METRO BANK

Business user guide

Administration, preferences and audit reporting

This guide will help you with administration settings, preferences and audit reporting when using Commercial Online Banking and Business Online Plus.

Verifying actions

To confirm it's you each time you carry out certain actions – such as managing users, adding beneficiaries and making payments – you'll need to generate a one-time passcode with your security device or accept a push notification using the Metro Bank Authenticator app.

Note: if you're offline, or haven't enabled push notifications, you can also use your Metro Bank Authenticator app to generate a one-time passcode – you can read more on that below.

Note: If your security device is lost, damaged or stolen, or you can't access the Metro Bank Authenticator app, call us on 0345 08 08 508 or visit us in store.

Verifying an action using your security device:

- Turn your device on by pressing OK
- Enter your six-digit PIN and press OK
- When 'Select App' appears on the device, enter 1
- Enter the eight-digit security code the device generates into the Code field on your Online Banking screen
- A confirmation message will show up on your Online Banking screen if you've entered your details correctly.

To make payments using the Metro Bank Authenticator app:

If you're online

When you receive a push notification on your mobile:

- tap it to open your Metro Bank Authenticator app
- use your Face ID, fingerprint or pin code to log in
- read the pop-up and tap Accept to proceed or Decline to cancel
- A pop-up will let you know if your approval was successful
- A confirmation message will show up on your Online Banking screen if you've entered your details correctly.

If you're offline

If your phone has no signal you can still approve actions:

- when prompted, click 'Didn't receive a notification' on your Online Banking screen and follow the instructions
- open your Metro Bank Authenticator app
- select Payment Authorisation)
- when prompted use your Face ID, fingerprint or pin code to log in
- Type the passcode you see into your Online Banking screen - it's valid for 30 seconds - and click Next
- A confirmation message will show on your Online Banking screen if you've entered your details correctly.

Levels of authorisation

There are three levels of authorisation for Online Banking. This relates to the number of users who need to approve an action, before that action can take place:

- Single means that **one** user is needed
- Dual means that **two** users are needed
- Verify means that **three** users are needed.

When you set up your Online Banking, you choose the approval level needed for specific actions. To amend the approval level after this, you'll need to get in touch with your Relationship Manager. Once the approval level has been set, you can customise the preferences for each user in the 'User List' tab – it's in the drop-down list below 'Administration' in the left-hand menu. To make changes to individual user rights, you will need the correct approval level from the bank.

There are different options when setting user preferences:

	View	Input	Verify	Authorise
View	x			
Input	x	x		
Verify	x	x	x	
Authorise	x	x	x	x

- **View** means the user can only view the account and transaction history
- **Input** means the user can input payments and beneficiaries
- **Verify** means the user can validate changes made by the Input user
- **Authorise** means the user approves changes made by the Input user, and confirms the approval by the Verify user.

In addition to these user preferences, any of the above users may be able to make admin changes and delete beneficiaries, depending on their individual permissions.

All actions and changes need to be approved in line with the company's authorisation levels and user permissions. For example certain actions may need:

- A second administrator or authoriser if 'Dual' administration has been selected
- A third administrator or authoriser if 'Verify' administration has been selected.

Administration functions

Administrators can manage each user's access to all accounts and companies, including payment limits.

Administration menu

The Administration menu has the following drop-down options:

- User List
- Account Groups
- Access Groups
- Mandates.

User List

This is a list of all current users and their rights (Fig 1). You can use this to manage each user's access rights, account groups, and the mandates assigned to them. Here's how:

- **Search for a user:** type their first and/or last name in the search field. Users can be arranged by name, access group, mandate or account group.
- **Creating user rights:** you can create access groups, mandate or account groups which you can assign to users depending on the business needs.
- **Change access rights for a user:** select a user to amend and choose from the three options under the 'Administration' tab: Account Groups, Access Groups and Mandate. You can then assign users to an existing access group, mandate or account group.
- **Amend access rights for multiple users:** select an access group to view from the 'Administration' tab, and set the access level by ticking or unticking. This will change the user rights for everyone in that group.
- **Add a new user:** please get in touch with your Relationship Manager.

Fig 1: User List

Account Groups

Users need to be in an Account Group to view and manage accounts (Fig 2). You can edit these groups to determine which accounts a user can access. Here's how:

• Select the Account Group you want to edit

• Choose which accounts are included in the group

• You can preview the group's details by clicking the eye icon

• To include an account, search for the name or number on the left-hand side, and then click the arrow on the right-hand side to add it to the 'Include' list

To exclude an account, follow the same steps, but click the arrow for the 'Exclude' list

• You can also use the 'Include All company accounts' or 'Exclude All company accounts' toggles on the right-hand side to edit all your accounts in one go

• Click 'Update' to finish

• You will then be prompted to enter your password and follow the instructions on your Online Banking screen to generate a one-time passcode using your security device or the Metro Bank Authenticator app.

Fig 2: Account Groups

Note: These actions and changes may need to be approved by:

- A second administrator or authoriser if 'Dual' administration has been selected
- A third administrator or authoriser if 'Verify' administration has been selected.

Note: an Account Group can't be deleted once you've created it.

New Account Groups

To create a new account group, select 'Create New' and then follow the same steps as above.

**Note:** once you've created an Account Group, its name can't be changed.

Tip: You can name the account groups by definition - for example, 'Access all accounts' or 'Access all savings accounts'.

Access Groups

Users need to be in an Access Group to view and operate accounts (Fig 3). You can edit these groups to determine the level of access a user has and what actions they can complete. Here's how:

- Choose the Access Group you want to edit
- Set the access level for each user by ticking or unticking
- You can preview the group's details by clicking the eye icon
- Click 'Update' to finish
- You will then be prompted to enter your password and follow the instructions on your Online Banking screen to generate a one-time passcode using your security device or accept a push notification using the Metro Bank Authenticator app.

Fig 3: Access Groups
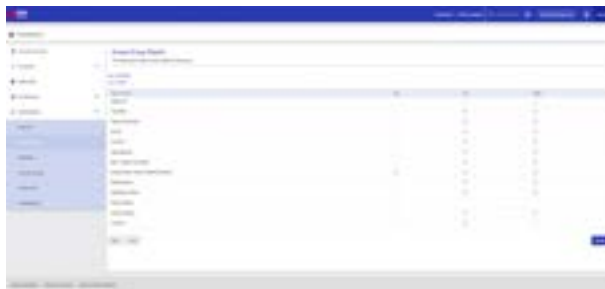
Creating new Access Groups

- Select 'Access Groups' under the Administration tab in the left-hand menu
- Select 'Create New'
- Enter a title, a description, and tick the permissions required
- Click 'Save' to finish
- You will then be prompted to enter your password and follow the instructions on your Online Banking screen to generate a one-time passcode using your security device or accept a push notification using the Metro Bank Authenticator app.

Tip: You can name the Access Groups by definition - for example, 'View and Input' or 'Full Permissions User'.

Mandates

You can use mandates to set transfer and payment value limits for transactions made by users and groups. Here's how:

Creating new Mandates

- Select 'Mandates' under the Administration tab in the left-hand menu
- Click 'Create New'
- Enter the payment limits for each payment type and each authorisation level
- Click 'Save' to finish
- You will then be prompted to enter your password and follow the instructions on your Online Banking screen to generate a one-time passcode using your security device or accept a push notification using the Metro Bank Authenticator app.

Amending existing Mandates

- Select the Mandate you want to edit (Fig 4)
- You can preview the group's details by clicking the eye icon
- Click 'Amend' to change the limits for each transaction type
- Click 'Update' to finish
- You will then be prompted to enter your password and follow the instructions on your Online Banking screen to generate a one-time passcode using your security device or accept a push notification using the Metro Bank Authenticator app.

Note: limits set for each transfer and payment type must be within the overall payment limits set by Metro Bank for your company which is shown on the right hand side of the page. By applying super User Limits and permissions to a mandate group, any user in that group will be able to make payments up to the super user limit without needing further authorisation. Bulk and Batch payments are excluded from Super Limits.

Fig 4: Update Mandate Permissions

Note: once you've created a mandate, its name can't be changed.

Tip: You can name the mandate groups by definition - for example, 'Company Limits or 'Limited to 10K'.

Assigning Mandates, Access Groups and Account Groups to a user

Each user's account on your system will automatically be given default settings (Fig 5). You can change these settings in line with any Mandates, Access Groups or Account Groups you have already set up. Here's how:

- Select the user you want to edit from the 'User List'
- Choose the Mandates, Access Groups and Account Groups you want to assign to the user from the lists on the right-hand side
- You can preview the details by clicking the eye icon
- Click 'Save' to finish.

Fig 5: Assigning Mandates, Access Groups and Account Groups to a user

Setting your preferences

You can choose how you would like to receive your monthly bank statements – by post or paperless. To do this:

- Select 'Preferences' from the 'Administrations' tab
- Use the toggles under the 'Paperless' column to choose which option you want
- Click on the Account Name or Number to go the account's Transaction Summary.

Audit Reporting

Daily audit reports will be created for your company. You can download and view all existing audit reports to see historic payments, transfers, user access rights and all user activity.

To do this, select 'Audit Reports' from the 'Administrations' tab.

Next steps

If the authorisation levels are set as **Dual** or **Verify**, these actions will need to be approved. You can find further help and guidance in the Transaction Approval guide on at **metrobank**online.co.uk.

Need support?

We hope this guide helps you make the most of business banking online. If you have any questions or want to speak to us, call 0345 08 08 508 or visit us in store.