who is the Sponsor

Enrol an Existing User to ONE® ID Services

On the services page, select **Add A Service**

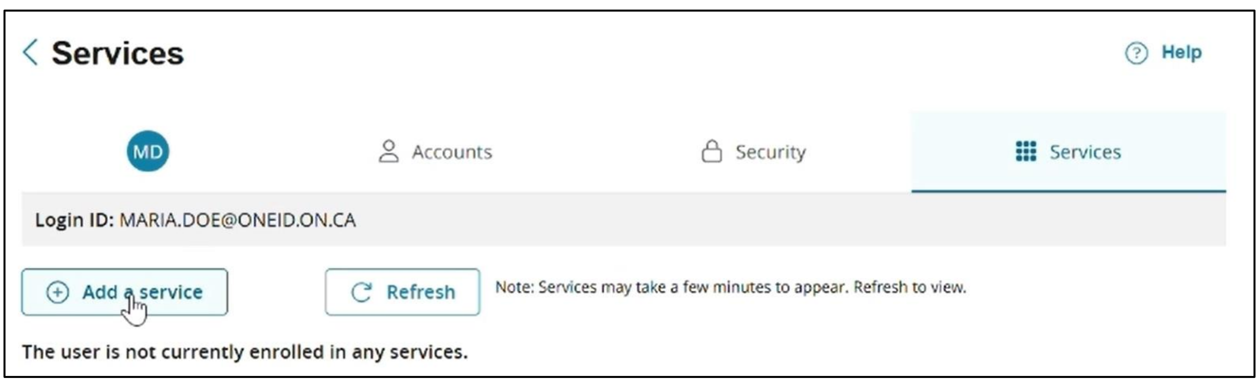


Figure 46 - Add A Service

In the sponsoring organization, enter the organization they would be provisioned under and in service or role select the desired service. Press **Add** once finalized:

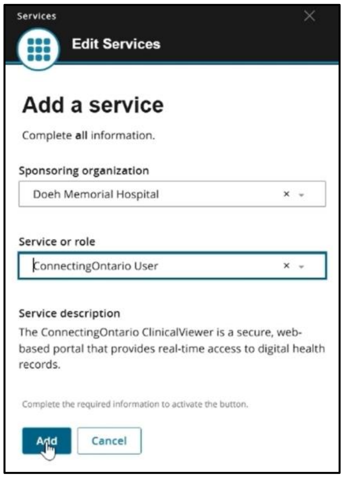


Figure 47 - Adding a New Service

The service has now been added to the selected account.

NOTE: You will only be allowed to add services under the sponsorship of the organization for which you are LRA for. IE; if you are an LRA for 'Doeh Memorial Hospital' and not for 'James Regional Hospital' you can only enrol a user for services under the sponsorship of 'Doeh Memorial Hospital' and not 'James Regional Hospital'.

How to Revoke a Service

To revoke a service, select **View Sponsors** of the enrolment you would like to revoke (as shown in sub-section *How to View a User's Services),* now press the user sponsorship under which you would like to revoke the service from:

Figure 48 - Press the Sponsor

A **Details and Attributes** Screen will arise, to which the LRA selects **Revoke** to revoke the service that was provisioned under the sponsorship of the mentioned organization:

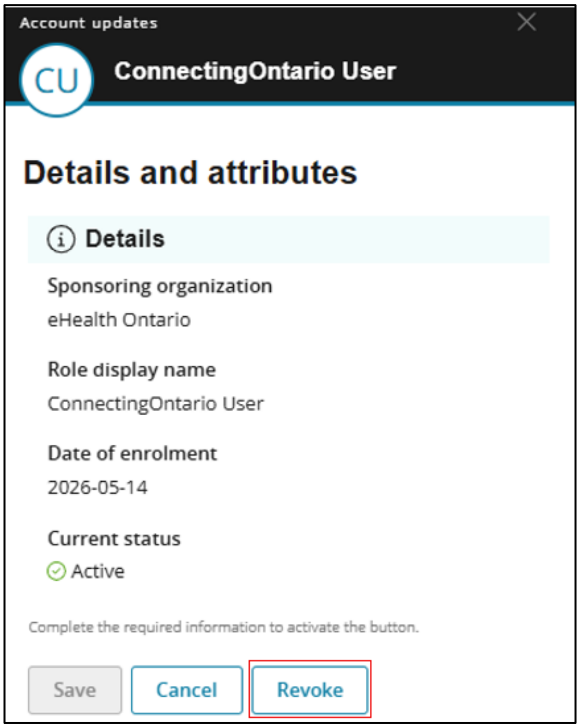


Figure 49 - Press Revoke

Once you press this button, ONE® ID will ask the LRA to confirm if they would like to proceed with the revocation. Simply press **Revoke** again to proceed. The user enrolment is now revoked.

NOTE: You will only be allowed to revoke services under the sponsorship of the organization for which you are LRA for. IE; if you are an LRA for 'Doeh Memorial Hospital' and not for 'James Regional Hospital' you can only revoke a user for services under the sponsorship of 'Doeh Memorial Hospital' and not 'James Regional Hospital'.

Appendix L – How to Register/Enroll a New User

Local Registration Authorities (LRAs) can view the profiles of end users sponsored by their organization. They can also register new users, update profile details, including resetting passwords, changing personal information, and adding or revoking services. This guide provides step-by-step instructions for registering and enrolling new users in ONE® ID.

To register a user on ONE® ID, first begin with the steps in [Appendix G - *How to View a User Account*](). After the step of pressing **Search,** simply select '**Create Account'** rather than selecting an existing profile:

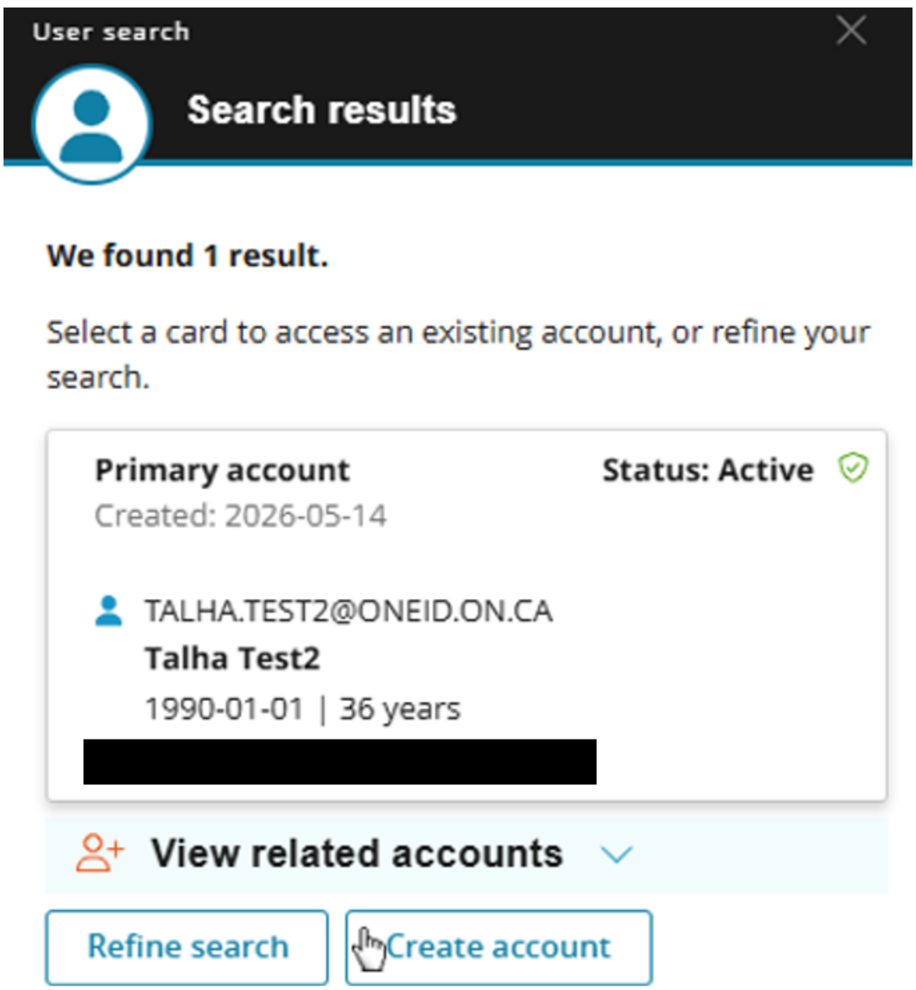


Figure 50 – Create New Account

Now input the user's personal information, including legal first/last name, preferred first/last name, date of birth and preferred language:

Figure 51 - Create User Profile

Next, select the regulatory college the user is a part of (if applicable) and input their license number. The system should inform you that the license has been verified against our system. If the license number cannot be verified, please contact the Ontario Health Service Desk at 1-866-250-1554 or OH-servicedesk@ontariohealth.ca to get this detail amended.

If the user is not part of a regulatory college, skip this step and select 'create user profile':

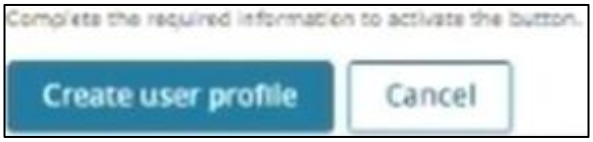


Figure 52 - Create user profile button

Next you will need to validate the user's identity using identity documentation. Please select the organization the client is working with.

- If your organization is under the ONE® ID Registering Organization model, you have the option to select '**I checked the Organization's ID Records**' or any of the below options listed in the next bullet. Select **Continue** once you are satisfied with your selection:

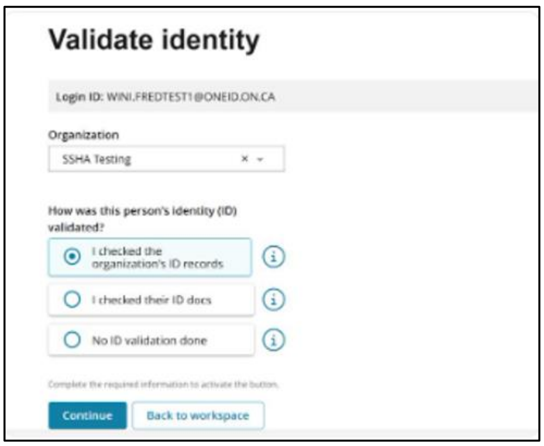


Figure 53 - Validate Identity (Registered Organization)

- If your organization is not under the ONE® ID Registering Organization Model, you will not have the above option, rather you can select between '**I checked their ID docs**', and '**No ID validation done**' and select **Continue**.
    - Selecting '**No ID validation done**' is not recommended as the user will not be able to be enrolled for any services leveraging PHI until ID validation is complete. If you do select this option, refer to subsection *Adding/Changing a User's Identity Documents* to add identity documents to user's profile after their registration is completed

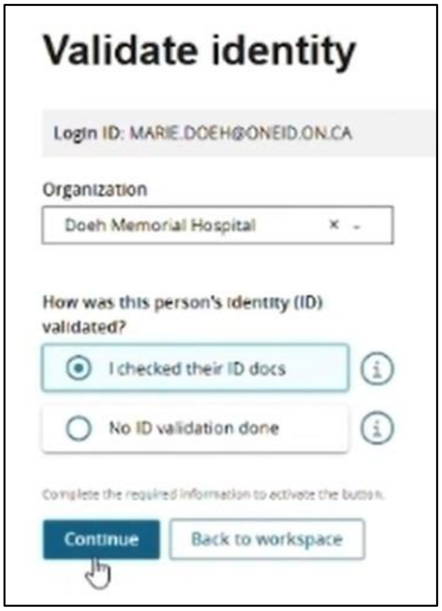


Figure 54 - Validate Identity (Non-Registered Organization)

Now, select how you know the user and select the primary ID documents (and secondary documents, if applicable) you wish to validate, then select **Save and continue** once you have input the required information:

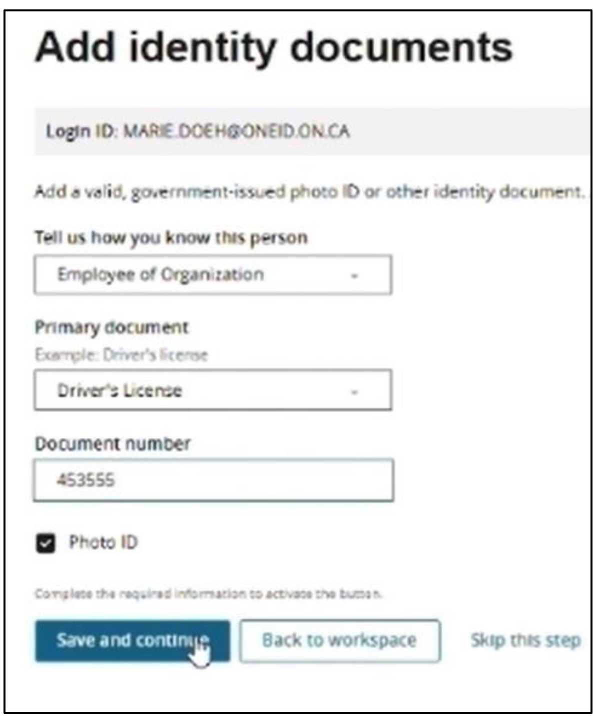


Figure 55 - Picking ID to add

For a list of all acceptable primary and secondary identity documentation, please refer to Appendix A.

Now you must configure the client's security information, including email, contact phone number and service desk questions. It is also highly recommended for the user to configure a mobile device in the optional text box as well, but this is optional.

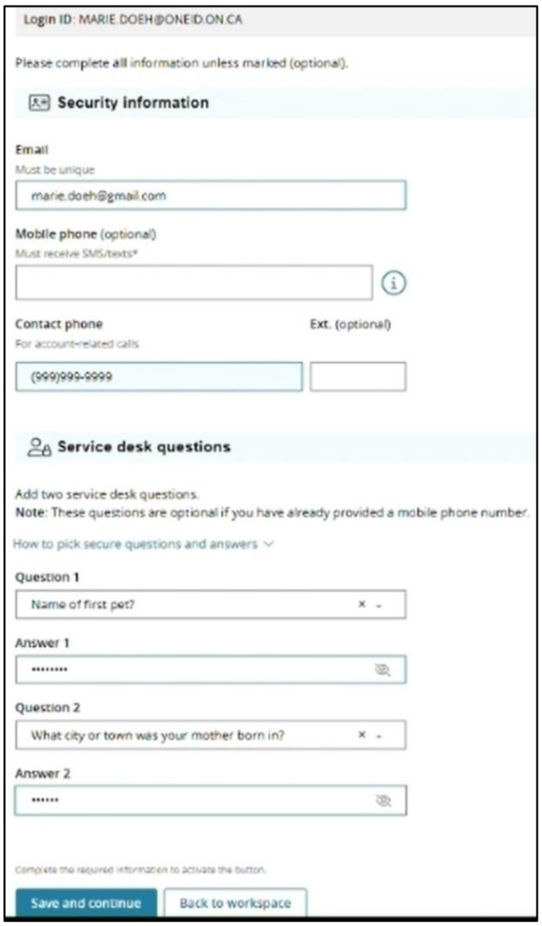


Figure 56 - Filling out Security Info

Once you have input the requisite information, press **Save and Continue**.

Enrolling a New User for a Service

The next screen will give you the option to enroll a user for a service before completing their registration. To do, select **Add a service**. In the sponsoring organization, enter the organization they would be provisioned under and in service or role select the desired service. Press **Add** once finalized:

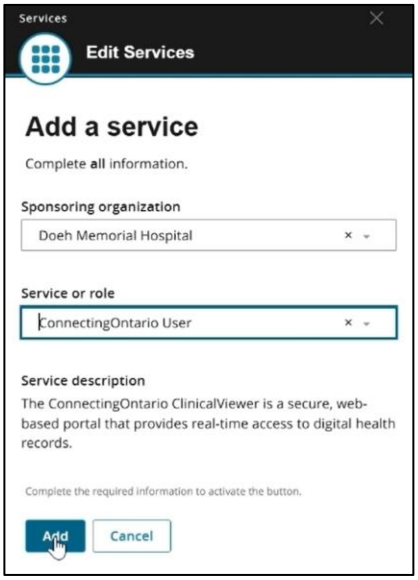


Figure 57 - Add a Service

When you have completed the provisioning, press '**Complete Registration**'. A registration email will now be sent to the user with their new ONE® ID Login ID and instructions to self complete their account. Have the user follow the prompts provided in the email link to self complete their account. If the user requires assistance with this step, please refer to them the [ONE® ID Registrant Reference Guide] for further guidance on self completion steps.

Appendix M – Panorama Guided Workflow

This appendix will briefly cover sponsorship, enrolment and registration of users to the Panorama Guided Workflow (PGW) service. You can find additional resources for Panorama Guided Workflow at the Public Health Ontario Website

NOTE: This section pertains to the Panorama Guided Workflow Service in particular. If you are looking for guidance regarding Panorama Service, please go to Appendix D

Sponsorship

The following organizational units are currently the only sponsors for the Panorama Guided Workflow (PGW) service:

- Non-Public Health Unit (Non-PHU) organizations (e.g., pharmacies, long-term care homes, retirements homes, hospitals, primary care physicians)
- Ministry of Health and Long-Term Care – Health Services Cluster

Registration

For users that do not already have a ONE ID account, validation of identity information is a prerequisite for account creation and enrolment of users into the PGW service. The identity validation method can vary depending on your organization. Refer to Identity Validation for detailed options.

Enrolment

To add the PGW service and applicable role, follow the enrolment steps summarized below.

NOTE*:* A user cannot be enrolled in both PGW and Panorama services under different sponsoring organizations using the same ONE ID account. If access to PGW and Panorama is required under separate sponsoring organizations, a subsidiary ONE ID account must be created to access the services under the different sponsoring organizations.

- From the ONE ID home page, select **My workspace (LRA)**, **Create / modify ONE ID account**
- In the Login tab, type in full or partial ONE ID account to search, press Search button

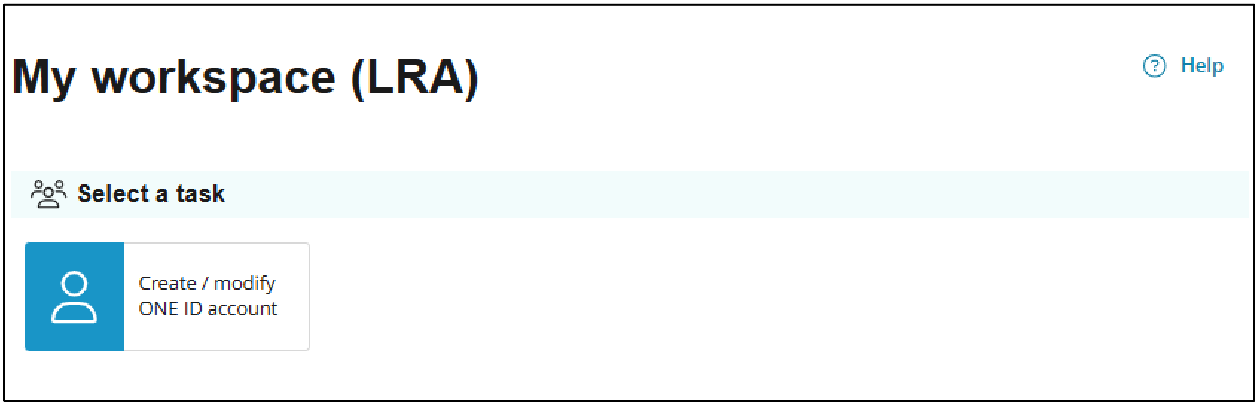


Figure 58 - My Workspace

- Click on the profile that appears in the search result to proceed with modification:

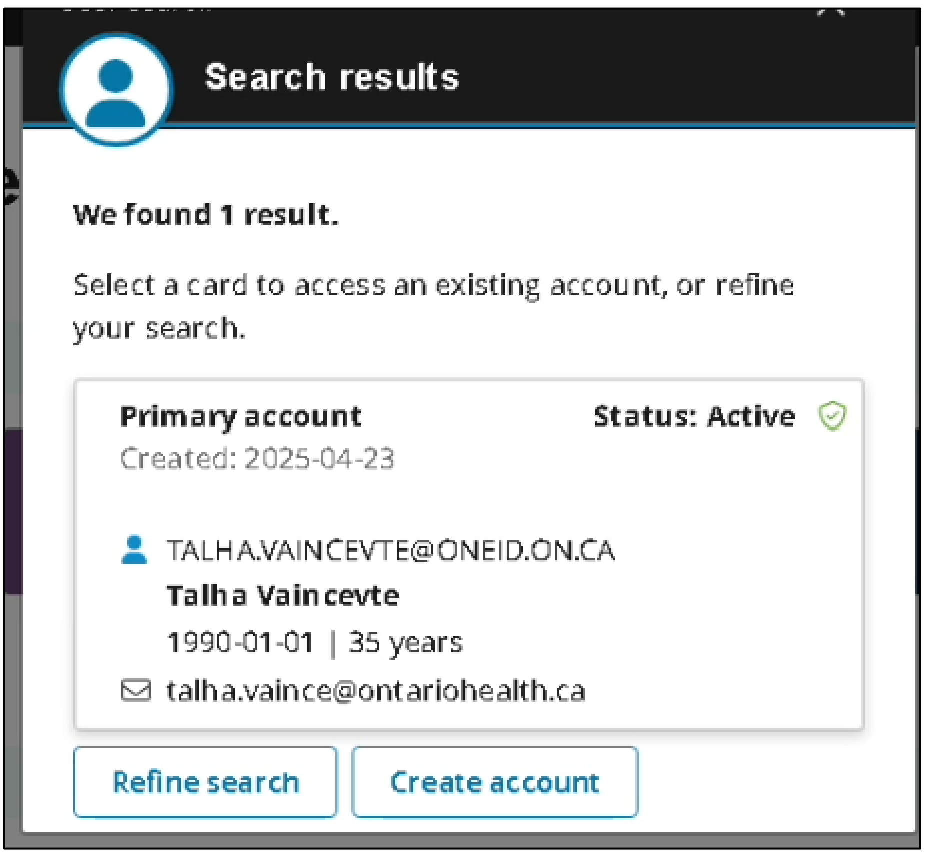


Figure 59 - Search by LOGIN ID Results

- The next page will ask upon whose authority you are requesting to change the account, select '**Mysel**f' as account requester, and press continue. You will now be at the user's profile screen: Select the **Services** tab and click **Add a service**

- Select **Sponsoring organization** (type to search) and **Service or role** (select Panorama Guided Workflow)
- Enter the additional attributes as specified in the sponsorship request from the authorized sponsor directly in the required fields in the system
    - **Organization:** The name of the organization in ONE ID (e.g., ABC Pharmacy – Store 1234 – 123456).
    - **Role(s):** Only one (1) of the following PGW roles (Each applicant may only be associated with one (1) role):
        - Guided Flow – All (Edit & View)
        - Guided Flow – All (View Only)
        - Guided Flow – Immunization (Edit & View)
        - Guided Flow – Inventory (Edit & View)
    - **Service Delivery Location(s):** Usually the name of the organization, appended with "– SDL" (e.g., ABC Pharmacy – Store 1234 – 123456 – SDL). If there is more than one, list them all separated by a comma.

NOTE: The Role indicated on the attribute screen is used by the administrator to create the user account directly in the Panorama application.

- Press **Add** when you are satisfied with your inputs
- The user is now successfully enrolled to PGW

Panorama Guided Workflow Administrator

When a user is provisioned with the Panorama Guided Workflow role or their enrolment is modified in the Ontario Health ONE ID Online system, the Panorama Guided Workflow Administrator will receive a system generated email notification with the enrolment information. This information is used by the authorized Panorama Guided Workflow Administrator to create user accounts and configure role-based access permissions within the Panorama Guided Workflow application itself.

- If the registrant is a new PGW user and is being provisioned for any PGW service roles, the enrolment attributes fields (i.e. organization, role, and service delivery location) must be completed.
- If a registrant already has a Panorama Guided Workflow service role in their profile and the existing role is being modified by the administrator in the PGW application, the enrolment attributes will not be requested again in the ONE ID Online system (Ie; the

LRA should make *no* changes to the user's ONE ID Account). If you would like such a change to be made, please contact your PGW Administrator.

  - Alternatively, you can complete the required service request forms available online at the Public Health Ontario website to request a PGW role change or link an existing PGW user to a provider, by emailing these forms to the Ontario Health Service Desk.

- An email notification will be generated for the following Panorama Guided Workflow service role modifications:
  - Panorama Guided Workflow service role added to a new or existing Registrant.
  - Panorama Guided Workflow service role is deleted, and a new role is added to an existing registrant.
  - Panorama Guided Workflow enrolment is revoked.

Enrolling a User in Panorama Guided Workflow with Training Role

If a user has been authorized to access the PGW Training Environment, a subsidiary account will have to be created for the user. The registration information from the parent ONE ID account (i.e. personal information) will be automatically copied over to create the subsidiary account, however the LRA still needs to confirm the client's preferred name and login ID details. In particular, Login ID must be created for the PGW training ONE ID subsidiary account in the format of FirstName.LastNameTR@oneid.on.ca, so it can be easily identified.

Refer to sub-section Making a Subsidiary Account for Panorama Training or Panorama Guided Workflow Training. Alternatively, you can also send an email request to Ontario Health Registration Agents to Create the Subsidiary Account in your stead.

Requesting Panorama Guided Workflow Access for Multiple Organizations

PGW is a single sponsor enrolment; in other words, only one PGW enrolment can be associated with a user's ONE ID account regardless of the sponsoring organization. Once this enrolment has been added to a registrant's profile, it will not be available for selection again in their ONEID profile. To add a PGW enrolment under the sponsorship of an additional organization, a subsidiary account will need to be made. Existing ONE ID user ID format of **firstname.lastname@oneid.on.ca** from the parent account will be replicated for the subsidiary account; however, with a number added to the prefix to create a new unique user ID.

As an example:

- if the user operates at two pharmacies, with the first pharmacy being the primary location of operation, the user's parent ONE ID account will contain the PGW enrolment sponsored by the first pharmacy while the subsidiary account will contain the second enrolment sponsored by the second.
- The administrator will configure each of the two user accounts to have access to the data for both pharmacies respectively so that the user cannot view both sets of data at the same time in any location, in other words the user cannot view first pharmacy's data when they are located at the second pharmacy and vice versa.
- The user will have to manage multiple accounts and will have to login to each separately.

NOTE: Primary ONE ID account and subsidiary ONE ID accounts share contact information, so if user knows their subsidiary account login ID that was created, then they can enter that, click forgot password, and they can reset it themselves

If the user requires PGW access at multiple locations like the above example, refer to the steps contained in the subsection Making a Subsidiary Account for Additional Panorama/PGW Locations. Alternatively, you can also send an email request to Ontario Health Registration Agents to Create the Subsidiary Account in your stead