Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

COVAX

Multi Factor Authentication (MFA)

TROUBLESHOOTING GUIDE

Last updated - 14.6.2022 Ver2

TROUBLESHOOTING:

FORGOTTEN PHONE/SMART DEVICE:

If a person leaves their phone or smart device with the authenticator app at home or cannot access it, they will need a temporary verification code generated in order to access Covax. In order to receive this temporary verification code, a case must be raised on Service Cloud (see *Raising a case on Service Cloud* below).

Please ensure the nature of the request is stated, **e.g. Forgotten phone** and include a contact number.
When the case has been raised on Service Cloud, the NSD Covid Team will generate a temporary verification code for the person to sign in with. The NSD Covid Team will contact the Case Owner via phone in order to speak to the person directly and relay the code in a secure manner.

This code will only remain active for **12 hours**.

NOTE: It should be stressed that it is important that the person must keep this temporary verification code hidden and secure. Keeping the temporary verification code written on a post it or piece of paper near the device, for example, is not permitted.

LOST OR STOLEN PHONE/SMART DEVICE:

If a person has either lost their smart device or had their smart device stolen, the Multi Factor Authentication link between the persons Covax account and the authenticator app on their smart device must be disconnected by the NSD Covid Team and a temporary verification code will be generated by the NSD Covid Team in order to allow the person to access Covax.

Please raise a case on Service Cloud (see *Raising a case on Service Cloud* below) asking for the phones Multi Factor Authentication Link to the authenticator app to be disconnected and for a temporary verification code to be issued. Please ensure the nature of the request is stated in the case, **I.E. Lost/Stolen phone** and include a contact number**.** When the case has been raised on Service Cloud, the NSD Covid Team will generate a temporary verification code for the person to sign in with.

The NSD Covid Team will call the Case Owner via phone in order to speak to the person directly and relay the code in a secure manner.

This code will only remain active for **12 hours**.

NOTE: It should be stressed that it is important that the person must keep this temporary verification code hidden and secure. Keeping the temporary verification code written on a post it or piece of paper near the device, for example, is not permitted.

MFA SETUP WITH INCORRECT APP:

If a person has downloaded and completed the MFA setup with an app other than the Microsoft Authenticator app, such as the "Salesforce Authenticator" app, then they should switch over to the Microsoft Authenticator App. To do this, the link between the Covax account and the incorrect app will need to be disconnected by the NSD Covid Team. To disconnect the link please raise a case on service cloud for the incorrect authenticator app to be disconnected (see *Raising a case on Service Cloud* below).

Please ensure the nature of the request is stated, **I.E. MFA Setup with incorrect app.** Once the old link is disconnected, the person can download the Microsoft Authenticator app to their smart device and login to their Covax account to prompt MFA Setup. Please note that, if a person deletes the Salesforce App and downloads the correct Microsoft app without doing this, they will be unable to access their Covax account.

MICROSOFT AUTHENTICATOR APP DELETED:

If a person already has MFA setup but then deletes the Microsoft Authenticator app from their smart device, then they will need go through the MFA set up process again. However, the existing link between their Covax account and the deleted authenticator app must be disconnected by the NSD Covid Team. To disconnect the link, raise a case on service cloud for the deleted authenticator app to be disconnected (see *Raising a case on Service Cloud* below).

Please ensure the nature of the request is stated, **I.E. Microsoft Authenticator App Deleted.** Once the old link is disconnected, the person can download the app and login again to prompt MFA Setup. If a person deletes the Microsoft Authenticator App and then re-downloads the app without doing this, they will not be able to access their Covax account or set up MFA with the new app.

PERSON HAS NEW SMART DEVICE:

If a person has a new smart device, the existing link between the authenticator app on the old smart device and the Covax account must be disconnected by the NSD Covid Team. This is to allow the person to set up a new link with the authenticator app on the new device. To have the existing link disconnected, the person must raise a case on service cloud (see *Raising a case on Service Cloud* below).

Please ensure the agent states the nature of this request, **I.E. New phone/smart device, please disconnect MFA from old phone/smart device.** Once the old link has been disconnected, when the person attempts to log in again, they will be prompted to set up the MFA.

CODE NOT BEING RECOGNISED/NOT VALID:

The first step is to check that the time on the persons smart device with the authenticator app is exactly the same as the time on the device with the Covax account – both devices must be the exact same time.

You may need to check that the time and date settings on the persons smart device are set to **automatic** and not set up manually as this can affect the code being recognised by Covax when entered on the computer.

- Samsung phone – Select Settings, then General Management, then Date and Time, and ensure Automatic date and time is selected.
- iPhone - Turn on Set Automatically in Settings > General > Date & Time.
  This automatically sets your date and time based on your time zone. If there's available time zone update, your device lets you know. Allow your device to use its current location to determine the correct time zone. To do this, go to Settings > Privacy > Location Services > System Services and select Setting Time Zone.

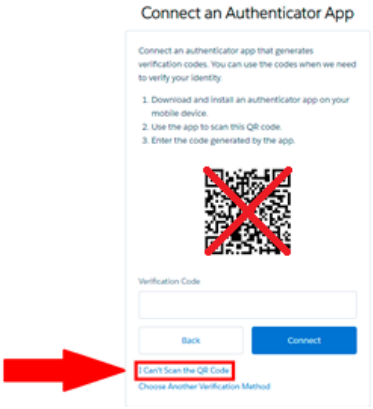
Once the settings have been changed, enter the code on the system and it should recognise the correct code. **PLEASE NOTE:** In some cases, you may need to restart the smart device if it is still not recognising the code.

If the automatic time is different to the time on the device with the Covax account, then the person needs to manually set the time on the smart device that has the authenticator app to match the time on the device with the Covax account, to the nearest second.

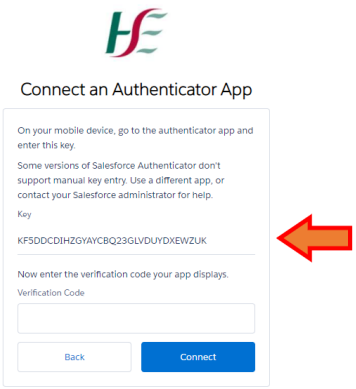
UNABLE TO SCAN QR CODE:

If you are unable to scan a QR code:

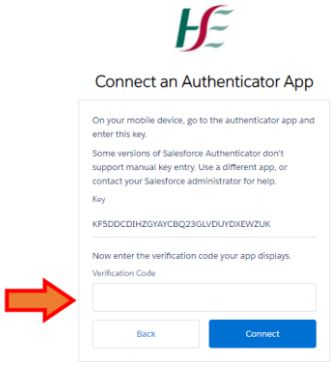
- Click on "I Can't Scan the QR Code" on the screen in Covax – this is located below the Back and Connect buttons on the QR code screen.



- This will generate a long code (Highlighted in the image below) that you can use to connect the App on your smart device to your Covax account by following the next steps.



- Open MS Authenticator App and Select **Add Account** from the three dots on the top right corner of the screen.
- Select "**Other account (Google, Facebook, etc.)** this brings up the screen to scan the QR code, however please select **Enter Code Manually** at the bottom of the screen
- Under **Account Name** enter the name you want use to identify this account in your Authenticator app, for example HSE Covax.
- Then enter the **Secret Key** which is the code that appears on the screen in Covax in the first step above when you clicked on "I Can't Scan the QR Code" on your computer. Please note this is free text and it can be difficult to distinguish between O (character) and 0 (number), so please take care entering this key into the App.
- Once they Secret Key has been entered into the App, the new account should be created under the App. You should then enter the six-digit code generated by the app into the box labelled "**Verification Code**" below the "Key" on the computer (see below) and click on **Connect**. This will connect the App on your smart device to your Covax account. Once connected you will only need to enter the six-digit code when logging on again.



MFA LOCKOUT:

Attempting to enter an MFA code unsuccessfully **10 times** will result in an MFA lockout. This lockout will remain in place for **1 hour**. There is no option to bypass the lockout as this is a necessary security precaution built into the Covax salesforce platform.

MFA lockouts may occur for a number of reasons as listed above in the troubleshooting guide. All of the following scenarios will result in an incorrect MFA code being generated on the Microsoft Authenticator app which may lead to an MFA lockout:

- Time and date settings on the smart device are not matching the device with the Covax account.
- Person has deleted their old Microsoft Authenticator app without correctly setting up a new version (MFA Link still tied to old app).
- Person has a new smart device but MFA has not been setup correctly (MFA link tied to app on old device).

Please do not persist with invalid/unsuccessful MFA attempts and instead raise a case on Service Cloud (see *Raising a case on Service Cloud* below) so the NSD Covid Team may diagnose and resolve the issue.

Raising a case on Service Cloud

When you need to raise a case on service cloud (e.g. to request MFA setup or to raise cases in relation to trouble shooting issues found in this guide) you can request your onsite ICT agent to raise the case on your behalf.

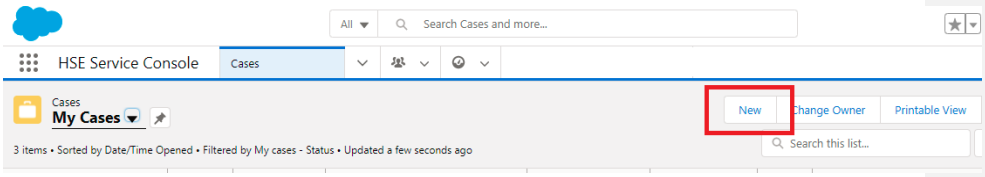
If you do not have access to an ICT agent, you can email covid19.support@healthservice.ie and copy and paste the following into the subject line of the email - Multi-factor Authentication (MFA). Give the details of your request in the body of the email and a member of the NSD Covid Team will contact you in relation to your case.

If you are an Ops Admin then you can raise the case directly yourself on Service Cloud. The details on this process are as follows and are also contained in myTrailead via module MOD 1B - "How to Raise a Support Request or Log an Incident":

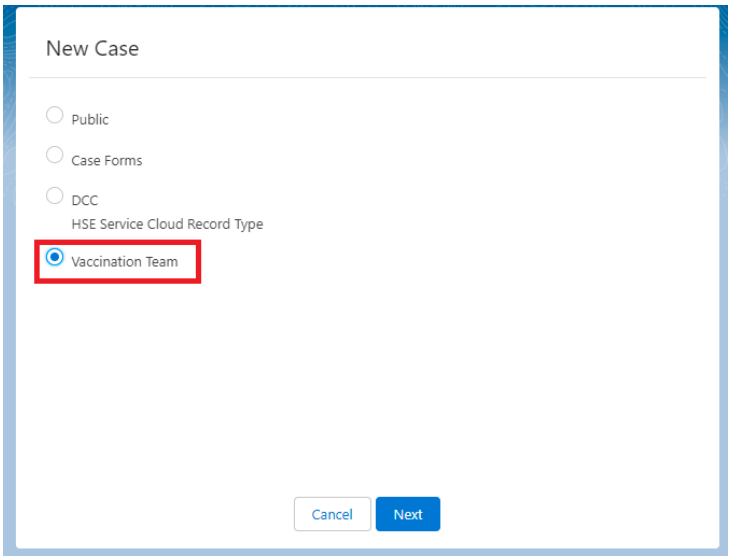
Commented [ZF1]: Hi Chris, can you include the module number here for this, i cant remember what it is, thanks

Raising a case on Service Cloud

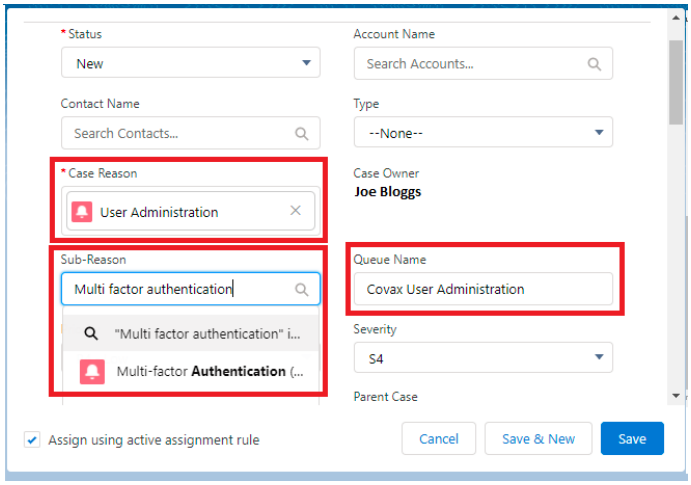
Please ensure you are on the HSE Service Console by selecting this from the nine-dots. Select Cases the drop-down menu to the right of the words HSE Service Console (you may need to type the word Cases if this is the first time you have used this functionality). From here you will click on the "New" option highlighted below.



Please select the "Vaccination Team" option and Click Next.



You will then be directed to begin filling out the case details. Please enter the Case Reason (User Administration), the Sub Reason (Multi Factor Authentication) and the Queue name (COVAX user Administration). These fields are highlighted in the image below.



Following this, the last step is to fill out the case description. Simply state the Subject of the case (e.g. MFA Forgotten Phone) and then a brief description of the case itself. Once you click on the Save button, the case will be raised.