Australian Government
Australian Taxation Office

Print entire document

Using Access Manager

- https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/ (https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/)
- Last modified: 25 Oct 2019
- QC 40983

Using Access Manager

With Access Manager, you can control and manage the relationships between businesses, agents and providers, and the permissions of staff using ATO online services.

Functions include:

- Access and permissions (for businesses) – manage your employees' access to your business tax records.
- Access and permissions for Tax agents and BAS agents – manage your employees' access to your clients' tax records.
- Business appointments – appoint another business to act on behalf of your business. The appointed business is able to manage their staff's access to businesses they are acting on behalf of.
- Restricted clients – tax agents and BAS agents can use this function to restrict their employees' access to particular clients.
- Notify us of a hosted SBR software service – (previously *Nominate online software service provider*) enables businesses and registered agents to notify us of their hosted SBR software service providers, they use for transactions to and from the ATO, using their hosted software (cloud) environments.

AUSkey replacement

From **1 April 2020** myGovID and Relationship Authorisation Manager (RAM) will replace AUSkey and Manage ABN connections (your ABN connected to your myGov).

RAM is connected to Access Manager. This means when you authorise a person to act for a business using RAM, you can set their permissions in Access Manager at the same time. You can also transfer the permissions of existing AUSkey users using the 'Import AUSkey users' function in RAM.

As a result, you will notice some different fields in Access Manager.

In the **Access and permissions** screen:

- 'Credential type' is now 'Authorisation type' – lists authorisation types such as authorised user, principal authority, authorisation administrator, Standard AUSkey, Admin AUSkey and Device
- new 'Access level' – lists the level of access for each user. 'Full' means the user has all permissions, 'Custom' means you can assign and remove user permissions and 'None' means no permissions have been assigned.
- new 'Expiry' – lists the authorisation expiry date of authorised users in RAM (not available to AUSkey users).
- the 'last access date' field is temporarily unavailable.

In the **Modify access and permissions** screen, registered tax and BAS agents can use 'Assign RANs' to provide user access to their registered agent numbers (RANs).

See also:

- Relationship Authorisation Manager (/General/Gen/Relationship-Authorisation-Manager/)
- myGovID (/General/Gen/myGovID/)

Next steps:

- As a user of Access Manager, you should familiarise yourself with the Responsibilities for using Access Manager.

Access and permissions

- https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=2 (https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=2)

- Last modified: 25 Oct 2019
- QC 40983

Assigning and managing permissions for staff is one of the main functions of Access Manager. It enables businesses to manage which ATO online services and functions their employees can access.

If you're using Relationship Authorisation Manager (RAM), see Access Manager via RAM for more information.

Administrators

Administrators (Administrator AUSkey holders or connected myGov users with Administrator access) have unrestricted access to ATO online services such as the portals. Called Access Administrators, they also have the ability to set Standard user permissions in Access Manager.

Once you assign permissions to Standard users, anything they do within ATO online services is legally binding to your business.

Standard users

Standard users (Standard AUSkey holders or connected myGov users with Standard access) have a very limited access to ATO online services by default. To gain authorisation to access more services, they must be assigned specific permissions in Access Manager by an Administrator or an Access Administrator. Standard users cannot login to Access Manager unless they are made an Access Administrator.

New Standard users must login for the first time to a portal before an Administrator can see their account in Access Manager.

Device AUSkeys

Device AUSkeys are used for computer to computer transactions, through the SBR channel. Although Device AUSkeys have a human custodian (an Administrator or Standard AUSkey holder) they require their own set of permissions to transact on behalf of a business, assigned by an Access Administrator.

An initial transaction with a new Device AUSkey, through the SBR channel, must be performed before an Administrator can see the account in Access Manager.

Access Administrators

Standard users who can manage the permissions of other Standard users and perform other functions in Access Manager are called Access Administrators. Only a 'full' Administrator can authorise a Standard user to become an Access Administrator.

An Access Administrator can login to Access Manager to modify the access and permissions for other Standard users in the business.

A Standard user who is an Access Administrator cannot appoint other users as Access Administrators or modify their own access.

Permissions

Access Manager permissions for ATO and ABR online services (/general/online-services/in-detail/using-access-manager/access-manager-permissions-for-ato-and-abr-online-services/) provides a full list of permissions and which online service they provide access to.

Assign access and permissions

For Administrators to assign permissions to their current Standard users:

- Log in to Access Manager.
- Select **Access and permissions** from the left hand menu.
- Select the user in the table. If the user isn't listed, they need to log in to our online service (such as the portal). This creates a profile and the user will display in the table.
- Select the relevant permissions. The **Select all** and **Clear all** buttons above the list can be used to select or clear all permissions for the user.
- Select **Save**.

Copy permissions

To copy the permissions for one user to another:

- Select **Access and permissions** from the left hand menu.
- Select **Copy permissions** from the blue menu bar.
- Select the user that you want to copy the permissions from the drop down list.
- Select the user that you want to copy the permissions to. You can select one user or multiple users.
- Select **Save**.

Manage access administrators

To manage access:

- Select **Access and permissions** from the left hand menu.

- Select the user in the table.
- To modify access
  - Access Administrator: To add or remove access for an Access administrator, select the **No** or **Yes** radio button. If **Yes** is selected, the user will have the authority to log in to Access Manager and update permissions for other standard users.
  - Select **Save**.

Disabling users

To disable access:

- Account status: To change the status of the account, select the **Active** or **Disabled** radio button. If **Disabled** is selected, the user will not be able to log in to Access Manager or any ATO online services such as the portals. A disabled account can be reactivated by selecting the **Active** radio button.
- Select **Save**.

Removing users

- Select **Access and permissions** from the left hand menu.
- Select the user in the table. Select **Remove account**. If removed, the user will not be able to log in to Access Manager or any ATO online services such as the portals. A removed account does not cancel the user's AUSkey. A removed account can be restored and made active.
- Select **Confirm**.

Restoring users

- To restore user
  - Select **Access and permissions** from the left hand menu.
  - Select **Past credential holders history** from the blue menu bar.
  - Select **Restore** for the relevant user.
  - Select **Confirm**.
  - Select the restored user in the table on the Access and permissions page.
  - Select **Active** against the Account status.
  - Select **Save**.

- To view information about when a user was removed or restored
  - Select **Access and permissions** from the left hand menu.
  - Select **Past credential holders history** from the blue menu bar.
  - Select the user.

  - Select **Close**.

Business appointments

- https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=3 (https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=3)
- Last modified: 25 Oct 2019
- QC 40983

If you're using Relationship Authorisation Manager (RAM), see Access Manager via RAM for more information.

Who has access to my business – explained

This function, available under **Business Appointments** from the left hand menu in Access Manager enables you, as the principal business, to appoint another business to be your agent for tax purposes.

Permissions – When you create an appointment, you select specific permissions to authorise the services the agent may access on your behalf.

Managing appointments – Existing business appointments can be viewed, modified (permissions changed), or removed.

Note: Permissions for users in the appointed business are managed by Access Administrators in the business, based on the permissions you granted. All Administrators in the appointed business have automatic access to the permissions you granted their business.

Whose business I can access – explained

This function is for businesses who are appointed as agents, to act on behalf of the principal businesses that gave them access.

An appointed business can:

- view businesses they can act on behalf of
- view permissions a business has granted them

- authorise their own users or Device AUSkeys to an appointment and grant them permissions.

Agent permissions – The agent can assign permissions to users in its own business, to access a principal business. Only permissions authorised by the principal can be assigned to the users in an appointed business.

The auto access function allows Administrators in the appointed business to add and remove permissions for their Standard users. Credential holders with auto access:

- get access to future business appointments given to the business
- get authorisation to all permissions made available by each business appointment.

Permissions can be manually assigned for users requiring specific permissions.

Note: The **Whose business I can access** function is available under **Business Appointments** from the left hand menu in Access Manager.

Appointing an agent for tax purposes

An **agent for tax purposes** is an entity that you appoint to act on your behalf in the Business Portal. Transactions completed on your behalf by such an entity are legally binding, as if you had done them yourself.

An agent in this context is not the same as a registered tax agent or BAS agent. This agency relationship is separate to, and in addition to, any relationship you may have with a registered tax or BAS agent.

Your agent for tax purposes can view and work with your tax information in the portal. Before you allow your agent access to your information, make sure you fully understand the nature of a business to agent relationship.

Example – appointing an agent for tax purposes

You own:

- Company No. 1 Pty Ltd – operates a retail trading business that is also responsible for the tax and accounting affairs of all your other businesses.
- Company No. 2 Pty Ltd – invests in shares and rental properties.
- Company No. 3 Pty Ltd – operates a franchise business.

Each entity has an Australian business number (ABN). As the owner, you have an Administrator AUSkey for each entity.

Company No. 2 and Company No. 3 may want to appoint Company No. 1 as their agent for tax purposes. This would allow Company No. 1 to act on behalf of the other two companies for the purpose of viewing and working with their tax information in the portal.

This appointment would give you, as an authorised officer of Company No. 1, the ability to browse or undertake transactions for all three companies within the same portal session rather than logging in and out of the portal using three different security credentials.

It's important to note that the agent for tax purposes has the authority to act in the capacity of the business that appointed them. This means anything done by your agent for tax purposes will be assumed to have been done by your business. Your business will be legally liable for anything done by the agent on its behalf.

In this example, Company No. 2 and Company No. 3 will be bound by the action of Company No. 1 acting on their behalf.

Requirements to be an agent for tax purposes

For your agent for tax purposes to act on your behalf and delegate permissions to their own staff, they must:

- have a valid Australian business number (ABN)
- have valid AUSkeys for their users for this ABN
- use the Business Portal
- agree to be your agent for tax purposes.

Note: Do **not** create a business appointment for your registered tax practitioner (tax agent or BAS agent). Registered tax practitioners have access to their own online services (Tax Agent and BAS Agent portals) where they can access your records if you are their client.

Limiting the agent's access to your business information

When you create an appointment for an entity to act on your behalf using Access Manager, you can limit their level of access by using the permissions in the appointment. Only give them permissions for the services you want them to access. Administrators in the appointed entity have automatic access to the permissions you granted them. The appointed entity can further limit this set of permissions to users in their business requiring access.

We recommend that you develop agreed processes with businesses that you appoint as an agent for tax purposes so you can understand and be informed about:

- who you are granting access to (that is, who the Administrator AUSkey holders are)
- which Standard AUSkey holders they may grant access to, and the period of time for which they will have access.

All activities undertaken on your behalf by staff in the appointed entity are legally binding to your business.

Manage permissions

Appoint a business and assign permissions

The appointment is done by the principal business that is appointing another entity to act on their behalf.

To appoint a business:

- Select **Who has access to my business** from the left hand menu.
- Select **Appoint new business** from the blue menu bar.
- Enter the ABN for the business you want to appoint.
- Select **Continue**.
- Select the relevant permissions. The **Select all** and **Clear all** buttons above the list can be used to select and clear all permissions for the user.
- Select **Save**.

Administrators in the appointed business will automatically be given the permissions that you have assigned to their business.

Modify permissions for an appointed business

To modify the permissions for an appointed business:

- Select **Who has access to my business** from the left hand menu.
- Select the appointed business from the list.
- Select or unselect the permissions. The **Select all** and **Clear all** buttons above the list can be used to select and clear all permissions.
- Select **Save**.

Remove appointed business

To remove an appointed business (steps for principal business):

- Select **Who has access to my business** from the left hand menu.
- Select the appointed business from the list.
- Select **Remove Business Appointment**.
- Select **Confirm**.

An appointed business can also remove a business appointment. For example, where the appointed business no longer wants to act on behalf of the principal business, or where changes in the principle business mean that there is no person authorised to remove the appointed business in Access Manager.

To remove an appointed business (steps for appointed business):

- Select **Whose business I can access** from the left hand menu.
- Select the business to remove from the list.
- Select **Remove Business Appointment**.
- Select **Confirm**.

Assign access to credential holders for a principal business

Although Administrators in the appointed entity have automatic access to the permissions granted by the principal business, they will need to give access to any other users in their business requiring access.

Permissions that have been granted by the principal (appointing) business are displayed as read-only and cannot be changed.

Auto access feature

Permissions for Standard users and Device credentials can be updated either in bulk using the auto access feature (this gives the user all of the permissions assigned by the principal business) or by allocating each permission individually.

To add permissions in bulk for a Standard user:

- Select **Whose business I can access** from the left hand menu.
- Select **My credential holders with auto access**. This will list credential holders and allow the administrator to give the user auto access if they don’t already have it.
- Select **Give auto access** in the manage access column.

To add individual permissions for a Standard user:

- Select **Whose business I can access** from the left hand menu.
- Select the relevant business.
- Select **View authorised credential holders** from the blue menu bar.
- Select **Authorise new credential holder** from the blue menu bar.
- Select a credential holder from the list.
- Select the relevant permissions. Only permissions allocated to the appointed business are displayed. The **Select all** and **Clear all** buttons above the list can be used to select and clear all permissions for the user.

- Select **Save**.

Modify access to credential holders for a principal business

To manually select specific permissions for a credential holder, where auto access has been set, their auto access needs to be removed first and the specific permissions need to be assigned.

To remove auto access:

- Select **Whose business I can access** from the left hand menu.
- Select **My credential holders with auto access**.
- Select **Remove auto access**.

Next step:

- Once auto access has been removed, follow the steps to Assign access to credential holders for a principal business.

If auto access hasn't been set for the credential holder:

- Select **Whose business I can access** from the left hand menu.
- Select the relevant business.
- Select **View authorised credential holders** from the blue menu bar.
- Select a credential holder from the authorised credential holders list.
- Modify the permissions by selecting or un-selecting the checkboxes. Only permissions allocated to the appointed business are displayed. The 'select all' and 'clear all' buttons above the list can be used to select and clear all permissions for the user.
- Select **Save**.

Remove access to credential holders for a principal business

If auto access has been set for the credential holder:

- Select **Whose business I can access** from the left hand menu.
- Select **My credential holders with auto access**.
- Select **Remove auto access**.

If auto access hasn't been set for the credential holder:

- Select **Whose business I can access** from the left hand menu.
- Select the relevant business.
- Select **View authorised credential holders** from the blue menu bar.
- Select a credential holder from the list.
- Select **Remove Authorisation**.

- Select **Confirm**.

Tax and BAS agents

- https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=4 (https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=4)
- Last modified: 25 Oct 2019
- QC 40983

Authorising users to registered agent numbers

To give your staff access to the clients of your registered agent number, you need to authorise their AUSkey in Access Manager and give them the necessary permissions. If you have more than one registered agent number, you can assign a user with multiple agent numbers.

Access manager is now connected with Relationship Authorisation Manager (RAM). As a result, you may notice some different fields and terminology in Access Manager. Refer to AUSkey replacement (/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=1#AUSkey_replacement) for more information.

Assigning a registered agent number

To assign a registered agent number to your users:

- Select **Access and permissions** from the left hand menu.
- Select the user.
- Select **Assign RANs** on the 'modify access and permission' screen.
- Select the agent number you are giving access to (option to select all current and future RANs is available) on the 'tax practitioner access' screen.
- Select **Save** to return to the 'modify access and permissions' screen and select permissions in the **My Clients** tab.

Assigning user permissions to access your clients

When you have assigned a registered agent number to a user, you then need to setup the permissions they need to access your clients.

To assign permissions:

- Select **Access and permissions** from the left hand menu.
- Select the user's name from the main list.
- Under **Permissions** select the **Client tab**.
- Select the relevant permissions.
- Select **Save**.

Watch:

Media: Access Manager - desktop users
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiubz353p7 (http://tv.ato.gov.au/ato-tv/media?v=bd1bdiubz353p7) (**Duration:** 02:13)

Restricted clients (for registered agents)

As a registered agent you may restrict client accounts deemed to be sensitive or private, such as your own accounts. You may not want some or all of your staff with Standard AUSkeys to have access to these client accounts in the Tax Agent or BAS Agent Portals.

When you restrict a client, Access Administrators (by default) are the only users who will have access to that client's information. You can then specify which standard users will have access to that client in the Tax Agent or BAS Agent Portals.

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

To give permissions for Standard user to restricted clients:

- Select **Access and permissions** from the left hand menu.
- Select the user's name from the main list.
- Under **Permissions** select the **Client tab**.
- Select **Access to all restricted clients** permission.
- Select **Save**.

Notify us of a hosted SBR software service (previously Nominate online software provider)

- https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=5 (https://www.ato.gov.au/General/Online-

services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=5)
- Last modified: 25 Oct 2019
- QC 40983

If you have purchased or subscribed to hosted (cloud) SBR-enabled software, you can notify us of your hosted SBR software service providers, whose services you are using for transactions to and from the ATO. Your software provider will advise you if the software you have purchased is eligible.

Create and maintain notifications to us of your hosted SBR software services

To notify us of your hosted SBR software services:

- use the **My hosted SBR software services** function in Access Manager. To use this function, you need to be either
  - the principal authority or authorisation administrator in Relationship Authorisation Manager (RAM) – a new authorisation service available for eligible businesses to use
  - an Administrator AUSkey holder
  - connected with myGov (Manage ABN Connections) and have administrator access.

- you can phone us on **1300 85 22 32**.

See also:

- Relationship Authorisation Manager (/general/gen/relationship-authorisation-manager/)

Before you begin you will need:

- the hosted SBR software service provider's ABN or their name.
- the Software ID to complete the notification (your software service provider will advise of these details when you purchase or subscribe to their service).

Note: As an Administrator you'll only need to notify us of your hosted SBR software service provider once. You also have the ability to remove or change your notification, or notify us of another hosted SBR software service provider at any time.

To notify us of your hosted SBR software services (previously *Nominate an online software provider*):

- Select **My hosted SBR software services** from the left hand menu.
- Select **Notify the ATO of your hosted service**.

- Search for a hosted SBR software service provider in the list, or search by entering the ABN or name.
- Select the **ABN link** of a hosted SBR software service provider.
- Enter the software ID provided to you by your software service provider and select **Next**.
- Read the **Notification** statement then select **Save**.
- A green success message will appear on the next screen to confirm your notification.

Note: The entered Software ID must match what was provided by your software service provider otherwise your transmissions using the software provider's hosted services will not be successful.

If required, you can notify us of additional software providers you have by repeating the above steps.

Watch:

Media: Access Manager - cloud users
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiubzw6pi3 (http://tv.ato.gov.au/ato-tv/media?v=bd1bdiubzw6pi3) (**Duration:** 01:56)

Removing a notification to us

To remove a notification to us for your hosted SBR software service:

- Select **My hosted SBR software services** from the left hand menu.
- Your current hosted SBR software service providers will be displayed.
- Select the **ABN link** of the software service provider to modify or remove the notification.
- Select **Remove notification**.
- Select **Save**.
- A green success message will appear on the next screen confirming the removal.

Note: This will remove both the software service provider notification and all Software IDs.

Adding or removing a Software ID

You can add additional Software IDs for other users in your business or remove a Software ID which is no longer used or is invalid. To do this:

- Select **My hosted SBR software services** from the left hand menu.
- Your current hosted SBR software service providers will be displayed.

- Select the **ABN link** of a hosted SBR software service provider to modify or remove the notification.
- Enter new or corrected Software IDs in the **Add Software IDs** fields.
- Remove unwanted Software IDs by selecting them under the **Remove** heading.
- Select **Next** to review your changes.
- Select **Save**.
- A green success message will appear on the next screen confirming the changes.

If you need help

If you are having difficulty completing or managing your notifications, phone us on **1300 85 22 32**.

Responsibilities for using Access Manager

- https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=6 (https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=6)
- Last modified: 25 Oct 2019
- QC 40983

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

Data about individuals and entities within Access Manager is confidential. You must ensure that unauthorised people do not compromise the integrity of that data. If your computer will be unattended, even briefly, you must log out from Access Manager or lock your computer.

By logging into Access Manager, you agree to:

- comply with the terms and conditions of the AUSkey
- keep the AUSkey secure at all times
- not disclose your password or share it with others.

By providing others in the business with electronic access to the secure information of the business, through an AUSkey, as yourself or as an agent for tax purposes, you must understand the following.

- **User access and permissions** – what level of access is provided to each type of user (Administrator, Standard, Device) and the transactions the users can undertake (see

Access and permissions).
- **Business appointments** – the nature of your relationship with any entities you have appointed as an agent for tax purposes and what transactions your agent can undertake (see Business appointments).
- **Legally binding actions** – the actions these users and agents undertake through Access Manager are legally binding to your business.

If you're using Relationship Authorisation Manager (RAM), see Access Manager via RAM for more information.

Preventing unauthorised access to business information

If you have allowed your staff access to your secure information on the Business Portal, Tax Agent Portal or BAS Agent Portal, we strongly recommend that you:

- use Access Manager regularly to ensure that user's level of access to the portals is appropriate
- cancel AUSkeys (in the AUSkey Manager) if staff no longer require them or the AUSkey has been compromised
- immediately disable or remove a user's account in Access Manager 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 security credential
- keep passwords secure – they must not be shared.

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

Access Manager via RAM

- https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=7 (https://www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/?page=7)
- Last modified: 25 Oct 2019
- QC 40983

Relationship Authorisation Manager (RAM) is connected to Access Manager. This means when you authorise a person to act for a business using RAM, you can set their permissions for ATO online services in Access Manager at the same time.

The 'Import AUSkey users' function in RAM is also available, allowing you to transfer permissions (as granted in Access Manager) of existing AUSkey users associated with your business.

To set permissions in Access Manager through RAM or use the 'Import AUSkey users' function you need to be the principal authority or authorisation administrator.

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

- comply with the terms and conditions of myGovID and RAM
- keep your myGovID secure at all times and not share it with others.

See also:

- Responsibilities for using Access Manager

Permissions

Assigning and managing permissions for staff is one of the main functions of Access Manager. It enables businesses to manage which ATO online services and functions their employees can access.

To transfer the permissions (as granted in Access Manager) of existing AUSkey users to RAM, see Import AUSkey users (https://info.authorisationmanager.gov.au/import-auskey-users/) .

To set permissions in Access Manager through RAM:

1. Select **Custom** in the 'Agency access' section when you add a new user. 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 government online services offer this option) in the 'Customise access' section.
4. Once in Access Manager, choose the relevant permissions from the access and permissions displayed and **save**.

To view or modify existing permissions:

- Select the user.
- Select **view** or **modify**.
- Select **ATO Access Manager.**
- Once in Access Manager, select **Access and Permissions** from the left hand menu.

To disable, remove or restore an authorised user, go to RAM.

If your access level is set as **Full**, you automatically have access to all ATO online services, however you may not be an authorisation administrator. Avoid copying permissions from a full access user as this may cause an error to occur.

Device AUSkeys are not managed in RAM, however principal authorities or authorisation administrators can manage permissions for Device AUSkeys in Access Manager.

Device AUSkeys will be replaced with new machine credentials in **March 2020**. You can create machine credentials in RAM which will allow you to interact with our online services through your business software.

See also:

- Authorisations (https://info.authorisationmanager.gov.au/authorisations/)
- Machine credentials (https://info.authorisationmanager.gov.au/machine-credentials/)

Business appointments

When using the 'Who has access to my business' function, available under **Business Appointments** in Access Manager, through RAM, note that users will appear as 'Standard' users.

We are working on adding the 'Auto access feature' when using Access Manager from RAM. This means you will be able to update permissions for custom access users in bulk, giving the user all of the permissions assigned by the principal business.

Authorising users to registered agent numbers

If you're a registered tax or BAS agent, to give your staff access to the clients of your registered agent number (RAN), you need to authorise them in Access Manager and give them the necessary permissions. A user will need **Custom** access level in Access Manager at minimum to enable you to give them access to your RAN.

If you have **Full** access level or you are a principal authority you will automatically have access to all RANs.

Assigning user permissions to access your clients

As a registered agent you may restrict client accounts deemed to be sensitive or private, such as your own accounts. You may not want some or all of your staff with **Custom** access level users to have access to these client accounts in Online services for agents or the Tax or BAS Agent Portal.

When you restrict a client, only principal authorities and **Full** access level users (by default) will have access to that client's information. You can then specify which standard or **Custom** access users will have access to that client in Online services for agents or the Tax or BAS Agent Portal.

See also:

- Relationship Authorisation Manager (https://info.authorisationmanager.gov.au/)

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.

Copyright notice