Access Manager

How to manage access and permissions for ATO online services and functions using Access Manager.

About Access Manager

How to log in, set up and manage access and permissions for our ATO online services using Access Manager.

Access Manager permissions

How to manage which ATO online services and functions others can access.

Access Manager for business

How to appoint a business to act on your behalf in Online services for business or when using SBR-enabled software.

Access Manager for tax professionals

How to manage access to client tax records and restrict access to particular clients.

Access Manager for business software users

QC 40982

About Access Manager

How to log in, set up and manage access and permissions for our ATO online services using Access Manager.

Last updated 13 November 2024

On this page

Access Manager for ATO online services

Access Manager is used to **manage access and permissions** for:

- Online services for agents
- Online services for business
- Australian Business Register (ABR).

It also allows you to manage which functions others can access on behalf of your business.

To manage access for **Online services for foreign investors**, go to **Authorise a representative.**

Learn more about:

- Access Manager for business
- Access Manager for tax professionals
- Access Manager for business software users

Log in to Access Manager

To log in to Access Manager and manage permissions you need:

- a Digital ID, such as myID
- to be the principal authority or authorisation administrator in Relationship Authorisation Manager (RAM).

Log in to Access Manager

Access Manager through RAM

Relationship Authorisation Manager (RAM) is an authorisation service that allows you to access our online services on behalf of a business.

RAM is connected to Access Manager. When you authorise a person to act on behalf of your business using RAM, you can set their permissions in Access Manager at the same time.

By logging in to Access Manager through RAM, you agree to:

- comply with the terms and conditions of myID and RAM
- always keep your myID secure and not share it with others.

Log in to Relationship Authorisation Manager

Roles and authorisation types

Authorising and managing permissions for staff is one of the main functions of Access Manager. To do this, you need to be either of these authorisation types in RAM:

- **principal authority** – you have full access to ATO online services
- **authorisation administrator** – you can create and manage authorisations for others. This role must be authorised by a principal authority or another authorisation administrator.

If you're a principal authority or authorisation administrator in RAM, you automatically become an **administrator** in Access Manager. This means you:

- have access to all permissions for ATO online services – an authorisation administrator's permissions can only be modified by a principal authority
- can **set up authorisations** and grant Full, Custom or No access to users in RAM. Users with custom access have limited access to ATO online services and must be assigned specific permissions in Access Manager.

Note: Once you assign permissions to authorised users, anything they do in ATO online services is legally binding to your business.

Set permissions using RAM

In RAM you can set, view, modify, remove, disable, and restore permissions.

To set permissions in RAM when you add a new user:

1. Select **Custom** for **Australian Taxation Office** in the **Agency access**. Custom access users will be visible in Access Manager once the authorisation is created in RAM.
2. Complete the steps in the **Summary** section.
3. Select **ATO Access Manager**. Not all online services offer this option in custom set up.

You will now be in Access Manager.

View or modify permissions

To view or modify existing permissions in RAM:

4. Select the user.
5. Select **View** or **Edit.**
6. Select **ATO Access Manager**.

You will now be in Access Manager.

Responsibilities when using Access Manager

Access Manager allows you to manage who has electronic access to your business' tax information. It's your responsibility to regularly review and monitor who has access to your business records.

Data about individuals and entities in Access Manager is confidential. You must ensure that unauthorised people don't compromise the integrity of that data. If you leave your computer unattended, even briefly, you must log out from Access Manager or lock your computer.

When you log in to Access Manager, you agree to:

- comply with the terms and conditions of myID and RAM
- always keep your myID secure and not share it with others
- not disclose your myID password or share it with others.

By providing others with access to secure business information through myID and RAM, as yourself or as a representative for tax purposes, you must understand:

- **user access and permissions** – the level of access given to each type of user (Administrator, Authorised Custom, Authorised Full, Authorised Basic) and the transactions users can undertake. For more information, see Access Manager permissions.
- **business appointments** – the nature of your relationship with any entities you have appointed as a representative for tax purposes and what transactions they can undertake.
- **legally binding actions** – the actions these users and representatives undertake through Access Manager are legally binding to your business.

Preventing unauthorised access to business information

If your staff have access to your secure information in ATO online services, we strongly recommend that you:

- use Access Manager regularly to ensure that a user's level of access to our systems is appropriate
- immediately disable or remove a user's account in Access Manager and RAM if you have any concerns about their activities
- ensure that each person who deals with us online on behalf of your business has their own myID
- keep passwords secure – they must not be shared.

If you use hosted (online) SBR-enabled software, we strongly recommend that you limit access to stored business information to appropriate staff only. If you have any concerns, contact your digital service provider for advice.

QC 71002

Access Manager for business

How to appoint a business to act on your behalf in Online services for business or when using SBR-enabled software.

Last updated 22 July 2024

On this page

Appoint a business and assign permissions

The appointing business is known as the 'principal business'. Any actions taken by the appointed business are deemed to have been taken by the principal business.

Tax professionals **don't** require a business appointment, as they transact on your behalf using Online services for agents.

If an Authorised contact does not have an approved credential, they can appoint a business by completing a Cross entity authorisation nomination form.

To appoint a business and assign permissions:

1. Select **Who has access to my business**.
2. Select **Appoint new business**.
3. Enter the ABN of the business to be appointed.
4. Select **Continue**.
5. Select the relevant permissions, or the **Select all** and **Clear all** buttons above the list.
6. Select **Save**.

Administrators of the appointed business will automatically be given the permissions that are assigned.

Administrators will need to authorise any other users in the business who require access to the permissions as 'Standard users' (authorised users) in RAM.

Modify permissions for an appointed business

To modify the permissions for an appointed business:

1. Select **Who has access to my business**.
2. Select the appointed business from the list.
3. Select or unselect each permission, or the **Select all** and **Clear all** buttons above the list.
4. Select **Save**.

Remove a business appointment

To remove an appointed business:

1. Select **Who has access to my business**.
2. Select the appointed business from the list.
3. Select **Remove Business Appointment**.
4. Select **Confirm**.

Assign access to authorised users for a principal business

To assign permissions to Standard users (authorised users) in bulk:

1. Select **Whose business I can access**.
2. Select **My credential holders with auto access** – this will list all credential holders and let you give the user auto access if they don't already have it.
3. Select **Give auto access** from the **Manage access** column – this gives the user access to
    - any future business appointments given to the business
    - all permissions made available by each business appointment.

To assign individual permissions:

1. Select **Whose business I can access**.
2. Select the relevant business – you can search for the business using the ABN or business name.
3. Select **View authorised credential holders** – the business permissions displayed are the permissions that have been granted by the appointing business and are read only.
4. Select **Authorise new credential holder** – a list of users who already have access to the principal business will also appear under **Authorised credential holders**.
5. Select a user to assign access – you can search using their surname or given name.
6. Select **Credential holder list** – this list includes all users who don't have access to the appointing business.
7. Select the relevant permissions or use the **Select all** and **Clear all** buttons above the list. Only permissions allocated to the appointed business are displayed.
8. Select **Save**.

Modify or remove access to authorised users for a principal business

If auto access has been set, it needs to be removed before permissions can be modified. Removing auto access will remove all access.

To remove auto access:

1. Select **Whose business I can access**.
2. Select **My credential holders with auto access**.
3. Select **Remove auto access**.

If you removed auto access to modify access, follow the steps to [Assign access to authorised users for a principal business].

If auto access hasn't been set:

1. Select **Whose business I can access**.
2. Select the relevant business – you can search for the business using the ABN or business name.
3. Select **View authorised credential holders** – the business permissions which have been granted are by the appointing business and are read only.
4. Select the user.

To modify access:

1. Select or deselect the relevant permissions, or use the **Select all** and **Clear all** buttons above the list – only permissions allocated to the appointed business are displayed
2. Select **Confirm**.

If you're removing access:

1. Select **Remove Authorisation**.
2. Select **Confirm**.

QC 71004

Access Manager for tax professionals

How to manage access to client tax records and restrict access to particular clients.

Last updated 1 December 2022

Assign a RAN

To give employees 'Full', 'Custom' or 'Basic' access to the clients of your registered agent number (RAN), you need to assign it to them. You can assign multiple RANs if you have more than one.

To assign a RAN:

1. Select **Manage permissions**.
2. Select the user.
3. Select **Assign RANs** at the **Modify access and permission** screen.
4. Select the RAN you are giving access to on the **Tax practitioner access** screen.
5. Select **Save** to return to the **Modify access and permissions** screen.
6. Select **My Clients** and select permissions.

Assign permissions to access your clients

After you have assigned a RAN to a user, set up the permissions they need to access your clients.

To assign permissions:

1. Select **Manage permissions**.

2. Select the user.
3. Under **Permissions** select the **Client** tab.
4. Select the relevant permissions.
5. Select **Save**.

Assign permissions to restricted clients

You can restrict client accounts that are sensitive or private.

When you restrict a client, administrators and employees with Full access are the only users who can access that client's information. You can then specify which users can access that client in Online services for agents.

Clients can be restricted from **Restricted clients**, available from the left-hand menu in Access Manager.

To give permissions to restricted clients:

1. Select **Manage permissions**.
2. Select the user.
3. Under **Permissions** select the **Client tab**.
4. Select **Access to all restricted clients** permission.
5. Select **Save**.

Manage access to your client list

An authorised user in your practice can download your client list when they use Online services for agents.

To manage access to the client list bulk download function:

1. Select **Manage permissions**.
2. Select the user.
3. Under **Permissions** select the **Client tab**
    a. To allow access – select **View** at **Client list – bulk download**
    b. To remove access – deselect **View** at **Client list – bulk download**.

4. Select **Save**.

QC 71005

Access Manager for business software users

How to use Access Manager to notify us of your hosted SBR-enabled software and manage machine credential permissions.

Last updated 4 December 2024

On this page

Notify us of your hosted SBR software

If you have purchased or subscribed to hosted cloud-based SBR-enabled software, you need to notify us of your digital service provider.

You will use your SBR software for transactions to and from the ATO. Your digital service provider will advise you if the software you have purchased is eligible.

You only need to notify us of your digital service provider **once**. You can then remove, change or let us know about another provider at any time.

Before you begin you will need:

- the digital service provider's ABN or their name

- the software ID to complete the notification (your digital service provider will provide you with a software ID when you purchase or subscribe to their service).

Notify us of your hosted services

To notify us of your hosted SBR-enabled software services:

1. Log in to Access Manager.
2. Select **My hosted software services.**
3. Select **Notify the ATO of your hosted service.**
4. Search for a digital service provider in the list, or by typing the ABN or name.
5. Select the **ABN link** of your digital service provider.
6. Enter the software ID provided to you by your digital service provider and select **Next.**
7. Read the **Notification** statement then select **Save**.

A success message will appear on the next screen to confirm your notification.

The software ID must match the details provided by your digital service provider.

To let us know about additional SBR software services you have, repeat the above steps.

Remove a notification

To remove a notification for your hosted SBR-enabled software service:

1. Log in to Access Manager.

2. Select **My hosted software services**. Your current digital service providers will display.

3. Select the **ABN link** of the digital service provider to modify or remove the notification.

4. Select **Remove notification.**

5. Select **Save**.

A success message will appear on the next screen confirming the removal.

This will remove both the digital service provider notification and all software IDs.

Add or remove a software ID

You can add additional software IDs or remove a software ID which is no longer used or is invalid. To do this:

1. Log in to Access Manager.

2. Select **My hosted software services** – your current digital service providers will display.

3. Select the **ABN link** of a digital service provider to modify or remove the notification.

4. Type the new or corrected software IDs in the **Add Software IDs** fields.

5. Select **Remove** heading to remove unwanted software IDs.

6. Select **Next** to review your changes.

7. Select **Save**.

A success message will appear on the next screen confirming the changes.

Customise machine credential permissions

If you are using desktop or locally hosted software, you need your own machine credential to enable your software to interact with the ATO. You can manage the services a machine credential can access by editing permissions in Access Manager. Note some software may have permission management built in.

When you create a machine credential to interact with our online services through your business software, it will:

- automatically have full permissions
- not have access to business appointments

- not be selected for use in hosted SBR services.

Before you can edit the machine credential permissions in Access Manager, you need to:

- ensure the Agency access for the machine credential is set to **Custom** in Relationship Authorisation Manager (RAM)
- submit a **single** test lodgment through your SBR-enabled software. This ensures the machine credential details are registered in Access Manager and interactions with the ATO using this machine credential are successfully processed.

Once the **single** test lodgment is complete, the machine credential will appear in Access Manager, and you can edit permissions.

Manage permissions

To add or remove permissions for a machine credential:

1. Log in to Access Manager.
2. Select **Manage permissions.**
3. Enter the name of the machine credential in the **Family Name** field and select **Search**, or you can filter the list by Device or Machine.
4. Click on the Machine Credential name.
5. Add or remove permissions for the credential.
6. Select **Save**.

Add access to business appointments

To add access to business appointments for a machine credential:

1. Log in to Access Manager.
2. Select **Whose business I can access.**
3. Select **My credential holders with auto access.**
4. Enter the name of the machine credential in the **Family Name** field and select **Search** or you can filter list by Device or Machine.
5. Select **Give auto access for the preferred machine credential.**
6. Select **Save**.

Add access to an individual business

To add access to an individual business for a machine credential:

1. Log in to Access Manager.
2. Select **Whose business I can access.**
3. Search by ABN or business name.
4. Select the business you wish to provide access to.
5. Select **View authorised credential holders.**
6. Select **Authorise new credential holder.**
7. Enter the name of the machine credential in the **Family Name** field and select **Search.**
8. Select the machine credential.
9. Select all permissions – the machine credential will only have access to the permissions assigned by the appointing business.
10. Select **Save**.

Note this action is not applicable to machine credentials with Auto Access.

QC 71006

Cloud software authentication and authorisation

Standard Business Reporting cloud accounting software simplifies the way businesses and agents interact with the ATO.

Last updated 5 September 2022

On this page

Interacting with us

Online software solutions are available through software providers and:

- ensure compliant, secure and streamlined transactions online anytime from any device
- allow you to notify us of your hosted Standard Business Reporting (SBR) software service, so you can securely interact with us using cloud software
- co-exist with online software, including compatible desktop solutions.

Use the SBR product register to confirm if your hosted SBR software provider is certified for the online cloud solution. Once you have subscribed to, or purchased SBR cloud-based software, you need to notify us of your hosted SBR software provider's details.

How to notify us

To complete your one-off notification, choose from the following options.

- If you're the entity's primary or authorised contact on our records, an eligible associate or authorised business staff, log in to **Access Manager**. Follow the steps to notify us of your **hosted SBR software services.**
- If you're having difficulties or you're a registered agent helping your client to notify, phone **1300 85 22 32** with the following information
  - proof of record ownership (for example personal TFN, date of birth, address, recent ATO-generated notice)
  - your Australian business number (ABN), or if you are a registered agent, you can use your registered agent number (RAN)
  - the name or ABN of your software provider
  - your unique software ID (provided by your software provider).

Frequently asked questions

Can I have more than one online software provider?

Yes. You can have more than one online software provider.

Can I have multiple software IDs?

Yes. You can have multiple software IDs. Your software provider can advise you.

If I complete a notification for hosted SBR software services will this affect any of my other accounting programs?

No. You can use other accounting programs in addition to SBR software services. Check with your software provider on any specific changes relating to your individual programs.

Do registered agents need to complete a notification for each RAN?

If you're a registered agent and have multiple RANs, the notification applies to the ABN for the entire practice; you don't need to notify for each RAN.

Do registered agents have the authority to complete the notification on behalf of their client?

Yes. An agent can do the software ID notification on behalf of the employer regardless of whether they will be processing payroll/lodging the pay events.

Use the software ID registered, for the party that will be lodging. If they think that both the agent and/or the employer may lodge at different times, there is the ability to register multiple software IDs (for example the employers and the agent's software ID).

Why am I receiving an error when I lodge?

Ensure the following are correct:

- your tax practice ABN is the one you have linked to your agent number
- your client's TFN/ABN is correct and is linked to your RAN (if you have more than one RAN, check it is the correct one)
- where you have more than one ABN, you are using the right ABN (that is, the same ABN provided when completing your software provider notification or registered in Access Manager).

For more information see the **Practitioner lodgment service (PLS) user guide**.

Can I use cloud software for other government agencies?

The solution is implemented in the ATO Access Manager and is only for the ATO. A similar solution has been implemented for the Unique Student Identifier in Relationship Authorisation Manager. Other agencies may choose to leverage the latter solution.

QC 44965

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.