Canada Border Services Agency | Agence des services frontaliers du Canada

CARM Client Portal

User Guide

Delegation of Authority in the CARM Client Portal

Revision date: December 13, 2022

Canada

Purpose of this guide

This guide will explain the delegation of authority process. There are two parts to delegation of authority within the CARM Client Portal: providing access to employees within your company by assigning user roles, and importers providing access to service providers by establishing a business relationship.

Important note:

Prior to reading this guide, it is suggested that you first review the **User guide – Onboarding to the CARM Client Portal**. This guide offers step by step processes for creating both individual and business accounts in the CARM Client Portal, as well as steps for linking these accounts. These actions are necessary pre-requisites that must take place before users can delegate authority within the portal.

Table of contents

1. Overview of delegation of authority

1.1 Overview

User roles

As an importer, customs broker, or trade consultant you will be able to delegate authority for various roles in the CARM Client Portal to your employees. The user roles given to employees define which actions individual users can take within given business and program accounts, as well as their visibility attributes (what information each user can see).

Note:

A business account is the legal entity with a business number (BN9). Every business account has at least one program account (RM), however some importers may have multiple program accounts.

Business relationships

Importers can set up business relationships with their service providers (customs brokers and/or trade consultants) to allow them to transact business with the CBSA on their behalf. More information on business relationships is provided in **Section 5: Managing business relationships from the importer's point of view**.

Having the appropriate delegation of authority for employees and service providers enables multiple users to view information or act on behalf of the business. Trade chain partners (TCPs) will have the ability to view which of their employees have access to their account in real time, and to make appropriate updates to this access via the CARM Client Portal.

The different roles and relationships between users fall under pre-set conditions that allow or prevent users from performing certain tasks (for example, viewing notifications, making payments, submitting rulings, etc.) based on the access they have been granted.

First-time setup steps for importers

1. Designate at least one Business Account Manager (BAM) (see **User guide – Onboarding to the CARM Client Portal**).
2. BAM creates their personal account in the CARM Client Portal (see **User guide – Onboarding to the CARM Client Portal**)
3. Additional employees create their own personal accounts in the CARM Client Portal and request access to the business account (see **User guide – Onboarding to the CARM Client Portal**)
4. BAM grants access to employees by assigning users roles (see **Section – Managing pending employee access requests**)
5. BAM establishes a business relationship with one or more customs brokers and/or trade consultants (see **Section – Managing business relationships**)

First-time setup steps for customs brokers or trade consultants

1. Designate at least one Business Account Manager (BAM) (see **User guide – Onboarding to the CARM Client Portal**)
2. BAM creates their own personal account as the BAM of the service provider (see **User guide – Onboarding to the CARM Client Portal**)
3. Service provider employees create their own personal accounts and request access to the business account of the service provider (see **User guide – Onboarding to the CARM Client Portal**)
4. BAM grants access to employees by assigning users roles (see **Section – Managing pending employee access requests**)
5. BAM requests a business relationship with clients (importers) (see **Section – Requesting a business relationship (service provider overview**)
6. Create client groups (see **Section – Creating client groups**)
7. Assign employees and clients into these groups (see **Section – Assigning employees to clients and client groups** and **Section – Adding and removing clients from groups**)

2. User roles and permissions in the CARM Client Portal

This section will explain the various user roles that can be given to employees within a business. **Section 3 – Assigning user roles step-by-step** will provide the step-by-step walkthrough of how to assign these user roles to employees within the business.

User roles define the actions that each individual user can take within given business and program accounts. The various roles that users can hold within the portal include:

- Business Account Manager (BAM)
- Program Account Manager (PAM)
- Editor
- Reader
- Unassociated User

2.1 Business Account Manager (BAM)

User role	Description
Business Account Manager (BAM)	BAMs have full access to all CARM Client Portal functionality for a business account and all of its associated program accounts. Every business account (importer, customs broker and/or trade consultant) will require at least one BAM. This role is automatically given to the initial individual who links their user account to their business by completing the business registration process. The purpose of this role is to assume the primary management of the business account. **Note:** This role does not need to be assigned to the person legally listed in the incorporation, proprietorship, or partnership documentation of the business. This user role should be held by an individual with active involvement in the management of the business account.

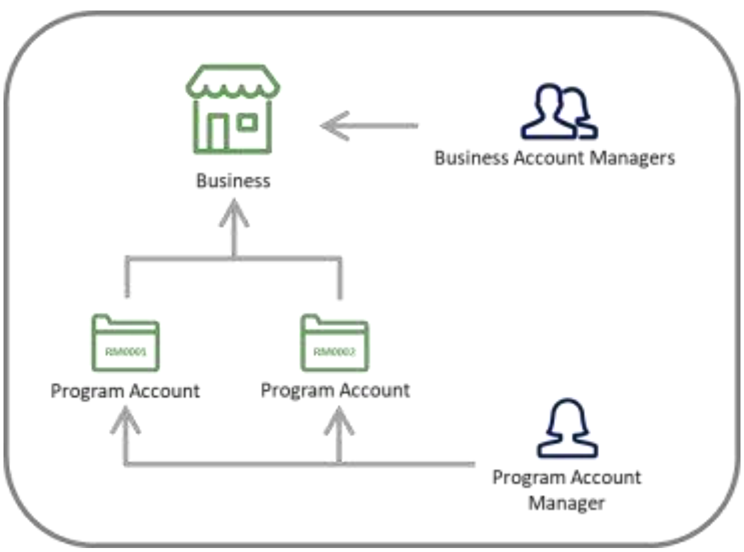
Important note:

Due to the importance of the BAM role, it is highly recommended that the role of BAM be assigned to at least one other user. If it were to happen that a BAM's account became inaccessible, having another BAM avoids the possibility of losing all access to business management activities.

2.2 Program Account Manager (PAM)

User role	Description
Program Account Manager (PAM)	The PAM role gives full access to all CARM Client Portal functionality for a specific program account (BN15) only. This role is useful if there is more than one program account, and the BAM wishes to give access to certain program accounts only. The purpose of this role is to assume the management of a program account alongside the BAM.

The image below shows a visual illustration of the relationship between a BAM and a PAM:



2.3 Editor

User role	Description
Editor	The Editor role can perform operational activities in the CARM Client Portal (for example, request rulings, make payments, etc.).

2.4 Reader

User role	Description
Reader	The Reader role can view operational activities in the CARM Client Portal (for example, rulings, payments, financial information).

2.5 Unassociated user

User role	Description
No user role assigned	Unassociated users have registered their individual profile on the CARM Client Portal but have not yet linked their business or have not been accepted as an employee of a business. Unassociated users have no access.

2.6 Permissions

Each user role has an associated set of permissions that control what the user can do in the CARM Client Portal. These are grouped into nine related functions.

User groups / Resources	BAM	PAM	Editor	Reader
Organization (Business profile information, list of programs)	Edit	No access	No access	No access
Users access (Manage pending requests, manage list of users)	Edit (assign users to business and programs)	Edit (assign users to program)	No access	No access
Business relationships (Send a request, manage pending requests, manage existing relationships)	Edit	Edit (can only send a new request)	No access	No access
Upload documents (Upload a new document)	Edit	Edit	Edit	No access
Program (Program profile information)	Edit	Edit	No access	No access
Finance (Transaction history, Statement of Account (SOA), invoices)	Read	Read	Read	Read
Payment (Credit allocation, credit card payment and interact payment)	Edit	Edit	Edit	Read
Pre-Authorized Debit (Banking information)	Edit	No access	No access	No access
Rulings (Ruling requests and decisions)	Edit	Edit	Edit	Read

3. Assigning user roles step-by-step

Managing employees is an activity reserved for BAMs and PAMs, although only BAMs are able to remove users. Users cannot update or remove their own access. Remember that a BAM can manage access for the whole business account, however a PAM can only manage access for their specific program account(s).

3.1 Employee access request (pre-requisite)

Employees must register and create an individual user account on the CARM Client Portal, then request access to their employer.

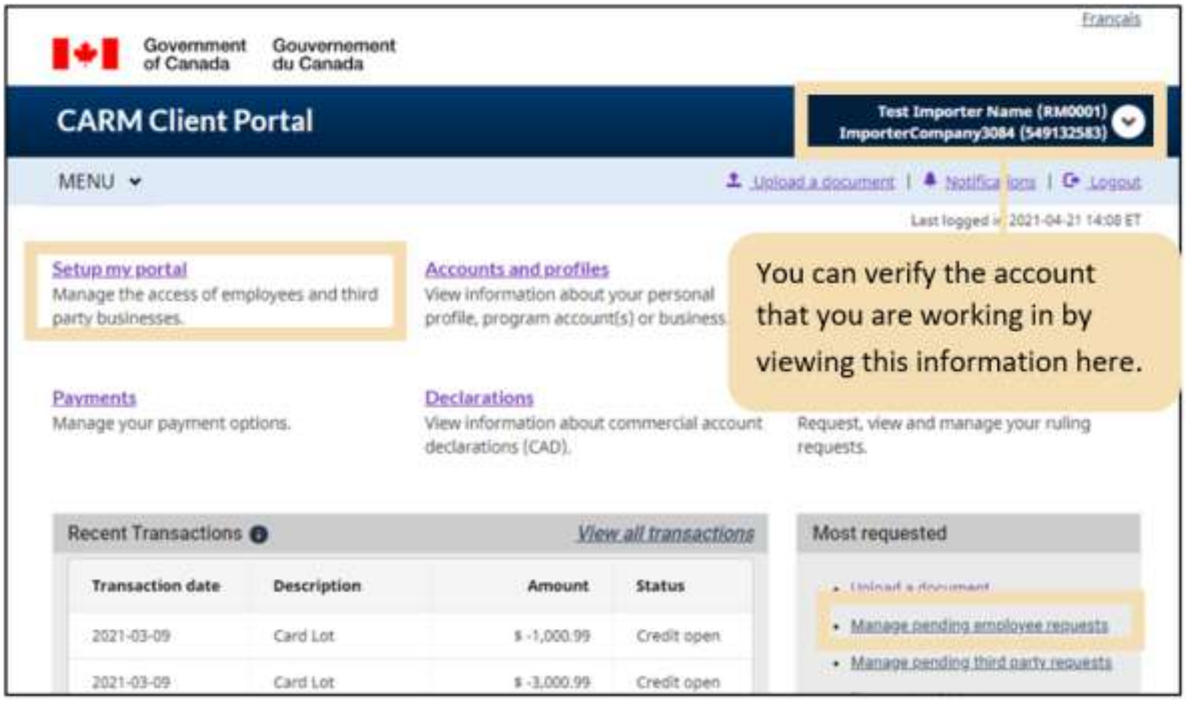
When this process has been completed successfully, employers will receive a **pending access** request from the employee that they will be able to action. This request will remain in a pending state and the employee will be considered an **Unassociated user** until the employer either accepts the access request and assigns a user role to the employee or rejects the employee access request.

Note:

To learn more about creating an individual user account, see **User guide – Onboarding to the CARM Client Portal**.

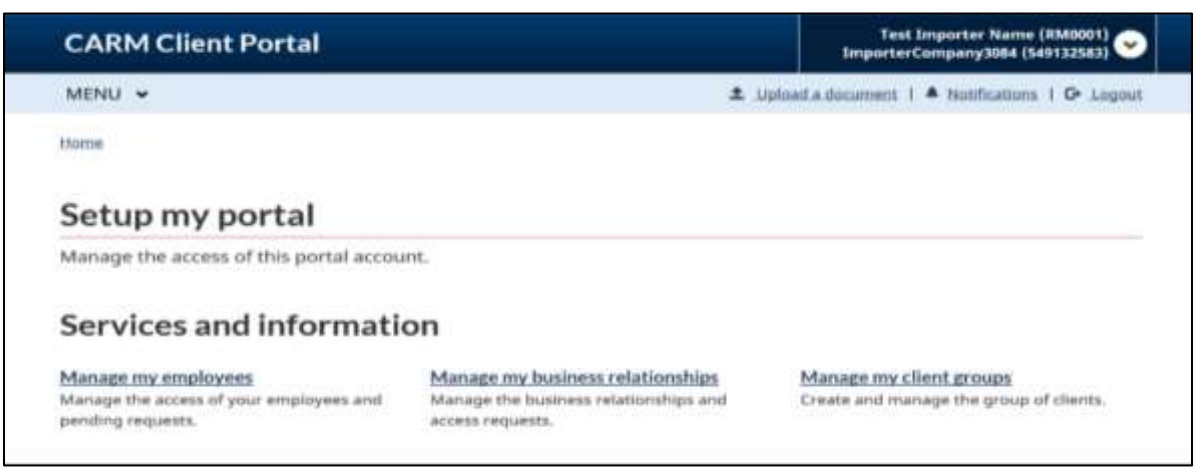
3.2 Managing pending employee access requests

1. Click either **Setup my portal** or **Manage pending employee requests**.

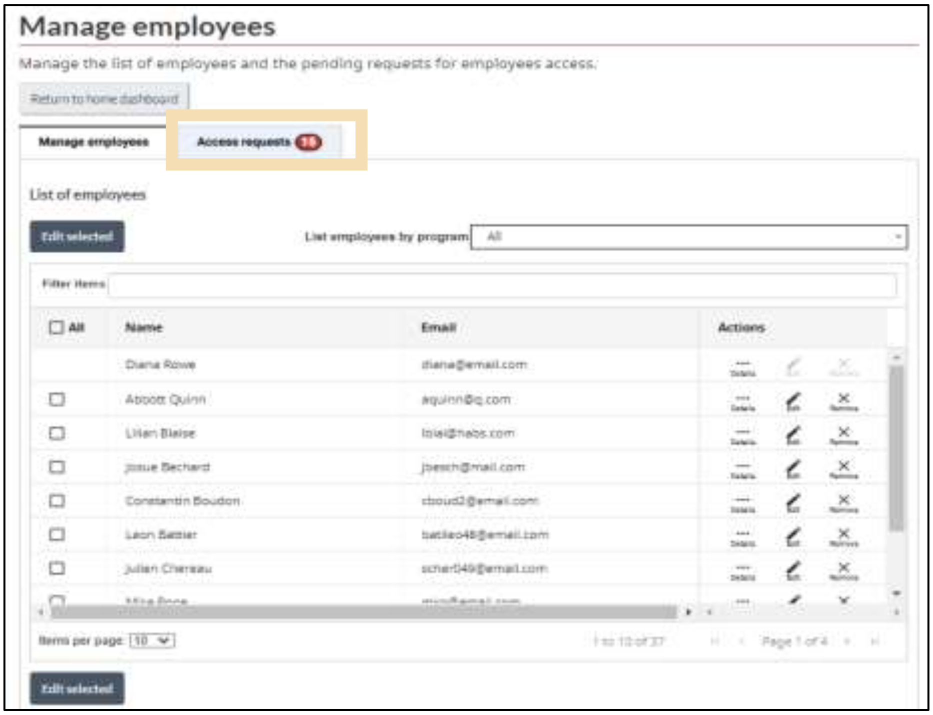


Note:

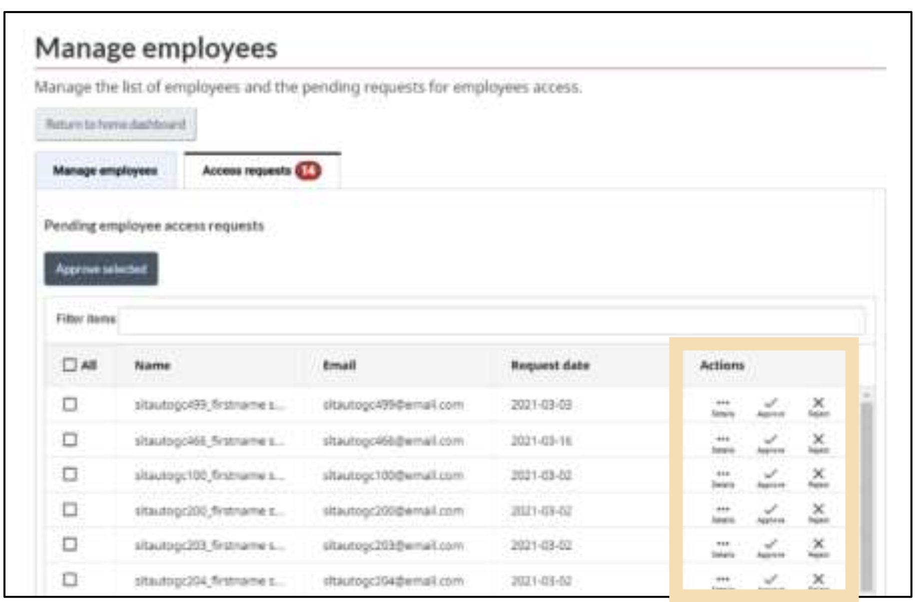
If you select **Setup my portal**, you will be taken to the below screen.



2. Select the **Access requests** tab. Any employees that have requested access to the business will be displayed here.



3. Click **Approve** or **Reject** in the **Actions** column, if you know the action you would like to take. If you would like to view additional information about the request, click **Details**.

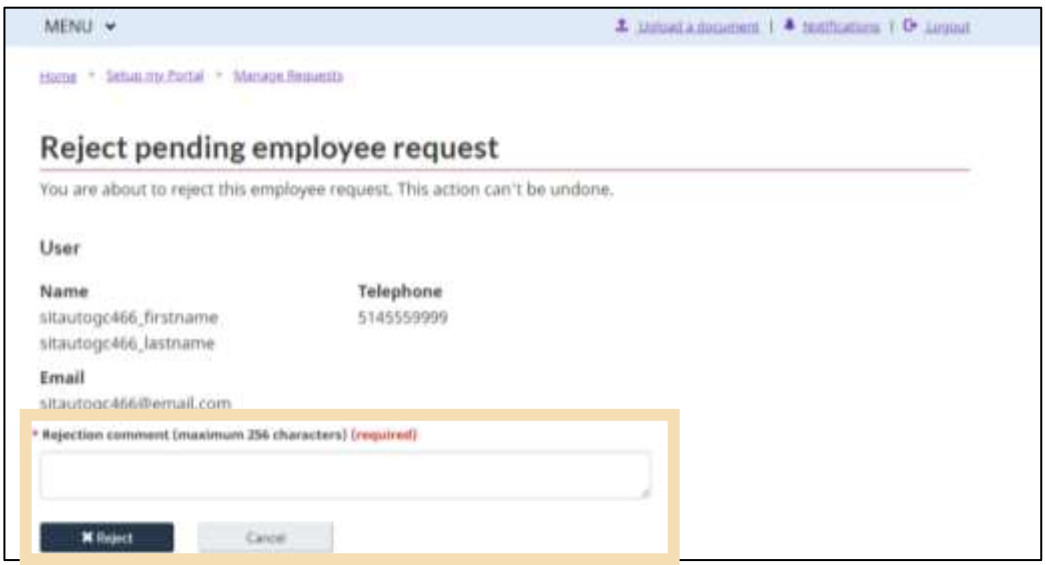


Note:

The BAM or PAM of a business can approve an employee access request. It is the responsibility of the manager approving the request to validate that the user is an employee of the business.

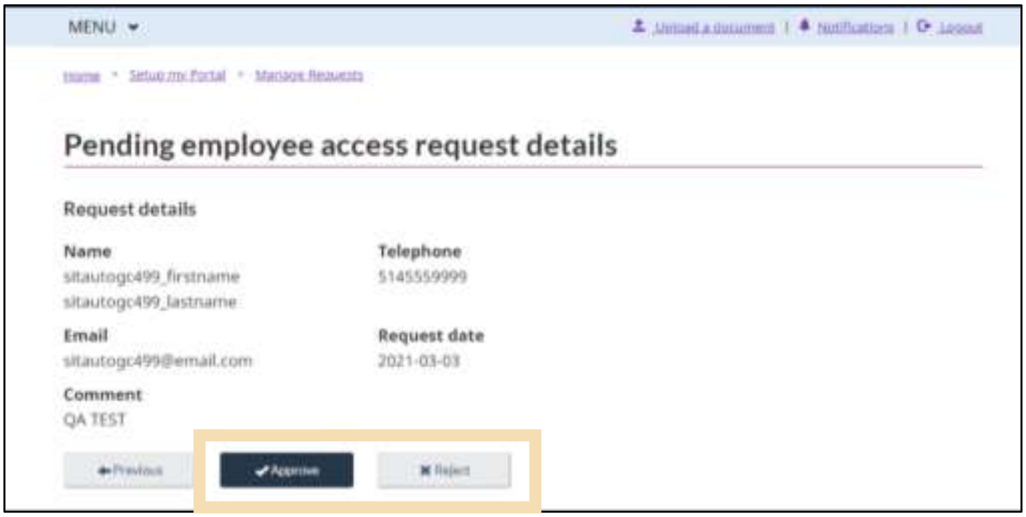
Note:

If you choose to reject a pending employee request, you will be brought to the below screen. A justification must be provided in the comments of the rejection notice. The **Unassociated user** will be able view and acknowledge the rejected request and its comment.



Note:

If you choose to view additional details about the request, you will be able to review comments from the requestor regarding the request and can **Approve** or **Reject** from this page.

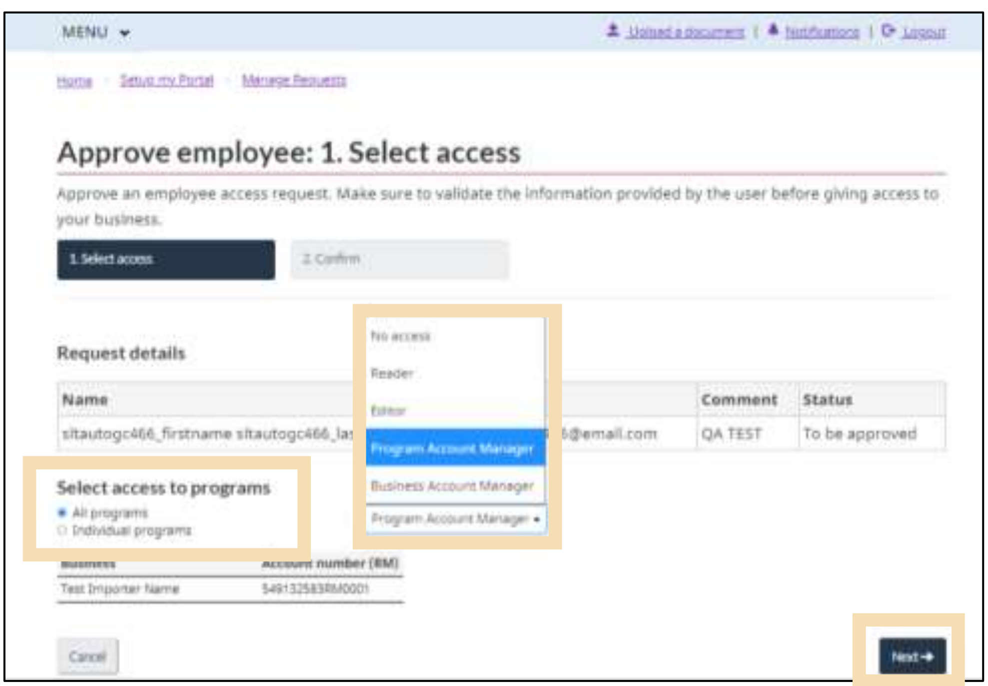


If you have chosen to approve the employee access, you will be required to assign the employee a user role and determine their level of access.

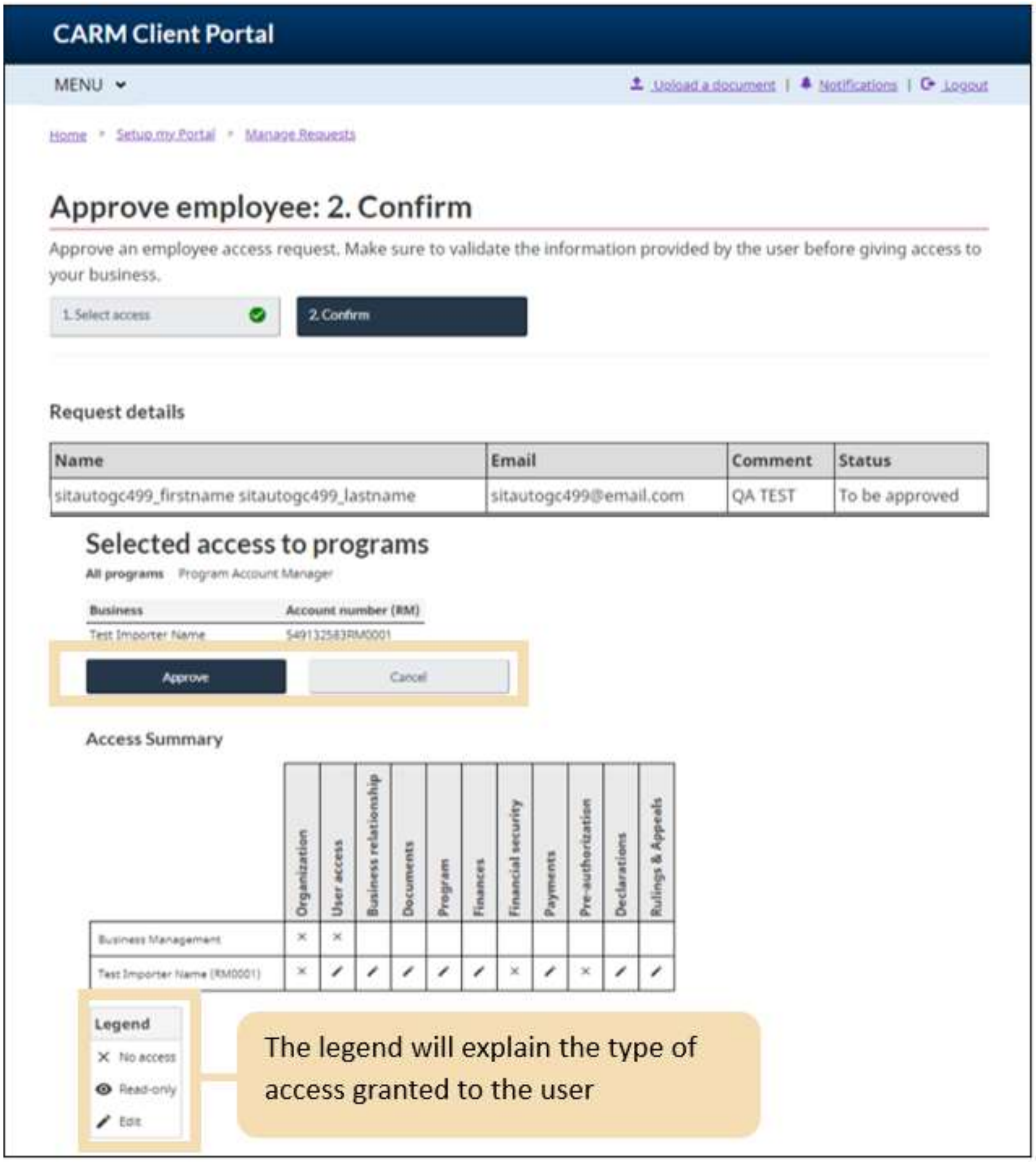
4. Select whether the employee should have access to **All programs** or **Individual programs**.

5. From the drop-down list**,** select the **user role**.

6. Click **Next.**



7. Review the details of the employee's user role and access. Then, click **Approve** to proceed, or **Cancel** to restart the process.



Note:

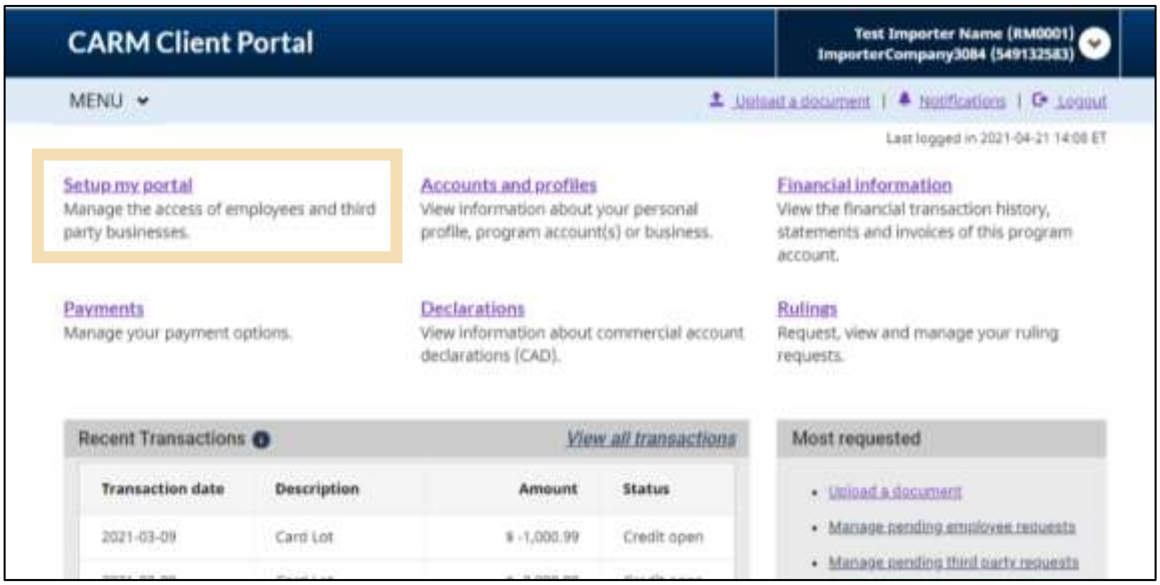
To learn more about managing employee access, please review the informational video:

- **How to delegate authority to employees in the CARM Client Portal**

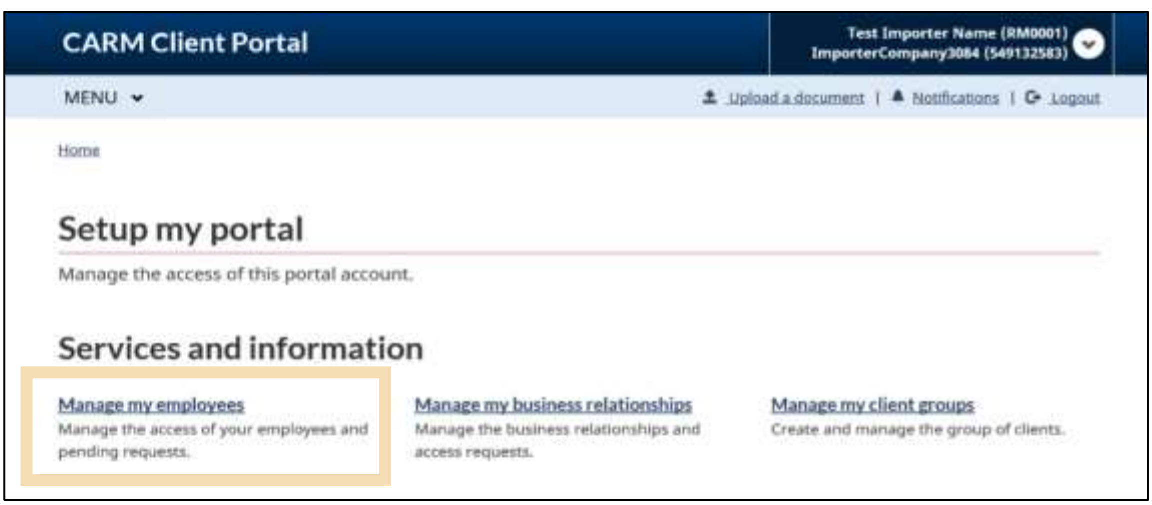
3.3 Editing employee user roles

Editing user roles is similar to the process demonstrated in [Section 3.1](#) for approving employee access.

1. Select **Setup my portal** from the CARM Client Portal home page.



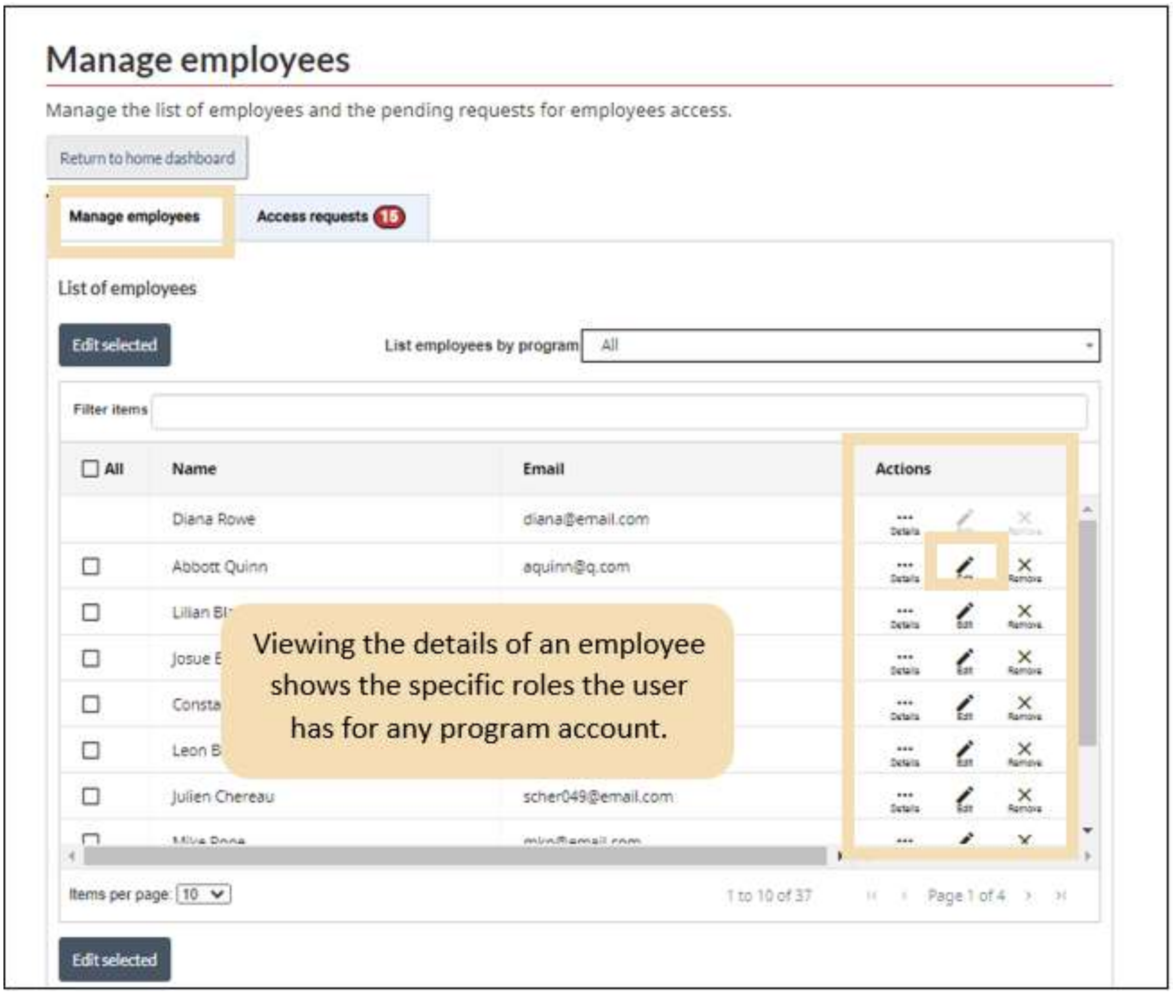
2. Select **Manage my employees**.



You will be taken to the **Manage employees** page. This page enables BAMs and PAMs to view all the employees associated to the business or program account. It also enables them to manage access details of users and review pending requests.

On the **Manage employees** tab, available actions are displayed in the far-right **Actions** column. You can choose to view employee details, edit employee roles/access, or remove an employee (BAM only).

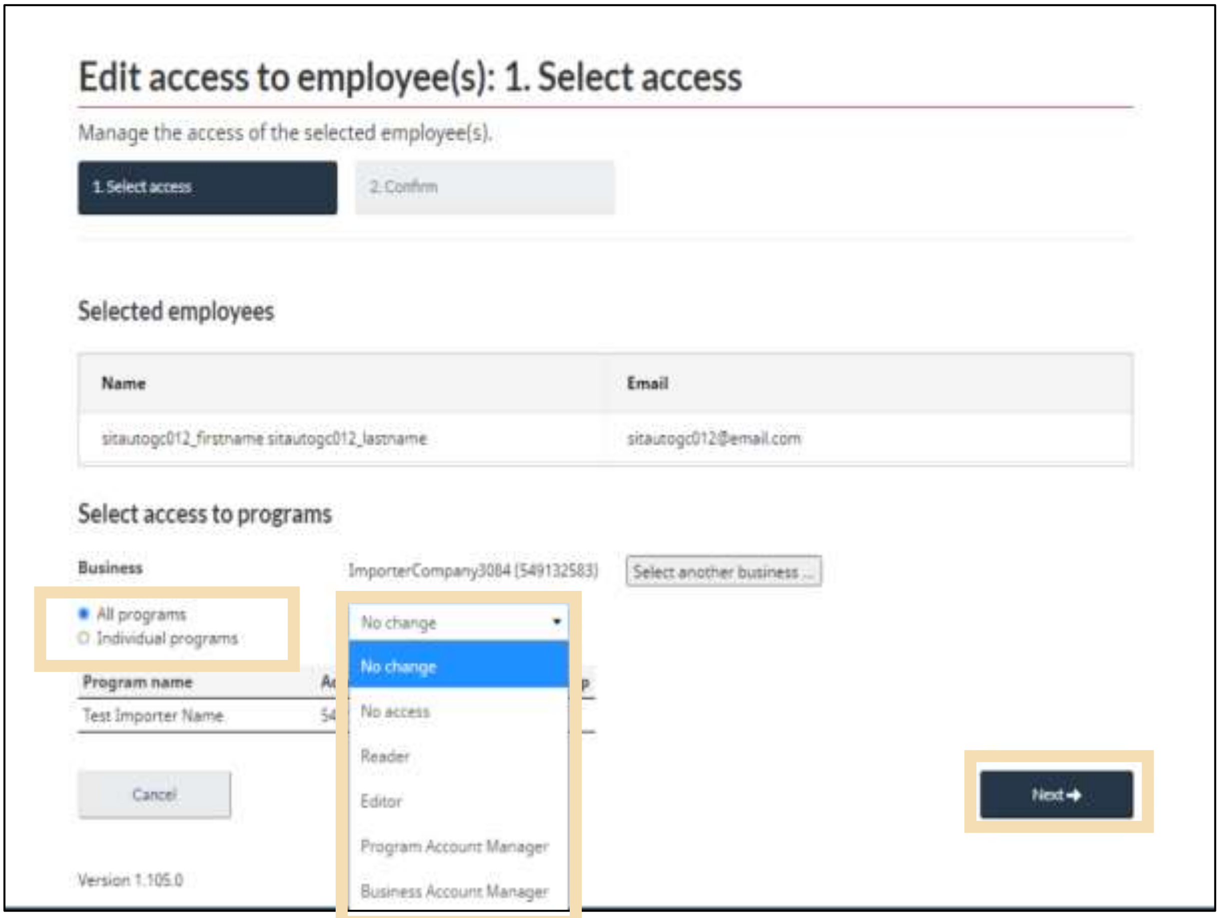
3. Select the **Edit** icon to edit an employee's role and access.



4. Select whether the employee should have access to **All programs** or **Individual programs**.

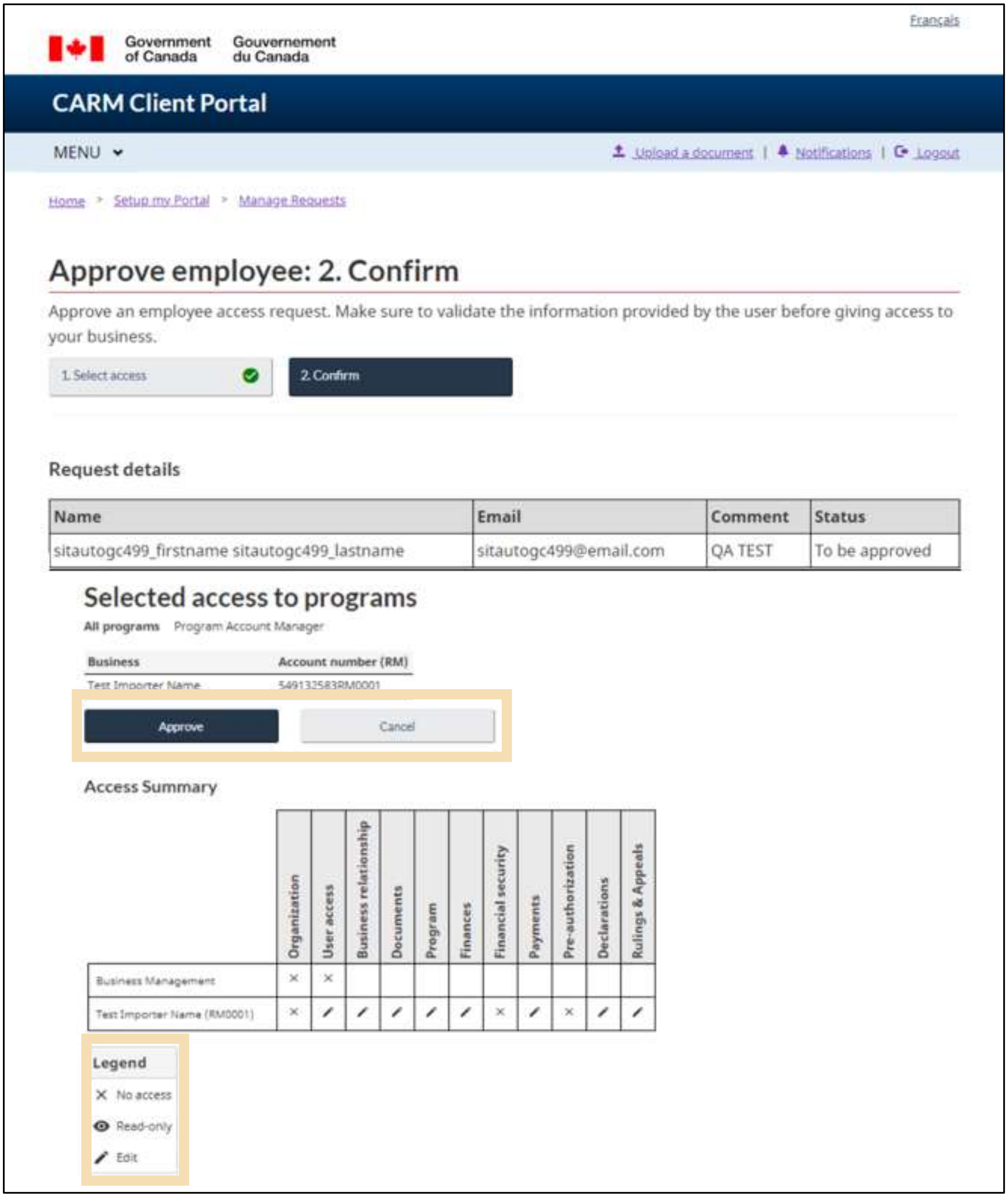
5. From the drop-down list, select the new **user role** that you would like the employee to receive.

6. Click **Next**.



Edit access to employee(s): 1. Select access
Manage the access of the selected employee(s).
1. Select access
2. Confirm
Selected employees
Name
Email
sitautogc012_firstname sitautogc012_lastname
sitautogc012@email.com
Select access to programs
Business
ImporterCompany3084 (549132583)
Select another business ...
All programs
Individual programs
No change
No change
No access
Reader
Editor
Program Account Manager
Business Account Manager
Program name
Test Importer Name
Cancel
Next
Version 1.105.0

7. Review the details of the employee’s user role and access. Click **Approve** to proceed or **cancel** to restart the process.



Note:

Only BAMs are able to remove an employee. This action revokes all access to the employer's business account and to its business relationships. If the removed user is later approved back for the same business account, previous access details will not be restored.

Note:

Editing BAM roles:

A user promoted to BAM:

- Receives automatic access to the employer's business account and program account(s)

A user demoted from a BAM:

- Loses all BAM permissions and only keeps the permissions of new use role (PAM, Editor, and Reader).

Note:

Remember that users cannot edit their own access and can only manage the access of others in a hierarchical manner. BAMs have the greatest level of access, then PAMs. For example, BAMs can edit the access of all employees, including other BAMs, but a PAM can't edit the access of a BAM. Editors and Readers cannot manage the access of themselves or others.

4. Business relationships in the CARM Client Portal

In the CARM Client Portal, business relationships can be established between a client (importer) and its service provider(s). Once established, the business relationship will allow a service provider (for example, customs broker and/or trade consultant) to act on behalf of their client(s) and manage their account(s) within the CARM Client Portal. In order to establish this relationship, service providers will need to send a request to their client requesting a relationship.

Once there is a business relationship, the BAM or PAM of the service provider can assign their employees to work on their clients' accounts.

There are two (2) options of relationships between an importer and its service provider(s):

- **Business management relationship:** grants access to the business account (BN) and all program accounts (RM) to the service provider, including any programs added in the future.
- **Program management relationship:** grants access to only selected program accounts (RM) to the service provider.

The importer determines the type of relationship to grant to its service provider(s).

4.1 Business management relationship

If the importer gives their service provider the **business management** type of relationship, the BAM of the service provider is automatically given the pBAM (proxy BAM) role for the importer's accounts.

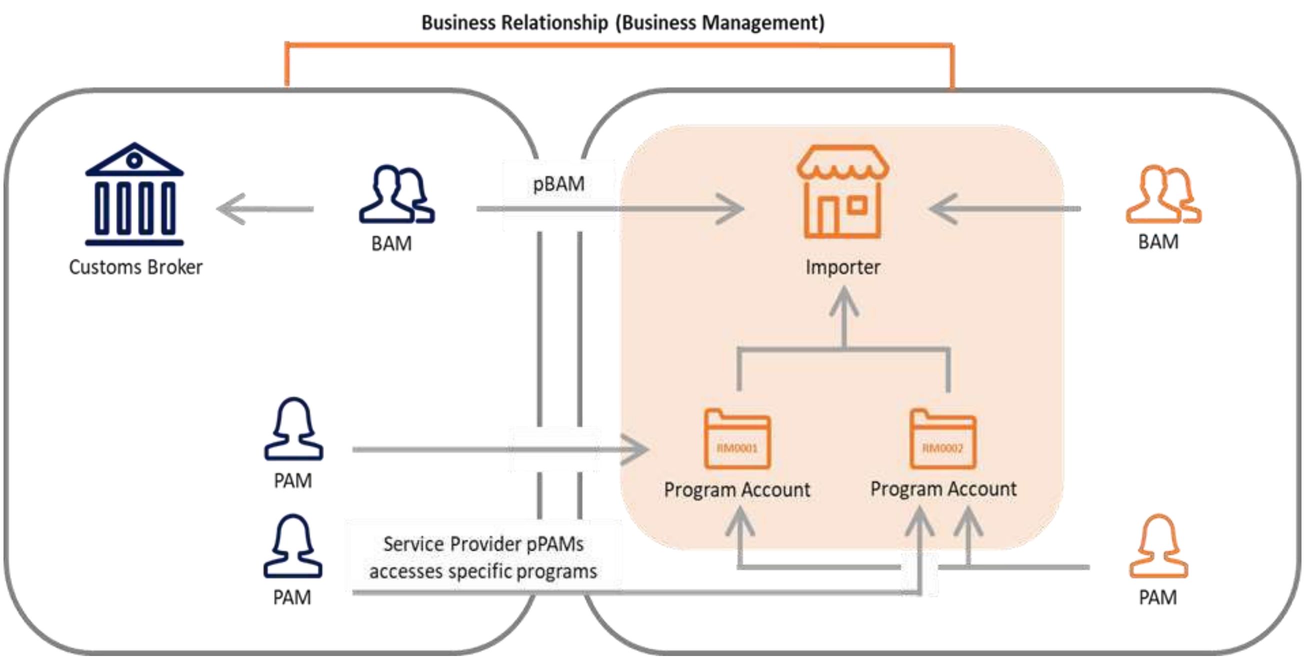
The pBAM role gives near full access to all CARM Client Portal functionality for an importer's business account and all of its program accounts, with the following exceptions:

- The pBAM does not have access to the client's sensitive information (bank account)
- The pBAM cannot see or manage the details or access for the importer's employees or other business relationships that the client holds

This pBAM role can:

- Perform operational activities in the CARM Client Portal for all of the importer's program accounts (for example, request rulings, make payments, view the statements of account, invoices and payments made)
- Manage the access of the service provider's employees for the importer's business account and all of the program accounts

This diagram illustrates an example of a **business management relationship** access type in which employees of the service provider gain access at the importer's business account level.

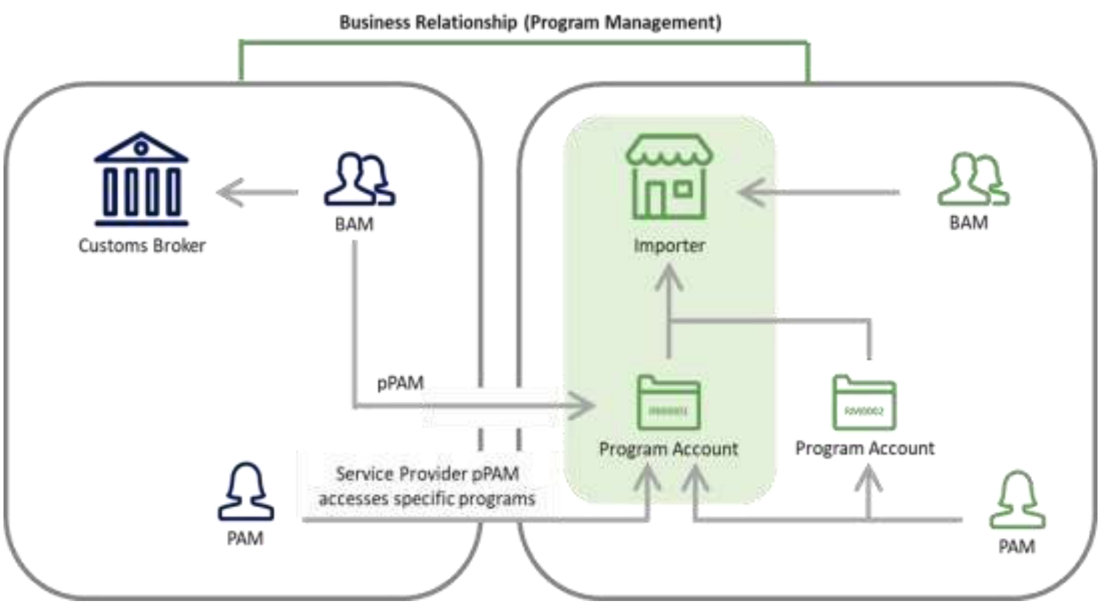


4.2 Program management relationship

If the importer gives their service provider the **program management** type of relationship, the BAM of the service provider is automatically given the pPAM role for the importer's program accounts.

This role gives near full access to all CARM Client Portal functionality for an importer's program account (RM). The purpose of this role is to assume the management of a client's specific program account without providing access to the business profile.

This diagram illustrates an example of a **program management relationship** access type in which employees of the service provider gain access to one of the importer's program accounts (but not both).



> **Note:**
>
> The pBAM or pPAM will assign their employees user roles that will determine their access (pPAM, pEditor or pReader).

4.3 Visibility attributes

Visibility attributes control which requests or transactions a service provider can view based on who submitted the information. These attributes are assigned to the service provider by the importer.

The three visibility attributes are as follows:

1. **Submitted by the service provider:** Defines the requests or transactions that a service provider submitted within the business relationship.
    - This attribute is always enabled for a service provider so that they may always see the work they have accomplished on behalf of their client
    - When the business relationship expires, the service provider and the importer both continue to see the requests or transactions previously submitted
2. **Submitted by the client:** Defines the requests or transactions that the client submitted on their own behalf, outside of the business relationship.
    - This attribute would most likely be used in a situation where the client actively submits requests and transactions in parallel to the service provider
    - When the business relationship expires, this attribute is disabled automatically for the service provider
3. **Submitted by other businesses:** Defines the requests or transactions that another service provider submitted for the client within a separate business relationship.
    - This attribute would most likely be used in a situation where a client has multiple business relationships overlapping the same program accounts
    - When the business relationship expires, this attribute is disabled automatically for the service provider
    - **Exception:** even if this visibility is granted, one service provider is not able to view ruling requests or decisions that were submitted by a different service provider

The following table outlines the visibility of submissions based on which party submitted the request or transaction, and the visibility attribute(s) assigned to the service provider by the client.

Request or Transaction submitted by: Selected visibility attributes:	Employee of Service provider	Employee of Client	Employee of another Service provider
☑ **Submitted by the Service Provider**	Visible	Non Visible	Non Visible
☑ **Submitted by the Service Provider** ☑ **Submitted by the Client**	Visible	Visible	Non Visible
☑ **Submitted by the Service Provider** ☑ **Submitted by other businesses**	Visible	Non Visible	Visible
☑ **Submitted by the Service Provider** ☑ **Submitted by the Client** ☑ **Submitted by other businesses**	Visible	Visible	Visible

Note:

Expired: This user role is intended for BAMs of service providers with an expired business relationship. It has the same access rights as a Reader. It allows the BAM of the service provider to view information that they had previously submitted on behalf of a client.

Note:

Restricted actions for service providers in both business and program management relationships include the following:

- Editing the business account or program account information
- Viewing or editing pre-authorized debit authorizations
- Viewing collection-related notifications and payment arrangements
- Viewing or editing the client's pending business relationship requests, and its list of active business relationship
- Viewing or editing the client's access requests, and its employees' accesses

The following table outlines the visibility of submissions based on which party submitted the request or transaction, and the visibility attribute(s) assigned to the service provider by the client.

User groups / Resources	pBAM	pPAM	pEditor	pReader
Organization (Business profile information, list of programs)	Read	No access	No access	No access
Users access (Manage service provider employees user roles)	Edit (assign users to delegated business and programs)	Edit (assign users to delegated program)	No access	No access
Business relationships (List of business relationships)	No access	No access	No access	No access
Upload documents (Upload a new document)	Edit	Edit	Edit	No access
Program (Program profile information)	Read	Read	No access	No access
Finance (Transaction history, Statement of Account (SOA), Invoices)	Read	Read	Read	Read
Payment (Credit allocation, credit card payment and interact payment)	Edit	Edit	Edit	Read
Payment Pre-Authorization (Banking information)	No access	No access	No access	No access
Rulings (List of rulings, ruling decisions)	Edit	Edit	Edit	Read

4.4 Requesting a business relationship (service provider overview)

Service providers in the CARM Client Portal will also be required to set up both individual and business accounts, much like the process their clients would follow.

Note:

To view the process on setting up and linking these accounts, refer to the **User guide: Onboarding to the CARM Client Portal**

To review the process on managing employee access for a business account, see **Sections 3.1 and 3.2** of this guide on Managing and editing employee access.

Within the portal, service providers will have the ability to take the following actions as they relate to their business and employee management:

- Request new business relationships
- View or cancel pending business relationship requests
- View rejected business relationship requests
- Act on behalf of a client when a business relationship is approved
- Assign clients of their active business relationship to client groups
- Manage employee access, and assign employees to clients or client groups
- Keep a restricted view-only access of expired business relationships

Note:

Only a service provider can initiate a business relationship. It is their responsibility to send a request to their client.

Prior to performing transactions on behalf of their clients, service providers must initiate the relationship by sending a business relationship request to their client. This process is detailed in the following section below.

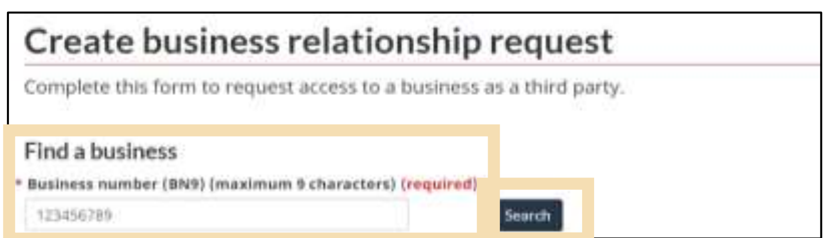
4.5 Requesting access to a client (for service providers)

All service providers must first establish a business relationship with their clients to be able to transact within the CARM Client Portal on their behalf.

Once a relationship is established, the service provider will be able to assign its employees to the clients' accounts in order to carry out the activities agreed upon in their service contract.

To request a business relationship, a Business Account Manager (BAM) or a Program Account Manager (PAM) will have to:

1. Search for the client's business account by entering the client's business number.



2. Provide a meaningful comment to justify the request and send the request.

The additional comments will help the BAM or PAM of the importer's account to identify if the business relationship should be granted, as well as the level of access that the service provider needs. Failure to provide a meaningful justification may result in a rejected request.

Once the request for the Business Relationship has been submitted, there are three possible statuses that service providers will see:

1. **Pending request:** A business relationship request will remain in a pending state until the client either approves or rejects it. **Note:** The BAM or PAM of the service provider may cancel the request at any point while it is in a pending status.

2. **Rejected business relationship request:** A business relationship request can be rejected by either the BAM of the client, or the PAM requesting it. Note: Requests can be re-sent, but the original rejected request must first be cancelled by the service provider before a new one can be sent.

3. **Approved business relationship request:** An approved business relationship will automatically grant access to the delegated client account.

Note:

- If the client approves a relationship as a **business management relationship,** all the BAMs of the service provider will automatically be assigned as third-party BAMs (pBAM)
- If the client approves a relationship as a **program management relationship**, all the BAMs of the service provider will be assigned as third-party PAMs (pPAM) for the delegated client program account(s)

5. Managing business relationships from the importer's point of view

5.1 Managing business relationships

For an importer, managing a business relationship with a service provider is a similar process to managing access for employees.

In order for a service provider to be able to transact within the CARM Client Portal on behalf of an importer, a business relationship must first be established. Only then will the service provider be able to assign its employees to the clients' accounts to carry out the activities agreed upon.

In order to grant access to third party service providers, the following steps must be completed:

1. (pre-requisite) Third party service providers request access

Note:

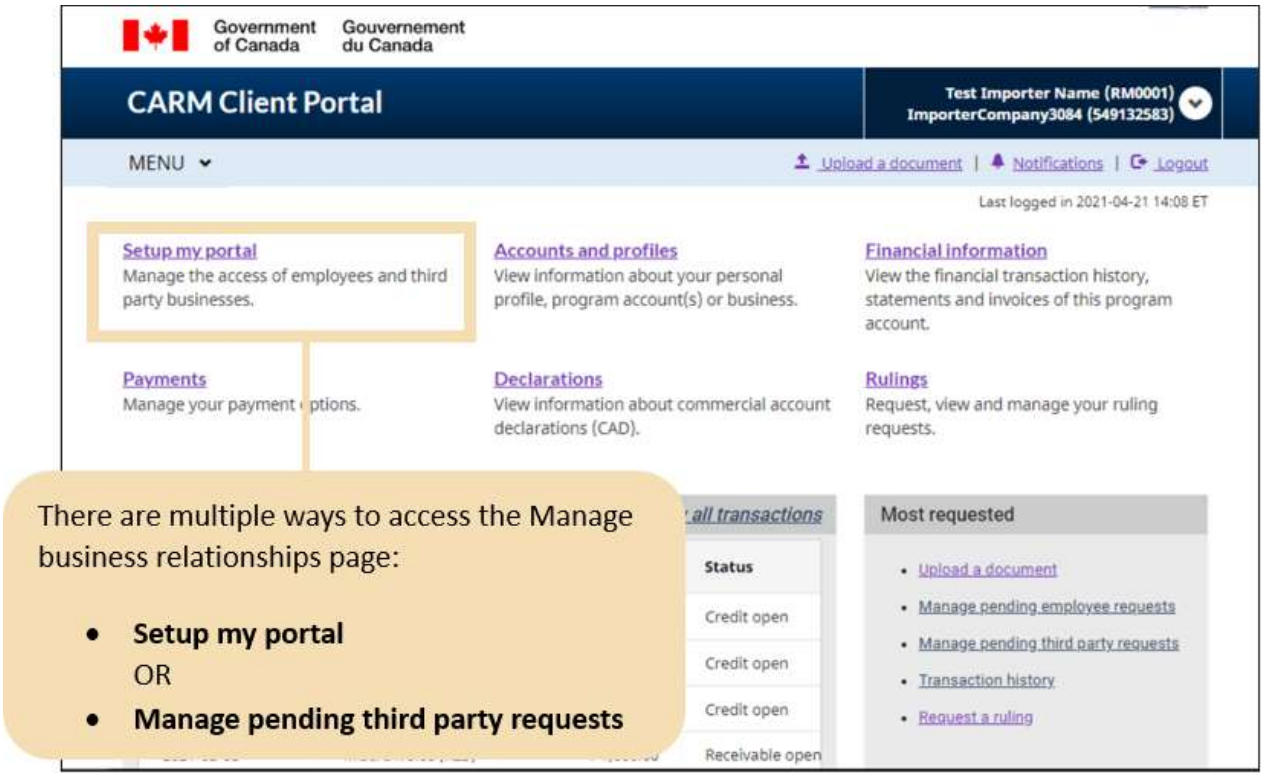
The process for how service providers can request access to their clients is covered in a **Delegation of authority for third party service providers** separate section of this guide.

Please see **Section 6.2 – Assigning employees to client and client groups**.

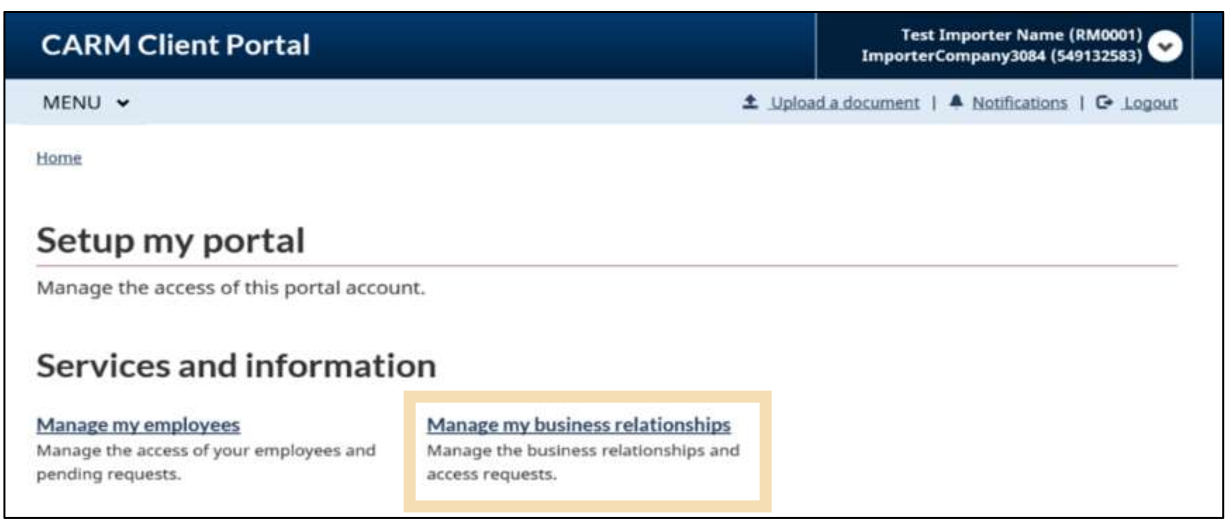
When this process has been completed successfully, importers will receive a pending access request from the service provider that they will be able to action.

The steps that follow outline this process from the importer's point of view.

2. Click either **Setup my portal** or **Manage pending third party requests**.



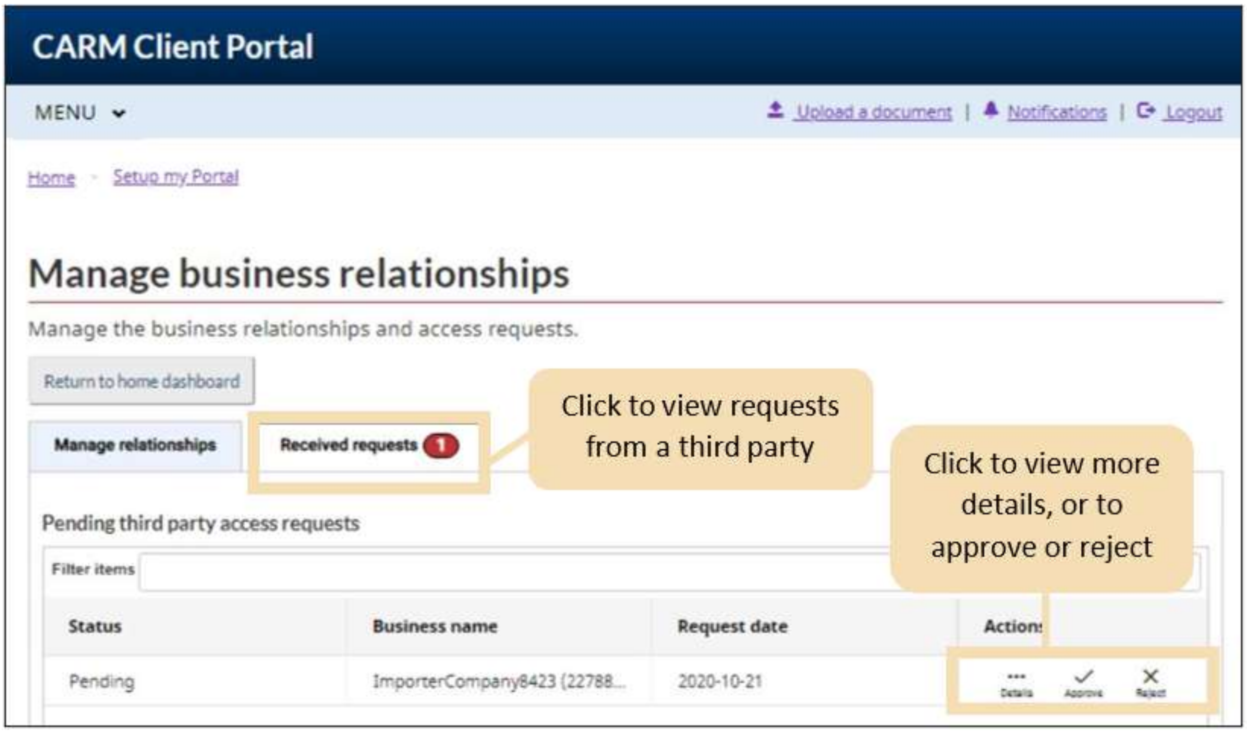
3. If you select **Setup my portal,** you will be taken to this screen. Click on **Manage my business relationships**.



4. Select the **Received requests** tab. Any third parties that have requested access to the business will be displayed here.

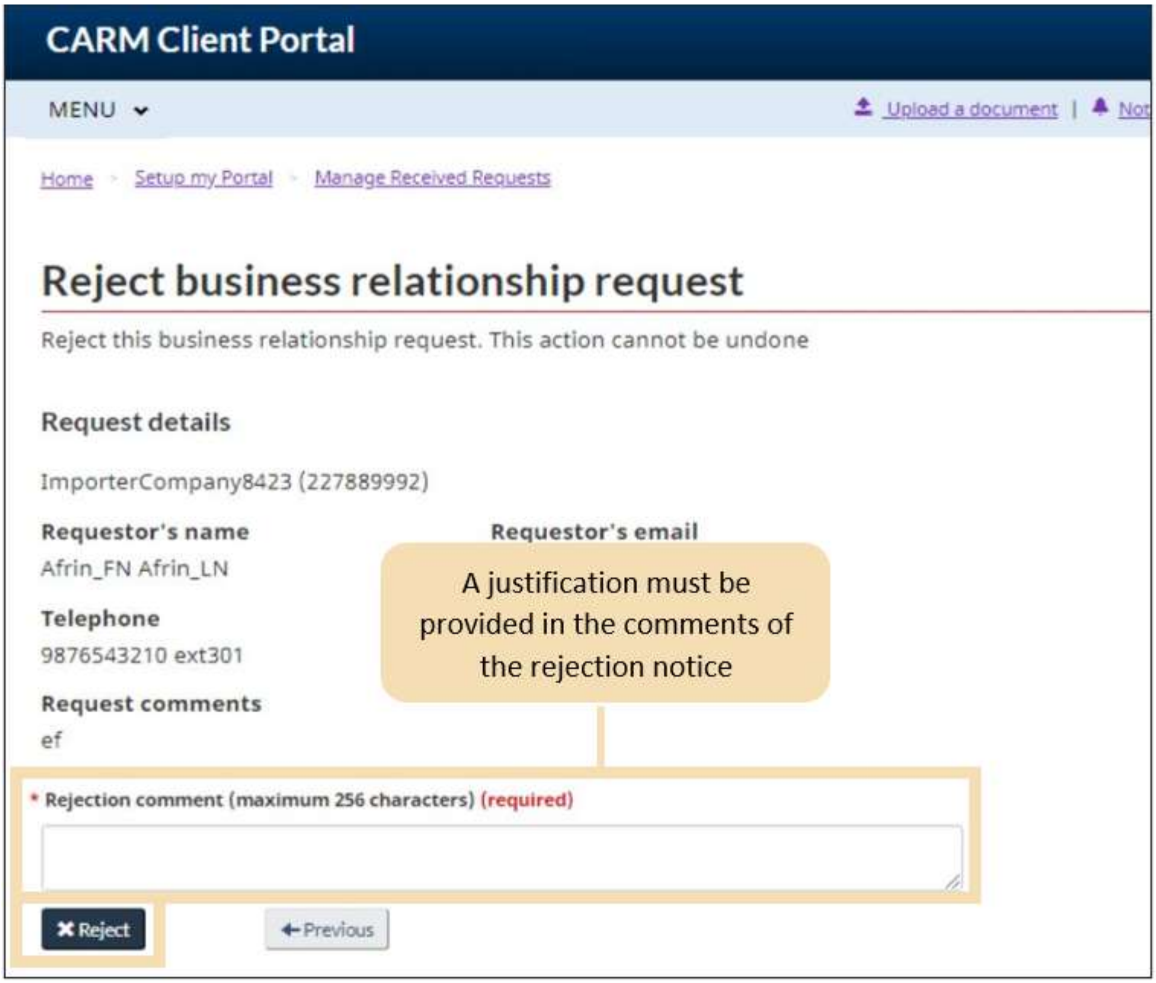
   a) If you would like to view additional information about the request, click **Details**.

   b) Click **Approve** or **Reject** in the **Actions** column, if you know the action you would like to take.



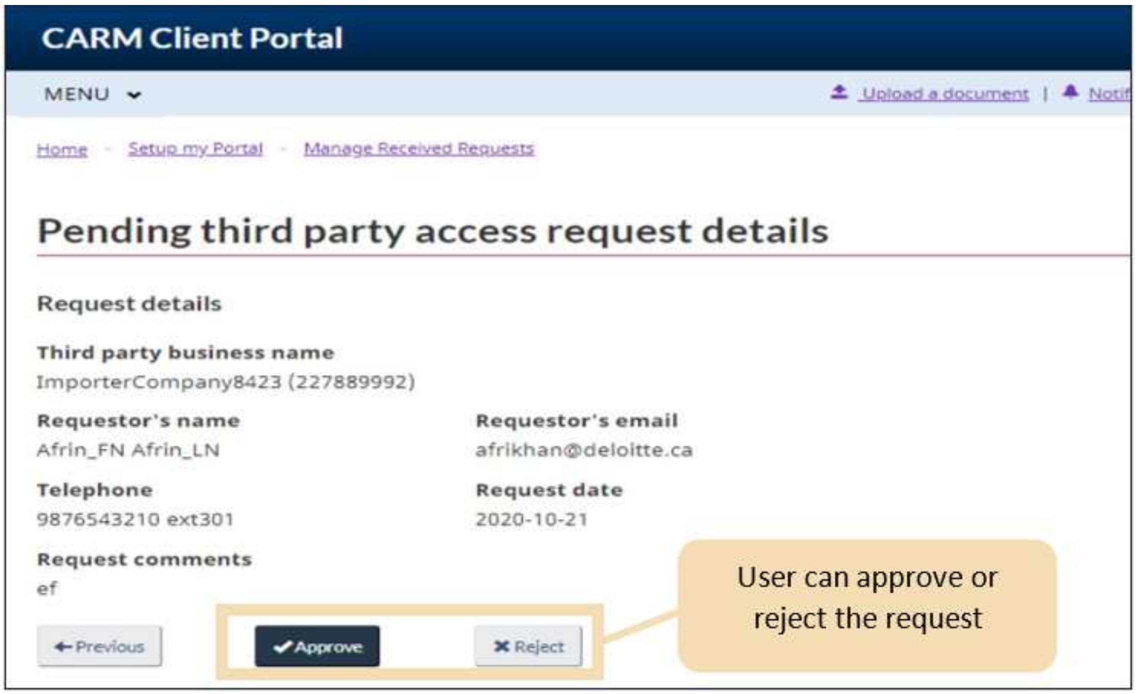
Note:

If you choose to **reject a pending third party request**, you will be brought to the below screen. A justification must be provided in the comments that will be sent back to the third party to view.



Note:

If you choose to view additional details about the request, you will be able to review comments from the third party regarding the request and can **Approve** or **Reject** from this page.

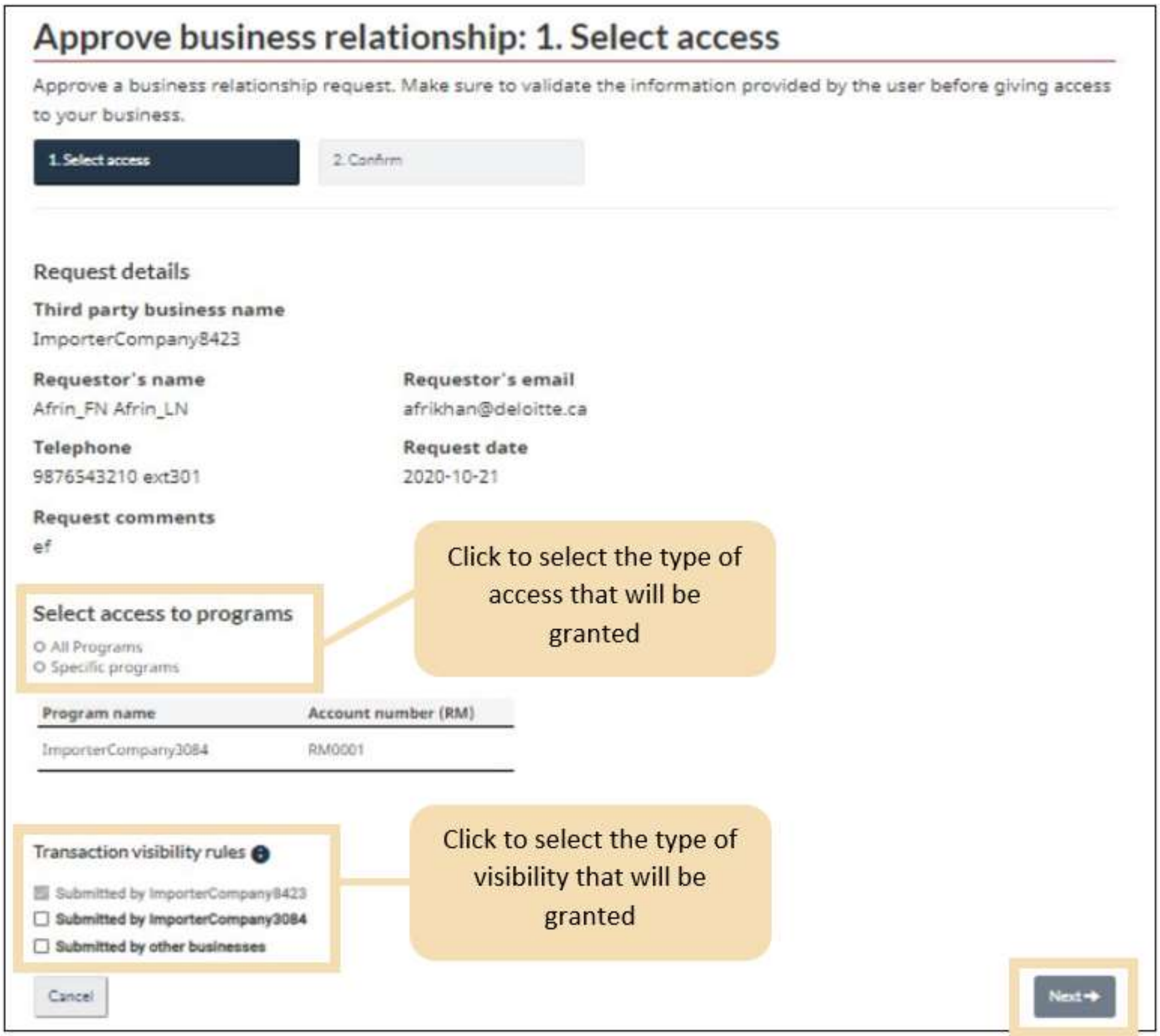


If you have chosen to approve the third-party service provider's access, you (as a client) must choose the **Access Type** and the **Visibility Attributes** of the service provider.

a) Select whether the third party should have access to **All programs** or **Specific programs**.

b) Select the **Transaction Visibility rules** for the third party.

c) Click **Next.**

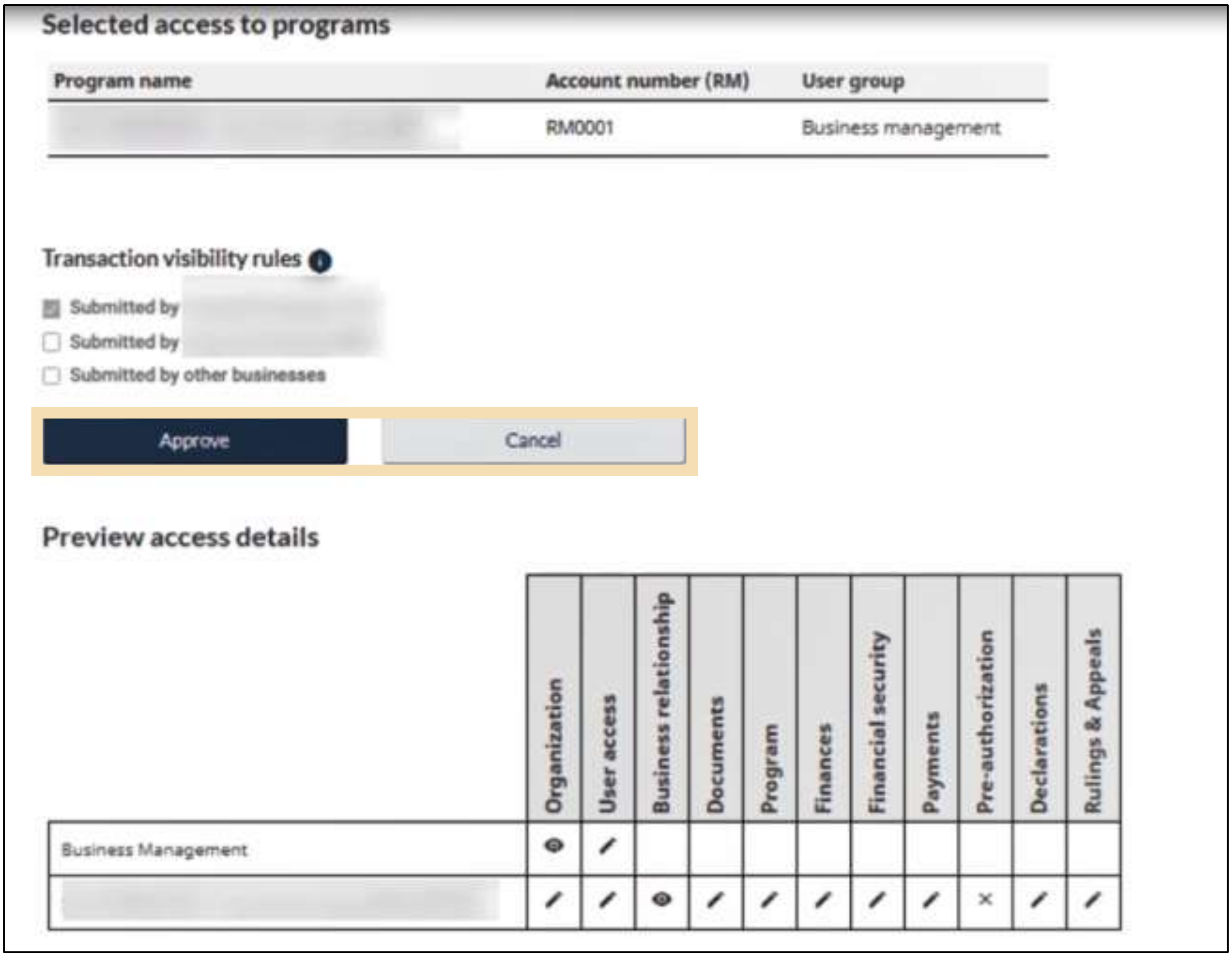


d) Review the access details that you have assigned to third party.

e) Click **Approve** to continue or **Cancel** to exit the process.

Note:

The service provider will be notified via the CARM Client Portal that their relationship request has been accepted once the relationship has been approved.



Note:

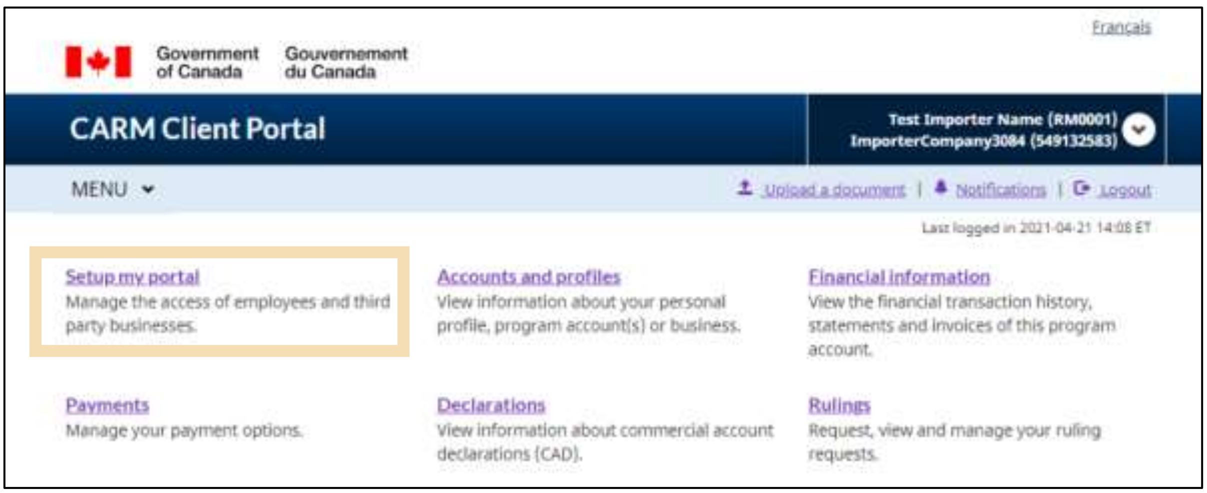
If you would like to see step-by-step walkthrough of the process, please review the following video:

- [How to delegate authority for a third party service provider in the CARM Client Portal]

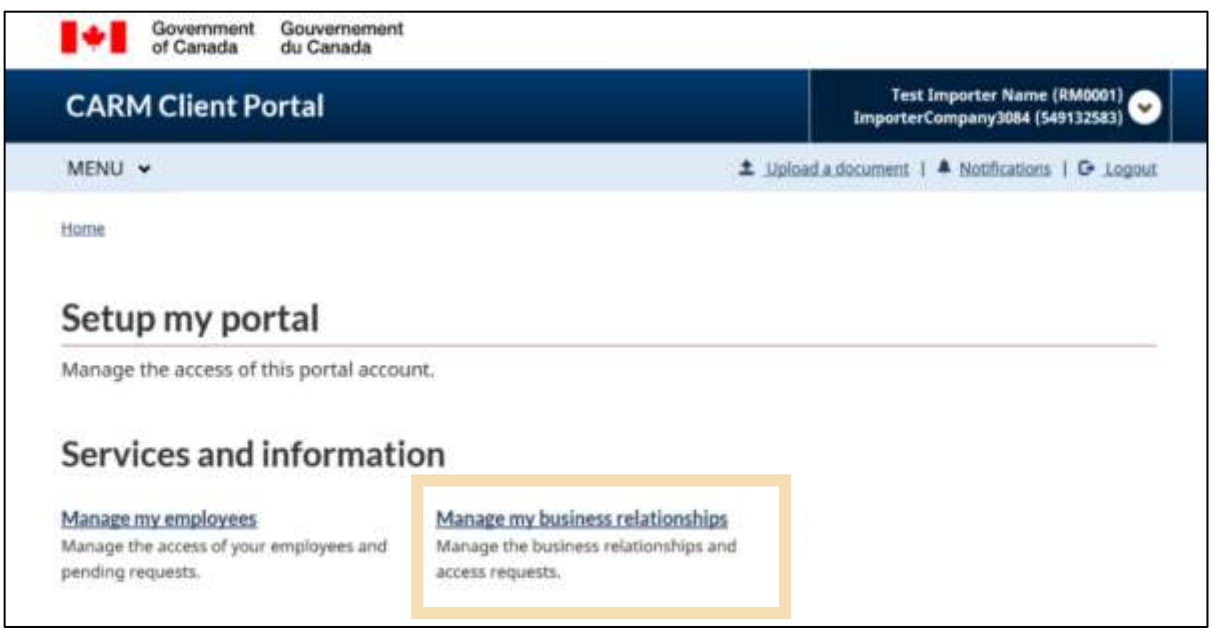
5.2 Edit access for third party service providers

Editing access for service providers is similar to the process for editing access for employees. This action can only be performed by a BAM.

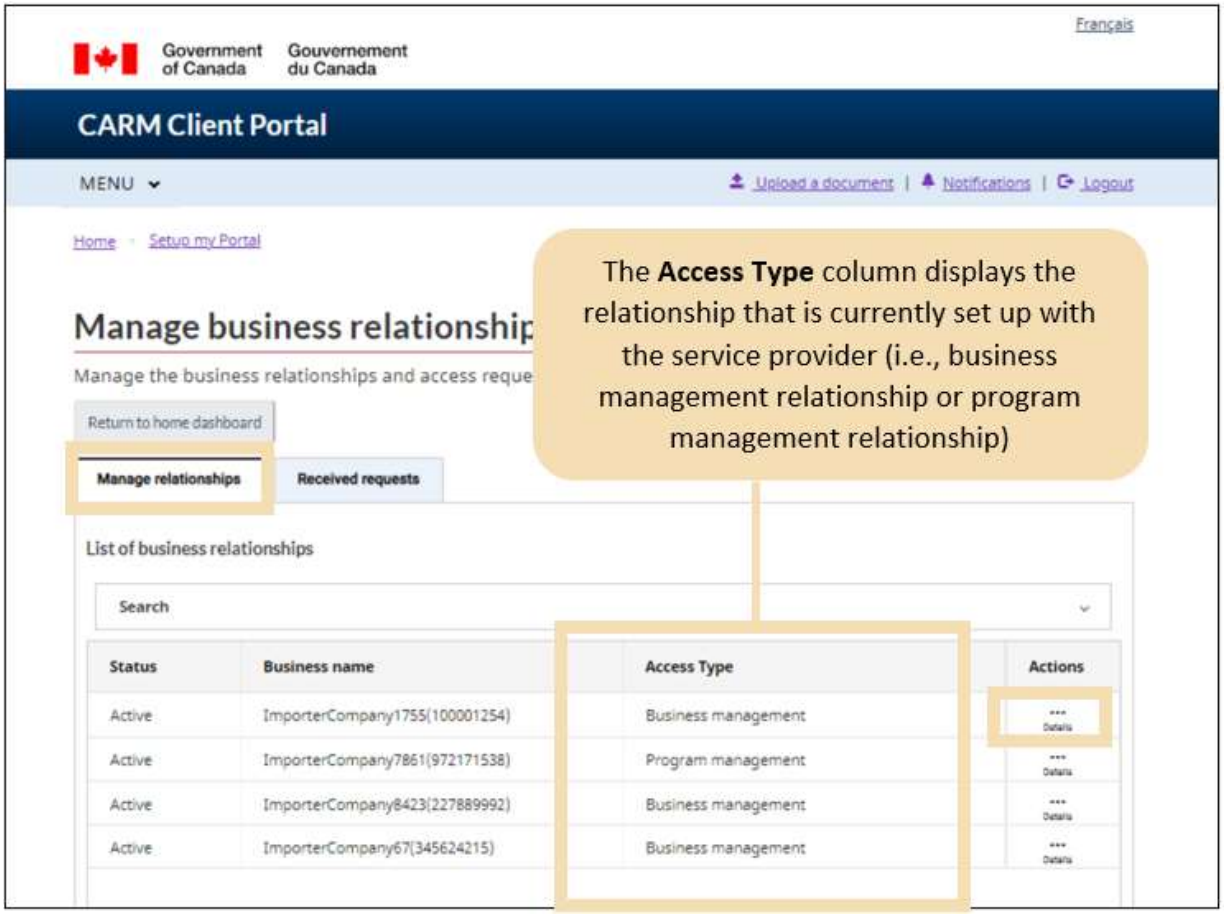
1. Select **Setup my portal.**



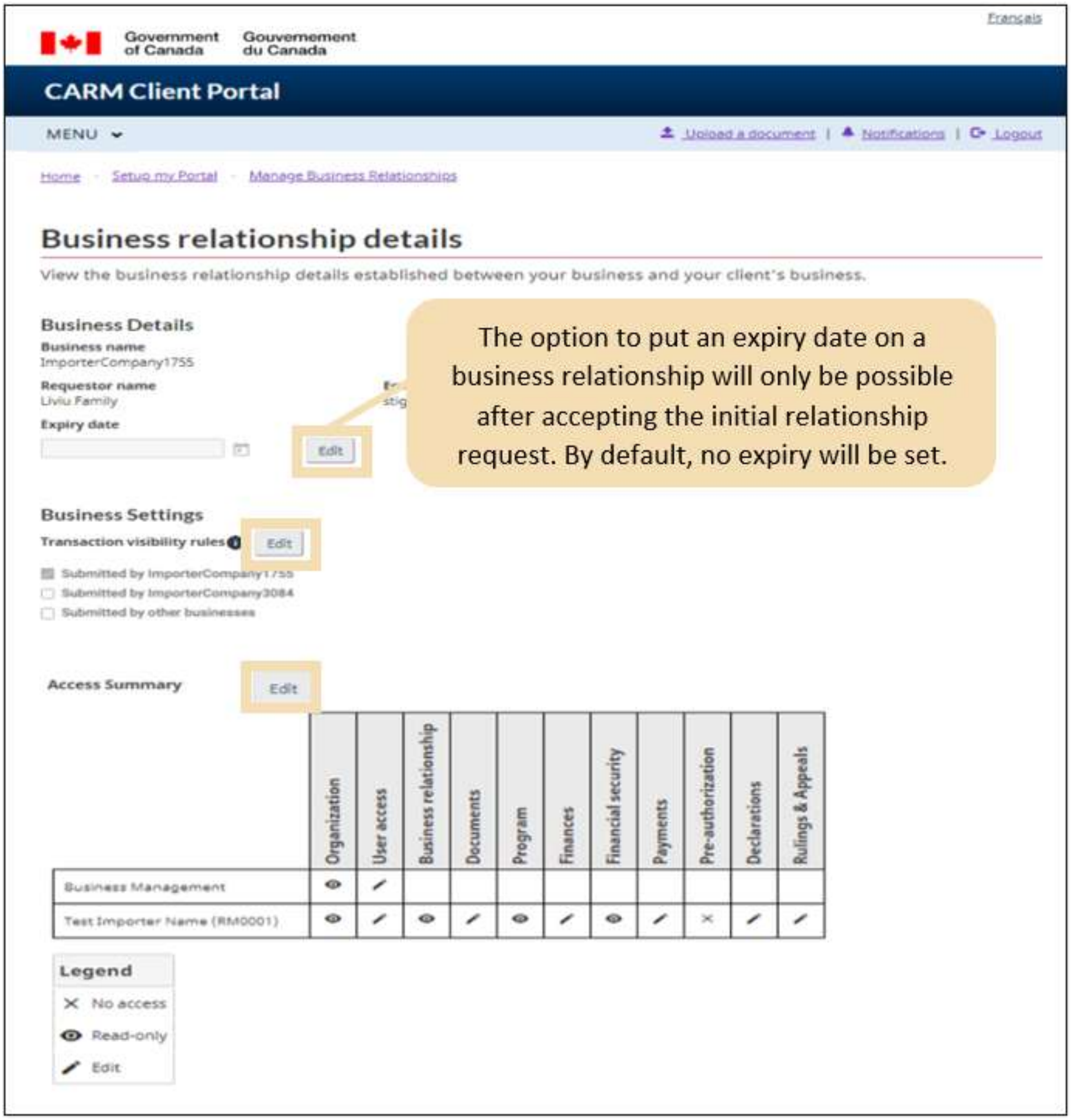
2. Select **Manage my business relationships.**



3. On the **Manage Relationships** tab, select **Details** to view and edit the access type of the service provider.



4. On this page, you will be able to edit details pertaining to the business relationship, including **Expiry date** of the relationship, visibility rules, and access type. Click **Edit** to adjust these details as required.



Note: Expiring a business relationship

- All employees including the BAM of the service provider will lose all access to the client's program accounts, and visibility attributes will be automatically removed.
- A business relationship can be re-established between the service provider and client, but re-establishing a business relationship after it is expired will not retrieve the previous configuration (access type and visibility attributes) of the relationship, nor the user roles and client group structure the service provider had for the client.

Note: Updating the access types of a service provider

If a client upgrades a relationship to business management:

- All the BAMs of the service providers that have been acting as pPAMs, are promoted to pBAMs.
- All the employees associated to a client group containing the updated client automatically gain access to all the programs per their group role (see section **6.3** for more information on client groups).

If a client downgrades a relationship to program management:

- All the pBAMs of the service provider are demoted to pPAMs.

If a client removes a program account from a business relationship:

- All service provider employees lose access to the removed program(s).

6. Delegation of authority activities for third party service providers

Once the business relationship has been granted by the client, only the pBAM or pPAM will have access to the client's account.

There are two ways to provide access to the service provider employees:

1. By assigning an employee to a **specific client**, or
2. By assigning the employee to a **client group** for bulk access management.

These processes are covered in further detail in the below sections.

Note:

To view these process steps around both managing and editing employee access please reference the following sections in this guide:

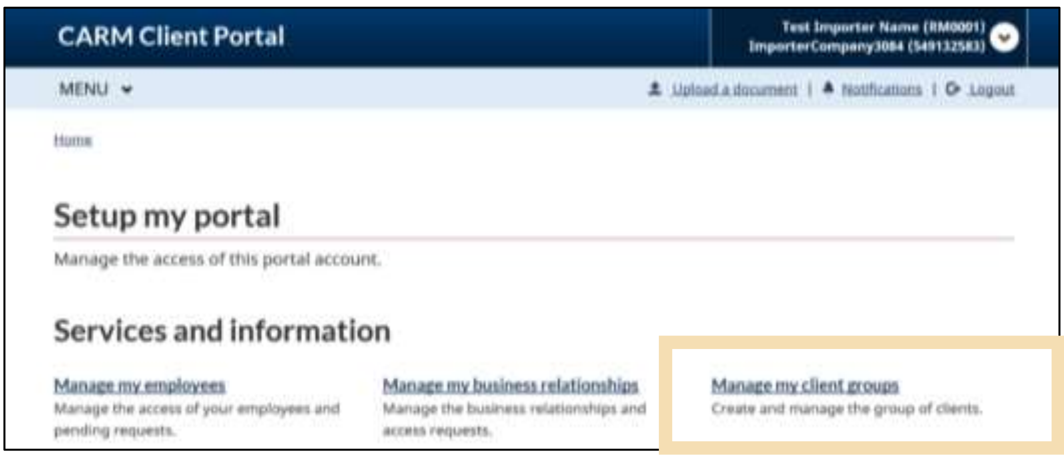
- **Managing employee access to your business account**
- **Editing employee user roles**

6.1 Creating client groups

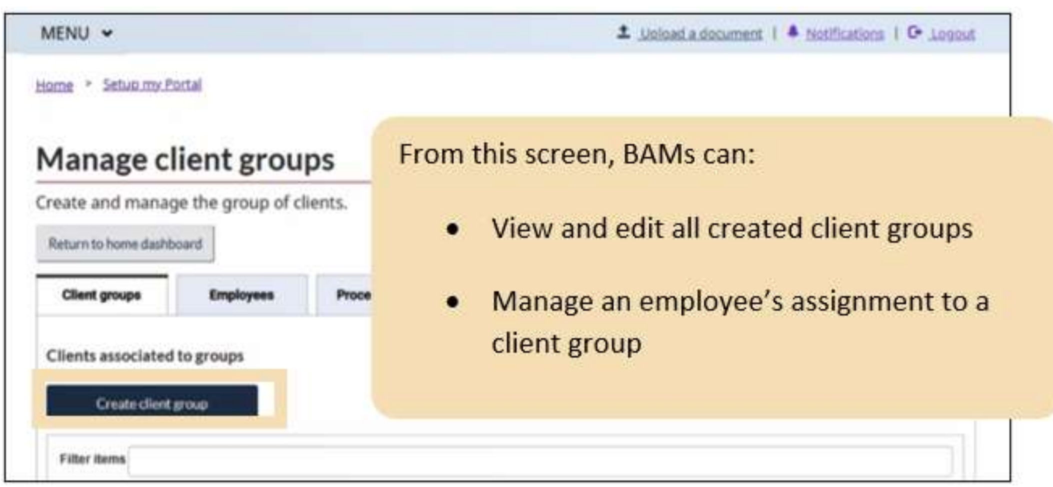
Creating client groups is a portal function that is available to service providers only. Creating groups is a helpful way for customs brokers or trade consultants with a large number of clients to manage and organize their relationships. This gives pBAMs the ability to assign their employees to whole client groups, instead of needing to individually assign employees to various clients.

To create a client group, follow the below steps:

1. From the **Setup my portal** page, click **Manage my client groups.**



2. Click **Create client group.**

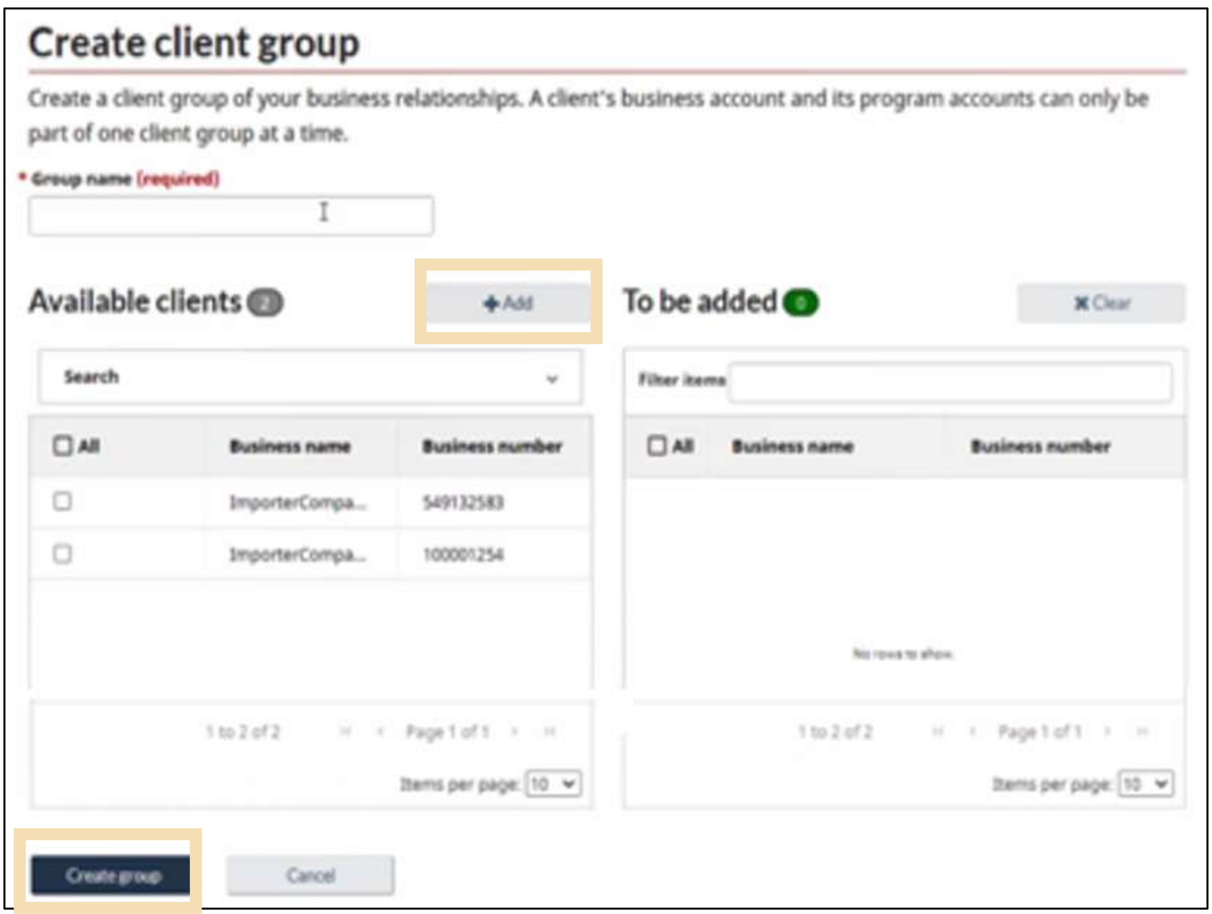


3. Input a **Group name.**
4. Select the clients that you would like to add to the group from the list of **Available clients** and click **Add** to move these clients to the **To be added** box.

Note:

There are no restrictions on the maximum number of client business accounts that can be included within the same client group.

5. Click **Create group.**



Note:

To be considered **available** a client business account must:

- Be in an active business relationship
- Not be associated to another client group set up by the service provider

A client business account can be associated with multiple client groups throughout all the service providers within the CARM Client Portal.

6.2 Assigning employees to clients and client groups

To give employees access to a client's account, the BAM or PAM must also be a pBAM or pPAM for the client.

A service provider PAM must also be assigned as a pPAM for each client to also be able to delegate access of an employee to a client's account.

Note:

Giving (and removing) access to a service provider's employee for an individual client business account is done the same way as managing employee access under the service provider's business account. To view these process steps around both managing and editing employee access please reference the following sections in this guide:

- **Managing employee access to your business account**
- **Editing employee user roles**

Note:

Remember that the service provider BAMs and PAMs can always see requests and transactions its employees have submitted.

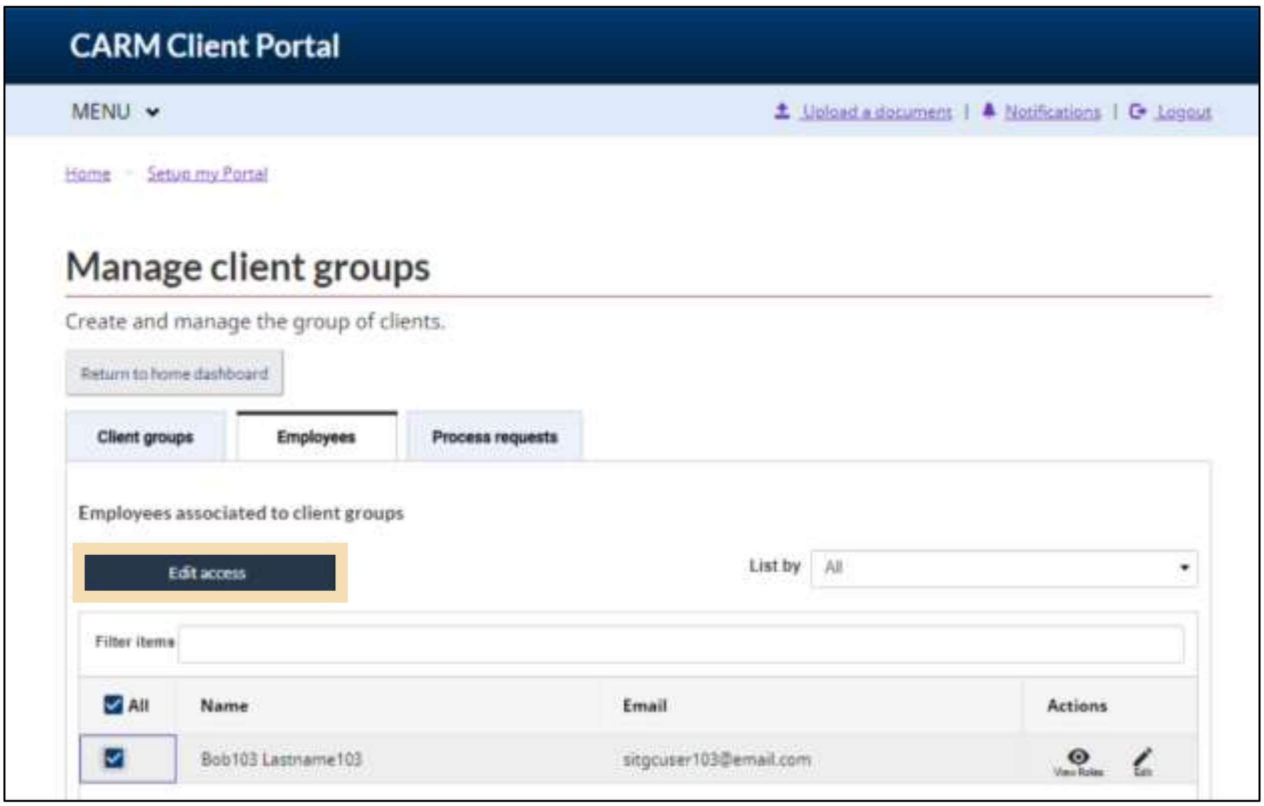
For service providers with a large number of clients, it is recommended that users manage employees' access through the client group function.

The steps below outline the process to assign employees to client groups:

1. Select the **Employees** tab from the **Manage client groups** page.
2. Click the **Edit access** button.

Note:

You can use the check boxes on the left to select multiple employees at one time.

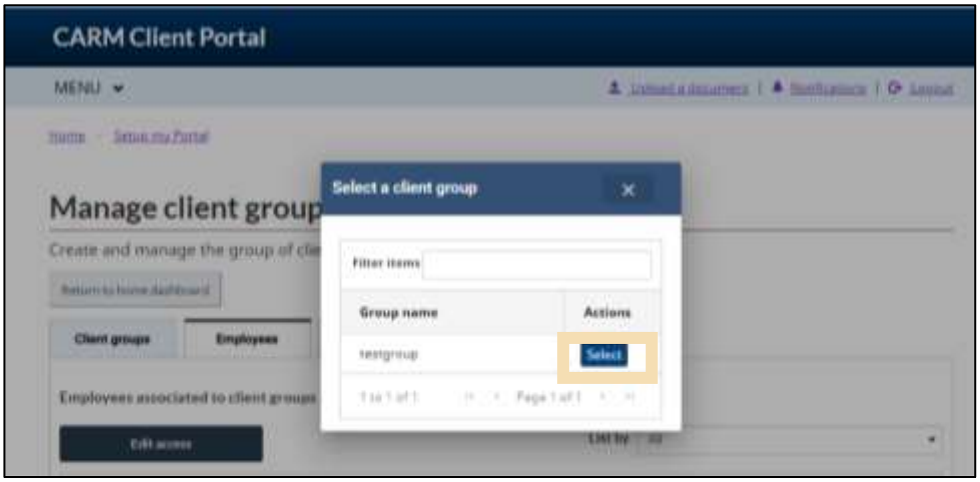


Note:

The service provider BAM already has access to all client business accounts. As such, only a PAM, Editor, or Reader can be assigned to a client group by a BAM.

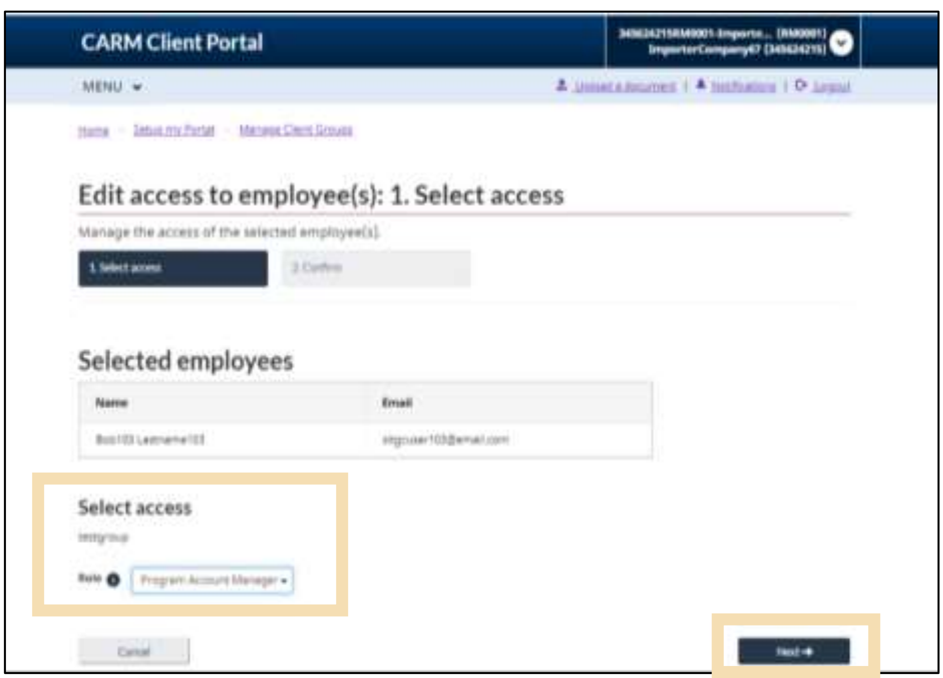
3. The below pop-up screen will display. Locate the client group that you would like to assign the employee to from those listed under the **Group name** column.

4. Click **Select.**



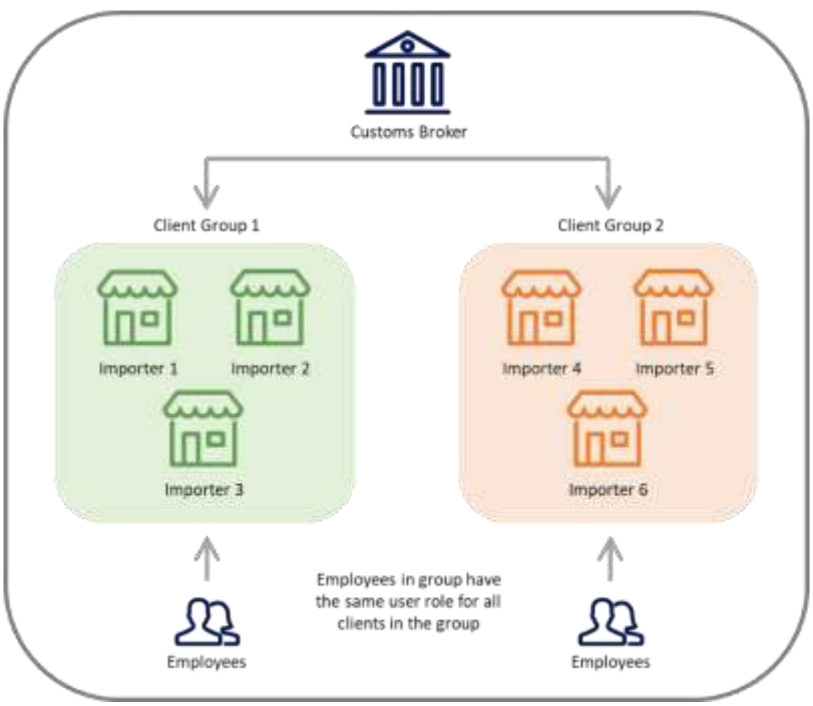
5. Select the **role** that the employee should be granted in relation to the client group from the drop-down menu.

6. Click **Next.**



7. Review the assigned **role** and **access summary** on the confirmation screen that appears.
8. Click **Save changes** to assign the employee to the group or **Cancel** to exit the process.

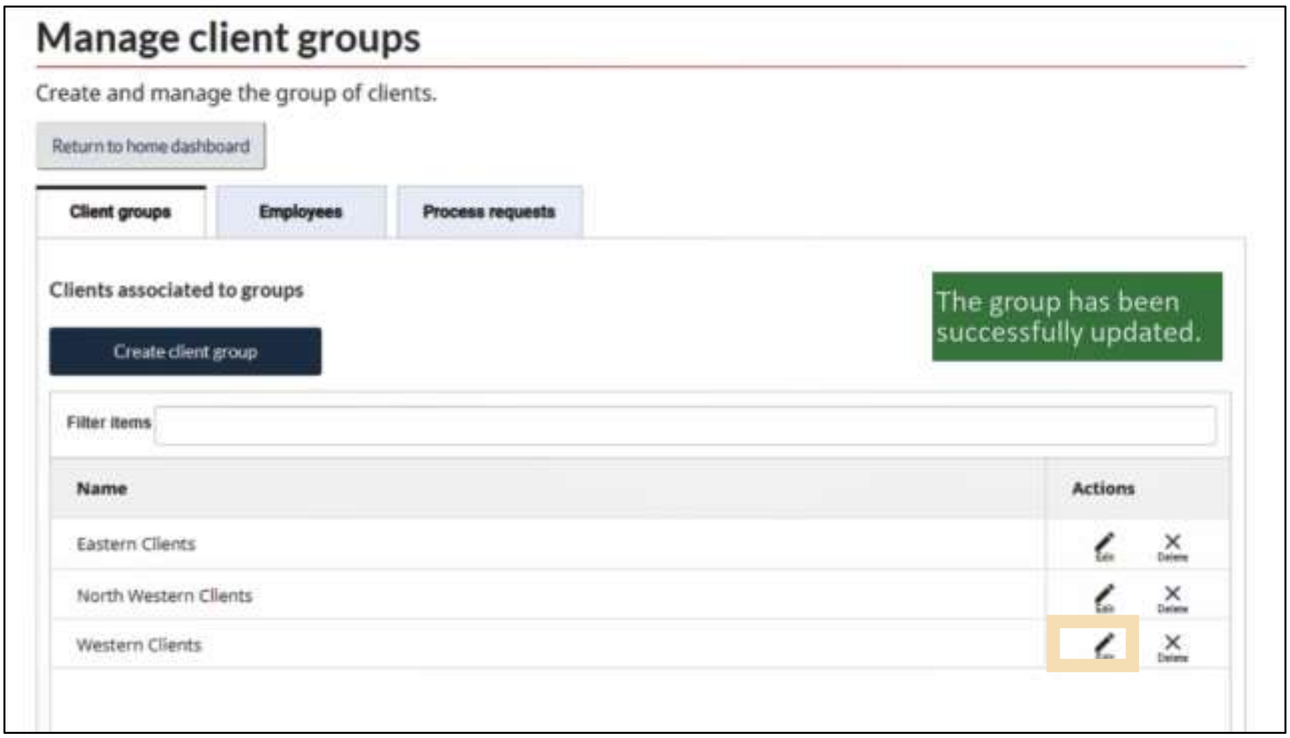
The below visual depicts how user roles are assigned to employees acting on behalf of a client group.



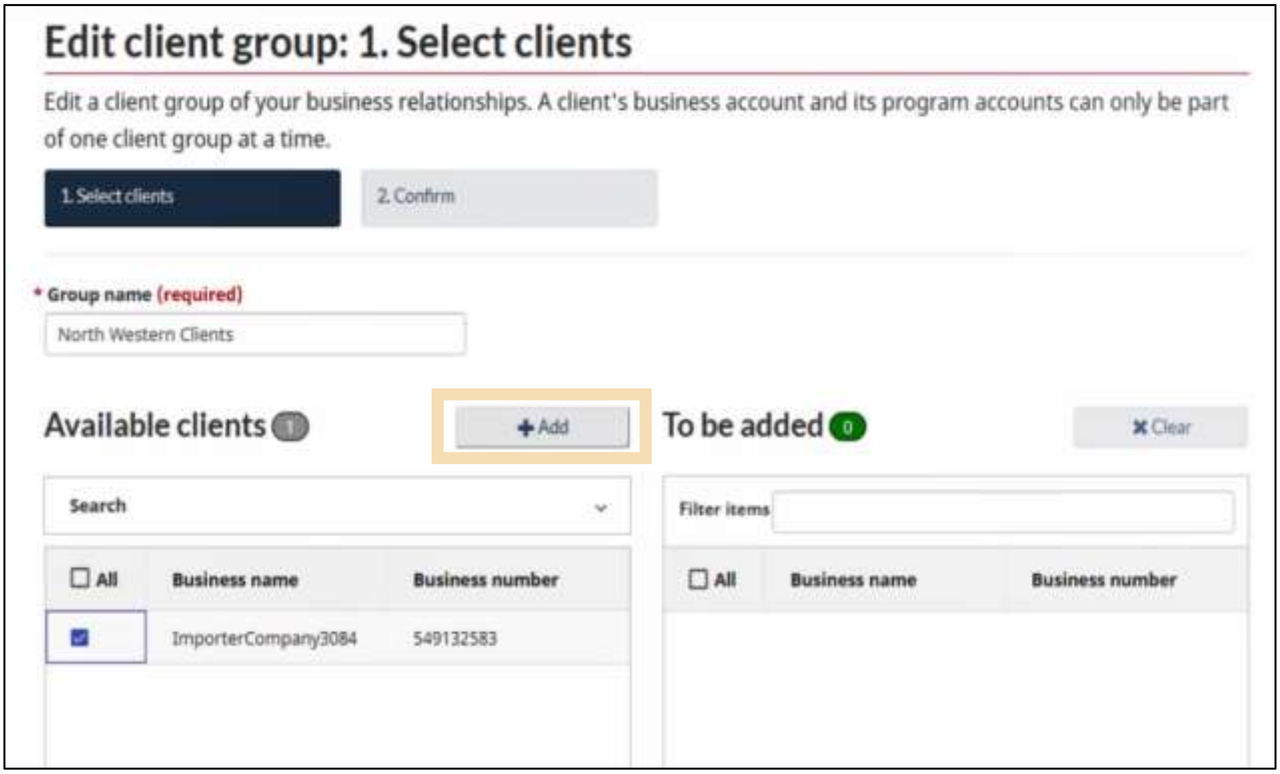
6.3 Adding and removing clients from groups

Clients can easily be added or removed from client groups as needed.

1. From the **Manage client groups** screen, click on **Edit** beside the client group that you would like to make adjustments to.



2. If you would like to add a client, select the client(s) from the **Available clients** list, and click **Add**.



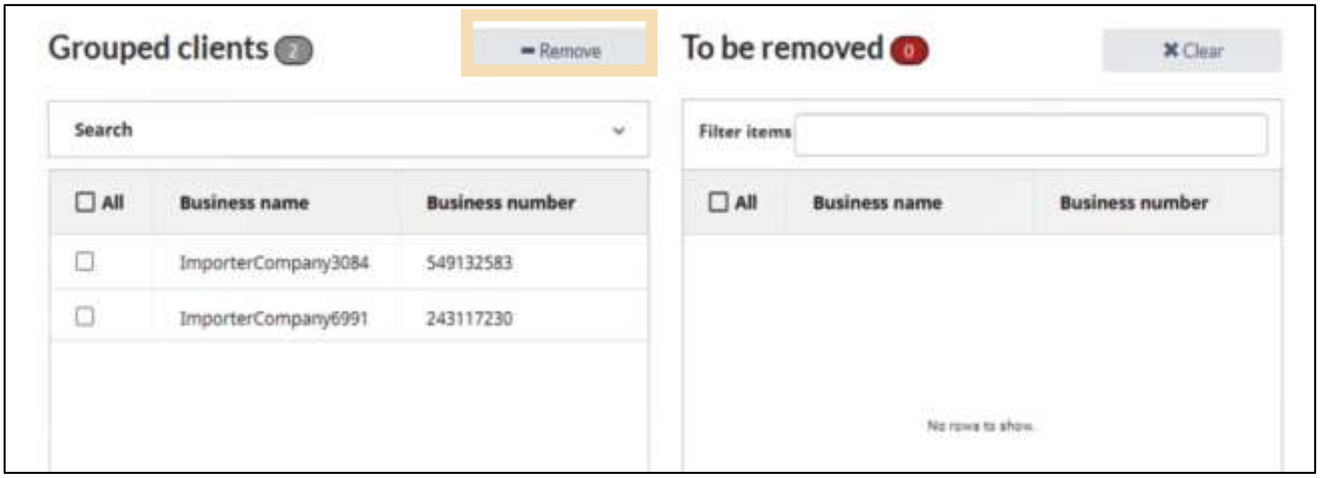
Note:

Adding a client to a group will automatically give access to the employees associated with this group according to the default roles they were assigned for the client group.

From the **Manage my employees** page it is possible to:

- Update the user role of your employees against the client group
- Override the default role by managing the employees' access for a specific business and program account

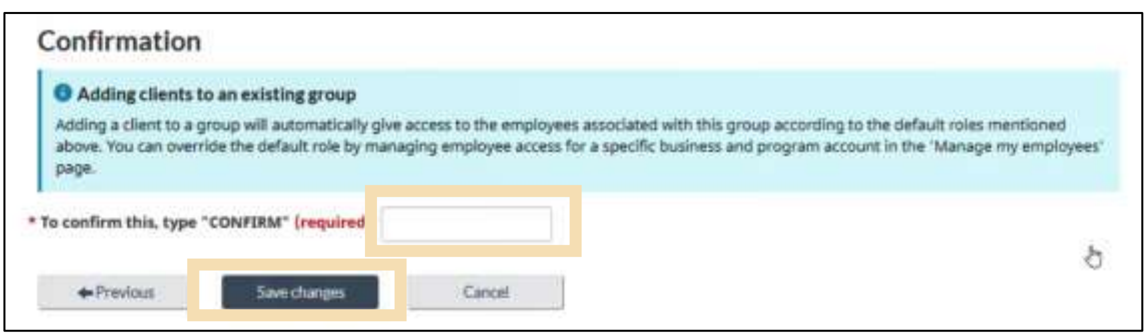
3. If you would like to remove a client from a group, scroll lower on the same page. Select clients from the **Grouped clients** list and then click the **Remove** button.



Note:

Removing a client from a group removes access for employees associated with that client's business account, with the exception of BAMs. This action cannot be undone.

4. In both instances (adding or removing a client from a group), you will need to click **Next** at the bottom of the screen. You will then be directed to a **Confirmation** page. The example for adding clients is displayed below. Type **CONFIRM** in the box.
5. Click **Save changes.**



6.4 Deleting a client group

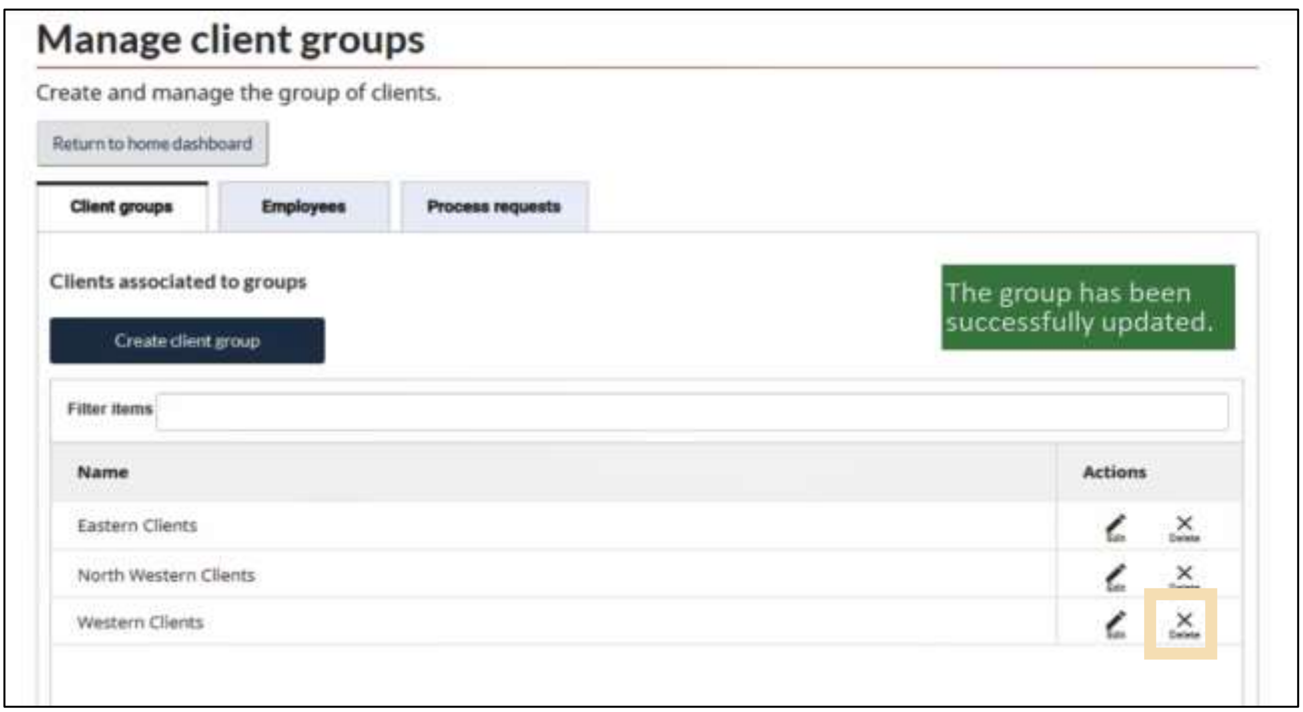
Deleting a client group removes the association of its employees and clients from the group. Any employees that were associated with the client group will lose access to all the clients' program account(s) within the deleted group.

Once deleted, the client business accounts that were associated with the group will once again be available to be associated with a new or different client group.

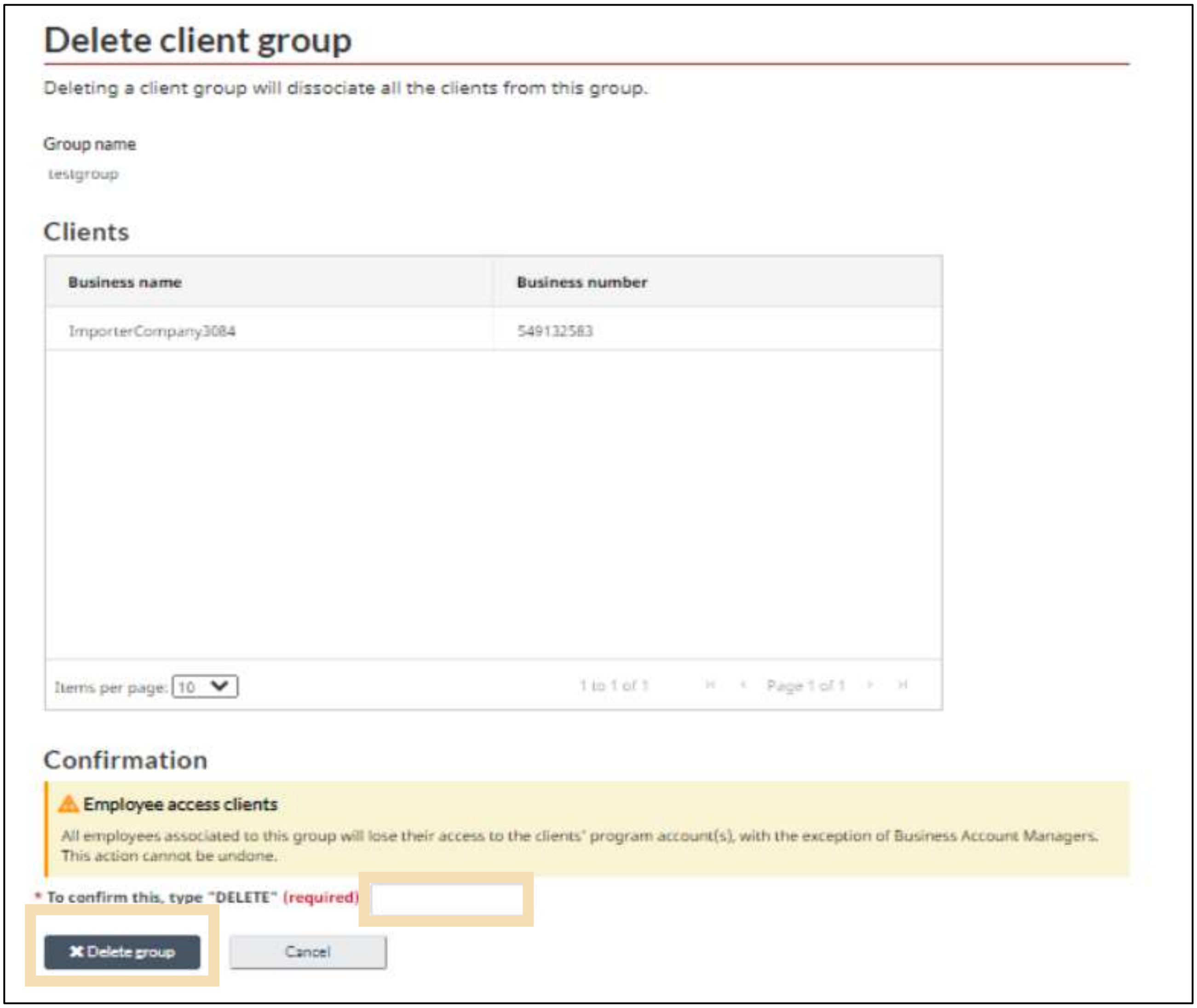
Note:

Deleting a client group is an action that cannot be undone.

1. From the **Manage client groups** page, click **Delete** beside the group that you would like to remove.

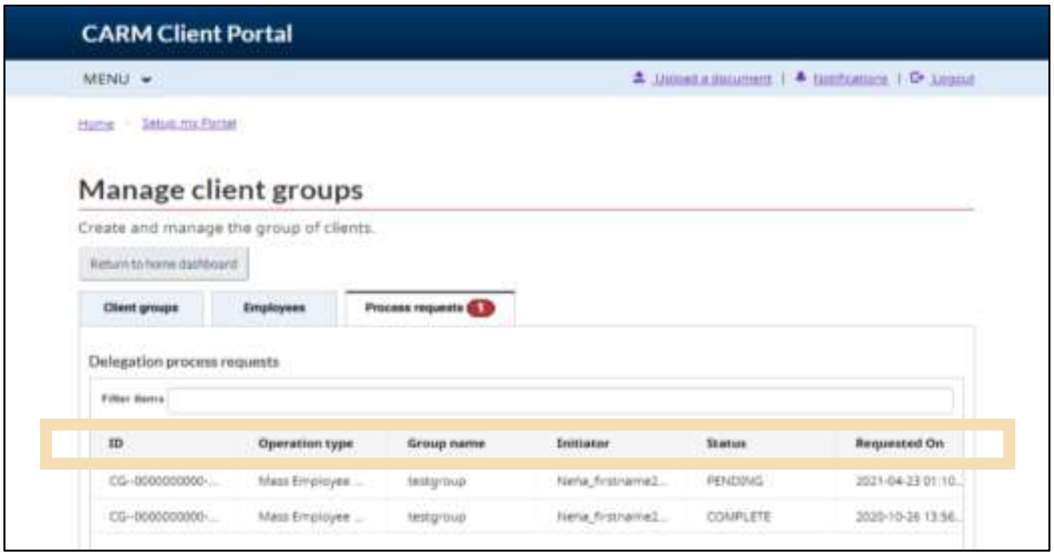


2. Type **DELETE** in the box to confirm the action.
3. Click **Delete group**.



6.5 Client group process requests

Because some client groups may contain thousands of program accounts, updating a group could require the processing of hundreds of thousands of system transactions, including updates to the user roles of a service provider's employees. As such, delays are a possibility.



The process request table located on the **Manage client groups** page allows service provider BAMs to monitor if any operations may be pending, failed, or completed.

- **System ID**: Generated ID that is helpful if technical support is required
- **Operation type**: Describes the operation requested in the system
- **Group name**: Identifies which group is impacted by the operation
- **Initiator**: Identifies which user triggered the operation
- **Status:** Identifies the current stage of the operation
- **Requested on**: Displays date and time that the operation was initiated

Note:

If you would like to see additional information on managing client groups, please reference the below video:

- **How to manage a client group in the CARM Client Portal**