ANZ WORLDLINE
Payment Solutions

ANZ eGATE™
VPC access code & AMA change guide

Summary

This guide will outline the steps required to change the VPC access codes & AMA user passwords on ANZ eGATE™(MIGS).

To comply with Payment Card Industry Data Security Standard (PCI DSS) 4.0, changes are required for Virtual Payment Client (VPC) access codes, and passwords for Advanced Merchant Administration (AMA) users every 365 days. This guide will assist you to regularly update these VPC access codes & AMA passwords.
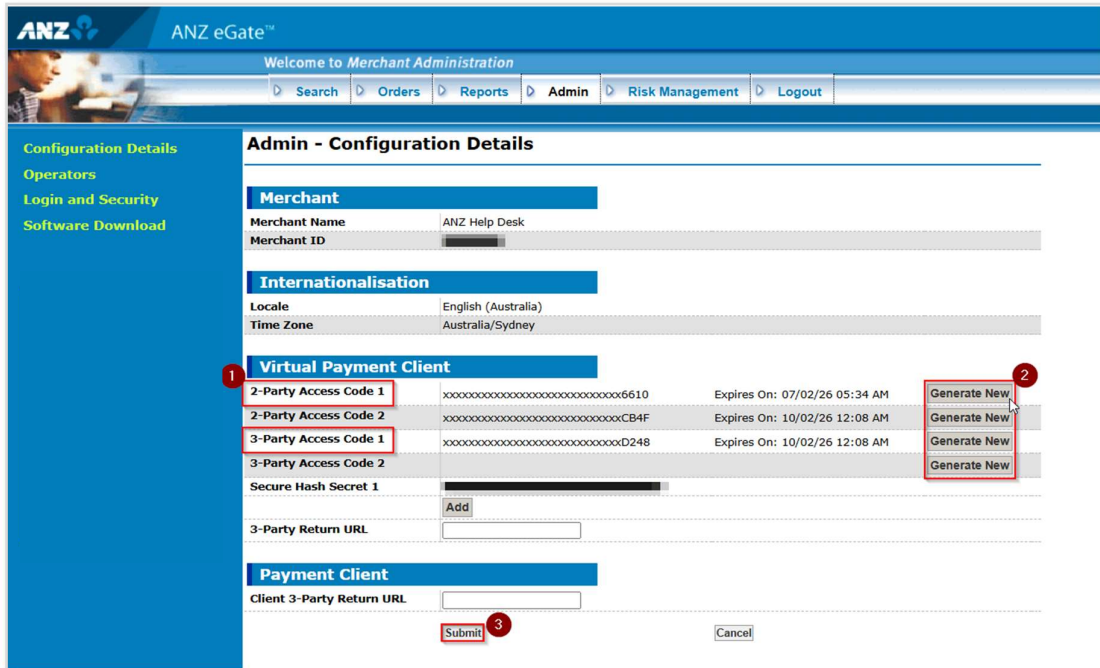
Contents

Generating a new VPC Access Code

1. **Log in to ANZ eGate Merchant Administrator with your Primary Operator account.**
   - Navigate to **Admin** and then **Configuration Details** to access your Access Code page, as shown below.

Note: The account must have "Modify the merchant configuration" enabled in operator permissions. The default administrator superuser cannot be used for this process.

2. **On Configuration Details click on the Edit button, as shown below.**

3. Generate new VPC Access Codes

Referring to the image below:

① On the Edit page, identify which **Access Code** you will require based on your current website/application integration* with **ANZ eGate (MIGS)**:

- **If your website / application uses the Merchant hosted method**, you will require a 2-Party access code.
- **If your website/application uses the Server-hosted** (redirect) method, you will require a 3-Party access code.
- If your website/application is currently using the existing **2-Party Access Code 1 or 3-Party Access Code 1**, you may wish to generate the corresponding **Access Code 2** first to avoid impacting your integration before you have modified the Access Code in your website's backend.

Important: The Access Code will expire after 365 days. It is recommended to set up a reminder notification with two weeks advanced notice to re-action this procedure.

*Refer to the Virtual Payment Client Integration Guide (MIGS) to help you identify which method your website is currently using and the Access Code field to update.

② Click **Generate New**.

③ Copy this code and store separately before clicking **Submit**. Once you click **Submit**, it will mask the generated Access Code and cannot be re-copied.

4. Update your website or API with the copied Access Code.

- Update the "vpc_AccessCode" parameter in your client/website's backend scripts for the payment gateway accordingly.
- If you use a plugin, you will find and update the Access Code field within the plugin settings page.

Note: It is recommended to have an experienced web developer or technician make these updates to your client/website, to ensure this update is made correctly.

5. Test your integration by running a mock payment through your checkout.

- Use test cards to verify the change works.
- Test cards are listed in the last section of this guide, for reference and use.
- If you see a '403 - Authentication Error', then you will need to check if you have updated the "vpc_AccessCode" parameter correctly.
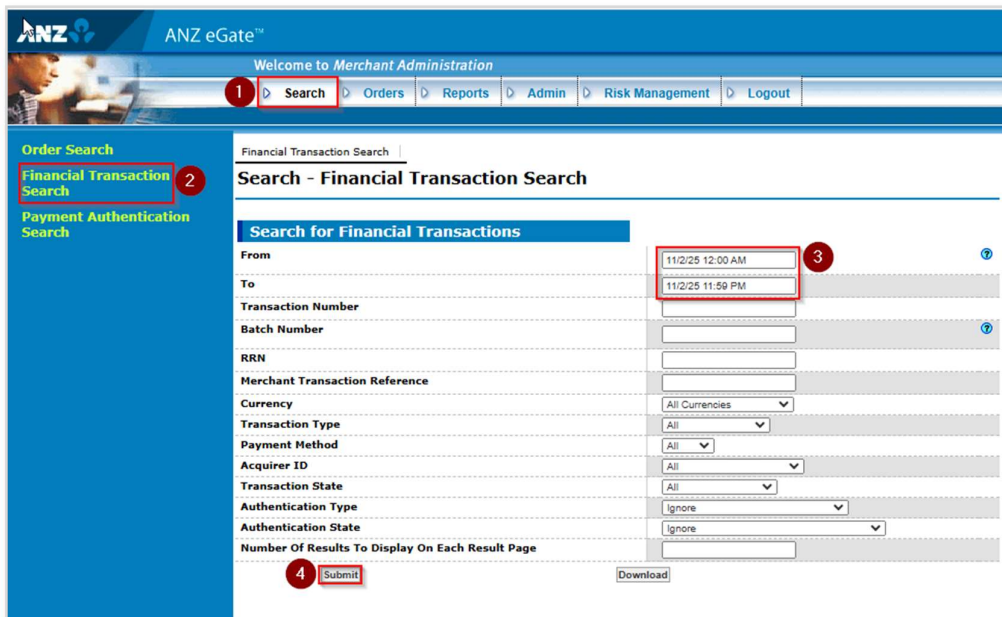
Note: You should not need to use a real card, as you only need to test that the request is passed to the gateway, but the transaction itself does not need to be successful to prove the connection is established.

6. Check your financial records on ANZ eGate

Once you have submitted the payment, you should be able to locate a record of it in **Financial Transaction Search** in **ANZ eGate Merchant Administrator**.

To search, referring to the image below:

① Choose **Search** from the options on top of the screen

② Select **Financial Transaction Search** from the options on the right hand side of the screen

③ Enter the relevant search criteria

④ Press **Submit**

# Generating a new Advanced Merchant Administrator (AMA) password

This is required if you have created an operator with "Advanced Merchant Administration" enabled and using it with the Virtual Payment Client to directly access the MIGS Payment Gateway to perform all transaction related actions (for example, captures, refunds, voids and QueryDR) via integrated merchants' software interfaces.

1. **Log in to ANZ eGate Merchant Administrator with your Primary Operator account, as shown below.**

   Note: This account must have "Perform operator administration" enabled in operator permissions. The default administrator superuser can also be used for this process.
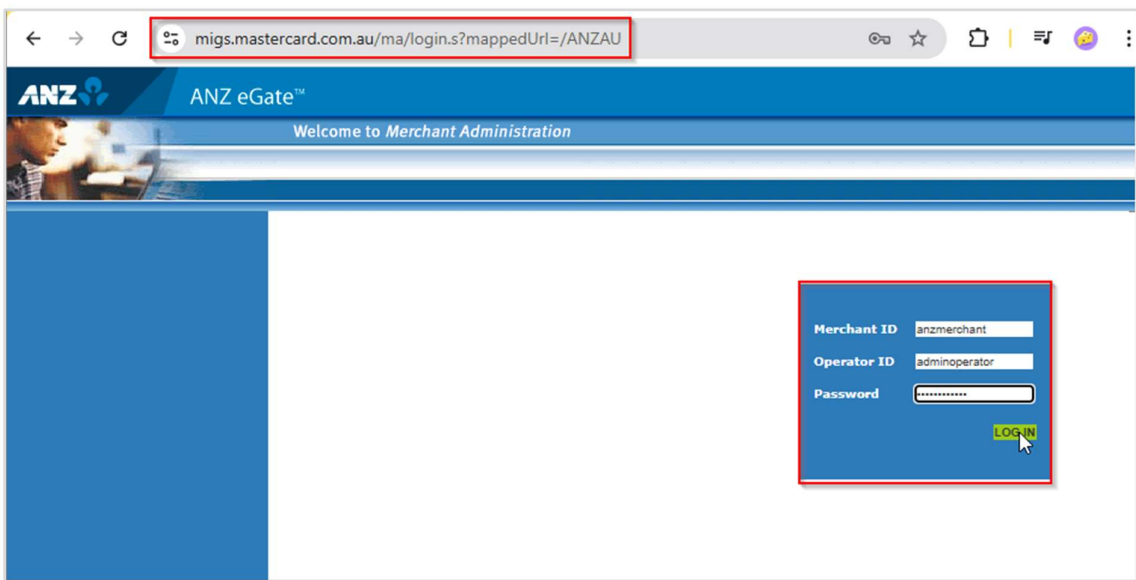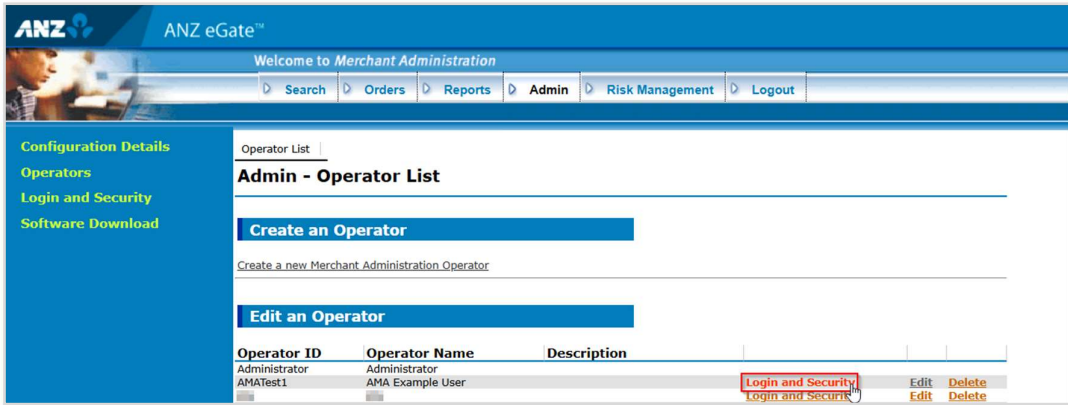

2. **Navigate to <u>Admin</u> and then <u>Operators</u> to access your Operators list, as shown below.**
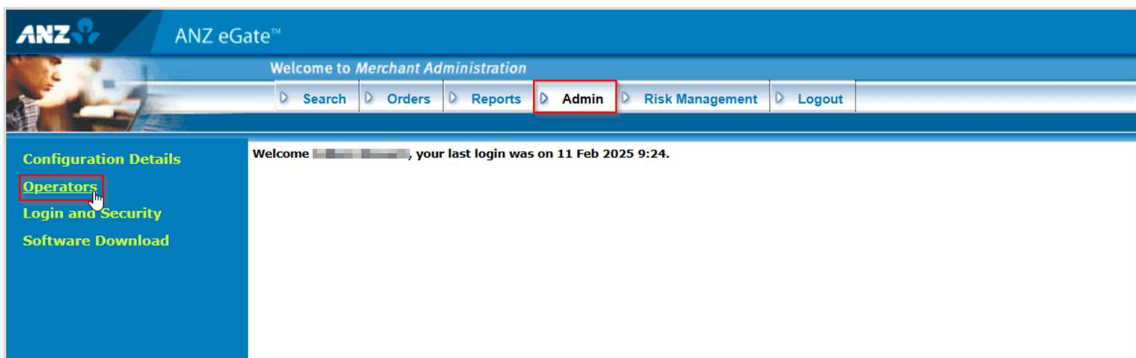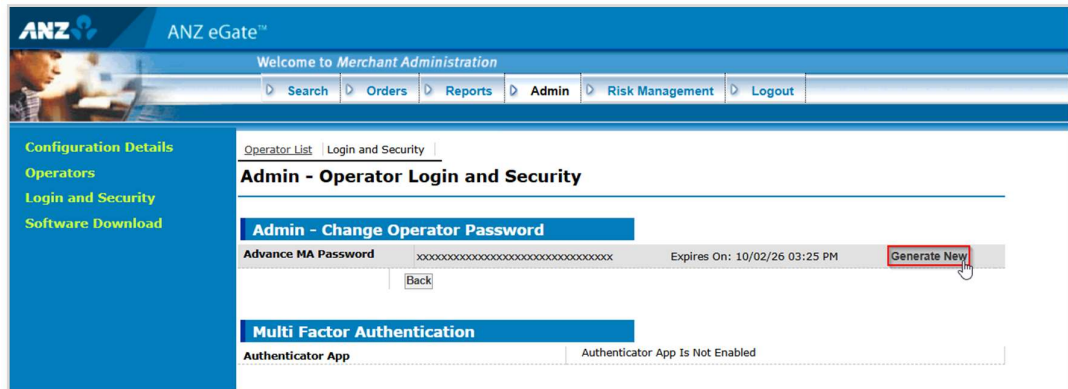
3. Generate a new AMA password

> **Before you proceed, make sure you are ready to perform this change in your client/web backend before completing these steps.**

- On your AMA enabled Operator, click on **Login and Security**, as shown below.

- On the Login and Security page click **Generate New**, as shown below, to generate a 32-character length alphanumerical password for the AMA Operator.

- A browser pop-up, such as the image below, will appear warning you that changing the password will disrupt any active processes relying on the existing password.
- Click OK to replace the AMA password on ANZ eGate.
- Copy the newly generated password and store separately before leaving this page. Once you leave this page, it will mask the generated password and cannot be re-copied.

Example

4. **Update your client/website backend with new AMA password**
   - With the copied password, update the "vpc_Password" parameter in your client/website's backend scripts for the payment gateway accordingly.
   - If you use a plugin, you will find and update AMA Password field within the plugin settings page.

   Note: It is recommended to have an experienced web developer or technician make these updates to your client/website, to ensure this update is made correctly.

   Important: The AMA password will expire after 365 days. It is recommended to set up a reminder notification with two weeks advanced notice to re-action this procedure.

5. **Test and confirm new password is working**
   - Test any function that uses the AMA user in your gateway integration and check for a successful outcome.

Test Cards

The purpose of testing is to ensure that your integration is performing correctly with the payment server and receiving the appropriate responses to display to your card holder. For example if an 'insufficient funds' or 'invalid card' response is returned it is important your integration can interpret this and display appropriately to your card holder.

Response Codes Testing

The information below is applicable only in the testing environment, i.e. when you are using your test merchant profile.

The test bank simulator is configured to allow the user to change the responses received against the test card numbers. To view the responses for each transaction you must log-in to the Merchant Administrator portal and perform an Order or Financial transaction Search. The TEST merchant profile is accessed when you log-in to the Merchant Administrator portal by prefixing "TEST" to the "Merchant ID" field (e.g. TESTxxxxxxxxxx).

The below test card numbers **(Table 1)** can be used to trigger the different response codes by varying the Expiry Date for the transaction. The following table shows how the various response codes can be triggered varying the Expiry Date.

The test bank simulator is configured to allow the user to change the response received against the provided test card numbers by varying the Expiry Date for the transaction. The following table shows how the various response codes can be triggered varying the Expiry Date.

Table 1 - Testing by EXP - Cards and Responses

BRAND	PAN	Card Security Code
MASTERCARD	5577 8100 0000 0004	Any 3 digits
DINERS CLUB	3012 3400 0000 00	Any 3 digits
VISA	4434 2600 0000 0008	Any 3 digits
JCB	3528 0000 0000 0007	N/A

Expiry Date	Response code definition	Acquirer Response Code
3901	0	Transaction approved
2302	1	Transaction could not be processed
2205	2	Transaction declined - contact issuing bank
2808	3	No reply from Processing Host
2704	4	Card has expired
2701	5	Insufficient credit

*For example, to obtain a response code of 1 on a MasterCard, simply send a transaction with expiry date 23/02 (yy/mm) against one of the above MasterCard numbers.

American Express testing card

BRAND	PAN
AMEX	3456 7800 0000 007

Expiry Date	Response code definition	Acquirer Response Code
3901	00	Transaction approved
3102	92	Transaction could not be completed
2201	01	Transaction declined – Refer to Card Issuer
3101	91	Card Issuer Unavailable
2704	54	Card has expired
2701	51	Insufficient credit

Mastercard testing card

BRAND	PAN
MASTERCARD	2223 0000 0000 0007
MASTERCARD	2223 0000 0000 0023
MASTERCARD	2223 0000 0000 0031

Expiry Date	Response code definition	Acquirer Response Code
3901	0	Transaction approved
2201	E	Transaction could not be processed
2205	2	Transaction declined - contact issuing bank
2808	3	No reply from Processing Host
2204	4	Card has expired
2701	5	Insufficient credit

Card security code (CSC) Result Code

The CSC is in addition to the bank card number which is embossed or printed on the card. The CSC is used as a security feature, in situations where a PIN cannot be used.

The following table shows how the various CSC response codes that can be triggered by varying the CSC value. Most Issuing banks will fail a transaction due to incorrect CSC in production.

All the transactions will get approved with any CSC Value except 104 CSC Value

To view the responses for each CSC test you must log-in to the Merchant Administrator portal and perform a Financial transaction Search. Click on 'Transaction Number' then 'Order ID.'

Here you will see the response under 'Card Details' - "CSC Result Code = P"

CSC Value	Name	Response Code
100	Valid or Matched CSC	M
104	Code Invalid or Not Matched	N
102	CSC Not Processed	P

*For example, to obtain a response code of P on a MasterCard, simply send a transaction with CSC 102 against one of the above MasterCard numbers

QUESTIONS?
For technical support, please contact ANZeCommerceSupport@worldline.anz.com.

ANZ WORLDLINE
Payment Solutions