

RSA Console User Guide for ONE ID Local Registration Authorities

Ontario Health | 2024-09-05



**Ontario
Health**

Table of Contents

About this Document	1
Purpose	1
Scope.....	1
References.....	1
RSA Console.....	1
Logging In	2
RSA Home Page	5
Home	5
Dashboard	6
Identity.....	6
Authentication.....	6
Access, Reporting & Help	6
Assigning Tokens.....	7
Enabling/Disabling Tokens	10
Replacing a Token	12
Reusing a Token.....	15
Resetting PIN	16
Support	18

About this Document

Purpose

The purpose of this guide is to describe the detailed procedures of the token management functions that a Local Registration Authority (LRA) can perform in the RSA Console. Tokens require provisioning in the RSA console after the user's ONE® ID account is enrolled. The RSA Console also enables LRAs them to replace and activate user tokens as well as reset PINs without intervention of the Ontario Health Service Centre.

Scope

This document contains procedures for the following:

- [Assigning Tokens](#)
- [Enabling/Disabling tokens](#)
- [Resetting Token PINs](#)
- [Replacing Tokens](#)

References

For detailed procedures on how to enroll users in ONE ID, please refer to the [ONE ID Local Registration Authority User Guide](#) located on the [ONE ID Registration Community site](#).

RSA Console

The RSA console is used to support token management for ONE ID enrolments that require a token. Please note that some disabled options appear and can be disregarded as they are not currently available through Ontario Health.

Logging In

To log in, navigate to <https://prds.ontariohealth.ca/>

- 1) Enter your ONE ID Login ID and passcode (PIN immediately followed by six-digit token code displayed on RSA Token)



Figure 1 - MFA

- 2) Click **Log In**
- 3) Enter your ONE ID Login ID and password:

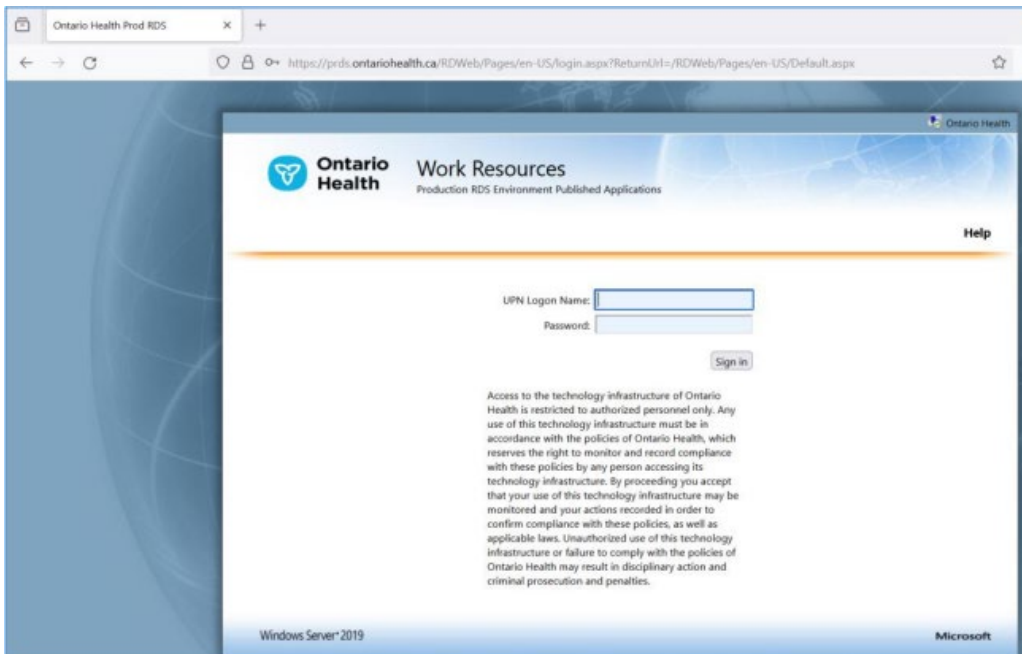


Figure 2 - RDS Login Screen

- 4) Click **Sign In**

5) Click **RSA Web Security Console**:

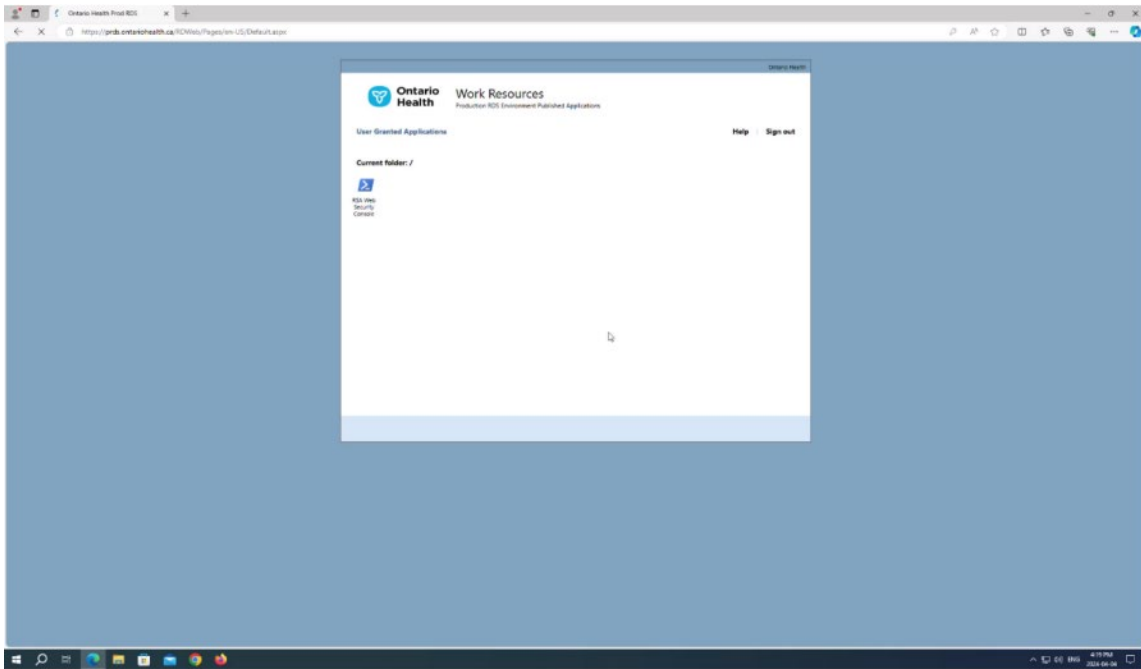


Figure 3 - RDS 2019 Environment

6) Upon clicking, the Remote Desktop Protocol File for the Console will be downloaded to your computer. Open this file to launch the application.

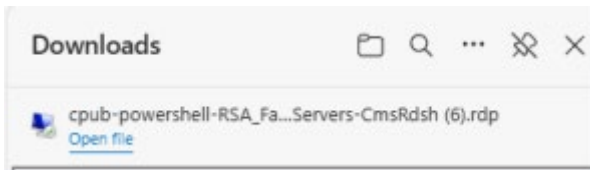


Figure 4 - RDP File

7) Upon launching, you will be asked to provide your ONE Login and Password again. This will typically pop up once per a day's session. Click **OK**

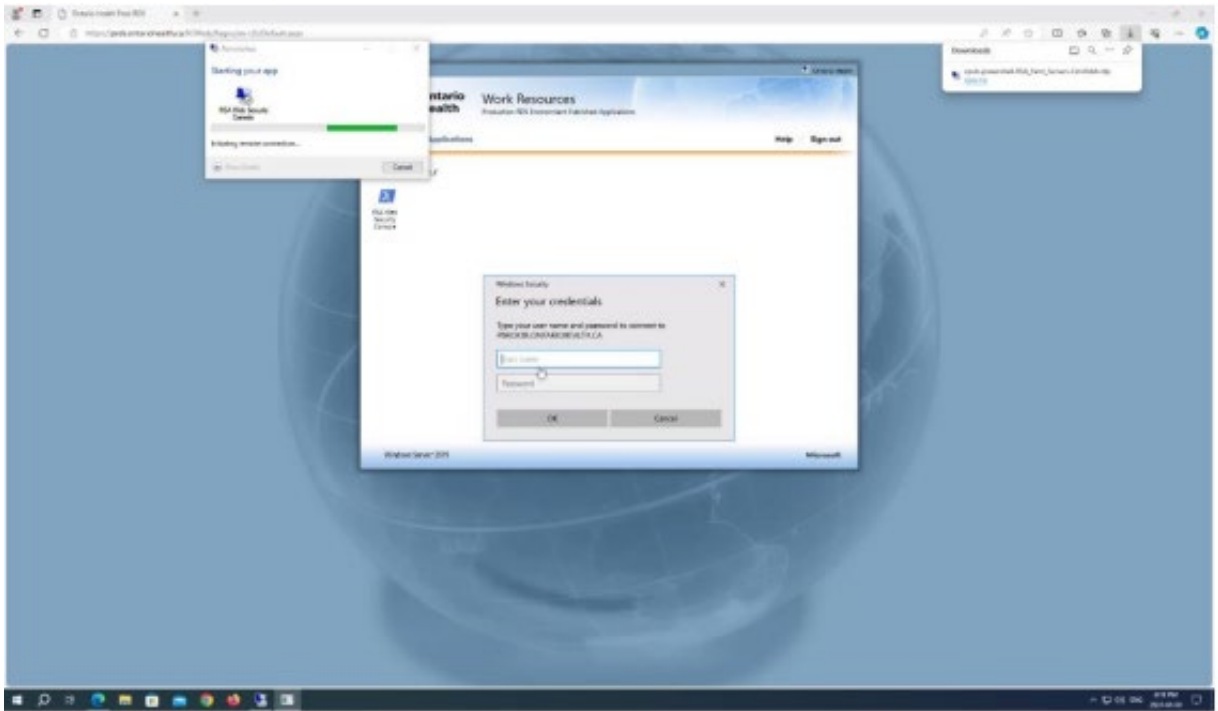


Figure 5 - RDP File Login

8) On the secure logon screen, enter your ONE ID Login ID.

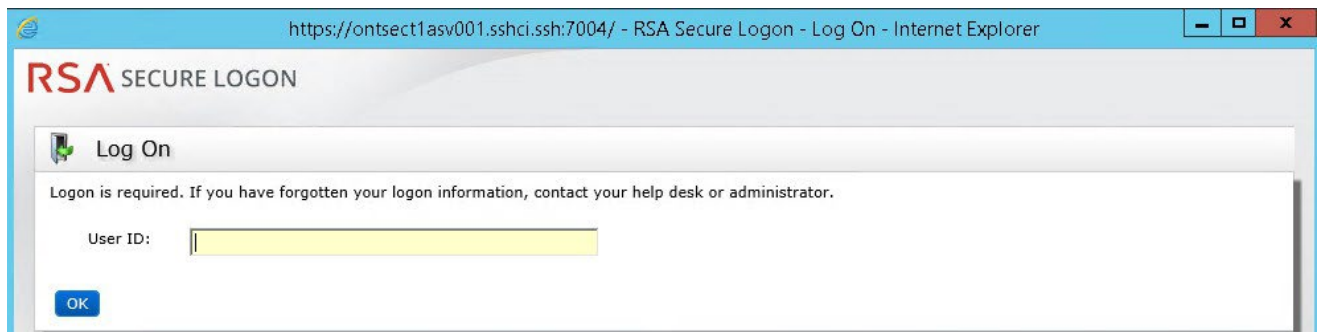


Figure 6 - RSA Logon Screen

9) Click **OK**

- 10) Choose whether you would prefer to enter your ONE ID password (Password) or ONE ID token code+pin (Passcode) and click **Log On**:

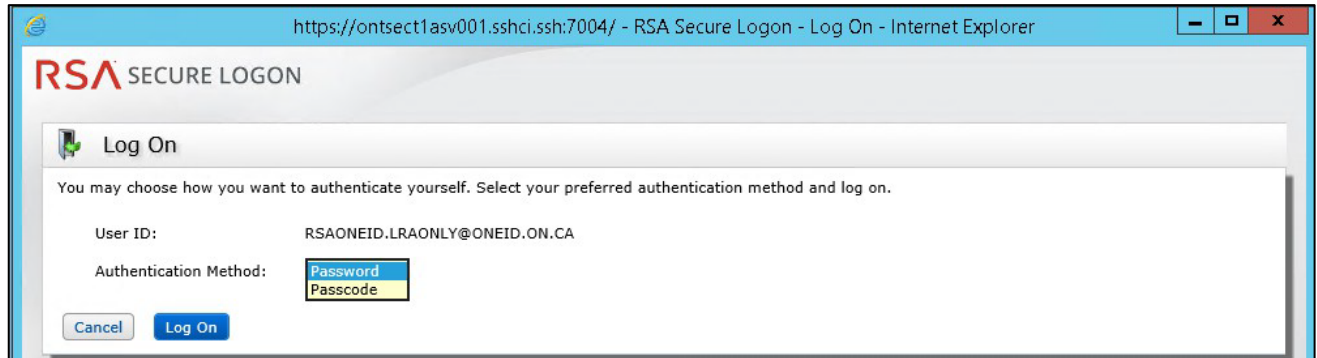


Figure 7 – RSA Authentication Option

- 11) Enter your ONE ID Password or Passcode (PIN immediately followed by six-digit token code) and click **Log On**.
- 12) Upon successful Authentication, the **Home Menu** opens.

RSA Home Page

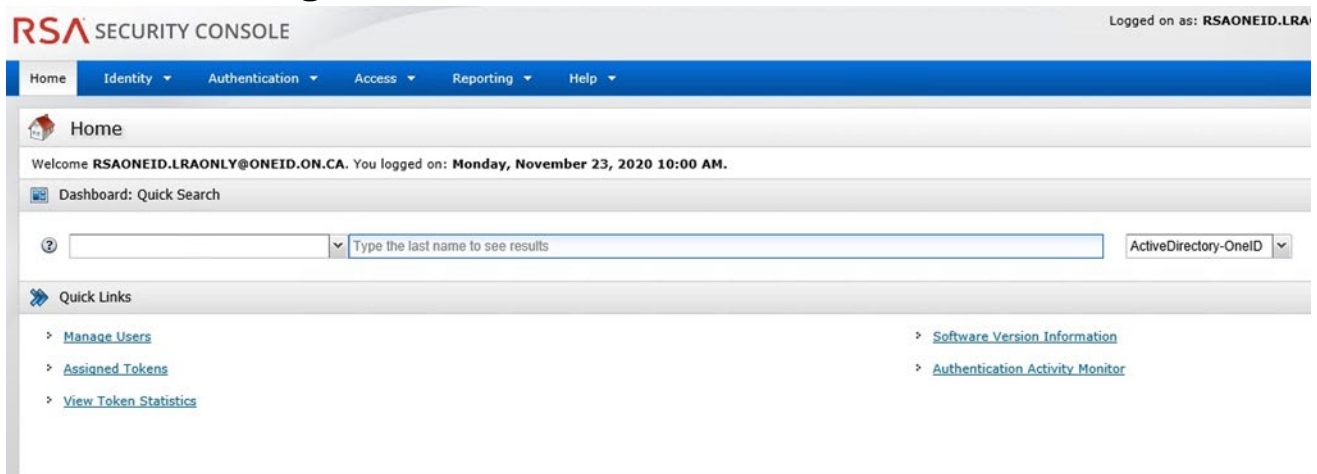


Figure 8 - RSA Quick Search

Home

If at any time you wish to return to the Home Page, click Home.

Dashboard

The Dashboard allows you to search for a user or a token serial number and complete all activities you may need to action for your users. LRAs would use the dashboard for all their token activities.

Identity

The Identity Menu allows you to search for a user with expanded search criteria.

Authentication

Allows you to search for a token with expanded search criteria.

Access, Reporting & Help

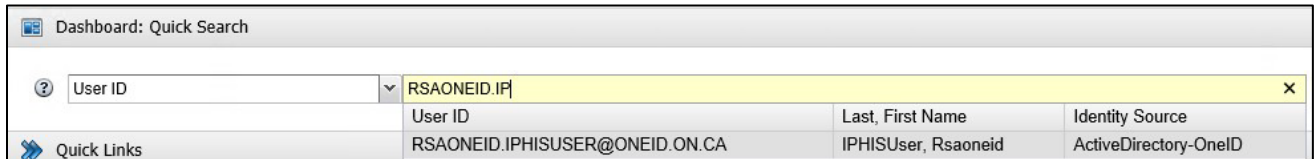
These menu options are not available for selection. For any help required with the RSA Console, please contact the Ontario Health Digital Service Desk.

Assigning Tokens

Prior to assigning a token to a new or existing user, the user's account must be enrolled for a service that requires a token. If the user does not have an enrolment that requires a token or their enrolment or account is in suspended or revoked status, their account will not be displayed in RSA.

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.

- 1) From the **Home Page, Dashboard: Quick Search** section, select **User ID** from the drop-down menu.
- 2) Enter the **ONE ID Login ID** of the account to assign a token.
- 3) RSA will return any matching results; click on the account you wish to assign a token:



Dashboard: Quick Search			
User ID	Last, First Name	Identity Source	
RSAONEID.IPHISUSER@ONEID.ON.CA	IPHISUser, Rsaoneid	ActiveDirectory-OneID	

Figure 9 - Quick Search

- 4) You are directed to the Dashboard for the account selected, navigate to the **Assigned SecurID Tokens** field:

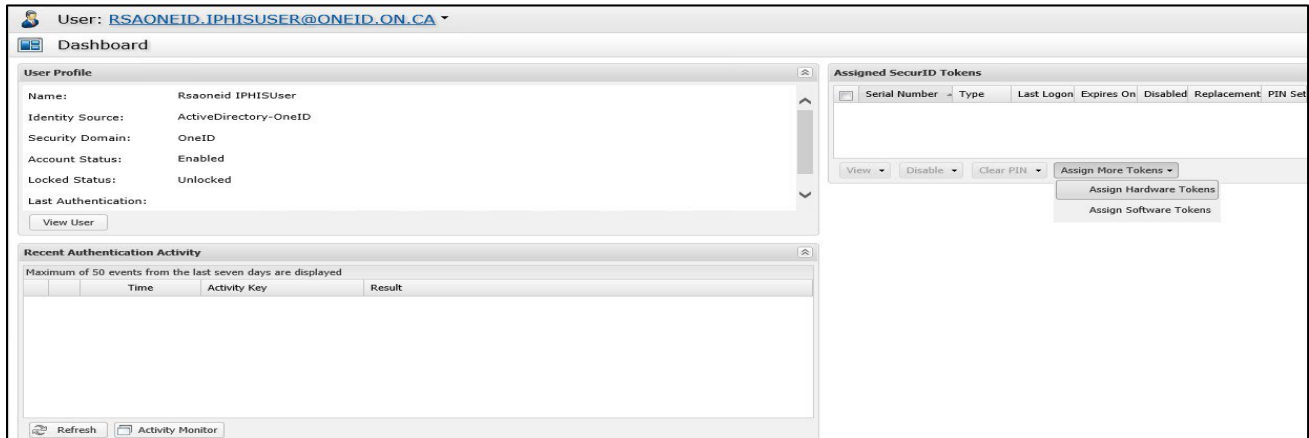


Figure 10 - User Dashboard

- 5) Select **Assign More Tokens**, then **Assign Hardware Tokens**
 - a. **Note:** that **Assign Software Tokens** is not available to use)
- 6) Enter the serial number of the token you wish to assign in the Select Tokens pop-up window and Click Search:
 - a. **Note:** Do not select a token shown in the list presented unless it is the token you have on hand.
 - b. **Note:** If the token serial number is already assigned to another user, the search will not return any results.

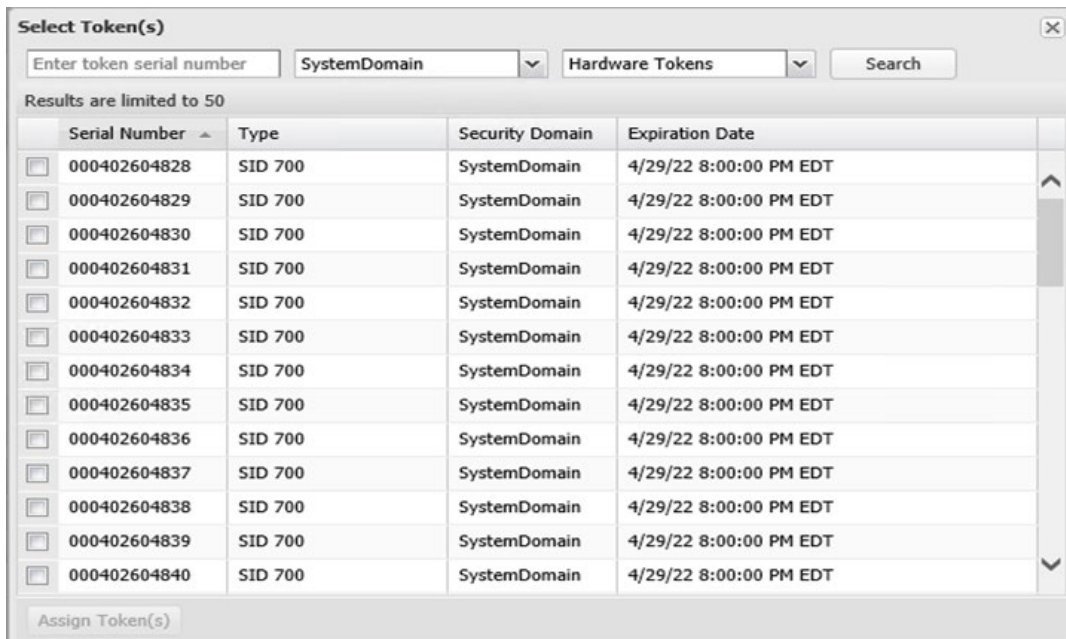


Figure 11 – Searching for Token

7) Select the **checkbox** next to the token serial number and click **Assign Token(s)**:

Select Token(s)

402605017 SystemDomain Hardware Tokens Search

Results are limited to 50

	Serial Number ▲	Type	Security Domain	Expiration Date
<input checked="" type="checkbox"/>	000402605017	SID 700	OneID	4/29/22 8:00:00 PM EDT

Assign Token(s)

Figure 12 - Assign Token

8) You are directed back to the Dashboard with a display message that the token has been successfully assigned:

✓ Successfully assigned token(s) 000402605017 to RSAONEID.IPHISUSER@ONEID.ON.CA.

User Profile

Name: Rsaoneid IPHISUser
 Identity Source: ActiveDirectory-OneID
 Security Domain: OneID
 Account Status: Enabled
 Locked Status: Unlocked

Assigned SecurID Tokens

<input type="checkbox"/>	Serial Number ▲	Type	Last Logon	Expires On	Disabled	Replacement	PIN Set	New PIN
<input checked="" type="checkbox"/>	000402605017	SID 700		4/29/2...				✓

View Disable Clear PIN Assign More Tokens

Figure 13 - Assignment Confirmation

Enabling/Disabling Tokens

Token activation is no longer available through ONE ID. To enable (activate) or disable a token, the token must be assigned to a ONE ID account with an enrolment that is neither suspended nor revoked.

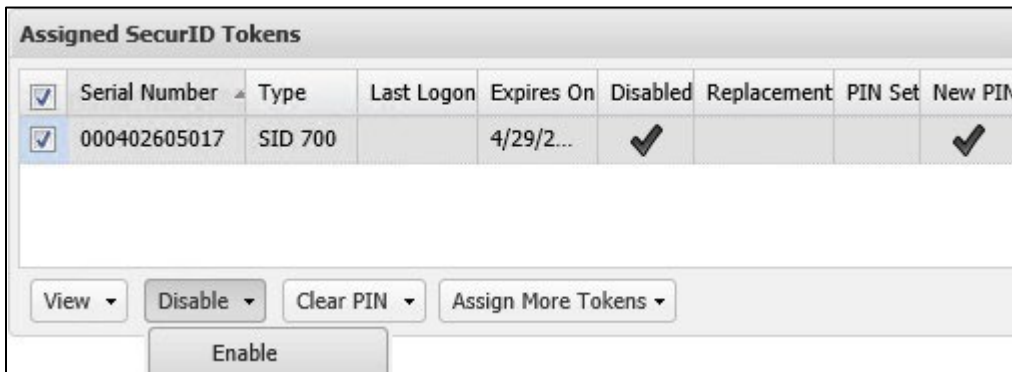
- 1) From the **Home Page, Dashboard: Quick Search** section, select User ID from the drop-down menu.
- 2) Enter the **ONE ID Login ID** of the account to activate a token.
- 3) RSA will return any matching results, click on the account you wish to enable/disable a token.



User ID	Last, First Name	Identity Source
RSAONEID.IPHISUSER@ONEID.ON.CA	IPHISUser, Rsaoneid	ActiveDirectory-OneID

Figure 14 - Quick Search

- 4) You are directed to the Dashboard for the account selected, navigate to the Assigned SecurID Tokens field.
- 5) Click the Checkbox next to the token serial number you wish to enable/disable.
- 6) Click **Disable/Enable**.



Serial Number	Type	Last Logon	Expires On	Disabled	Replacement	PIN Set	New PIN
<input checked="" type="checkbox"/> 000402605017	SID 700		4/29/2...	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>

View ▾ Disable ▾ Clear PIN ▾ Assign More Tokens ▾

Enable

Figure 15 - Click Enable

-
- 7) A pop-up window will be displayed requesting you to confirm your action, click Disable/Enable Token(s).

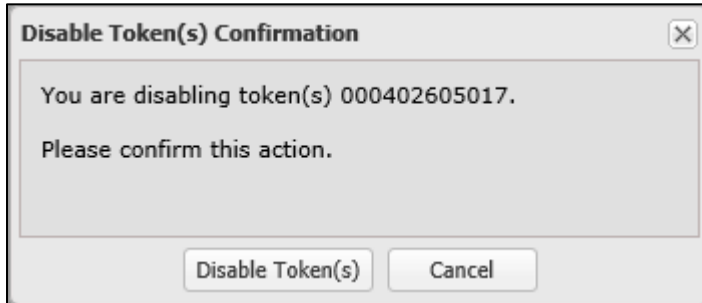


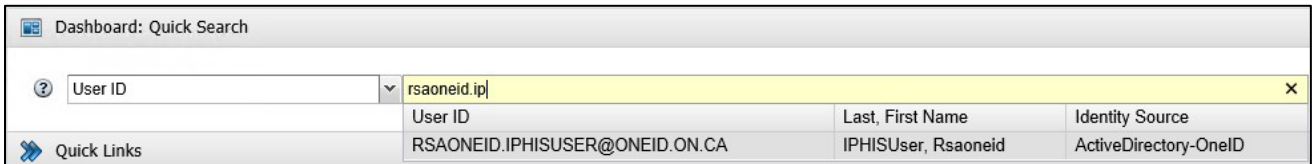
Figure 16 - Disable Confirmation

- 8) You are directed back to the Dashboard with a display message that the token has been successfully enabled or disabled.

Replacing a Token

A token can be replaced for a user that requires a new token (i.e. misplaced or faulty token).

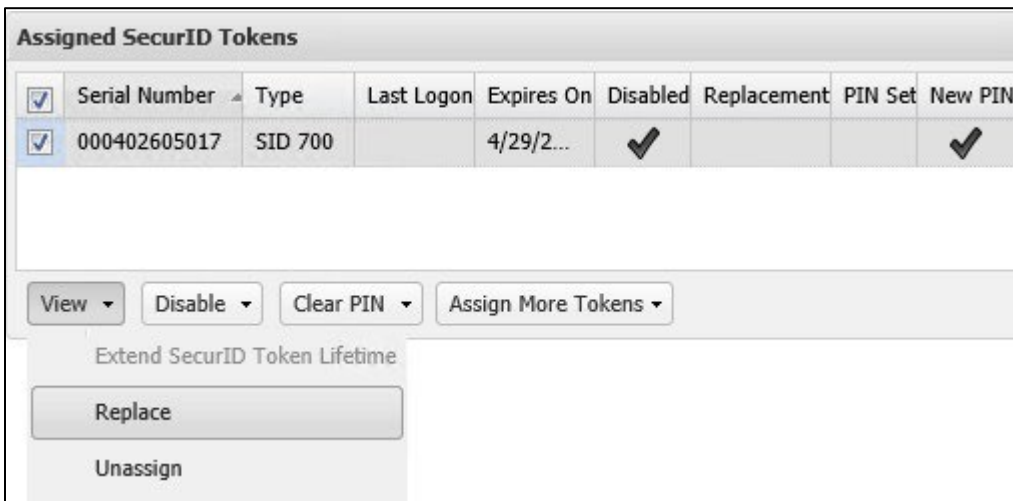
- 1) From the **Home Page, Dashboard: Quick Search** section, enter the user **ONE ID Login ID** and select the matching result returned:



Quick Links	User ID	Last, First Name	Identity Source
	RSAONEID.IPHISUSER@ONEID.ON.CA	IPHISUser, Rsaoneid	ActiveDirectory-OneID

Figure 17 - Quick Search

- 2) From the user **Dashboard**, select the **token** you wish to replace in **the Assigned SecurID Tokens** field.
- 3) Under the **View** menu, select **Replace**:



<input checked="" type="checkbox"/>	Serial Number	Type	Last Logon	Expires On	Disabled	Replacement	PIN Set	New PIN
<input checked="" type="checkbox"/>	000402605017	SID 700		4/29/2...	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>

View ▾ Disable ▾ Clear PIN ▾ Assign More Tokens ▾

Extend SecurID Token Lifetime

Replace

Unassign

Figure 18 - Click Replace

4) The **Select a Replacement Token** pop-up window appears:

Results are limited to 50

Serial Number	Type	Security Domain	Expiration Date
000402604828	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604829	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604830	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604831	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604832	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604833	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604834	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604835	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604836	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604837	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604838	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604839	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT
000402604840	SID 700	SystemDomain	4/29/22 8:00:00 PM EDT

Replace Token Copy the SecurID PIN to the replacement token

Figure 19 - Token Search

- 5) Enter in the **serial number** of the token you have available to assign as a replacement.
- 6) Click **Search**
 - a. **Note:** Do not select a token shown in the list presented unless it is the token you have on hand.
 - b. **Note:** If the token serial number is already assigned to another user, it will not return any results
- 7) Select the **Checkbox** of the token serial number:

Select a Replacement Token
✕

▼

▼

Results are limited to 50

Serial Number	Type	Security Domain	Expiration Date
000413469753	SID 700	OneID	11/29/23 7:00:00 PM EST

Copy the SecurID PIN to the replacement token

Figure 20 - Select the replacement token

- 8) This action is defaulted to copy the PIN of the previous token to the replacement token. Please confirm with the user if they need to set a new PIN and uncheck it if required. Click **Replace Token**.
- 9) You are directed back to the Dashboard with a display message that the token has been successfully replaced and you will see both tokens listed under the **Assigned SecurID Tokens** field.

Reusing a Token

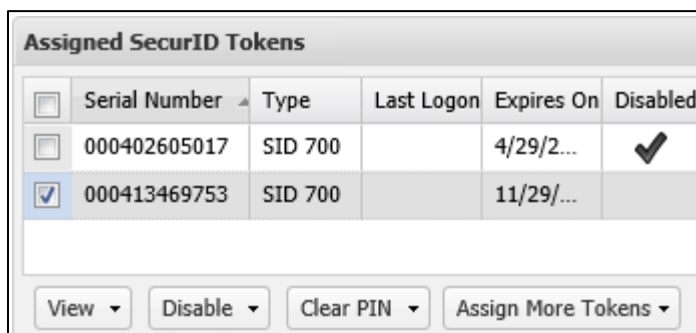
When an enrolment is revoked, ONE ID checks if the user account has any other enrolments that require a token. If a token is no longer required it will be automatically unassigned from the account within twenty four hours. The account will also no longer be displayed in RSA until it is enrolled for a service that requires use of a token again.

If a token needs to be reused immediately, please contact the Ontario Health Digital Service Desk.

Resetting PIN

You can reset a user's PIN if they have forgotten it. **Before proceeding, please ensure to verify their identity in ONE ID via challenge questions or reviewing their employee ID.** Alternatively you can direct the user to the Ontario Health Digital Service Desk.

- 1) From the user Dashboard page under the **Assigned SecurID Tokens** section, select the token record that requires a PIN reset and click on **Clear PIN**:



Assigned SecurID Tokens					
<input type="checkbox"/>	Serial Number	Type	Last Logon	Expires On	Disabled
<input type="checkbox"/>	000402605017	SID 700		4/29/2...	✓
<input checked="" type="checkbox"/>	000413469753	SID 700		11/29/...	

View ▾ Disable ▾ Clear PIN ▾ Assign More Tokens ▾

Figure 21 - PIN Reset

- 2) A pop-up window will be displayed requesting you to confirm your action, click Clear PIN(s):

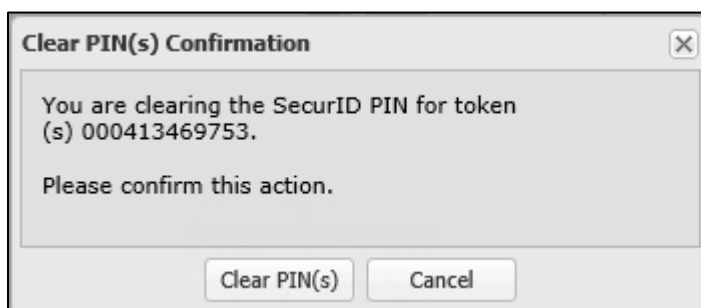


Figure 22 - PIN Reset Confirmation

-
- 3) You are directed back to the Dashboard with a display message that the PIN has been successfully cleared.
 - a. **Note:** For a user to set a new PIN, advise them to login as per their standard instructions and leave the PIN section blank, the system will then prompt them to create a new PIN. If they



Support

Please contact the Ontario Health Digital Service Desk for any support requirements in the use of the RSA Console or for users requiring token activation.

Tel: 1-866-250-1554 (24/7 support)

Email: OH-DS_Servicedesk@ontariohealth.ca