

## Getting Started For Terminal Operations

### SECURITY MANAGEMENT

The user profile maintenance functions will be primarily performed by the participants. HKEX shall assign a unique user ID for each delegated administrator (DA) of the Participant, while DA shall assign user IDs for their users. Each Participant should assign at least three delegated administrators (DAs), including one DA maker and two DA checkers, acting separately to perform the user profile maintenance functions including create, change and delete user profile. Please refer to table 3.2.1 for the full list of security functions.

To appoint a DA, a Participant must submit to HKEX the eService Form – DA 3 “CCASS / CCMS Terminal Delegated Administrator Application/ Maintenance Form” (as stated under “[HKEX Website](#)”). Upon receipt of the valid form, HKEX will provide to the Participant concerned a unique user ID for the DA. The Participant must ensure that its DA setup his password and the designated channel to obtain One-Time-Password (OTP) immediately upon receipt of the user ID. Please refer to Section 3.3 for detailed procedures.

The Security Management functions are accessible via a separate URL <https://www.ccass.com/dms>. The logon procedures for the Security Management are basically the same as those for accessing other CCMS functions, except that users should type <https://www.ccass.com/dms> instead of the CCMS URL in the box next to the address field when they logon to the security management functions. Please refer to Section 3.4 for the detailed logon procedures.

Table 3.2.1 lists the functions and reports related to Security Management transactions.

**TABLE 3.2.1: Functions and reports related to Security Management transactions**

	<b>Functions</b>	<b>Section in this User Guide</b>
Terminal operation functions	<ul style="list-style-type: none"> <li>• User Profile Maintenance</li> <li>• Get Authorisation Code</li> </ul>	<p style="text-align: center;">Section 7.2.1 Section 7.2.8</p>
Reports	<ul style="list-style-type: none"> <li>• User Group Listing (with Accessible CCMS Functions)</li> <li>• User Profile Listing</li> <li>• Disabled User Listing</li> <li>• User Profile Maintenance Report</li> </ul> <p style="text-align: center;"><i>The above reports are available for retrieval through the Security Management.</i></p>	<p style="text-align: center;">Section 7.2.2 Section 7.2.3 Section 7.2.4 Section 7.2.6</p>

Table 3.2.2 summarises the administration rights that can be assigned to the DAs regarding the Security Management functions to be performed by Participants.

**TABLE 3.2.2: Administration rights related to Security Management transactions**

Administration Rights	Function	Remarks
Maintain User Profile	<ul style="list-style-type: none"> <li>• Create User Profile</li> <li>• Input user name, email address, transaction limits and user groups and assign user ID</li> </ul>	Given that there is available user accounts. Maker-checker mechanism is provided.
	<ul style="list-style-type: none"> <li>• Change User Profile</li> </ul> Input / modify user name and email address, input transaction limits and user groups; unlock, enable or disable a user profile	Maker-checker mechanism is provided.
	<ul style="list-style-type: none"> <li>• Delete User Profile</li> </ul>	
	<ul style="list-style-type: none"> <li>• Enquire User Profile</li> </ul>	
	<ul style="list-style-type: none"> <li>• Get Authorisation Code</li> </ul>	For enquiry of the authorisation code by checker.
	View Listings <ul style="list-style-type: none"> <li>• User Group Listing (With Accessible CCMS Functions)</li> <li>• User Profile Listing</li> <li>• Disabled User Listing</li> </ul>	
	View Report <ul style="list-style-type: none"> <li>• User Profile Maintenance Report</li> </ul>	