00 Introduction to COVax$_{ON}$ and User Setup

Ontario

Introduction to COVax$_{ON}$ and User Setup

Introduces the COVax$_{ON}$ system and describes how a user is set up in COVax$_{ON}$.

Profiles

COVax user

Core Tasks

Below are tasks you may need to perform. **Click the relevant link**:

#	Section	Description
1.	Introduction to COVax$_{ON}$	Summary of the COVax$_{ON}$ solution and its purpose
2.	COVax$_{ON}$ Technology: Authorized Organizations and Vaccination Events	Description of authorized organizations (AOs) and vaccination events (VEs) within COVax$_{ON}$
3.	COVax$_{ON}$ User Access	Details on COVax$_{ON}$ user profile types and access levels
4.	COVax$_{ON}$ Account Setup	Steps to set up user accounts using the Salesforce two-factor authentication application: • Section 4A – Accessing the Salesforce Support Email • Section 4B – Setting Up Two-Factor Authentication • Section 4C – Changing Your Password
5.	Reset Your Password to Login to COVax$_{ON}$	Steps to reset your password if you forget your password
6.	Subsequent Logins to COVax$_{ON}$	Steps to properly login to COVax$_{ON}$ after a user's account has initially been setup
7.	Accessing COVaxON Outside of Canada	Restricting User Login to COVaxON outside of Canada
8.	Clearing Cache and Logging Out of COVax$_{ON}$	Steps to clear browser cache and properly logout of COVax$_{ON}$
9.	Hardware Requirements and Device Setup On-Site	Description of the hardware and devices required onsite to operate COVax$_{ON}$
10	Offline Solution if COVax$_{ON}$ is Unavailable or the Client Does Not Consent to Digital Data Collection	Summary of the paper process used to document a client's vaccination if they are unable to be recorded in COVax$_{ON}$

1. Introduction to COVax$_{ON}$

COVax$_{ON}$ is a secure cloud-based solution which supports COVID-19 vaccine clinics and authorized organizations (AOs). The system is real-time, anywhere, anytime if the user has an authorized account and a device with browser and internet connectivity.

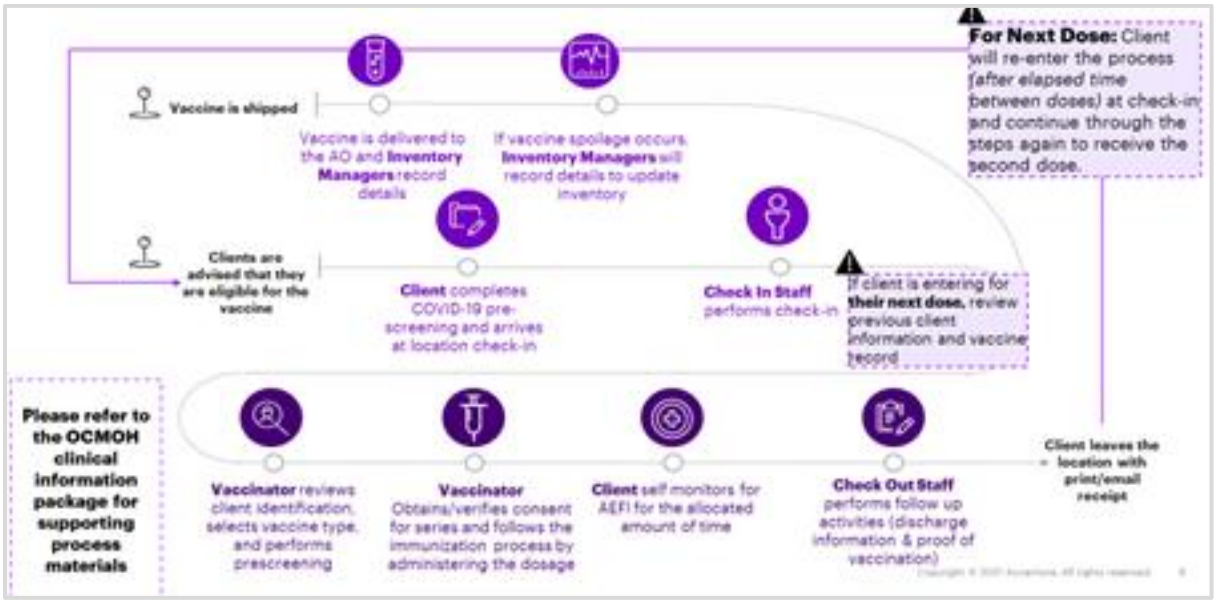
COVAX$_{ON}$ provides standard processes, workflows, and a common set of digital tools (e.g., scheduling, client management, recording point-of-service and out of province doses, inventory management, receipt of vaccination, operational reporting) while ensuring standardized high-quality data for the provincial response to the fight against COVID-19.

The COVax$_{ON}$ system operates on customer relationship management (CRM) software called Salesforce.

COVax$_{ON}$ System Overview

- Tracks the receipt and usage of vaccine inventory
- Supports clinical operations by capturing client information, consent, and the documentation of administered vaccines.
- Provides technical and operational dashboards and reports to drive insight

The process depicted below demonstrates how COVax$_{ON}$ records vaccine-related information:



Additional Training Materials

To learn more about the various functions in COVax$_{ON}$, please refer to the relevant job aid outlined below. All job aids are located on the Ministry of Health (MOH) SharePoint site and are refreshed regularly based on the latest functionality release.

00 Introduction to COVax$_{ON}$ and User Setup

Ontario

#	Job Aid Title	Job Aid Description
00	**Introduction to COVax$_{ON}$ and User Setup** *(This document)*	Introduces the COVax$_{ON}$ system and describes how a user is set up on COVax$_{ON}$.
01	**Inventory**	Creating shipments, shipment line item(s), processing inventory for shipment line items (SLIs), allocating inventory to vaccination events (VEs), and reconciling inventory as part of ongoing operations.
02	**Create Vaccination Event**	Creating and managing a vaccination event (VE) associated to an authorized organization (AO), allowing for the tracking of inventory at a set location.
03	**Search, Create and Maintain Client Information**	1. Searching for a client record in COVax$_{ON}$. 2. Creating a new client record. 3. Maintaining client information: • Request data collection and communication consent • Update client information • Update sociodemographic information • Alerts • Clinical notes • Associate client to a VE (Individual client, bulk client upload) • Mark client as inactive • Merge duplicate client records
04	**New Immunization Record – Administered**	1. Documenting an immunization record via a guided flow. 2. Reviewing dose functionality to change the status of an immunization record. 3. Reviewing client immunization records. 4. Recording adverse event after immunization (AEFI).
05	**New Immunization Record – Historical**	Documenting historical doses for out of province (OOP), where a client may have received one/multiple doses outside of Ontario which need to be recorded in COVax$_{ON}$. Documenting non-Ontario stock (NOS), where a client may have received one/multiple doses from non-Ontario vaccine stock (e.g., federal stock used for correctional facilities, military groups, embassies) which need to be recorded in COVax$_{ON}$.
06	**Generate Receipt**	Generating and printing a PDF receipt, and/or receive an email certificate via a URL link to access the vaccine certificate via the COVID-19 patient portal.
07	**PCP Vaccinators and Clinic Coordinators**	• Documenting client consent for service • Recording an administered vaccine • Recording any inventory adjustments at the vaccination event (VE) level.
08	**Exemptions**	Documentation of a client COVID-19 exemption record in COVax$_{ON}$.
09	**Reporting and Dashboard**	Leveraging various reports and dashboards to aid in understanding of what each report/dashboard displays and how they can be used to gain useful insights for operational purposes. In addition, COVax$_{ON}$ navigation tips can be found in this job aid.

#	Job Aid Title	Job Aid Description
10	**Creating Tasks for Inter-AO Communications**	Sending and receiving communications for users between different authorized organizations (AOs) in COVax$_{ON}$.
11	**Bulk Client Upload**	Overview on how to prepare and upload new client data into COVax$_{ON}$ using the bulk client upload functionality.

2. COVax$_{ON}$ Terminology: Authorized Organizations and Vaccination Events

The terms *authorized organization* (AO) and *vaccination event* (VE) describe two distinct entity types. These terms are relevant to all COVax$_{ON}$ users.

- **Authorized organizations** (AOs) are the entities that are requested by the ministry (via signed agreements) to receive and manage vaccine stock. This is the umbrella organization where vaccine stock is received directly from the federal government or from other organizations. AOs also have accountability for COVax$_{ON}$ users.
    - An **Authorized Organization** field is listed on each user profile. Users can perform functions within COVax$_{ON}$ for the AO on their profile, and users are unable to change this AO manually.
- **Vaccination events** (VEs) are the physical locations where vaccine administration takes place. These *events* are created by an AO at a specific *venue* that uses the vaccine stock that the AO has received and is accountable for. AOs are responsible for the creation of vaccination events (VEs) in COVax$_{ON}$ to capture stock for which they are accountable.
    - Creation of VEs by AOs allows for pre-population of **vaccine event inventory** (VEI) for tracked inventory and clients in COVax$_{ON}$ ahead of the event to minimize manual data entry in COVax$_{ON}$. It also improves location efficiency and data quality during the VE, and reporting by the AO on specific VEs.
    - Creation of VEs by AOs also allows for the pre-population of **vaccine event product lot** (VEPL) for untracked inventory and clients in COVax$_{ON}$ ahead of the event to minimize data entry into COVax$_{ON}$. It also improves location efficiency and data quality during the VE, and reporting by the AO on specific VEs.
    - VEs are flexible and can be created to cover a time period for a client's dose. They can involve one or multiple lots of inventories.

The Relationship Between AO and VE

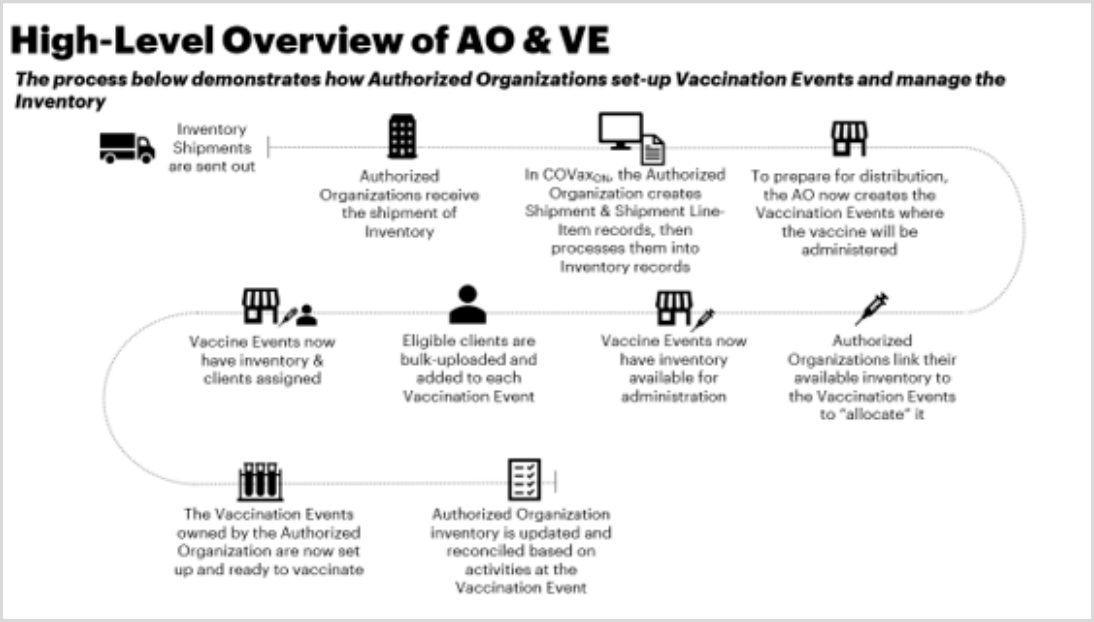
There is typically a one-to-many relationship between AOs and VEs. One AO owns and allocates inventory to multiple VEs. This relationship is seen when the AO is a public health unit (PHU), hospital, or clinic. For pharmacies, there is a one-to-one relationship between the AO and VE. Each pharmacy acts as their own AO and VE.

Examples of AOs to VE Structures

Authorized Organization (AO)	Public Health Unit	Specific Pharmacy Location	Public Health Unit	Hospital/Clinic
Vaccination Event (VE)	1 VE for each **primary care physician** location under the PHU AO	1 VE for each **pharmacy location** under the specific pharmacy location AO	1 VE for each **long-term care home, retirement home, nursing home** under the PHU AO	1 VE for each location at the **hospital** under the hospital AO
Example	Dr. Zanders Office within the Toronto Public Health PHU	Rexall Store #009 VE within the Rexall Store #009 AO	St. Albans Retirement Home VE within the Toronto Public Health PHU	Separate floors/ wings administering different products as the VE within Peterborough hospital

The logic surrounding what users can perform in COVax$_{ON}$ is based on the AO tagged to the user's profile and the AO's associated VEs:

- From the **Vaccination Events** tab, you can only see VEs associated to your AO
- Users can see shipments across AOs, but they cannot edit the shipment if it does not belong to their AO
- There are no restrictions to uploading clients or modifying client records based on VE on the client record
- Vaccinators can only administer doses to clients with inventory owned by the AO on their profile and allocated to the VE they are working at
- Vaccinators can only see inventory to administer to the client if it is associated to the same VE as the VE on the client's record
- Inventory managers can only create, manage, and transfer inventory associated to their user profile's AO
- Inventory managers and site super users can create and manage VEs associated to the same AO as their user profile's AO



3. COVax$_{ON}$ User Access

A. Creating User Accounts in COVax$_{ON}$

COVax$_{ON}$ user accounts can be created using two different methods. For both methods, the account must be created by Information Technology Services (ITS):

- **Bulk user upload**
    - Site leads populate the USERS_LOAD_TEMPLATE excel document (found on the MOH SharePoint site) and send it to the ITS team.
    - The bulk upload tool is used to upload the list of users provided by the site lead prior to the first date of vaccinations.
- **Ad hoc user creation**
    - If a new user was not included in the user bulk upload (described above) and requires COVax$_{ON}$ access, the designated site lead has the authority to request access for a new user(s) to be added to COVax$_{ON}$ by submitting a ticket to the ITS team.

B. User Account Permissions

All user accounts are associated with a *profile type* and an associated AO. A user's profile and AO assignment drives their ability to perform activities within COVax$_{ON}$. The chart below outlines the core six (6) user profiles in COVax$_{ON}$ and the associated activities that can be performed at each level.

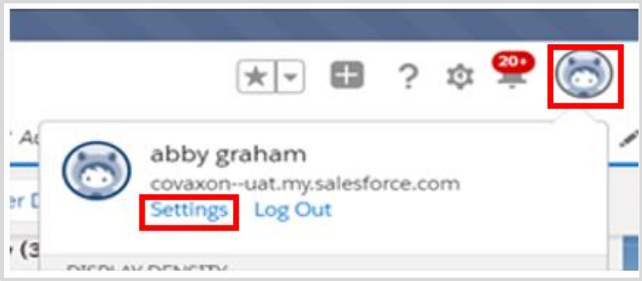
Core Profile Types with Defined Access to COVax$_{ON}$

User Profile	Functionality Profile Has Access To	Reports/Dashboards Profile Has Access To
COVax Inventory Manager	• Create shipments, inventory line items, and inventory records • Link inventory to VEs; create and manage VE records • Report inventory reconciliations at the AO and VE levels • Manage transfers and recalls	• Read and export Vaccine Inventory Report, Summary Client Dose Admin Reports
COVax Site Staff	• Search clients and update client information	• Read and export Vaccine Inventory Report, VE and AO Inventory Report, Summary Client Dose Admin Reports, and Clients with Highest Risk (28 Days) Report • View AO site Dashboard, AO Scheduling Dashboards, and the associated linked reports
COVax Vaccinator	• Search clients and update client information • Vaccinate clients • Review Dose admin records • Read-only access for VE records	• View AO Site Dashboard, AO Scheduling Dashboards, and the associated linked reports

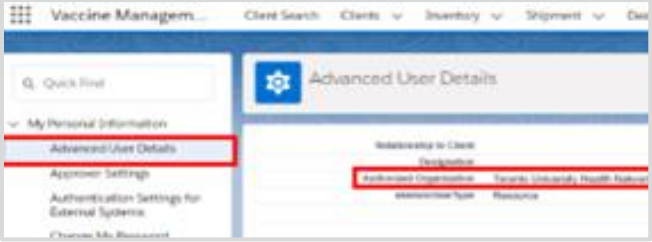
User Profile	Functionality Profile Has Access To	Reports/Dashboards Profile Has Access To
COVax Site Super User	• Inventory manager functionalities • Vaccinator functionalities • Mass data client upload • Review Dose admin records • Merge duplicate clients	• Read and export Vaccine Inventory Report, VE and AO Inventory Report, Detailed Client Dose Admin Reports, Summary Client Dose Admin Reports, and Client with Highest Risk (28 Days) Report • View AO site Dashboard, AO Scheduling Dashboards, and the associated linked reports
COVax Clinic Coordinator	• All vaccinator permissions • Report inventory reconciliations at the VE level (wastage, extra doses from vial, no consent)	• View AO Site Dashboard, AO Scheduling Dashboards, and the associated linked reports
COVax PCP Vaccinator	• All vaccinator permissions • Report inventory reconciliations at the VE level (wastage, extra doses from vial, no consent)	• View AO Site Dashboard, AO Scheduling Dashboards, and the associated linked reports

C. Viewing User AO Assignments

1. Click on the Salesforce avatar on the top right corner of the page.
2. Select **Settings**.



3. Navigate to *Advanced User Details.*
4. Scroll down to check your **Authorized Organization**.



D. Users Who Work Across Multiple AOs

- Separate login credentials will be granted for users who work across multiple AOs.
- Contact the site lead of the new AO access is required from. They will submit a request to the ITS team to grant the additional login credentials.
- Users with multiple accounts will use the same email for all accounts, but with a slightly modified username. For example:

- **Account 1** – FIRSTNAME.LASTNAME@emaildomain.com.covaxon
- **Account 2** – FIRSTNAME. LASTNAME@emaildomain.com.covaxon2

- Site leads are encouraged to regularly audit the list of users and revoke access to any inactive users. In the case that a site lead is uploading a user for a secondary account, ensure to indicate that in the USERS_LOAD_TEMPLATE which is used to upload users to COVax$_{ON}$.

E. Users Who Work Across Multiple VEs within the Same AO

- These users do not require multiple logins and will be able to successfully use the system for one or more VEs.

F. Users Who Require Changes to their Profile

There are certain cases where a user's profile may need to be changed (e.g., if they are improperly mapped to an AO, or if their profile type (e.g., vaccinator, site staff) needs to be updated. The process outlined below is to be followed for profile changes:

- **Users at clinics/hospitals/LTCH/RH** – users must reach out to their site lead and request a user profile change. The site lead will confirm their reasoning and reach out to the ITS team on the user's behalf. The ITS team will grant the user refreshed login credentials based on the update they are requesting.
- **Users at pharmacies** – users can request a user profile change via designated trainers.

Note: This process is only appliable to changing user's profile. Adding new users to an AO or moving a user from one AO to another will follow the process explained above.

4. COVax$_{ON}$ Account Setup

When a new user is setup in COVax$_{ON}$, they must follow the two-factor authentication steps (below) when initially setting up their account. All COVax$_{ON}$ users require two (2) devices each time they log into COVax$_{ON}$: (1) a smartphone, and (2) a tablet or computer for using COVax$_{ON}$.

For existing users that are adding a secondary account to the Salesforce authenticator app, skip to section 4B (Setting up Two-Factor Authentication), step 11.

Attention new COVax$_{ON}$ users:

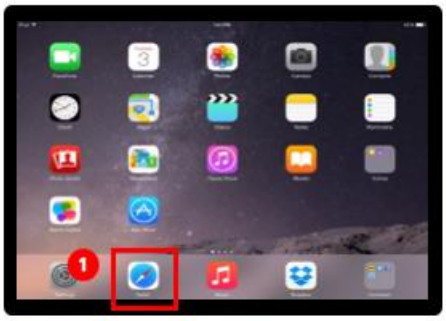
- Please setup your account prior to the first day of administering vaccinations
- The step-by-step instructions for doing so are included in this job aid
- You will require your smartphone (or mobile device) and a separate device (e.g., laptop or iPad)

Recommended browsers:

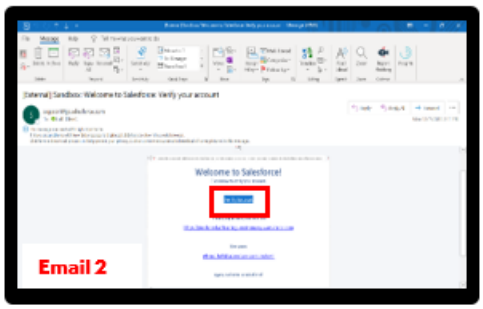
- **For iPad** – Safari
- **For desktop/laptop** – Safari, Google Chrome, Microsoft Edge, or Mozilla Firefox

A. Accessing the Salesforce Support Email

1. On the provided tablet, computer, or laptop, open COVax$_{ON}$ in one of the recommended browser applications.
2. Using the search bar, enter the URL of your email provider (e.g., Gmail, Outlook, UHN).



3. Log into your email account.
4. Open one of the following emails from support@ip.salesforce.com:
   - **Email 1** – copy the email link and paste it into a separate browser window
   - **Email 2** – right click the **Verify Account** button, select **Copy Hyperlink**, and paste the URL into your browser.

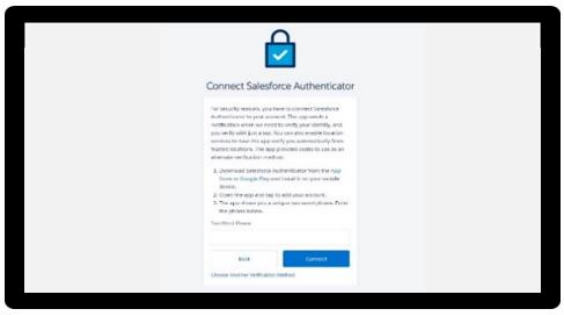


5. Once the link is pasted in your browser, click **Enter**.
6. A new Safari window will open. You will see the **Acceptable Use Policy**. Scroll down to read through the policy. To agree to the terms, click the **Finish** button at the bottom.

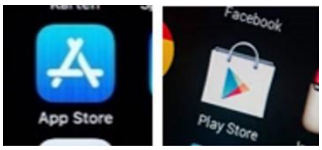
B. Setting Up Two-Factor Authentication

Two-factor authentication is a security feature that adds a second layer of security to the user authentication process through approval on their smartphone or mobile device (secondary device). Each time a user logs in to COVax$_{ON}$, they will require their mobile device on hand to approve the login. For any account timeout issues, please inquire with your site lead about contacting the MOH ITS team.

1. You will be directed to this screen. Do not exit this window. Set the tablet, computer, or laptop aside and grab your mobile device.

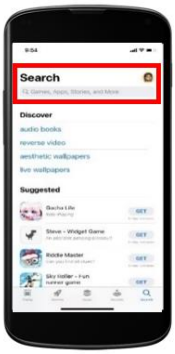


2. On your mobile device, open either the **Google Play** (for Android or Pixel) or **Apple App Store** (for iPhone).

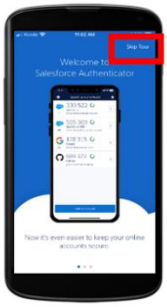


Note: If you have already gone through the registration process on the Salesforce authenticator app, and see a two-word phrase, skip to step 12 to setup a new account.

3. Using the search bar, type in 'Salesforce Authenticator'. Click on the title **Salesforce Authenticator**.

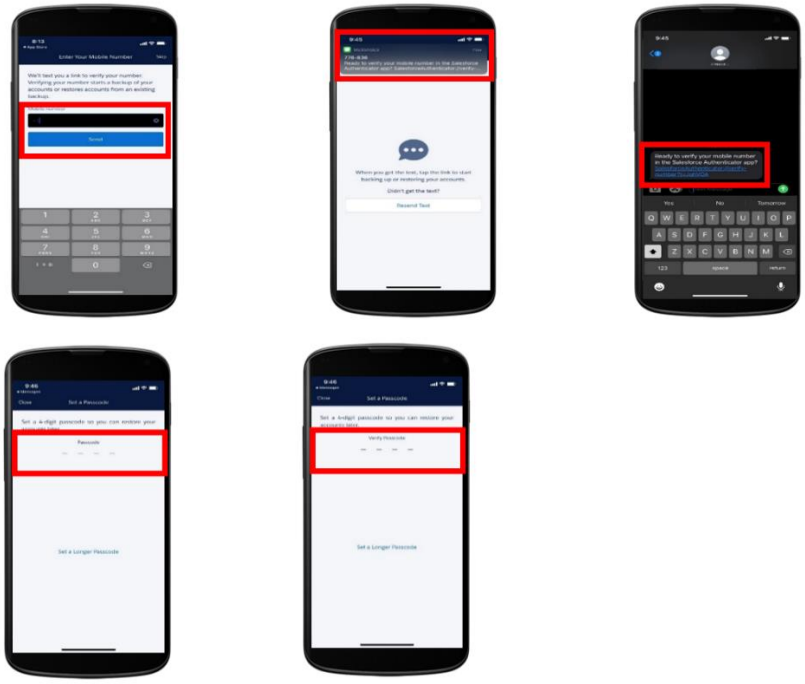


4. Click **Get**. Enter your Play Store or App Store credentials if needed.
5. *Still on your mobile device*, open the Salesforce Authenticator app.
6. When asked if you **allow this application to send notifications**, select 'Allow'.
7. Click **Skip Tour** at the top right of the screen.



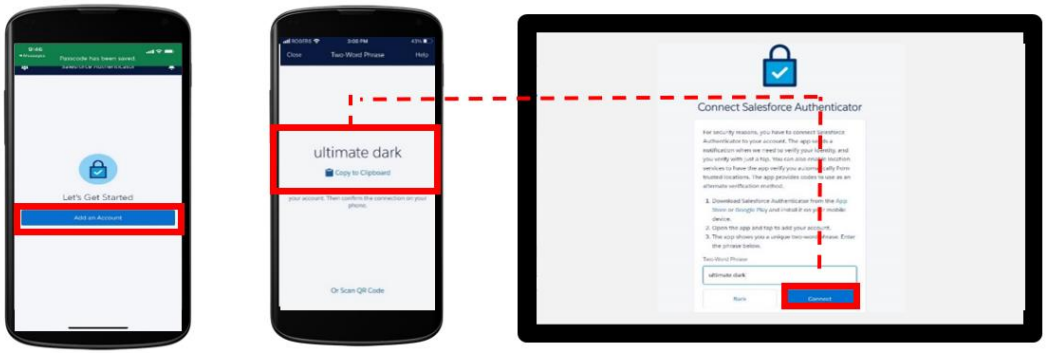
Enter your mobile phone number using the keypad. Click **Send** to have Salesforce send you an automated SMS message.

8. Wait to receive an automated SMS message from Salesforce. Once you have received the SMS message, open the message. Click the **link** that is provided.
9. Once you click the **link**, another window will open on your mobile device.
10. Choose a 4-digit **passcode**, and then verify that passcode by entering it in a second time.

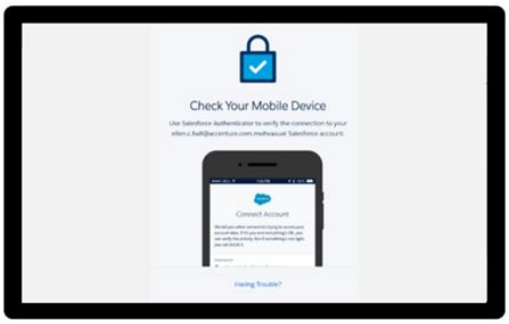


11. A green message will appear at the top of your screen indicating that the passcode has been saved. Click **Add an Account** to continue.

    Note: If you have already gone through the registration process on the Salesforce authenticator app, and you are logging into a new environment, you can start here by selecting **Add an Account**.
12. On your mobile device within the Salesforce authenticator app, you will see a **two-word phrase** provided.
13. *Put your mobile device down.* Using the tablet, computer, or laptop, go back to the browser window from step 1. Enter the **two-word phrase** in the box.

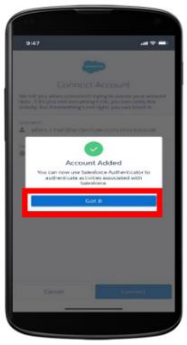


14. The following message will appear. Follow the prompt and *go back to your mobile device*.



15. On your mobile device, open the Salesforce authenticator app.
16. The following screen will appear. Click **Connect**.

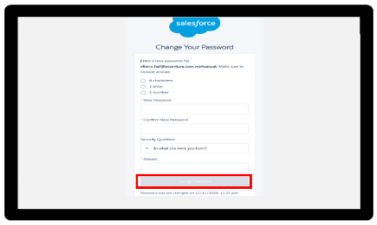
17. The app will indicate that the connection is successful. Click **Got It** to confirm.
18. The Salesforce authenticator app will ask you to approve the account. Click **Approve**.



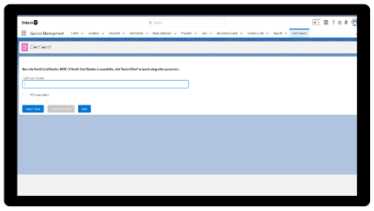
C. Changing Your Password

1. Using the tablet, computer, or laptop, go back to the browser window from step 14 above. Follow the prompts to create a suitable password. Ensure that you remember this password for future use. Click **Change Password**. You will then be logged in. You must remember this password to log into COVax$_{ON}$.

   Note: You may have to repeat this step if you forget your password, or if it is incorrectly entered in the future.

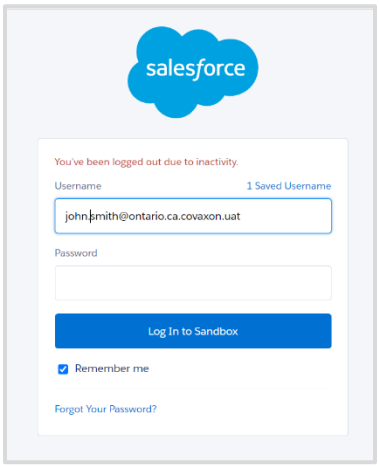


2. Once logged int, the COVax$_{ON}$ home page will appear as follows:

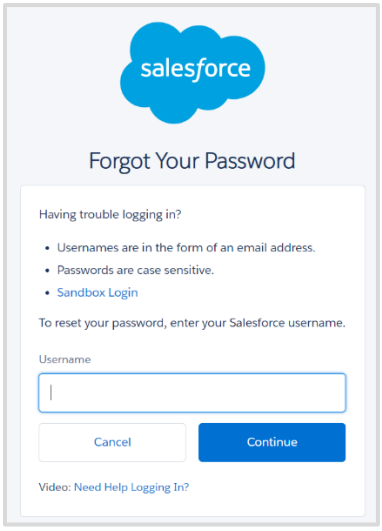


5. Reset Your Password to Login to COVax$_{ON}$

1. Click on the **Forgot Your Password** hyperlink.



2. Enter your **Username** and click **Continue**.



3. Check your inbox for email notification to finish resetting your password. Ensure you check your junk mail folder.

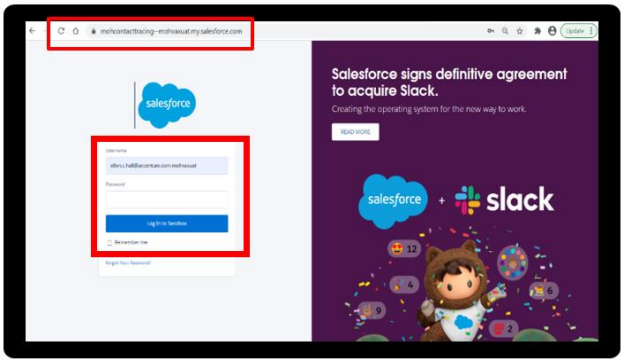
4. On your mobile device, open the Salesforce authenticator app.
5. Enter the numbers displayed on the authenticator app.
6. Change your password by entering a **New Password** confirming the new password.
7. **Save** the updated information.

Notes:

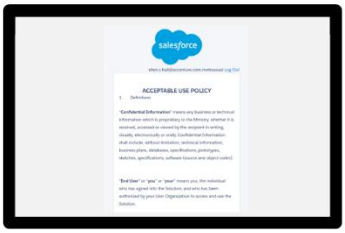
- You do not require an **authorized contact** to reset your password unless your account has also been deactivated. (Note: Your account will be auto deactivated after not logging in for three consecutive weeks.)
- You cannot perform the password reset on the same device you have your Salesforce authenticator app installed on (most likely your mobile device). As such, you'll need to open the email from a different device such as a work computer or MOH iPad.
- The email link expires after 24-hours.

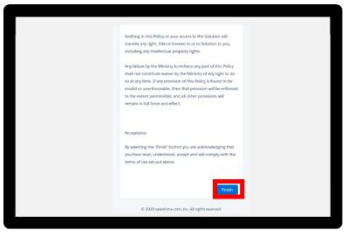
6. Subsequent Logins to COVax$_{ON}$

1. Open COVax$_{ON}$ by opening your browser (Safari, Google Chrome, or Microsoft Edge) and go to the COVax$_{ON}$ URL link: https://covaxon.my.salesforce.com.
2. Enter **username** and **password** credentials. Click on **Log In To Sandbox**.



3. Users will see the **Acceptable Use Policy**. Scroll down to read through the policy. Click the **Finish** button at the bottom of the acceptable use policy to agree to the terms.





4. The first time a user normally logs in, mobile device registration is required.
    - Ensure you change the country to 'Canada'
    - Enter your mobile phone number, then click **Register**

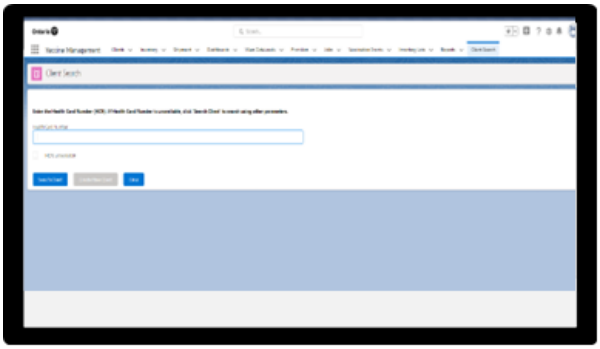
5. Users will receive a text message on their mobile device with a **verification code**.
    - Enter this code on the screen
    - Click **Verify**

Note: This is a one-time step. Once you complete this step, it will not appear for future logins.

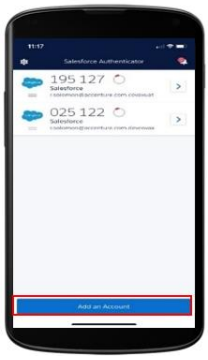
Note: Users that have two (2) login credentials for COVax$_{ON}$, may be asked to **Add an Account** prior to approval.

6. On your mobile device, users will receive a request from the Salesforce authenticator app.
7. Open the application and click **Approve**.

8. On the tablet, computer, or laptop, the COVax$_{ON}$ home page will open.



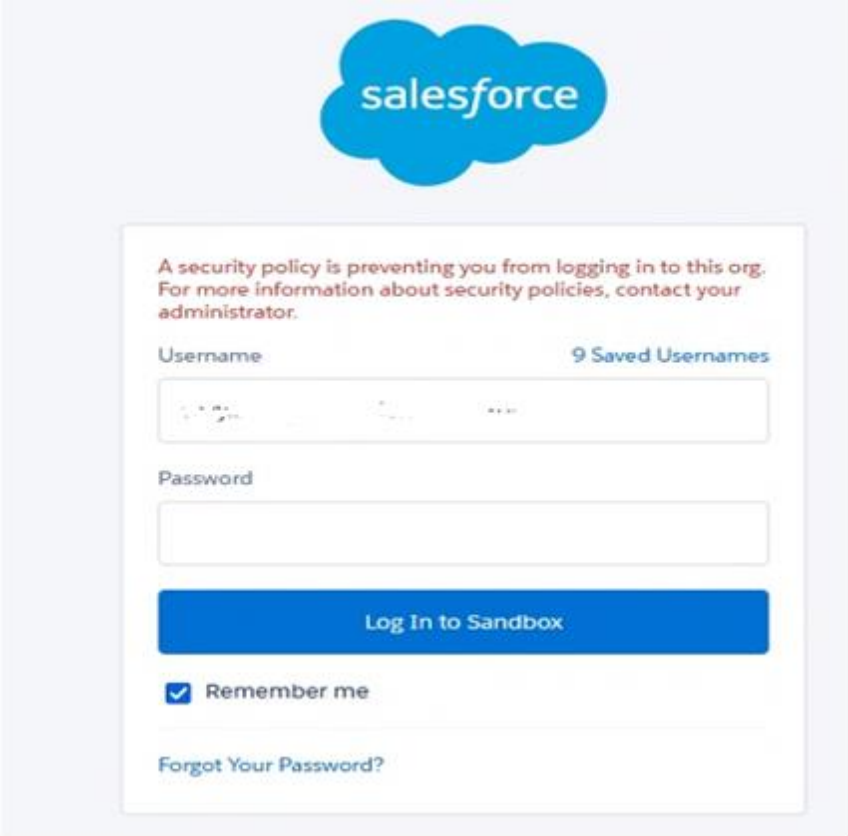
9. If using multiple Salesforce logins (e.g., if you belong to multiple AOs and require different logins), you will need to add a new account to your Salesforce authenticator app. On the app home screen, click **Add an Account**.



7. Restricted User Login to COVax$_{ON}$ Outside of Canada

Users can only log into the COVaxON application from within Canada. In addition, some users with VPN connections routed through another country will also be unable to access the application.

Users accessing the COVaxON application outside of Canada will receive the following error message.

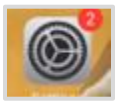


8. Clearing Cache and Logging Out of COVax$_{ON}$

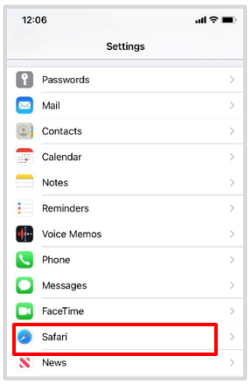
A. Clearing the Cache

If the COVax$_{ON}$ solution is lagging or having trouble loading the data, try clearing the cache. To do this, follow the steps below for an iPad, or follow alternative steps for the specific device. It is recommended that this is done prior to logging on and also as part of the logout routine.

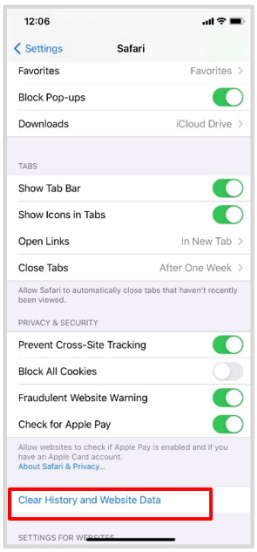
1. Open device **Settings**.



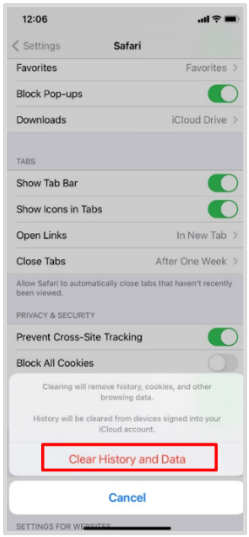
2. Scroll down to select 'Safari'.



3. Scroll down to select 'Clear History and Website Data'.



4. Click **Clear History and Data**.

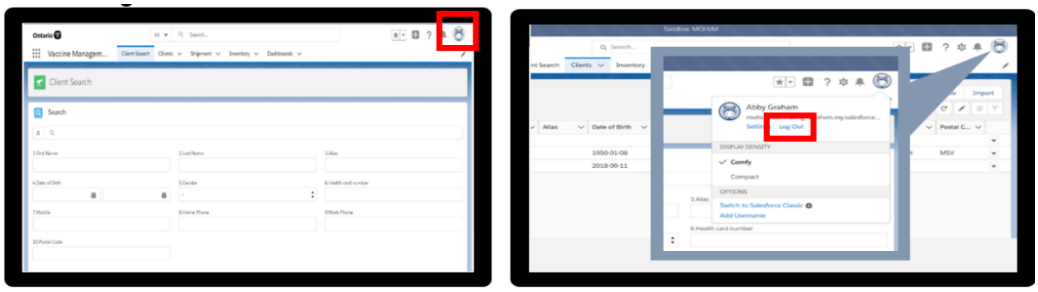


5. Sanitize each iPad according to individual site protocols.

B. Logging Out of COVax$_{ON}$

It is important that at the end of each use, and before exchanging devices with another user, the user logs out of their COVax$_{ON}$ account. Some locations have been provided with their own devices to access COVax$_{ON}$. Therefore, the instructions below are recommended to **properly log out of COVax$_{ON}$**.

1. On the tablet, computer, or laptop, click on the icon on the top right corner of the COVax$_{ON}$ home screen. Select 'Log Out'.



2. Exit the browser window.
3. Go to **Settings** and clear the cache (website and browsing history) for the next user.
4. **Do not** save the password in the Salesforce login page. This will prevent other users from easily logging in.
5. Sanitize shared devices according to individual site protocols, then return the device to onsite IT.

9. Hardware Requirements and Device Setup Onsite

Hardware Overview

There are four (4) types of hardware devices required onsite:

- **Mobile device** – you will require a smartphone onsite to access the Salesforce authenticator app
- **Second device (tablet, computer, or laptop)** – this must have proper internet connection to access COVax$_{ON}$ (Salesforce), and a recommended browser: Safari, Google Chrome, Microsoft Edge, or Mozilla Firefox
- **Printer** – to print the client receipt, you must have a working printer onsite (further instructions are provided below)
- **Access point Wi-Fi routers** – *if LTE does not work* for Bell, TELUS, and Rogers network carriers (further instructions are provided below)

Follow these steps to maintain hardware and software onsite:

1. Open COVax$_{ON}$ by opening your browser (Safari, Google Chrome, or Microsoft Edge) and go to the COVax$_{ON}$ URL link: https://covaxon.my.salesforce.com.
2. If COVax$_{ON}$ is lagging or have trouble loading, go the **Settings** on the device and clear your cache (website and browsing history). Then log back into COVax$_{ON}$.
3. **Do not** save the password in the Salesforce login page. This will prevent other users from easily logging in.
4. Always logout from your COVax$_{ON}$ account at the end of your shift.
5. Sanitize the device after each use based on location protocol.

Hardware Setup

There are three (3) types of devices that may be available onsite:

- **iPad** – Air Model 8th Generation
- **Printers** – Brother RuggedJet4 Mobile, and Brother Thermal Printer (TD-4550DNWB)
- **Access point Wi-Fi routers** – *if LTE does not work* for Bell, TELUS, and Rogers network carriers

1. **iPad setup** – some locations have been provided with their own iPads to access COVax$_{ON}$
    - The COVax$_{ON}$ location iPads will be preconfigured and hardened via the MDM ITS Intune policy
    - The iPad's password information will be communicated via email to the ITS and hospital support staff
    - The iPads will be preset and will be ready for use at the site
    - The change the font size on an iPad:
        - On the Safari browser, select the **aA icon** in the URL ribbon to increase the font size displayed on the screen. Select the smaller 'A' to make the font smaller, and the larger 'A' to make the font larger, or
        - Select **Ctrl+** on the iPad keyboard while the browser is open to increase the font size

2. Printers

a. **Brother RuggedJet4 Mobile** – from a network connectivity perspective, the printers can be setup using two options/ scenarios:

Option 1 (PREFERRED) – iPads are <u>not</u> connected to an access point router (provided by Bell, TELUS, Rogers)

Setup Printer Instructions:

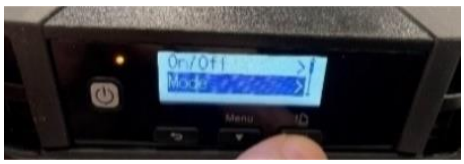
1. Click **MENU** --> Select **WLAN** --> Click **OK**, **OK**

2. Enable **WLAN** --> Select **On/Off** --> Click **OK**

3. Select **ON** --> Click **OK**

4. On **WLAN** --> Click **OK**

5. Scroll to **MODE** --> Click **OK**



6. Select **DIRECT** --> Click **OK**

Option 2 (Fallback) – iPads are connected to an access point router (provided by Bell, TELUS, Rogers) due to a poor signal (poor signal = iPads are connected to an access point)

Setup Printer Instructions:

1. Click **MENU** --> Select **WLAN** --> Click **OK**

2. Enable **WLAN** --> Select **On/Off** --> Click OK

3. Select **ON** --> Click **OK**

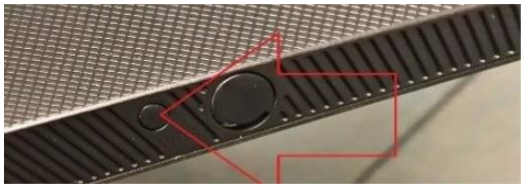
4. On **WLAN** --> Click **OK**

5. Then select **WPS** --> Click **OK**

6. Select **Button Push** --> Click **OK**

7. When the screen shows **WPS Settings** -->

8. Go to the router and press **WPS** button



Note: The printer display will show **Finished** when the connection between the printer and the router is established.

b. **Brother Thermal Printers (TD-4550DNWB)** – from a network connectivity perspective, the printers can be set up using two options/scenarios:

Option 1 (PREFERRED) – connecting the printer to the router via WPS

Setup Printer Instructions:

1. Place printer within range of wireless access point/router. The range may differ depending on the environment.

2. Click **MENU**.
3. Use the arrows to select the following: **WLAN** --> **OK** --> **WBS Button Push OK**.
4. You can also configure the setting using the PIN code by selecting --> **WPS PIN Code**.
5. Use the arrows to select **START** --> **OK**.
6. Press the **WPS button** on your wireless access point/router. When the connection is established, the **WLAN icon** appears on the printer's LCD.

   Notes:

   - Printers will try to connect using WPS for 2 minutes. If **OK** is pressed during that time, the printer continues trying to connect for an additional 2-minutes.
   - Please repeat the steps again to add a second TD-4550DNWB printer to the same LTE hub if required.

Option 2 (Fallback) – connecting the printer using Wireless Direct (if LTE hub fails)

Setup Printer Instructions:

1. Set the printer to **Wireless Direct** mode using the LCD menu.
2. Press **MENU** --> use arrow keys to select **WLAN** --> press **OK**.
3. Use arrow keys to select **WLAN ON/OFF** --> press **OK**.
4. Use arrow keys to select **ON** --> press **OK**.
5. Use arrow keys to select **WLAN** --> press **OK**.
6. Use arrow keys to select **NETWORK MODE** --> press **OK**.
7. Use arrow keys to select **DIRECT MODE** --> press **OK**. The **Wireless Direct icon** will appear on the LCD.
8. On your mobile device's Wi-Fi settings screen, select your printer's SSID and enter the password.
   - The default SSID is: SSID: 'DIRECT-*****_td-4550DNWB'
   - The default password is: '455*****'

     Where '*****' are the last 5-digits of the product serial number.
9. It may take several minutes until the connection is complete.

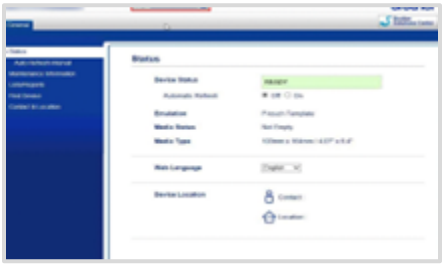
Printing Receipts

Brother Thermal Printer (TD-4550DNWB):

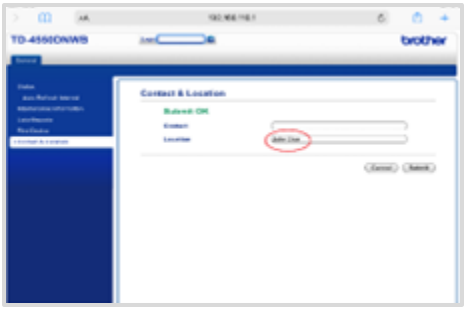
- **How to cut paper for the TD-4550DNWB printer**:
  - **Important Note:** The automatic cutters have been backordered. You will receive either the printer with the cutter installed or with no cutter at all. Once the cutters are back in stock, they will be shipped to you. The printer can still be used without the cutter.
  - **With the cutter** – the receipt will be cut to size automatically
  - **Without the cutter** – tear the receipt against the existing printer housing in a swift upward motion (45-degree angle). See picture below for more details.

- **Paper size setup for the TD-4550DNWB printer**:
    - The paper size can be configured using the web-based management by connecting the iPad to the printer via 'Wireless Direct' option.
    - Select **Printer** settings --> **Paper Size Setup** --> select **RD 102** --> click **Submit**.
- **Location information:**
    - Using web-based management to input the location information, users are able to add a distinguishing location name to identify the printer associated to themselves
        1. Connect the iPad's Wi-Fi to the **DIRECT MODE**.
        2. Print the printer configuration to find out **the IP address associated** to the printer:

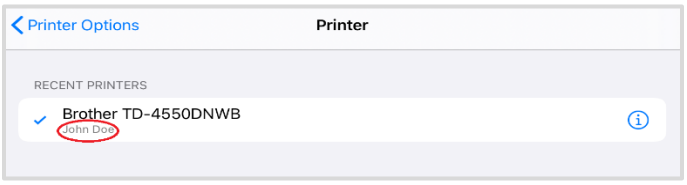
            Select **Menu** (scroll down) --> select **Information** (scroll down) **-->** select **Print Configuration** (identify the printer's IP address at the bottom of the printed receipt)
        3. Type **http://printer_ip_address/** into your browser (where 'printer_ip_address' is the IP address (e.g., 192.168.118.1) or the print server name).



        4. Click on **Contact & Location**.
        5. In the **Location** field, type a unique name and click **Submit**.



6. The location of the printer will be visible, preventing confusion when multiple printers under printer options are available and are using the same printer's name.



Note: The access routers used at locations will be set up with the appropriate SSIDs and passwords based on consultation with the ITS support team.

3. Access routers setup – SSID and passwords

- Access point routers are set up with the same SSID and password per site
- For pilot, all the access routers will be preconfigured and set up with appropriate SSID and password, and labeled prior to shipping onsite
- The router password information will be communicated via email to the ITS support staff
- The following provides a visual with access router info for each carrier, as well as the label information:

These Wi-Fi hubs are a back-up option if LTE is not working

TELUS Access Router and Label visual:

ROGERS Access Router and Label visual:

BELL Access Router and Label visual:

10. Offline Solution if COVax$_{ON}$ is Unavailable or Client Does Not Consent to Digital Collection

If required, client vaccination information can be captured in a paper form instead of the COVax$_{ON}$ digital solution.

There are four (4) situations where the COVax$_{ON}$ offline solution can be used:

- **The client doesn't consent to data collection during check-in** – in this case, the client information should be tracked outside of COVax$_{ON}$ using the paper process
- **The COVax$_{ON}$ system goes down (connectivity is lost) during vaccinations that are taking place** – in this case, the paper process can be used to continue vaccinating clients during the outage period. Once the outage is over, the data should be retroactively input into COVax$_{ON}$ within 72-hours of the vaccination date.

- **A mobile vaccination team conducting vaccinations at a rural or remote location without connectivity** – in this case, the paper process can be used during the time of vaccination, and then the data should be retroactively input into COVax$_{ON}$ within 72-hours of the vaccination date
- **A temporary team of staff are conducting vaccinations who are not trained on COVax$_{ON}$ or are not users of COVax$_{ON}$** – in this case, the paper process should be used the time of vaccination, and then the data should be retroactively input into COVax$_{ON}$ by a trained user within 72-hours of the vaccination date

Notes:

- There are various versions of offline data entry forms, depending on the vaccine product. They can be found on the MOH SharePoint site and there is a dedicated contact per location that has access to SharePoint and can disseminate the documents further.
- The completed paper forms should be filed for reference when the client returns for their next dose. The inventory manager should be made aware that there were doses administered outside of COVax$_{ON}$ so that they can adjust the inventory availability as required.

To use the offline process, complete the following steps:

1. Client brings the completed consent form to the COVID-19 vaccination event.
2. The clinician confirms that the form has been fully completed.
3. Client presents the completed form to the vaccinator.
4. Vaccinator confirms the client has no contraindications and has consented to service. **Note:** If the client has contraindications or has not consented to service, the vaccinator indicates this in the *For Clinic Use Only* section on the consent form.
5. Vaccinator completes the *For Clinic Use Only* section on the consent form, excluding the appointment date for the second dose, returns the form to the client, and directs them to the check-out area.
6. Client presents the form to the check-out clinician who books the client for the second dose appointment, creates a manual paper receipt (using the data from the top of the consent form), including the date and time of the next appointment, and gives it to the client.

Impact to inventory:

- When a client follows the offline paper process, their dose administration is not captured within COVax$_{ON}$. Therefore, the inventory will not be decremented in COVax$_{ON}$ and the doses available quantity will not be accurately reflected.
- The number of clients that did not consent to digital data collection and used the paper process should be tracked and an inventory adjustment must be made following the dose administration to ensure the doses available quantity is accurately reflected in COVax$_{ON}$.
- Refer to the **01 – Inventory** job aid (within the training folder on MOH SharePoint) for details on how to adjust the inventory quantity for clients who did not consent to digital data collection.