RESERVE BANK INFORMATION AND TRANSFER SYSTEM

Member Administration User Guide

24 June 2023

R I T S

1. MEMBER ADMINISTRATION

This user guide should be read together with the *Overview of Functionality* guide.

1.1 Overview

The Member Administration module provides functions for the management and administration of user profiles in RITS.

Key points to note:

RITS Passwords must comply with the following criteria

- RITS Passwords should be created so that others have difficulty guessing.
- RITS Passwords must be 14 to 32 characters long and must contain a combination of at least three of the four character types: upper case letters, lower case letters, numbers and special characters – please see Appendix for a full list of allowable special characters.
- RITS Passwords are case sensitive.
- Users cannot re-use their 10 most recent passwords.

RITS Password expiry

- RITS Passwords expire after 90 days.
- The user is prompted to change his/her RITS password on each of the 5 days before the password expiry date.
- Once the RITS password has expired, the user must enter a new RITS password. Use the existing RITS password to logon and follow the prompts to set a new one. If the existing RITS password has been forgotten, contact the Password Administrator to set a new one.
- If the user cannot remember the old RITS password the user should ask the Password Administrator to set a new one.

Unsuccessful logon attempts

- After three consecutive entries of an incorrect RITS password (within a period of 24 hours), the user's status is automatically changed to *Inactive*. To regain access to RITS the Password Administrator is required to:
- set the User's status to Active in **User Privileges**; and
- set a new RITS password for the user in **Password Admin**.
- After 15 unsuccessful attempts to enter the Token Codeword the token is locked. To regain access to RITS, the user must:
  - Re-format the token and reset the Token Codeword;
  - contact the Password/Certificate Administrator to arrange for the revocation of the certificate and the issuance of a replacement RITS digital certificate;
  - complete a *Request to Revoke/Issue Certificates/Replace Expiring Certificates Form* and send it to the RITS Help Desk to enrol for a replacement RITS digital certificate.

RITS Password resets

- RITS Password resets by your Password Administrator or the RITS Help Desk requires the user to change the password at the next logon to RITS.

A user's status in RITS is managed by the Password/Certificate Administrator or RITS Help Desk. A user can have the following statuses:

- *Active* – User can access RITS, provided a digital certificate is valid.
- *Inactive* – User cannot access RITS, but the record of the user remains and it is possible to re-activate the user; and

User's links to branches

To perform certain actions the user must be linked to the branch that is engaging in the action.

These actions include:

- the entry, amendment and deletion, authorisation and enquiry in Cash Transfers;
- the management of the Cash Account Status of queued transactions;
- the setting of override statuses at the Cash Account level;
- the setting of Cash Account Sub-Limit;
- the participation in a batch in the Batch Facility; and
- the entering of batches as the Batch Administrator.

The Password Administrator manages users' links to branches in the function **User Privileges.**

Functions and Roles

- Functions are allocated via roles.
- The Password Administrator is responsible for allocating roles.
- Every user is allocated the role – All Users (except for users that will only have the role Overnight Enquiry or Limited Overnight Enquiry). This provides the user with some basic functions and activates the Main menu.
- Functions contained in a role can be viewed in the function User Privileges, by selecting a user and accessing the Roles for this User button. Select a role to view the functions in that role.
- No user can allocate roles to himself or herself.

Authorisations

- The Member decides the functions that must be authorised. The RITS Help Desk is responsible for entering the requirement into RITS, on written instructions from the Member.
- To give a user the ability to authorise cash transfers, manual FSI entry or manual FRI entry, the Password Administrator allocates the role Authorise Cash Transfer Entry, Manual FSI Authorisation or Manual FRI Authorisation.
- To give a user the ability to authorise any other function, the Password Administrator allocates the role – **Authoriser** and selects the functions that the user can authorise. This is done by selecting the **Authorisations** button in the **User Details** screen of **User Privileges** to access the function selection screen.
- Password Administrators cannot allocate authorisation privileges to themselves.

Certificates

- Certificates are managed by the Password/Certificate Administrator in the function **User Privileges**.
- Certificates will expire two years from the certificate collection date.
- The Password/Certificate Administrator activates a certificate by entering the Activation Code.
- The Password/Certificate Administrator can also revoke a certificate. A user cannot access RITS with a revoked certificate, but if the user is already logged on to RITS when the certificate is revoked, only enquiries can be performed.
- A replacement for a revoked certificate will take approximately 20-30 minutes to be issued.
- Certificates can have the status:
    - *Pre-enrolled* – following the creation of a new RITS user, the RITS user is pre-enrolled to obtain a certificate. This pre-enrolment is done by the RITS Help Desk.
    - *Collected* – the user has enrolled for their certificate and it has been downloaded to their token, but is awaiting 'activation' by the Password/Certificate Administrator in **User Privileges**.
    - *Active* – the certificate is 'live'.
    - *Revoked* – the certificate can no longer be used to access RITS.
    - *Expired* – the certificate can no longer be used to access RITS.
- Three months before the expiry of a certificate the user and their Password Administrator(s) are reminded by email to obtain a new certificate. The new certificate is obtained in the same way as the first certificate. The new certificate remains in collected status until it is activated. Upon activation, the old certificate is automatically revoked. The user must use the Token Administration functionality to delete the old certificate from the USB token.

Variable session time-out

- After 15 minutes (the default setting) of inactivity during a session, the user is automatically logged out of RITS.
- Password Administrators may extend this to 30 minutes or 60 minutes for selected users who, because of their work, spend extended periods of time in RITS.
- Because extended settings impact system performance and raise potential security risks, it is recommended that Administrators allocate extended session time-outs to selected users only.
- Users who have been granted extended session time-out should ensure the security of their RITS login by removing the token when they leave their PC.
- The approach adopted by Members should be consistent with their own internal security policies.

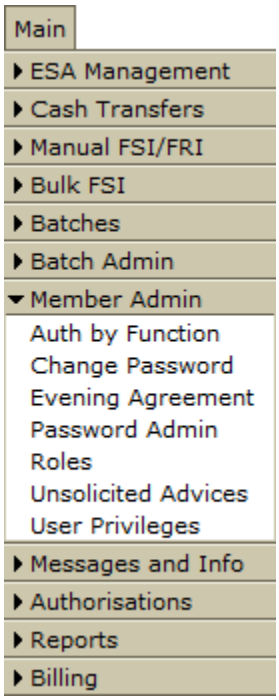
1.2 Available functions

- **Auth by Function** – view the functions that require an authorisation as determined by the Member. See the *Authorisations User Guide* for details of this function.
- **Change Password** – permits a user to change his or her own password.
- **Evening Agreement** – enter into, or cancel the obligation to participate in the Evening Session.
- **Password Admin** – permits the Password Administrator to give a new password to a user.
- **Roles** – view the roles that are available to Members and the functions that are contained in each role.
- **Unsolicited Advices** – manage the selection of Automated Information Facility messages and LVSS advices and responses.
- **User Privileges** – used by the Password/Certificate Administrator to:
  - maintain user details (including the status of the user);
  - set extended session time-out to selected users;
  - allocate user links to branches;
  - allocate roles (functions);
  - specify the functions that the user can authorise;
  - activate digital certificates on behalf of users; and/ or
  - revoke digital certificates.

A view only version of this function is available to all users.

1.3 RITS Menu

After logging on to RITS, the Main menu is displayed on the left-hand side of the screen. Select the **Member Admin** tab to expand the menu as displayed below.



1.4 RITS function descriptions

RITS Function	Description
Auth by Function	View the functions that require an authorisation.
Change Password	User changes own password.
Evening Agreement	Enter into or cancel the obligation to operate in the Evening Session.
Password Admin	Password Administrator resets or changes a user's password.
Roles	View the roles that are available to users and the functions that are contained in each role.
Unsolicited Advices	Maintain the selection of Unsolicited Advices in the Automated Information Facility and for Low Value Settlement Service (LVSS) messages.
User Privileges	Maintain user details, allocate user links to branches, allocate roles and specify the functions that the user can authorise, activate digital certificates on behalf of users and revoke digital certificates.

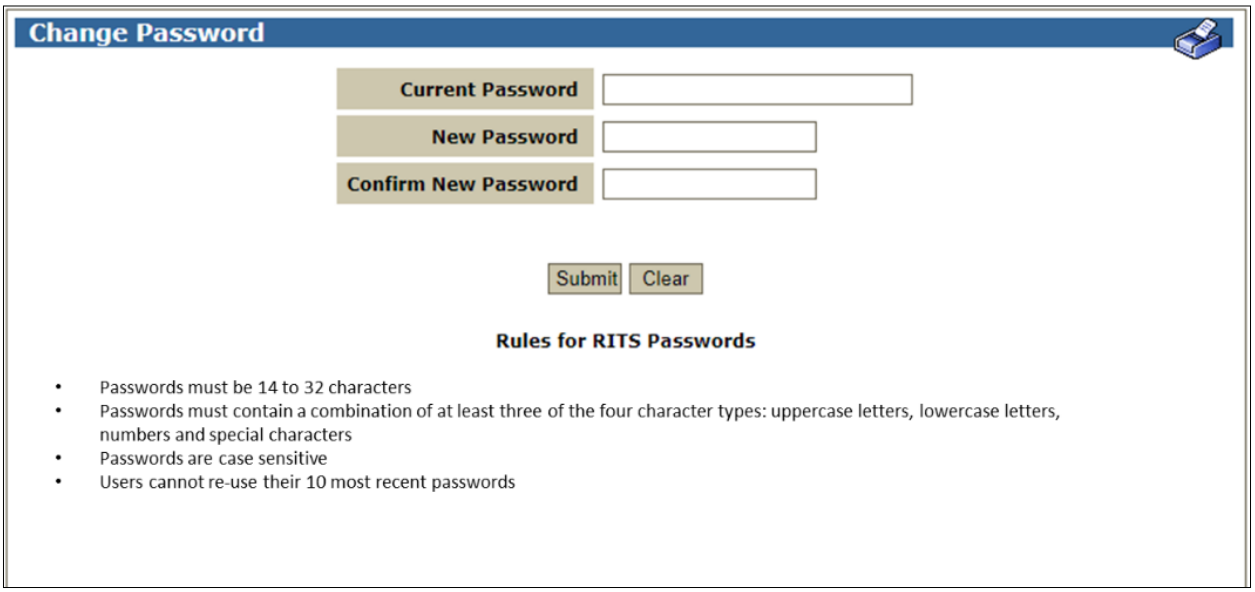
2. CHANGE PASSWORD

2.1 Key points

- Users can change their own RITS passwords.
- Passwords expire after 90 days.
- Users are prompted by RITS on each of the 5 days before their passwords expire to enter new passwords.
- After the password has expired, a user must enter a new password. Use the existing password to logon and follow the prompts to set a new one.
- If the user cannot remember the old password, request the Password Administrator to set a new password.
- Passwords must be 14 to 32 characters long and must contain a combination of at least three of the four character types: upper case letters, lower case letters, numbers and special characters – please see Appendix for a full list of allowable special characters.
- Passwords are case sensitive.
- Users cannot re-use their 10 most recent passwords.

2.2 Change Password entry screen

Select **Change Password** from the **Member Admin** tab on the menu.



2.2.1 Entry fields

Field	Description
Current Password	Entry field for the current password.
New Password	Entry field for the new password. Passwords should be created so that others have difficulty guessing. Passwords must be 14 to 32 characters long and must contain a combination of at least three of the four character types: upper case letters, lower case letters, numbers and special characters – please see Appendix for a full list of allowable special characters. Passwords are case sensitive. Users cannot re-use their 10 most recent passwords.
Confirm New Password	Entry field for the new password. Re-type the new password. This entry must match the one entered in the 'New Password' field.

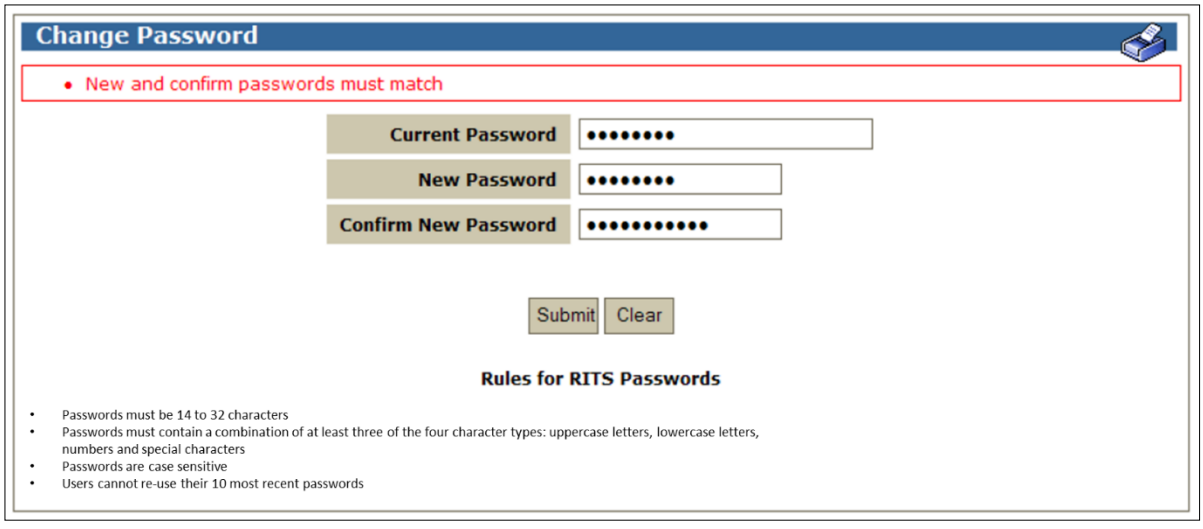
2.2.2 Actions

Button	Description
Submit	Select **Submit** to change the password.
Clear	Select **Clear** to clear all details entered.

2.3 Change Password

Enter the current password and the new password. Re-type the new password in the 'Confirm New Password' field. Submit the entries.

The entries in the 'New Password' and the 'Confirm New Password' fields must match. If they do not match, the following screen is displayed.



If they do match, a notification screen is displayed to confirm that the password has been changed. The new password is active from this point and must be used at any subsequent logons.

3. EVENING AGREEMENT

3.1 Key points

- Match an evening agreement with the RBA (Member ACHO) to undertake the obligation to participate in the Evening Session.
- Unmatch an evening agreement with the RBA (Member ACHO) to indicate that the obligation to participate in the Evening Session is no longer applicable.
- Changes to a Member's Evening Agreed status should only be made after consultation with the Manager, Membership and Governance, (email ritsmembership@rba.gov.au).

3.2 Matching process

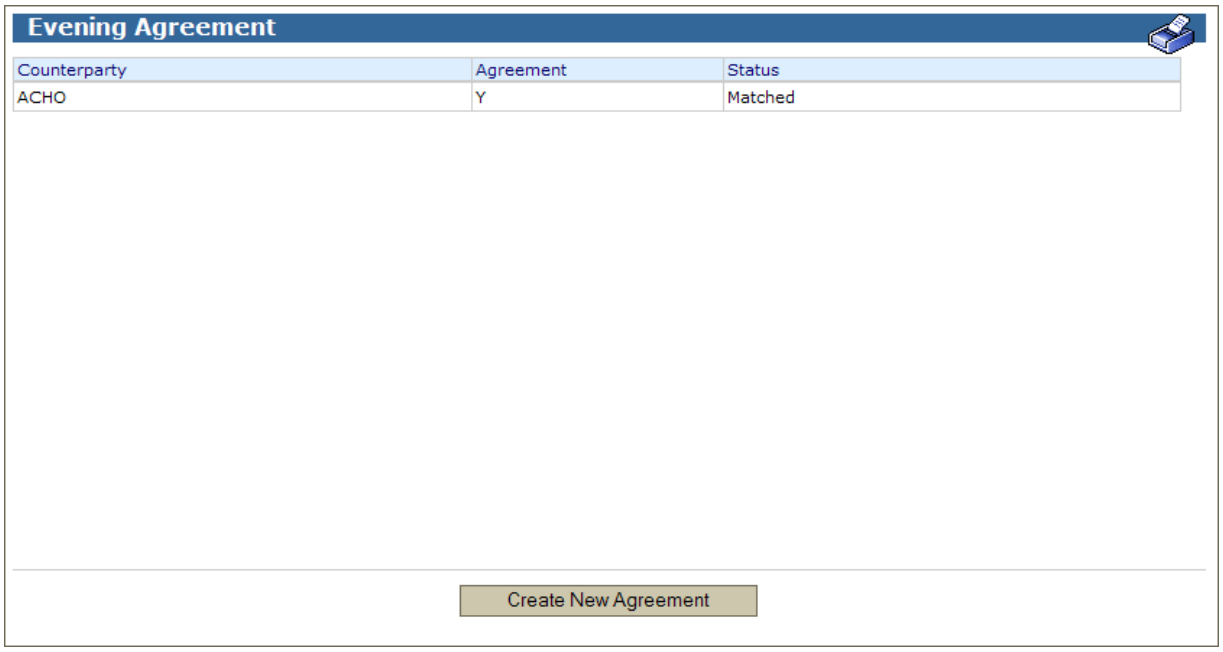
The creation and extinguishing of an EVENING agreement is a matching process. The entries and the associated status changes are shown in the following table.

In the example shown, the Member has entered first; however, either party can make the first entry.

Action	**Member's view**		**ACHO's view**	
	Entry: **Establish (Y), Extinguish (N)**	**Status**	**Entry:** **Establish (Y), Extinguish (N)**	**Status**
Member enters an agreement with ACHO	Y	No Counterparty Entry	Y	Counterparty Entry Only
ACHO matches the agreement with Member	Y	Matched	Y	Matched
Member changes Y to N to extinguish agreement	N	Unmatched	Y	Unmatched
ACHO changes Y to N to match the extinguish action of the Member	N	Matched	N	Matched

3.3 Evening Agreement entry screen

Select **Evening Agreement** from the **Member Admin** tab on the menu. The following screen is displayed. If an agreement already exists its status will be displayed. If there is no existing agreement the screen will be empty, but the 'Create New Agreement' button will be available.



3.4 Amend an Evening Agreement

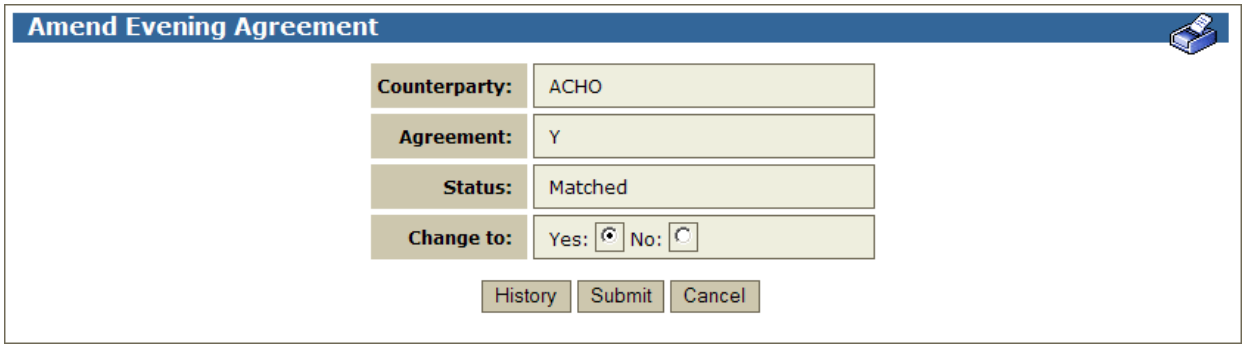
3.4.1 Display fields

Field	Description
Counterparty	The counterparty is always ACHO.
Agreement	Y – create agreement/ N – extinguish agreement.
Status	The status of the agreement. Possible statuses are: *No Counterparty Entry* *Counterparty Entry Only* *Unmatched* *Matched*.

3.4.2 Actions

Button	Description
Select a row	Select a row to open the Amend Evening Agreement screen.
Create New Agreement	Select **Create New Agreement** to enter an evening agreement.
Printer Icon	Select the **Printer Icon** to print the page.

Select the row of the agreement in the Evening Agreement screen to open the **Amend Evening Agreement** screen. The following screen is displayed.



3.4.3 Display/Entry fields

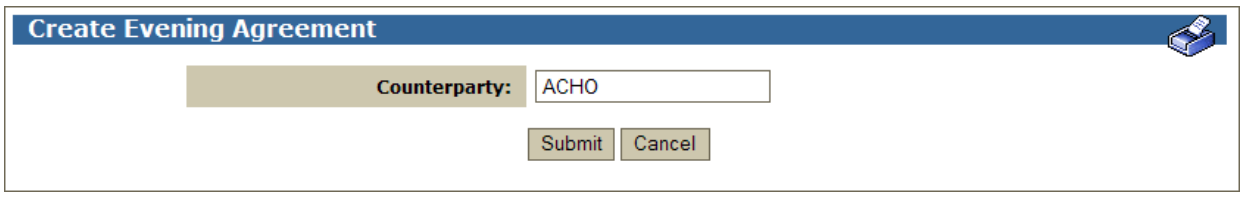
Field	Description
Counterparty	The counterparty is always ACHO.
Agreement	Y indicates that an Evening Agreement is in place.
Status	Either No Counterparty Entry/ Counterparty Entry Only/ Unmatched/ Matched.
Change to	**Yes** or **No**. Select **Yes** to indicate the desire to establish an agreement and **No** to cancel an existing agreement.

3.4.4 Actions

Button	Description
Submit	Select **Submit** to enter the change into RITS.
Cancel	Select **Cancel** to cancel any entries and return to the Evening Agreement screen.
History	Select **History** to open the history of entries made to establish and extinguish agreements.

3.5 Create a New Evening Agreement

Select the **Create Evening Agreement** link in the Evening Agreement screen to open the **Create Evening Agreement** screen.



3.5.1 Entry fields

Field	Description
Counterparty	The counterparty is always ACHO.

3.5.2 Actions

Button	Description
Submit	Select **Submit** to enter your side of the agreement into RITS.
Cancel	Select **Cancel** to cancel any entries and return to the Evening Agreement screen.

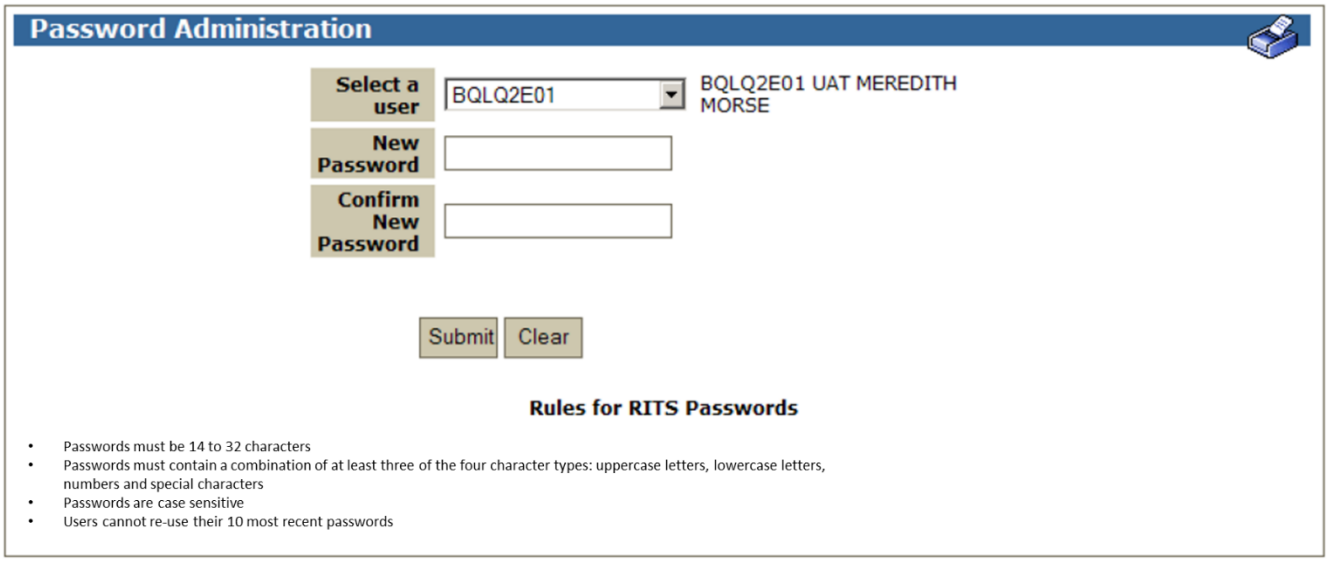
4. PASSWORD ADMINISTRATION

4.1 Key points

- Used by the Password Administrator to reset or change a user's password.
- Note that a password reset in this function must be changed by the user at the next logon to RITS.
- Users use the function **Change Password** to change their own password.
- Passwords must be 14 to 32 characters long and must contain a combination of at least three of the four character types: upper case letters, lower case letters, numbers and special characters – please see Appendix for a full list of allowable special characters.
- Passwords are case sensitive.
- Users cannot re-use their 10 most recent passwords.

4.2 Password Administration entry screen

Select **Password Admin** from the **Member Admin** tab on the menu.



4.2.1 Entry fields

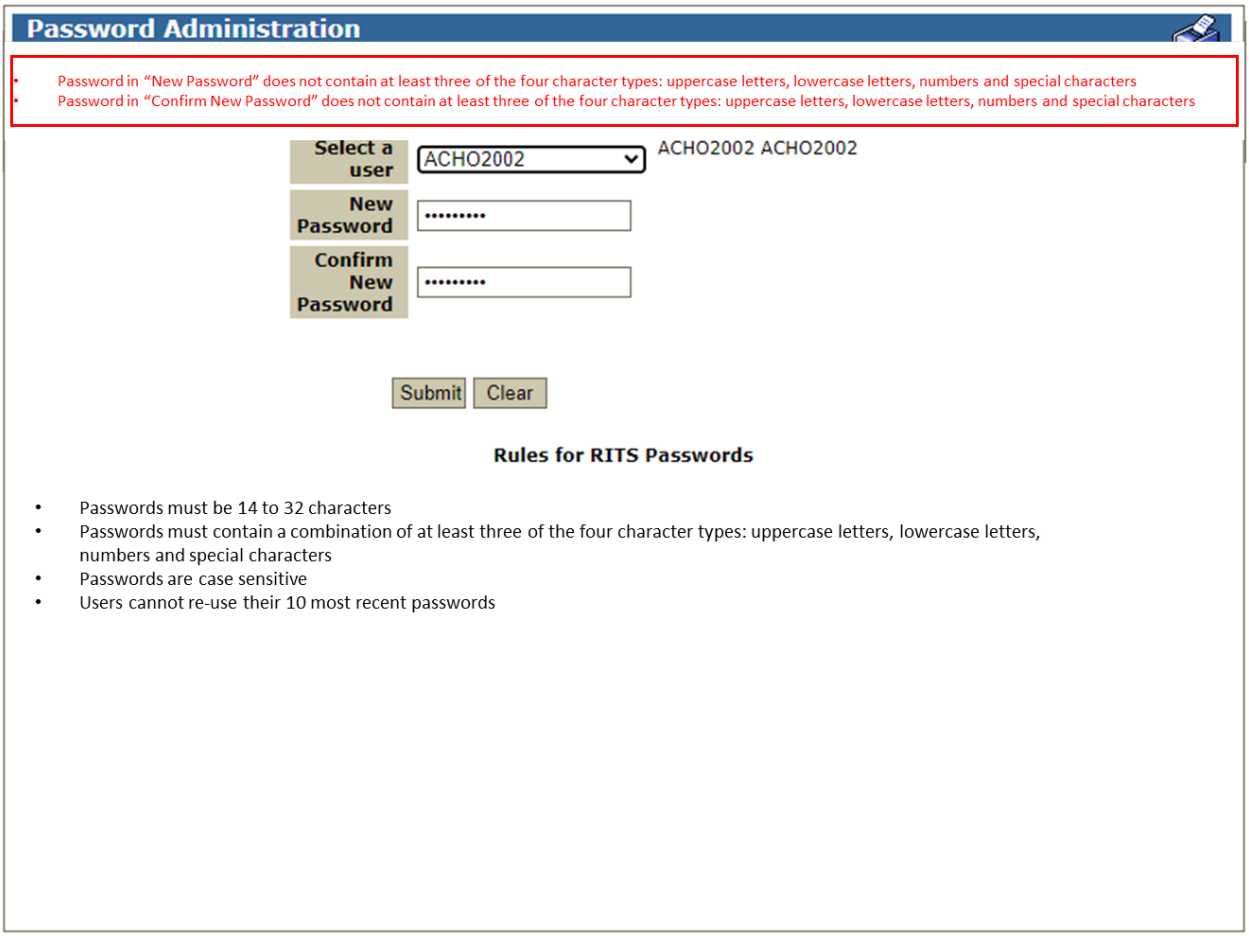
Field	Description
Select a User	Select the logon of the user who needs their password changed, (e.g. BQLQ2E01). If there are no active status users the following message is displayed when the function is selected from the menu – 'No active users in list'. This situation could arise when a new Member is in the process of enrolling users.
User's name	The name of the user is displayed beside the RITS logon.

Field	Description
New Password	Entry field for the new password. Passwords should be created so that others have difficulty guessing. Passwords must be 14 to 32 characters long and must contain a combination of at least three of the four character types: upper case letters, lower case letters, numbers and special characters – please see Appendix for a full list of allowable special characters. Passwords are case sensitive. Users cannot re-use their 10 most recent passwords.
Confirm New Password	Entry field for the new password. Re-type the new password. This entry must match the one entered above.

4.3 Change a user's RITS Password

Enter the current password and the new password. Re-type the new password in the 'Confirm New Password' field. Submit the entries.

The entries in the 'New Password' and the 'Confirm New Password' fields must match. If they do not match, the following screen is displayed.



If they do match, a notification screen is displayed to confirm that the RITS password has been changed.

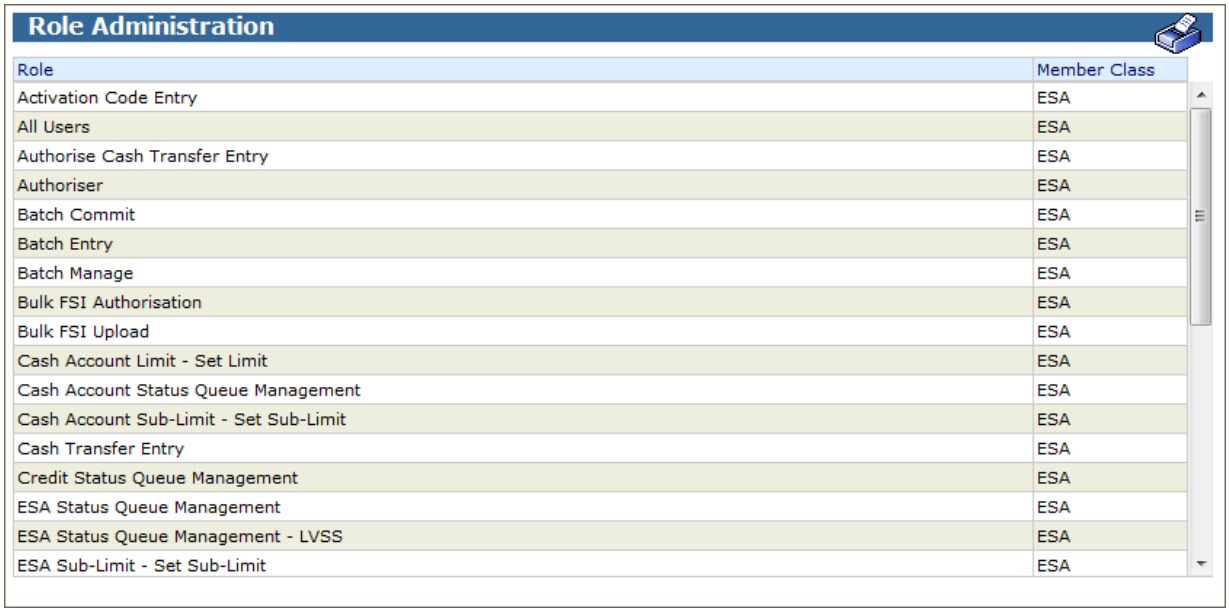
5. ROLES ENQUIRY

5.1 Key points

- View the roles available to Members and the functions contained in each role.

5.2 Roles Enquiry screen

Select **Roles** from the **Member Admin** tab on the menu. The following screen is displayed, populated with the list of roles.



5.2.1 List headings

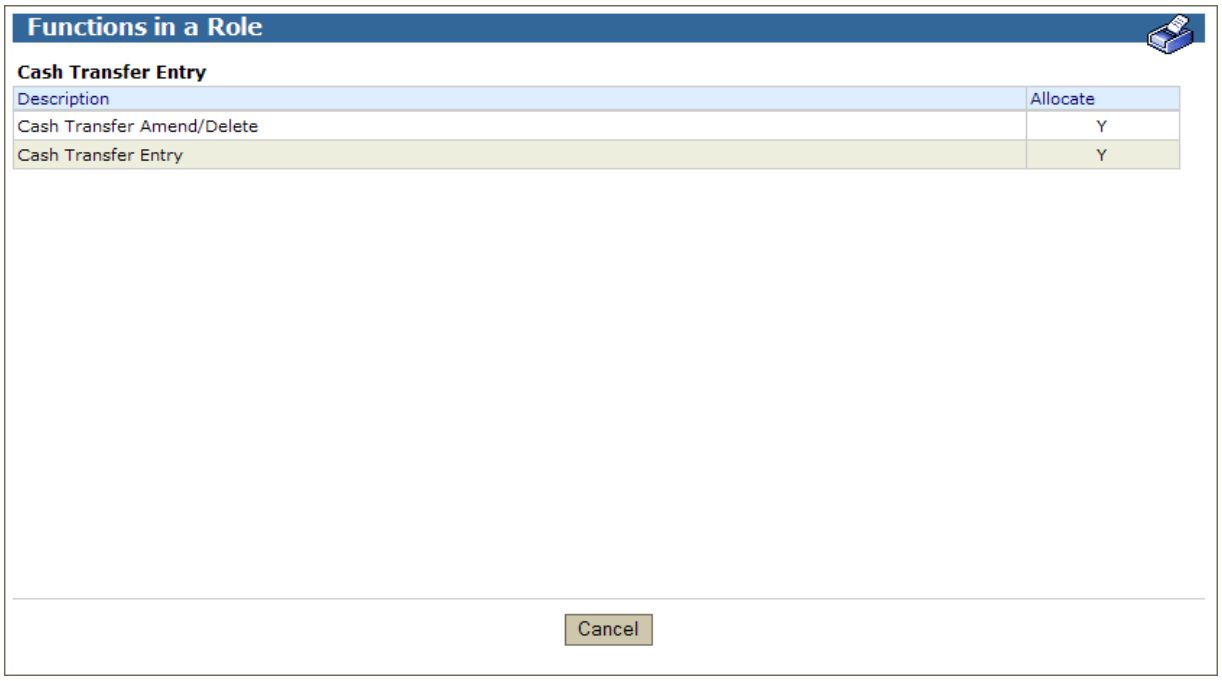
Field	Description
Roles	A list of the roles in RITS.
Member Class	The Member Class (ESA) for ESA Holders.

5.2.2 Actions

Button	Description
Select a row	Select a row in the table to open the Functions in a Role screen.

5.3 Functions in a Role screen

After selecting a **Role** from the list in the previous screen, the following screen is displayed.



5.3.1 List headings

Field	Description
Description	The name of the function(s) that are contained in the Role.
Allocate	A similar screen to this is used by the RITS System Administrators to construct the functions in the Roles. The 'Allocate' column is relevant to those screens.

5.3.2 Actions

Button	Description
Cancel	Select **Cancel** to return to the Roles list screen.

6. UNSOLICITED ADVICES

6.1 Key points

- Maintain the Member's selections to receive Unsolicited Advices.
- Maintain the Member's selections to receive Pre- and Post-Settlement Advices.
- Maintain the Member's selections to receive LVSS advices and responses.
- The selection of Pre- and-Post Settlement advices is by Transaction Source for some feeders and by branch for others. Refer to section 6.7 for detailed instructions.
- More information is available in the RITS/SWIFT Interface User Guide, which can be found on the RITS Information Facility.

6.2 Unsolicited Advices list screen

Select **Unsolicited Advices** from the **Member Admin** tab on the menu. The following is displayed, populated with the Unsolicited Advices that are available to Members.

Unsolicited Advices

Message Type	Sub Message Type	Description	Receive Advice	BIC Reference
198	003	Unsolicited Recall Advice (RITS trans)	☐	Please Select
198	006	Unsol Change ESA Status Advice	☐	Please Select
198	009	Unsol Change Credit Status Advice	☐	Please Select
198	015	Change ESA Sub-Limit Advice	☐	Please Select
198	026	Client Cash Account Balances EOD Advice	☐	Please Select
198	030	Unsolicited Time Period Advice	☐	Please Select
198	038	Unsettled Advice (EOD) RITS/FINTRACS	☐	Please Select
198	039	Holiday Table Advice	☐	Please Select
941		RITS Start of Day Balance Advice	☐	Please Select
942	001	RITS ESA Interim Advice	☐	Please Select
950	111	ESA Statement End of Day Summary Advice	☐	Please Select
950	222	ESA Statement End of Day Advice	☐	Please Select
950	888	RITS ESA Interim Session Statement Advice	☐	Please Select
950	999	RITS ESA Reports Session Statement Advice	☐	Please Select

Pre/Post Settlement Advice | LVSS Messages | Submit

6.2.1 List/entry headings

Field	Description
Message Type	The SWIFT Message Type.
Sub Message Type	The SWIFT Sub Message Type.
Description	The description of the advice.
Receive Advice	The tick box to indicate if you wish to receive the advice.
BIC Reference	A list of BICs used by the Member. Select the appropriate BIC. Mandatory field.

6.2.2 Actions

Button	Description
Pre/Post Settlement Advices	This link opens the **Unsolicited Advices Pre/Post Settlement** screen. This screen shows the Member's selections for Pre/Post Settlement Advices and provides links to select or de-select advices and to maintain branch and source details for each advice.
LVSS Messages	This link opens the **LVSS Message Selection** screen. This screen shows the Member's selections for the optional LVSS Responses and Advices.
Submit	Select **Submit** to select to receive or discontinue receiving unsolicited advices.

6.3 Selecting to receive an Unsolicited Advice

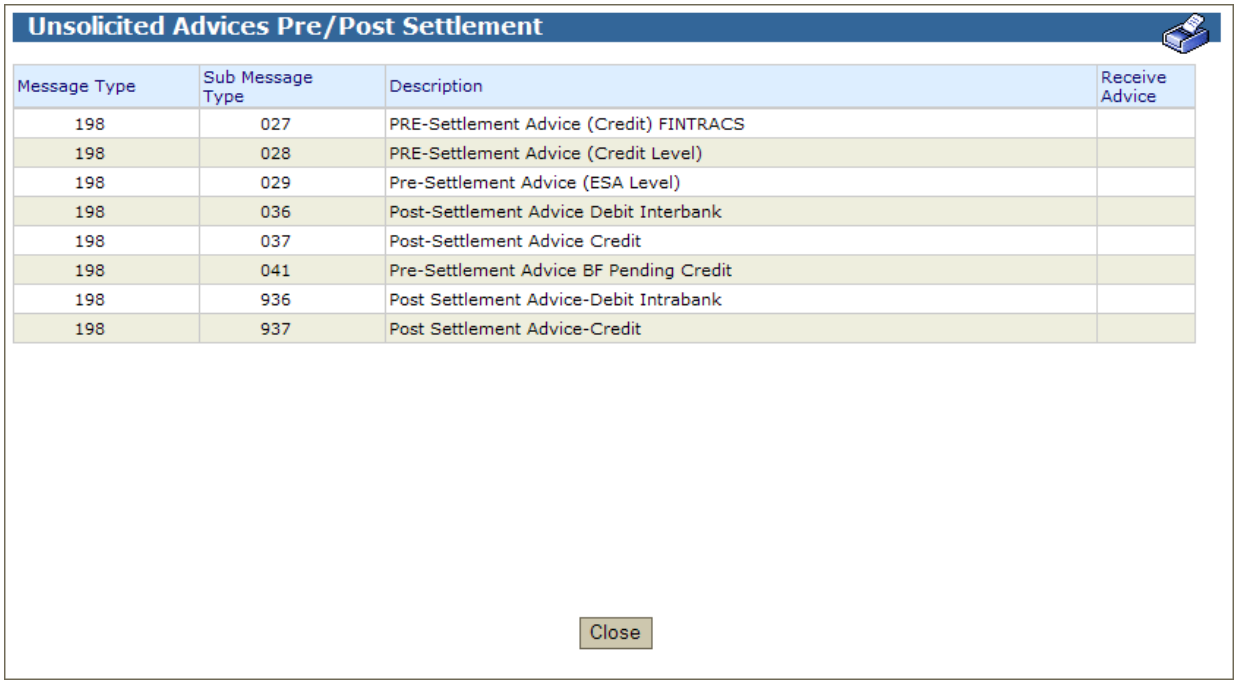
In the above screen, tick the box beside the advice (or advices) that you wish to receive. This action activates the BIC Reference selection list. Select the BIC from the list for each advice and select **Submit**. The selection of a BIC is mandatory for each advice.

To cancel selections that you have made before you press 'Submit', simply re-select the Unsolicited Advices function from the Menu.

To discontinue receiving an advice, un-tick the box and select **Submit**.

6.4 Unsolicited Advices Pre/Post Settlement screen

Select the **Pre/Post Settlement Advices** button in the Unsolicited Advices screen to open the Unsolicited Advices Pre/Post Settlement screen. The following enquiry screen is displayed, populated with the list of Pre/Post Settlement Advices that are available to Members. The screen also shows the Member's selections for these advices with 'Y' in the 'Receive Advice' column.



6.4.1 List headings

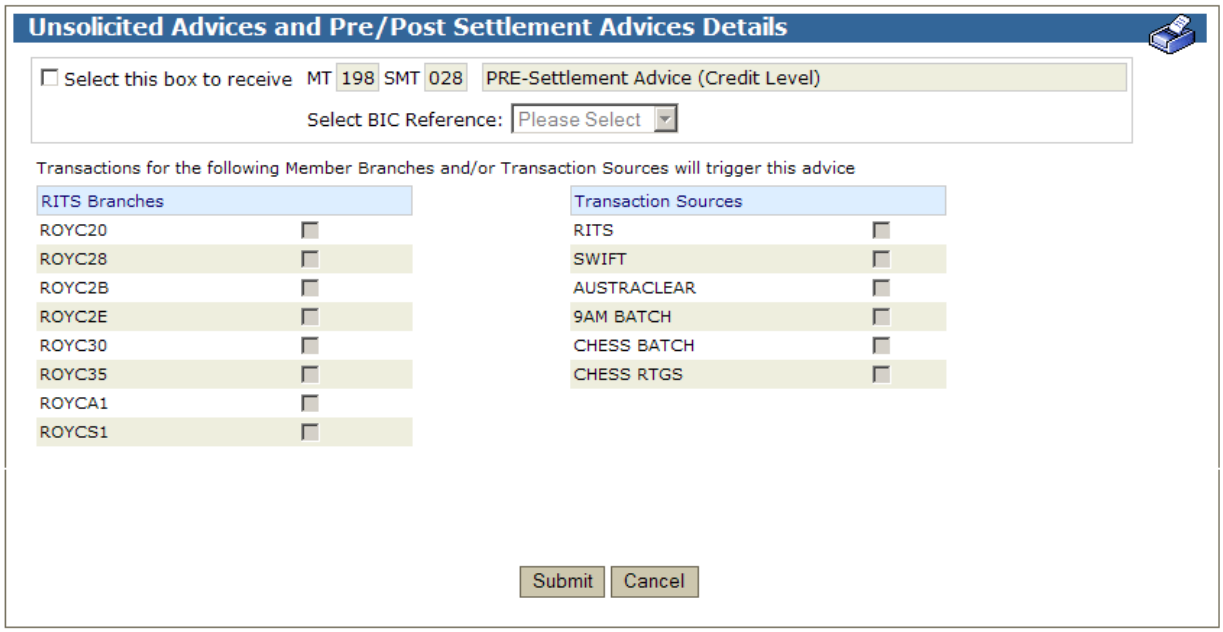
Field	Description
Message Type	The SWIFT Message Type.
Sub Message Type	The SWIFT Sub Message Type.
Description	The description of the Pre/Post Settlement Advice.
Receive Advice	Display only. 'Y' in this column indicates that the Member has selected to receive the advice.

6.4.2 Actions

Button	Description
Close	Select **Close** to close the screen and return to the Unsolicited Advices screen.
Select a row	Select a row in the table to open the Unsolicited Advices and Pre/Post Settlement Advices Details screen.

6.5 Unsolicited Advices and Pre/Post Settlement Advices Selection screen

After selecting a row in the previous screen, the following screen is displayed. Its purpose is to permit the selection of the Pre/Post Settlement Advice and to select the transaction source and/or the RITS branch or branches for which the advice will be generated.



6.5.1 List/entry headings

Field	Description
RITS Branches	The active RITS branch(es) of the Member. Tick or un-tick as appropriate. Advices are not supported for all branches. Refer to section 6.7. At least one branch or one transaction source must be selected.
Transaction Sources	The sources of transaction processed through RITS. Tick or un-tick as appropriate. Transaction Source – CHESS BATCH – is redundant. Advices for the source are selected via the 2M branch. At least one branch or one transaction source must be selected.

6.5.2 Actions

Button	Description
Select this box to receive the advice	Tick the box to elect to receive the Pre/Post Settlement Advice. Un-tick the box to discontinue receiving the Pre/Post Settlement Advice.
BIC Reference	Select the BIC from the list of the Member's BICs.
Submit	Select **Submit** to enter the selections into RITS.
Cancel	Select **Cancel** to clear entries and return to the Unsolicited Advices Pre/Post Settlement screen.

6.6 Unsolicited Advices and Pre/Post Settlement Advices Selection screen

Enter the **Unsolicited Advices Pre/Post Settlement** screen and select the advice that you wish to receive by selecting the row.

This action opens the **Unsolicited Advices and Pre/Post Settlement Details screen.**

In this screen:

- Select to receive the advice by ticking the box in the top left-hand corner of the screen.
- Once this is done the BIC Reference box becomes active. From the list of BICs provided, select the appropriate BIC. The selection of a BIC is mandatory.
- Now, tick a box beside a RITS branch or branches and/or a Transaction Source. The Pre/Post-Settlement Advice will be generated for transactions that belong to the branch or branches chosen and/or from the transaction source chosen. As some advices must be selected by Transaction Source and other by branch, refer to section 6.7 for details. At least one branch or one transaction source must be selected.
- Select **Submit**.

To discontinue receiving the advice, un-tick the box in the top left-hand corner of the screen and select Submit.

To amend any details, make changes in the screen and submit them.

6.7 Guide for setting up branch and transaction source details

The following is a guide to the setting up of branch and transaction source details to receive Pre/Post-Settlement Advices.

The selection of advices varies on the basis of transaction source or RITS branch.

Transaction Sources:

- RITS – RITS Cash Transfers entered in any branch and ESA Interest (ESINT) and RITS Allocation Transaction leg of an FSS Top-Up or FSS Withdrawal.
- SWIFT – payments in the SWIFT PDS.
- AUSTRACLEAR – transactions in the Austraclear System
- 9AM BATCH – transactions in the 9am Batch (refers to obligations entered via the National Collator, not via the LVSS. Since the completion of LVSS migration in October 2012, the selection of this Source will not result in the production of any advices.)
- CHESS Batch – transactions in the CHESS batch
- CHESS RTGS – transactions in the CHESS feeder

Separate branch selections may be made to obtain advices for transactions in specific branches:

- transactions in batches (CHESS, Mastercard, eftpos, PEXA and ASXF batches);
- RITS Cash Transfers entered by a particular branch; and
- LVSS transactions.

ESA Interest transactions will be shown if the Member selects their "2E" branch.

6.7.1 Select advices

Detailed instructions are contained in the following table.

Advice	Comments	RITS Branches	Transaction Source

Pre-Settlement Advices			
MT198 SMT027 **Pre-Settlement Advice – Austraclear (Credit Level)**	For Austraclear transactions **only**. Must be selected in the Austraclear System and also in Unsolicited Advices in RITS. Advices are generated and sent for the client account that is specified in the Austraclear System.		**AUSTRACLEAR**
MT198 SMT028 **Pre-Settlement Advice (Credit Level)**	To receive advices for transactions in the CHESS-RTGS feeder. To receive advices for RITS Cash Transfers undertaken in any branch, and ESA interest transactions. To receive advices for SWIFT PDS payments.		**CHESS RTGS** **RITS** **SWIFT**
	To receive advices for transactions in the CHESS Batch.	**MEMB2M**	
	To receive advices for transactions in the PEXA Batch.	**MEMB2P**	
	To receive advices for transactions in the ASXF Batch.	**MEMBXF**	
	To receive advices for transactions in the Mastercard Batch.	For example, **MEMB2E**, **MEMBMC**	
	To receive advices for transactions in the eftpos Batch.	For example, **MEMB2E**, **MEMBEB**	
	To receive advices for RITS Cash Transfers undertaken in a specific branch.	For example, **MEMB2E**, **MEMB20**	

Advice	Comments	RITS Branches	Transaction Source
	To receive advices for LVSS transactions undertaken in a specific branch.	For example, **MEMBLC**, **MEMBLD**	
MT198 SMT029 **Pre-Settlement Advice (ESA Level)**	To receive advices for transactions in the CHESS-RTGS feeder. To receive advices for transactions in Austraclear. (Advices are generated and sent for the client account that is specified in the Austraclear System.) To receive advices for RITS Cash Transfers undertaken in any branch, and ESA interest transactions. To receive advices for SWIFT PDS payments.		**CHESS RTGS** **AUSTRACLEAR** **RITS** **SWIFT**
	To receive advices for transactions in the CHESS Batch.	**MEMB2M**	
	To receive advices for transactions in the PEXA Batch.	**MEMB2P**	
	To receive advices for transactions in the ASXF Batch.	**MEMBXF**	
	To receive advices for transactions in the Mastercard Batch.	For example, **MEMB2E**, **MEMBMC**	
	To receive advices for transactions in the eftpos Batch.	For example, **MEMB2E**, **MEMBEB**	
	To receive advices for RITS Cash Transfers undertaken in a specific branch.	For example, **MEMB2E**	
	To receive advices for LVSS transactions undertaken in a specific branch.	For example, **MEMBLC**, **MEMBLD**	
MT198 SMT041 **Pre-Settlement Advice (Pending Credit)** **Only available for the batch feeder.**	To receive advices for the CHESS Batch.	**MEMB2M**	
	To receive advices for the PEXA Batch.	**MEMB2P**	
	To receive advices for the ASXF Batch.	**MEMBXF**	

Advice	Comments	RITS Branches	Transaction Source
	To receive advices for the Mastercard Batch.	For example, **MEMB2E**, **MEMBMC**	
	To receive advices for transactions in the eftpos Batch.	For example, **MEMB2E**, **MEMBEB**	
Post-Settlement Advices			
MT198 SMT036 **Post-Settlement Advice – (Interbank Debit)** **MT198 SMT037** **Post-Settlement Advice – (Interbank Credit)**	To receive advices for transactions in the CHESS-RTGS feeder. To receive advices for transactions in Austraclear. To receive advices for RITS Cash Transfers undertaken in any branch, and ESA interest transactions To receive advices for SWIFT PDS payments.		**CHESS RTGS** **AUSTRACLEAR** **RITS** **SWIFT**
	To receive advices for ESA interest, RITS Cash Transfers, and transactions in the Mastercard Batch or eftpos Batch (where relevant) undertaken in the "2E" branch.	**MEMB2E**	
	To receive advices for transactions in the CHESS Batch.	**MEMB2M**	
	To receive advices for transactions in the PEXA Batch.	**MEMB2P**	
	To receive advices for transactions in the ASXF Batch.	**MEMBXF**	
	To receive advices for transactions in the Mastercard Batch.	For example, **MEMB2E**, **MEMBMC**	
	To receive advices for transactions in the eftpos Batch.	For example, **MEMB2E**, **MEMBEB**	
	To receive advices for RITS Cash Transfers undertaken in a specific branch.	For example, **MEMB20**	

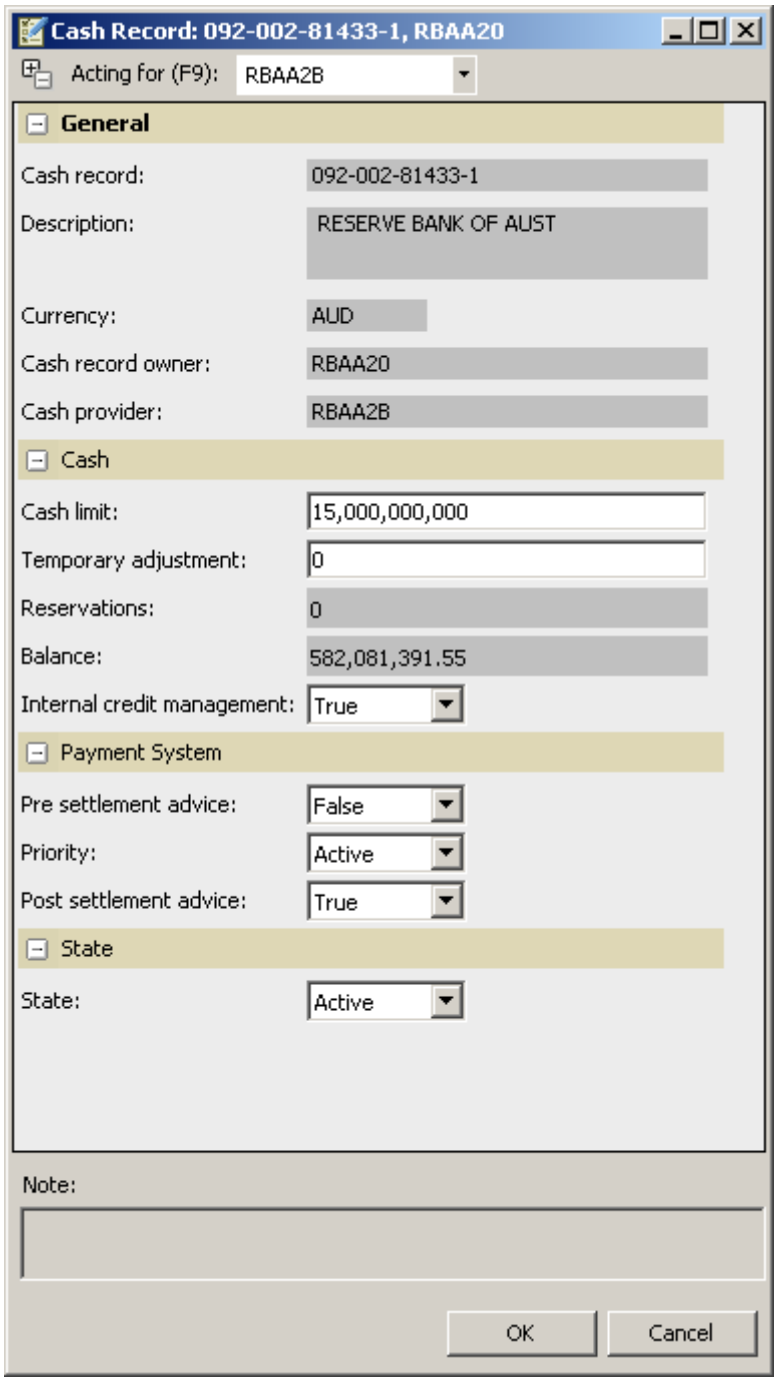
Advice	Comments	RITS Branches	Transaction Source
MT198 SMT936 **Post-Settlement Advice – (Intrabank Debit)**	To receive advices for transactions in the CHESS-RTGS feeder. To receive advices for transactions in Austraclear.	**MEMBFS**	**CHESS RTGS** **AUSTRACLEAR**
MT198 SMT937 **Post-Settlement Advice – (Intrabank Credit)** **If these advices are selected, MT198 SMT036 & 037 advices are sent.**	To receive advices for RITS Cash Transfers undertaken in any branch. To receive advices for a RITS Allocation Transaction leg of an FSS Top-Up or FSS Withdrawal. To receive advices for SWIFT PDS payments.		**RITS** **RITS** **SWIFT**

6.8 Setting statuses and pre-settlement advice flags in Austraclear

Pre-Settlement Advices for particular Austraclear clients (at the Austraclear cash account level) may be obtained by making a selection in both the relevant Austraclear function and in the RITS function Unsolicited Advices Maintenance. This degree of selection is not available for Post-Settlement Advices, which, if selected in Unsolicited Advices Maintenance in RITS, can only be obtained for ALL Austraclear transactions that are sent to RITS.

The following is the screen used in the Austraclear system to request pre-settlement advices and to set the Credit and ESA statuses for transactions using the Austraclear cash account (called Cash Record in Austraclear). These settings come to RITS as part of the settlement request.

This feature permits the participating bank in Austraclear to request pre-settlement advices for particular client on the basis of Austraclear cash account. Thus, the participating bank can manage its clients as required – with credit checking done in Austraclear (using a cash account limit setting) or in RITS (using the Credit Status and its management).



The selections made in the Cash Record have the following impacts.

Cash Record selection	**Impact**
Internal credit management:	If = False, the Credit Status is set to D. The Austraclear System ignores the "Cash Limit" and credit checking is done in RITS. If = True, the Credit Status is set to A. Credit checking is done in Austraclear using the Cash Limit.
Priority:	If = Active, the ESA Status is set to A. If = Deferred, the ESA Status is set to D.

Cash Record selection	Impact
Pre settlement advice:	If = False, send "N" in the Settlement Request for the Pre-Settlement Advice ESA (MT198 SMT029). RITS will not generate an advice. If = True, send "Y". RITS will generate the advice.
Post settlement advice: *(see note about this misleading field name)*	If = False, send "N" in the Settlement Request for the Pre-Settlement Advice Austraclear Credit (MT198 SMT027). RITS will not generate an advice. If = True, send "Y". RITS will generate the advice. *(Note: This explanation is not a mistake. The Austraclear Cash Record screen shows "Post settlement advice". This field is misnamed – it controls the pre settlement advice Austraclear Credit (MT198 SMT027)).* *Post settlement advices are not controlled from Austraclear. They are controlled from the Unsolicited Advices function in RITS. Note that if selected in RITS, a post settlement advice is sent for every Austraclear transaction.*

Credit management performed in RITS:

For a client account where credit management is conducted in RITS, "Internal Credit Management" is set to False and the *Post settlement advice* field is set to True. The Credit status is set to Deferred to hold the transaction on the System Queue while the bank's payments system assesses the client's credit using the pre-settlement advice credit before sending an AIF command to change the Credit status to Active.

Some banks set both the Credit and ESA statuses to Deferred and send an MT198 SMT031 (Change ESA and Credit Status Request) to change both to Active or Priority.

The pre-settlement advices must also be selected in Unsolicited Advices in RITS.

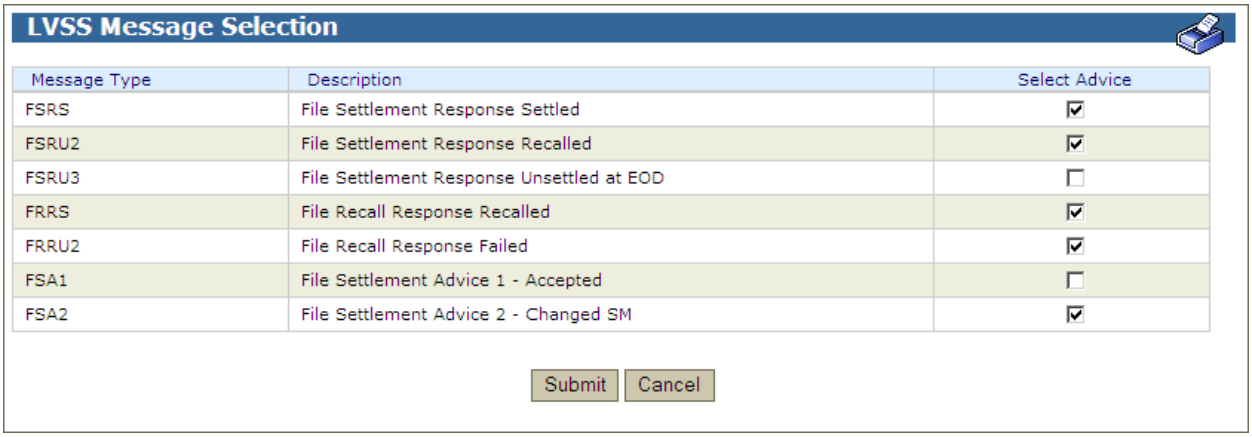
6.9 LVSS Message Selection screen (Update version)

Select the **LVSS Messages** button in the Unsolicited Advices screen to open the LVSS Message Selection screen. The following update screen is displayed when the Member has the correctly allocated role. It is populated with the list of LVSS Responses and Advices that are available for selection.

When the RITS Member does not have the update role, an enquiry version of this screen is displayed, which shows the Member's selections, but does not allow them to be amended.

The screen shows checkboxes that indicate whether a message has been selected. If the checkbox is checked, the Member will receive that message.

FSRU1 and FRRU1 messages are not selectable as they are mandatory and will always be sent.



6.9.1 List headings

Field	Description
Message Type	The Message Type of the selectable Response or Advice.
Description	The description of the LVSS Message.
Select Advice	Checkbox. When checked, this indicates that the Member has selected to receive the message.

6.9.2 Actions

Button	Description
Submit	Select **Submit** to update entries in the message selections.
Cancel	Select **Cancel** to close the screen and return to the Unsolicited Advices screen.

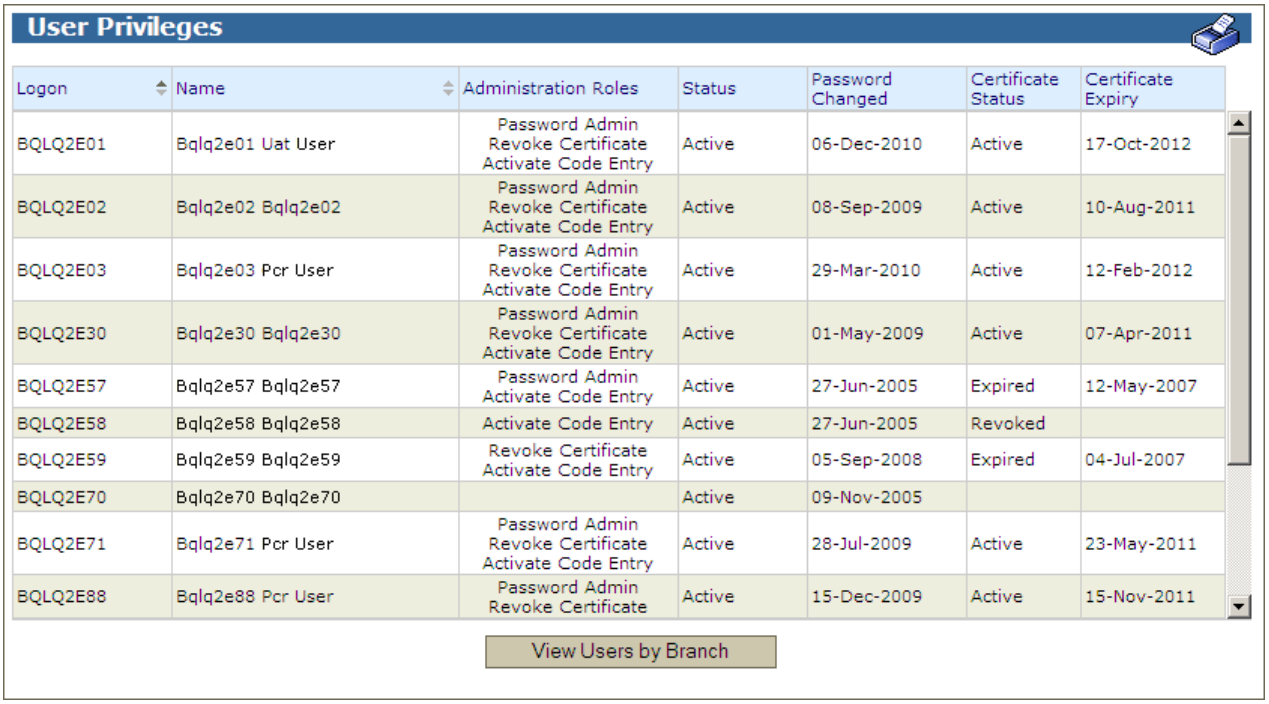
7. USER PRIVILEGES

7.1 Key points

- Used by the Password/Certificate Administrator to:
  - update a user's details;
  - manage a user's status;
  - set an extended session time-out parameter for selected users;
  - establish a user's links to a branch or branches;
  - enquire on user's links to branches by branch;
  - allocate roles to users and enquire on the functions in each role;
  - specify the functions that a user may authorise;
  - enquire on the status of a user's RITS digital certificate;
  - activate a user's RITS digital certificate; and
  - revoke a user's RITS digital certificate.
- A view-only version is available to all users to enquire on their own profiles and privileges.
- Password Administrators cannot allocate roles or set authorisation privileges for themselves.
- Note: The revocation of an expired certificate and the issuance of a new certificate will take approximately 20 – 30 minutes.

7.2 User Privileges user list screen

Select **User Privileges** from the **Member Admin** tab on the Menu. A list of all users of the Member is displayed.



7.2.1 List headings

Field	Description
Logon	Displays the user's logon of the Member.
Name	Displays the user's name.
Administration Roles	Details the roles granted to users to perform the task of Password/Certificate Administrator. An entry in this column identifies the user as a Password/Certificate Administrator and/or empowered to activate digital certificates and/or revoke certificates.
Status	Displays the status of the user – *Active* or *Inactive*.
Password Changed	Displays the date when the user's password was last changed.
Certificate Status	Displays the Certificate Status: • *Pre-enrolled* – the RITS Help Desk has initiated the certificate process by pre-enrolling the user. • *Collected* – the certificate has been downloaded to the user's token and is awaiting 'activation' by the Password/Certificate Administrator. • *Active* – the certificate is 'live' and permits access to RITS. • *Revoked* – the certificate has been revoked. No further access to RITS is possible. • *Expired* – the certificate has expired. A new certificate is required to regain access to RITS.
Certificate Expiry	Displays the expiry date of certificate. Certificates are issued with a life of around 2 years.

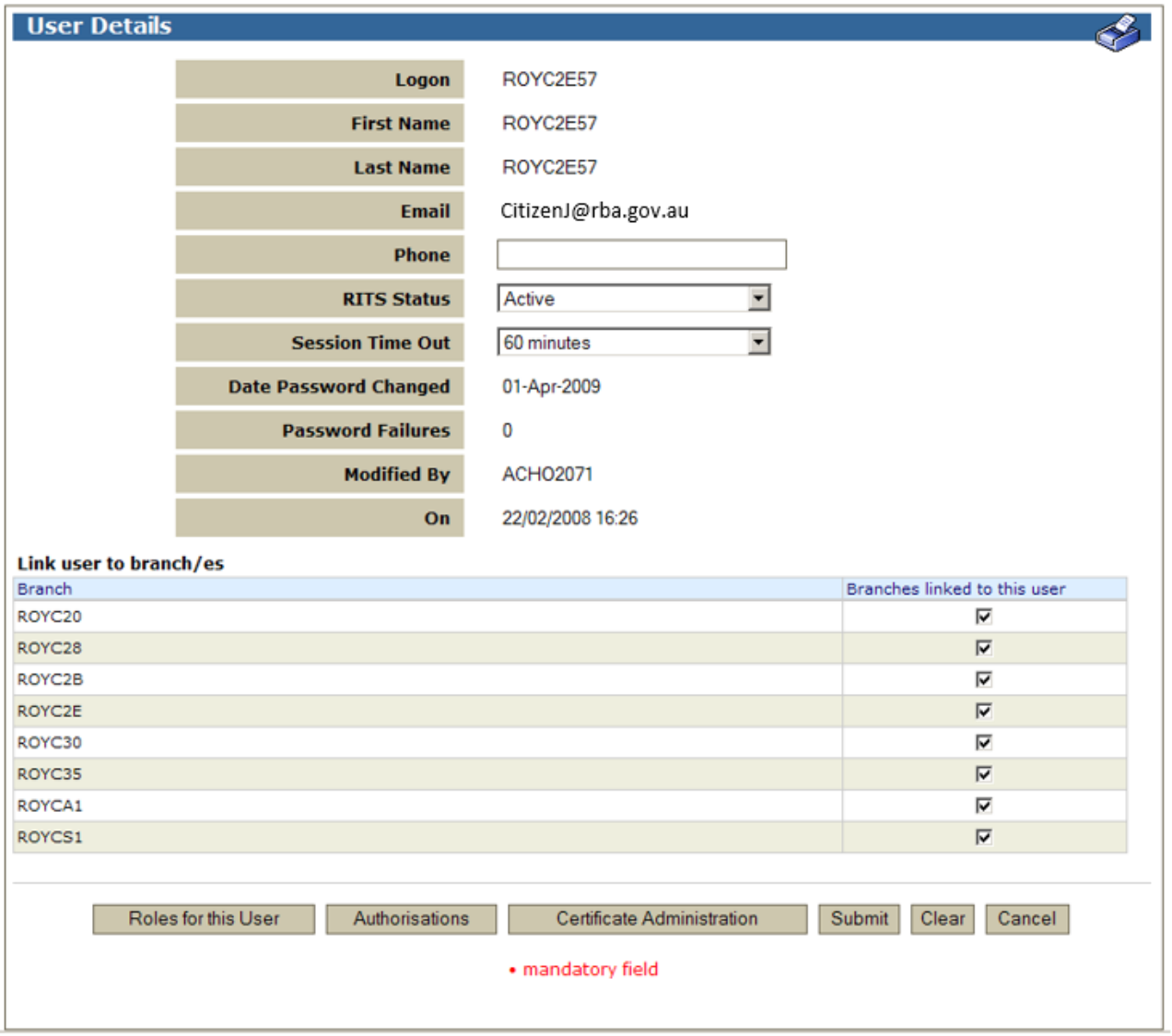
7.2.2 Actions

Button	Description
View Users by Branch	Select **View Users by Branch** to display the list of users linked to the branches of the Member.
Select a User	Select a row in the table to open the User Details screen for the user selected.

7.3 User Details screen

Select a row in the table in the **User Privileges** screen to open the User Details screen for that user.

7.3.1 List headings – user details



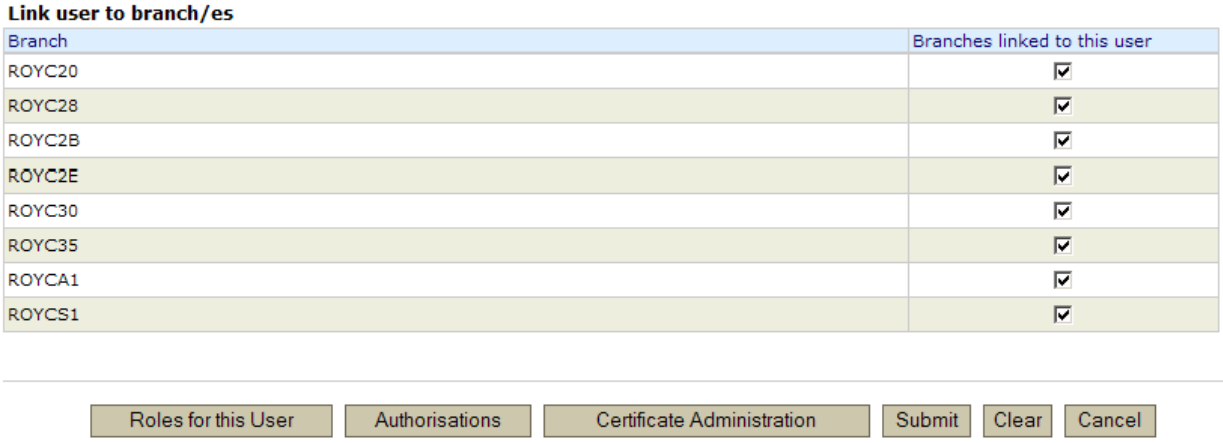
Field	Description
Logon	Displays the user's logon.
First Name	Displays the user's first name.
Last Name	Displays the user's last name.
Email	Displays the user's email address.
Phone	Entry field for user's phone number.
RITS Status	Entry field for user status - *Active*, *Inactive* or *Inactive/Revoke Certificate*.

Session Time-Out	Permits the setting of a user's session time-out (i.e. the period of time of no activity before the user is logged out automatically) for 15 minutes (the default), 30 or 60 minutes.
Date Password Changed	Displays the date when the user's password was last changed.
Password Failures	Displays the number of password failures. Within a 24-hour period the user is allowed 3 failed attempts to enter the password. On the fourth attempt, the user's status is automatically changed to *Inactive*. The counter is reset to zero when the user successfully logons again or 24 hours after the first failed attempt. Note that the Token Codeword must be correctly entered before the count of an incorrect password is registered.
Modified by	Displays the Password Administrator's logon for the last changes to details in this screen.
On	Displays the date and time when the last changes to details in this screen were made.

7.3.2 List headings – Link users to branch/es

Field	Description
Branch	Displays the branches of the Member.
Branches linked to this user	Shows which branches the user is linked to. Tick the relevant boxes to link the user to selected branches for this member. When linked to a branch, a user may perform actions for that branch in: • Cash Transfers; • Cash Account Queue Management; • Bulk Cash Account Status; • Override Cash Account Status; • Cash Account Sub-limit; and • Batch participant or Batch Administrator. The user must also be allocated the appropriate role/s. Untick a box to remove the user's access to the branch.

7.3.3 Actions



Button	Description
Roles for this User	Opens the User Roles screen. The Password Administrator uses this screen to allocate roles to users.
Authorisations	Opens the Authorisations by User screen. The Password Administrator uses this screen to specify the functions that the user is permitted to authorise.
Certificate Administration	Opens the Certificate Administration screen. The Password/Certificate Administrator uses this screen to activate or revoke a user's digital certificate.
Submit	Select **Submit** to update entries in user details and/or user branch links.
Clear	Select **Clear** to clear entries in user details and/or user branch links.
Cancel	Select **Cancel** to clear entries and return to the User Privileges screen.

7.4 Change User details

In the **User Details** screen enter or change the phone number details, change the RITS Status of the user or set an extended session time-out period. The User Details screen can be accessed by selecting the row of a user in the User Privileges screen.

In the same screen, select the branches that the user is linked by ticking or un-ticking the boxes supplied.

When the entries are completed, select **Submit** to make the changes, **Clear** to reset the screen or **Cancel** to discontinue the action and return to the **User Privileges** screen.

Users must be made *Inactive* if they are out of the office for an extended period.

7.4.1 Actions

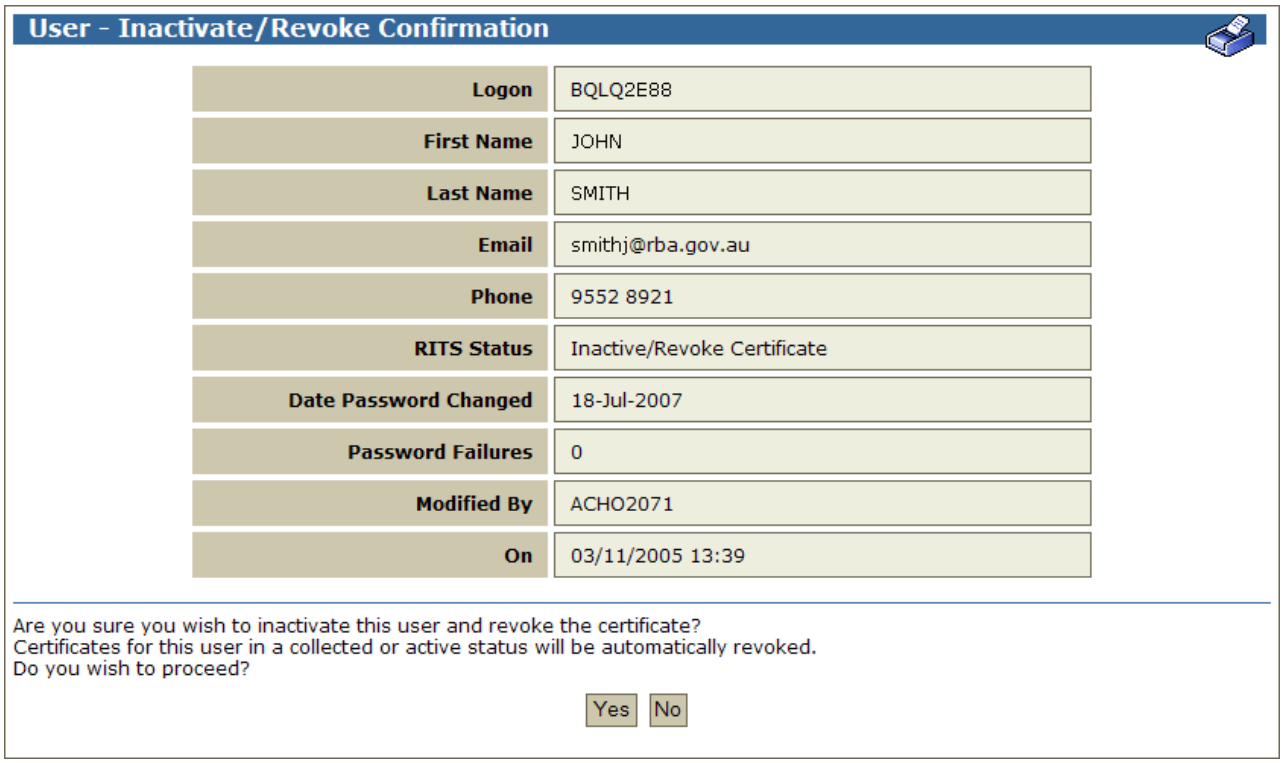
Button	Description
Submit	Select **Submit** to update entries in user details and/or user branch links.
Clear	Select **Clear** to clear entries in user details and/or user branch links.
Cancel	Select **Cancel** to clear entries and return to the User Privileges screen.

7.5 Change User status

In the **User Details** screen the user's status may be changed. The options are *Active*, *Inactive* and *Inactive/Revoke Certificate*.

Inactive/Revoke Certificate changes the user's status to inactive and revokes the user's certificate in the one action.

When this option is submitted a confirmation screen is provided.

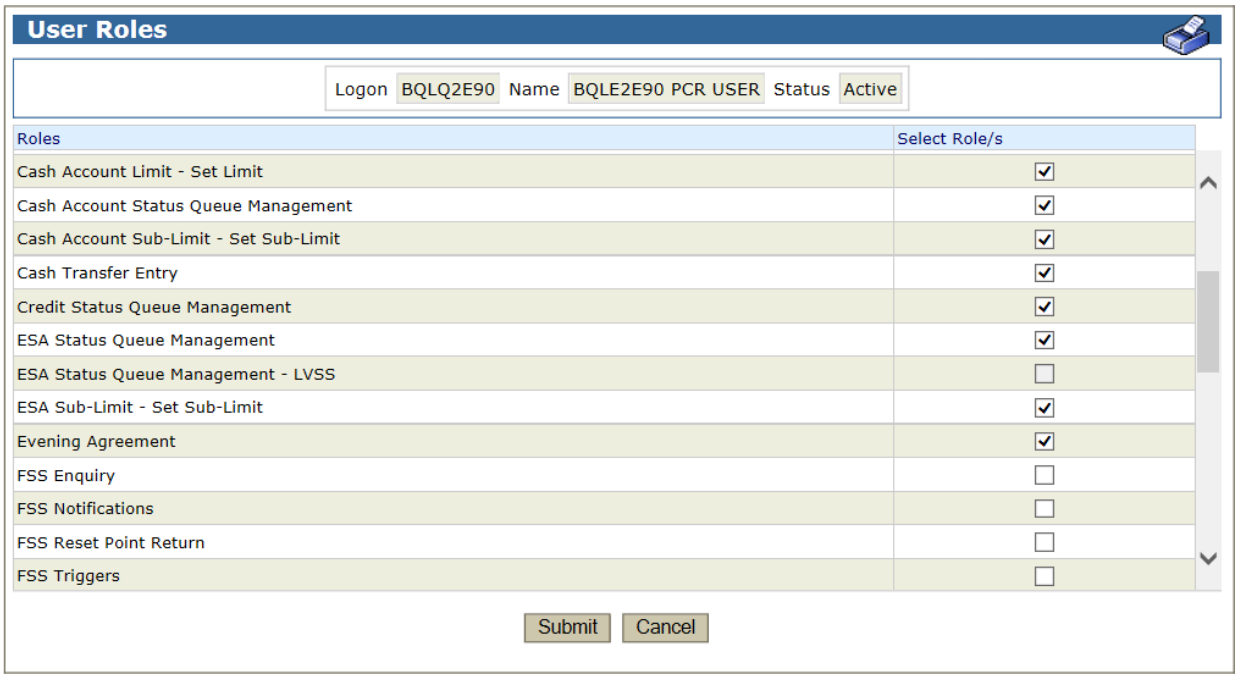


7.5.1 Actions

Button	Description
Yes	Select **Yes** to continue with the action.
No	Select **No** to cancel the action and return to the User Details screen.

7.6 Roles for this User screen

Select the **Roles for this User** button on the **User Details** screen. The User Details screen can be accessed by selecting a user in the User Privileges screen.



7.6.1 List headings

Field	Description
Roles	Displays a list of the roles available to the user.
Select Role(s)	Tick box entry field. Select to allocate the role. De-select to remove the role from the user.

7.6.2 Actions

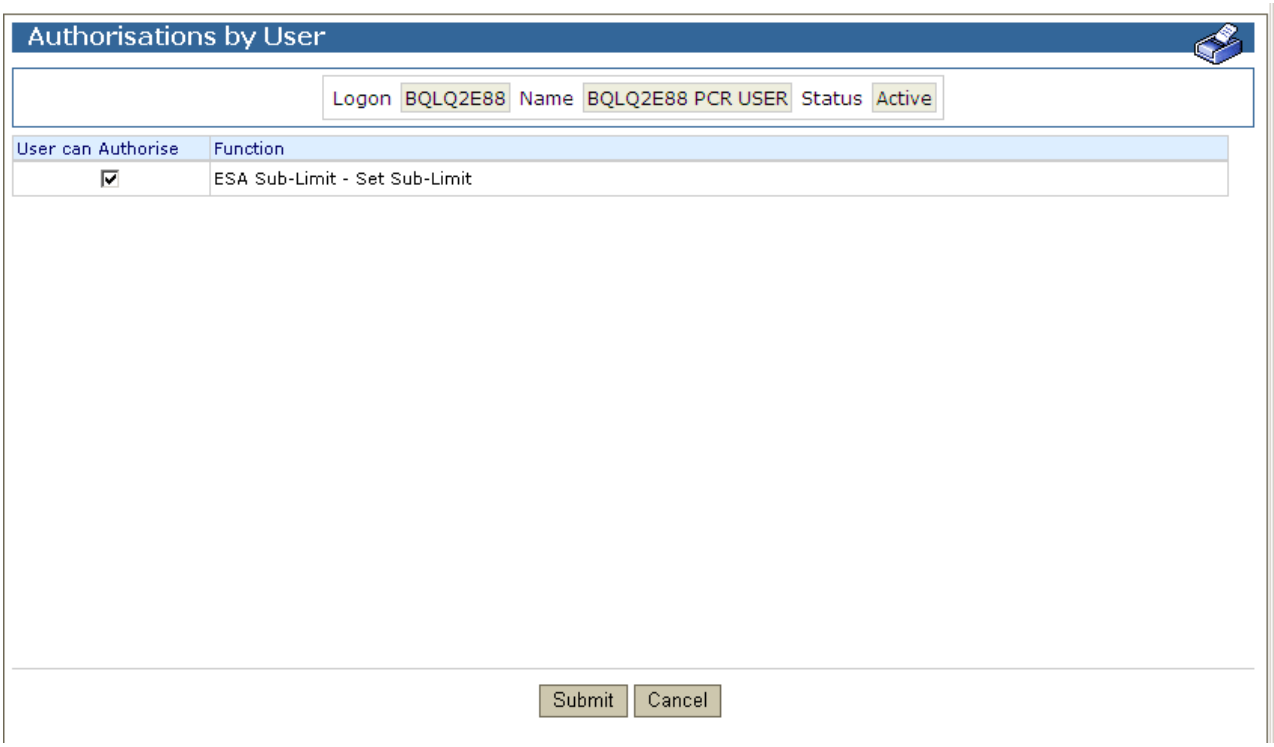
Button	Description
Submit	Select **Submit** to update entries in Roles for this user.
Cancel	Select **Cancel** to clear entries and return to the User Details screen.
Select a role	Select a role by clicking on the role name to open a screen showing the functions contained in that role.

7.7 Allocate roles to users

Tick or un-tick the boxes supplied to add or remove a role/ roles for the user. Use **Submit** to make the changes or **Cancel** to discontinue the action and return to the **User Details** Screen.

7.8 Authorisations by User screen

Select the **Authorisations** button on the **User Details** screen. The **User Details** screen can be accessed by selecting the row of a user in the **User Privileges** screen.



7.8.1 List headings

Field	Description
User Can Authorise	Tick box entry field. Select to specify the functions that the user is permitted to authorise. Un-tick to remove a user's ability to authorise a function.
Function	List of functions for which the member has specified that authorisation is required.

7.8.2 Actions

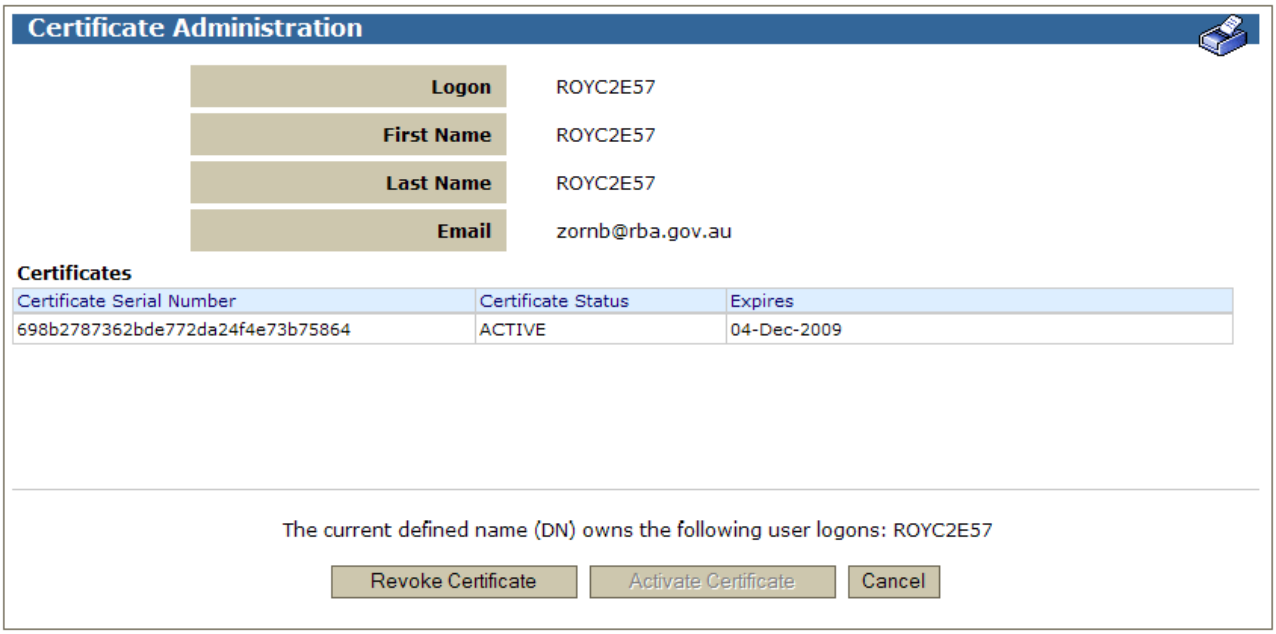
Button	Description
Submit	Select **Submit** to update entries in Authorisations.
Cancel	Select **Cancel** to clear entries and return to the User Details screen.

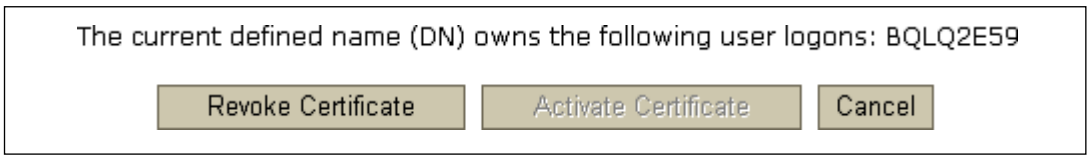
7.9 Specify functions that the user may authorise

Tick or un-tick the boxes supplied to specify the functions that the user may authorise. Use **Submit** to make the entries or **Cancel** to discontinue the action and return to the **User Details** screen.

7.10 Certificate Administration screen

Select the **Certificate Administration** button on the **User Details** screen. The User Details screen can be accessed by selecting the row of a user in the User Privileges screen.





7.10.1 List headings

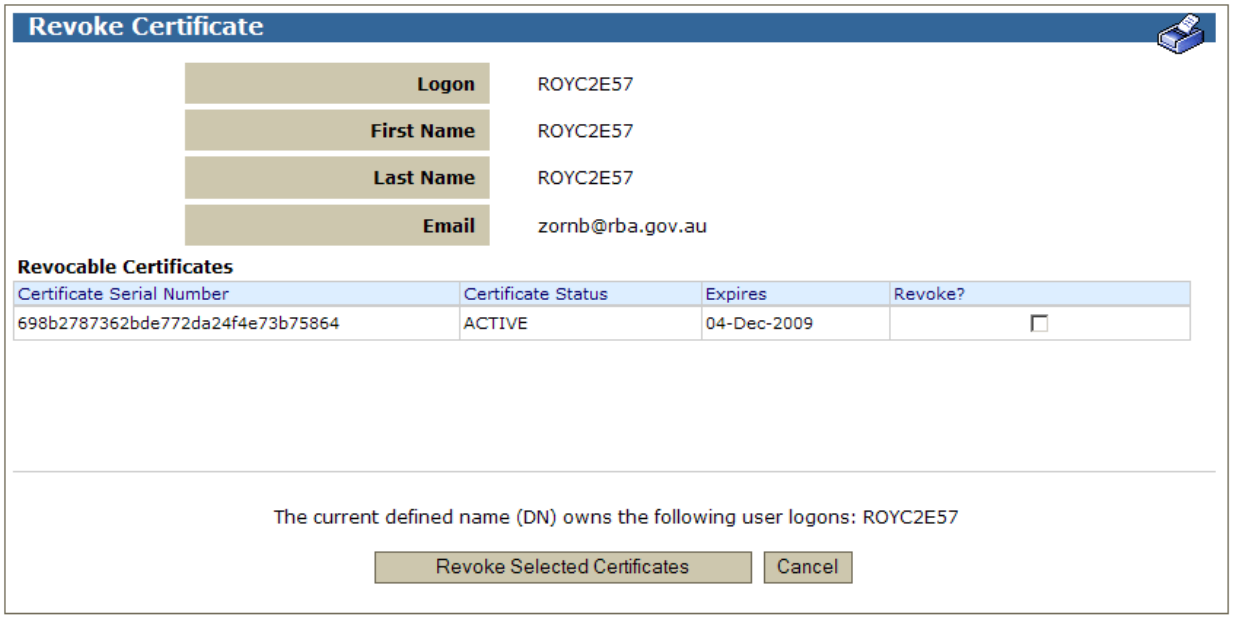
Field	Description
Certificate Serial Number	Displays the Certificate Serial Number.
Certificate Status	Displays the Certificate Status as *Pre-enrolled*, *Collected*, *Active*, *Revoked* or *Expired*.
Expires	Displays the Certificate Expiry date. Certificates are issued with a life of around 2 years.

7.10.2 Actions

Button	Description
Revoke Certificate	Select **Revoke Certificate** to revoke a user's digital certificate. This prevents a user from logging into RITS, or re-logging in after being timed out in a current session. The user still has access to make enquiries in RITS for as long as the session remains active.
Activate Certificate	Select **Activate Certificate** to activate the certificate by entering the Activation Code.
Cancel	Select **Cancel** to return to the User Details screen.

7.11 Revoke Certificate screen

Select **Revoke Certificate** on the **Certificate Administration** screen. The **Certificate Administration** screen can be accessed from the **User Details** screen. The **User Details** screen can be accessed by selecting the row of a user in the **User Privileges** screen.



Select the certificate(s) to revoke by checking the box(es) provided. More than one certificate can be revoked at a time.

Use caution as the action to revoke the certificate(s) takes effect immediately. To provide the user with access to RITS again, the user must enrol for a new certificate.

7.11.1 List headings

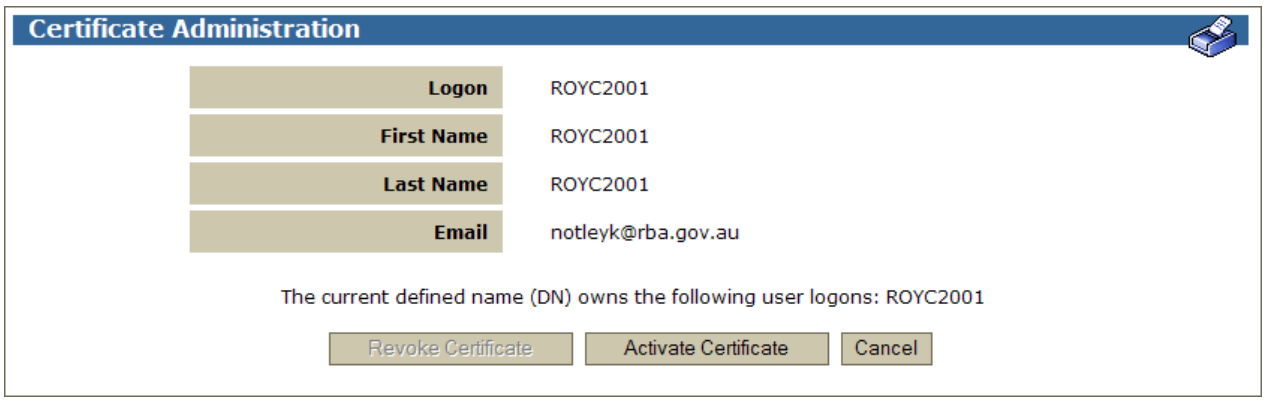
Field	Description
Certificate Serial Number	Displays the Certificate Serial Number.
Certificate Status	Displays the Certificate Status as *Pre-enrolled*, *Collected*, *Active*, *Revoked* or *Expired*. Certificates with an *Active* or *Collected* status may be revoked.
Expires	Displays the Certificate Expiry date.
Revoke?	Tick box entry field. The tick box is available for certificates with an Active or Collected status.

7.11.2 Actions

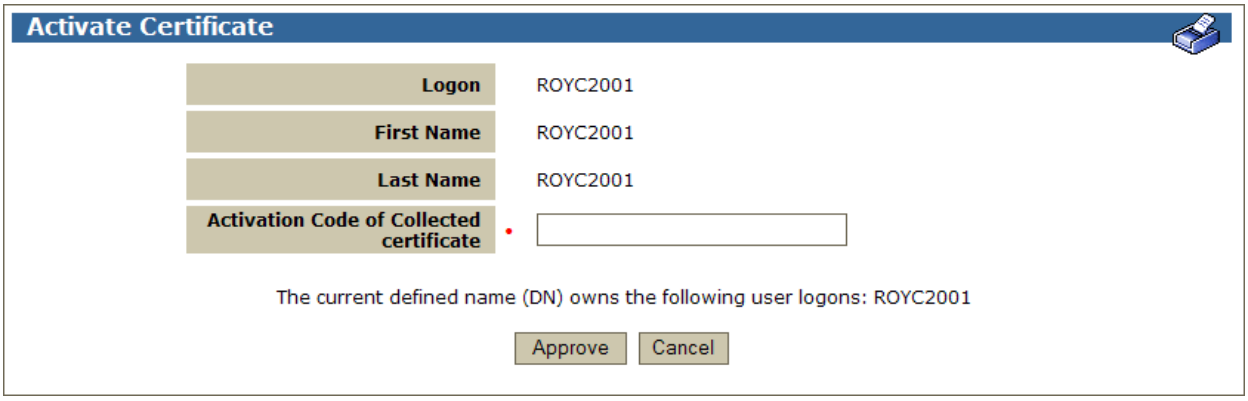
Button	Description
Revoke Selected Certificates	Select **Revoke Selected Certificates** to revoke the certificate(s) selected. This button is greyed out and is unavailable if no certificates in the list are in the status Active or Collected.
Cancel	Select **Cancel** to cancel any selections made and to return to the Certificate Administration screen.

7.12 Activate Certificate screen

Select the **Activate Certificate** button from the **Certificate Administration** screen. The **Certificate Administration** screen is accessed by selecting the **Certificate Administration** button on the **User Details** screen. The **User Details** screen can be accessed by selecting a user in the **User Privileges** screen.



The **Activate Certificate** screen is displayed.



7.12.1 List headings

Field	Description
Logon	Displays the user's logon.
First Name	Displays the user's first name.
Last Name	Displays the user's last name.
Activation Code of Collected Certificate	Entry field for the Activation Code. Copy or type the Activation Code provided by the user into this field. Note that the Activation Code is case sensitive.

7.12.2 Actions

Button	Description
Approve	Select **Approve** to activate the Certificate.
Cancel	Select **Cancel** to cancel any selections made and to return to the Certificate Administration screen.

In the **Activate Certificate** screen, copy or type the Activation Code.

The Activation Code must be entered exactly. Note that it is also case sensitive.

Use **Approve** to activate the certificate.

If the action is unsuccessful (because of an error in entering the code) an error message is displayed.

Use **Cancel** to discontinue the action and return to the Certificate Administration screen.

Appendix – RITS User Password Policy – Special Characters List

The following table lists all characters that can be used as "special characters" in the RITS User Password Policy. No other symbols are permitted.

Character	Name	Unicode
	Space	U+0020
!	Exclamation	U+0021
"	Double quotation mark	U+0022
#	Number sign (hash)	U+0023
$	Dollar sign	U+0024
%	Percent	U+0025
&	Ampersand	U+0026
'	Apostrophe	U+0027
(	Left parenthesis	U+0028
)	Right parenthesis	U+0029
*	Asterisk	U+002A
+	Plus	U+002B
,	Comma	U+002C
-	Minus	U+002D
.	Full stop	U+002E
/	Slash	U+002F
:	Colon	U+003A
;	Semicolon	U+003B
<	Less than	U+003C
=	Equal sign	U+003D
>	Greater than	U+003E
?	Question mark	U+003F
@	At sign	U+0040
[	Left bracket	U+005B
\	Backslash	U+005C

Character	Name	Unicode
]	Right bracket	U+005D
^	Caret	U+005E
_	Underscore	U+005F
`	Grave accent (back tick)	U+0060
{	Left brace	U+007B
|	Vertical bar	U+007C
}	Right brace	U+007D
~	Tilde	U+007E