e-Submission System

User Manual

For

Authorised Person, Administrator, Security Officer and DI Users

October 2020
# Table of Contents

1 INTRODUCTION ......................................................................................................................... 4  
1.1 User Identification ................................................................................................................. 4  
1.2 User Types .......................................................................................................................... 5  
1.3 Site Conventions ................................................................................................................... 6  
1.4 Document Conventions ........................................................................................................ 8  

2 LOGIN TO E-SUBMISSION SYSTEM ....................................................................................... 9  
2.1 First-time login to e-Submission System ................................................................................ 9  
2.1.1 User Activation via Software Token (MobilePASS) ...................................................... 9  
2.2 Logging into the ESS ............................................................................................................. 15  
2.3 Login with SMS Password .................................................................................................... 17  
2.4 Forgot User ID ...................................................................................................................... 19  
2.5 Forgot User Password .......................................................................................................... 21  

3 COMMON ADMIN FUNCTIONS ............................................................................................... 23  
3.1 View Your Company’s Profile ............................................................................................... 23  
3.2 View and Update Your Own User Profile ............................................................................. 24  
3.3 Change Your Own User Password ....................................................................................... 25  

4 FOR AUTHORISED PERSON .................................................................................................. 26  
4.1 User Menu for Authorised Person ........................................................................................ 26  
4.2 Profile Admin ....................................................................................................................... 27  
4.2.1 Create a User ................................................................................................................ 27  
4.2.2 Delete a User ................................................................................................................. 29  
4.2.3 Approve User Creation by Security Officer ................................................................. 31  
4.3 Change of Administrator or Security Officer ...................................................................... 33  
4.4 Appointment of Agents for Publication Related Matters .................................................... 35  
4.4.1 Appoint an Agent ........................................................................................................ 36  
4.4.2 Edit an Appointment .................................................................................................... 39  
4.4.3 Delete an Appointment ............................................................................................... 40  
4.5 Appointment of Approvers .................................................................................................. 41  
4.5.1 Enable Appointment of Approvers function ............................................................... 41  
4.5.2 Appoint an Approver .................................................................................................. 44  
4.5.3 Edit an Appointment .................................................................................................... 46  
4.5.4 Delete an Appointment ............................................................................................... 47  
4.6 Appointment of Agents for Listing Related Matters ............................................................ 48  
4.6.1 Appoint an Agent ........................................................................................................ 49  
4.6.2 Edit an Appointment .................................................................................................... 50  
4.6.3 Delete an Appointment ............................................................................................... 51  
4.7 Approve to Revoke a Security Token .................................................................................. 52
1 Introduction

1.1 User Identification

Your company is required to register for access to the system. If your registration is successful, HKEX will create your Company Profile on the system. HKEX will also create user accounts for your company’s Authorised Person, Administrator, Security Officer, Disclosure of Interests (“DI”) user and up to 8 Publication Related Matter and up to 8 Listing Related Matter users. After registration, Security Officer and/or Authorised Person can create additional user accounts for new users of the company, if required.

The URL of the e-Submission System (ESS) is https://www1.eSubmission.hkex.com.hk. A user account includes a User ID, a User Password and a One-Time Passcode generated from security token that are required to login to the system.

A login user should be defined as an Authorised Person, Administrator, Security Officer, DI user in order to use the functions as set out in the respective sections in this manual.

For Publication Related Matter users, please refer to User Manual for Publication Related Matters for further details.

For Listing Related Matter users, please refer to User Manual for Listing Related Matters for further details.
## 1.2 User Types

The following table lists the user role of Authorised Person, Administrator, Security Officer and DI user in ESS.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorised Person (Primary Authorised Person and/or Secondary Authorised Person)</td>
<td>An Authorised Person is a person at a company who is the HKEX’s primary contact for subsequent administrative matters. Authorised Person can: - maintain user profile list, including create/delete user accounts, approve user creation by Security Officer and change of Administrator/Security Officer; - approve to revoke of user’s security token; - appointment of agents for Publication Related Matters; - appointment of approvers; and - appointment of agents for Listing Related Matters</td>
</tr>
<tr>
<td>Administrator</td>
<td>An Administrator is the person at a company who maintains the company’s details on the ESS. Administrator can: - update the company’s profile; - maintain the company’s “Related Stock Code List” (applicable for Main/GEM board and Exchange Traded Products issuers); - submit the request to HKEX for change of Authorised Person; - maintain submission template (applicable for Structured Product issuers); - view the submission log of Listing Related Matter ; - view the submission log of Publication Related Matter; and - view e-Form submission log.</td>
</tr>
<tr>
<td>Security Officer</td>
<td>The Security Officer is the person who controls the access rights and manages the assigned token of the other users of his/her company. Security Officer can: - unlock all user accounts (except own account); - update the user profile of Publication Related Matter users, Listing Related Matter users and DI users; - disable login the Publication Related Matter users and Listing Related Matter users (i.e. due to resignation); - submit request to Authorised Person to create user account; - submit request to Authorised Person to revoke user’s security token; and - assign a security token to a user.</td>
</tr>
<tr>
<td>DI user (only applicable to Listed Issuers)</td>
<td>DI User is a person at a company who has been delegated the right to receive an email notification and access (i.e. viewing or downloading) the complete set of DI notices and related documents when a DI notice concerning his/her company is received through the DION System.</td>
</tr>
</tbody>
</table>
1.3 Site Conventions

Before Login

After Login
Header

- Clickable link to Home Page of the HKEX website.

- Font size selection icon (i.e. Small/Normal/Large) to select the displayed font size of the Left Panel and the Content Frame of the ESS website. The font size of the button will remain intact even if the font size is changed. Normal font size is selected by default.

- Language selection icon (i.e. English and Traditional Chinese) to select the displayed language.

Left Panel

- Display the system date/time and general information.

Content Frame

Before login,

- Display the login page content and links to Login with SMS Password, Forgot User ID, Forgot User Password and Registration.

After login, the Content Frame will extend to the Left Panel for display the Function page content.

- Display the Login User Name and the system date/time at the top left.

System Message

- Error message is displayed on red message box.
- Information message is displayed on green message box.

Main Menu

- A drop-down menu will be displayed when placing the cursor over the menu item.

Footer Links

- Link to general information for user's reference.
1.4 Document Conventions

The following conventions will be used in this manual:

Menu Item

- In bold, e.g. Admin

Page

- In bold, italic, e.g. Company Profile

Field

- In italic, e.g. Company Website

Action Button

- In capital letters, e.g. MY PROFILE
2 Login to e-Submission System

You must login the ESS for profile maintenance. Open the web browser and enter the web address: https://www1.esubmission.hkex.com.hk. The ESS Main page (i.e. the login page) will be displayed.

2.1 First-time login to e-Submission System

You need to setup your security token on your first-time login to the ESS. Download the software token application “SafeNet MobilePASS” on your mobile device from App Store or Google Play™ before your first-time login.

2.1.1 User Activation via Software Token (MobilePASS)

1. At the login page, input your User ID. User Activation page will be displayed.
2. Fill in your Registered Email Address.
3. To setup your password, type in a new password in New Password and re-enter the new password in Confirm New Password.

NOTE:
User password is case-sensitive. It must be 8 to 15 characters long with a combination of letters (both upper & lower case) and number (0-9).

4. Click REQUEST. The Token Policy String will be displayed on User Activation page (see step 9 below).
5. Launch your MobilePASS in your mobile device.
6. Create a software token on your MobilePASS.

<table>
<thead>
<tr>
<th>Google Play™</th>
<th>App Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click on the top right corner and choose “Create Token” from menu bar.</td>
<td>Click “+” on the right menu bar.</td>
</tr>
</tbody>
</table>

Figure 2.3 MobilePASS Application Menu

7. On your MobilePASS, input your New Token Name and tap "Activate".

Figure 2.4 MobilePASS – Create New Token
8. On your MobilePASS, tap "Manual Enrollment". ("Auto Enrollment" is not applicable to ESS)

![Figure 2.5 MobilePASS - Token Enrollment](image)

9. Input the *Token Policy String* (generated in step 4) to the MobilePASS and tap "Continue".

![Figure 2.6 MobilePASS - Token Policy String](image)
10. An Activation Code will be displayed on MobilePASS screen. Enter the Activation Code on User Activation page. DO NOT tap “Continue” on MobilePASS screen until you have activated your account successfully (see step 14 below).

Figure 2.7 MobilePASS – Activation Code

11. Click REQUEST on User Activation page. A One-Time Password will send to your registered mobile phone number via SMS and to your registered email address via email. Input One-Time Password.

Figure 2.8 One-Time Password sent via SMS to registered mobile phone number

12. Click ACTIVATE.
13. If your user account has been activated successfully, the acknowledgement page will be displayed. You will be redirected to **User Main** page after 5 seconds.

![Successful activation screen](image)

**Figure 2.9 Successful activation screen**

14. Tap “Continue” on MobilePASS screen to generate the One-Time Passcode.

![MobilePASS – Generate the One-Time Passcode](image)

**Figure 2.10 MobilePASS – Generate the One-Time Passcode**

15. Login to ESS by inputting your **User ID**, **User Password** and **One-Time Passcode** generated from your MobilePASS.

![One-Time Passcode generated from MobilePASS](image)

**Figure 2.11 One-Time Passcode generated from MobilePASS**
NOTE:

- Following the steps above, you can set up multiple tokens (up to 10 user accounts) within a single MobilePASS application if you have different roles in the ESS.

- If your assigned token has been revoked previously (e.g. change of mobile device), your Security Officer has to assign a new token to you. You have to repeat the steps above to re-activate your user account.

- If you have tapped “Continue” on MobilePASS screen accidentally such that you could not enter the Token Policy String in step 9 or Activation Code in step 10 above, you need to remove the token from your MobilePASS application and restart the user activation from step 1 again. You can follow the steps below to remove a token.
  - Tap 📡 on the token screen;
  - Then, tap “Delete Token” (“Deactivate Token” is not applicable to ESS);
  - Tap “Delete” to confirm, your token will be removed from your MobilePASS. A deleted token cannot be used again.

![Figure 2.12 MobilePASS – Delete a token](image1)

- If you need to change the token name of your assigned token, you can follow the steps below.
  - Tap 🔄 on the token screen;
  - Then, tap “Change Token Name”;
  - Enter a new token name and tap “Continue”.
  - Your token will be displayed with the new token name.

![Figure 2.13 MobilePASS – Change Token Name](image2)
2.2 Logging into the ESS

1. On ESS Main page, enter your User ID, Password and One-Time Passcode (OTP) generated from the assigned security token and then click LOGIN.

![ESS Main Page](image)

**Figure 2.14 ESS Main Page**

**NOTE:**
- User Password is case sensitive.
- If an incorrect User Password and/or OTP generated from the security token was entered 5 consecutive times, your user account will be locked until it is unlocked by your company’s security officer. A locked account cannot be used.
- If the date when you last changed your password is more than 90 days ago, the system will require you to change your user password immediately. You will not be able to use any function on the ESS until your password is changed (refer to Section 3.3 “Change Your Own User Password”).
- If you leave the ESS idle for 30 minutes, you will be logged out automatically for security reason.
- Multiple logins are not allowed.
- If you have forgotten your User ID, you can click *Forgot User ID* to retrieve your login ID (refer to Section 2.4 “Forgot User ID”).
- If you have forgotten your User Password, you can click *Forgot User Password* to reset your password (refer to Section 2.5 “Forgot User Password”).
- If you cannot retrieve One-Time Passcode (OTP) from your assigned security token, you can click *Login with SMS Password* which serves as a back-up channel for you to access the ESS (refer to Section 2.3 “Login with SMS Password”).
2. **A Disclaimer** page will be displayed. Read the disclaimer statement carefully. Then click ACCEPT AND CONTINUE to accept the terms and conditions to proceed or click EXIT to go back to **Main page**.

![Figure 2.15 Disclaimer Statement](image)

3. **User Home** will be displayed.

![Figure 2.16 User Home Page – Authorised Person / Security Officer / DI User](image)

![Figure 2.17 User Home Page - Administrator](image)
2.3 Login with SMS Password

Login with SMS Password is a back-up channel for users to access the ESS when user cannot retrieve OTP from the assigned security token. User can click Login With SMS Password at the Main page to request a One-Time Password by providing User ID and Password. The One-Time Password will be sent through SMS to user’s registered mobile number.

To login the ESS with SMS Password,

1. Click Login with SMS Password at the Main page.

![Figure 2.18 ESS Main Page](image)

2. The Login with SMS Password page will be displayed. Enter your User ID, User Password and the characters in the image. Click SUBMIT.

![Figure 2.19 Login with SMS Password Page](image)
3. A One-Time Password will be sent to your registered mobile phone number via SMS. Input One-Time Password and click LOGIN.

![Login with SMS Password page](image)

Figure 2.20 Login with SMS Password page

4. A Disclaimer page will be displayed. Read the disclaimer statement carefully. Then click ACCEPT AND CONTINUE to accept the terms and conditions to proceed or click EXIT to go back to Main page.
2.4 Forgot User ID

1. If you have forgotten your User ID, you may click Forgot User ID at the Main page.

![Figure 2.21 ESS Main page](image)

2. The Forgot User ID page will be displayed. Fill in your User Name (User Given Name & Family Name), Registered Email Address, Company Code, the characters in the image and click SUBMIT.

![Figure 2.22 Forgot User ID page](image)
3. An email will be sent to the registered email address listing all User IDs matched with the information provided in step 2 above.

![Figure 2.23 Forgot User ID – System generated email](image)

Figure 2.23 Forgot User ID – System generated email
2.5  Forgot User Password

1. If you have forgotten your user password, you may click *Forgot User Password at Main page.*

![Figure 2.24 ESS Main page](image)

2. The *Forgot User Password* page will be displayed. Fill in your *User ID, Registered Email Address*, the characters in the image and click SUBMIT.

![Figure 2.25 Forgot User Password page](image)
3. An email contains the URL to reset your password will be sent to your registered email address. Click the URL in the email.

![Image](image1.png)

Figure 2.26 Forgot User Password – System generated email

4. The **Reset Password** page will be displayed. To reset your user password, input your **User ID**, **New Password** and **Re-type New Password**. Click **SUBMIT**.

![Image](image2.png)

Figure 2.27 Forgot User Password – Reset Password

5. After your User Password has been reset successfully, an acknowledgement page will be displayed.

**NOTE:**
- User password is case-sensitive. It must be 8 to 15 characters long with a combination of letters (both upper & lower case) and number (0-9). It shall not be the same as any of the last 5 passwords (including your Current Password).
- The URL to reset the User Password will be expired after 30 minutes.
3 Common Admin Functions

This section covers the common Admin functions which are applicable to Authorised Person, Administrator, Security Officer and DI user. For functions which are specific to certain user type, please refer to the corresponding Profile Admin section below.

3.1 View Your Company’s Profile

1. Select Profile Admin under Admin from Main Menu.

![Profile Admin menu](image1)

Figure 3.1 Profile Admin menu

2. The Company Details page will be displayed.

![Company Details page](image2)

Figure 3.2 Company Details page
3.2 View and Update Your Own User Profile

1. Select **Profile Admin** from **Admin** under Main Menu.

2. At **Company Details** page, click **MY PROFILE**.

3. The **User Profile** page will be displayed. The fields: **Salutation, Position, Phone No, Mobile No., Email** (Corresponding Address and Access to DI Data are applicable to Authorised Person only) can be amended as required. Other fields are displayed for reference only. Click **SAVE** after you have finished editing.

4. If your profile has been updated successfully, an acknowledgment message will be displayed.

5. Select **HOME** in the Main Menu on the top of the page to return to the **User Home** page.
3.3 Change Your Own User Password

1. Select Profile Admin under Admin from Main Menu.

2. At Company Details page, click MY PROFILE.

3. The User Profile page will be displayed. Click CHANGE USER PASSWORD.

4. The Change User Password page will be displayed. Input your Current Password. Type in a New Password and re-enter the New Password. Click SAVE.

![Figure 3.4 Change User Password page](image)

**NOTE:**
- User Password is case-sensitive. It must be 8 to 15 characters long with a combination of letters (both upper & lower case) and number (0-9). It shall not be the same as any of the last 5 passwords (including your Current Password). User Password is not allowed to change again within 24 hours.

5. If your password has been changed successfully, an acknowledgement message will be displayed.

6. Select HOME in the Main Menu on the top of the page to return to the User Home page.
4 For Authorised Person

This section only covers functions unique to the Authorised Person.

4.1 User Menu for Authorised Person

The Authorised Person user menu is subdivided into the following categories:

![Diagram of Authorised Person User Menu]

Figure 4.1 Authorised Person User Menu
4.2  Profile Admin

Under Profile Admin, you can create or delete a Publication Related Matter user, a Listing Related Matter user or a DI user of the company and approve the user creation initiated by Security Officer.

4.2.1  Create a User

1. Select Profile Admin from Admin under Main Menu.

![Figure 4.2 Authorised Person User Menu](image)

2. At Company Details page, click USER LIST.

![Figure 4.3 Company Profile page](image)

3. The User Profile List page will be displayed. Click NEW.

![Figure 4.4 User Profile List page](image)
4. A blank User Profile page will be displayed. Select the User Type. Enter the new user’s details, including User Name, Contact Information etc. After you have inputted the User Name, the User ID of the new user will be displayed immediately in the User ID field. **You should note the new User ID.** Click ADD.

5. If the user has been created successfully, an acknowledgement message will be displayed.

6. Click BACK TO HOME to return to the **User Home** page.

**NOTE:**
- Once the user account has been created successfully, the new user can immediately setup his/her token at the first-time login to the ESS (refer to “First-time Login to e-Submission System” on relevant user manual for user activation procedure).
4.2.2 Delete a User

1. Select Profile Admin from Admin under Main Menu.

2. At Company Details page, click USER LIST.

3. The User Profile List page will be displayed. You may enter User ID and/or User Name and click SEARCH to search for a specific user. Select the user to delete by checking the appropriate selection box and click USER DETAILS.

4. The User Profile page will be displayed. View and confirm the user profile to be deleted, then click DELETE.
5. The Confirmation dialog box will be prompted. Click CONFIRM.

![Confirmation dialog box]

Figure 4.9 Delete User - Confirmation

6. If the user account has been deleted successfully, an acknowledgement message will be displayed. The security token of the deleted user will be revoked at the same time.

![Acknowledgement message]

Figure 4.10 Delete User – Acknowledgement

7. Click BACK TO HOME to return to the User Home page.
### 4.2.3 Approve User Creation by Security Officer

1. Select **Profile Admin** from **Admin** under Main Menu.
2. At **Company Details** page, click **USER LIST**.
3. The **User Profile List** page will be displayed. The status of new user created by Security Officer is marked “Pending Approval” in red. Select the user by clicking the selection box and click **USER DETAILS**.

![Figure 4.11 User Profile List page](image)

4. The **User Profile** page will be displayed. Review the new user profile and click **APPROVE**. Alternatively, should you find the user detail need to amend, click **REJECT**.

![Figure 4.12 User Profile page](image)
5. If the request has been approved or rejected successfully, an acknowledgement message will be displayed. For rejected request, the Security Officer has to submit a new request for user creation.

![Figure 4.13 Approve User Creation by Security Officer – Acknowledgement](image)

6. Click BACK TO HOME to return to the User Home page.

NOTE:
- Once the user account has been created successfully, the new user can immediately setup his/her token at the first-time login to the ESS (refer to “First-time Login to e-Submission System” on relevant user manual for user activation procedure).
4.3 **Change of Administrator or Security Officer**

1. Select **Change of Administrator or Security Officer** under **Admin** from Main Menu.

![Change of Administrator or Security Officer menu](image1)

Figure 4.14 Change of Administrator or Security Officer menu

2. The **Change of Administrator or Security Officer** page will be displayed. Select **Request For** as “Change Administrator” or “Change Security Officer” as appropriate.

![Change of Administrator or Security Officer page](image2)

Figure 4.15 Change of Administrator or Security Officer page
3. Enter the user profile of the new Administrator or new Security Officer, including User Name, Contact Information etc. After you have inputted the User Name, the User ID of the new user will be displayed immediately in the User ID field. **You should note the new User ID.** Click CONFIRM.

![Figure 4.16 Request for Change of Administrator/ Security Officer](image)

4. The Confirmation dialog box will be prompted. Click CONFIRM to confirm the change.

![Figure 4.17 Change of Administrator or Security Officer page – Confirmation box](image)

5. If the Administrator or Security Officer has been changed successfully, an acknowledgement message will be displayed. The assigned token of original Administrator or Security Officer will be revoked at the same time.

![Figure 4.18 Change of Administrator – Acknowledgement](image)

6. Select HOME in the Main Menu to return to the **User Home** page.

**NOTE:**
- The new Administrator or Security Officer can immediately setup his/her assigned token at the first-time login to the ESS (refer to Section 2.1 “First-time Login to e-Submission System”).
4.4 Appointment of Agents for Publication Related Matters

Authorised Person of a listed issuer can appoint its representing agents to submit and/or approve documents on its behalf. You can also set criteria to control the submissions to be made by its appointed agents, either by the number of submissions or a time range or both. Upon appointment, Authorised Person of an agent can view assignment via this function.

The appointment is listed in the ascending order of status and its start time.

1. Select Appointment of Agents for Publication Related Matters under Admin from Main Menu.

   ![Figure 4.19 Appointment of Agents for Publication Related Matters menu]

2. For listed issuers, the Appointment of Agents for Publication Related Matters page will display a list of appointed agents, including the status and details of the respective appointments.

   ![Figure 4.20 Appointment of Agents for Publication Related Matters page (Listed Issuers)]

3. For agents, the Appointment of Agents for Publication Related Matters page will display a list of representing listed issuers, including the status and details of the respective appointments.

   ![Figure 4.21 Appointment of Agents Publication Related Matters page (Agents)]
4.4.1 Appoint an Agent for Publication Related Matters

1. Click CREATE at Appointment of Agents for Publication Related Matters page.

![Figure 4.22 Create new appointment](image)

2. The relevant input boxes will be displayed. Enter Company Code, the Company Name of the agent will be displayed. Alternatively, enter the Company Name to search for the agent. Company Name of the matched agents will be listed for selection.

![Figure 4.23 Search for Agent Company](image)
3. Select one of the Appointment Criteria to limit the appointment according to:-
   - "No. of Submissions Only" to pre-set the maximum number of submissions; or
   - "Time Range Only" to pre-set time range; or
   - "Time Range and No. of Submissions" to pre-set both time range and the maximum number of submissions.

Figure 4.24 Select Appointment Criteria

4. Depending on selected Appointment Criteria, input the appointment Start Time / End Time and/or No. of Submissions.

5. Assign the Appointment Type to determine the role of the agent by selecting:-
   - “Approval Only” to allow an agent to approve submissions on your behalf; or
   - “Submission Only” to allow an agent to make submissions on your behalf; or
   - “Submission & Approval” to allow an agent to make and approve submissions on your behalf.

Figure 4.25 Assign Appointment Type
6. Click CONFIRM.

7. If the appointment has been created successfully, an acknowledgement message will be displayed. You may continue to appoint more agents by repeating the above steps or click BACK TO HOME to return to the User Home page.

![Figure 4.26 Acknowledgement](image)

**NOTE:**

- Agent can submit/approve the submission on behalf of the listed issuer only if the appointment status is “Active”.
- The Appointment Status will become “Expired” if its preset time range (i.e. End Time) has expired or the No. of Submission become zero.
- Expired appointment will remain on the list for 30 days for record purpose.
- The count of the No. of Submission of the Agent’s appointment will be deducted by one in the following situation (including Submission for Publication and Correction of headline categories of a published document):
  - A submission is approved by the subject agent (either submitted by the issuer or other authorising agents); or
  - A submission is submitted by the subject agent and approved by the issuer.
4.4.2 Edit an Appointment

Authorised Person of a listed issuer can edit the active appointment. If the appointment of the agent has been expired, you have to create a new appointment for that agent (refer to Section 4.4.1 for details).

1. Select the appointment you wish to edit by checking the appropriate selection box and click EDIT at Appointment of Agents for Publication Related Matters page.

![Figure 4.27 Select appointment for editing](image)

2. Update the Appointment Criteria, Appointment Type, Start Time / End Time and No. of Submissions, where appropriate. Click CONFIRM.

![Figure 4.28 Edit an appointment](image)

3. If the appointment has been updated successfully, an acknowledgement message will be displayed. Click BACK TO HOME to return to the User Home page.

![Figure 4.29 Acknowledgement message](image)
4.4.3 Delete an Appointment

Authorised Person of a listed issuer can discontinue the appointment of your authorised agent by deleting its appointment. After the appointment has been deleted successfully, the agent is no longer able to represent the issuer to submit or approve any submission for Publication Related Matters.

1. Select the appointment you wish to delete by checking the appropriate selection box and click DELETE at Appointment of Agents for Publication Related Matters page.

![Figure 4.30 Select appointment for deletion](image)

2. The Confirmation dialog box will be prompted. Click CONFIRM to delete.

![Figure 4.31 Delete confirmation](image)

3. If the appointment has been deleted successfully, an acknowledgement message will be displayed. Click BACK TO HOME to return to the User Home page.

![Figure 4.32 Acknowledgement message](image)
4.5 Appointment of Approvers

Authorised Person of listed issuers and agents can exercise control over the approval of document submissions of each approver according to its own internal control procedures of your company by enabling the Appointment of Approvers function. You can set criteria to control approvals to be made by your appointed approvers, either by the number of approvals or a time range or both.

The default setting is **disabled** (meaning that every approver can approve document submissions without restrictions). Authorised Person should practically consider to decide “Enable” or “Disable” this function according to its own internal control procedure. If this function has been enabled, there would be a need to maintain the appointment list on a continuing basis.

4.5.1 Enable Appointment of Approvers function

To enable this function:

1. Select **Appointment of Approvers** under **Admin** from Main Menu.

   ![Appointment of Approvers](image1)
   
   **Figure 4.33 Appointment of Approvers menu**

   The **Appointment of Approvers** page will be displayed. It is set to be Disabled by default. Click the ENABLE radio option button to enable appointment of approvers.

   ![Appointment of Approvers](image2)
   
   **Figure 4.34 Appointment of Approvers page**
3. The Confirmation dialog box will be prompted. Click CONFIRM to enable.

![Figure 4.35 Enable the Appointment of Approvers – Confirmation](image)

4. After the **Appointment of Approvers** function has been enabled, you need to appoint at least one approver to ensure a smooth submission process. For detail, refer to Section 4.5.2 to appoint an approver.

**NOTE:**

- After the Appointment of Approvers function has been enabled, only the approver with “Active” appointment can approve submission for publication, correction of headline categories of a published document and submission for AP/PHIP.

- Email notification will be sent to Authorised Person and/or Approver of Publication Related Matter user reminding the expiry of the appointment according to the following scenarios:
  - Email notification will be sent to Authorised Person(s) and appointed approver on the 7 business days before the appointment will expire; and

```plaintext
HDI e-Submission System - Expiration of Approver Appointments (Reminder)

Dear Sir/Madam,

Please note that the following appointments will expire on 12 Oct 2020.
User ID: E2CE9DA4
User F4T name: Weng, Aqua
Appointment Period: 08/07/2020 to 15/10/2020

After expiry of the appointment, the related Approver will no longer be allowed to approve submission of documents for publication purpose. To ensure a smooth submission process, please immediately review and update the appointment list through the ‘Appr. Info’ function of the e-Submission System. For detailed instructions, please refer to the “User Manual for Authorized Person” which can be accessed through the link at the bottom of the e-Submission website.

If you have any queries, please call our hotline on 852-2888 8828 during the operational hours of the e-Submission System or the case officer of the Listing Department.

The Stock Exchange of Hong Kong Limited
13/10/2020

(Not an automatically generated email. Please do not reply directly to this email.)
```

![Figure 4.36 Expiration of Approver appointments (reminder)](image)
- Email notification will be sent to Authorised Person(s) and appointed approver on the expiration day of the appointment; and

Figure 4.37 Expiration of Approver appointments (today)

- Email notification will be sent to Authorised Person(s) on the next business day when all appointments of the company have expired.

Figure 4.38 Expiration of Approver appointments
4.5.2 Appoint an Approver

1. Click CREATE at Appointment of Approvers page. The relevant input boxes will be displayed.

![Appointment of Approvers page – Create new appointment](image)

2. All Approvers will be listed in the Approver pull-down menu. Select an approver from the list.

3. Select Appointment Criteria to limit the appointment according to:
   - "No. of Submissions Only" to pre-set the maximum number of submissions; or
   - "Time Range Only" to pre-set time range; or
   - "Time Range and No. of Submissions" to pre-set both time range and the maximum number of submissions.

![Appointment of Approvers page – Appointment Details](image)
4. Depending on selected Appointment Criteria, input the appointment Start Time / End Time and/or No. of Submissions. Click CONFIRM.

5. After the appointment has been created successfully, an acknowledgement message will be displayed.

6. Click CREATE to appoint more approvers or click BACK TO HOME to return to the User Home page.

NOTE:

- The count of the No. of Submission in the appointment will be deducted by one on the following situation:-
  - Approved submission for publication; or
  - Approved submission for correction of headline categories; or
  - Approved submission for AP/PHIP (applicable for agent only).

- The Appointment Status will become “Expired” if its preset time range (i.e. End Time) has expired or the No. of Submission become zero. **After expiry of the appointment, the related Approvers will no longer be allowed to approve submission of documents for publication purpose.**

- Expired appointment will remain on the list for 30 days for record purpose.

- To ensure a smooth submission process, an up-to-date appointment list should be maintained on a continuing basis.

- Authorised Person should consider its own operational needs and internal control procedures when presetting the Appointment Criteria.
4.5.3 Edit an Appointment

Authorised Person can only edit the active appointment. If the appointment has been expired, you have to create a new appointment for that approver (refer to Section 4.5.2 for details).

1. Select the appointment you wish to edit by checking the appropriate selection box and click EDIT at Appointment of Approvers page.

![List of appointments](Figure 4.42 List of appointments)

2. Update the Appointment Criteria, Start Time / End Time and No. of Submissions, where appropriate. Then, click CONFIRM.

![Edit appointment](Figure 4.43 Edit appointment)

3. If the appointment has been updated successfully, an acknowledgement message will be displayed. Click BACK TO HOME to return to the User Home page.

![Acknowledgement message](Figure 4.44 Acknowledgement message)
4.5.4 Delete an Appointment

You can discontinue the appointment of your approver by deleting his/her appointment. After the appointment has been deleted successfully, the approver is no longer able to approve any submission.

1. Select the appointment you wish to delete by checking the appropriate selection box and click DELETE at Appointment of Approvers page.

2. The Confirmation dialog box will be prompted. Click CONFIRM to delete the appointment.

3. If the appointment has been deleted successfully, an acknowledgement message will be displayed. Click BACK TO HOME to return to the User Home page.
4.6 Appointment of Agents for Listing Related Matters

Authorised Person of a listed issuer can appoint its representing agents to submit Listing Related Matters e-Form on its behalf. Upon appointment, Authorised Person of an agent can view assignment via this function.

The appointment is listed in the ascending order of status and its start time.

1. Select Appointment of Agents for Listing Related Matters under Admin from Main Menu.

2. For listed issuers the Appointment of Agents for Listing Related Matters page will display a list of appointed agents, including the status and details of the respective appointments.

3. For agents, the Appointment of Agents for Listing Related Matters page will display a list of representing listed issuers, including the status and details of the respective appointments.
4.6.1 Appoint an Agent for Listing Related Matters

1. Click CREATE at Appointment of Agents for Listing Related Matters page.

![Create new appointment](image)

Figure 4.51 Create new appointment

2. The relevant input boxes will be displayed. Enter Company Code, the Company Name of the agent will be displayed. Alternatively, enter the Company Name to search for the agent. Company Name of the matched agents will be listed for selection.

![Search Company](image)

Figure 4.52 Search Company

3. Input the appointment Start Time / End Time.

4. Click CONFIRM.

5. If the appointment has been created successfully, an acknowledgement message will be displayed. You may continue to appoint more agents by repeating the above steps or click BACK TO HOME to return to the User Home page.

![Acknowledgement message](image)

Figure 4.53 Acknowledgement message

**NOTE:**
- Agent can submit on behalf of the listed issuer only if the appointment status is “Active”.
- The Appointment Status will become “Expired” if its preset time range (i.e. End Time) has expired.
- Expired appointment will remain on the list for 30 days for record purpose.
4.6.2 Edit an Appointment

Authorised Person of a listed issuer can edit the active appointment. If the appointment of the agent has been expired, you have to create a new appointment for that agent (refer to Section 4.6.1 for details).

1. Select the appointment you wish to edit by checking the appropriate selection box and click EDIT at Appointment of Agents for Listing Related Matters page.

![Figure 4.54 Select appointment for editing](image)

2. Update the End Time and click CONFIRM.

![Figure 4.55 Appointment of Agents page – Edit appointment](image)

3. If the appointment has been updated successfully, an acknowledgement message will be displayed. Click BACK TO HOME to return to the User Home page.
4.6.3 Delete an Appointment

Authorised Person of a listed issuer can discontinue the appointment of your authorised agent by deleting its appointment. After the appointment has been deleted successfully, the agent is no longer able to represent the issuer to submit e-Form on Listing Related Matters.

1. Select the appointment you wish to delete by checking the appropriate selection box and click DELETE at Appointment of Agents for Listing Related Matters page.

![Figure 4.56 Select appointment for deletion](image)

2. The Confirmation dialog box will be prompted. Click CONFIRM to delete.

![Figure 4.57 Appointment of Agents – Delete confirmation](image)

3. If the appointment has been deleted successfully, an acknowledgement message will be displayed. Click BACK TO HOME to return to the User Home page.

![Figure 4.58 Acknowledgement message](image)
4.7 Approve to Revoke a Security Token

When Security Officer revokes the assigned token of your company’s user, a dialog box will be prompted for your approval:

![Figure 4.59 Approval of token revocation]

1. Input your User Password and One-Time Passcode (OTP) generated from your assigned token for approval. Click CONFIRM.

NOTE:
- You will only use the REQUEST ONE-TIME PASSWORD button as a back-up channel when you cannot retrieve OTP from the assigned token. Enter your User Password, then clicks REQUEST ONE-TIME PASSWORD button. An OTP will be sent to your registered mobile number via SMS. Enter the OTP in the One-Time Passcode field.
- For details of Security Officer to revoke an assigned security token, please refer to Section 6.3 “Token Management”.
5 For Administrator

This section only covers functions unique to the Administrator. For the procedures of download template, please refer to the Section 7 of User Manual for Listing Related Matters.

5.1 User Menu for Administrator

The Administrator user menu is subdivided into the following categories:

![Diagram of Administrator User Menu]

NOTE:

(1) Applicable to Structured Product Issuers only.

Figure 5.1 Administrator User Menu
5.2 Profile Admin

Under Profile Admin, you can maintain your company's profile and view your company's user profile list.

5.2.1 Maintain Company's Profile

1. Select Profile Admin under Admin from Main Menu.

![Figure 5.2 Profile Admin menu](image)

Figure 5.2 Profile Admin menu

2. The Company Details page will be displayed. Click AMEND COMPANY PROFILE.

![Figure 5.3 Company Details page](image)

Figure 5.3 Company Details page
3. The fields Company Name, Company Website, Address, and Fax No. can be amended as required. Others are for reference only. Click SAVE after you have finished updating your profile.

Figure 5.4 Amend Company Profile

4. If the company profile has been updated successfully, an acknowledgement message will be displayed.

5. Select HOME in the Main Menu to return to the **User Home** page.

Note:

- Under the Listing Rules, every listed issuer must have its own website for publication of regulatory filings. Listed issuers should fill in the *Company Website* field with the hyperlink which should direct investors to the regulatory filings, and not the home page of its company's website. The Exchange uses this information to update a list of company's website addresses on the HKEXnews website.
5.2.2 View User Profile List

1. Select Profile Admin under Admin from Main Menu.

2. The Company Details page will be displayed.

3. Click USER LIST. The User Profile List page will be displayed. You may enter User ID and/or User Name and click SEARCH to search for a specific user. Users who matched with the specified criteria will be listed.

4. Click BACK TO HOME to return to User Home page.
5.3 Change of Authorised Person

Administrator can submit the request to HKEX for a change of Primary or Secondary Authorised Person and add or remove the Secondary Authorised Person.

5.3.1 Change of Authorised Person or Add a Secondary Authorised Person

1. Select Change of Authorised Person under Admin from Main Menu.

2. The Change of Authorised Person page will be displayed. Select Request For “Change of Primary Authorised Person” or “Change of Secondary Authorised Person” or “Add Secondary Authorised Person” as appropriate.
3. Enter the new Authorised Person’s details, including User Name, Contact Information etc. The User ID of the new Authorised Person will be displayed after you have inputted the User Name.

![User Profile - Change of Authorised Person](image)

**Figure 5.8 Change of Authorised Person – Change or Add Authorised Person**

4. Click ADD FILES to upload the supporting document(s). Repeat until all file(s) are uploaded. Enter the File Description for each uploaded file. You may upload up to 5 supporting files (in PDF, TIFF, JPG or DOCX format) (such as board resolutions). The file size of each supporting file should not exceed 10MB.

5. Review the submission details. Click SUBMIT.

6. A Confirmation dialog box will be prompted. Click CONFIRM to submit the request.

![Confirmation](image)

**Figure 5.9 Change of Authorised Person page – Confirmation**

7. If the request has been submitted successfully, an acknowledgement message will be displayed.

![Acknowledgement](image)

**Figure 5.10 Change of Authorised Person – Acknowledgement**

8. Select HOME in the Main Menu to return to the **User Home** page.
NOTE:

- After successful submission, an email notification will be sent to the Administrator.

**Figure 5.11 Sample Email - Change of Authorised Person Request Acknowledgement**

- If the change of Authorised Person has been approved, an email notification will be sent to the Administrator and the New Authorised Person. You may also find the User ID of the new Authorised Person in the email notification. The previous Authorised Person will be removed from the User Profile List. The new Authorised Person can proceed to setup his/her security token on the first-time login to the ESS (refer to Section 2.1 “First-time login to e-Submission System”).

**Figure 5.12 Sample Email – Request for change of Authorised Person processed**
5.3.2 Remove Secondary Authorised Person

1. Select **Change of Authorised Person** under **Admin** from Main Menu.

2. The **Change of Authorised Person** page will be displayed. Select **Request For** “Remove Secondary Authorised Person”, the details of the Secondary Authorised Person will be displayed for reference.

   Click **ADD FILES** to upload the supporting document(s). Enter the File Description for each uploaded file, such as board resolutions. Click **SUBMIT**.

3. A Confirmation dialog box will be prompted. Click **Confirm** to submit the request.
4. If the request has been submitted successfully, an acknowledgement message will be displayed.

![Image](4. If the request has been submitted successfully, an acknowledgement message will be displayed.)

Figure 5.15 Change of Authorised Person – Acknowledgement

5. Select HOME in the Main Menu to return to the User Home page.

NOTE:

- After successful submission, an email notification will be sent to the Administrator.

![Image](NOTE: After successful submission, an email notification will be sent to the Administrator.)

- After the request for removal of the Secondary Authorised Person has been approved, an email notification will be sent to the Administrator. The User account of the Secondary Authorised Person will be removed from the User Profile List.

![Image](After the request for removal of the Secondary Authorised Person has been approved, an email notification will be sent to the Administrator.)
5.4 Maintain Related Stock Code

The “Related Stock Code List” is a list of stock codes maintained by listed issuers in ESS for their related listed issuers and listed securities. It is used for validating the stock codes entered into the “Stock Code of Related Issuer(s)” field in each submission. For the avoidance of doubt, the “Related Stock Code List” will not be applicable to debt issuers and structured product issuers.

To maintain the related stock code list:

1. Select Related Stock Code List Maintenance under Admin from Main Menu.

   ![Figure 5.18 Related Stock Code List Maintenance menu](image)

   Figure 5.18 Related Stock Code List Maintenance menu

2. The Related Stock Code Maintenance page will be displayed. The related stock code list will be displayed in the list in ascending order of stock code.

   ![Figure 5.19 Related Stock Code Maintenance page](image)

   Figure 5.19 Related Stock Code Maintenance page
5.4.1 Add a Related Stock Code

1. Click ADD at the Related Stock Code Maintenance page. The Related Stock Code input box will be displayed.

2. Enter the Stock Code and its stock short name will be displayed for reference. Click SAVE.

3. If the related stock code has been added successfully, an acknowledgement message will be displayed.

4. Click BACK TO HOME to return to the User Home page.

NOTE:
- If the related stock code is not a valid stock code, an error message will be displayed.
5.4.2 Remove a Related Stock Code

1. At the Related Stock Code Maintenance page, click REMOVE next to the stock code you wish to remove.

![Figure 5.23](image1.png)

Figure 5.23 Related Stock Code List Maintenance - Remove a related stock

2. A Confirmation dialog box will be prompted. Click CONFIRM to remove.

![Figure 5.24](image2.png)

Figure 5.24 Related Stock Code List Maintenance - Confirmation

3. If the related stock code has been deleted successfully, an acknowledgement message will be displayed.

![Figure 5.25](image3.png)

Figure 5.25 Related Stock Code List Maintenance – Acknowledgement

4. Click BACK TO HOME to return to the User Home page.
5.5 Document Submission

Administrator can view the submission log of both Listing Related Matter and Publication Related Matter of the company.

5.5.1 View Listing Related Matter Submission Log

The Administrator can view the document submission log in the last 365 days submitted by:-
- users of your company, regardless of whether they have been submitted on behalf of your own company or other companies; and
- users of other companies on behalf of your company.

To view the Listing Related Matter Document Submission Log:

1. Select **Listing Related Matter Submission Log** under **Document Submission** from Main Menu.

![Figure 5.26 Listing Related Matter Submission Log Menu](image)

2. The Document Submission Log page will be displayed. You can use different criteria (by **Subject Company Code**, **Case Number** and **Submission Date Range**) to filter the document submission log and click RETRIEVE. Search results matched with the criteria will be listed in descending order by submission date/time.

![Figure 5.27 View Document Submission Log](image)

3. Select HOME in the Main Menu to return to the **User Home** page.
5.5.2 View Publication Submission Log

An Administrator can view the submission history of Publication Related Matter, including the submission which is:-

- submitted / approved by the company user; and
- submitted / approved by the authorised agent on behalf of your company.

To view the Publication Submission Log:

1. Select Publication Submission Log under Document Submission from Main Menu.

![Publication Submission Log Menu](image)

2. The Publication Submission Log for the last 7 days will be listed by default. You can use different criteria (Submission Type, Submission Number, Stock Code of Issuer, Case Number, Tier 1 Headline and Last Modified Date Range) to filter the document submission log and then click SEARCH. Search results matched with the criteria will be listed in descending order by submission date/time, and then by ascending order of status will be listed.

![View Publication Submission Log](image)

3. Select HOME in the Main Menu to return to the User Home page.
5.6 View E-Form Submission Log

The Administrator can view the submission log in the last 3 months submitted by:-

- users of your company, regardless of whether they have been submitted on behalf of your own company or other companies; and
- users of other companies on behalf of your company.

To view the E-Form Submission Log:

1. Select **E-Form Submission Log** under **E-Form** from Main Menu.

![Figure 5.30 E-Form Submission Log Menu](image)

2. The E-Form Submission Log page will be displayed. You can use different criteria (by **Subject Company Code**, **Case Number** and **Submission Date Range**) to filter the E-Form submission log and click RETRIEVE. Search results matched with the criteria will be listed in descending order by submission date/time.

![Figure 5.31 E-Form Submission Log](image)

3. Select HOME in the Main Menu to return to the **User Home** page.

**NOTE:**
- Only Listing Related Matter user can view and download his/her own submitted e-Forms (in read-only PDF).
5.7 Submission Template Management (applicable to Structured Products issuers only)

Administrator of Structured Product Issuers can create up to 12 submission templates.

To view the list of submission templates:

1. Select **Submission Template Management** from Main Menu.

![Submission Template Management menu](image1.png)

Figure 5.32 Submission Template Management menu

2. The **Submission Template Management** page will be displayed. The Issuer Name template is listed at the top of the template list; other submission templates are listed in ascending order of the template name.

![Submission Template Management page](image2.png)

Figure 5.33 Submission Template Management page
5.7.1 Edit Issuer Name

The Issuer Name is used for auto-generated titles in Publication Related Matter submission, refer to Section 5.1 of User Manual for Publication Related Matters for further details. To edit the Issuer Name template:

1. On the Submission Template Management page, select the template name is “Issuer Name”. Click EDIT.

![Figure 5.34 Submission Template Management page – Select Issuer Name](image)

2. The Issuer Name Template page will be displayed. Update the English Issuer Name and Chinese Issuer Name where appropriate. Click SAVE.

![Figure 5.35 Issuer Name Template page – Edit Issuer Name](image)

NOTE:

- Update in the English and Chinese Issuer Name will not update the company name in the company profile.

3. If the Issuer Name template has been updated successfully, an acknowledgement message will be displayed on page will be displayed.

![Figure 5.36 Submission Template Management page – Acknowledgement](image)

4. Click OK to return to User Home page.
5.7.2 Create a Submission Template

1. At the Submission Template Management page, click NEW. A blank submission template will be displayed. Fill in the submission details, including the Template Name, Contact Information, Headline Categories, Title(s) etc. Click SAVE.

Figure 5.37 Submission Template Management page – Create Template

2. If the submission template has been created successfully, an acknowledgement page will be displayed.

Figure 5.38 Submission Template Management page – Acknowledgement

3. Click OK to return to Submission Template Management page.
5.7.3 Edit a Submission Template

1. At the Submission Template Management page, select the template you wish to edit by checking the appropriate selection box. Click EDIT.

   Figure 5.39 Submission Template Management page – Template selection

2. The Submission Template Management – Edit Template page will be displayed. Update the details of the submission template where appropriate. Click SAVE.

   Figure 5.40 Submission Template Management page – Edit Template

3. If the submission template has been updated successfully, an acknowledgement page will be displayed.

4. Click OK to return to Submission Template Management page.
5.7.4 Delete a Submission Template

1. At the Submission Template Management page, select the template (except the Issuer Name template) you wish to delete by checking the appropriate selection box. Click DELETE.

   ![Figure 5.41 Submission Template Management page – Template selection](image)

2. A Confirmation dialog box will be prompted. Click CONFIRM to delete.

   ![Figure 5.42 Submission Template Management page – Delete Template](image)

3. If the submission template has been deleted successfully, an acknowledgement message will be displayed.

   ![Figure 5.43 Submission Template Management page – Acknowledgement](image)

4. Select HOME in the Main Menu to return to the User Home page.
6 For Security Officer

This section only covers functions unique to the Security Officer.

6.1 User Menu for Security Officer

The Security Officer user menu is classified into the following categories:

![Security Officer User Menu Diagram]

Figure 6.1 Security Officer User Menu
6.2 **Profile Admin**

Under Profile Admin, you can perform the following user profile administrative function:

- submit the request to your Authorised Person for creation of a Publication Related Matter user, Listing Related Matter user or a DI user; and
- amend the user profiles of Publication Related Matter/Listing Related Matter users/DI user; and
- unlock other user accounts except own account; and
- disable / enable the login of the Publication Related Matter/Listing Related Matter user.

### 6.2.1 Request User Creation

To create a Publication Related Matter user, Listing Related Matter user or a DI user:

1. Select **Profile Admin** from **Admin** under Main Menu.

![Figure 6.2 Security Officer User Menu](image)

2. At **Company Details** page, click **USER LIST**.

![Figure 6.3 Company Profile page](image)
3. The **User Profile List** page will be displayed. Click NEW.

![Image 1](image1.png)

**Figure 6.4 User Profile List page**

4. A blank User Profile page will be displayed. Select the User Type. Enter the new user’s details, including User Name, Contact Information etc. After you have inputted the User Name, the User ID of the new user will be displayed immediately in the User ID field. **You should note the new User ID.** Click ADD.

![Image 2](image2.png)

**Figure 6.5 User Profile page**
5. If the request for user creation has been submitted, an acknowledgement message will be displayed. A new user is created with status “Pending Approval” marked in red in the User Profile List.

![User Profile List](image)

Figure 6.6 Create User - Acknowledgement

NOTE:
- The new user account creation is not completed yet. The Authorised Person of your company has to approve the user creation by the security officer (refer to Section 4.2.3 “Approve User Creation by Security Officer”).

6. Click BACK TO HOME to return to the User Home page.
6.2.2 Amend Users’ Profile

To amend the user profile of a Publication Related Matter user, Listing Related Matter user or a DI user:

1. Select **Profile Admin** from **Admin** under Main Menu.
2. At **Company Details** page, click **USER LIST**.
3. The **User Profile List** page will be displayed. Select the record you wish to amend by checking the appropriate selection box and click **USER DETAILS**.

4. The **User Profile** page will be displayed. Make the necessary amendment for the user - **Salutation**, **Position**, **Phone No or Email**. Other user details including **User Type**, **User ID**, **Family Name and Given Name**, **Mobile No.**, and **Access to DI** are not editable. Click save after you have finished amending the user profile.

5. If the user profile has been updated successfully, an acknowledgement message will be displayed.

6. Click **BACK TO HOME** to return to the **User Home** page.
6.2.3 Unlock a User

The user account will be locked when the user enters an invalid User Password and/or OTP generated by security token for 5 consecutive times. The user cannot login the system until the Security Officer unlocks the account.

To unlock a user:

1. Select Profile Admin from Admin under Main Menu.

2. At Company Details page, click USER list.

3. The User Profile List page will be displayed. The user’s Locked status is displayed as “Yes”. Select the locked user by checking the appropriate selection box and click UNLOCK.

   Figure 6.9 User Profile List page

4. If the user has been unlocked successfully, an acknowledgment message will be displayed. The user’s Locked status is displayed as “No”.

   Figure 6.10 Unlock User - Acknowledgement

5. Click BACK TO HOME to return to User Home page.
6.2.4 Disable / Enable a User Login

If a user resigns from the company, his/her account should be set to “resigned”. When the “Resign” flag is marked ‘Yes’, a user’s login will be disabled. This function can also be used to temporarily suspend a user from submitting documents through the ESS. If you have resumed the access of that user, you have changed the “Resign” flag to “No” such that s/he can login to ESS with the original assigned token.

The Security Officer can disable/enable the access to ESS of a Publication Related Matter user and Listing Related Matter user. To disable a user:

1. Select Profile Admin from Admin under Main Menu.
2. At Company Details page, click USER LIST.
3. The User Profile List page will be displayed. Select the record you wish to terminate by checking the appropriate selection box and click USER DETAILS.

![Figure 6.11 User Profile List page](image)

4. The User Profile page will be displayed. Change the radio button of Resigned from “No” to “Yes” and click SAVE.

![Figure 6.12 User Profile page](image)

5. If the user profile has been updated successfully, an acknowledgement message will be displayed.
6. Click back to home to return to the User Home page.
6.3 Token Management

Users’ tokens are managed by their company’s Security Officer. Security Officer can revoke a user’s token (to be approved by Authorised Person) and assign a new token to a user.

6.3.1 Change/Loss of Mobile Device

If your company’s user reported his/her mobile device (containing the software token) has been changed, lost or stolen, you should immediately revoke his/her token (to be approved by Authorised Person) to prevent unauthorized access.

1. Select **Token Management** under **Admin** from Main Menu.

2. The **Token Management** page will be displayed. A list of users in ascending order of User ID. Select the user who reported change/loss of mobile device by checking the appropriate selection box. Click **REVOKE TOKEN**.

3. A dialog box will be prompted for approval by Authorised Person. Authorised Person should enter the User Password and One-Time Passcode to confirm.
NOTE:
- If there is more than one Authorised Person in your company, select an Authorised Person by clicking the radio button.
- If the token to be revoked is belonged to the Authorised Person, s/he enter the User Password, then clicks REQUEST ONE-TIME PASSWORD button. An OTP will be sent to his/her registered mobile number via SMS. Enter the OTP in the One-Time Passcode to revoke the token.

4. If the token has been revoked successfully, an acknowledgement message will be displayed. The token status is now changed to “Revoked”.

Figure 6.16 Token Management page – Revoke Token Acknowledgement

5. If the user has been equipped with a new mobile device, you can assign a new token to the user. Select the user by checking the appropriate selection box and click ASSIGN TOKEN. A Token Assignment Detail dialog box will be prompted.

Figure 6.17 Token Management page – Select User to assign Software Token
6. Review the assignment detail and click Confirm.

![Token Assignment Detail dialog box](image1.png)

Figure 6.18 Token Assignment Detail dialog box

7. If the token has been assigned successfully, an acknowledgement message will be displayed. The token status is now changed to “Assigned”. New token User is required to re-activate his/her user account (refer to the section “First-time login to e-Submission System” of respective user manual for details).

![Token Management page – Assign Token Acknowledgement](image2.png)

Figure 6.19 Token Management page – Assign Token Acknowledgement

8. Select HOME in the Main Menu to return to the **User Home** page.

**NOTE:**

- To Revoke a user’s token, please refer to step 2 to step 4.
- To Assign a new token to a user, please refer to step 5 to step 7.
- Once the token has been revoked, user is required to re-activate his/her user account and set-up a new token in his/her mobile device. If user is using a same mobile device, the original token should be deleted. If user is equipped with a new mobile device, it is also recommended to uninstall the mobile app Safenet MobilePASS from his/her old mobile device.
7 For DI User

DI User has been delegated the right to receive an email notification and access (i.e. viewing or downloading) the complete set of DI notices and related documents when a DI notice concerning his/her company is submitted through the DION System. There are only user maintenance functions for DI user in ESS.

7.1 User Menu for DI User

The DI user menu is classified into the following categories:

![DI User Menu Diagram]

**NOTE:**
- For the Admin function of DI user, refer to Section 3 “Common Admin Functions” above.
8 Exit the System

It is recommended that you logout the system if you finish your session or are about to leave your computer unattended. The function that is partially completed will be lost when you logout the system. You should therefore complete the function before logging out of the system.

To exit the ESS:

1. Select LOGOUT in the Main Menu on the top of the page.

2. The ESS Main page will be displayed.

3. Close the browser window.