



StepXpress for Multos

User Manual

Date: 24/03/2023

Author: Services Team

Document Number: SN-MA-0005

Revision Number: 3.2

Multos Ltd, Limited Distribution

Table of Contents

1. Getting Started	5
1.1 Introduction	5
1.2 Logging into StepXpress	5
1.2.1 Registration link expiration	6
1.3 System status display	7
1.4 Inactivity forced logout	8
1.5 Two Factor Authentication	9
1.5.1 Two Factor Authentication via Email	9
1.5.2 Two Factor Authentication via Authentication App	9
1.5.3 Installing your Two Factor Authentication	10
1.5.4 Logging in via an Authenticator App	14
2. Managing Accounts	15
2.1 Change Password	15
2.1.1 Reset Password.....	16
2.1.2 User Locked Out	16
2.2 Setting up / Updating your Security Questions	17
3. Home Page – Welcome to StepXpress	18
3.1 Issuers	18
3.2 Applications	19
3.2.1 Introducing Applications	19
3.2.2 Creating a New Application	19
3.2.3 View Details of an Application	21
3.3 Delete Redundant Applications.....	22
3.4 Search function in multiple pages	22
3.5 Enablement Data	23
3.5.1 Introducing Enablement Data	23
3.5.2 New Enablement Data Request.....	23
3.5.3 View Details of a Request	25
3.5.4 Status of a Request	26
3.5.5 Notification of Request Completion	26
3.5.6 Download Response Files	26
3.5.7 Templates	26
3.5.8 Saving a Template (In advance).....	26
3.5.9 Saving a Template (at the end of an enablement request).....	28
4. Certificate Requests	29
4.1.1 Introducing Certificates	29
4.1.2 StepXpress Certificate Screens	29
4.1.3 Requesting Certificates (ALC & ADC)	29
4.1.4 View Details of a Request	34

4.1.5	Status of a Request	34
4.1.6	Downloading Certificate Request	34
5.	Tools	36
5.1.1	File Checker.....	36
5.1.2	TKCK & HM	37
6.	Users	38
6.1	Account Administrator	38
6.2	Account User:.....	38
6.3	Managing Users	38
6.3.1	Users	38
6.3.2	Add New Users	39
6.3.3	Edit a User.....	39
6.3.4	Web Services	40
6.3.5	Managing user roles	41
7.	Multos Concepts	42
7.1	Application Delete Certificates (ADC)	42
7.2	Application Load Certificates (ALC)	42
7.2.1	Input data to request ALC.....	43
7.2.2	How a card uses an ALC	43
7.2.3	When new ALCs are required	43
7.3	Application Load Unit (ALU)	44
7.4	Creating a Confidential Application Load Unit.....	45
7.5	Application Loading.....	45
7.6	Application Signature	45
7.7	Application Registration.....	45
7.8	Input Data for Application Registration	46
7.8.1	Default and Shell Applications	47
7.9	Answer to Reset (ATR).....	47
7.10	Additional MULTOS Data (AMD)	47
7.11	Enablement.....	47
7.11.1	What does Enablement Data include	48
8.	Troubleshooting	49
8.1	Web Browser Support	49
8.2	Solving Common Problems and Errors	49

Revision status

Revision	Status	Date	Description	Author
1.0	Initial Draft	19.10.16	Initial Draft	MD
1.0	Release	28.10.16	Final Draft	MD
2.0	Review	02.07.18	Initial Review	MS
3.0	Review	06.05.22	New Update Release	FS & DC
3.1	Review	12 07 22	New Update Release	AT
3.2	Review	24.03.23	Update to Guide	DC

Copyright 2022 MULTOS Ltd. This document is confidential. No part of this document may be reproduced, published or disclosed in whole or part, by any means: mechanical, electronic, photocopying, recording or otherwise without the prior written permission of MULTOS Ltd. StepNexus is a trading name of MULTOS Ltd.

1. Getting Started

1.1 Introduction

StepXpress is a secure web portal that allow users to request the data they need to enable MULTOS cards and load applications.

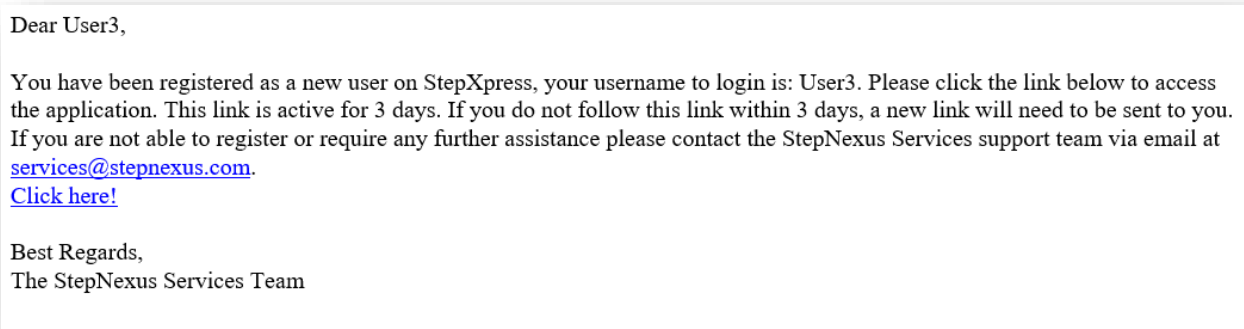
1.2 Logging into StepXpress

StepXpress can be accessed by visiting the following URL <https://www.stepxpress.com/>

To log on to StepXpress a user requires their **User ID and Password**.

When a brand new user account is set up they will receive an email notification stating they have been registered to StepXpress.

This email will contain a registration link to follow allowing the user access to StepXpress for the first time.



By clicking on the link **Click Here!**
The system will direct the new
User to the password set up page.

Please ensure to setup your
password by following the
guidelines.

*NOTE: If the password criteria is
not met you will not be able to
proceed to set your password.*

A password setup form with five guidelines listed at the top: 'Must include lowercase characters', 'Must include uppercase characters', 'Must include digits', 'Must include symbols', and 'Must be 10 characters or more'. Below the guidelines are two input fields: 'New password:' and 'Repeat new password:'. At the bottom of the form is a button labeled 'Set password'.

Once the Password has been correctly set up, the User will be redirected to the Security question set up page.

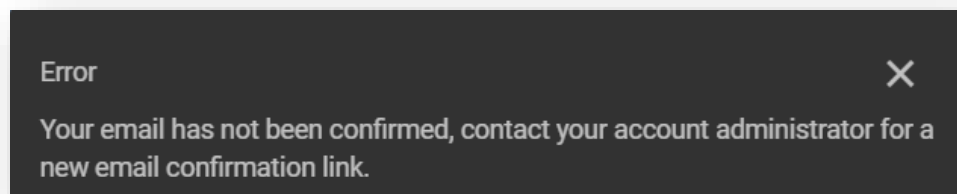
A pop up message will confirm when the security questions process has been successfully completed.

The User has now access to the system.

NOTE: The Account Administrator has the ability to create new users. If the account administrator is not known please contact services@stepnexus.com

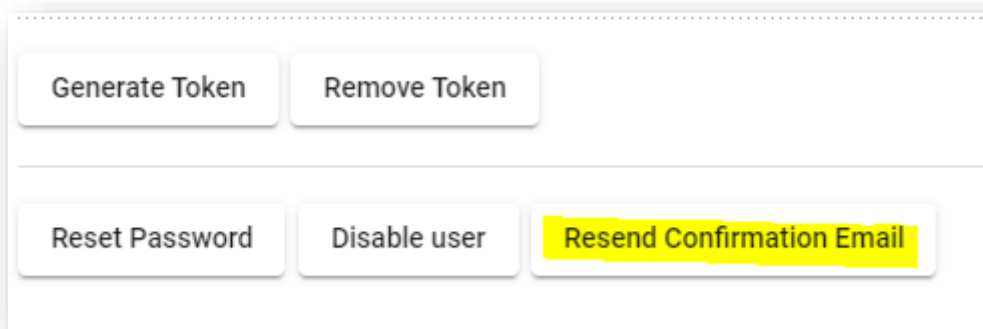
1.2.1 Registration link expiration

The registration link will expire after 3 days, so if the link has not been clicked on within this timeframe a new confirmation email will need to be sent out. The following screen will appear:



The Account Administrator has the ability to resend a confirmation email following these steps:

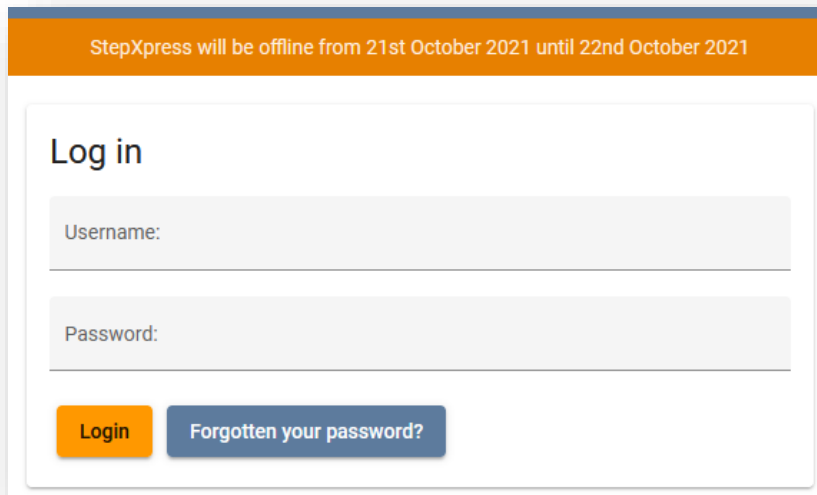
1. After logging in as an Administrator click on the tab **Users**
2. Select the user
3. Click on **Resend Confirmation email**



4. The user will receive a new email containing the link for the registration link.

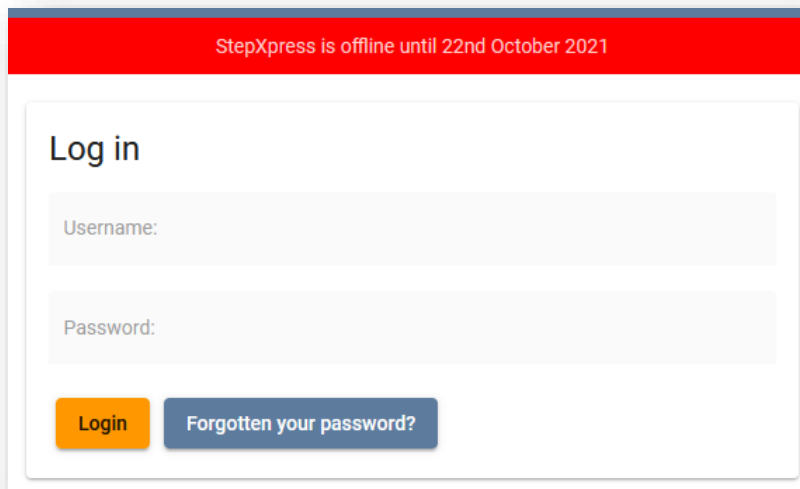
1.3 System status display

At times StepXpress will need to be down for planned maintenance. Before this a warning message will be displayed in the banner as shown below.



The screenshot shows a web interface for StepXpress. At the top, there is an orange banner with the text "StepXpress will be offline from 21st October 2021 until 22nd October 2021". Below the banner is a white login box with the title "Log in". Inside the box, there are two input fields: "Username:" and "Password:". Below the "Password:" field, there are two buttons: an orange "Login" button and a blue "Forgotten your password?" button.

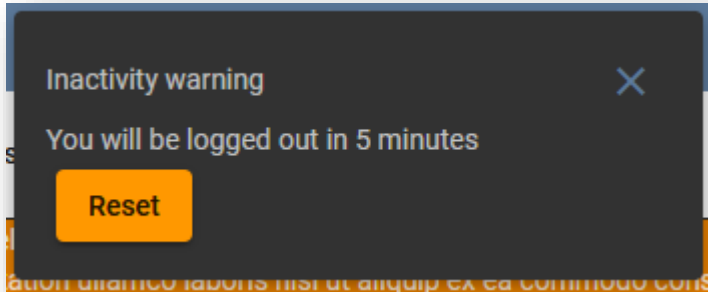
During down time where StepXpress will not be accessible an offline banner will be displayed as shown below. While this is showing the log-in fields will be disabled.



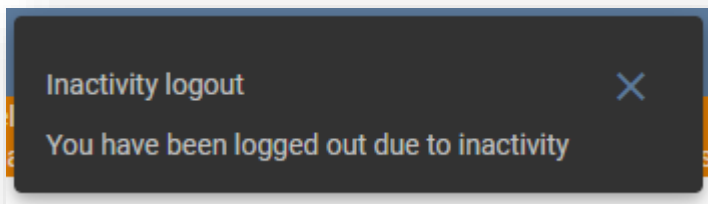
The screenshot shows the same StepXpress login interface as above, but with a red banner at the top that reads "StepXpress is offline until 22nd October 2021". The login box below still contains the "Log in" title, "Username:" and "Password:" fields, and the "Login" and "Forgotten your password?" buttons. According to the text, these fields and buttons are disabled during this time.

1.4 Inactivity forced logout

After 25 minutes of inactivity a warning message will be displayed that you are about to be logged out due to inactivity, as shown below. This timer can be reset using the "Reset" button on the warning.



If you are inactive for a further 5 minutes, 30 minutes in total, then you will be logged out and redirected back to the log-in page, with the below message showing, to explain why you have been logged out.



1.5 Two Factor Authentication

All users will be required to input a six digit authentication code on login.

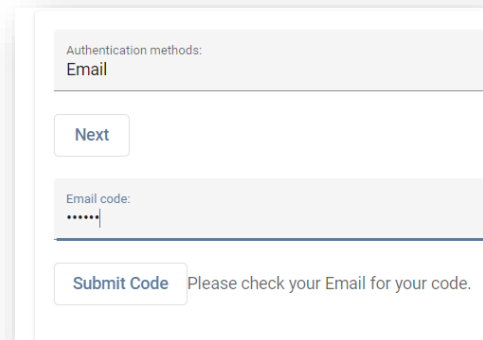
The code can be found using either of the following methods,

1.5.1 Two Factor Authentication via Email

By default, all users on the system will have access to two factor authentication via email. This method sends an email to the user's associated email address containing a six digit code on login.

The user will need to enter the code into the **Authentication Code** input box and click on the **Submit Code** button within a set period of time to authenticate their login attempt.

If the input code is incorrect or has timed out, the user can request a new code by clicking on **Next** button under the Authentication Method

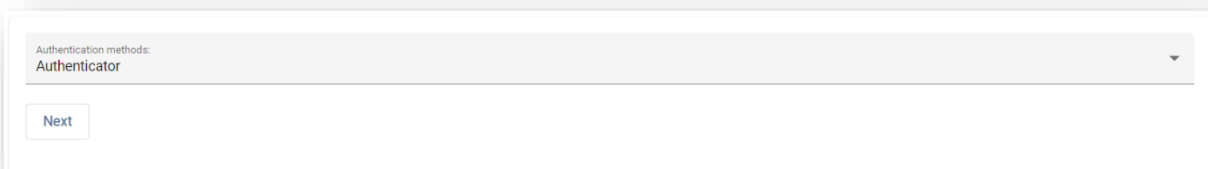


The screenshot shows a web form for email-based two-factor authentication. At the top, a dropdown menu is set to 'Email' under the heading 'Authentication methods:'. Below this is a 'Next' button. Further down, there is an 'Email code:' label followed by a six-digit input field with dots. At the bottom, there is a 'Submit Code' button and a message: 'Please check your Email for your code.'

1.5.2 Two Factor Authentication via Authentication App

As well as the default authentication via email method, the user has the option of linking an authentication app to their user account.

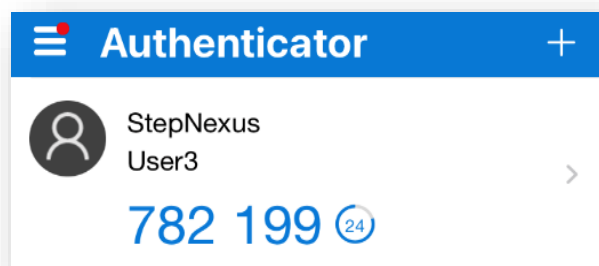
On login, if the user has a linked Authentication App, they will be given the option to authenticate via authentication app, selectable from the **authentication method** drop down list.



The screenshot shows a web form for app-based two-factor authentication. A dropdown menu is set to 'Authenticator' under the heading 'Authentication methods:'. Below the dropdown is a 'Next' button.

To log in via an authentication app, the user needs to open their chosen linked authentication app on their mobile device and enter the code listed under StepXpress (*Username*) where *Username* is your username on the system.

If the 6 digit input code is incorrect or has timed out, the user just needs to use the authentication app again to receive a new code.



The screenshot shows a mobile app interface for an authenticator. The top bar is blue with a hamburger menu icon, the text 'Authenticator', and a plus icon. Below the bar, there is a user profile section with a person icon, the text 'StepNexus User3', and a right arrow. At the bottom, a large blue code '782 199' is displayed next to a circular timer icon showing '24'.

To use an authentication app on the system, you will first need to have an authenticator app installed on your mobile device. StepNexus services recommend **Microsoft Authenticator**, however other authenticator apps are available.

PLEASE NOTE: All screenshots in relation to the Microsoft Authenticator App were taken against the android/iOS version of the app. Version number: 6.5.95. The screenshots shown within this guide may be different depending on the app version of Microsoft authenticator and the mobile device operating system that you are using. However, all steps should remain the same.

Extra documentation and help regarding the use of Microsoft Authenticator can be found at the following web address: <https://support.microsoft.com/en-us/account-billing/download-and-install-the-microsoft-authenticator-app-351498fc-850a-45da-b7b6-27e523b8702a>

1.5.3 Installing your Two Factor Authentication

If you do not currently have an authentication app installed on your mobile device, follow these steps to get set up with the recommended Microsoft Authenticator app.

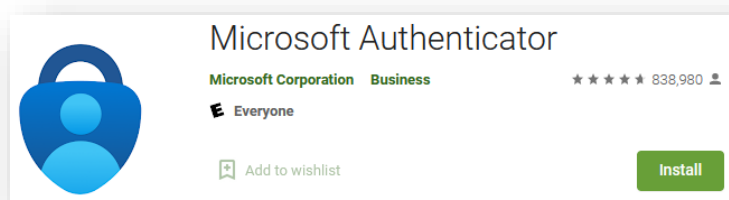
1. Open up the app store on your mobile device. This will be;
 - The Google play store for android devices,
 - The App store for Apple IOS devices (iPhone, iPad)
2. Once on the relevant app store for your device, use the search functionality to search for the term '**Microsoft Authenticator**'
3. Your device will list the apps related to your search query. You should select the one named 'Microsoft Authenticator'.

It is a free app published by the Microsoft Corporation. If the app is not showing as free or published by 'Microsoft Corporation', you may have selected the incorrect app. In this case, return to the search results and try again.

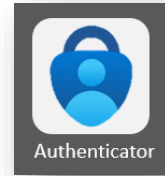
Microsoft authenticator app on Apple App Store



Microsoft authenticator app on Google Play Store



4. Click on the **Install / Get** button to download and install the authenticator app on your device.
5. Once installed, go back to your device's home screen or app drawer and you should now be able to find the newly installed app icon which should be called 'Authenticator'.



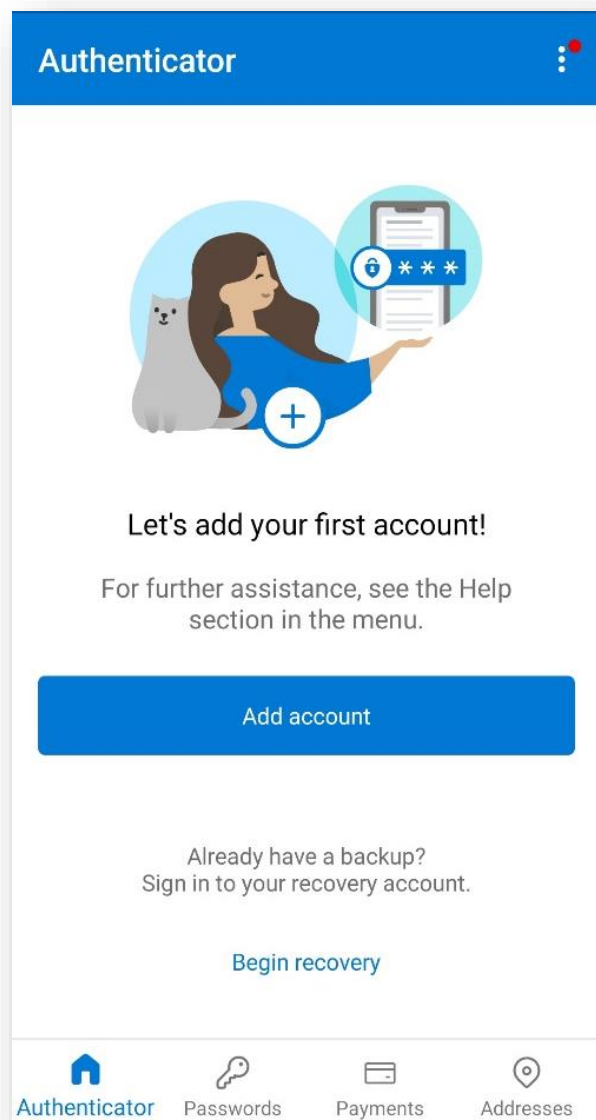
Once you have installed Microsoft Authenticator, follow these steps to set it up with your two factor authentication account.

1. Log into the StepXpress system using the authentication via email method.
2. Click on your username in the top right hand corner to access your user settings.
3. Navigate to the **Setup Authenticator** tab.

4. Open the Microsoft Authenticator app on your mobile device.
(If you do not have Microsoft Authenticator on your mobile device, please see section 1.3.3 above for instructions on how to install it.)

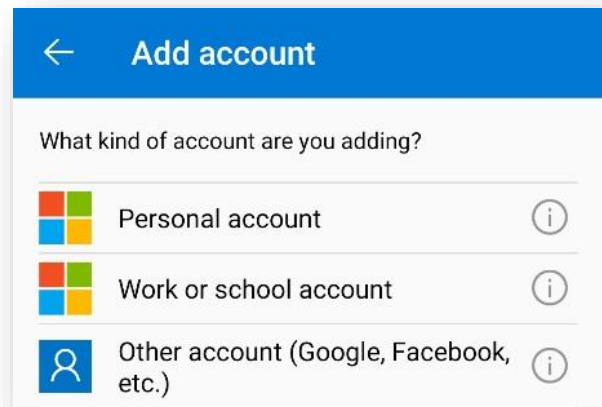
5. You should now see a screen similar to the screenshot on the right →

6. Click the **Add Account** button →



7. You will be asked to select what kind of account you are wanting to add.

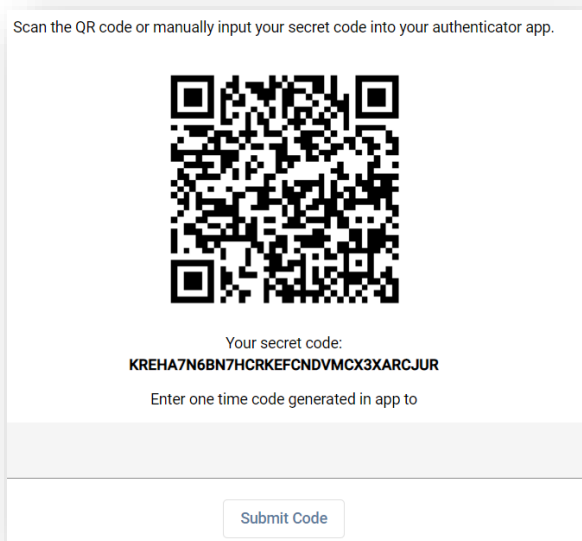
8. Click on '**Other Account (Google, Facebook, etc.)**' →



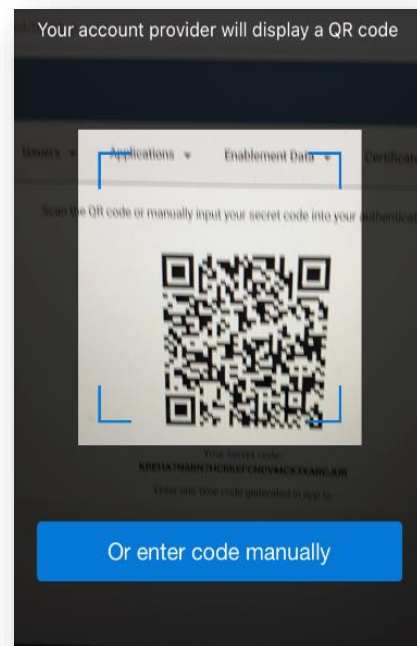
9. The app will open the camera on your device. Use this camera to scan the QR code provided by the StepXpress system on the **Authenticator App** page.

(You may need to allow your device to use your camera. A pop up on the screen should be asking for permission to use the camera. Choose '**Allow**')

**Authenticator App webpage
on StepXpress**

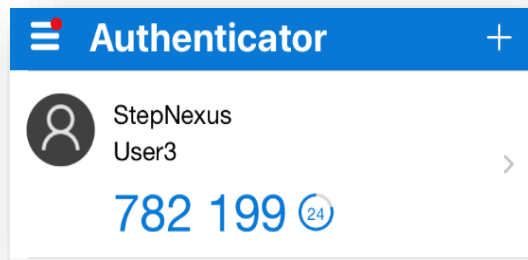


**Authenticator App viewed
through mobile device**

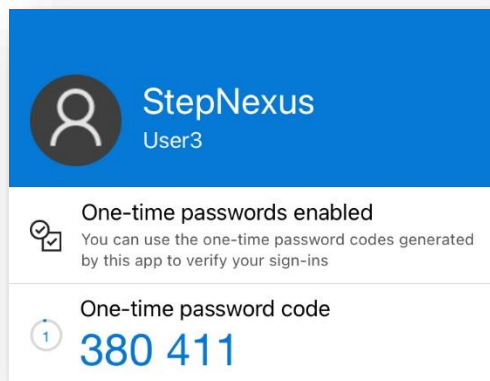


***PLEASE NOTE:** If the camera is unable to scan the QR code then the device may be paired manually by pressing the '**Or enter code manually**' option on the screen and entering a name for the account and the secret key shown below the QR code. Click **Finish** to add the account.

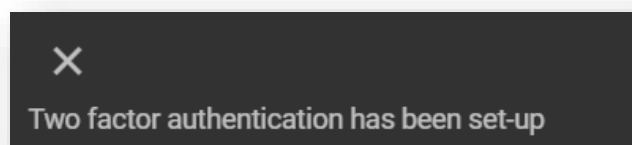
10. The Authentication App will be updated with an account listing the StepNexus system and your username.



11. To see your Two Factor Authentication code on the Microsoft Authentication App, click on your user account within the app. This will bring up a 6 digit One-time password code.



12. Input the six digit code the app outputs into the **Authentication Code** input box on the StepXpress system and click **Submit Code** to pair the authenticator app with your account.
13. A message will appear to show whether you were successful at setting up your authenticator app.



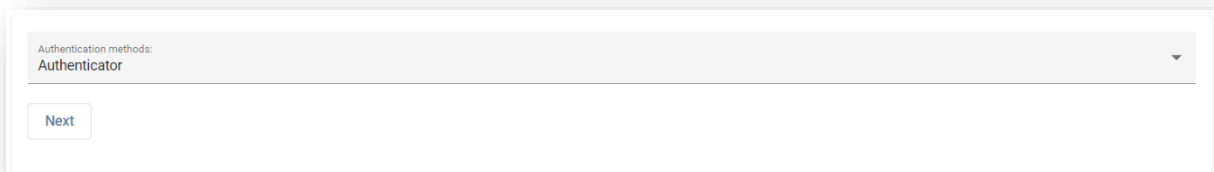
Once you have set up the Microsoft Authenticator app with your account on your mobile device, you will be able to log in via the authenticator app when logging into the system.

1.5.4 Logging in via an Authenticator App

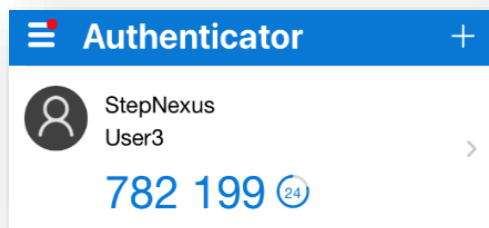
When logging into the StepXpress system, if you have an Authenticator app such as Microsoft Authenticator set up as per sections 1.3 you will be able to log in via your authenticator app.

To log in via your Authenticator App,

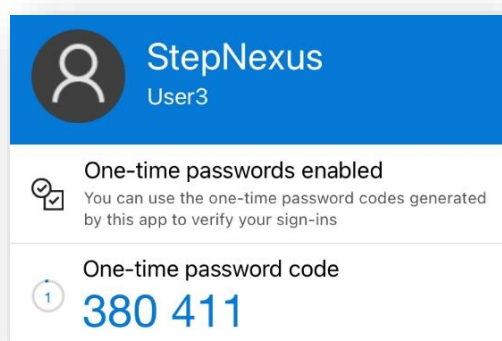
1. Log into the StepXpress system as usual with your username and password
2. When you reach the Two Factor Authentication stage of logging in, select '**Authenticator**' from the authentication method drop down box.



3. On your mobile device, open your authenticator app.
4. The app should automatically list your Two Factor Authentication accounts that you have set up.



5. To see your Two Factor Authentication code on the Microsoft Authentication App, click on your user account within the app.



6. Input the six digit code the app outputs into the Authentication Code input box on the StepXpress system and click Submit Code.
7. You should now be logged into the system.

2. Managing Accounts

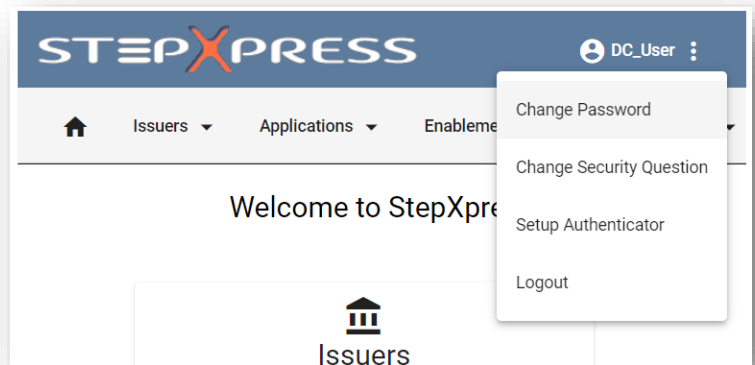
Located on the top right on the page, click on your username and open the menu for the following actions:

2.1 Change Password

To change password perform the following steps:

1. Click on the menu bar icon next to your Username at the top right of the screen

2. Click on '**Change Password**'



3. Enter the **current password**

4. Enter the **new password**

5. Confirm the new password - Please ensure to setup your password following the guidelines.

**PLEASE NOTE: If the password criteria is not met you will not be able to proceed to set your password.*

6. Click on the **Change Password** button

A screenshot of the 'Change Password' form. It has three input fields: 'Current password:', 'New password:', and 'Repeat new password:'. Each field is followed by a list of password requirements, each with a green circle icon: 'Must include lowercase characters', 'Must include uppercase characters', 'Must include digits', 'Must include symbols', and 'Must be 10 characters or more'. At the bottom of the form is a 'Change password' button.

2.1.1 Reset Password

If a password is lost or forgotten the system can initiate a password reset. To request a password reset:

1. Access the StepXpress Login Screen via the URL <https://www.stepxpress.com/>
2. Click on the '**Forgotten your password?**' button next to the **login** button
3. Enter the username and email address
4. Complete the Security question (*to set up your security questions, please see section 2.2*)
5. If you have entered the correct answer the password will be reset and a link will be sent to the email address that is registered on the system
6. **Click on the link provided in the email sent to your inbox**
7. Enter your new Password twice.
8. The system will redirect the user back to the login page to login with the new credentials.

2.1.2 User Locked Out

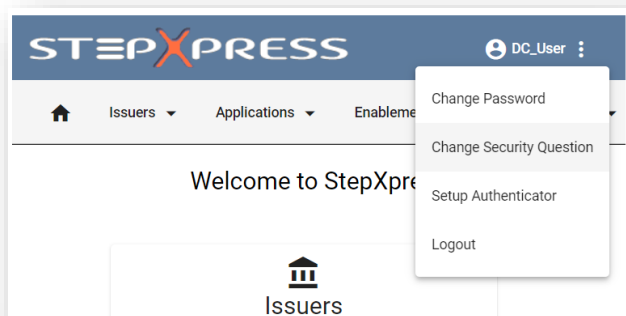
If a user is locked out of StepXpress after failing security 3 times an email will be automatically sent to invite them to unlock and reset their password.

When you click the link sent to your email you are prompted with a security question which you have to answer to unlock your user.

This email will have a link that is valid for 1 hour. After this link has expired a new one can be requested by selecting the 'forgotten your password' option.

Alternatively, an Account Administrator can unlock the user as well as StepNexus Services Administrators (services@stepnexus.com).

2.2 Setting up / Updating your Security Questions



1. Click on the menu bar icon next to your Username at the top right of the screen.

2. Click on **Change Security Question**

A screenshot of the 'Change Security Question' form in the StepXPRESS application. The form is titled 'Select a security question:' and contains three identical sections. Each section has a dropdown menu for selecting a question and a text input field for the answer. At the bottom of the form is a 'Save' button. The navigation bar at the top includes links for Home, Issuers, Applications, Enablement Data, and Certificates.

3. Select 3 Security Questions from the dropdown lists provided and type in your answers

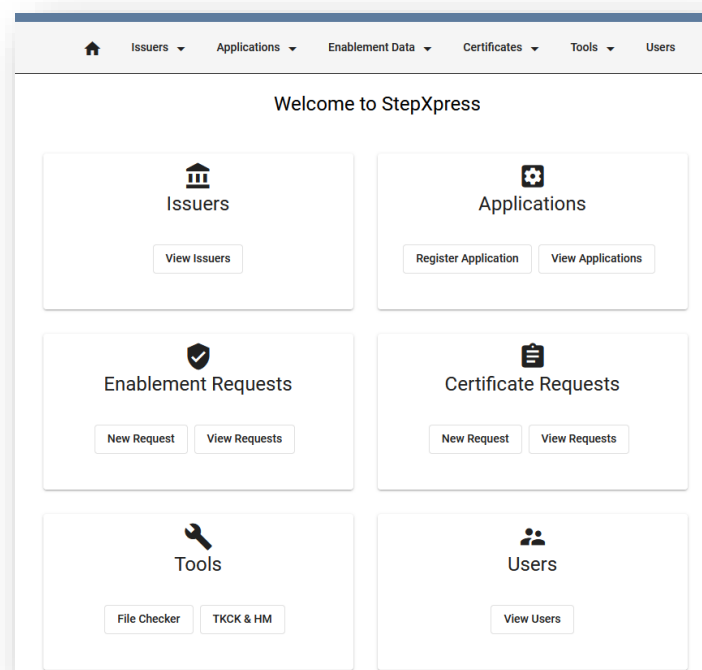
PLEASE NOTE: Three questions and answers must be submitted in order to save)

4. Press '**Save**'

3. Home Page – Welcome to StepXpress

The Home Page hub displays shortcuts to the main functionalities of the system (also accessible from the tabs on the top menu bar).

It is divided into sections so that a user (dependant on their selected roles) can complete from the following six activities:



3.1 Issuers

3.2 Applications

3.3 Enablement Requests

3.4 Certificate Requests

3.5 Tools

3.6 Users

3.1 Issuers

Click on **View issuers** to open a list of the issuers linked to the account. This page will show the following information

- *Issuer ID*
- *Issuer Name*
- *Issuer Reference*
- *Description*
- *Status (Active/On Hold)*

The Issuers are maintained by a System Administrator rather than an Account Administrator.

Within User Roles, it is possible to set up a user that may only access data for a Single Issuer within the account. This feature is useful when working with third party organizations that also need to access data, such as Service Providers.

If there are any questions regarding Issuers, please contact services@stepnexus.com

3.2 Applications

3.2.1 Introducing Applications

Applications to be loaded onto MULTOS cards need to be registered with StepXpress. The term 'register' in this context means to associate a specific Application with a specific Issuer.

Note that an Application must be registered in relation to each and every Issuer intending to use it.

What is Application Registration?

The Application Registration informs StepXpress about the characteristics of an Application (code size, data size etc.) and associates the Application with an Issuer. If any of the registered details change, the Application must be re-registered.

Each new registration creates a new variant of the Application. For example Applications where the data size changes would require a new variant to be registered.

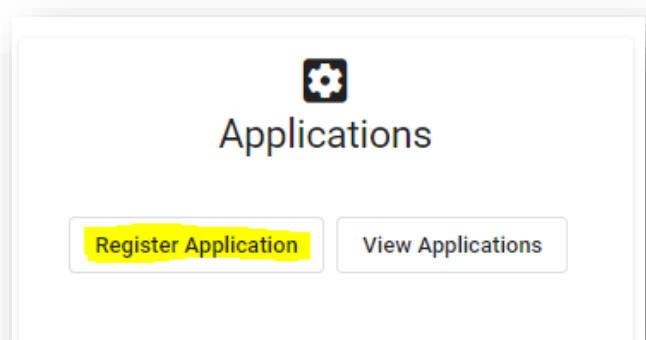
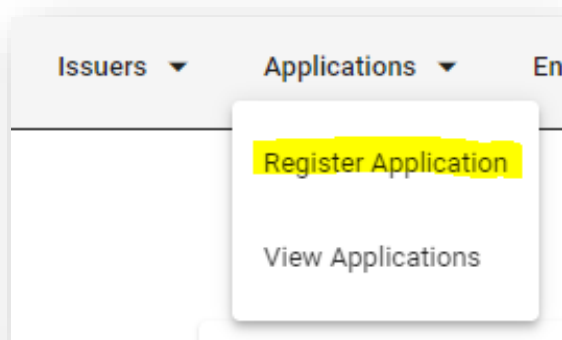
Applications must be registered in order to produce the correct Application Load or Delete Certificates. An Application Load Certificate contains essential details that will be verified by a card during Application loading.

Additionally, we have now combined the application registration process with the certificate requests section (see section 4.1.3 for more details). It is also now possible to create a single use application.

3.2.2 Creating a New Application

To create a new Application:

1. Select **Register Application** from either the Home page or the Applications page.



2. Once a reference has been entered. Select from the following options before clicking **Next**:

1 Step 1

Issuer 12000221-Test

Reference
Your reference for this application. Up to 50 characters.

Application Selection

☒ New Application

☐ Select Application

☐ Import file

Next

a. **New Application** – Request to create and register a new application.

b. **Previously Registered Application**

- If the Application is similar to an Application already registered a user can select the required Application from the drop down menu.

c. **Import a file.** An Application Definition File can be imported by browsing for the required file.

Please specify a file with .aif / .dat / .json / .xml file formats. The file must be less than 10 kb in size.

3. If this is a brand new Application users will need to complete all fields (see example below). If a user has uploaded a previously registered Application into the first screen, all the Application details will now be visible and can be amended accordingly.

Register new Application

← Back to List

Step 1 Define Application

Description
Application friendly name

Application ID
1-16 hex bytes.

Application Code Hash
Exactly 20 hex bytes.

Code Size	Data Size	Session Size	DIR Size	FCI Size
0	0	0	0	0

All sizes are decimals in the range 0 to 65535

Application Type **ALU Type**

Interface **ATR Historical Bytes**

Card Blocking **PIN Sharing**

Memory Allocation Method

Bytes

- ☐ Proprietary Load ☐ Strong Crypto
- ☐ Retain Session ☐ Maintain Selection
- ☐ Process Events ☐ Dual FCI
- ☐ Peripheral Access ☐ Card Manager

Previous Submit

4. Once all the details are entered correctly, click **Submit** to process this request.

5. A Status Report will be displayed to confirm that the Application has now been registered.

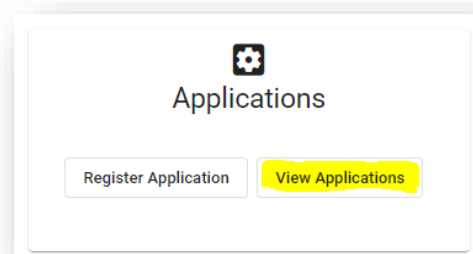
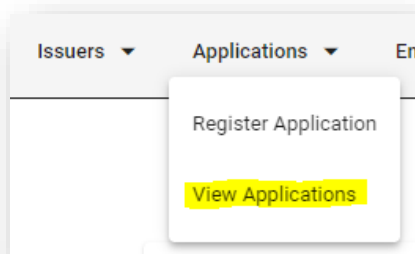
STEPXPRESS DC_User

Application Details [← Back to List](#)

Variant	2
Issuer	12000221-Test
Application ID	11
Description	set_atr_confidential
Code Size	134
Data Size	256
Session Size	0
Dir Size	16
Fci Size	16
Code Hash	515067E6FEF6DC547890E423B10A9F6D0A760B6
ALU Type	Confidential
ATR Historical Bytes	Writes to Primary ATR, Secondary ATR and ATS
Application Type	Standard
Dual FCI	<input type="checkbox"/>
Memory Allocation	<input type="checkbox"/>
Proprietary Load	<input checked="" type="checkbox"/>
Strong Crypto	<input checked="" type="checkbox"/>
Interface	Contact and Contactless
Card Block	<input type="checkbox"/>
Card Unblock	<input type="checkbox"/>
Retain Session	<input type="checkbox"/>
Maintain Selection	<input type="checkbox"/>
Process Events	<input type="checkbox"/>
Card Manager	<input type="checkbox"/>
Peripheral Access	<input type="checkbox"/>
PIN Access	Own PIN
Reference	test
Requested	May 6, 2022, 12:22:00 PM
Requested By	DC_User

3.2.3 View Details of an Application

- 1) Select **View Applications** from the Home page.



- 2) The Application details will be displayed on a list. There is also a search function on the top left to help filter what you are looking for.

Applications [New Request](#)

Filter applications

Reference	Application ID	Variant	Description	Issuer ID	Issuer Name	Created By	Created At	Delete
test_2	11	3	set_atr_confidential	12000221	12000221-Test	DC_User	06/05/2022, 12:27 PM	
test	11	2	set_atr_confidential	12000221	12000221-Test	DC_User	06/05/2022, 12:22 PM	
A0000000000001	11	1	set_atr_confidential	12000221	12000221-Test	jspeck	18/01/2022, 3:24 PM	
Application Reference I	11	1	set_atr_confidential	11000003	Issuer 11000003	jspeck	04/11/2021, 8:41 AM	

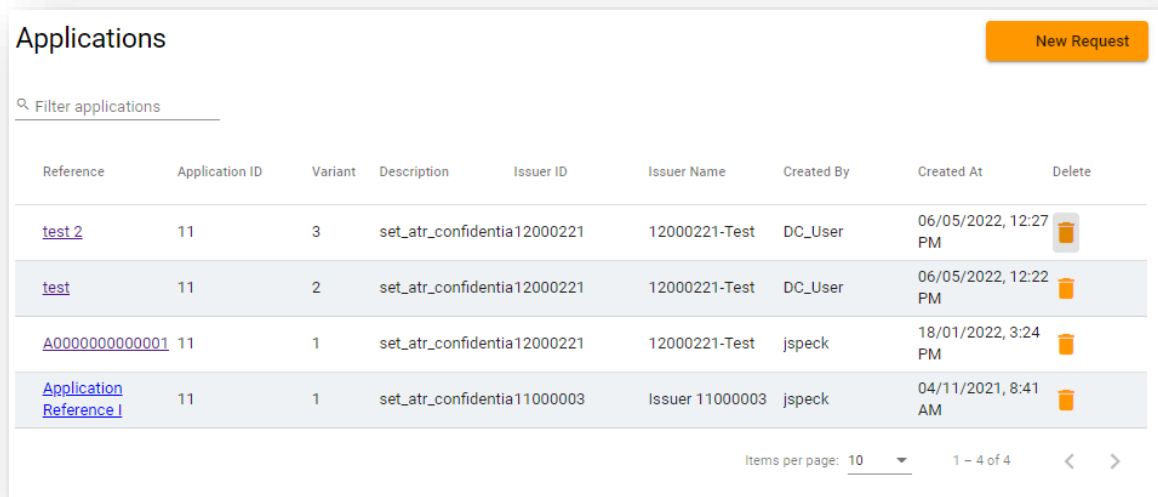
Items per page: 10 1 - 4 of 4

3.3 Delete Redundant Applications





All users with the role *Application Maintenance* will be able to delete applications registered under their account. By removing your redundant applications you will be able to locate your active ones with ease.

How to delete redundant applications

Step 1. Navigate to the View Applications Page



The screenshot shows the 'Applications' page with a search bar and a 'New Request' button. Below is a table with columns: Reference, Application ID, Variant, Description, Issuer ID, Issuer Name, Created By, Created At, and Delete. The table contains four rows of application data. The 'Delete' column contains a trash can icon for each row.

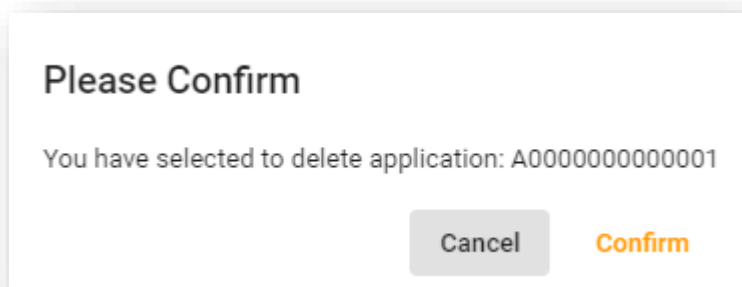
Reference	Application ID	Variant	Description	Issuer ID	Issuer Name	Created By	Created At	Delete
test 2	11	3	set_atr_confidentia12000221	12000221-Test	DC_User	DC_User	06/05/2022, 12:27 PM	
test	11	2	set_atr_confidentia12000221	12000221-Test	DC_User	DC_User	06/05/2022, 12:22 PM	
A00000000000001	11	1	set_atr_confidentia12000221	12000221-Test	jspeck	jspeck	18/01/2022, 3:24 PM	
Application Reference I	11	1	set_atr_confidentia11000003	Issuer 11000003	jspeck	jspeck	04/11/2021, 8:41 AM	

Items per page: 10 1 - 4 of 4

Step 2. Press the Delete Icon.



Step 3. Select **Confirm**.



A confirmation dialog box titled 'Please Confirm' with the message 'You have selected to delete application: A00000000000001'. It has two buttons: 'Cancel' and 'Confirm'.

Please Confirm

You have selected to delete application: A00000000000001

Cancel Confirm

3.4 Search function in multiple pages

There is a new search bar at the top of Enablement, Certificates and Applications pages. This is a live and interactive search – information will appear as you type, making it easier to find what you are looking for.

3.5 Enablement Data

3.5.1 Introducing Enablement Data

Enablement Data is a packet of data containing MULTOS information and a card number

(MCD Number). Using Enablement Data, a MULTOS card can be enabled with a corresponding MCD number in the Enablement Data.

Issuers and Bureaus obtain Enablement Data for each MULTOS smart card that they want to enable.

These functions available for enablement requests are dependent on the roles allocated by the Administrator.

3.5.2 New Enablement Data Request

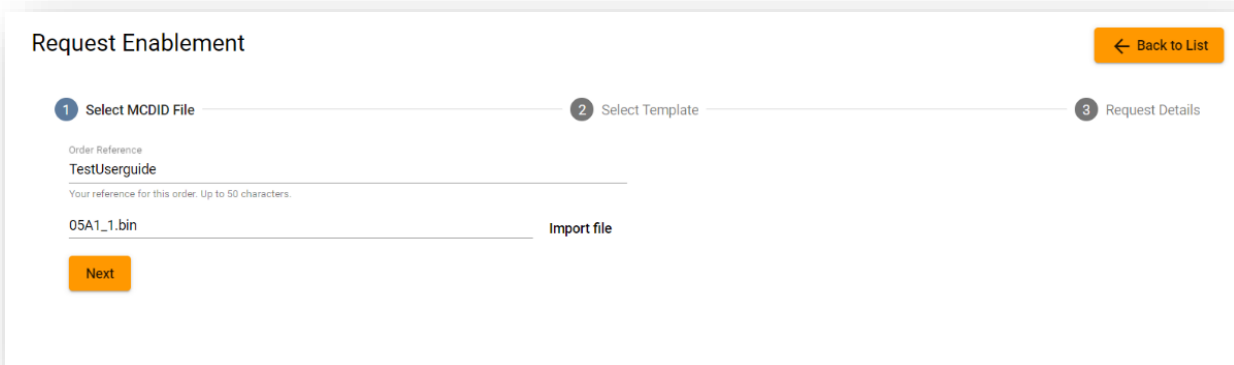
A new Enablement Data Request can be created either from the homepage or navigating into the Enablement data tab.

Warning: When creating a request for enablement data, please ensure to select the correct Issuer ID from the drop down menu, as once a request proceeds this will result in fees payable under the terms of the Subscription and User Agreement.

Before a user starts they must have a list of card identifiers from the manufacturer of the MULTOS smart cards they are using. All the cards listed in one request file must have the same MULTOS mask type. This will normally be the case where all the cards are from the same manufacturing batch.

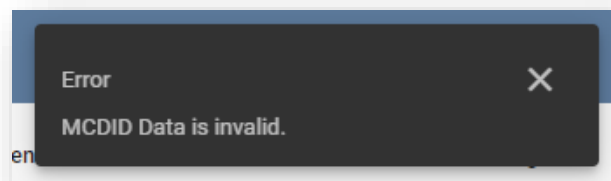
New enablement data Request:

1. Click on new request from homepage or Enablement data tab, the following screen will appear:



2. Enter the order reference and import the MCDID files.

StepXpress will perform initial validation of the MCDID file at this stage to check for basic errors. It will show an error message if there are any problems. If this occurs please see section 5.1.1 – File Checker for further evaluation of your MCDID File.



3. If file is OK, then Click **Next** to be taken to the *Select Template* section.

- On select template you can either continue without a Template, use an existing template or import a template from file. Click **Next** to proceed.

(For more details on Templates, see section 3.5.7)

Request Enablement

Select MCDID File 2 Select Template

Number Of Cards 1

Mask Details

Manufacturer ID 05
Mask Description 05A1
IC Type A1

Select Template

Templates allow you to automatically populate enablement request parameter settings.

☒ Continue without template

☐ Import file

Back **Next**

- Select the appropriate values that apply to the MULTOS mask for the Cards in the batch.

It is recommended that the default values are accepted, however, it is important to verify that these values meet requirements. Note also that "default values" are the pre-populated values of Product ID, ATRs, X & Y parameters and AMD.

Request Enablement

Select MCDID File 2 Select Template

Number Of Cards 1

Mask Details

Manufacturer ID 05
Mask Description 05A1
IC Type A1

Issuer 12000221-Test
Product ID 1

0-255 default is 1
Primary ATR 3B600000 (3B600000) ▾

Secondary ATR 3B600000 (3B600000) ▾

AMD 0133v001 (AMD DEFAULT 0133v001) ▾

X & Y Parameters X=0B Y=0C (XY1) ▾

Back **Submit**

- Press **Submit** to progress this request.

7. A confirmation page will display with the details of the request.

Enablement Request Details

← Back to List

Request Status

Your request has been submitted and is in a queue. You will receive an email once it has completed processing

Number of Cards	1
Mask Details	
Manufacturer ID	05
Mask Description	05A1
IC Type	A1
Request Details	
Issuer ID	12000221
Product ID	1
AMD	AMD DEFAULT 0133v001: (0133v001)
Primary ATR	3B600000: (3B600000)
Secondary ATR	3B600000: (3B600000)
X Param	0B
Y Param	0C
Order Reference	TestUserguide
Requested	Mar 25, 2022, 9:14:00 AM
Requested By	FS_User

Actions

[Export Template](#)
[Save as Template](#)

Processing includes further validation checks. Press **Back to List** to go back to the Enablement Data Page. The new request will be listed.

3.5.3 View Details of a Request

To view a particular Enablement Request, click on the **View Requests** button under the Enablement Requests tab. The Request details will be displayed on a list. Use the *filter requests* search to help locate your request.

Enablement Requests							+ New Request
Filter requests							
Order Reference	Issuer ID	Issuer Name	Created By	Created At	Quantity	Status	
test2904	12000221	12000221-Test	FS_User	29/04/2022, 12:57 PM	1	✓	
TestUserguide	12000221	12000221-Test	FS_User	25/03/2022, 9:14 AM	1	✓	
240322	12000221	12000221-Test	FS_User	24/03/2022, 3:31 PM	1	!	
18_01_2022_Web_Ser	12000221	12000221-Test	jspeck	20/01/2022, 9:50 AM	1	✓	
18_01_2022_Web_Ser	12000221	12000221-Test	jspeck	19/01/2022, 10:23 AM	1	✓	
6B71-18012022-RETRY	12000221	12000221-Test	GT_Admin	18/01/2022, 1:34 PM	1	✓	
6B71-18012022	12000221	12000221-Test	GT_Admin	18/01/2022, 1:30 PM	1	!	
AR Test	12000010	catherine test	AR_User	30/11/2021, 4:02 PM	1	✓	
Order Reference	11000003	Issuer 11000003	jspeck	12/11/2021, 10:11 AM	1	✓	
Order Reference	11000003	Issuer 11000003	jspeck	12/11/2021, 10:11 AM	1	⌘	
Items per page: 10 1 - 10 of 10 < >							

3.5.4 Status of a Request

The details and status displayed are highlighted by a colour and symbol for each request as follows:

Processed OK / Successful	=	GREEN / Tick Symbol
In process / not yet completed	=	WHITE / Hourglass Symbol
Completed with Errors	=	RED / Exclamation Mark (!)

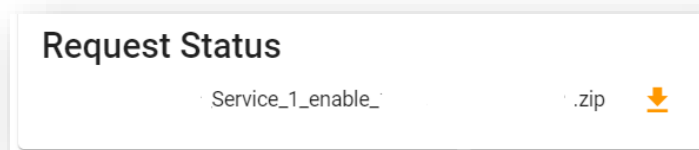
3.5.5 Notification of Request Completion

Once a request has been processed a notification e-mail will be sent stating that the request has been completed

3.5.6 Download Response Files

To download the response file:

1. Click on the order reference of the request that need to be downloaded.
2. Click on the **orange icon download button** in the request status field



3. Select the file to be collected by clicking on the file to download.

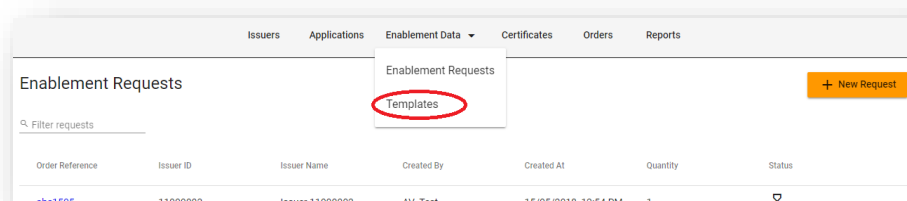
Response files will be available for download for a maximum of 28 days.

3.5.7 Templates

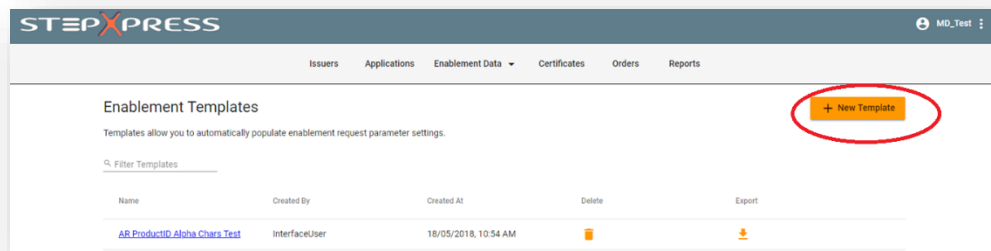
This new feature will allow you to save parameters on your account to request enablement. This will save time when raising multiple enablement requests, allowing you to make multiple requests with the same parameters. You can opt to create a template in advance or save a template at the end of your enablement request.

3.5.8 Saving a Template (In advance)

Step 1. Navigate to Enablement Data tab and click on **Templates**



Step 2. Select **New Template**



Step 3. Enter template details then Click **Next**

The screenshot shows the 'Create Enablement Template' form in the STEPXPRESS application. The page has a header with the application name and a navigation bar. Below the navigation bar, there is a section titled 'Create Enablement Template' with a sub-header 'Templates allow you to automatically populate enablement request parameter settings.' A 'Back to List' button is in the top right corner. The form is divided into two steps: '1 New Template' and '2 Template Details'. The 'New Template' step contains a 'Name' field with a 'Must be unique' note, a 'Select Mask' dropdown menu, and an 'Upload Template File' option with a 'BROWSE...' button. A 'Next' button is at the bottom.

Step 4. Enter details for request (Issuer, ID, AMD etc.) and click **Submit**

The screenshot shows the 'Create Enablement Template' form in the STEPXPRESS application, specifically the '2 Template Details' step. The page has a header with the application name and a navigation bar. Below the navigation bar, there is a section titled 'Create Enablement Template' with a sub-header 'Templates allow you to automatically populate enablement request parameter settings.' A 'Back to List' button is in the top right corner. The form is divided into two steps: '1 New Template' and '2 Template Details'. The 'Template Details' step contains a 'Template Name' field with the value 'Test'. Below this is a 'Mask Details' section with a table showing 'Manufacturer Id' (05), 'Mask Description' (0510), and 'IC Type' (10). The 'Issuer' field is set to '11000003: Issuer 11000003'. The 'Product ID' field is set to '1'. The 'Primary ATR' field is set to '3B600000 (3B600000)'. The 'Secondary ATR' field is set to '3B600000 (3B600000)'. The 'AMD' field is set to '0145v001 (AMD 0145v001)'. The 'X & Y Params' field is set to 'X=0B Y=0C (XY1)'. At the bottom, there are 'Back' and 'Submit' buttons.

Step 5. A summary of the template is then provided

Edit Enablement Template: Test 123

Templates allow you to automatically populate enablement request parameter settings.

Name
Test 123

Must be unique
Mask
0510

Issuer
11000003: Issuer 11000003

Product ID
1

O-255 default is 1
Primary ATR
3B600000 (3B600000)

Secondary ATR
3B600000 (3B600000)

AMD
0145v001 (AMD 0145v001)

X & Y Params
X=0B Y=0C (XY1)

Created By MD_Test at May 30, 2018, 8:55:07 AM

Submit

3.5.9 Saving a Template (at the end of an enablement request)

1. Navigate to the Enablement Request Details screen for your chosen request.

Enablement Request Details

← Back to List

Request Status

Items Processed Successfully	99
Items Processed With Errors	0
Items Left to Process	1

99%

Mask Details

Manufacturer Id	05
Mask Description	05A1
IC Type	A1

Request Details

Issuer ID	11000003
Product ID	1
AMD	AMD DEFAULT 0133v001: (0133v001)
Primary ATR	3B600000: (3B600000)
Secondary ATR	3B600000: (3B600000)
X Param	0B
Y Param	0C
Order Reference	Test
Requested	May 30, 2018, 10:00:00 AM
Requested By	MD_Test

Actions

Export Template

Save as Template

2. Select option to **Save as template**.

**NOTE: If preferable, you can still request enablement without using a template*

4. Certificate Requests

4.1.1 Introducing Certificates

An Application Load Certificate (ALC) is a certificate containing authorization for an application to be loaded onto one or more MULTOS Cards. If more than one variant of an application has been registered then the correct ALC must be used for the variant being loaded. Furthermore, the ALC grants authorization to load the Application only onto a particular series of MULTOS masks and not all types of devices. If a particular application is to be loaded by a particular Issuer onto many different MULTOS masks then it is likely that many different ALCs will be required.

4.1.2 StepXpress Certificate Screens

The Certificates page displays all Certificate Requests.

A new request can be made from either the Home page or the Certificates page.

StepXpress provides the ability to upload a group of MCD's and generate a per card ALC request.

Creating Load/Delete data requests may result in fees payable under the terms of the Subscription and User Agreement.

4.1.3 Requesting Certificates (ALC & ADC)

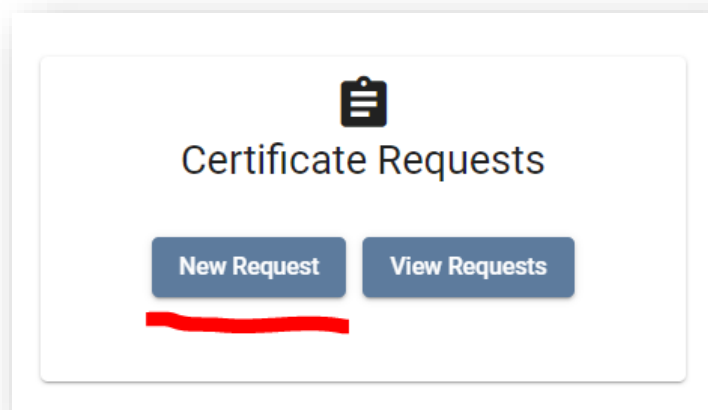
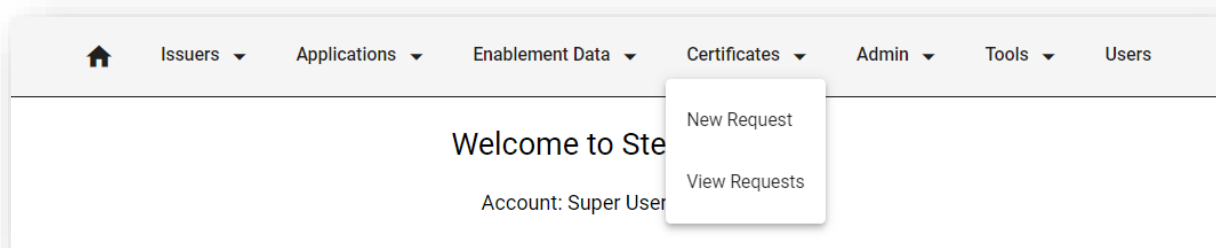
The application registration process is combined with certificate requests to make the certificate process easier and available in one place.

It is important to recognise that if more than one variant of an application has been registered then the correct ALC must be used for the variant being loaded. Furthermore, the ALC grants authorization to load the application only onto a particular series of MULTOS masks. If a particular application is to be loaded by a particular Issuer onto many different MULTOS masks then it is likely that many different ALC's will be registered.

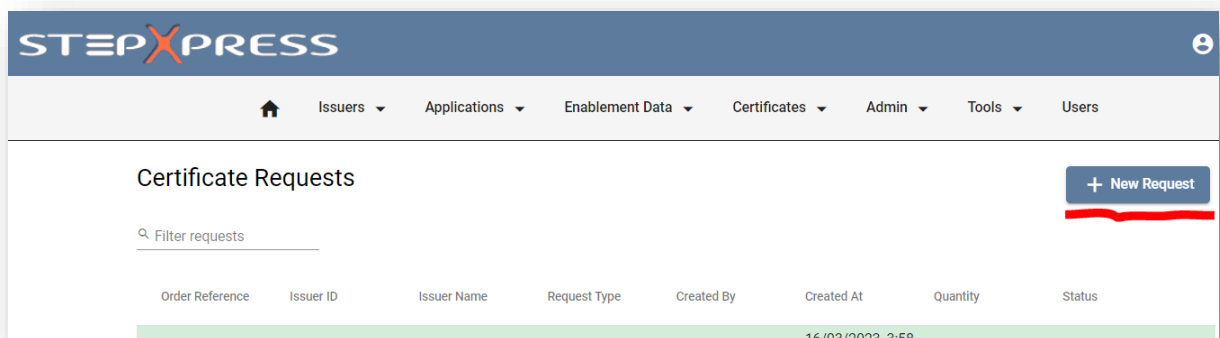
To create a request for ALC/ADC you will need to create a new Certificate Request.

To create a New Certificate Request:

a. On the Home page, go to the Certificates section and select **New Request** from the dropdown list.



b. If you are viewing certificates on the Certificates Requests page, click the **+ New Request** button.



Step 1. Select Issuer

Request Certificate

← Back to List

1 Select Issuer

2 Certificate Parameters

3 Summary

4 Processing

Order Reference

Your reference for this order. Up to 50 characters.

Issuer

☒ Select Application

☐ Application Definition file upload

Import file

Application Details

Description

Application friendly name

Application ID

1-16 hex bytes.

Application Code Hash

Code Size

0

Data Size

0

Session Size

0

DIR Size

0

Exactly 20 hex bytes.
FCI Size

0

All sizes are decimals in the range 0 to 65535

Application Type

ALU Type

Interface

ATR Historical Bytes

Card Blocking

PIN Sharing

Memory Allocation Method

Bytes

☐ Proprietary Load

☐ Strong Crypto

☐ Retain Session

☐ Maintain Selection

☐ Process Events

☐ Dual FCI

☐ Peripheral Access

☐ Card Manager

Next

Select an **Issuer** then **Select Application** or **ADF file** to upload. Application details will be populated accordingly. *Please be aware that the application details section at the bottom of Step 1 is only a summary based on the application you have selected / uploaded.*

Once the required details are in the fields, click **next**.

NOTE: If the application you are using has an ALU Type of 'Confidential' (or is set in this manner during Step 1) it will require the upload of an APK during Step 2. If the application is not Confidential then there is no need to upload an APK file during Step 2.

You can see the ALU Type of the application in the Application Details section of Step 1.

ALU Type

Please select an ALU Type

ATR Historical Bytes

PIN Sharing

Own

☐ Proprietary Load

☒ Strong Crypto

☐ Retain Session

☐ Maintain Selection

☐ Process Events

☐ Dual FCI

☐ Peripheral Access

☐ Card Manager

ALU Type

Confidential (Signed & Encrypted)

ATR Historical Bytes

PIN Sharing

Own

☐ Proprietary Load

☒ Strong Crypto

☐ Retain Session

☐ Maintain Selection

☐ Process Events

☐ Dual FCI

☐ Peripheral Access

☐ Card Manager

Step 2. **Certificate Parameters**

The request can be completed in one of two ways:

1. Select the device mask (or mask set) from the drop down menu, for non-card specific requests.

NOTE: If the ALU type of the chosen application is set to Confidential during Step 1 you must import an APK file at this stage to proceed. This is not required if the application's ALU type is not confidential.

The screenshot shows the 'Request Certificate' form at Step 2: Certificate Parameters. At the top right is a 'Back to List' button. Below the title is a progress bar with four steps: 1. Select Issuer, 2. Certificate Parameters (current), 3. Summary, and 4. Processing. The main section is titled 'Select Mask Set' with a red error message 'Please select a Mask Set'. Below this, there are two checkboxes: 'Request: Load' and 'Delete', both of which are checked. There is an 'APK file upload *' field with an 'Import file' button to its right. At the bottom, there is an 'Advanced Options' dropdown menu and two buttons: 'Back' and 'Next'.

2. Alternatively, click **Advanced Options** to enter a single MCDID or upload an MCDID batch file.

**PLEASE NOTE: The 'ALC History Required' tickbox should be selected only if the application specifically requires it. If the MCD is to retain a record of the ALC used to load this application, please check this box. This would prevent the same ALC from being used twice on the same MCD.*

Additionally, selecting both the 'Load' and 'Delete' boxes on this page will enable the creation of the ALC and related ADC in the same request.

Note: The Provider Key is the identifier of the key that is to be used for this request.

The screenshot shows the 'Advanced Options' form. It starts with a title 'Advanced Options' and a section 'Card Specific MCDID'. Below this is a note: 'If the certificate you are requesting is only for use with specific card(s) please use one of the options below to specify the MCDID(s) to use.' There are three radio button options: 'My certificate is not card specific' (selected), 'Single MCDID' (with a note '8 hex bytes'), and 'MCDID list file upload' (with an 'Import file' button). Below these are two 'Product ID' fields, each with a dropdown menu and a checked 'All products' checkbox. There is an 'Additional Products' button. The next section is 'Control Dates', which has a checked 'All control dates' checkbox and a date range selector with 'Month' and 'Year' dropdowns for both 'From' and 'To'. There is also an unchecked 'ALC History Required' checkbox. At the bottom are 'Back' and 'Next' buttons.

Once all the required fields are completed select **Next**.

Step 3. **Summary**

Request Certificate

← Back to List

1 Select Issuer 2 Certificate Parameters 3 Summary 4 Processing

Request Summary

MaskSet
Issuer
Order Reference
Product ID
Control Dates
Requires ALC
Requires ADC
ALC History

MaskSet: test
Issuer: ALL - ALL

Application Details

Application ID: A2000000000001
Description: App1
Code Size: 63432
Data Size: 35990
Session Size: 512
Dir Size: 156
Poi Size: 255
Code Hash: 1122334455667788990011223344556677889900
ALU Type: Unprotected
ATR Historical Bytes: Writes to Primary ATR
Application Type: Standard
Dual FCI: ☐
Memory Allocation: ☐
Proprietary Load: ☐
Strong Crypto: ☒
Interface: Contact only
Card Block: ☐
Card Unblock: ☐
Retain Session: ☐
Maintain Selection: ☐
Process Events: ☐
Card Manager: ☐
Peripheral Access: ☐
PIN Access: ☐
Own PIN: ☐

Back Submit

A **Request Summary** will be provided allowing the requester to check the values used in the request.

Click **Submit** to proceed.

Step 4. **Processing**

StepXpress will perform the initial validation checks of the Certificate file to check for basic errors. A Status Report will then be displayed to confirm that the request has been submitted.

Request Certificate

← Back to List

1 Select Issuer 2 Certificate Parameters 3 Summary 4 Processing

Request(s) Processing

See the status of your order below:

ALC

Your request has completed processing. To retrieve your order please download the following file:

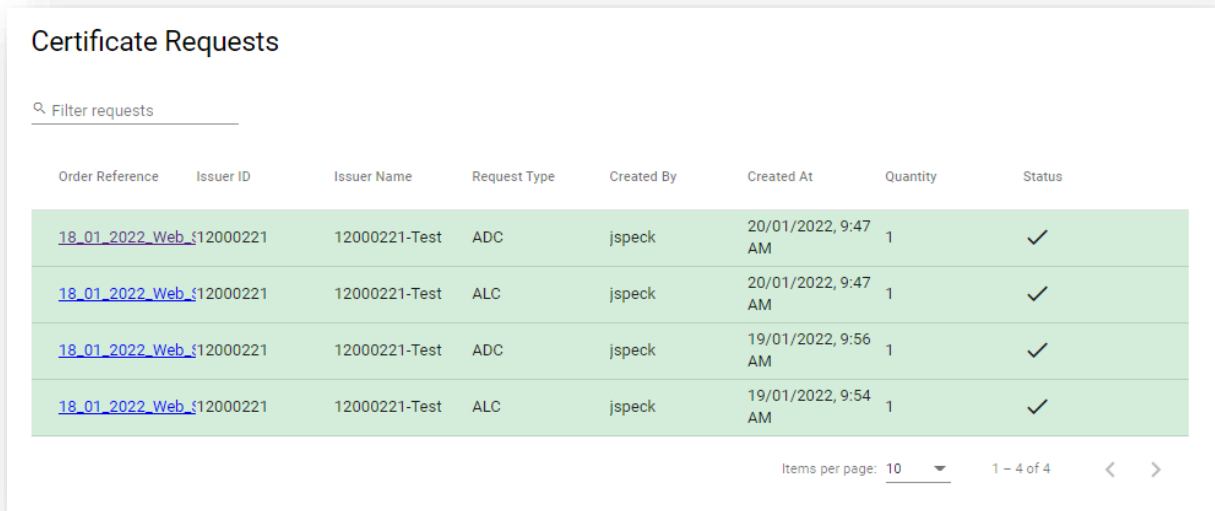
test_ALC_11000003_20180702.zip

← Back to List + Request Another Certificate

Press **Back to List** to go back to the Certificates page whereby the new request will be listed and you can see the status of the order (also see 1.9.4)

4.1.4 View Details of a Request

To view a particular Certificate Request, click on the **View Requests** button under the Certificate Requests tab. The Request details will be displayed.



Filter requests							
Order Reference	Issuer ID	Issuer Name	Request Type	Created By	Created At	Quantity	Status
18_01_2022_Web_Se12000221	12000221	-Test	ADC	jspeck	20/01/2022, 9:47 AM	1	✓
18_01_2022_Web_Se12000221	12000221	-Test	ALC	jspeck	20/01/2022, 9:47 AM	1	✓
18_01_2022_Web_Se12000221	12000221	-Test	ADC	jspeck	19/01/2022, 9:56 AM	1	✓
18_01_2022_Web_Se12000221	12000221	-Test	ALC	jspeck	19/01/2022, 9:54 AM	1	✓
Items per page: 10						1 - 4 of 4	< >

4.1.5 Status of a Request

The status of the latest requests is shown on the Certificates page. This is shown by a colour and Symbol for each request as follows:

Processed OK / Successful	=	GREEN / Tick Symbol
In process / not yet completed	=	WHITE / Hourglass Symbol
Completed with Errors	=	RED / Exclamation Mark (!)

4.1.6 Downloading Certificate Request

To download the response file:

1. Select the Certificate from the **Orders Reference** column on the left in the Certificate Requests Page

2. All response files available for download will be highlighted in Green with a link to click.

Certificate Requests

+ New Request

Filter requests

Order Reference	Issuer ID	Issuer Name	Request Type	Created By	Created At	Quantity	Status
18_01_2022_Web_Se12000221	12000221	12000221-Test	ADC	jspeck	20/01/2022, 9:47 AM	1	✓
18_01_2022_Web_Se12000221	12000221	12000221-Test	ALC	jspeck	20/01/2022, 9:47 AM	1	✓
18_01_2022_Web_Se12000221	12000221	12000221-Test	ADC	jspeck	19/01/2022, 9:56 AM	1	✓
18_01_2022_Web_Se12000221	12000221	12000221-Test	ALC	jspeck	19/01/2022, 9:54 AM	1	✓

Items per page: 101 - 4 of 4

Certificate Details
Back to List

Request Status
18_01_2022_Web_Service_1_ADC_12000221_20220120.zip

Mask Details

Application Details

Manufacturer ID68
Mask DescriptionTest
IC Type71
Request Details
Issuer ID12000221
Product ID1
Control DatesALL - ALL
Certificate TypeADC
ALC History Requiredfalse
Order Reference18_01_2022_Web_Service_1
RequestedJan 20, 2022, 9:47:00 AM
Requested Byjspeck

Application ID11
Descriptionset_atr_confidential
Code Size134
Data Size256
Session Size0
Dir Size16
Fci Size16
Code Hash515067E6FEF6DC547890E423B10A9F6DD0A760B6
ALU TypeConfidential
ATR Historical BytesWrites to Primary ATR, Secondary ATR and
ATSS
Application TypeStandard
Dual FCI
Memory Allocation
Proprietary Load
Strong Crypto
InterfaceContact and Contactless
Card Block
Card Unblock
Retain Session
Maintain Selection
Process Events
Card Manager
Peripheral Access
PIN AccessOwn PIN

3. Once on the Certificate Requests page you will be shown the status and will be given an option to click on the **orange download** button in the Request Status field.

Response files will be available for download for a maximum of 28 days.

5. Tools

Tools contains two functionalities – the file checker, and the TKCK & HM checker.

5.1.1 File Checker

The screenshot shows the STEPXPRESS File Checker interface. At the top is a blue header with the STEPXPRESS logo and a user profile 'User_Test'. Below the header is a navigation bar with links: Home, Issuers, Applications, Enablement Data, Certificates, Tools, Accounts, and Users. The main content area is titled 'File Checker' and contains a form with the following fields: 'MCDID File *' with an 'Import file' button, 'Max records *' with a value of '0', and a 'Number of records per file (0 = Default 20,000 records, maximum 150,000 records per file)' field. A 'Submit' button is at the bottom of the form.

The MCDID File Checker will allow you to check if the contents of a MCDID File are valid and can be used to request enablement. Invalid records are split from the valid to help identify issues and process correct files. A download option for both valid and invalid records is available.

This screenshot shows the 'File Checker' interface with the 'Results' tab selected. The 'MCDID File *' field contains '05A1_1.bin'. The 'Report' section displays the following information: 'Total Records in the MCDID File:...1', 'Total Duplicates Records Removed:...0', 'Total Invalid Records Removed:.....0', and '1 valid records have been split in 1 file(s) you can download'. Below the report, the 'Files ready to use' section shows a download link for '05A1_1_05-A1_1_1_2022-05-06.bin'.

Example 1
Valid File



This screenshot shows the 'File Checker' interface with the 'Results' tab selected. The 'MCDID File *' field contains '6B69_1.bin'. The 'Report' section displays the following information: 'Total Records in the MCDID File:...1', 'Total Duplicates Records Removed:...0', 'Total Invalid Records Removed:.....1', and '0 valid records have been split in file(s) you can download'. Below the report, the 'Invalid Records' section shows a message: 'This file contains the records which are deemed invalid because the mask has not been found in our database.' and a download link for 'invalid_6B69_1.bin'.

Example 2
Invalid File

5.1.2 TKCK & HM

The TKCK & Hash Modulus (HM) files are available to view from this page which is accessible by selecting the TKCK & HM button on the welcome page / tabs.

You will have the ability to search & filter the data files available and download these masks from the right hand column by clicking on the Device Mask.

 Issuers ▾ Applications ▾ Enablement Data ▾ Certificates ▾ Tools ▾		
Mask Data Files		
TKCK & HM		
 Filter Mask Data Files		
Device Mask	Description	Download
Items per page: 10 ▾ 0 of 0 < >		

6. Users

6.1 Account Administrator

The Account Administrator is responsible for managing the Users within their Account. When an Account is created, the default user is automatically assigned the Account Administrator role.

The Account Administrator:

- Can edit their own user details.
- Can edit other user details
- Can create users associated to own account.
- Can assign roles to users from this level down.
- Can create another Account Administrator.

6.2 Account User:

A user associated to a specific account with either access to a single issuer or all issuers on that account.

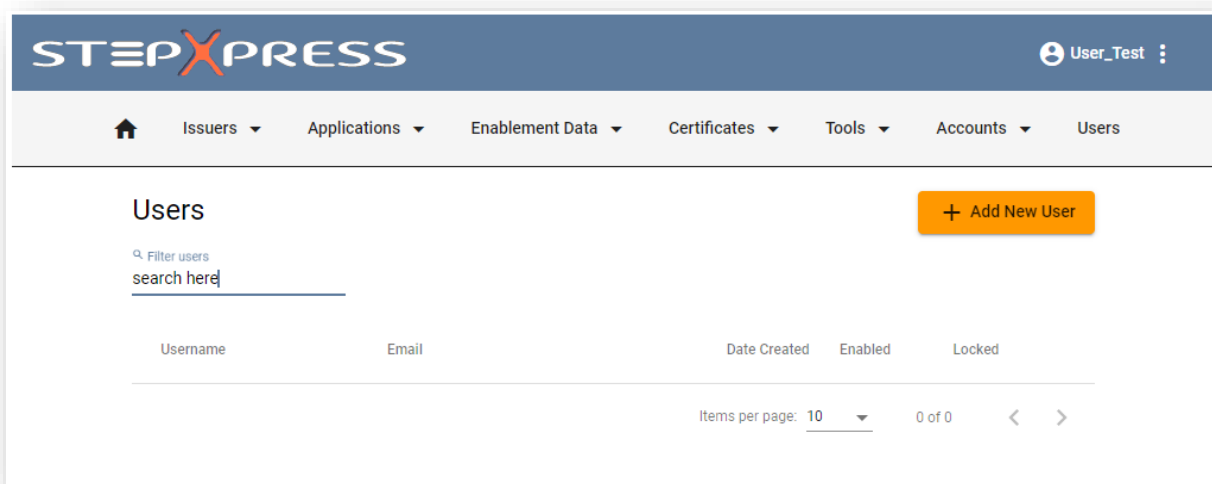
- This user does not have access to any administration options.
- If the user is associated to a single issuer, the user can only view/maintain for the specific issuer's data, depending on the issuer roles set by the "Account Administrator".

6.3 Managing Users

6.3.1 Users

Click on the users tab to see the list of users or enter the name in the search field.

A list of all users will appear.

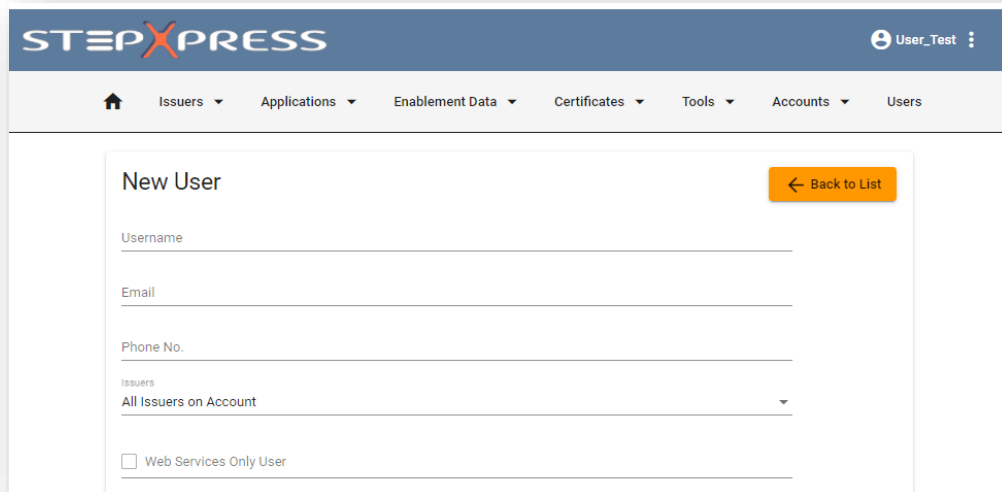


6.3.2 Add New Users

Before creating a new user, a valid email address must be known. The new user's login details will be sent to the email address used at setup.

The users' roles must also be decided upon.

**NOTE: If contacting StepNexus for user creation, you will need to complete a User Setup Form which StepNexus Services can provide.*



The screenshot shows the 'New User' form in the StepXpress application. The form is located within a navigation menu that includes 'Issuers', 'Applications', 'Enablement Data', 'Certificates', 'Tools', 'Accounts', and 'Users'. The form itself has a title 'New User' and a 'Back to List' button. It contains several input fields: 'Username', 'Email', 'Phone No.', and a dropdown menu for 'Issuers' (currently set to 'All Issuers on Account'). There is also a checkbox labeled 'Web Services Only User'.

1. Click on **add new users**
2. *enter the required fields*
3. *select the appropriate roles for the new user (see section 6.3.4)*
4. Click on **create a new user**

The new user will receive 1 email containing a link for the initial registration. the link will expire after 3 days. The user will be prompted to create a password for their account. *(Please see section 1.2 for more details)*

6.3.3 Edit a User

StepXpress has facilities to restrict the data and functions that a user can access.

Depending upon the user roles assigned, it may be possible that access is denied to a particular screen or data.

For example; it is possible to setup a User that may order Enablement data, but may not access the Applications or Certificates functions.

If roles need amending, the Account Administrator should be contacted. If the Account Administrator is not known please contact services@stepnexus.com for further assistance.

1. Search for the user in the search field - the user's details will then be displayed.
2. The Account Administrator can edit/update the following:
 - Email address
 - Phone number
 - Select which Issuer (*See Section 3.1*) is associated to the User
 - Enable the Web Service Only User function (see section 6.3.4 Web Service)
 - Generate and remove Tokens (see section 6.3.4 Web Service)
 - Reset a Password
 - Disable the user

STEPXPRESS AccountAdmin

Home Issuers Applications Enablement Data Certificates Tools Users

Edit User User3

Back to List

Username User3	Date Created 2022-05-03 01:57 PM
Email User3@testemail.cim	Last Login 0001-01-01 12:00 AM
Phone No. 98765432190	Last Password Changed 2022-05-05 01:51 PM
Issuers All Issuers on Account	Service Token c3896333-3437-4965-8960-42a83b24d10f

☐ Web Services Only User

User Roles

Generate Token **Remove Token**

Reset Password **Disable user**

6.3.4 Web Services

There is also the functionality to complete requests via Web Services. Web Services provides an automated systems interface that enables tighter integration with card management systems and can simplify the process of issuing MULTOS and step/one cards. The Web Services API provides programmatic access to perform enquiries and make requests using a simple, powerful and secure interface. If you desire access to Web Services you will need to request access by contacting services@stepnexus.com. After you have access to it, any user can be enabled as service user only by ticking the appropriate box. The user set up a Web service user only will require a Token.

6.3.5 Managing user roles

An Account Administrator has the ability to control how users have access to certain functions and data within their StepXpress account. This is achieved by setting their User Roles. Each User can be assigned one or more of the following roles on their account.

- Enablement Maintenance - User can maintain Enablement data.
- Issuers View - User can view Issuer data.
- Account administrator – the User will have Admin roles
- Enablement View - User can view Enablement data.
- Applications View - User can view Application data.
- Certificates View - User can view Certificate data.
- Certificates Maintenance - User can maintain Certificate data.
- Applications Maintenance - User can maintain Application data.

User Roles

☒ Select All

	Role Name
<input type="checkbox"/>	EnablementMaintenance
<input type="checkbox"/>	IssuersView
<input type="checkbox"/>	AccountAdministrator
<input type="checkbox"/>	EnablementView
<input type="checkbox"/>	ApplicationsView
<input type="checkbox"/>	CertificatesView
<input type="checkbox"/>	CertificatesMaintenance
<input type="checkbox"/>	ApplicationsMaintenance

Save changes

7. Multos Concepts

MULTOS Concepts provides basic background on MULTOS card technology.

MULTOS Card Personalization

Card personalization is the process of adding Applications, cardholder specific data and printing to a MULTOS card.

Personalization is usually performed on batches of cards at a Card Bureau.

MULTOS is an open standard and employs standard card personalization methods across all types of Application.

This standardization helps Issuers and Bureaus to minimize the investment in software and specialist skills required when working with new MULTOS Applications.

Enabling MULTOS Cards

Before MULTOS cards can be used, they must be associated with an Issuer.

During enablement, the card ATR is specified and also additional MULTOS data may be loaded.

Loading Applications

Applications to be loaded to MULTOS cards are termed Application Load Units.

Each new variant of an Application must be registered with StepXpress.

Loading on an Application requires the Issuer's permission in the form of an Application Load Certificate.

According to the type of Application Load Unit, a Key Transformation Unit (KTU) may also need to be supplied to load an Application.

7.1 Application Delete Certificates (ADC)

An Application Delete Certificate contains permission for an application to be deleted from one or more MULTOS cards.

The Certificate contains the Application ID (AID) of the application to be deleted.

To delete an application, the certificate is presented to a card. The card checks the certificate, and if valid, will delete the application.

7.2 Application Load Certificates (ALC)

An Application Load Certificate contains permission for an application to be loaded onto one or more MULTOS cards.

Neither StepXpress nor the Issuer needs to know the contents of the specific application for which they are providing the certificates. This allows the Application Provider to keep private the contents of the code and data being loaded.

7.2.1 Input data to request ALC

In creating the request for an ALC the main items to be determined are:

ROM ID – the version and implementation of MULTOS on which the Application is to be loaded.

Application ID and Application variant – which together identify the Application to be loaded (as previously registered with StepXpress).

Product ID – which enables the ALC to specify the set of cards the Application may be loaded to, based upon Product ID. It is possible to select 'all Product IDs' or 'a single product

ID within the specified range' or Click 'Advanced Options' to enter multiple (additional 7)

Product IDs.

Controls Data Dates - which enables the ALC to specify which MCDS the ALC works with based on when their MSM Controls were created. It is possible to select a specific Control

Date range or leave box ticked to select all Control Dates (default).

Single MCD – which enables the ALC to be restricted to a single MULTOS card (in which case the MCD number must be specified).

Application Provider Public Key (required for protected and confidential ALUs only).

The ALC also incorporates application specific information derived from the Application registration information – for example the size of the application.

The ALC on its own is of no use – it must be used in conjunction with an associated Application Load Unit. The card compares the information provided in the ALC and the data previously loaded to it at the Enablement stage.

7.2.2 How a card uses an ALC

The card checks the ALC against the card parameters created at the time of Enablement and also against the Application being loaded. The card will load the Application if the:

- Issuer ID matches the ALC Issuer ID.
- Card Product ID matches a Product ID constraints specified in the ALC.
- Card Enablement date matches the Enablement date(s) constraints specified in the ALC.
- Card MCD number matches the MCD number contained in the ALC (if specified).
- Application specific data (e.g. size) is consistent with the data in the ALU.
- An ALC contains a declaration of the memory required by the Application (for the creation of the security firewalls) and a flag which constrains the use of cryptography called from the MULTOS operating system by the Application. The latter is required to address regulatory restrictions associated with the export of high strength cryptography.

7.2.3 When new ALCs are required

New ALCs are required when:

- Any of the Application parameters change.
- If cards are enabled with new product IDs or dates that are not covered by the scope of the existing ALC.
- If a new MULTOS mask is used and the mask is not covered by the scope of the existing ALC.

Please note, if more than one variant of an Application has been registered then the correct ALC must be used for the variant being loaded. Furthermore, the ALC grants permission to load the Application only onto a particular series of MULTOS masks and not all types of device. If a particular Application is to be loaded by a particular Issuer onto many different MULTOS masks then it is likely that new ALCs will be registered.

7.3 Application Load Unit (ALU)

Applications are loaded to MULTOS cards as Application Load Units (ALUs).

Data Preparation and ALU Generation solutions will format Applications correctly for loading.

An Application Load Unit consists of code and data. The basic parameters of an Application must be registered with StepXpress prior to loading.

The ALU Type defines how you protect the source code of the Application.

There are three value; ALUs may be either 'unprotected', 'protected' or 'confidential'.

The Application Provider or Developer will advise the correct ALU Type for an Application.

In many cases Applications will contain data particular to the cardholder. MULTOS provides the flexibility to incorporate this data in an ALU prior to loading in a data preparation and ALU generation process.

Alternatively an Application can be loaded to the card in a 'generic' form and then subsequently customized to a particular cardholder.

Unprotected ALU

The source code is in clear text. This option should be selected if there is no reason to keep the Application code confidential or if the Application does not contain secret keys.

Protected ALU

A protected ALU is signed to protect its integrity in the loading process.

The source code is signed with the Application Provider Key. This ensures the integrity of the source code. It protects against the code being changed by third parties.

Confidential ALU

A confidential ALU is also signed and contains portions that are encrypted, typically in order to protect keys employed within the Application.

The source code is signed with the Application Provider Key and encrypted using a Key Transformation Unit. This ensures the confidentiality of the code. This protects the code from being read or changed by third parties.

Application Provider Key

If the ALU is 'protected' or 'confidential' the Application Provider will need to supply the Issuer with an Application Key which is incorporated into Application Load Certificate requests.

7.4 Creating a Confidential Application Load Unit

To create a confidential ALU, encryption is performed using the unique public key of the card.

This public key is provided by StepXpress and is contained within the response to a request for Enablement data.

The location of the encrypted sections of the code and data and the keys used to perform the encryption, are defined in a key transformation unit (KTU).

7.5 Application Loading

The high-level steps required to load an Application to a MULTOS card are as follows:

- Create an Application Load Unit (ALU). An ALU embodies the Application code, Application data, DIR record and FCI record.
- Register the Application with StepXpress for use by an Issuer.
- Request an Application Load Certificate (ALC) from StepXpress. An ALC authorizes the loading of an Application to a card.
- Load the ALU and ALC to the MULTOS card.

7.6 Application Signature

To create the Application Signature, the Application Provider signs the Application with the private key of an asymmetric key pair. The public key of this key pair must be provided for incorporation into the ALC request for the Application.

7.7 Application Registration

Applications to be loaded onto MULTOS cards need to be registered with StepXpress.

The term 'register' in this context means to associate a specific Application with a specific

Issuer. Note that an Application must be registered in relation to each and every Issuer intending to use it.

The Application Registration informs StepXpress about the characteristics of an Application (code size, data size etc.) and associates the Application with an Issuer.

If any of the registered details change, the Application must be re-registered.

Each new registration creates a new variant of the Application. A new variant will be required, for example, for Applications where the data size changes.

Registration associates an Application with a specific Issuer.

Applications must be registered in order that the correct Application Load Certificates can be produced. An Application Load Certificate contains essential details about the Application that will be verified by a card during Application Loading.

When an Application is loaded to a MULTOS card, the card checks that the details contained in the Application Load Certificate match the Application. If the details do not match, the card will reject the Application and not load it to the card.

When an Application should be registered

Applications must be registered before any Load or Delete Certificates can be ordered.

Provided the Application has been registered once, it is not necessary to re-register an Application every time a new Application Load or Delete Certificate is required. If multiple Load or Delete Certificates are required for the same Application then they can be requested without having to re-register the Application.

If, however, any of the registered characteristics of the Application change then it will be necessary to re-register the Application as a new variant.

7.8 Input Data for Application Registration

The Application Provider or Developer will provide specific information relating to the Application in order for the registration to be completed. Some personalization or data preparation systems also provide information for use in Application Registration.

If you are unsure what information to provide when registering an Application please contact the Application Provider or Developer.

Application ID

Code size

Data size

Session data size

DIR record size

FCI size

Code hash

Application selection type (shell, default, normal)

ALU type (unprotected, protected, confidential)

Whether the Application uses any of the MULTOS cryptographic primitives

Whether the Application is designed to communicate over contact or contactless interfaces

Whether the Application needs to alter the historic bytes of an ATR or ATS

The level of PIN Access supported

If Card Blocking and/or Unblocking is supported

If a session can be retained

If selection is maintained

If Dual FCI is supported

If memory can be allocated in blocks

7.8.1 Default and Shell Applications

The Application Type defines how the Application will act on power up.

There are three options:

1. Default Application – On power up this Application will be automatically selected, MULTOS will perform subsequent Application selections.
2. Shell Application - On power up this Application will be automatically selected, this Application must perform subsequent selection of other Applications.
3. Standard MULTOS Application – Requires the Application to be selected by MULTOS. There may only be one instance of a Default or Shell Application on a card.

7.9 Answer to Reset (ATR)

The Answer-To-Reset is a series of bytes sent by the card to the terminal after the card is first activated by the terminal and a reset signal is sent. These bytes inform the terminal of the operating conditions, options and requirements of the card during subsequent communications.

The ATR is specified in an Enablement Request for a card.

ATRs can be specific to a card platform, or to a combination of platform and Application.

MULTOS supports dual ATR functionality, that is, a second ATR may be available from the card. In this case there will be a Primary ATR and a Secondary ATR.

The Primary ATR is issued when a card is reset by a terminal after a power down (a 'cold' reset); the Secondary ATR is issued by a card after being reset by a terminal without the power being cycled first (a 'warm' reset).

If a Secondary ATR is not specified for a MULTOS 4 card, then StepXpress will set it to be the same as the Primary ATR.

7.10 Additional MULTOS Data (AMD)

Additional MULTOS Data (AMD) is a mechanism to supply additional information to a MULTOS card at the time when it is enabled.

Typically AMD is used to introduce a new or revised function to the operating system of a MULTOS card. The AMD mechanism is a secure and controlled method to apply a software 'patch' to a MULTOS card.

AMD is selected in the Enablement Data Request.

7.11 Enablement

The process of card Enablement takes a generic, stock MULTOS card and ties it to the Issuer.

Enablement data can be thought of as the birth certificate of the MULTOS card that gives it its identity.

Enablement data is generated by StepXpress based upon authorized instructions by the Issuer.

Loading of Enablement data is secured by the transit keys created at the time of manufacture.

After the Enablement process each card is tied to the Issuer, has a unique MULTOS card number, a unique asymmetric key pair and configuration data specified by the Issuer. The

Issuer can now issue cards safe in the knowledge that he is in complete control of what can be subsequently loaded to the card.

The Enablement process effectively achieves the following:

Sets the Issuer ID within the card.

Establishes the parameters within the card that govern how Application Load and Delete Certificates will work (with respect to Product ID and Enablement data date).

Configures the card answer to reset (ATR - Primary and Secondary).

This is a 'one-time' process and, therefore, care should be taken to configure the card correctly.

Enablement is achieved through applying MULTOS card Enablement data to each card.

Card specific Enablement data must be requested from StepXpress for each batch of cards to be processed. Therefore, the request for Enablement data includes a list of MCDIDs which identify all the cards in the batch.

7.11.1 What does Enablement Data include

Based on the file received from the Issuer, StepXpress will generate Enablement data for each chip represented in the MCDID list.

The card already possesses a unique identifier - the MCDID, but it requires a new one, one that identifies the Issuer to whom it belongs. Within this there are four fields:

1. Issuer ID - This is a unique 8 digit number that identifies the Issuer.
2. Issuer Product ID - Each card belongs to a single Product ID, one of 256 and its use is decided by the Issuer for ease of card management.
3. MCD Number - This is a unique card identity based on the MCDID injected by the Enablement Data.
4. The final field is the date on which the Enablement data was produced. This is to the granularity of one month.

The card is also given its own key pair. The public key is then certified by the KMA and used to secure the loading process. The Application loader can be confident that a specific card is legitimate and that the encrypted Application Load Unit can only be decrypted by that legitimate card.

The Enablement data for each card is encrypted by StepXpress using the card's unique transport key and sent either directly to the Bureau or to the Issuer. The encryption ensures that the Enablement data can only be loaded onto the card it is intended for.

The Bureau loads the data onto each MULTOS card. Once the data has been decrypted the card becomes activated and is now ready for Applications to be loaded.

8. Troubleshooting

8.1 Web Browser Support

StepXpress is designed to be supported using *Microsoft Edge & Windows 10*. However it should be expected to work on all modern web browsers.

8.2 Solving Common Problems and Errors

Error	Solution
Locked User	Contact the Account Administrator to enable the User ID (or Contact services@stepnexus.com)
Forgotten Password	<p>The password can be reset via the landing page by selecting the button Forgotten your password?</p> <p>A temporary password will be sent to your email. Once entered, you be prompted to enter one of your choice.</p>
Unable to view specific pages	You may not have the appropriate roles allocated to your user. Contact the Account Administrator to check (or Contact services@stepnexus.com)
Batch Status not updated (WHITE)	The request appears to be stuck 'in process' and is not completed. Send an e-mail to services@stepnexus.com and they can investigate.
Order not processed (RED)	Send an e-mail to services@stepnexus.com and they can investigate. We recommend providing the MCDID used if an enablement request.
Cannot request under Issuer required	The user role may have been set to only access a single Issuer. This can be confirmed by viewing user roles. If there is a need access to other Issuers please contact the Account Administrator or services@stepnexus.com .
Device Type Invalid	<p>The MULTOS mask specified is marked as invalid on the system.</p> <p>Contact services@stepnexus.com to request that the problem be investigated. Please provide details of the request.</p>
MISA not Recognised	The specified MULTOS mask is not correctly configured on the system. Contact services@stepnexus.com to request that the configuration for the mask is corrected. Please include details of the MULTOS mask.
Page Cannot Be Displayed	Internal firewall may block site. Ensure site is in the allow list
Correct AMD not available on request	<p>The specified AMD is not configured on the system.</p> <p>Change the AMD requested or contact services@stepnexus.com to request that the AMD is linked to the specified mask. Please include details of the MULTOS mask (or the Card Number) and the AMD.</p>
A Setting has been configured incorrectly	Ensure using correct browser. Contact services@stepnexus.com to ensure Active X settings in browser correct.
Not receiving automated emails	Ensure company spam filter not blocking emails. If not, contact services@stepnexus.com to investigate further.

Data unsuitable for this device type	<p>An AMD is registered on the system but it is not linked to the specified MULTOS mask.</p> <p>Change the AMD requested or contact services@stepnexus.com to request that the AMD is linked to the specified mask. Please include details of the MULTOS mask (or the Card Number) and the AMD.</p>
---	---

If further assistance is required please contact services@stepnexus.com