ANZ TRANSACTIVE – GLOBAL ADMINISTRATION USER GUIDE

September 2019

Public

CONTENTS

OVERVIEW

About this guide

This user guide contains information and procedures for using the Administration component in ANZ Transactive – Global. This user guide will be updated when there is new and/or updated information. Please ensure you regularly check our Online Resources page at anz.com/onlineresources for the most up-to-date copy.

Administration is used to manage the following users:

- ANZ Transactive – Global Cash Management users (account reporting, deposit reporting, payments and direct debits)
- ANZ Commercial Cards users
- ANZ Loans users

Some details may not be relevant for the administration of your users.

Online Help

The online help in ANZ Transactive – Global allows you to access screen-specific help and frequently asked questions.

Online Resources

You can access the ANZ Transactive – Global User Guides and other information from the ANZ Transactive – Global Online Resources page. To access the page, click the Help icon within the application and then the Online Resources link.

Further Assistance

If you require further assistance, please contact your local Customer Service Centre. Details can be found at anz.com/servicecentres.

INTRODUCTION

Administration Models

Your organisation will have been set up with one of the following Administration Models:

- Triple Administration: using this model, an Administrator cannot modify or approve changes to their own permissions, therefore a minimum of three Administrators are required
- Dual Administration: using this model, Administrators can modify their own permissions but require a second Administrator to approve the changes
- Single Administration: where only one Administrator is required to make all changes. This model is only available to Sole Traders or a Proprietary Company with a Sole Director/Secretary.

Organisations using dual or triple administration models will need two or three Administrators to approve some changes that are made to a user. These changes include generating a password for a user, enabling a disabled user and deleting a user.

NOTE: Changes to an Administration Model must be implemented by ANZ and will require paperwork to be signed by authorised signatories.

Administrator Functions

Your organisation has assigned Administrators who can perform the following tasks in ANZ Transactive – Global:

- Create Company Managed users and manage these users (password resets, disabling, enabling and deleting)
- Manage user permissions (Roles and User Attributes)
- Create and manage custom roles*
- Create Account Groups*
- Manage product settings and payment Authorisation Matrixes for each Division that you are entitled to*
- Create and manage Authorisation Panels*
- Create Confidential Data Groups*

* Not available for Administrators who have Commercial Cards roles only

NOTE: Administrators must log in with a security device to have access to administration tasks.

ANZ Managed and Company Managed Users

Users in ANZ Transactive – Global are either ANZ Managed or Company Managed. To check who manages a user, go to the User Management screen and click on View > Managed By > Company Managed on the Control Bar.

Company Managed users

Company Managed users are created and managed solely by your organisation administrators and can perform various tasks depending on the role that is assigned to them. As they can only log in using a password, there are restrictions on what functions they can perform.

NOTE: If your organisation has ANZ Cash Management products and ANZ Commercial Cards, an Administrator must have administration rights for both to be able to view and manage users that are entitled to both products.

ANZ Managed users

Users will be ANZ managed for various reasons, including that they require a security device to perform a particular function in the application. In all instances, ANZ Managed users must be maintained by ANZ. If you need to complete any of the following for an ANZ Managed user, please contact your ANZ representative:

- Modify user details (e.g. name, address, email, phone number)
- Disable/enable a user
- Delete a user
- Generate a password for a user (user to call the Customer Service Centre), this applies to user that log in with password only without Security Device.

USER PERMISSIONS

Users are assigned User Permissions which specify how they interact with the system. A user needs to be assigned:

1. One or more **Roles** which define the tasks that the user can perform in the system such as the ability to approve domestic payments
2. **User Attributes** which specify the accounts, billing entities, loans, approval discretions and payment purposes available to the user within the assigned role

System Roles

System roles are created by ANZ and cannot be edited. If you need to create a custom role, refer to the Create a Custom Role section.

IMPORTANT: If your organisation has both Cash Management and Commercial Cards, your Administrators need to have one Cash Management Administration role plus one Commercial Cards Administration role in order to be able to view and act on all users.

Cash Management Roles

NOTE: Users can be assigned multiple Cash Management roles (account reporting, deposit reporting, payments and direct debits). Users have permissions granted by any of their assigned roles regardless of limitations on their other roles.

ROLE NAME	PERMISSIONS
All Entitlements	• Create, edit, delete, approve, recall, stop or copy all types of payments and direct debits • Resubmit all types of payments • Create, edit, delete, approve, recall or copy all types of payment and direct debit templates • Create, edit, approve and delete beneficiaries in the Payee List • Create, edit, approve and delete payers in the Payer List • Accept Get Rate for International Payments and Transfers • Generate all types of payment and direct debit reports • View and download reports for Operating Accounts • View and download reports for Term Deposits
Approve	• View and approve all types of payments and direct debits • View and approve all types of payment and direct debit templates • Approve beneficiaries in the Payee List • Approve payers in the Payer List • Accept Get Rate for International Payments and Transfers • Generate all types of payment and direct debit reports • View and download reports for Operating Accounts • View and download reports for Term Deposits
Create	• Create, edit, delete, recall, resubmit, stop or copy all types of payments and direct debits • Create, edit, delete, recall or copy all types of payment and direct debit templates • Create, edit and delete beneficiaries in the Payee List • Create, edit and delete payers in the Payer List • Generate all types of payment and direct debit reports • View and download reports for Operating Accounts • View and download reports for Term Deposits
Create & Approve (Not Own)	• Create, edit, delete, recall, stop or copy all types of payments and direct debits • Resubmit all types of payments • Approve payments and direct debits the user has not created or last modified • Create, edit, delete, recall or copy all types of payment and direct debit templates • Approve payment and direct debit templates the user has not created or last modified • Create, edit, approve and delete beneficiaries in the Payee List • Create, edit, approve and delete payers in the Payer List • Accept Get Rate for International Payments and Transfers

ROLE NAME	PERMISSIONS
	• Generate all types of payment and direct debit reports • View and download reports for Operating Accounts • View and download reports for Term Deposits
Reporting	• View and download reports for Operating Accounts • View and download reports for Term Deposits
Customer Admin	• Create and delete users • Edit user details, roles and permissions • Create, edit and delete custom roles • Approve changes made to users and custom roles by other Administrators • Generate user reports **NOTE**: This role can only be assigned by ANZ.

Commercial Cards Roles

NOTE: Users can be assigned only **one** Commercial Cards role.

ROLE NAME	PERMISSIONS
Reporting Officer	• Access assigned billing entities for reconciliation purposes
Authorised to Enquire	• Access assigned billing entities for reconciliation purposes • Enquire and raise service requests for a billing entity and associated cards
Identification Officer	• Verify the identity of new cardholders **NOTE:** This role can only be assigned by ANZ.
Authorised Signatory	• Create and manage Commercial Cards users in Administration. An Authorised Signatory can only view and manage users with the same or fewer (of the same) billing accounts they have access to. • Approve changes made to users by other Administrators • Other Administration functions, including access to Audit History • Access assigned billing entities for reconciliation purposes • Enquire, raise and approve service requests for a billing entity and associated cards **NOTE:** This role can only be assigned by ANZ.
Authorised Signatory + Identification Officer	• Create and manage Commercial Cards users in Administration. An Authorised Signatory can only view and manage users with the same or fewer (of the same) billing accounts they have access to. • Approve changes made to users by other Administrators • Other Administration functions, including access to Audit History • Access assigned billing entities for reconciliation purposes • Enquire, raise and approve service requests for a billing entity and associated cards • Verify the identity of new cardholders **NOTE:** This role can only be assigned by ANZ
User Administration	• Create Company Managed users and manage these users (password resets, disabling, enabling and deleting) • Edit user details, roles and permissions • Approve changes made to users by other Administrators • Generate user reports **NOTES:** • This role can only be assigned by ANZ • It is recommend that a user with this role is assigned access to All Billing Entities so that they can view and manage all Commercial Cards users

Loan Role

NOTE: Users entitled to Loans are managed by an Administrator with the Customer Admin (Cash Management) role.

ROLE NAME	PERMISSIONS
Loan Reporting	• View and download reports for Loans

User Attributes

User Attributes specify the following for each Product Family:

- **Cash Management Product Family:** specify the accounts, term deposits, approval discretions, Confidential Data Groups and payment purposes (Standard/Payroll) available to a user within an assigned role
- **Commercial Cards Product Family:** specify the billing entities available to a user within an assigned role
- **Loans Product Family:** specify the loans available to a user within the role

NOTE: Available user attributes will differ depending on the selected role and your geography.

Cash Management User Attributes

<table>
<tr><th colspan="2">ATTRIBUTE</th><th>DESCRIPTION</th></tr>
<tr><td rowspan="4">Payments</td><td>Account Access</td><td>Details the accounts a user can access for each of the following payment products:
• AU Domestic (Direct Credit)
• AU Domestic (OSKO)
• AU Domestic (RTGS)
• NZ Domestic (Direct Credit)
• NZ Domestic (SCP)
• AU BPAY
• Multibank Payments
• International Payments
• Transfers
Choose one of the following options to specify the accounts a user is entitled to for each payment product:
• Select All to allow the user to access all registered accounts and any accounts registered in the future
• Select Selected to allow the user to access:
> Specific accounts only - click Add to specify one or more accounts
> Account Groups - click Add Account Groups to specify one or more account groups
• Selecting None results in the user not being able to access this payment product</td></tr>
<tr><td>Payment Purpose</td><td>• If Standard is selected, a user can access standard payment products: AU Domestic Payments (Direct Credit, OSKO, RTGS), NZ Domestic Payments (Direct Credit, SCP), AU BPAY, Multibank Payments, International Payments and Transfers
• If Payroll is selected, a user can access Domestic Salary Payments</td></tr>
<tr><td>Confidential Data Group</td><td>Choose one of the following options to specify the Confidential Data Groups a user is entitled to:
• Select All to allow the user to access all Confidential Data Groups and any Confidential Data Groups created in the future
• Select Selected to allow the user to access specific Confidential Data Groups - click Add to specify one or more Confidential Data Groups
• Select None if the user should not have access to any Confidential Data Groups</td></tr>
<tr><td>Approval Discretions</td><td>Details the payment discretion limits a user is entitled to approve. These can be:
• Daily – The total amount a user is permitted to approve in one day
• Transaction – The amount a user is permitted to approve for one transaction (including single items within a batch)
• Batch – The amount a user is permitted to approve for a total batch
Enter Daily, Batch and Transaction approval limits for each available payment type. Leave a field blank to set no limit.
By default, approval discretions are set according to the following table:
<table>
<tr><th>PAYMENT TYPE</th><th>DAILY</th><th>BATCH</th><th>TRANSACTION</th></tr>
<tr><td>AU Domestic (Direct Credit)</td><td>AUD1,000,000</td><td>No value set</td><td>No value set</td></tr>
<tr><td>AU Domestic (OSKO)</td><td>AUD25,000</td><td>No value set</td><td>No value set</td></tr>
<tr><td>AU Domestic (RTGS)</td><td>AUD25,000</td><td>No value set</td><td>No value set</td></tr>
<tr><td>NZ Domestic (Direct Credit)</td><td>AUD1,000,000</td><td>No value set</td><td>No value set</td></tr>
</table></td></tr>
</table>

ATTRIBUTE		DESCRIPTION
		NZ Domestic (SCP) | AUD25,000 | No value set | No value set AU BPAY | Unlimited | No value set | No value set Multibank Payments | Unlimited | No value set | No value set International Payments | AUD25,000 | No value set | No value set Transfers | Unlimited | NA | No value set **NOTE:** Where multiple roles set conflicting approval discretion values for a payment type, the lowest approval discretion value will apply.
Balance & Transaction Reporting	Operating Accounts Account Access	Details the Operating Accounts a user can access for reporting. Choose one of the following options to specify the accounts a user is entitled to: • Select **All** to allow the user to view and generate reports for all registered accounts and any accounts registered in the future • Select **Selected** to allow the user to view and generate reports for specific accounts only - click **Add** to specify one or more accounts • Selecting **None** gives the user access to no accounts for reporting
	Deposits Account Access	Details the Term Deposits a user can access for reporting. Choose one of the following options to specify the deposits a user is entitled to: • Select **All** to allow the user to view and generate reports for all registered term deposits and any term deposits registered in the future • Select **Selected** to allow the user to view and generate reports for specific term deposits only - click **Add** to specify one or more term deposits • Selecting **None** gives the user access to no term deposits for reporting
Receivables	Account Access	Details the accounts a user can access for the following receivable products: • AU Domestic (Direct Debit) • NZ Domestic (Direct Debit) Choose one of the following options to specify the accounts a user is entitled for each receivable type. • Select **All** to allow the user to access all registered accounts and any accounts registered in the future • Select **Selected** to allow the user to access: > Specific accounts only - click **Add** to specify one or more accounts > Account Groups - click **Add Account Groups** to specify one or more account groups • Selecting None results in the user not being able to access this receivable product
	Approval Discretion	Details the receivable discretion limits a user is entitled to approve. These can be: • **Daily** – The total amount a user is permitted to approve in one day • **Transaction** – The amount a user is permitted to approve for one transaction (including single items within a batch) • **Batch** – The amount a user is permitted to approve for a total batch Enter Daily, Batch and Transaction approval limits for each available receivable type. Leave a field blank to set no limit. By default, approval discretions are set according to the following table: **PAYMENT TYPE** | **DAILY** | **BATCH** | **TRANSACTION** AU Domestic (Direct Debit) | Unlimited | No value set | No value set NZ Domestic (Direct Debit) | Unlimited | No value set | No value set

Commercial Cards User Attributes

SETTING	DESCRIPTION
Billing Entities	Details the Billing Entities a user can access for Commercial Cards. Choose one of the following options to specify the billing entities a user is entitled to: • Select **All** to allow the user to access all registered billing entities and any billing entities registered in the future

SETTING	DESCRIPTION
	• Select **Selected** to allow the user to access specific billing entities only - click **Add** to specify one or more billing entities

Loans User Attributes

SETTING	DESCRIPTION
Loan Reporting	Details the Loans a user can access for reporting. Choose one of the following options to specify the accounts a user is entitled to: • Select **All** to allow the user to view and generate reports for all registered loans and any loans registered in the future • Select **Selected** to allow the user to view and generate reports for specific loans only - click **Add** to specify one or more loans

Managing Multiple Roles

Where users have multiple roles, each of their roles may have different permissions. In these instances, users will have permissions granted by *any* of their assigned roles regardless of limitations on their other roles, e.g.:

If a user has the following Roles and User Attributes:

- **Create** role with access to **All** accounts for Direct Credit payments; and
- **Create & Approve (Not Own)** role with access to **selected accounts only** for Direct Credit payments; and
- **Approve** role with access to no accounts for Direct Credit payments;

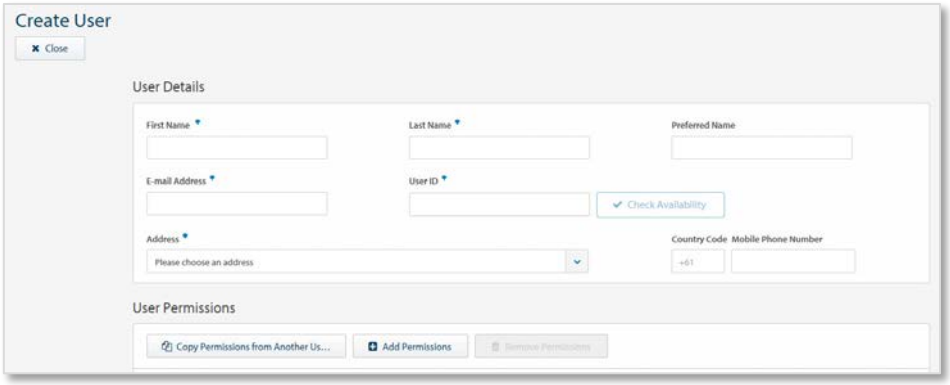
Then the user will be able to:

- Create Direct Credit payments using all registered accounts, regardless of what is specified in the **Create & Approve (Not Own)** role; and
- Approve Direct Credit payments (other than their own) from those accounts specified in the **Create & Approve (Not Own)** role, regardless of the limitations on the **Approve** role.

CREATE USER

Administration > Create User

The Create User screen allows you to create a Company Managed user in ANZ Transactive – Global. To add an ANZ Managed user, contact ANZ.

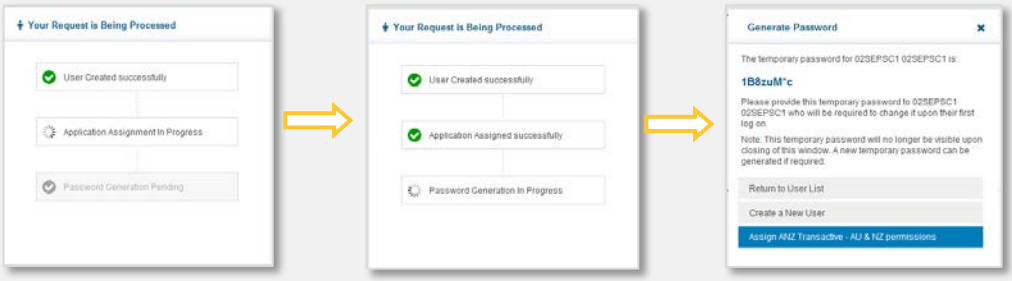


To create a Company Managed user, follow the steps below:
NOTE: Mandatory fields are marked with an asterisk.

STEP	ACTION
1	On the Menu, click **Administration** > **Create User**. **RESULT:** The Create User screen is displayed.
2	Complete the **User Information** details:

FIELD	HOW TO COMPLETE
First Name*	Enter the user's legal first name.
Last Name*	Enter the user's legal surname or family name.
Preferred Name	Details entered into the First Name field will be automatically transferred to this field. To change the user's Preferred Name, simply type over the existing text.
Email Address*	Enter the user's email address. ANZ recommends email addresses are personal to the user being registered, as this is used for emailed scheduled reports.
User ID*	The User ID field is populated after you enter the user's first and last name and follows this structure: • First four letters of the user's surname, then; • First letter of the user's first name, then; • First three letters of the user's organisation name. E.g. The User ID for John Citizen from ABC Co. would be CITIJABC. You can click **Check Availability** to confirm the availability of the User ID. **NOTES:** • Spaces are not permitted • The User ID is not case-sensitive but will be converted to capitals/uppercase • Up to 60 alphanumeric characters and special characters (_ - . @) are permissible, but this is not recommended • Combinations which would result in offensive words or terms can be avoided by substituting letters for numbers with the User ID
Address*	Select an address from the drop-down list or click on **+Add New Address** to add a new address.

FIELD	HOW TO COMPLETE
Address Line 1*	Enter the first line of the user's physical work address. **NOTE:** PO Box addresses must not be entered.
Address Line 2	Enter the second line of the user's address.
City/Suburb*	Enter the suburb or city of the user's address.
State/Province/Region	Enter the state, province or region of the user's address.
Country*	Select the country of residence from the drop-down list.
Zip/Postal Code	Enter the zip or postal code of the user's address.

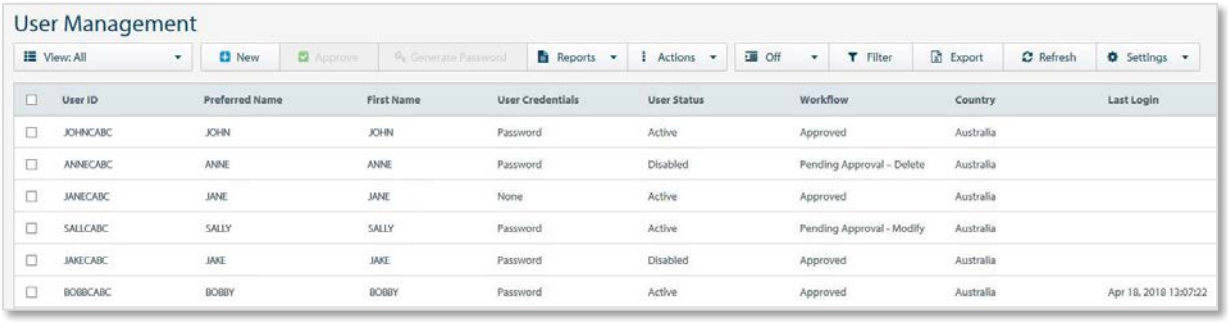
STEP	ACTION
	Country Code and Mobile Phone Number: Enter the user's country calling code in the first field, e.g. +61. Enter the remaining digits of the user's mobile phone number without leading zeros in the second field. E.g. 412 123 456. **NOTE:** Landline numbers must not be entered.
3	Complete the **User Permissions** section: **ACTION** — **STEPS** Copy Permissions from Another User: 1. Click **Copy Permissions from Another User**. **RESULT:** The Select A User pop-up window is displayed. 2. Select another user from the list and click **Copy From User**. **RESULT:** A pop-up message is displayed advising which new permissions have been added to the current user or advising that the selected user's permissions cannot be copied. Add Permissions: 1. Click **Add Permissions**. **RESULT:** The Select A Role pop-up window is displayed. 2. Select a system or custom role to assign to the user and click **Continue**. **RESULT:** The Permissions Settings pop-up window is displayed. 3. If your organisation is set up in a hierarchy, select a Division from the drop-down list. 4. Change the default User Attributes if required and click **Add Permission**. **RESULT:** A confirmation message is displayed and the role will be added to the User Permissions table. **NOTE:** To assign additional roles to the user, repeat this process. Only one Commercial Cards role can be assigned to a user. Remove Permissions: Tick the checkboxes next to permissions in the list you want to remove and click **Remove Permissions**. Edit Permissions: 1. Click the **Settings icon** next to a permission to edit User Attributes. **RESULT:** The Permissions Settings pop-up window is displayed. 2. Choose User Attributes for the role and click **Save**
4	If your organisation uses a panel approval workflow, assign an Authorisation Group (A-J) to the user. **NOTES:** > Applicable only for users that have approval permissions > Only one Authorisation Group can be assigned to a user
5	Click **Submit**. **RESULT:** A "**Your Request is Being Processed**" progress box is displayed. As each stage is completed the progress box will be updated accordingly.  **Stage 1:** User Created **Stage 2:** Application Assigned (if applicable) **Stage 3:** Generate Password
6	• For Organisations that require one Administrator to create and approve requests, a confirmation message is displayed with the password that has been generated for the user. Provide the User ID and temporary password to the new user. The User Status is set to **Active** and the Workflow is set to **Approved**. • For Organisations requiring two or more Administrators to approve requests, the password will be generated upon final approval. The User Status is set to **Active** and the Workflow is set to **Pending Approval - Register**. **NEXT:** Approve/Reject an action made to a user.

USER MANAGEMENT

User Management in ANZ Transactive – Global allows your organisation to view and manage users with access to ANZ Transactive – Global.

User Management Screen

Administration > User Management



- Use the **Control Bar** to quickly and easily access key tasks. See the Getting Started User Guide for full details.
- Use the **View** button to display users by User Status, Workflow Status or Managed By
- Click **New** to Create a User
- Use **Settings** to save the View and Group selected
- Right-click on a user to View, Edit, Delete, Disable, Enable, Approve or Reject an action performed on the user, Generate a Password, View Audit History, generate an Audit History Report, User Activity Report or User Details Report.

User Management Screen Columns

The User Management screen shows the following columns in a grid. If you do not see one of the columns, right click on a column heading and tick the checkboxes next to the columns you wish to see (or click **Reset Grid Columns**).

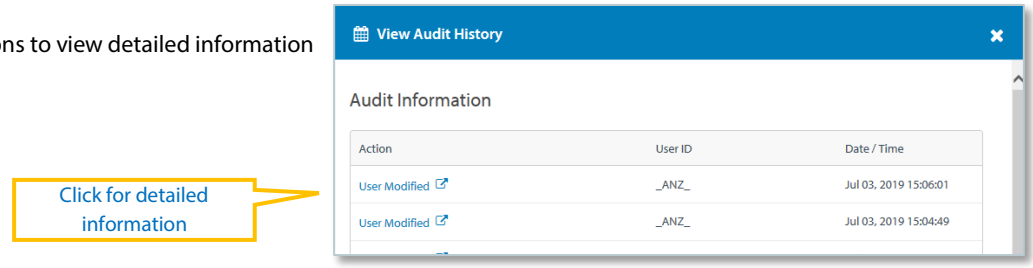
COLUMN	DESCRIPTION
User ID	The unique ID assigned to the user.
Last Name	The user's legal surname or family name.
First Name	The user's legal first name.
Preferred Name	This can be the same or different to the user's First Name or Last Name.
User Credentials	A user's credentials. This can be Password or Security Device and Password or Security Device.
User Status	The current status of the user. Refer to the User Status section for more details.
Workflow	The last action performed on the user by an Administrator. Refer to the Workflow Status section for more details.
Country	The country of the user's address.
Last Login	The last time the user logged into ANZ Transactive – Global.

View User Audit History

To view the actions performed on a user by ANZ or an Administrator, either:

1. Tick the checkbox next to the user in the list and click **Actions > View Audit History** on the Control Bar or
2. Right-click the user in the list and click **View Audit History** in the context menu

Click on individual actions to view detailed information on the changes made.

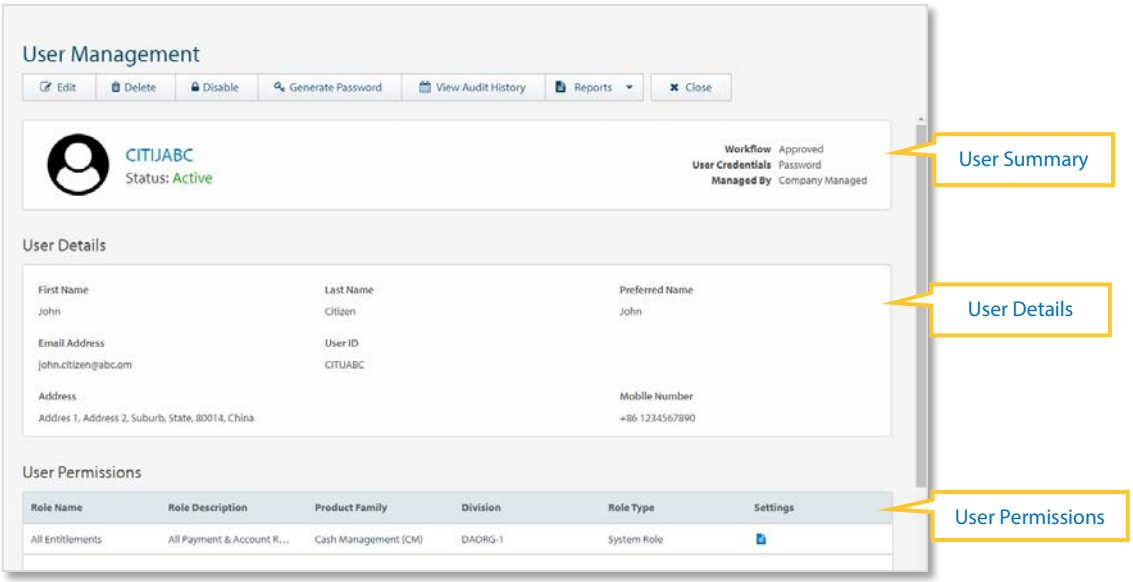


USER DETAILS SCREEN

Administration > User Management > *(select user in list)*

The User Details screen groups a user's information into the following categories:

- User Summary
- User Details
- User Permissions (Roles and User Attributes)



> Use the **Control Bar** to quickly and easily access key tasks. The actions available are dependent on the user Status, Workflow and if they are ANZ or Company managed.

> Click View Audit History to see a history of Administration actions performed on this user

> Click **Reports** to generate a user report

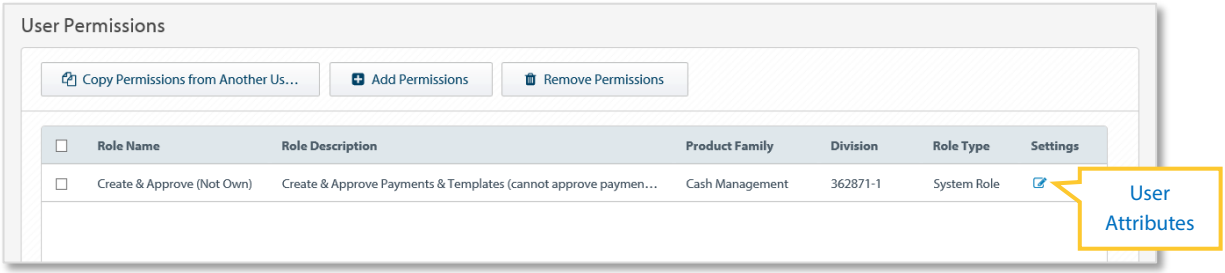
User Summary

FIELD	DESCRIPTION
User ID	The User ID used by the user to log into ANZ Transactive – Global.
Status	The current status of the user. Refer to the User Status section for a description of each User Status.
Workflow	The last action performed on the user by an Administrator. Refer to the Workflow Status section for a description of each Workflow.
User Credentials	Details what type of user credentials are assigned to the user, e.g. Password, Security Device & Password, Security Device.
Managed By	Displays 'Company Managed' if the user is Company Managed or displays 'ANZ' if the user is ANZ Managed.

User Details

FIELD	DESCRIPTION
First Name	The user's legal first name.
Last Name	The user's legal surname or family name.
Preferred Name	The user's preferred name. This can be the same or different to the user's first name or surname.
Email Address	The user's registered email address.
User ID	The unique ID assigned to the user.
Address	The user's registered address.
Mobile Number	The user's registered country calling code and mobile phone number.

User Permissions

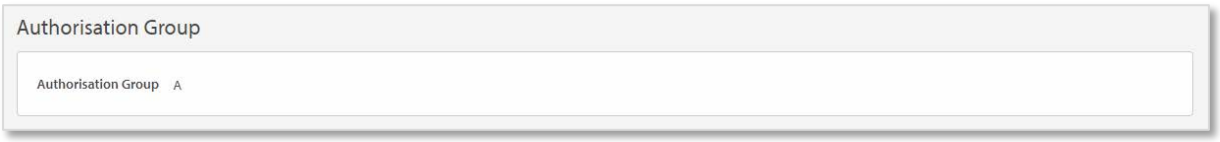


The User Permissions section displays the roles assigned to a user.

- To view Role Permissions, go to the Role Management screen
- To view User Attributes, click on the Settings icon

FIELD/BUTTON	DESCRIPTION
Role Name	The role assigned to the user, e.g. All Entitlements, Reporting Officer.
Role Description	A description of the role.
Product Family	The product family of the role, e.g. Cash Management, Commercial Cards, Loans.
Division	The Division that the role, product family and accounts/billing entities are registered to.
Role Type	The type of role. This can be System (managed by ANZ) or Custom (self-managed).
Settings	Click the **Settings** icon to view **User Attributes** which specify the accounts, billing entities, loans, Confidential Data Groups, approval discretions and payment purposes available to a user within the assigned role.

Authorisation Group



If your organisation uses Authorisation Panels, the Authorisation Group assigned to the user is displayed.
NOTE: Only visible if the user can authorise payments and/or direct debit requests.

WORKFLOW STATUS

The workflow of the user describes the last action that was performed on the user by an Administrator. The table below describes each workflow.

WORKFLOW	DESCRIPTION
Pending Approval - Register	The user has been added to ANZ Transactive – Global and requires approval from another Administrator.
Pending Approval - Deregister	The user has been deregistered by ANZ and is awaiting approval from another ANZ Registration team member.
Pending Approval - Modify	The user's details have been modified and the changes require approval from another Administrator.
Pending Approval - Enable	An Enable action has been performed on the user and requires approval from another Administrator. The user will remain in a 'Disabled' status until approval is provided.
Pending Approval - Password Reset	A Generate Password action has been performed on the user and requires approval from another Administrator before the temporary password will be generated.
Pending Approval - Delete	A Delete action has been performed on the user and requires approval from another Administrator. The user will be set to a 'Disabled' status until approval is provided. A user can be re-enabled from this status.
Approved	One of the following actions has been performed by an Administrator: • Registration of the new user has been approved. User Status will update to Active. • Registration of the new user has been rejected. User Status will update to Deleted. • Modifications made to the user have been rejected and the changes will not be updated. User Status will remain unchanged. • Modifications made to the user have been approved. User Status will remain unchanged. • User has been disabled and the User Status will be set to Disabled. User Status will update to Disabled. • Request to enable the user has been rejected. User Status will update to Disabled. • Request to enable the user has been approved. User Status will update to Active. • Request to generate the password for a user has been rejected. User Status will remain unchanged. • Request to generate the password for a user has been approved. User Status will remain unchanged. • Request to delete the user has been rejected. User Status will update to Disabled. • Request to delete the user has been approved. User Status will update to Deleted.

MODIFY USER DETAILS

To modify details of a Company Managed user, follow the steps below:

NOTE: To modify the details of an ANZ Managed user, contact ANZ.

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	Locate the user in the list. To find a user, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the user in the list to display the **User Details** screen.
4	Click **Edit** on the Control Bar. The following fields are editable: • First Name • Last Name • Preferred Name • Email Address • Address • Phone Number • User Permissions (see the Assign/Modify/Remove a User's Roles and User Attributes section for details)
5	Click **Save** on the Control Bar when the updates have been made. **RESULT:** A confirmation message is displayed. The result depends on the type of user and Administration Model being used: • For organisation that require one Administrator to modify user details, a confirmation message is displayed with user details have been successfully updated. The Workflow is set to **Approved** • For organisation that require two or more administrator to modify user details, the updates to the user will require additional approval. The user's Workflow is set to **Pending Approval - Modify**. Another Administrator must approve the user before the changes are implemented. **NEXT:** Approve/Reject an action made to a user.

GENERATE A PASSWORD FOR A USER

To generate a password for a Company Managed user, follow the steps below:

NOTE: To generate a password for an ANZ Managed user, the user must contact ANZ.

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	Locate the user in the list. To find a user, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the user in the list to display the **User Details** screen.
4	Click **Generate Password** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes** to proceed with the request. **RESULT:** • For Organisations that require one Administrator to create and approve requests, a confirmation message is displayed with the password that has been generated for the user. Provide the temporary password to the user. The Workflow will be **Approved**. • For Organisations requiring two or more Administrators to approve requests, the password will be generated upon final approval. The Workflow is set to **Pending Approval - Password Reset**. Another Administrator must approve the request. **NEXT:** Approve/Reject an action made to a user.

DISABLE A USER

To disable a Company Managed user, follow the steps below:

IMPORTANT: When you disable a user's access, they will be unable to log into the system. The following functions will still operate:

- 'In-flight' payments and direct debit requests that the user created before they were disabled will continue to move through the payment approval and release process
- Any payments or direct debit requests released by the user **prior** to being disabled will continue to be extracted and processed by ANZ systems
- Any payment schedules established by the user will continue to be acted on
- You will continue to be charged for any of these activities that result in a fee

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	Locate the user in the list. To find a user, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the user in the list to display the User Details screen.
4	Click **Disable** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes**. **RESULT:** A confirmation message is displayed to confirm that the user has been disabled. The User Status will be set to **Disabled**.

ENABLE A USER

To enable a Company Managed user's access to ANZ Transactive – Global and all underlying applications, where they have been disabled, follow the steps below.

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	On the Control Bar, click **View** > **User Status** > **Disabled**.
3	Click the user in the list to display the User Details screen.
4	Click **Enable** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes** to proceed with the request. **RESULT:** • For Organisations that require one Administrator to create and approve requests, a confirmation message is displayed to confirm that the user has been enabled. The User Status is set to **Active** and the Workflow is set to **Approved**. • For Organisations requiring two or more Administrators to approve requests, the user will have a User Status of **Disabled** and a Workflow of **Pending Approval – Enable**. Another Administrator must approve the user before they are enabled. **NEXT:** Approve/Reject an action made to a user

DELETE A USER

To delete a Company Managed user, follow the steps below:

NOTES:

- To delete an ANZ Managed user, contact ANZ
- This action **cannot** be reversed. Once a user has been deleted, the user must be recreated to reinstate their access.

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	Locate the user in the list. To find a user, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the user in the list to display the User Details screen.
4	Click **Delete** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes** to proceed with the request. • For Organisations that require one Administrator to create and approve requests, a confirmation message is displayed to confirm that the user has been deleted. The User Status is set to **Deleted** and the Workflow is set to **Approved**. • For Organisations requiring two or more Administrators to approve requests, the User Status is set to **Disabled** and a Workflow of **Pending Approval - Delete**. The user remains in the Disabled status until the Delete action is either approved or rejected by another Administrator. **NEXT:** Approve/Reject an action made to a user.

ASSIGN/MODIFY/REMOVE A USER'S ROLES AND USER ATTRIBUTES

To assign, modify or remove roles and user attributes for a user, follow the steps below.

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	Locate the user in the list. To find a user, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the user in the list to display the **User Details** screen.
4	Click **Edit** on the Control Bar.
5	Choose one of the following actions: **ACTION** — **STEPS** Copy Permissions from Another User — 1. Click **Copy Permissions from Another User**. **RESULT:** The Select A User pop-up window is displayed. 2. Select another user from the list and click **Copy From User**. **RESULT:** A pop-up message is displayed advising which new permissions have been added to the current user, or advising that the selected user's permissions cannot be copied. Add Permissions — 1. Click **Add Permissions**. **RESULT:** The Select A Role pop-up window is displayed. 2. Select a role to assign to the user and click **Continue**. **RESULT:** The Permissions Settings pop-up window is displayed. 3. If your organisation is set up in a hierarchy, select a Division from the drop-down list. 4. Choose User Attributes for the role 5. Click **Add Permission** **RESULT:** A confirmation message is displayed and the role will be added to the User Permissions table.

STEP	ACTION	
		NOTES: • To assign additional roles to the user, repeat this process. Only one Commercial Cards role can be assigned to a user. • For more information on Roles and User Attributes, refer to the User Permissions section.
	Remove Permissions	Tick the checkboxes next to permissions in the list you want to remove and click **Remove Permissions**.
	Edit Permissions	1. Click the **Settings icon** next to a permission to edit settings for that permission. **RESULT:** The Permissions Settings pop-up window is displayed. 2. Choose User Attributes for the role and click **Add Permission**
6	Click **Save** on the Control Bar. **RESULT:** • For Organisations that require one Administrator to create and approve requests, the Workflow is set to **Approved**. • For Organisations requiring two or more Administrators to approve requests, the Workflow is set to **Pending Approval - Modify**. **NEXT:** Approve/Reject an action made to a user	

APPROVE OR REJECT AN ACTION MADE TO A USER

If your organisation is set up with a Dual or Triple Administration Model, you will need to approve or reject certain actions made to a user. The following actions need approval:

- Creating a user
- Modifying a user's permissions
- Modifying a user's details
- Generating a password for a user
- Enabling a user
- Deleting a user

To **APPROVE** an action made to a Company Managed user, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	On the Control Bar, click **View** > **Workflow Status**, then click: • **Pending Approval - Register** (to approve the creation of a new user) • **Pending Approval - Modify** (to approve modifications made to a to a user's permissions) • **Pending Approval - Password Reset** (to approve a password generated for a user) • **Pending Approval - Enable** (to approve the enabling of a user) • **Pending Approval - Delete** (to approve the deletion of a user)
3	Click the user in the list to display the User Details screen.
4	Click **Approve** on the Control Bar. **RESULT:** A confirmation message is displayed.

STEP	ACTION
5	Click **Yes**. **ACTION APPROVED** — **RESULT** Creation of user — A Generate Password pop-up window is displayed with the user's temporary password. Provide the User ID and password to the new user. The user will be required to change this password when they log in next. The user will now have a User Status of **Active** and a Workflow of **Approved**. Modifications made to permissions — A confirmation message is displayed advising that your action has been successful. The updates to the user will be implemented and the Workflow will update to **Approved**. Password generation — A Generate Password pop-up window is displayed with the user's new temporary password. Ensure you take note of the password on screen and provide it to the appropriate user or person who initiated the password generation. The user will be required to change this password when they login next. The user will now have a Workflow of **Approved**. Enabling the user — A confirmation message is displayed advising that your action has been successful. The user will have a User Status of **Active** and a Workflow of **Approved.** Deleting the user — A confirmation message is displayed advising that your action has been successful. The User Status is set to **Deleted** and the Workflow is **Approved**.

To **REJECT** an action made to a Company Managed user, follow the steps below:

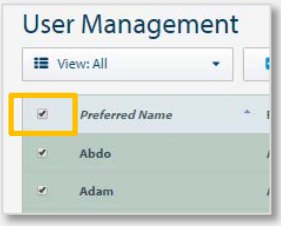
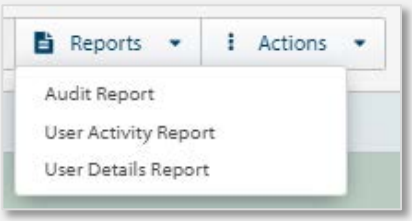
STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	On the Control Bar, click **View** > **Workflow Status**, then click: • **Pending Approval - Register** (to reject the creation of a new user) • **Pending Approval - Modify** (to reject modifications made to a user) • **Pending Approval - Password Reset** (to reject a password generated for a user) • **Pending Approval - Enable** (to reject the enabling of a user) • **Pending Approval - Delete** (to reject the deletion of a user)
3	Click the user in the list to display the User Details screen.
4	Click **Reject** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes**. **RESULT:** A Reject Comments window is displayed requesting a reason.
6	Enter your rejection reason and click **Submit** to confirm your action. **ACTION REJECTED** — **RESULT** Creation of user — The user will now have a User Status of **Deleted** and a Workflow of **Approved**. Modifications made to user — The changes made to the user will not be implemented and the Workflow will update to **Approved**. Password generation — The User Status will remain as it was and the Workflow will be **Approved**. Enabling the user — The user will have a User Status of **Disabled** and a Workflow of **Approved**. Deleting the user — The User Status remains **Disabled** and the Workflow is **Approved**.

USER REPORTS

There are three types of user reports that can be generated:

REPORT	DESCRIPTION	FORMATS
Audit Report	Details the actions that have been made to a user, the Administrator who performed the action and when it occurred.	CSV, PDF
User Activity Report	Provides a report detailing users' interactions with the system, including timestamps, IP addresses, services, functions and actions involved. Can be generated from Administration or Report Centre.	CSV, PDF
User Details Report	Provides a user's general details and the applications, roles, account access and approval discretions assigned to the user.	CSV, PDF

To generate a report for one or more users, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **User Management**. **RESULT:** The User Management screen is displayed.
2	Locate the user in the list. To find a user, click **Filter** on the Control Bar and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Tick the checkboxes next to the users to be included in the report. **HINT:** To select all users, tick the box next the first column header: 
4	Select the required report from the **Reports** drop-down on the Control Bar:  **RESULT:** The Generate Report pop-up window will display.
5	Enter the required criteria and click **Submit**. **RESULT:** A confirmation message is displayed to confirm that the report has been generated. The report will be available in the **Administration > Download Reports** section.

ROLE MANAGEMENT

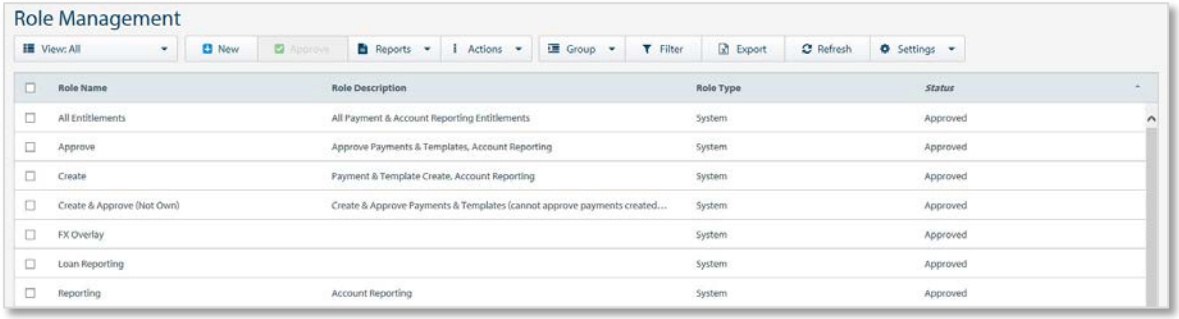
Role Management in ANZ Transactive – Global allows your organisation to view the Role Permissions assigned to each role and to create and edit custom roles.

NOTE: Commercial Card roles are not available in the Role Management screen.

ROLE MANAGEMENT SCREEN

Administration > Role Management

The Role Management screen provides details of System and Custom roles that can be assigned to users in your organisation who have access to ANZ Transactive – Global.



- Use the **Control Bar** to quickly and easily access key tasks. See the Getting Started User Guide for full details
- Use the **View** button to display **All** Approved and Pending Approval roles or **Deleted** to display roles that are in a Deleted status
- Click **New** to Create a Custom Role
- Use **Settings** to save the View and Group selected
- Right-click on a role to View, Edit, Copy, Delete, Approve or Reject, View Audit History or generate a Role Details Report

NOTE: Administrators can view details for system (non-custom) roles but cannot edit them.

Role Management Screen Columns

The Role Management screen shows the following columns in a grid. If you do not see one of the columns, right click on a column heading and tick the checkboxes next to the columns you wish to see (or click **Reset Grid Columns**).

COLUMN	DESCRIPTION
Role Name	The unique name of the role.
Role Description	A brief description of the role.
Role Type	The type of role. This can be System (managed by ANZ) or Custom (self-managed).
Status	The status of the role. Refer to the Role Status section for a description of each role Status.

View Role Audit History

To view the audit history of actions performed on a custom role in ANZ Transactive – Global, either:

1. Tick the checkbox next to the role in the list and click **Actions > View Audit History** on the Control Bar or
2. Right-click the role in the list and click **View Audit History** in the context menu

NOTE: Audit History is not available for system roles.

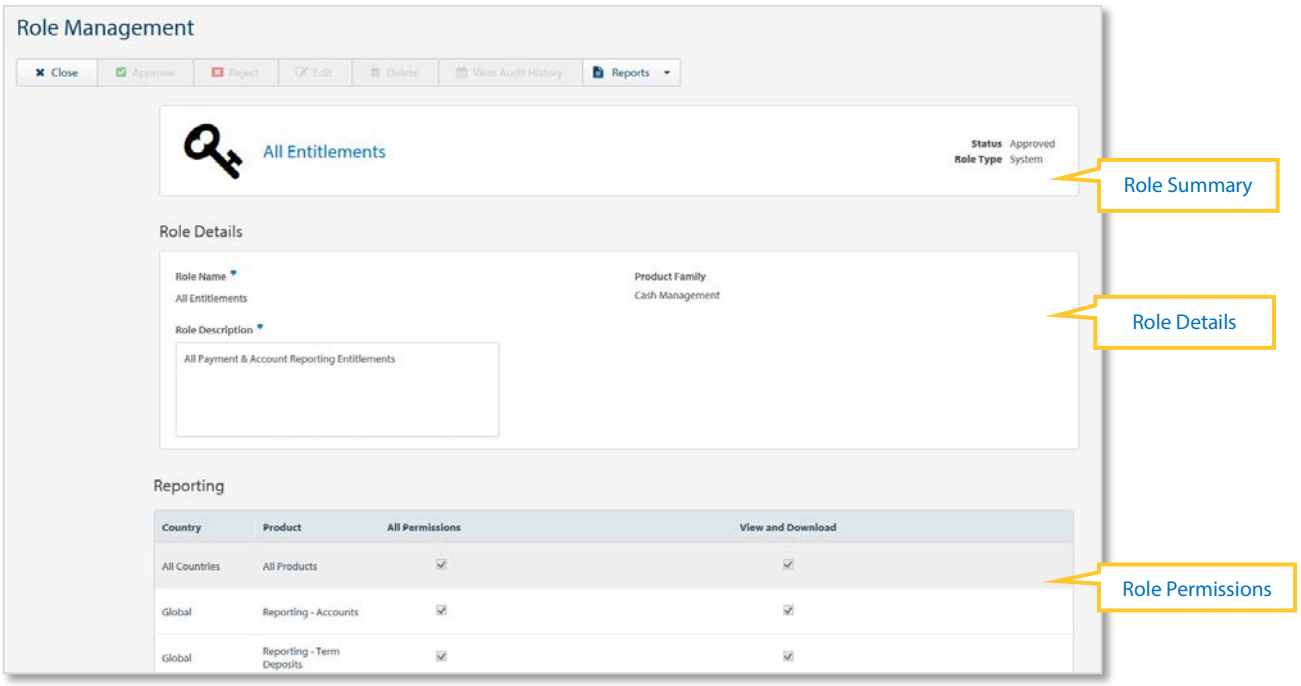
Click on individual actions to view detailed information on the changes made.

Click for detailed information

ROLE DETAILS SCREEN

Administration > Role Management > *(Select role in list)*

The Role Details screen provides information on the permissions the selected role grants to a user.



Use the **Control Bar** to quickly and easily access key tasks. The Actions available are dependent on the role status and if the role is a system or custom role.

- Click View Audit History to see a history of Administration actions performed on this role

Information on the Role Details screen is grouped into the following categories:

- Role Summary
- Role Details
- Role Permissions

Role Summary

FIELD	DESCRIPTION
Role Name	The unique name of the role.
Status	The current status of the role. Refer to the Role Status section for a description of each role status.
Role Type	The type of role. This can be System (managed by ANZ) or Custom (self-managed).

Role Details

FIELD	DESCRIPTION
Role Name	The unique name of the role.
Product Family	The product family of the role, e.g. Cash Management, Loans.
Role Description	A brief description of the role.

Role Permissions

Role permissions detail what a user can do in the system and are grouped into categories i.e. Reporting, Payment Management, Template Management and Payee Management. The table below shows the permissions that can be granted by a role.

NOTES:

- The product categories available depend on your organisation's subscribed ANZ services
- Available accounts, term deposits, loans, Confidential Data Groups, approval limits and payment purposes granted by a role are defined individually under User Attributes

CATEGORY	PERMISSION	DESCRIPTION
Reporting (set permissions for each available Product)	View and Download	View and download reports for Operating Accounts and/or Term Deposits.
Payment Management (set permissions for each available Product)	View	View payments
	Make Payments to Adhoc Payees	View and create payments to ad hoc payees (payees that are not approved in the Payee List). Includes managing payments; edit, delete, recall, resubmit, stop or copy.
	Make Payments using Approved Templates or Payees	View and create payments using approved templates or approved beneficiaries in the Payee List. Includes managing payments; edit, delete, recall, resubmit, stop or copy.
	File Import	View payments and import payment files.
	Get Rate/Trade	View payments and Get Rate/Trade for cross-currency payments.
	Approve	View payments and approve payments created by another user. A user with this permission can also Get Rate/Trade for cross-currency payments.
	Allow Self Approval	View payments and self-approve payments created by the user. Can only be ticked if "Approve" and either "Make Payments to Adhoc Payees" or Make Payments using Approved Templates or Payees" are ticked.
Receivables Management (set permissions for each available Product)	View	View direct debit requests
	Make Payments to Adhoc Payers	View and create direct debit requests to ad hoc payers (payers that are not approved in the Payer List). Includes managing direct debit requests; edit, delete, recall, stop or copy.
	Make Payments using Approved Templates or Payers	View and create direct debit requests using approved templates or approved payers in the Payer List. Includes managing direct debit requests; edit, delete, recall, stop or copy.
	File Import	View direct debit requests and import direct debit files.
	Approve	View direct debit requests and approve direct debit requests created by another user.
	Allow Self Approval	View direct debit requests and self-approve direct debit requests created by the user. Can only be ticked if "Approve" and either "Make Payments to Adhoc Payers" or Make Payments using Approved Templates or Payers" are ticked.
Template Management (set permissions for each available Product)	View	View templates.
	Manage	View, create, edit, delete, recall and copy templates.
	Approve	View templates and approve templates created by another user.
	Allow Self Approval	View templates and self-approve templates created by the user. Can only be ticked if "Manage" and "Approve" are ticked.
Payee Management	View	View beneficiaries in the Payee List.
	Manage	View, create, edit and delete beneficiaries in the Payee List.
	Approve	View beneficiaries and approve beneficiaries added to the Payee List by another user.
	Allow Self Approval	View beneficiaries and self-approve beneficiaries added to the Payee List by the user. Can only be ticked if "Manage" and "Approve" are ticked.

ROLE STATUS

The status of a role describes the last action that was performed on the role by an Administrator. The table below describes each status.

WORKFLOW	DESCRIPTION
Pending Approval	The role has been created or modified and requires approval from another Administrator before it can be assigned to users or before the modifications are implemented.
Pending Approval - Delete	A Delete action has been performed on the role which requires approval from another Administrator. The role cannot be assigned to users.
Approved	The role is able to be assigned to users.
Deleted	The role has been deleted and cannot be assigned to users.

CREATE A CUSTOM ROLE

Custom roles can be created by Administrators in your organisation, allowing you to assign custom permissions. To create a custom role, follow the steps below:

NOTES:

- Currently only Cash Management (account reporting, deposit reporting, payments and direct debits) custom roles can be created
- Users can be assigned multiple custom roles
- Available accounts, deposits, Confidential Data Groups, approval limits and payment purposes granted by a role are defined individually for each user under User Permission Settings

STEP	ACTION
1	On the Menu, click **Administration** > **Role Management**. **RESULT:** The Role Management screen is displayed.
2	Click **New** on the Control Bar. **RESULT:** The New Role screen is displayed.
3	Complete the **Role Details** section: **NOTE:** Mandatory fields are marked with an asterisk. **FIELD** — **HOW TO COMPLETE** Role Name* — Enter a unique Role Name for the role. **NOTES:** • Role Names must be unique. For the purpose of determining this, Role Names are not case-sensitive. • Up to 60 alphanumeric characters and special characters (_ - . @) are permissible, but this is not recommended. Role Description* — Enter a description for the role. **NOTE:** Up to 200 alphanumeric characters and special characters (_ - . @) are permissible.
4	Assign permissions to the role. For details on each permission, see the Role Permissions section. **NOTES:** • Each row represents a Product in a particular Country • Each column represents a permission • Tick the **All Permissions** checkbox in any row to tick all checkboxes in that row • Tick any permission checkbox in the **All Countries** row to tick all checkboxes in that column • The product categories available depend on your organisation's subscribed ANZ services
5	Click **Submit**. **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The Role Status is set to **Approved** and the role can be assigned to users. • Dual/Triple Administration Model: The updates to the role require additional approval. The Role Status is set to **Pending Approval**. Another Administrator must approve the creation of the role before it can be assigned to users. • **NEXT:** Approve/Reject an action made to a role.

EDIT A CUSTOM ROLE

To edit a custom role, follow the steps below:

NOTE: System roles cannot be modified.

STEP	ACTION
1	On the Menu, click **Administration** > **Role Management**. **RESULT:** The Role Management screen is displayed.
2	Locate the role in the list. To find a role, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the role in the list to display the **Role Details** screen.
4	Click **Edit** on the Control Bar. The following fields are editable: • Role Description • Permissions
5	If required, edit the **Role Description**.
6	If required, edit permissions assigned to the role. Users who are assigned this role will have all ticked permissions. For details on each permission, see the Role Permissions section. **NOTES:** • Each row represents a Product in a particular Country • Each column represents a permission • Tick the **All Permissions** checkbox in any row to tick all checkboxes in that row • Tick any permission checkbox in the **All Countries** row to tick all checkboxes in that column • The product categories available depend on your organisation's subscribed ANZ services
7	Click **Save** on the Control Bar when the updates have been made. **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The Role Status is set to **Approved** and the changes are implemented. • Dual/Triple Administration Model: The updates to the role require additional approval. The Role Status is set to **Pending Approval**. Another Administrator must approve the modification before the changes are implemented. **NEXT:** Approve/Reject an action made to a role.

DELETE A CUSTOM ROLE

To delete a custom role, follow the steps below:

NOTES:

- System roles cannot be deleted
- This action **cannot** be reversed. Once a role has been deleted, the role must be recreated to reinstate it.
- A role can only be deleted if it is not currently assigned to any users

STEP	ACTION
1	On the Menu, click **Administration** > **Role Management**. **RESULT:** The Role Management screen is displayed.
2	Locate the role in the list. To find a role, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the role in the list to display the Role Details screen.
4	Click **Delete** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes** to proceed with the request. **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The Role Status is set to **Deleted** and the role can no longer be assigned. • Dual/Triple Administration Model: The updates to the role require additional approval. The Role Status is set to **Pending Approval - Delete** and the role cannot be assigned to users. Another Administrator must approve the Delete action before the changes are implemented. **NEXT:** Approve/Reject an action made to a role.

APPROVE OR REJECT AN ACTION MADE TO A CUSTOM ROLE

If your organisation is set up with a Dual or Triple Administration Model, you will need to approve or reject certain actions made to a role. The following actions need approval:

- Creating a custom role
- Modifying a custom role
- Deleting a custom role

To **APPROVE** an action made to a custom role, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Role Management**. **RESULT:** The Role Management screen is displayed.
2	Locate the role in the list. To find a role, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the role in the list to display the Role Details screen.
4	Click **Approve** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes**. **ACTION APPROVED** — **RESULT** Creating custom role — The role status is set to **Approved** and the role can be assigned to users. Modifying role permissions — A confirmation message is displayed advising that your action has been successful. The updates to the role will be implemented and the role status will update to **Approved**. Deleting the role — A confirmation message is displayed advising that your action has been successful. The role status is set to **Deleted** and the role can no longer be assigned to users.

To **REJECT** an action made to a custom role, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Role Management**. **RESULT:** The User Management screen is displayed.
2	Locate the role in the list. To find a role, click **Filter** and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Click the role in the list to display the Role Details screen.
4	Click **Reject** on the Control Bar. **RESULT:** A confirmation message is displayed.
5	Click **Yes**. **RESULT:** A Reject Comments window is displayed requesting a reason.
6	Enter your rejection reason and click **Submit** to confirm your action. **ACTION REJECTED** — **RESULT** Creating custom role — The role is not created and is removed from the system. Modifying role permissions — The updates to the role will not be implemented and the role status is set to **Approved**. Deleting the role — The Delete action is rejected and the role status is reverted to its previous setting.

ROLE DETAILS REPORT

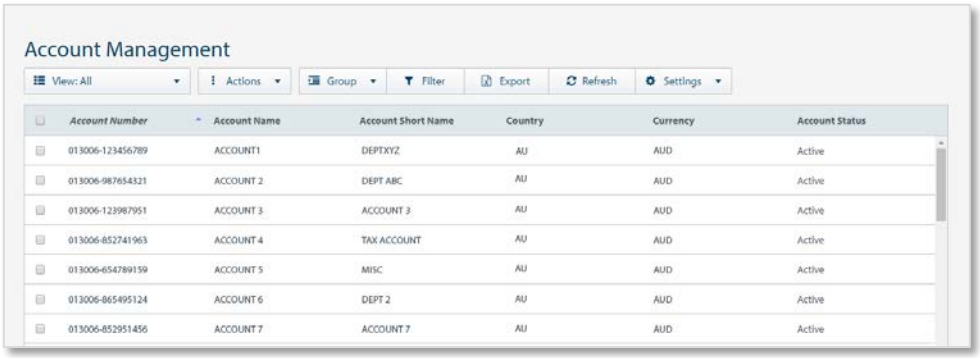
The Role Details Report includes the name, description, type, status and permissions assigned to a role. To generate a Role Details Report for one or more roles, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Role Management**.
2	Locate the role in the list.
3	Tick the checkbox next to the role to be included in the Role Details Report.
4	Click **Reports > Role Details Report** on the Control Bar. **RESULT:** The Generate Report pop-up window will display.
5	Enter the required criteria and click **Submit**. **RESULT:** A confirmation message is displayed to confirm that the report has been generated. The report will be available in the **Administration > Download Reports** section.

ACCOUNT MANAGEMENT

Administration > Account Management

Account Management displays a list of accounts registered to your organisation.



- Use the **Control Bar** to quickly and easily access key tasks. See the Getting Started User Guide for full details.
- Use **Settings** to save the Group selected
- Right-click on a row to View or Edit the account in the list

Account Management Screen Columns

The Account Management screen shows the following columns in a grid. If you do not see one of the columns, right click on a column heading and tick the checkboxes next to the columns you wish to see (or click **Reset Grid Columns**).

COLUMN	DESCRIPTION
Account Number	Registered account number.
Account Name	Registered account name.
Account Short Name	Account name that is displayed in the system. You can change this by editing the account.
Country	The country in which the account is domiciled.
Currency	The currency code of the account.
Account Status	The status of the account: Active, Closed

ACCOUNT DETAILS SCREEN

Administration > Account Management > *(Select account in list)*

The Account Details screen provides information on the account, including the Legal Entity Name, Address, Bank/Branch, the products the account is entitled to and the Account Short Name.

EDIT ACCOUNT SHORT NAME

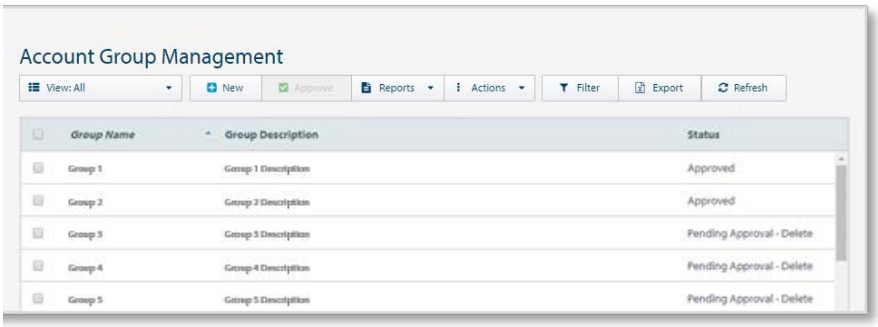
To modify the account name that is displayed in the system, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Account Management**. **RESULT:** The Account Management screen is displayed.
2	Locate the account in the list. To find an account, click **Filter** on the Control Bar and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Right-click on the account in the list and click **Edit.** **RESULT:** The Account Details screen is displayed.
4	Edit the Account Short Name and click on the **Save** button on the Control Bar. **RESULT:** A message will be displayed advising that the account has been modified.

ACCOUNT GROUP MANAGEMENT

Administration > Account Group Management

Account Group Management enables your organisation to group a set of accounts together and entitle the account group to users.



- Use the **Control Bar** to quickly and easily access key tasks. See the Getting Started User Guide for full details.
- Change the View to only see deleted account groups
- Right-click on a row to View, Edit, Delete, Copy, Approve, Reject, View the Audit History of the Account Group or generate an Account Group Report

Account Group Management Screen Columns

The Account Group Management screen shows the following columns in a grid.

COLUMN	DESCRIPTION
Group Name	The Account Group Name assigned by your organisation.
Group Description	The Account Group Description assigned by your organisation.
Status	The status of the account group: Approved, Pending Approval, Pending Approval - Delete

ACCOUNT GROUP DETAILS SCREEN

Administration > Account Group Management > *(Select account group in list)*

The Account Group Details screen provides information on the account group, including the status, last edited details and a list of accounts in the group.

CREATE ACCOUNT GROUP

To create a new Account Group, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Account Group Management**. **RESULT:** The Account Group Management screen is displayed.
2	Click **New** on the Control Bar
3	Enter a **Group Name** and a **Group Description**
4	Click **Add** in the Accounts section. **RESULT:** The **Accounts Search** pop-up window is displayed.
5	Select one or more accounts in the list and click **OK**. **RESULT:** The selected accounts are displayed in the Accounts list.
6	Click **Submit** **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The account group status is set to **Approved** and the account group can be assigned to users • Dual/Triple Administration Model: The account group status is set to **Pending Approval**. Another Administrator must approve the creation of the Account Group before it can be assigned to users. **NEXT:** Approve/Reject an action made to an Account Group

EDIT ACCOUNT GROUP

To edit an Account Group, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Account Group Management**. **RESULT:** The Account Group Management screen is displayed.
2	Locate and click on the account group in the list to display the Account Group Details screen.
3	Click **Edit** on the Control Bar.
4	Edit the account group details as required.
5	Click **Save** on the Control Bar when the updates have been made. **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The account group status is set to **Approved** and the changes are implemented. • Dual/Triple Administration Model: The updates to the account group require additional approvals and the status is set to **Pending Approval**. Another Administrator must approve the modification before the changes are implemented. **NEXT:** Approve/Reject an action made to an Account Group.

DELETE ACCOUNT GROUP

To delete an Account Group, follow the steps below:

NOTE: This action cannot be reversed. Once an Account Group has been deleted it cannot be reinstated.

STEP	ACTION
1	On the Menu, click **Administration** > **Account Group Management**. **RESULT:** The Account Group Management screen is displayed.
2	Locate and click on the account group in the list to display the Account Group Details screen.
3	Click **Delete** on the Control Bar. **RESULT:** A confirmation message is displayed.
4	Click **Yes** to proceed with the request. **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The account group is removed from list. You can view deleted account groups in the View > Deleted menu on the Account Group Management screen Control Bar. • Dual/Triple Administration Model: The updates to the account group require additional approval and the status is set to **Pending Approval – Delete**. Another Administrator must approve the Delete action. **NEXT:** Approve/Reject an action made to an Account Group.

APPROVE OR REJECT AN ACTION MADE TO AN ACCOUNT GROUP

If your organisation is set up with a Dual or Triple Administration Model, you will need to approve or reject certain actions made to an Account Group. The following actions need approval:

- Creating an account group
- Modifying an account group
- Deleting an account group

To **APPROVE** an action made to an Account Group, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Account Group Management**. **RESULT:** The Account Group Management screen is displayed.
2	Locate and click on the account group in the list to display the Account Group Details screen.
3	Click **Approve** on the Control Bar. **RESULT:** A confirmation message is displayed.
4	Click **Yes**.

STEP	ACTION
	ACTION APPROVED / **RESULT** Creating an account group — The account group status is set to **Approved** and can be assigned to users. Modifying an account group — A confirmation message is displayed advising that your action has been successful. The updates to the account group will be implemented and the status will update to **Approved**. Deleting an account group — A confirmation message is displayed advising that your action has been successful. The account group status is set to **Deleted** and can no longer be assigned to users.

To **REJECT** an action made to an account group, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Account Group Management**. **RESULT:** The Account Group Management screen is displayed.
2	Locate and click on the account group in the list to display the Account Group Details screen.
3	Click **Reject** on the Control Bar. **RESULT:** A confirmation message is displayed.
4	Click **Yes**. **RESULT:** A Reject Comments window is displayed requesting a reason.
5	Enter your rejection reason and click **Submit** to confirm your action. **ACTION REJECTED** / **RESULT** Creating an account group — The account group is not created and is removed from the system. Modifying an account group — The updates to the account group will not be implemented and the status is set to **Approved**. Deleting an account group — The Delete action is rejected and the status is reverted to its previous setting.

ACCOUNT GROUP REPORT

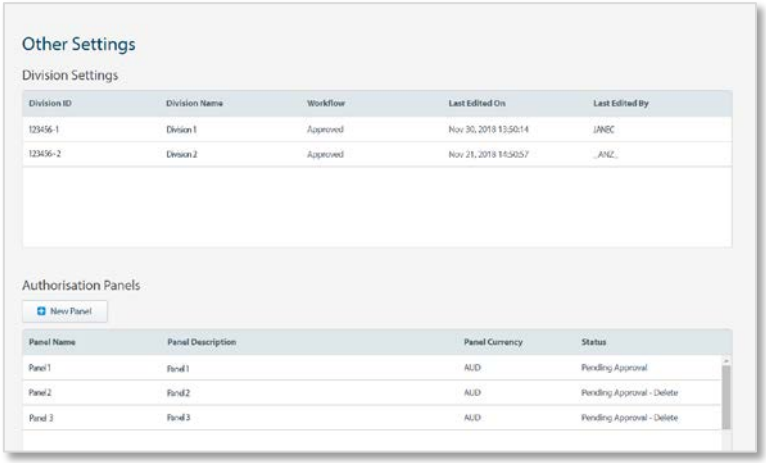
The Account Group Report includes the name, description, type, status and accounts assigned to an account group. To generate an Account Group Report for one or more account groups, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Account Group Management**. **RESULT:** The Account Group Management screen is displayed.
2	Locate the account group in the list. To find an account group, click **Filter** on the Control Bar and enter a search string into one or more of the text fields that appear under the column headings. Search results will be dynamically displayed.
3	Tick the checkbox next to the account group to be included in the report.
4	Click **Reports > Account Group Report** on the Control Bar. **RESULT:** The Generate Report pop-up window will display.
5	Enter the required criteria and click **Submit**. **RESULT:** A confirmation message is displayed to confirm that the report has been generated. The report will be available in the **Administration > Download Reports** section.

OTHER SETTINGS

Administration > Other Settings

Other Settings displays a list of Divisions that are registered to your Organisation, the Authorisation Panels that you have setup for payments and direct debit requests, and Confidential Data Groups that you have created to restrict user access to certain templates and payments.



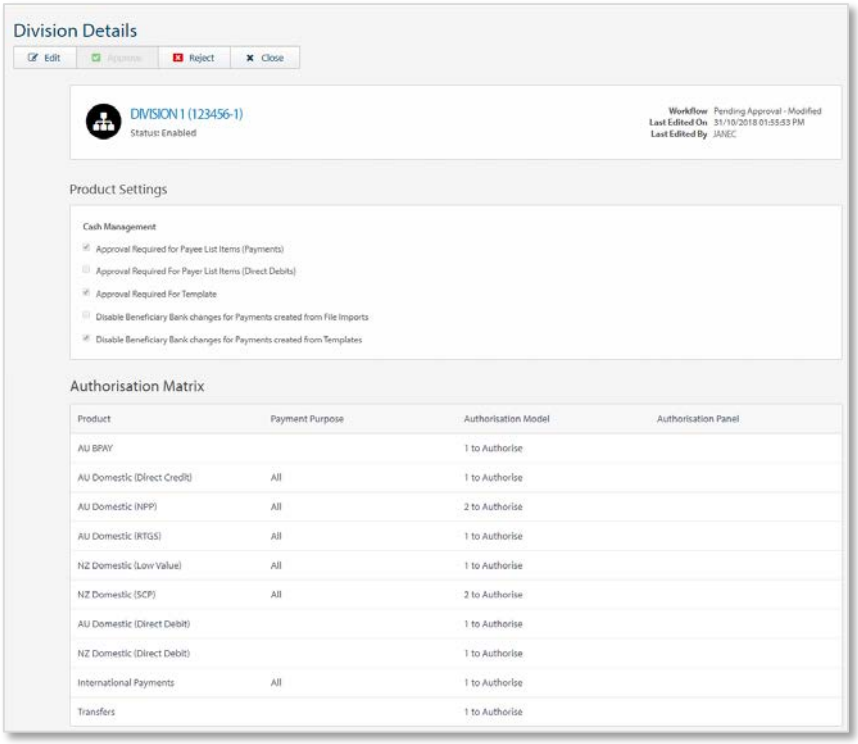
DIVISION SETTINGS

The Division Settings grid displays a list of Divisions that are registered to your Customer ID. You will only see multiple divisions if your Organisation is setup in a hierarchy structure. To view or modify product setting or to define the Authorisation Model for each product; 1 to Authorise, 2 to Authorise or Panel, click on the Division in the grid.

DIVISION DETAILS SCREEN

Administration > Other Settings > *(click Division in list)*

The Division Details screen displays the Product Settings and the payment Authorisation Matrix enabled for the selected Division.



Product Settings

To change the following Product Settings, click on the **Edit** button on the Control Bar:

PRODUCT SETTING	DESCRIPTION
Approval Required for Payee List Items (Payments)	If selected, all new, modified or deleted payees in the Payee List will need to have one approval before the change is implemented.
Approval Required For Payer List Items (Direct Debits)	If selected, all new, modified or deleted payers in the Payer List will need to have one approval before the change is implemented.
Approval Required For Template	If selected, all new, modified or deleted Templates will need to have one approval before the change is implemented.
Disable Beneficiary Bank changes for Payments created from File Imports	If selected, all payments created from file imports will be restricted. Specifically, new beneficiaries cannot be added to a payment and beneficiary details cannot be changed. Note that you can still change the Amount and Lodgement Reference for the beneficiary.
Disable Beneficiary Bank changes for Payments created from Templates	If selected, all templates created will be restricted. Specifically, new beneficiaries cannot be added to a payment and beneficiary details cannot be changed. Note that you can still change the Amount and Lodgement Reference for the beneficiary.

Authorisation Matrix

To change the payment and direct debit Authorisation Matrix, click on the **Edit** button on the Control Bar.

For Domestic Payments, you can change **Payment Purpose**:

> **All:** Provides access to all Payroll and Standard domestic payments
> **Payroll:** Provides access to Domestic Salary Payments
> **Standard:** Provides access to Domestic Payments (Direct Credit, NPP, RTGS), International Payments, BPAY and Transfers

For all payment and direct debit products, you can change the **Authorisation Model:**

> 1 to Authorise
> 2 to Authorise
> Panel (once selected, choose an Authorisation Panel from the drop-down list)

AUTHORISATION PANELS

Administration > Other Settings

Panel approval allows your organisation to setup threshold amounts and up to six approver sequences, for your payments and direct debit requests. You can also create account rules if your organisation needs restrictions on who can approve based on the funding account.

Examples of where changing to panel approval may assist your organisation:

> You need at least three users in the payment approval workflow
> You need to fix the last approver in order to maintain a release step: this user will send payments for processing and will be the only approver who needs a security device
> You want a particular approver sequence to be followed
> You want to restrict user's approving payments for certain thresholds: e.g. payments up to $50,000 need two approvals and payments up to $100,000 need three approvals
> You need payments funded from a specific account to be approved by certain users

Panels can be set up in the following orders:

> **Fixed First:** Fix the first person to approve with any other approvers in random order
> **Fixed:** Fix the entire approval path
> **Fixed Last:** Fix the last person to approve with any other approvers in random order
> **Fixed First & Last:** Fix the first and last person to approve with the other approvers in random order
> **Not Fixed:** The order of approval is random

Let's look at an example where an organisation has eight approvers where:

> One approver who is assigned to Authorisation Group A
> Three approvers are assigned to Authorisation Group B
> Two approvers are assigned to Authorisation Group C
> Two approvers are assigned to Authorisation Group D

The organisation wants to have only certain employees approving payments for certain thresholds, and they want to fix the order of who approves the payments in some instances. The following Panel has been created to ensure that their authorisation rules are adhered to:

Threshold	Sequence	Authorisation Groups						Panel Rules
		1	2	3	4	5	6	
0 > $50,000	Not Fixed	C	D					> A payment up to $50,000 needs two approvals > The approvals can be actioned in any order > One approver needs to be from Authorisation Group C and one from Authorisation Group D > The last approver will need their security device to send the payment for processing
0 > $100,000	Fixed	C	C	B				> A payment up to $100,000 needs three approvals > The first and second approvers needs to be from Authorisation Group C. The last approver needs to be from Authorisation Group B. > The last approver from Authorisation Group B will need their security device to send the payment for processing
0 > $999,999,999	Fixed Last	A	B	C	B			> A payment up to $999,999,999 needs four approvals > The first, second and third approvers need to be from Authorisation Group A, Authorisation Group B and Authorisation Group C in no order > The last approver needs to be from Authorisation Group B > The last approver from Authorisation Group B will need their security device to send the payment for processing

CREATE AN AUTHORISATION PANEL

A Panel can be as simple or as complex as is required. It can contain one or more thresholds, and each threshold can contain one or more sequences of approvers.

To create a new panel, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Other Settings**. **RESULT:** The Other Settings screen is displayed.
2	In the **Authorisation Panel** section, click on the **New Panel** button. **RESULT:** The New Panel screen is displayed.
3	Enter the **Panel Details**: **FIELD** — **DESCRIPTION** Panel Name* — Enter a Panel Name up to 40 characters. Payment Currency* — Select a Payment Currency from the drop-down list. Panel Description* — Enter a Panel Description up to 40 characters.
4	Enter the **Panel Rule 1** details: **FIELD** — **DESCRIPTION** Accounts — Set accounts the panel rule is applied to: • Select **All** to apply the panel rule to all registered accounts and any accounts registered in the future • Select **Selected** to apply the panel rule to specific accounts only (select this option and click **Add** to specify accounts)

STEP	ACTION
5	Enter the **Thresholds** details: **FIELD** — **DESCRIPTION** Threshold 1 Maximum Amount* — Enter the maximum threshold amount the panel can approve in whole dollars, with no commas or spaces e.g. 100000. For an unlimited threshold, type 99999999999. Add approver sequence — Select one or more Authorisation Groups (A-J) from the six drop-down fields. Order — Select the approver order for the panel: • **Fixed First:** Fix the first person to approve with any other approvers in random order • **Fixed:** Fix the entire approval path • **Fixed Last:** Fix the last person to approve with any other approvers in random order • **Fixed First & Last:** Fix the first and last person to approve with the other approvers in random order • **Not Fixed:** The order of approval is random
6	If required, click on the **Add Sequence** button to apply another approval sequence to this threshold and add the approver sequence and order.
7	If required, click on the **Add New Threshold** button to add a new threshold to the panel and repeat Step 5.
8	After all of the panel details have been entered, click **Submit.** **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The panel status is set to **Approved** and the panel is ready to be used. • Dual/Triple Administration Model: The panel requires additional approval before it can be used and the status is set to **Pending Approval**. Another Administrator must approve the panel before it can be used. **NEXT:** Approve/Reject an action made to an Authorisation Panel.

EDIT AN AUTHORISATION PANEL

To edit an Authorisation Panel, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Other Settings**. **RESULT:** A list of Division and Authorisation Panels are displayed.
2	Locate and click on the Authorisation Panel in the list to display the Authorisation Panel Details screen.
3	Click **Edit** on the Control Bar.
4	Edit the panel details as required.
5	Click **Save** on the Control Bar when the updates have been made. **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The panel status is set to **Approved** and the changes are implemented. • Dual/Triple Administration Model: The updates to the panel require additional approvals and the status is set to **Pending Approval**. Another Administrator must approve the modification before the changes are implemented. **NEXT:** Approve/Reject an action made to an Authorisation Panel.

DELETE AN AUTHORISATION PANEL

To delete an Authorisation Panel, follow the steps below:

NOTE: This action cannot be reversed. Once a panel has been deleted, the panel must be recreated to reinstate it.

STEP	ACTION
1	On the Menu, click **Administration** > **Other Settings**. **RESULT:** A list of Division and Authorisation Panels are displayed.
2	Locate and click on the Authorisation Panel in the list to display the Authorisation Panel Details screen.
3	Click **Delete** on the Control Bar. **RESULT:** A confirmation message is displayed.
4	Click **Yes** to proceed with the request. **RESULT:** A confirmation message is displayed. The result depends on the type of Administration Model being used: • Single Administration Model: The panel is removed from the Authorisation Panels list. • Dual/Triple Administration Model: The updates to the panel require additional approval and the status is set to **Pending Approval – Delete**. Another Administrator must approve the Delete action. **NEXT:** Approve/Reject an action made to an Authorisation Panel.

APPROVE OR REJECT AN ACTION MADE TO AN AUTHORISATION PANEL

If your organisation is set up with a Dual or Triple Administration Model, you will need to approve or reject certain actions made to an Authorisation Panel. The following actions need approval:

- Creating an Authorisation Panel
- Modifying an Authorisation Panel
- Deleting an Authorisation Panel

To **APPROVE** an action made to an Authorisation Panel, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Other Settings**. **RESULT:** A list of Division and Authorisation Panels are displayed.
2	Locate and click on the Authorisation Panel in the list to display the Authorisation Panel Details screen.
3	Click **Approve** on the Control Bar. **RESULT:** A confirmation message is displayed.
4	Click **Yes**. **ACTION APPROVED** — **RESULT** Creating panel — The panel status is set to **Approved** and the panel can be used. Modifying panel — A confirmation message is displayed advising that your action has been successful. The updates to the panel will be implemented and the panel status will update to **Approved**. Deleting panel — A confirmation message is displayed advising that your action has been successful and the panel is removed for the Authorisation Panels list.

To **REJECT** an action made to an Authorisation Panel, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Other Settings**. **RESULT:** A list of Division and Authorisation Panels are displayed.
2	Locate and click on the Authorisation Panel in the list to display the Authorisation Panel Details screen.
3	Click **Reject** on the Control Bar. **RESULT:** A confirmation message is displayed.
4	Click **Yes**. **RESULT:** A Reject Comments window is displayed requesting a reason.
5	Enter your rejection reason and click **Submit** to confirm your action. **ACTION REJECTED** — **RESULT** Creating panel — The panel is not created and is removed from the system. Modifying panel — The updates to the panel will not be implemented and the panel status is set to **Approved**. Deleting panel — The Delete action is rejected and the panel status is reverted to its previous setting.

DIVISION DETAILS REPORT

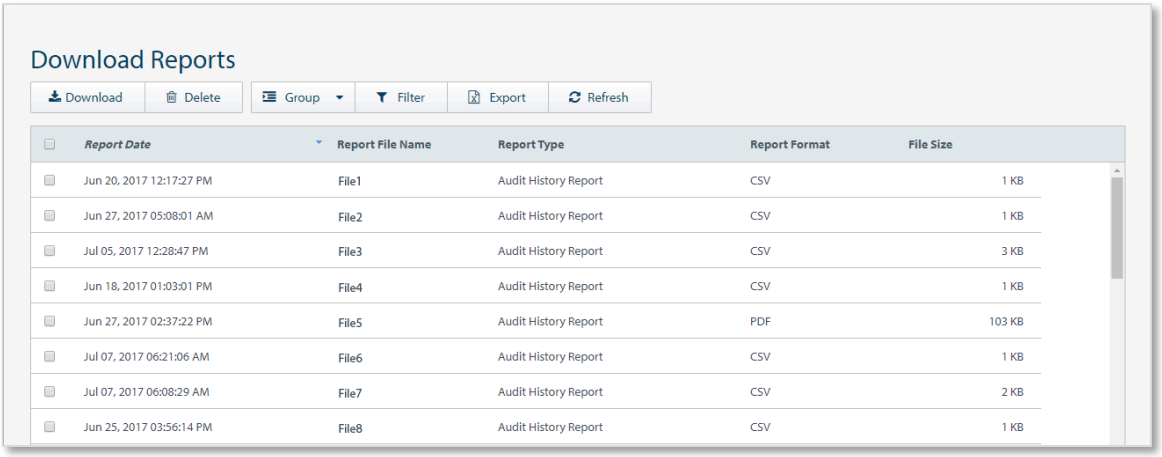
The Division Details Report includes the Customer ID, division details, preferences, Authorisation Matrix and panel details assigned to a division. To generate a Division Details Report for a division, follow the steps below:

STEP	ACTION
1	On the Menu, click **Administration** > **Other Settings**.
2	Click on the Division in the Division Settings list.
3	Click **Reports > Division Details Report** on the Control Bar. **RESULT:** The Generate Report pop-up window will display.
4	Enter the required criteria and click **Submit**. **RESULT:** A confirmation message is displayed to confirm that the report has been generated. The report will be available in the **Administration > Download Reports** section.

DOWNLOAD REPORTS

Administration > Download Reports

From the Download Reports screen in the Administration menu, view all administration reports that have been generated.



From the list, you can select one or more reports in the list and right-click to download or delete the selected reports. It is recommended that you delete files that are no longer required on a regular basis.

Use the **Download** button on the Control Bar to download the files you have selected.

Download Reports Screen Columns

COLUMN	DESCRIPTION
Report Date	Date and time when the report was created.
Report File Name	Name of the report.
Report Type	Type of report, e.g. Audit Report.
Report Format	Format of the report, e.g. CSV, PDF.
File Size	File size of the report.