Online services

- https://www.ato.gov.au/General/Online-services/
- Last modified: 05 Dec 2022
- QC 40868

Register with our online services to access a secure range of tax and super services in one place.

ATO online services and myGov
How to create a myGov account, link to the ATO and use our online services.

Foreign investors
How to manage your registrations and obligations for investments in Australia.

Accessing online services with myGovID and RAM
How to access online services on behalf of a business or entity.

Businesses
Access Online services for business and Standard Business Reporting (SBR)-enabled software.

Not-for-profits
Find out about managing your reporting and transactions as an NFP organisation

Tax agents
How to access Online services for agents, practitioner lodgment service (PLS), Standard Business Reporting (SBR) and ABR.

BAS agents
How to access Online services as a BAS agent, practitioner lodgment service (PLS), Standard Business Reporting (SBR).

ATO app
Find out how to download the ATO app and use it to manage your tax and super on the go.

Access Manager
Manage access and permissions for ATO online services on behalf of your business.

ATO digital wholesale services

Find out about the digital wholesale services we offer digital service providers.

[AUSid](#)
How to set up AUSid to access Online services for non-residents.

[Identity security and scams](#)
How to verify a scam and protect your personal information.

[Online security](#)
How to stay safe online and how we protect you and your information.

[Technical support](#)
Get help and support for common errors and known issues with online services.

[System maintenance](#)
Find out when your online services will be unavailable in part or full for maintenance.

[Voice authentication](#)
Find out how to set up your voiceprint to confirm your identity and its benefits.

Authorised by the Australian Government, Canberra.

ATO online services and myGov

- https://www.ato.gov.au/General/Online-services/ATO-online-services-and-myGov/
- Last modified: 03 Sep 2022
- QC 70312

How to create a myGov account, link to the ATO and use our online services.

[Create a myGov account and link it to the ATO](#)
How to create a myGov account and link to the ATO as an individual or sole trader.

[When you can't sign in to your myGov account](#)
How to access your myGov account if you can't sign in.

[Using ATO online services](#)
How individuals and sole traders can use ATO online services to manage their tax and super in one place.

[ATO and myGov communications](#)
Find out how we use myGov to communicate with you, including through your myGov Inbox.

[ATO access to myGov – terms and conditions and privacy](#)
Find out your rights and responsibilities when using your myGov account to access ATO online services or the ATO app.

Create a myGov account and link it to the ATO

- https://www.ato.gov.au/General/Online-services/ATO-online-services-and-myGov/Create-a-myGov-account-and-link-it-to-the-ATO/
- Last modified: 08 Dec 2022
- QC 63135

How to create a myGov account and link to the ATO as an individual or sole trader.

On this page

- [Create a myGov account](#)
- [Link your myGov account to the ATO](#)
- [myGov sign in options](#)
- [Sign out – don't unlink](#)
- [Troubleshooting linking issues](#)

Create a myGov account

A myGov account lets you link to and access a range of government services online in one place.

When you create a myGov account, use:

- an email address that only you have access to - don't use a shared email.
- an Australian mobile number to receive SMS security codes to sign in.

If you don't provide an Australian mobile number, you'll need to update your [myGov sign in option](#). You can't use Answer a secret question as your sign in option when linking to or accessing our online services.

For instructions, see our Easy Read [How to create a myGov account and link to your tax and super](#).

You can also create an account by selecting Continue with Digital identity, if you have set up the myGovID app to a Standard identity strength.

Create a myGov account

If you already have a myGov account but you can't sign in, go to [when you can't sign in to your myGov account](#).

Link your myGov account to the ATO

Media: Link your myGov account to the ATO
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiubfo8e4m⬈ (Duration: 02:55)

Before you start trying to link:

- get the [information you will need to link to us on myGov](#)
- check you're not using Answer a secret question as your [myGov sign in option](#).

To link to us:

1. Sign in to your myGov account.
2. Select View and link services on the myGov home page.
3. Under Link a service heading, select Link next to Australian Taxation Office.
4. Select I agree to the terms and conditions of use.
5. Enter or confirm your personal details.
6. Answer [2 questions about your tax record](#).
7. Select I agree to verifying and linking my record.

If you don't have the required information to link, you'll need to [phone us](#) to get a unique linking code. We will need to [ask you questions to prove who you are](#). This is to protect the privacy of your account.

myGov sign in options

To link your myGov account to us you must use one of these 3 sign in options:

- [myGovID app](#)⬈ – set up to a Standard identity strength.
- SMS security codes – using an Australian mobile number.
- [myGov Code Generator app](#)⬈ .

Use the myGovID app or myGov Code Generator app, if you:

- don't have an Australian mobile number
- are overseas
- have poor mobile reception.

Once you link, you can then use the [ATO app](#) or the [myGov app](#)⬈ to securely access ATO online services.

Check or change your sign in option

Check and update how you sign in to myGov following these steps:

1. Sign in to your [myGov account](#)⬈
2. Go to My account.
3. Select Account settings.

4. Select Sign in options.
5. To update your sign in, follow the prompts.

When changing your sign in option, you can also enable an additional sign in option as a backup. If you connect your myGovID app, it can automatically be used in addition to your existing sign in option.

If you change your sign in option to Answer a secret question, your myGov account will be unlinked from the ATO as this is a less secure sign-in option.

Sign out – don't unlink

When you finish using ATO online services, return to myGov and sign out. You don't need to unlink.

If you unlink, you won't see our messages in your myGov Inbox or have access to ATO online services. To access our online services again, relink ATO to your myGov account.

Troubleshooting linking issues

If you have trouble linking to us, check:

- your systems meet the minimum system requirements
- help and support for our online services (including error codes)
- if the system is impacted by our system maintenance.

Information you need to link myGov to the ATO

- https://www.ato.gov.au/General/Online-services/ATO-online-services-and-myGov/Create-a-myGov-account-and-link-it-to-the-ATO/Information-you-need-to-link-myGov-to-the-ATO/
- Last modified: 03 Sep 2022
- QC 65312

Find out what information you need to link your myGov account to ATO online services.

On this page

- Linking to ATO online services
- Bank account details
- PAYG payment summary
- Centrelink payment summary
- Notice of assessment
- Super account details

- [Dividend statement](#)
- [Troubleshooting errors and issues](#)

Linking to ATO online services

To link your myGov account to us, you need to answer 2 questions about information in your tax record. This content explains what information you need and where to find it.

Bank account details

Use either a bank account:

- where you receive your income tax refund
- that has earned interest in the last 2 years.

You'll need the bank account:

- BSB number (no spaces or symbols)
- account number (no spaces).

You can usually find this information by logging in to your bank's mobile app, web account or on your bank statement.

If you've lodged your tax return using a tax agent, it may be their bank account details on your ATO record.

If you're unable to provide bank account details, select a different question.

PAYG payment summary

Use a PAYG payment summary issued in the last 2 years.

You'll need your gross income in whole dollars. Don't use cents, spaces, '$' or symbols.

If you don't have a copy of your summary or don't know your gross income, select a different question.

Centrelink payment summary

Use a Centrelink payment summary issued in the last 2 years.

You'll need your taxable income in whole dollars. Don't use cents, spaces, '$' or symbols. If your taxable income is zero, you can't use this question.

You can find these details on the annual statement that Centrelink provides you.

If your myGov account has a link to Centrelink, you can sign in and get the details online.

If you don't have a copy or don't know your taxable income, select a different

question.

Notice of assessment

Use a notice of assessment (NOA) issued in the last 5 years.

You will need:

- the date of issue – enter the date in the format 'dd/mm/yyyy'
- Our reference number – no spaces.

You can find these details in the top right-hand corner of your NOA.

If you don't have a copy, select a different question.

Super account details

Use a super account statement from the last 5 years.

You will need your:

- member account number (up to 16 characters)
- super fund's Australian business number (ABN).

You can also find these details on:

- an email or letter from your fund
- a membership card.

If the super fund's ABN is not on one of these items or more than one ABN is included, you can look them up at Super Fund Lookup.

If no money has been contributed to your super account in the last 12 months, your account may be inactive. Use another super account or select a different question.

Dividend statement

Use a dividend statement from the last 2 years.

You need your investment reference number. Include all numbers with no spaces.

If you don't have a dividend statement, you may find these details on an email or letter from your investment body. If you don't have this information, select a different question.

Troubleshooting errors and issues

If you receive an error message or experience an issue when entering the above information, see our help and support for online services.

When you can't sign in to your myGov account

- https://www.ato.gov.au/General/Online-services/ATO-online-services-and-myGov/When-you-can-t-sign-in-to-your-myGov-account/
- Last modified: 03 Sep 2022
- QC 63819

How to access your myGov account if you can't sign in.

On this page

- Sign in issues
- Recover your account using myGovID
- Create a new myGov account and relink to the ATO

Sign in issues

You may not be able to sign in to your myGov account because you:

- changed your mobile phone number
- went overseas and no longer have access to your Australian mobile number
- deleted the myGov Code Generator app
- can't answer your secret question
- forgot your password.

If you forget your password, reset it by selecting Forgot password on the myGov sign in page.

When you can't sign in to your myGov account, you can either:

- recover your account using myGovID
- create a new myGov account and relink to the ATO – you must use this option if you used the myGov Code Generator app to sign in.

Recover your account using myGovID

If you used SMS security codes or Answer a secret question as your sign in option, you can use myGovID to recover your account.

To recover your myGov account, download the myGovID app and set it up to a Strong identity strength .

Your name, date of birth and email address for your myGov account must match the details you use to set up your myGovID.

After you set up your myGovID, you can recover your account:

1. Go to the myGov sign in page.
2. Enter your username and password and select Sign in.
3. Select I didn't get my code or I can't answer my question.

4. Select Continue with Digital Identity.
5. Sign in with your myGovID.

In future, you can use your myGovID to sign in to myGov. To do this select Continue with Digital Identity on the myGov sign in page and follow the prompts.

If you have SMS codes enabled, you can continue to receive these by updating your contact details in myGov with your new mobile phone number. This can be done in Account settings.

Create a new myGov account and relink to the ATO

If you can't recover your account using myGovID, you need to create a new myGov account and relink to the ATO.

You can choose to use a different email address when creating your new account. If you want to use the same email address, myGov help desk must release it.

Contact the myGov help desk:

- In Australia. phone 13 23 07 and select option 1
- Outside Australia, phone +61 1300 169 468.

Avoid losing access

To avoid losing access to your new myGov account, we recommend you use either the myGovID app or myGov Code Generator app if you:

- don't have an Australian mobile number
- are going overseas and won't have access to your Australian mobile number
- have limited mobile reception.

You can also enable a back-up sign in option:

1. In myGov, go to My account.
2. Select Account settings.
3. Select Sign in options and follow the prompts.

If you connect your myGovID, you'll automatically be able to use it with your existing sign in option.

Using ATO online services

- https://www.ato.gov.au/General/Online-services/ATO-online-services-and-myGov/Using-ATO-online-services/
- Last modified: 12 Oct 2022
- QC 40974

How individuals and sole traders can use ATO online services to manage their tax and super in one place.

On this page

- Before you start
- Manage your personal and tax details
- View your tax information
- Lodge and pay your tax
- Manage your other lodgments as a sole trader
- View, manage and access your super

Before you start

To access our online services, you must create a myGov account and link it to the ATO.

Before you link to us, you can test the available functions and features in our online services using our ATO online services simulator.

Manage your personal and tax details

Use ATO online services to manage your personal and employment details. Find out how to:

- update your TFN details
- maintain your credit or debit card details

You can use ATO online services to access and complete commencement forms and services, such as:

- Tax file number declaration
- Superannuation standard choice
- Withholding declaration
- Medicare levy variation declaration

View your tax information

Use ATO online services to view your:

- Tax file number (TFN)
- Australian business number (ABN)
- Communication history
- Debt on hold
- Payment plan status or request a payment plan
- Additional tax information

Tax file number (TFN)

To view or find your TFN:

1. Go to My profile.

2. Select Personal details.

Australian business number (ABN)

To view or find your ABN if you're a sole trader:

1. Go to My profile.
2. Select Personal details.

Communication history

To view or find most past communications about your tax information:

1. Go to My profile.
2. Select Communication.
3. Select History.

Debt on hold

To view a debt on hold:

1. Go to Tax.
2. Select Accounts.
3. Select Tax accounts.
4. Select the account you want to view.
5. Select Filter.
6. Update the from' date to 01/01/2000, then select Filter button.
7. Search for the transactions, non-pursuit, re-raise of non-pursuit, partial re-raise of non-pursuit, and 'cancellation of non-pursuit' – the net amount of the debit minus the credit is the remaining balance of the debt on hold.

You can download a copy of the transactions by selecting Download – you will need to choose the download format CSV or HTML.

Payment plan status or request a payment plan

You may be eligible to set up, adjust or cancel an existing payment plan. You can set up a payment plan online if you owe $100,000 or less.

To check the status or set up a payment plan:

1. Go to Tax.
2. Select Payments.
3. Select Payment plans.

Additional tax information

You can also use ATO online services to:

- access your income statement
- view your notice of assessment
- view third-party data we hold on your securities (share and unit) records

- [view your study or training support loan account online](#)
- [review and print copies of individual tax documents](#) such as a notice of assessment, income statement or lodge income tax return
- receive notifications and communications from us in your [myGov Inbox](#)

Lodge and pay your tax

Find out more about how to lodge and pay your tax using ATO online services:

- [Lodge your tax return online with myTax](#)
- [Check the progress and status of your return](#)
- [Correct (amend) your income tax return](#)
- [Lodge a non-lodgment advice](#)
- [Lodge, pay, vary or manage your PAYG instalments online](#)
- [Lodge your claim for a refund of franking credits](#)

Manage your other lodgments as a sole trader

Use ATO online services to manage your other lodgments:

- [Add, update or cancel tax registrations](#)
- [Lodge super guarantee charge statement](#)
- [Single touch payroll (STP) deferral or exemptions](#)
- [Request a transfer or refund](#)
- [Lodge a private ruling or objection application](#)
- [Send or access secure mail](#)
- [Information about managing your lodgments](#)

Add, update or cancel tax registrations

To add, update or cancel a tax registration:

1. Select Tax.
2. Select Manage.
3. Select Tax registrations.

Add a tax registration

To add a tax registration:

1. Select Current registrations.
2. Select Add.
3. Go to the Select registration drop-down menu and choose from the list
   - Goods and services tax (GST)
   - Income tax withholding (ITW – also known as PAYG withholding or PAYGW)
   - Luxury car tax (LCT)
   - Wine equalisation tax (WET)
   - Fuel tax credits (FTC).
4. Complete the registration details in the form.

Update a tax registration

To update a tax registration:

1. Select Update next to the tax registration.
2. Complete the mandatory fields.

Cancel a tax registration

To cancel a tax registration:

1. Select Cancel next to the tax registration.
2. Type the date the cancellation takes effect.
3. Select the reason for cancellation.

Lodge super guarantee charge statement

To lodge a super guarantee charge statement:

1. Select Tax.
2. Select Lodgments.
3. Select Reports and forms.
4. Select Super guarantee charge statement.

Single touch payroll (STP) deferral or exemptions

To apply for a Single Touch Payroll deferral or exemption:

1. Select Employment.
2. Select Manage employees.
3. Select STP deferrals and exemptions.

Request a transfer or refund

To request a transfer between your accounts, or a refund:

1. Select Tax.
2. Select Accounts.
3. Select Transfer request or Refund request.

Lodge a private ruling or objection application

To lodge an application for a private ruling or objection:

1. Select Tax.
2. Select Lodgments.
3. Select Reports and forms.
4. Then select either
   - Private ruling application
   - Lodge an objection
   - Submit further information for lodged private ruling or objection.

Send or access secure mail

To send or access secure mail:

1. Select My profile.
2. Select Communication.
3. Select Secure mail.

Information about managing your lodgments

For more information about managing your lodgments, see:

- Lodging and paying PAYG instalments
- How to vary your PAYG instalments
- Lodging your activity statement online
- Revising an earlier activity statement
- Lodge and amend taxable payments annual report (TPAR)
- Stapled super funds for employers

View, manage and access your super

For information about how to view, manage and access your super using ATO online services, see:

- Early access to your super
- Keeping track of your super
- YourSuper comparison tool
- Viewing your super accounts
- Searching for lost super.
- Small Business Superannuation Clearing House
- Making an election to release money from super
- First home super saver scheme (FHSS)

ATO and myGov communications

- https://www.ato.gov.au/General/Online-services/ATO-online-services-and-myGov/ATO-and-myGov-communications/
- Last modified: 03 Sep 2022
- QC 46113

Find out how we use myGov to communicate with you, including through your myGov Inbox.

On this page

- About myGov communications
- Using your myGov Inbox
- Support

About myGov communications

If you have a myGov account linked to us, we'll send you messages and reminders through your myGov Inbox or ATO online services.

You may receive general communications, like promotional information, through [SMS or email](#).

Due to legal and privacy requirements, personal information like your tax file number (TFN) can't be emailed to you.

To receive your ATO mail through the post, phone us on 13 28 61.

myGov sign in homepage

When signed in, you may receive notifications for 'Payments and Claims' from other government agencies. We won't communicate with you through this feature.

Communication preferences

You can set or change your [communication preferences](#).

If you use a tax or BAS agent, you and your agent can view most correspondence sent to you or your agent on your behalf.

If you don't have a myGov account linked to us, you'll receive your ATO mail through the post or it will be sent to your tax or BAS agent.

Using your myGov Inbox

Information about ATO messages to your myGov Inbox:

- [New message notifications](#)
- [Messages in your myGov Inbox](#)
- [If you unlink the ATO from your myGov account](#)

New message notifications

You'll get an email, SMS or push notification from myGov when there's a new message from us in your myGov Inbox. The default setting for new message notifications is email.

You need to sign in to your myGov account to view the message. We'll never email or SMS you a link to sign in to an online service.

Change your myGov Inbox notifications

To change how your message notifications are sent:

1. Sign in to your myGov account.
2. Select My account.
3. Select Account Settings.

4. Select Contact details.
5. Edit your myGov notifications.

Messages in your myGov Inbox

Messages from us may include:

- notices such as notices of assessment
- statements of account
- confirmation and reminder notices
- activity statements or instalment notices.

Messages in your myGov Inbox may contain links to our online services.

You can save or print the messages and included PDF documents for your records.

You can't reply to messages we send through your myGov Inbox.

If you unlink the ATO from your myGov account

If you unlink us from your myGov account, you won't be able to access our messages in your myGov Inbox. We recommend saving or printing these records before you unlink.

To receive messages to your myGov inbox, relink the ATO to your myGov account.

Support

You can find support for:

- myGov Inbox
- Messages from the ATO
- Accessibility

myGov Inbox

For help with your myGov Inbox:

- visit the myGov website
- phone the myGov help desk on 13 23 07.

Messages from the ATO

For questions about an ATO message you've received, contact us.

If you prefer to speak to us in a language other than English, phone us using the Translating and Interpreting Service on 13 14 50.

If you have difficulty hearing or speaking to people over the phone, contact us through the National Relay Service (NRS).

Accessibility

If you're vision impaired or use adaptive technology, you may not be able to access PDF documents sent through myGov. For assistance, contact us.

ATO access to myGov – terms and conditions and privacy

- https://www.ato.gov.au/General/Online-services/ATO-online-services-and-myGov/ATO-access-to-myGov---terms-and-conditions-and-privacy/
- Last modified: 03 Sep 2022
- QC 58332

Find out your rights and responsibilities when using your myGov account to access ATO online services or the ATO app.

On this page

- Terms and conditions of use
- Privacy notices

Terms and conditions of use

Our terms and conditions of use include:

- Acknowledgement
- Nomination for the purposes of managing your myGov account
- Confirming your identity
- Your myGov Inbox

Acknowledgement

I acknowledge that the nomination of Services Australia on behalf of the Commonwealth of Australia to receive and disclose my information for the purposes of managing my myGov account, does not limit the Commonwealth from performing duties or exercising powers under law.

Nomination for the purposes of managing my myGov account

The nomination of Services Australia will allow myGov to disclose your name, date of birth and your contact information to other federal government agencies that you have already linked to, or decide to link to. The disclosure of details will allow myGov to confirm your identity between these agencies and provide those agencies with notifications of changes of your details.

Confirming your identity

Your ability to link to and access online services for individuals and ATO

communications from your myGov inbox will depend on how you confirm your identity when signing into your myGov account.

If you link the ATO to your myGov account on or after 1 June 2019, you must confirm your identity by using myGov security codes or the myGov access app to access online services for individuals and ATO communications from your myGov inbox.

If you have linked the ATO to your myGov account before 1 June 2019 and confirm your identity by:

- using myGov security codes or the myGov access app, it will be mandatory from 1 June 2019 to use them to access online services for individuals and ATO communications from your myGov inbox. If you later change to secret questions and answers to confirm your identity, you will not be able to access online services for individuals and ATO communications from your myGov inbox and we will send your communications to your address we have on record
- using secret questions and answers, you can continue to access online services for individuals and ATO communications from your myGov inbox. To improve your online security, you should use myGov security codes or the myGov access app to confirm your identity.

myGov inbox

You have agreed and designated your myGov inbox as your address for Australian Taxation Office (ATO) communications that the ATO sends or makes available for you to access electronically.

The designation of your myGov account and inbox as your address is subject to your Tax or BAS agent (authorised on your behalf) designating, or having previously designated ATO Online services for agents as your address to send some or all of your ATO communications. Where this occurs, your myGov inbox will remain your address for the ATO to send or make available communications that are not sent or made available to your agent. Not all ATO communications can be sent or made available for access electronically. You can access a list of the communication types that the ATO may send or make available electronically on the ATO website. The ATO may update this list from time to time.

Where an ATO communication is unable to be sent or made available electronically, the ATO will send the communication to your address we have on record.

You will receive a welcome message from the ATO in your myGov inbox to confirm the service is enabled.

You will be able to access and view your communications that are sent to your agent in online services for individuals.

You may receive notifications from myGov alerting you that communications have been sent to your myGov inbox. This service is provided as a courtesy and does not limit your obligation to regularly access your myGov inbox to check for ATO

communications.

Privacy notices

Our privacy notices include:

- [Collecting your tax file number](#)
- [Privacy](#)
- [Information about your device](#)
- [Use of information](#)
- [Our privacy policy](#)

Collecting your tax file number

The ATO is authorised by the *Taxation Administration Act 1953* to request your tax file number (TFN). We will use your TFN to identify you when linking your myGov account to the ATO. It is not an offence not to provide your TFN. However, if you do not provide your TFN, you will not be able to link your myGov account to the ATO and access online services for individuals.

Privacy

The ATO is authorised by the *Taxation Administration Act 1953* to request personal information from you. We will use this information to confirm your identity when you link the ATO to your myGov account and use online services for individuals.

If we do not collect this information, you will not be able to link the ATO to your myGov account and access online services for individuals.

Where authorised by law to do so, we will give this information to Services Australia for the purposes of administering myGov.

The ATO also provides taxpayer information to treaty partners overseas under [international tax agreements](#) with many other countries.

Information about your device

Your browser and information you provide will be recorded for authentication purposes as part of the myGov linking process such as:

- your internet protocol address (IP address)
- the date and time of the use of the authentication service
- the authentication information you provided
- successful and unsuccessful attempts at authenticating.

Use of information

The ATO may use this information to:

- confirm your identity
- compile statistics and reports to enhance ATO systems and services

- identify and respond to issues that may indicate authentication integrity is at risk
- detect, investigate and prosecute criminal offences.

The ATO's privacy policy

Our privacy policy is available on our website. The policy contains important information about your privacy, including information about how you can access and seek correction of information we hold about you, how you may complain about a breach of the Australian Privacy Principles and how the ATO deals with privacy complaints.

Foreign investors

- https://www.ato.gov.au/General/Online-services/Foreign-investors/
- Last modified: 05 Dec 2022
- QC 71016

Managing your registrations and obligations for investments in Australia.

Online services for foreign investors
Work out how foreign investors can manage obligations relating to Australian investments using Online services.

Foreign investment in Australia
Find out how foreign investors can apply and register their investment with us.

Online services for foreign investors

- https://www.ato.gov.au/General/Online-services/Foreign-investors/Online-services-for-foreign-investors/
- Last modified: 05 Dec 2022
- QC 71017

Foreign investors will use Online services to manage their obligations relating to Australian investments.

On this page

- Online services will be available soon
- Using Online services for foreign investors

Online services will be available soon

The [foreign investment reforms](#) received Royal assent on 10 December 2020.

As part of these reforms, we expect to make Online services for foreign investors available from 26 June 2023, supporting a new Register of Foreign Ownership of Australian Assets ([the Register](#)) from 1 July 2023.

Online services for foreign investors will allow you as a foreign investor and your representatives to interact with us online, to:

- streamline your management of registration obligations and other transactions related to Australian investments
- provide better security of your information, by verifying your digital identity before you sign in
- store important information to use in future interactions with us so you don't have to provide that information again.
- make it easier to communicate with us.

Our current online forms relating to [foreign investment in Australia](#) obligations will be moved into Online services for foreign investors.

Using Online services for foreign investors

Online services for foreign investors will let you manage registration obligations and other transactions relating to Australian investments online.

You as a foreign investor and your representatives will be able to use Online services to:

- lodge foreign investment applications for residential land and pay associated fees
- manage your personal foreign investment details
- manage residential and non-residential asset registrations
- view the history of your residential and non-residential assets (from 1 January 2021)
- lodge vacancy fee returns and pay associated fees
- monitor your residential foreign investment application status
- review any asset registrations
- review your vacancy return lodgments
- review your payment history
- delegate authority to representatives to act on your behalf as an individual or for an entity.

We'll provide more details about the service in 2023, including how to get ready for the change.

For more information for foreign investors, see [foreign investment in Australia](#).

Accessing online services with myGovID and RAM

- https://www.ato.gov.au/General/Online-services/Accessing-online-services-with-myGovID-and-RAM/
- Last modified: 12 Dec 2022
- QC 58557

Set up myGovID and Relationship Authorisation Manager (RAM) to access our online services on behalf of a business.

On this page

- What is myGovID and RAM
- Our online services that require myGovID
- Set up your myGovID
- Link your myGovID to a business using RAM
- Business software user
- Support

What is myGovID and RAM

myGovID is the Australian Government's Digital Identity app. Download it to your smart device to prove who you are when logging in to a range of government online services. It is different to a myGov account.

RAM is an authorisation service that allows you to act on behalf of a business online when linked with your myGovID. You'll use your myGovID to log in to RAM.

Together, myGovID and RAM allow you to access our online services on behalf of a business or entity.

Media: How to get started with myGovID and RAM
https://tv.ato.gov.au/ato-tv/media?v=bd1bdiunw8unkp (Duration: 01:47)

Our online services that require myGovID

You need to use myGovID to log in to:

- Online services for business
- Online services for agents
- Online services for digital service providers
- Australian Business Registry Services (ABRS) online
- Access Manager
- Australian Business Register (ABR)
- ABR Explorer
- Departing Australia superannuation payment (DASP) online application

system.

View a list of all [government online services](#) you can access using myGovID.

Set up your myGovID

Your myGovID is unique to you and can't be shared. As it's your personal Digital Identity, you should set up your myGovID using a personal email address. It should not be a shared or work email address.

Set up your myGovID in 3 steps:

1. Download the myGovID app from the App Store or Google Play. The app is compatible with most smart devices.

   Only download the myGovID app from the official app stores listed above. Non-genuine versions of the myGovID app may be available from other sources.

2. Enter your details – open the myGovID app and follow the prompts to enter your full name, date of birth and personal email address.
3. Verify your identity – all of our online services can be accessed using a [myGovID](#) with a [Standard or Strong identity strength](#). If you have trouble verifying your identity documents or photo, refer to [Verifying your identity](#).

Unable to achieve a Standard identity strength

Business directors or associates

If there's no [principal authority](#) with at least a Standard myGovID who can link the business in RAM, you won't be able to use myGovID at this time.

Your business will need to use a different lodgment option like [Business software](#) or a registered tax agent.

Employees

If you can't achieve a Standard myGovID, you may be able to use a myGovID with a Basic identity strength to access some of our online services. You'll need to complete some extra steps.

For more information, refer to [Accessing our online services with a Basic myGovID](#).

Link your myGovID to a business using RAM

To access our online services on behalf of a business or entity, you need to link your myGovID to the business using RAM.

How you link depends on whether you're a:

- [Principal authority (including primary person)](#) – person responsible for a

business or entity
- [Authorised user or administrator](#) – someone who acts on behalf of a business or entity.

Before an authorised user or administrator can link their myGovID in RAM, the principal authority must link their Australian business number (ABN) in RAM first.

Principal authority (including primary person)

As the principal authority, you need to start the process by linking your ABN to your myGovID in RAM. This must be done before you or others can access government online services on behalf of the business.

If a principal authority or authorisation administrator is already acting on behalf of the business online, they can authorise you in RAM to act on behalf of the business.

The principal authority is either a:

- sole trader
- eligible individual associate listed on an ABN in the ABR such as a
  - trustee
  - director
  - partner

- primary person (no individuals listed as an associate in the ABR) such as a
  - director of a corporate trustee
  - authorised contact for a government agency
  - responsible person for an Australian charity.

To link the business in RAM as a [principal authority](#)☐, you need a Standard or Strong myGovID.

Once linked, you can access our online services on behalf of your business or entity and [set up authorisations](#)☐ for others to act on behalf of your entity.

Authorised user or administrator

To access our online services on behalf of a business or entity, a principal authority or authorisation administrator needs to authorise you in RAM.

Once you receive an authorisation request, use your myGovID to log in to RAM and [accept the authorisation](#)☐. You have 7 days to accept or decline the authorisation request before the code expires.

The principal authority is the person responsible for the business or a business associate – for example, a sole trader, trustee, director or public officer.

Authorisation administrators can [set up authorisations](#)☐ for others in RAM.

Business software user

If you use [Standard Business Reporting (SBR)-enabled software](#)⧉ to interact with our online services, you'll need a machine credential.

If you use cloud-based SBR-enabled software, your digital service provider will build the credential into your software.

If you use desktop or locally hosted software, you'll need to [create a machine credential](#)⧉ using RAM.

Support

- [Set up your access to Online services for business](#)
- [myGovID Help](#)⧉
- [RAM Help](#)⧉
- [myGovID – claiming deductions for phone and internet expenses](#) for a business
- [myGovID expenses](#) you can claim as an employee

Videos

- [Business experiences with myGovID and Relationship Authorisation Manager (RAM)](#)⧉

Trademarks and attributions

Android, Google Play and the Google Play logo are trademarks of Google LLC. Apple and the Apple logo are trademarks of Apple Inc., registered in the US and other countries and regions. App Store is a service mark of Apple Inc.

Accessing our online services with a Basic myGovID

- https://www.ato.gov.au/General/Online-services/Accessing-online-services-with-myGovID-and-RAM/Accessing-our-online-services-with-a-Basic-myGovID/
- Last modified: 09 Feb 2023
- QC 60964

Set up and use a Basic myGovID for restricted access to Online services for business or Online services for agents.

On this page

- [Restrictions when using a Basic myGovID](#)
- [Setting up Basic access to our online services](#)

Restrictions when using a Basic myGovID

For security purposes, some restrictions apply if you have a Basic myGovID.

These restrictions include what you can and can't do in Relationship Authorisation Manager (RAM), Online services for business and Online services for agents. These restrictions are related to activities that are higher risk.

For more information, see Basic myGovID restrictions.

Setting up Basic access to our online services

If you can't set up a myGovID with a Standard or Strong identity strength, you may be able to use a Basic myGovID to access Online services for business or Online services for agents.

These are the steps to access our online services with a Basic myGovID:

1. Set up your Basic myGovID.
2. Have an authorising representative authorise you in RAM.
3. Complete proof of identity requirements.
4. Have an 'authorising representative' set your permissions.

1. Set up your Basic myGovID

To set up your myGovID[⤢] with a Basic identity strength, download the myGovID app and add your legal name, personal email address and date of birth.

You can download the free myGovID app from the App Store or Google Play.

2. Have an authorising representative authorise you in RAM

An authorising representative has one of the following authorisation types in RAM:

- principal authority
- authorisation administrator
- government representative
- indirect associate
- responsible authority.

The authorising representative is usually the business owner or someone they've authorised to manage their business authorisations.

They need to create a new authorisation[⤢] for you in RAM. The name they use to create your authorisation needs to match the name in your myGovID app.

Once authorised, you will receive 2 emails:

- An authorisation request and code to accept in RAM – you should accept this in 7 days so that the code doesn't expire.
- A request to complete proof of identity requirements – make sure you've accepted the authorisation request before completing this step. You can find more information about the proof of identity requirements below.

3. Complete proof of identity requirements

The way you complete the proof of identity requirements depends on whether you:

- have an Australian TFN
- don't have an Australian TFN.

If you have an Australian TFN

Phone us to complete a proof of record ownership check and confirm your association with the business or entity. Have your TFN and Australian business number (ABN) details ready before you phone.

If you're phoning from:

- Australia – phone 1300 287 539 and select option 2 for myGovID enquiries
- overseas – phone +61 2 6216 1111 and ask to be transferred to myGovID enquiries between 8:00 am and 5:00 pm AEST, Monday to Friday.

All times are local time unless otherwise specified.

If you don't have an Australian TFN

Complete and send us the ATO use of Basic myGovID (NAT 75249, PDF, 182KB) form and attach copies of 2 certified identity documents. The name on these documents needs to match your name as displayed in the myGovID app. Refer to the form for a list of accepted documents.

Make sure that an authorising representative has authorised you as a Basic user in RAM and that you've accepted this authorisation before you submit the form.

Once we've received and checked your documents, you'll receive a confirmation email.

To find out about certifying your documents and language requirements, see Basic myGovID: proof of identity without a TFN.

4. Have an authorising representative set your permissions

Once you've accepted your authorisation and completed the proof of identity requirements, your authorising representative will receive an email with instructions to set your permissions in Access Manager. When this is complete, you can start using your myGovID.

Your authorisation is only valid up to 12 months at a time.

An authorising representative can renew your authorisation. You won't need to complete proof of identity requirements again if your authorising representative renews your authorisation before it expires. You and your authorising representative will receive email notifications before it expires.

Basic myGovID restrictions

- https://www.ato.gov.au/General/Online-services/Accessing-online-services-with-myGovID-and-RAM/Accessing-our-online-services-with-a-Basic-myGovID/Basic-myGovID-restrictions/
- Last modified: 01 Nov 2021
- QC 66706

If you're unable to achieve a Standard or Strong myGovID, you can use a Basic myGovID to access Online services for business and Online services for agents.

With a Basic myGovID, you cannot:

- be authorised as an authorisation administrator, machine credential administrator or authorised user in RAM
- use RAM to link a business, authorise others, manage authorisations or machine credentials
- access the Australian Business Register or Access Manager
- lodge a form that has a financial impact on the business
- complete activities that carry a higher risk within Online services for business or Online services for agents. You can check these restrictions below.

Online services for business restrictions

When using the Online services for business with a Basic myGovID you won't have access to the following common activities:

- view, add or update financial institution details
- view a statement of account
- add or update tax roles
- request or view an employee's stapled super fund details
- add, update or cancel registration details
- access another user's mail
- access business appointments and permissions enabled through cross entity authorisations (XEA).

Online services for agents restrictions

When using Online services for agents with a Basic myGovID, you won't have access to the following common activities:

- add, update or cancel client details
- add, update or cancel registration details
- bulk download client lists
- add or update financial institution details
- add or update tax roles
- request or view your client's employee's stapled super fund details
- submit payment plans
- update practice default communication details

- lodge a tax file number (TFN) declarations
- lodge return not necessary (RNN) or further return not necessary (FRNN)
- view or submit JobKeeper registrations.

Basic myGovID – proof of identity without a TFN

- https://www.ato.gov.au/General/Online-services/Accessing-online-services-with-myGovID-and-RAM/Accessing-our-online-services-with-a-Basic-myGovID/Basic-myGovID---proof-of-identity-without-a-TFN/
- Last modified: 31 Aug 2021
- QC 66707

To access Online services for business or Online services for agents using a Basic myGovID you need to prove your identity.

This page explains how to do this if you don't have an Australian tax file number (TFN).

How to complete proof of identity requirements

You need to complete and send us the ATO use of Basic myGovID (NAT 75249, PDF, 182KB) 🔽 form.

You need to include copies of two identity documents. The identity documents we accept are shown on the form. These documents should be certified. We will consider uncertified identity documents if COVID-19 restrictions mean you can't get them certified.

If you want your documents returned to you, you need to request this at the time of lodging and include your return postal address.

Once we have received and checked your documents, you'll receive a confirmation email.

Find out more about:

- Certifying your identity documents
- Consideration for uncertified identity documents
- Identity documents not in English

Certifying your identity documents

The following individuals are authorised to certify your identity documents outside of Australia:

- notary publics
- employees of an Australian
  - embassy
  - high commission
  - consulate – including consulates headed by Austrade honorary consulates.

The certifier needs to do the following in your presence:

- stamp, sign and annotate the copy of the identity document to state 'I have sighted the original document and certify this to be a true and correct copy of the original document sighted'
- initial each page
- list their name, date of certification, phone number and position.

See also:

- [Department of Foreign Affairs and Trade](#)⬀ for a list of Australian embassies, high commissions and consulates by country

Consideration for uncertified identity documents

Due to COVID-19 restrictions we may accept uncertified identity documents. If you can't certify your identity documents, you can tell us this on your form in Section B. You can then send your form with your uncertified documents to us for consideration.

If we accept your uncertified documents, we will request certified copies of your identity documents in future.

Identity documents not in English

If you provide documents that are in a language other than English, you must also provide an English translation made by an approved translation service.

All translations must include a statement from the authorised translator that it is a 'true and correct translation made from the document sighted'.

The translation should also display an official stamp, or similar, showing the certifier's accreditation.

Translations should also be accompanied by a certified copy of the original document in the language of origin, which has been stamped and signed as a true and correct copy by an approved certifier.

To obtain translations outside Australia and find an approved translator you can contact your nearest:

- Australian embassy
- high commission
- consulate.

See also:

- [Australian Department of Foreign Affairs and Trade](#)⬈ for a list of these offices by country.

Businesses

- https://www.ato.gov.au/General/Online-services/Businesses/
- Last modified: 14 Jul 2022
- QC 40955

Most of your business reporting and transactions can be done online through ATO online services.

On this page

- [Overview](#)
- [Online services for business](#)
- [Accessing Online services for business](#)
- [How to use Online services for business](#)
- [Standard Business Reporting (SBR)-enabled software](#)
- [Providing feedback](#)
- [Contact us](#)

Overview

Our online services are quick, easy, tailored, and secure. They let you manage your business reporting and transactions at a time that is convenient for you.

If you use a registered tax or BAS agent for your tax and superannuation matters, you can still access our online services.

You can do most of your business reporting and transactions with us online using:

- [Online services for business](#)
- [Standard Business Reporting (SBR)-enabled software](#)

If you're a sole trader, use myGov to access [Online services for Individuals and sole traders](#).

Online services for business

Online services for business is the default online service for approved self-managed super fund (SMSF) auditors, businesses, and other organisations to engage with us. Trustees of [self-managed superannuation funds](#) who have an ABN can also use this service. It's streamlined and contemporary – you can access it at any time on

multiple devices, including smart devices such as your mobile phone or tablet.

Online services for business will log out after 20 minutes of inactivity. If you are timed out, just log in again.

Log in to Online services for business

You can use Online services for business for most of your business interactions with us – for example:

- view, prepare, lodge and revise activity statements
- view, prepare, lodge and revise your taxable payments annual report
- create payment plans
- switch between your businesses with a single log in
- view statements of account and find your payment reference number (PRN)
- manage your accounts and update your tax registration details (for example, add or cancel a role)
- view your Single Touch Payroll reports
- register for goods and services tax (GST) and pay as you go (PAYG) withholding
- request stapled super fund details for new employees
- for SMSF auditors, prepare and lodge Auditor contravention reports (ACR) and Audit Complete Advices (ACA), including bulk ACA lodgment
- SMSF trustees can lodge an SMSF regulatory disclosure form, request SMSF specific advice, and lodge an amendment
- access secure mail subjects
- access the Small Business Superannuation Clearing House
- view and print tax returns and income tax history (if you are a sole trader, continue to use ATO Online)
- customise your home page.

Accessing Online services for business

To access Online services for business you'll need to sign in using myGovID.

If you're new to our online services, you will have to first set up your myGovID and then link it to your business in Relationship Authorisation Manager (RAM).

For access and set up assistance, see:

- Accessing online services with myGovID and RAM.
- Set up your access to Online services for business.

How to use Online services for business

The information below complements the prompts and help available throughout Online services for business. Additional help, relevant to the action you are

performing, is available by selecting the Help button within the service.

[Approved SMSF auditors](#) have access to various functions in Online services for business depending on the permissions set-up in [Access Manager](#).

The resources below outline the available functions:

- [General Online services for business functions](#)
- [Accounts and payments](#)
- [Lodgments](#)
- [Employees](#)
- [Profile](#)
- [Communication](#).

Standard Business Reporting (SBR)-enabled software

[Standard Business Reporting](#)⧉ (SBR) is a standard approach to online or digital record keeping to simplify business reporting obligations. Digital service providers build SBR rules into business software to make the software 'SBR-enabled'.

You can prepare and lodge reports to us directly from your SBR-enabled business software.

If you use SBR-enabled software, you can report using information that's already captured as part of the day-to-day operations of your business.

Credentials in SBR-enabled software

Your SBR-enabled software uses a credential that allows you to securely submit information to us.

When using cloud-based SBR software, you don't need to create this credential. Instead, your software provider will build it into your software. For more information, see [Cloud software authentication and authorisation](#).

If you use desktop or locally hosted SBR-enabled software (not cloud), you'll need to create a [machine credential](#)⧉ using [Relationship Authorisation Manager](#)⧉.

Providing feedback

We know you are busy and appreciate your support to help us improve our online services. To provide feedback complete the *Give us your feedback* form in Online services for business. You can find it at the bottom of every page.

Contact us

For assistance:

- With your tax and superannuation affairs, [contact us](#).
- For how-to videos and resources to help you set up your myGovID and link it with RAM, read [Accessing online services with myGovID and RAM](#)

- For help with the myGovID website, see [Need help](#)⧉
- For help with the RAM website, see [Help](#)⧉.

ATO Online services for business terms and conditions

- https://www.ato.gov.au/General/Online-services/Businesses/ATO-Online-services-for-business-terms-and-conditions/
- Last modified: 23 Dec 2020
- QC 63793

Terms and conditions of use of Online services for business

When we say:

- we, us and our – we mean the Australian Taxation Office (ATO)
- you and your – we mean you as the user of Online services for business
- Online services for business – we mean this electronic data system that we provide
- person – we mean an individual, a partnership and anybody whether incorporated or not.

How these terms and conditions apply

These terms and conditions apply to your current use of Online services for business.

These terms and conditions, your use of Online services for business, and information provided to you through Online services for business, are governed by the laws in force in the Australian Capital Territory, Australia.

Your obligations as a user of Online services for business

1. Access security

When you use a security credential to access Online services for business, you must:

- comply with the terms and conditions that relate to that security credential
- keep that security credential secure at all times
- not disclose that security credential to, or share it with, others.

You must not access Online services for business if access has either:

- not been issued to you
- been revoked by its issuing authority.

If the security credential issued to you has been compromised, or if there is any change in the information on which the issue of your security credential was based, you must notify the issuing authority immediately.

2. Permitted use of Online services for business

Businesses and approved self-managed super fund (SMSF) auditors are permitted use of Online services for business for the following functions and purposes:

- managing your business and personal details
- lodging or submitting certain forms
- sending secure messages
- viewing your business tax information
- viewing your communication preferences
- viewing, creating and updating payment plans
- maintaining and updating payment methods.

3. Data security

Data about individuals and entities provided to you through Online services for business is confidential. You must ensure that unauthorised persons do not have access to that data. If your computer will be unattended, even briefly, you must log out of Online services for business or lock your computer – see Online security for more information.

4. Acting for another person

To use Online services for business to access data relating to, or to carry out a transaction for another person, you must be currently appointed by that other person to access that data or carry out that transaction on their behalf. That appointment must not have been revoked.

If your appointment is:

- based on you holding a certain position (for example, as that other person's employee or agent for tax purposes) – you must currently hold that position
- under the *Corporations Act 2001* to act on behalf of the entity in your capacity as an insolvency practitioner – this appointment must be current

5. Employee access

If you are permitting access for employees to use Online services for business, you must ensure access is restricted to your employees and they are aware of and comply with these terms and conditions.

6. System use

Our digital services (including Online services for business) are designed and intended for human interaction only and must not be used for any other purpose

than those outlined in these terms and conditions.

By using Online services for business for the permitted uses as outlined in these terms and conditions it will ensure consistent system performance is maintained for all users.

You must ensure you do not, agree not to, enable others to cause disruption to the system.

This means that you are not allowed to use any third-party software or programs (like bots, scraper tools) to access, monitor, or copy Online services for business or its contents unless we have given you permission to do so.

7. Breach of terms and conditions

If you breach any of these terms and conditions, you must immediately:

- advise us of that breach
- stop using Online services for business until we advise you can.

A breach of these terms and conditions may result in one or more of the following actions:

- a direction to change your system usage
- suspending your access to the service
- terminating your access to the service.

8. Digital correspondence

By accepting these terms and conditions, you are agreeing to receive correspondence from us electronically.

There may be situations where correspondence is sent to you via multiple channels. This occurs because we need to meet the deemed service provisions contained in the *Taxation Administration Regulations 2017* and mandatory service requirements under the *Acts Interpretation Act 1901*.

9. Responsibility for actions

You will be responsible for (and you indemnify us against) any loss or damage to any person from either any:

- breach by you of these terms and conditions
- wilful, negligent or unlawful act or omission by you in relation to, or in the course of using Online services for business.

However, your liability to us will be reduced to the extent that any wilful, negligent or unlawful act or omission by us has contributed to that loss or damage.

Your responsibility for activities undertaken by you through Online services for business (for example, for updates, notices, statements, applications and other documents transmitted to us) will continue despite you ceasing to use Online

services for business or having access to it.

Our obligations

1. Privacy and secrecy obligations

For information about your privacy, refer to the [Privacy policy](). We will ensure that Online services for business complies with these laws at all times.

2. Provision of Online services for business

We can:

- limit your ability to use Online services for business
- terminate your access to Online services for business at any time
- work out the times and periods which Online services for business transmissions can take place
- vary the terms and conditions of use of Online services for business (so the terms and conditions applicable when you next use Online services for business may be different from these terms and conditions)
- review the activities of users of Online services for business to ensure they are meeting the relevant terms and conditions of use.

3. Online services for business and linked sites

Online services for business may not contain all the information that you need. We do not prepare (or necessarily endorse) the information not on our sites, even if linked to our site. We take no responsibility for your use of a site we are not responsible for or the information on it.

4. Information sent via Online services for business

We are not responsible for:

- the accuracy, veracity and completeness of material transmitted to us
- errors in the manner of the input of material transmitted to us
- any information you may lose as a result of equipment or power failures or our servers terminating your session due to prolonged periods of inactivity.

5. Limited liability

We will not be liable for any direct, indirect, incidental, special, consequential or exemplary damages (including for loss of profits, goodwill, information, data or other intangible losses) resulting from:

- the use or inability to use Online services for business
- unauthorised access or alterations of your transmissions to or from Online services for business
- activities resulting from the loss or misuse of your security credential
- statements or conduct of any third party
- any other matter relating to Online services for business.

6. No warranties by us

Except as specified in these terms and conditions, we give no implied or express warranties in relation to the use of Online services for business. All statutory warranties are, to the fullest extent permitted by law, expressly excluded.

General Online services for business functions

- https://www.ato.gov.au/General/Online-services/Businesses/General-Online-services-for-business-functions/
- Last modified: 09 Aug 2021
- QC 65231

Online services for business allows you to access a range of information about your business accounts from the home page, including accounts that require action or that have overdue amounts.

On this page:

- Customise the home page
- Log out
- Switch ABN
- Notifications
- For action
- Help aside
- Provide feedback

Customise the home page

Customising your home page lets you quickly access the functions most relevant to you. You can select up to eight quick links.

To change the quick links:

- select the Customise home page button at the bottom of the home page
- select or deselect the Quick links check box to choose what you want displayed.

Log out

You should log out of Online services for business when you are not using it.

Do this by clicking Logout in the top right-hand corner of the page.

Switch ABN

If you're an authorised contact for more than one entity, Online services for business allows you to switch between these entities without having to log in and out.

By selecting Switch ABN in the top right section of the screen, a list of entities you are authorised to access will appear. If there are more than 10 entities, you can search this list by name or ABN.

Notifications

The notification section on the home page alerts you to actions required or information we are giving you. These notifications are personalised to your myGovID login.

To view a list of notifications, select Notifications from the drop-down menu.

A maximum of six notifications are displayed at any one time.

Notifications will be for your information or to action and you:

- can dismiss information notifications at any time by selecting X
- can't dismiss an action required notification until you have actioned it – select Action now and you will be taken to the relevant function to complete the action.

For action

The 'For action' section on the home page displays a personalised view of lodgment and payment obligations.

The 'Lodgments' section will display lodgments that are upcoming and overdue. You can choose to view or prepare depending on the lodgment type.

The 'Payment' section displays your accounts with amounts owing to the ATO. Accounts have an indicator if they are overdue or in a payment plan. A debit amount not yet due, or an account in a payment plan, displays a view link taking you to the accounts screen. An overdue account displays a pay link taking you directly to the payment screen.

Help aside

Online services for business has a useful Help aside function.

To access, click on the '? Help' button on the right-hand side of the page.

This feature provides support and guidance relating to the page you are currently viewing in Online services for business.

For help on how to perform transactions within Online services for business, see How to use Online services for business.

Provide feedback

We developed Online services for business in collaboration with the users of service, including businesses, approved self-managed super fund auditors, and other organisations. Many of the enhancements we make are due to your feedback.

How to provide feedback

Give us feedback is located at the bottom of each screen in Online services for business. Provide as much detail as possible.

Our troubleshooting page lists issues we know about that may prevent you from completing an action in the system. We update this page when an issue has been resolved. Before providing your feedback, check this page to see if an issue is already listed.

Using your feedback

We use your feedback to:

- fix identified issues (like those listed on the troubleshooting page)
- investigate whether improvements can be made to the system
- find out what you like about the system and how are you using it.

We aren't able to respond to individual comments or questions.

If you wish to enquire about your tax affairs contact us.

You can keep up-to-date with the system enhancements we are planning by subscribing to our various newsletters.

Next step:

- ATO newsletter and alerts subscription centre

Account and payments in Online services for business

- https://www.ato.gov.au/General/Online-services/Businesses/Account-and-payments-in-Online-services-for-business/
- Last modified: 09 Aug 2021
- QC 65234

The 'Accounts and payments' menu allows you to access a range of functions, including making payment plans, arranging transfers or refunds, or paying amounts due.

On this page:

- [View your accounts](#)
- [Payment plans](#)
- [Payment options](#)
- [Transfers](#)
- [Refunds](#)

View your accounts

The accounts summary displays a complete list of accounts held with the ATO along with the payment reference number, any overdue amount and the account balance. You can view specific account types using the filter.

To access an account, select Accounts and payments, then Account summary. Then select the relevant Account name linked.

To filter the selected account:

- select Filter, then
    - enter the date range – From date and To date
    - process date order – displays results in the order transactions were processed by ATO
    - effective date order – displays results in the order the transaction was effective on the account (for amended or revised activity statements, the effective date shown will be the date the original transaction was due)

- select Order date to sort from Newest or Oldest
- select the check box to hide transactions which total to zero.
- then click Filter to sort and view transactions

You can also pay outstanding amounts using the payment options hyperlink and following the options.

Payment plans

You can make a payment plan online if the debt is under $100,000. At the Accounts and payments menu:

- select Payment plans
- select Add
- select account for payment plan and the amount
- select payment method and frequency
- enter payment date, upfront payment and instalments then select Calculate payment plan
- select Next and review the payment plan
- select the declaration then Submit.

You will receive a message with a receipt number once the plan has been submitted successfully.

To pay a payment plan by direct debit (via bank account or credit/debit card), see Manage cards.

For payment plans above $100,000, you will need to contact us.

Watch: Create a payment plan

Media: Create a payment plan
https://tv.ato.gov.au/ato-tv/media?v=bi9or7odbousrg (Duration: 2:29)

Payment options

From the Payments menu, you can:

- view your payment options
- obtain an electronic funds transfer (EFT) code.

You can download and print a payment slip when you access the payments screen from a specific account (for example, an activity statement account).

To pay by credit or debit card for amounts between $1 and $20,000,000:

- select credit or debit card
- filter by amount type (debit balance, overdue, or all)
- check the box beside the appropriate account in the Account details screen (the pre-filled amount to pay can be changed to any payment amount)
- type your card details
- choose to save the card details for future payments, this will not create a direct debit.

Maintain your cards for future payments by selecting Manage card details from the Profile menu. From here you can:

- view your stored cards
- add up to three cards for future use
- update stored card details
- delete stored cards.

Note: Storing a card for future payments does not set up a direct debit arrangement.

To pay by BPAY®:

- your electronic fund transfer (EFT) code is needed to pay an account or you can quote the EFT code as your customer reference number (the EFT code is different for each account)
- select BPAY from the Payment screen
- at Account details, all valid accounts are listed with payment reference numbers
- the Biller code is at the bottom of the screen.

To pay by direct debit:

- select Other payment methods from the Payment screen
- all applicable accounts will be displayed along with the payment reference number and the account balance.

ATO account details are displayed on the screen and can be printed.

Transfers

To request a transfer of a credit balance between accounts, select Accounts and payments > Transfer request.

Refunds

To request a refund of a credit balance on an account, select Accounts and payments > Refund request.

Lodgments in Online services for business

- https://www.ato.gov.au/General/Online-services/Businesses/Lodgments-in-Online-services-for-business/
- Last modified: 22 Feb 2022
- QC 65235

The 'Lodgments' menu in Online services for business allows you to lodge a range of forms and statements with the ATO.

On this page

- Lodge a business or instalment activity statement
- View and print tax returns
- Super guarantee charge statement
- Transfer balance account report
- Private rulings
- Objections
- File transfer
- Reported transactions
- Fuel tax credit non-GST
- Product Stewardship for Oil (PSO)

You can lodge an income tax return amendment via Secure mail.

Lodge a business or instalment activity statement

Activity statements are available under 'For action' or 'History'. You can view, print

and revise statements you've previously lodged in 'History'.

Activity statements that haven't been lodged are displayed as 'For action' and can be accessed from the home page or from the 'Lodgments' menu.

To complete your current activity statement:

- select either
  - Lodgments from 'For action'
  - Activity statements from the 'Lodgments' menu

- select Prepare next to the statement
- complete the mandatory details
- you can lodge a nil business activity statement (BAS) from the 'Prepare activity statement' screen by selecting Prepare as NIL
- tick the declaration
- select Save and exit to resume later or Lodge
- a confirmation screen will present with a unique receipt ID – the screen can be printed or saved as a PDF
- the total amount to pay will be presented on the screen with an option to pay now.

To view the GST property credits account:

- at the 'Lodgments' menu
- select GST property credits from the drop-down menu.

If no GST property credits exist, no records will display.

Find out about

- [Business activity statements](#)
- [Instalment notices for GST and PAYG instalments](#)

View and print tax returns

Online services for business allows you to view your lodgment history.

Income tax returns that haven't been lodged are displayed in 'For action' and can be viewed on the home page or from the 'Lodgments' menu by selecting Income Tax.

Lodged income tax returns are available to view and print at the 'Income tax' screen. Select History then View details beside the tax return. Once the return is viewed you can choose to print or save it as a PDF.

What you need to report and [how you lodge your tax return](#) for your business depends on your type of business entity.

Super guarantee charge statement

To lodge the [super guarantee charge (SGC)](#) statement, select Lodgments, reports and forms, and then Super guarantee charge statement.

Transfer balance account report

To lodge the transfer balance account report, select:

- Lodgments
- Reports and forms
- Transfer balance account report.

For information on completing the report, see [Super transfer balance account report instructions](#).

Private rulings

To apply for a [private ruling](#) within Online services for business, select:

- Lodgments
- Reports and forms
- Private ruling application.

Objections

To use Online services for business to lodge objections, select:

- Lodgments
- Reports and forms
- Lodge an objection.

For more information, see [Object to an ATO Decision](#).

File transfer

Select File transfer from Lodgment menu.

Files you can test or lodge are visible here.

Find out about

- [File transfer](#)

Reported transactions

Online services for business allows you to view third party data that we hold on taxable payments, government grants and business transactions received through payment systems. To view [Reported transactions](#), select:

- Lodgments
- Reports and forms
- Reported transactions.

Fuel tax credits non-business

Online services for business allows not-for-profit organisations (that are not

registered for GST) who operate emergency vehicles or vessels that provide emergency services and are clearly identifiable as such to register for fuel tax credit non-GST, lodge a claim or amend a previous claim.

You must claim within four years, and must keep records that support your fuel tax credit claim.

To register and claim Fuel tax credit non-GST, select:

- Lodgments
- Reports and forms
- Fuel tax credit non-GST.

Find out about

- Fuel tax credits non-business.

Product Stewardship for Oil (PSO)

To register and claim Product Stewardship for Oil (PSO), select:

- Lodgments
- Reports and forms
- Product stewardship for oil claim.

Employees in Online services for business

- https://www.ato.gov.au/General/Online-services/Businesses/Employees-in-Online-services-for-business/
- Last modified: 12 Jul 2022
- QC 65237

Use the Employees menu in Online services for business to manage your employer obligations.

On this page

- Single Touch Payroll
- Small Business Superannuation Clearing House
- Request stapled super fund details

Single Touch Payroll

Single Touch Payroll (STP) functions include:

- STP reporting
- STP deferral and exemption requests.

STP reporting

STP reporting allows you to view information reported for the business.

Select Employees – STP reporting.

You can then filter the data to view by financial year, date range, reporting branch or Business Management Software (BMS).

STP deferral and exemption requests

Select Employees – STP deferrals and exemptions to submit requests for:

- operational deferral
- transitional deferrals
- concessional reporting
- recurring deferrals
- exemptions
- no requirement to report
- finalisation declaration deferrals.

When a form is submitted, you will receive an ATO receipt ID. You'll be advised if the request has been accepted or has been sent for assessment.

Small Business Superannuation Clearing House

To access the Small Business Superannuation Clearing House, select Employees and then Small Business Superannuation Clearing house.

Request stapled super fund details

If you have new employees you may need to request their stapled super fund details from us.

To request a stapled super fund, select Employees – Employee super accounts. Previous stapled super fund requests will be displayed. Select Request to submit a new request.

Profile in Online services for business

- https://www.ato.gov.au/General/Online-services/Businesses/Profile-in-Online-services-for-business/
- Last modified: 05 Dec 2022
- QC 65239

You can use the Profile menu in Online services for business to manage your

business details with us.

On this page

- [Business details](#)
- [Business address](#)
- [Email address](#)
- [Authorised contacts](#)
- [Agent details](#)
- [Associates](#)
- [Financial institution details](#)
- [Manage card details](#)
- [Tax registrations – Add, update or cancel a tax type](#)
- [SMSF auditor details](#)

Business details

Selecting Business details from the Profile menu allows you to view Business information, including the business name, ABN and Tax file number as well as other related information.

To update the notification preferences, select the entity and update the channel preference. Where email is selected, you must provide an email address.

Business details, such as Company name or Public Officer details must be updated on the [Australian Business Register](#)⧉.

For more information, see [Update your details](#).

Business addresses

To update the business address, select Business addresses from the Profile menu.

Email addresses

To update an email address, select Email addresses from the Profile menu.

Authorised contacts

You can add, update, or delete authorised contacts by selecting Authorised contacts from the Profile menu.

To update or remove contacts listed on the ABR, go to [Australian Business Register](#)⧉.

Agent details

We're introducing an agent nomination process to businesses to strengthen security and help your business manage and authorise a registered agent to act on your behalf and manage your tax affairs.

Until the new feature is available to your business, your registered tax agent, BAS agent or payroll service provider will add or remove themselves as an agent, using the normal process.

View registered tax professionals by selecting Agent details from the Profile menu.

To nominate a registered agent:

- at Agent nominations
    - select Add
    - enter the registered agent number (RAN) or practice name that you'd like to nominate
    - select search
    - select the registered agent you want to nominate (if multiple results are returned, select the correct agent from the list)
    - carefully check that the agent's details are correct
    - complete the declaration then Submit the nomination form.

Your business may nominate more than one agent to manage different tax accounts.

The easiest and fastest way to search for the agent you want to authorise is to get the RAN from your agent and search using this number.

Extending a nomination

If the agent you've nominated needs additional time to add your business as a client, you can use the Extend feature.

The Extend feature will become available on the next calendar day after submitting a nomination. It will remain available for 7 calendar days (midnight on the 7th day) then will expire.

To extend a nomination:

- from Agent nomination, select Extend
- at the Extend agent nomination screen, check the details of the agent are correct
- complete the declaration and select Submit

The agent nomination has now been extended for an additional 7 calendar days from the time you submit the extend request.

If a nomination has expired, you won't be able to extend it. You'll need to resubmit a [new nomination](#).

You can delete an agent nomination by selecting Delete.

To cancel authority of a tax professional, [contact us](#).

Associates

You can view Associates of the business by selecting Associates from the Profile menu.

To update authorised contacts, select update. Authorised contacts with a relationship of 'ABR' can be updated through the [Australian Business Register](#)⧉.

Financial institution details

To view Financial institutions details for an account, select Financial institutions details from the Profile menu.

You can add, update, or delete details for the selected account.

Manage card details

Maintain your cards for future payments by selecting Manage card details from the Profile menu. From here you can:

- view your stored cards
- add up to three cards for future use
- update stored card details
- delete stored cards.

To update card details for an existing payment plan:

- select Manage card details from the Profile menu
- view your stored financial institution details or stored credit or debit card
- update the details if applicable.

Select Add to add a new credit/debit card, or click on the arrow to the right of a stored card to Edit or Remove your card details.

Information is available about how to [Set up a payment plan](#).

Add, update or cancel a tax type

Online services for business allows you to manage the different types of tax your business is registered for.

By choosing the Profile menu and selecting Tax registrations from the drop-down menu, you can add, update or cancel:

- goods and services tax (GST)
- income tax withholding (ITW – also known as PAYG withholding or PAYGW)
- luxury car tax (LCT)
- wine equalisation tax (WET)
- fuel tax credits (FTC).

To add a tax type:

- at 'Current registrations' select Add
- select Registration tax type from the drop-down menu

- type the details as prompted
- select Next
- review the summary
- select the declaration then Submit.

To update a tax type:

- select Update next to the relevant tax type to be updated
- type the required updates
- select Next
- review the summary
- select the declaration then Submit.

To cancel a tax type:

- select Cancel next to the account type to be cancelled
- type the date the cancellation takes effect and select the reason for cancellation
- select Next
- review the summary
- select the declaration and then Submit.

SMSF auditor details

SMSF auditor details can be entered in this screen for use in the Auditor Contravention reports (ACR) and Audit complete advice (ACA) forms.

Details entered here will only be used to pre-populate ACR and ACA forms and will not be used to update details with the ATO or ASIC.

Up to 100 different SMSF auditors can be saved.

To add an auditor:

- Click Add
- Enter a valid SMSF auditor number
- Enter auditor first name and surname
- Enter at least one contact number; phone, or mobile number
- Start typing the auditor's postal address and select the correct address from the drop-down list as it is presented – ensure the address is validated.
- Click Save

To edit an auditor:

- Select the auditor that requires editing
- Click Edit
- Change any fields – note the SMSF auditor number cannot be edited
- Click Save

To delete an auditor:

- Click the delete icon next to the auditor you wish to delete

- Select Yes 'Are you sure you want to delete'

For more information, see [Taxation registrations](#).

Communication in Online services for business

- https://www.ato.gov.au/General/Online-services/Businesses/Communication-in-Online-services-for-business/
- Last modified: 07 Feb 2023
- QC 65241

Use the Communication menu in Online services for business to communicate with us by Secure mail.

On this page

- [Secure mail](#)
- [Mailbox management](#)
- [Secure mail topics](#)
- [Communication history](#)
- [Communication preferences](#)
- [Your dealings](#)
- [Lodge amendments](#)

Secure mail

To access Secure mail, you need to select (tick) the View and action own mail permission in [Access Manager](#).

At the Communication menu, select Secure mail to securely communicate with us.

To send secure mail messages you will need:

- a separate secure mail message for each subject
- to ensure you attach all supporting documentation and that the attached documentation
  - is a maximum of 6 files
  - is less than 6MB in size (per file)
  - is in a suitable format (doc, .pdf, .rtf, .xls, .xml, .tif, .jpg, .zip, .bmp, .png, .gif, .mpp, .ppt, .docx, .dotx, .xlsx, .xltx, .pptx, .potx, .ppsx.)
  - is not encrypted (for example, password protected)
  - doesn't contain macros
  - doesn't contain formulas (copying and pasting information from one spreadsheet to another may introduce unseen elements in your

spreadsheet)

- is not an executable file (common executable file extensions include .exe, .app, .vb, .scr).

After sending your message, you will receive a receipt number.

You can also:

- view sent messages
- reply to messages
- allocate messages to other users (based on permissions)
- delete messages
- receive replies from us
- print messages
- set up email notifications to your preferred email address to advise you when you receive messages to your Online services for business mailbox
  - select Email notification at the bottom of the inbox, type or update your email address
  - email notifications will always be from our trusted email address – Taxofficeportalmessagenotify@ato.gov.au.

- access another users' mailbox to view and allocate mail (you cannot create, send or reply to an email in the business mailbox)
- access the Business mailbox to view delete, allocate or set up notifications (you cannot create, send or reply to an email in the Business mailbox).

To view the Business inbox or another user's mailbox, you need to select (tick) the Access other users' mail permission in [Access Manager](#).

Mailbox management

Warnings will appear when a mailbox is approaching or has exceeded the 500 message limit. The limit includes both emails in your mailbox and sent emails.

You will be asked to delete mail items to reduce your mailbox size. Exceeding the limit will impact a user's ability to create new emails or reply to received emails.

You can save a list of messages in your own inbox or sent items by using the Printer Friendly button (located at the bottom left of your screen). This gives you the option to print a hard copy or save the list as a PDF.

Alternatively, you can view a list of sent emails in [Your Dealings](#). This includes the status of the request.

To save copies of individual emails:

- open the email by clicking on the email hyperlink
- select the Printer Friendly button to print or save as a pdf.

Secure mail topics

Secure mail allows you to communicate with us on a range of topics and subjects. Topics and subjects are listed below.

Activity statements

Topic	Subject
Activity statements	Additional time to lodge – deferral request
Activity statements	Debit or nil balance query
Activity statements	How do I complete my activity statement?
Activity statements	Penalty or interest calculation
Activity statements	Remission of failure to lodge on time penalty More information: Requesting remission
Activity statements	Remission of general interest charge More information: How to request a remission of interest
Activity statements	Remission of non-electronic notification or non-electronic payment penalty

---

Debt and lodgment

Topic	Subject
Debt and lodgment	Additional time to lodge – deferral request
Debt and lodgment	Debit or nil balance query
Debt and lodgment	Penalty or interest calculation
Debt and lodgment	Remission of failure to lodge on time penalty
Debt and lodgment	Remission of general interest charge More information: How to request a remission of interest
Debt and lodgment	Remission of shortfall interest charge

	More information: How to request a remission of interest
Debt and lodgment	Taxable Payments Annual Report

Registrations

Topic	Subject
Registrations	Consolidation registration enquiry
Registrations	Grouping or Branching registration enquiry
Registrations	Non-residents registration enquiry
Registrations	GST Joint Venture Notification GST – joint venture – notification of forming, changing or cancelling (PDF, 345KB) ⬇

Income tax

Topic	Subject
Income tax	Additional time to lodge – deferral request
Income tax	Debit or nil balance query
Income tax	Div 7a Relief
Income tax	Income tax return amendment – companies More information: Lodge amendment
Income tax	Income tax return amendment – partnerships More information: Lodge amendment
Income tax	Income tax return amendment – superannuation funds More information: Lodge amendment
Income tax	Income tax return amendment – trusts More information: Lodge amendment
Income tax	Lodge Loss carry back form

Income tax	Lodge temporary full expensing schedule
Income tax	Submit 14ZYA notice
Income tax	Penalty or interest calculation
Income tax	Remission of failure to lodge on time penalty
Income tax	Remission of general interest charge More information: How to request a remission of interest
Income tax	Remission of shortfall interest charge More information: How to request a remission of interest
Income tax	Financial hardship refunds
Income tax	Certificate of Residency More information: Requesting a certificate of residency or status
Income tax	Request for Copies of tax documents More information: Copies of tax documents request
Income tax	ESIC Report NAT75119 unable to submit online
Income tax	Prior year IT amendment for earnout purposes
Income tax	Stapled Group – Choice Form
Income tax	Substituted Account Period

Pay as you go

Topic	Subject
Pay as you go	Instalments – Additional time to lodge – deferral request
Pay as you go	Instalments – Change instalment rate
Pay as you go	Instalments – Change PAYG cycle

Topic	Subject
Pay as you go	Instalments – Explanation of instalment rate
Pay as you go	Instalments – Other instalment queries
Pay as you go	Withholding – ATO cycle change letter received – Request to remain on current cycle
Pay as you go	Withholding – cycle change request – withholding amount less than $1 Million
Pay as you go	Withholding – cycle change request – withholding amount more than $1 Million

Superannuation

Topic	Subject
Superannuation	Account details – this option is only available to legal practitioners. Other requests will not be answered.
Superannuation	Approved SMSF Auditors – ACA bulk lodgments Audit complete advice (XLSX, 248KB)
Superannuation	Approved SMSF Auditors – Intelligence referrals
Superannuation	Approved SMSF Auditors – Number enquiries
Superannuation	Approved SMSF Auditors – P2P requests – application of the SIS Act & Regulations
Superannuation	Approved SMSF Auditors – IAR/ACR/ACA Enquiries
Superannuation	Approved SMSF Auditors – Auditing Standards/Audit related issues, online services and general enquiries
Superannuation	Direct claim payout from the superannuation holding account special account (SHA)
Superannuation	Fund Validation Service
Superannuation	Is a particular fund registered as a complying superannuation fund?
Superannuation	Lodge inactive low balance account – declaration
Superannuation	Lodge SGC Statement

	[SGC Statement spreadsheet version (XLS, 526KB)](#) ⤓
Superannuation	Lodge Super Guarantee Opt-Out form [Super Guarantee opt-out for high income earners with multiple employers (PDF, 315KB)](#) ⤓
Superannuation	Lodge USM adjustment Templates/non-Lodgment Advice
Superannuation	Lodgment – Transfer Balance Account Report
Superannuation	Manual payment request
Superannuation	Other
Superannuation	Payment and transfer of superannuation holdings reserve
Superannuation	Payment arrangement request
Superannuation	Penalty or interest calculation
Superannuation	Refund request
Superannuation	Remission of general interest charge
Superannuation	Small Business Superannuation Clearing House enquiry
Superannuation	SMSF Early Engagement and voluntary disclosure More information: [SMSF regulatory contravention disclosure form](#)
Superannuation	SMSF product ruling
Superannuation	SMSF specific advice More information: [Request for self-managed superannuation fund specific advice](#)
Superannuation	Statement of account or account query
Superannuation	Superannuation Provider Assessment Data

Refunds and remissions

Topic	Subject
Refunds/remissions	ATO pay interest on an early payment – request
Refunds/remissions	Client overpayment/double payment

Refunds/remissions	Excess imputation credit refunds
Refunds/remissions	Financial hardship refunds
Refunds/remissions	Interest paid on an overpayment of an income tax return
Refunds/remissions	Penalty or interest calculation
Refunds/remissions	Refund tax withheld
Refunds/remissions	Remission of failure to lodge on time penalty More information: Requesting remission
Refunds/remissions	Remission of general interest charge More information: How to request a remission of interest
Refunds/remissions	Remission of non-electronic notification or non-electronic payment penalty
Refunds/remissions	Returned refunds
Refunds/remissions	NRWT – Custodians

Fringe Benefits Tax (FBT)

Topic	Subject
Fringe Benefits Tax (FBT)	Additional time to lodge – deferral request
Fringe Benefits Tax (FBT)	Cancel FBT
Fringe Benefits Tax (FBT)	Change details for FBT
Fringe Benefits Tax (FBT)	Debit or nil balance query
Fringe Benefits Tax (FBT)	General FBT questions
Fringe Benefits Tax (FBT)	FBT Amendment request
Fringe Benefits Tax (FBT)	Other
Fringe Benefits Tax (FBT)	Penalty or interest calculation
Fringe Benefits Tax (FBT)	Register for FBT

Fringe Benefits Tax (FBT)	Remission of failure to lodge on time penalty More information: [Requesting remission](#)
Fringe Benefits Tax (FBT)	Remission of general interest charge More information: [How to request a remission of interest](#)

Other topics

Topic	Subject	Additional subject
View more topics	GST	Additional time to lodge – deferral request
View more topics	GST	ACNC – Elect to exclude grants
View more topics	GST	Charities, religious institutions, non-profit entities
View more topics	GST	Consolidation registration enquiry
View more topics	GST	Deferral of GST on importations (DGST)
View more topics	GST	Education courses
View more topics	GST	Export, import or online trading of goods and services
View more topics	GST	Financial supplies or insurance
View more topics	GST	Food, entertainment and SAM (simplified accounting method)

View more topics	GST	Government grant or funding, taxes, fees, charges
View more topics	GST	Grouping or Branching registration enquiry
View more topics	GST	GST Joint Venture Notification GST – joint venture – notification of forming, changing or cancelling (PDF, 345KB) ⬇
View more topics	GST	Land or property transaction (including retirement villages)
View more topics	GST	Motor vehicles or luxury car tax
View more topics	GST	Other sales, purchases or and tax invoice enquiry
View more topics	GST	Time limits on refunds or activity statement amendment
View more topics	GST	Assistance to register/update GST details electronically
View more topics	GST	GST at settlement
View more topics	GST	Registrations update
View more topics	Exploration incentives	EDI Advice
View more topics	Exploration incentives	EDI Lodgment
View	Exploration incentives	JMEI Advice

View more topics		
View more topics	Exploration incentives	JMEI Lodgment
View more topics	Lodge report	Annual investment income report extension of time
View more topics	Lodge report	Annual investment income report lodgment – PC spreadsheet
View more topics	Lodge report	Common Reporting Standard (CRS) extension of time
View more topics	Lodge report	Employee share scheme annual report extension of time
View more topics	Lodge report	Foreign Account Tax Compliance Act (FATCA) extension of time
View more topics	Lodge report	Non-resident interest, dividend and royalty annual report lodgment – PC spreadsheet
View more topics	Lodge report	Quarterly tax file number report extension of time
View more topics	Lodge report	Quarterly tax file number report lodgment – PC spreadsheet
View more topics	General questions/problems/help	Notify ATO of appointment of new public officer
View more topics	General questions/problems/help	Notification of legal representative
View more topics	Statement requests/account details	Debit or nil balance query

View more topics	Statement requests/account details	Penalty or interest calculation
View more topics	Statement requests/account details	Remission of failure to lodge on time penalty More information: [Requesting remission](#)
View more topics	Statement requests/account details	Remission of general interest charge
View more topics	Excise	Alcohol, fuel and petroleum products, tobacco, duty free store
View more topics	Excise	Audit
View more topics	Excise	Excise Returns More information: [Excise return and instructions](#)
View more topics	Excise	Fuel schemes enquiry
View more topics	Excise	Fuel tax credit enquiry (not to be used for registration requests)
View more topics	Excise	Other advice or lodgment enquiry
View more topics	Excise	Permission – movement and period settlement
View more topics	Excise	Remission, refund and drawback enquiry
View more topics	Excise	Wine equalisation tax enquiry (not to be used for registration requests)

View more topics	Excise	Product Stewardship for Oil (PSO) claim More information: [Product stewardship for oil program claim form](#)
View more topics	Excise	Product Stewardship for Oil (PSO) Category 1 Lab test results
View more topics	Excise	WET, FTC, LCT Registration.
View more topics	Insolvency	Bankruptcy
View more topics	Insolvency	Deed of Company Arrangement
View more topics	Insolvency	Liquidation
View more topics	Insolvency	Finalisations
View more topics	Insolvency	Indemnities
View more topics	Insolvency	New Insolvency Advice
View more topics	Insolvency	New Insolvency Advice – Voluntary Administration
View more topics	Insolvency	Notification of Creditors Meeting
View more topics	Insolvency	Part IX
View	Insolvency	Part X

View more topics		
View more topics	Insolvency	Preferences
View more topics	Insolvency	Receiver/Manager appointed More information: [Appointment or cessation of a representative of an incapacitated entity](#)
View more topics	Insolvency	SB – Restructuring
View more topics	Insolvency	Simplified Liquidation
View more topics	Insolvency	Section 129 Demand
View more topics	Insolvency	Tax Clearance
View more topics	Insolvency	Request for Documents – The insolvency option is only available for insolvency practitioners. Other requests will not be answered. More information: [Copies of tax documents request](#)
View more topics	Insolvency	Voluntary Administration
View more topics	Petroleum Resource Rent Tax	General enquiries
View more topics	Petroleum Resource Rent Tax	PRRT Return/Instalment lodgment More information: [PRTT return](#)
View more	Trustee Services	Day 1 Notification More information:

topics		

Communication history

Communication history gives you access to view available correspondence we send to you or your agent via the following channels:

- email
- SMS
- paper
- agent digital – used to send digital communications to your agent when they have set up Communication preferences to receive mail on your behalf
- ATO Online – used to send a digital copy of a statement of tax record and digital activity statement notice.

Some communications cannot be sent digitally. These will continue to be sent by post and will not be viewable in Communication history. We will continue to add more communication types to enhance this function further.

If you are a sole trader, you will need to use ATO Online services for individuals and sole traders to view your communication history.

To view your communication history:

- select Communication
- select Communication history.

To search using specific parameters:

- select Search
- select Type
    - Communications – list of available digital correspondence sent to you
    - Activity statements – Digital Activity Statement Notice – Digital quarterly GST and PAYG instalment notices

- select Time period using the drop-down menu
- select Channel
    - email
    - SMS
    - paper
    - agent digital
    - ATO online services

- then Search – results will be displayed
- select Download – a new window will open with the search results as an Excel spreadsheet
- select Print friendly version to print or save a copy.

You can view and download a digital activity statement notice for quarterly GST and

PAYG instalments (forms R, S and T) if you lodge activity statements electronically.

To view and download your digital activity statement notice from the client home page:

- select Communication
- select Communication history
- select Search
    - then select Activity statements tick box, and deselect Communications tick box
    - select the Time period and then Search – this will display the Digital Activity Statement Notice.

If your registered delivery preference is paper, we will continue to send paper instalment notices. We don't change your delivery preferences from paper to electronic unless you have lodged electronically.

Communication preferences

If you use a tax agent, Communication preferences allows you and your agent to choose where we send your digital ATO communications.

You can choose to have communications:

- sent to you
- sent to your registered agent.

You can also choose to have some communications sent to you and others to your registered agent.

Your agent can set your communication preferences on your behalf.

Your dealings

You can track the progress of the messages you've sent us, by using Your dealings in the Communications menu.

Lodge amendments

If you need to correct a mistake on your return, you can lodge this in Online services for business.

You will need to complete the amended return and then at the 'Communication' menu:

- select Secure mail then New
- select Topic: Income tax and Subject: Income tax amendment (and the relevant client type)
- attach amendment
- tick the declaration then Send.

You cannot [lodge an original income](#) tax return using Online services for business.

For business or super amendments, see [Request an amendment to a business or super tax return](#).

Approved SMSF auditors in Online services for business

- https://www.ato.gov.au/General/Online-services/Businesses/Approved-SMSF-auditors-in-Online-services-for-business/
- Last modified: 17 Mar 2022
- QC 65243

Online services for business allows approved self-managed super fund (SMSF) auditors to lodge the following documents online:

- audit complete advice (ACA)
- auditor/actuary contravention report (ACR).

Watch: Online services for business

Media: Online services for business
https://ato.vudoo.io/embed/55988302196 (Duration: 00:39)

[Log in to Online services for business](#)

On this page

- [Lodge an auditor/actuary contravention report](#)
- [Lodge an audit complete advice](#)
- [Complete and lodge bulk audit complete advices](#)

Lodge an auditor/actuary contravention report

To lodge an auditor/actuary contravention report:

- select the Lodgments menu
- select Reports and forms
- select Auditor contravention report
- select Prepare to start a new report or Resume to return to a previously saved report

- Select Financial year of audit using the drop-down option
- Enter Self Managed Super Fund (SMSF) ABN and click Search
- Enter total asset value as at 30 June for the year of audit
- Select whether this is a New or Revised report
- Click Next
- Enter Auditor details, you can do this manually by selecting Add an auditor from the drop-down options, or select an auditor from the list (auditor details can be added in the [SMSF auditor details](#) option under the profile menu).
- Manual entry of auditor details requires the following auditor information:
  - first name
  - last name
  - SMSF auditor number
  - phone number
  - mobile number
  - postal address

- You can choose to add these auditor details to be used in future reports by checking the box - select Save this auditor in SMSF auditors details for future reports
- Click Next
  - at 'Events – reporting an event'
    - select Add to report an event, you can report up to six events
    - answer 'Event started before the audit period'
    - type the start date of event
    - complete 'Describe the event and mitigating factors'
    - answer 'Contraventions fully rectified or trustees plan to fully rectify them'
    - enter 'Estimated completion date or date contraventions fully rectified'
    - if applicable, complete 'Planned or taken steps to rectify the contraventions'

  - at Contraventions
    - select from the sections or regulations contravened drop-down menu
    - if applicable, enter the maximum value of the contravention or regulation
    - answer 'Contravention or regulation fully rectified?'
    - if applicable, enter the outstanding value
    - if applicable, add another contravention
    - when finished select Save

  - Events – other questions
    - if applicable, answer the 'SMSF's financial position' question
    - if applicable, complete 'On what information did you base your opinion?'
    - if applicable, answer 'Additional information'
    - if applicable, complete 'Provide details'
    - select Next

- Summary
    - To print a draft copy of the ACR, select the 'Print friendly version' button before submitting.
    - Check the declaration.
    - Select Submit.

Up to 150 draft forms can be saved and completed within 6 months.

When the form is submitted successfully, a receipt number will be displayed and you can choose to print or save a copy of the submitted form.

Note: you will NOT be able to access a copy of the form after leaving this page.

Lodge an audit complete advice

To lodge an audit complete advice:

- at the Lodgments menu
- select Reports and forms
- select Audit complete advice
- complete the mandatory information on the form
    - select the financial year of audit using the drop down option
    - fund details
        - type the fund's ABN
        - select Search, the fund's name will be populated

- enter SMSF Auditor details, you can do this manually by selecting Add an auditor from the drop-down options or select an auditor from the list (auditor details can be added in the [SMSF auditor details](#) option under the profile menu).
- manual entry of auditor details requires the following auditor information:
    - first name
    - last name
    - SMSF auditor number
    - phone number
    - mobile number
    - postal address

- you can choose to add these auditor details to be used in future reports by checking the box - Save this auditor in SMSF auditors details for future reports
- select the declaration and Submit.

Complete and lodge bulk audit complete advices

To complete the 'audit complete advice' bulk template:

- download the template (XLSX, 248KB) ⬇ to your device
- complete the mandatory information on the template
    - auditor details
        - audit firm name
        - audit firm ABN
        - first name
        - last name
        - phone or mobile number
        - auditor address
        - SMSF auditor number

    - fund details
        - the fund ABN of SMSF you audited
        - name of SMSF
        - audit year
        - audit completion date

    - save the template as 'xls' or 'xlsx' (do not convert the completed template to a PDF).

Note: There is no requirement to lodge bulk audit complete advices when an audit complete advice or auditor contravention report has already been lodged for the same year.

To lodge a bulk audit complete advice:

- at the Communication menu
- select Secure mail from the drop-down menu
- select New at the inbox
- select the topic – Superannuation
- select the subject – Approved SMSF Auditor ACA bulk lodgment
- complete the mandatory information in the secure mail
- attach the completed audit complete advice bulk template
- type your email address
- type your contact details
- select the declaration and Send.

You will receive a receipt number once the mail is successfully sent.

Not-for-profits

- https://www.ato.gov.au/General/Online-services/Not-for-profits/
- Last modified: 15 Apr 2020
- QC 60014

As a not-for-profit organisation with an Australian business number (ABN) you may need to:

- lodge statements and returns (such as activity statements)
- update your ABN and tax file number (TFN) registration details
- view reports for Single Touch Payroll
- register for GST and PAYG.

Our online services provide quick, easy, and secure access to allow you to manage your reporting and transactions, at a time that is convenient for you.

If you use a registered tax or BAS agent for your tax and superannuation matters, you can still access our online services.

You can access our online services using the same steps as businesses.

Next step:

- Explore Online services – Businesses

Tax agents

- https://www.ato.gov.au/General/Online-services/Tax-agents/
- Last modified: 30 Mar 2020
- QC 40975

Most of your business reporting and transactions with us can be done online using:

- Online services for agents
- the practitioner lodgment service (PLS)
- Standard Business Reporting (SBR)
- Australian Business Register (ABR).

To access our online services, you'll need to use myGovID and Relationship Authorisation Manager (RAM).

The functions available to you will depend on your Access Manager permissions.

Online services for agents

Online services for agents is our main channel for you to interact with us online.

You can use it to:

- view and update your clients' registration details
- prepare, lodge, view and print activity statements for your clients
- view client account information

- request refunds and credit transfers on behalf of your clients
- communicate with us using secure practice mail
- view payment options, make and view payment plans and print payment slips
- test, lodge and download certain files using the file transfer function.

Log in to Online services for agents

See also:

- Online services for agents

Standard Business Reporting (SBR) and the practitioner lodgment service (PLS)

SBR is a standard approach to digital record keeping and simplifies reporting to government. The PLS is a service accessed by your practice management software and operates on the SBR platform. This service enables you to interact digitally with us through your SBR-enabled software.

You can prepare reports directly from your SBR-enabled practice software and lodge using the PLS for a wide range of tax returns, forms, statements and reports. You can also use it to report Single Touch Payroll, request reports and to prepare and revise activity statements.

If your SBR-enabled software is cloud based (online) you won't need to install a machine credential to interact with us. Instead, your digital service provider will build it into your software.

If you use desktop or locally hosted SBR-enabled software you will need to install a machine credential.

See also:

- Standard Business Reporting (SBR)⬂
- Machine credentials⬂
- Practitioner lodgment service
- Cloud software authentication and authorisation
- Single Touch Payroll
- Access Manager
- Online security
- Technical support

Australian Business Register

You can access your clients' Australian business number (ABN) details online using the Australian Business Register⬂. Use your myGovID to log in to the Tax professional services⬂ and:

- change secure ABN information (for example, postal address and public officer) and receive confirmation of the change in the same internet session
- apply for a tax file number (TFN)
- register for pay as you go (PAYG) or goods and services tax (GST).

See also:

- [Access Manager](#)
- [Online security](#)
- [Technical support](#)

Departing Australia superannuation payments (DASP) online system

You can use the DASP online intermediary application to claim superannuation on behalf of your temporary resident clients who have departed Australia and no longer have active visas.

Log in to the DASP online intermediary application system

See also:

- [DASP online intermediary application system](#)

myGovID and RAM for tax professionals

- https://www.ato.gov.au/General/Online-services/Tax-agents/myGovID-and-RAM-for-tax-professionals/
- Last modified: 16 Jun 2022
- QC 60632

How tax and BAS agents can use myGovID and Relationship Authorisation Manager (RAM) to access our online services.

On this page

- [Accessing Online services for agents](#)
- [Setting up myGovID and RAM](#)
- [Using myGovID and RAM](#)
- [Troubleshooting](#)

Accessing Online services for agents

To access Online services for agents (OSFA), Access Manager, the Australian Business Register (ABR) and other government online services, you'll need to use:

- myGovID – an app you download to your smart device which lets you prove who you are when logging into government online services. This is different to a myGov account, which lets you, as an individual, link to government online services from the one place.
- Relationship Authorisation Manager (RAM) – an authorisation service that allows you to act on behalf of a practice online when linked with your myGovID. You'll use your myGovID to log in to RAM.

Setting up myGovID and RAM

Each person acting on behalf of a practice needs their own myGovID and to be authorised in RAM.

myGovID

myGovID is your digital identity and unique to you. To access our online services, you'll need to [set up your myGovID](#) with at least a Standard identity strength.

When setting up your myGovID use a personal email address. myGovID is your personal digital identity and your identity documents will be linked to the email you choose. Once set up, your myGovID can be used for both personal and business matters, and you'll continue to use the same myGovID even if you change jobs.

The myGovID app uses the security features in your device, like fingerprint or face recognition, to protect your personal information. Your information is protected, including from your employer, who cannot access, use or cancel your myGovID.

To set up your myGovID on multiple devices, or to change to a new device, see [Setting up your myGovID again](#).

RAM

Before anyone can act on behalf of a practice a [principal authority](#) (person responsible for the practice) needs to link their myGovID to the practice in RAM.

You must be [authorised](#) in RAM by a principal authority or authorisation administrator to act on behalf of the practice. A principal authority or authorisation administrator will issue an [authorisation request](#) to your email. This does not need to go to your myGovID email address - it can be sent to your work email address.

Once you've accepted the authorisation request, you can use your myGovID to log in to our online services on behalf of your practice.

Using myGovID and RAM

Logging in with myGovID

When logging into an online service with your myGovID, you'll be directed to enter

the email address you used to set up your myGovID. A four-digit code will appear in your browser and you'll need to enter the code in your myGovID app.

Tip: select Remember me when you enter your email address on the myGovID login page. When using the same browser, you won't need to enter your email address each time you log in; you'll only need to accept the code in your myGovID app.

Responsible use of myGovID, RAM and online services

Using myGovID and RAM makes it easy for authorised persons to access relevant government online services anywhere and at any time. This doesn't change your obligation to interact professionally when using our online services.

You're responsible for using your myGovID to log in to OSFA and other government online services. You should never let anyone else use your myGovID, provide your log in code or enter your log in code for anyone. Each employee of a practice must set up their myGovID on a unique device; staff cannot share a myGovID or device.

You should only access records and transact where authorised to do so. Your principal authority and authorisation administrator can track your access to OSFA on behalf of the practice. Consult your practice policies for guidance on accessing and using government online services.

Your ongoing access to our systems is dependent on appropriate use of myGovID.

It's important you keep your myGovID, and your device, secure. Enable security features in your device such as fingerprint or face identification and avoid leaving your device unattended.

If you suspect someone has inappropriately accessed your myGovID, your device has been stolen or misplaced, or you've received an unprompted notification or email, report it straight away .

There is more information available on myGovID terms of use.

Troubleshooting

If you're experiencing issues, support is available:

- myGovID Help
- RAM Help
- Troubleshooting for businesses and tax practitioners
- Technical support – for known system issues
- System maintenance – for scheduled maintenance information

If you continue to experience issues, you can phone us for assistance.

BAS agents

- https://www.ato.gov.au/General/Online-services/BAS-agents/
- Last modified: 26 Jul 2021
- QC 40957

You can prepare, lodge and revise activity statements online using:

- Online services for agents
- the practitioner lodgment service (PLS)
- Standard Business Reporting (SBR).

To access our online services, you'll need to use myGovID and Relationship Authorisation Manager (RAM).

The functions available to you will depend on your Access Manager permissions.

Online services for agents

Online services for agents is our main channel for you to interact with us online.

You can use it to:

- prepare, lodge, view and print activity statements
- receive instant confirmation of your lodgment
- view and update your client's registration details
- view client account information
- view payment options, make and view payment plans and print payment slips
- communicate with us using secure practice mail
- test, lodge and download certain files using the file transfer function
- compare super funds using the YourSuper comparison tool.

Next step:

Log in to Online services for agents

See also:

- Online services for agents

Standard Business Reporting (SBR) and the practitioner lodgment service (PLS)

SBR is a standard approach to digital record-keeping and simplifies reporting to government. The PLS is a service accessed by your practice management software and operates on the SBR platform. This service enables you to interact digitally with us through your SBR-enabled software.

You can prepare reports directly from your SBR-enabled practice software and lodge using the PLS for a wide range of forms, statements and reports. You can also use it to report Single Touch Payroll, request reports and to prepare and revise activity statements.

If your SBR-enabled software is cloud based (online) you won't need to install a machine credential to interact with us. Instead, your digital service provider will build it into your software.

If you use desktop or locally hosted SBR-enabled software you will need to install a machine credential.

See also:

- Standard Business Reporting (SBR)
- Machine credentials
- Practitioner lodgment service
- Cloud software authentication and authorisation
- Single Touch Payroll
- Access Manager
- Online security
- Technical support

Self-managed superannuation funds

- https://www.ato.gov.au/General/Online-services/Self-managed-superannuation-funds/
- Last modified: 25 May 2022
- QC 69586

Online services for business is our default online service for SMSF trustees and auditors. You can use it anytime to manage your reporting obligations and other transactions.

SMSF Trustees

SMSF trustees can use Online services for business to connect with us for a range of transactions on multiple devices using Secure mail. Read our list of Secure mail topics.

You can select the:

- Lodgments menu to lodge a range of forms and statements with us, including your transfer balance account report (TBAR)
- Accounts and payments menu to access a range of functions including viewing

your accounts and making payment plans
- Profile menu to
  - update an address for your SMSF (postal, business, and email)
  - update your Electronic Service Alias
  - add an authorised contact
  - update and add Financial institution details.

You can also:

- lodge a SMSF regulatory contravention disclosure form
- request SMSF specific advice
- if you make a mistake on your SMSF annual return, lodge an amendment.

You can't lodge your SMSF annual return (SAR) via Online services, but you can view and print your lodgment history.

Access Online services for business and follow the same steps as businesses to login.

SMSF Auditors

For approved SMSF auditors and their staff Online services for business is a secure tool that can be used to:

- lodge new or amended auditor contravention reports (ACRs)
- lodge audit complete advices (ACAs)
- complete and lodge bulk audit complete advices.

Access Online services for business and follow the same steps as businesses to login.

ATO app

- https://www.ato.gov.au/General/Online-services/ATO-app/
- Last modified: 01 Feb 2023
- QC 40996

Use the ATO app to access and manage your tax and super on the go.

On this page

- Download the ATO app
- Using the ATO app
- Help and support
- Trademarks and attributions

Watch: Keep on top of your tax and super with the ATO app

Media: Keep on top of your tax and super with the ATO app
http://tv.ato.gov.au/ato-tv/media?v=bi9or7odg6341i ⧉ (Duration: 00:53)

Download the ATO app

The ATO app is a simple and easy way you can access and manage your tax and super on the go. The ATO app is free to download and use.

As an individual or sole trader, you can quickly access your personal tax and super information in one place. There are also several helpful features and tools you can use.

To use the ATO app, download it from Google Play or the App Store.

GET IT ON Google Play   Download on the App Store

Supported devices

The ATO app is compatible with most phones and tablets using:

- iOS and iPadOS 15 or later
- Android 8 or later.

From 1 July 2023 the ATO app will not support Android 8 or 9.

Find out more about ATO app system support and permissions.

Using the ATO app

The ATO app has a range of features and tools to help you keep on top of your tax and super. To take advantage of all the available features and personalise your experience, link your myGov account to the ATO.

From your mobile device, you will be able to access:

- Quick login
- Your tax return for 2021–22
- myDeductions
- Super
- Key dates for lodgments and payments
- View your tax accounts
- Employment income and super
- My personal details
- Registered agent details
- Tax withheld calculator
- ABN lookup tool
- Business performance check

Quick login

For quick access to your account, you can set up a log in using your mobile device's security features like face and fingerprint recognition. You will need to have a myGov account and link it to the ATO to access this feature.

Your tax return for 2021-22

Follow your tax return from start to finish. Using this feature, you can easily:

- check pre-fill information we receive from third parties and work out if you're ready to lodge
- view the options available to prepare and lodge your tax return
- check the progress of your tax return
- view the outcome of your return
- download and view your notice of assessment.

myDeductions

Whether you lodge your own tax return or use a tax agent, the [myDeductions](#) tool can help you keep and organise your tax records.

Throughout the year it's a fast, easy way to capture information on the go. Once you finalise your records for your tax return, you can:

- email your data either to yourself or to your tax agent
- upload your data to pre-fill your tax return whether you self-prepare or use a tax agent.

You can access myDeductions from the quick link on the ATO app home screen without the need to login. This is the screen you see when you first open the app.

Records you add are stored locally on your device and are only sent to us if you upload your completed records to your tax return. You should back-up your data regularly in case your device is broken, lost or stolen as this isn't an automatic process.

Super

The ATO app allows you to keep track of your super. It is secure and you can quickly and easily:

- view a list of all your super accounts, including accounts that you may be unaware of or have lost
- explore account balances and view super information and actions that are personalised to your circumstances
- access ATO Online to take steps to consolidate eligible accounts (including any ATO-held super) into one account.

Key dates for lodgments and payments

View when your lodgments and payments are due and seamlessly action them in ATO Online.

View your tax accounts

View your tax accounts, including Higher Education Loan Program (HELP) and activity statement accounts. Quickly access transactions, payment plan details and make payments in ATO Online.

Employment income and super

View the details your employer reports to us, including the date they report this information. Such as, your income, tax withheld and super contributions.

My personal details

Find your tax file number easily. You can also access ATO Online to keep your key personal and business details up to date.

Registered agent details

Check the details of your registered agent and communication preferences.

Tax withheld calculator

You can use the Tax withheld calculator to easily check how much tax should be withheld from salary or wages.

ABN lookup tool

Use the ABN lookup tool to search for a business's ABN and view other public information about the business. For example, you can check that the business you're purchasing goods from is registered for GST so you can claim GST credits.

Business performance check

Use the business performance check tool to compare the performance of your business to other small businesses in the same industry. The business performance check tool:

- uses annual small business benchmark data from over 100 different business types
- can estimate annual performance based on as little as one month's data (the more data, the better accuracy)
- allows you to compare the cost of goods sold and expenses with similar businesses
- provides financial performance ratios including ability to manage debt commitments and working capital
- compares subsequent reports in the tool with previous financial results to monitor any variations in performance.

Help and support

If you're having trouble with the ATO app, use our Help and support for online

[services](#) to find troubleshooting information for known issues or errors.

Trademarks and attributions

Android, Google Play and the Google Play logo are trademarks of Google LLC.

Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries and regions. App Store is a service mark of Apple Inc.

Authorised by the Australian Government, Canberra

myDeductions

- https://www.ato.gov.au/General/Online-services/ATO-app/myDeductions/
- Last modified: 17 Oct 2022
- QC 52615

In the ATO app, myDeductions is a free to record-keeping tool that makes it easier to keep records in one place.

On this page

- [Download the ATO app](#)
- [Record keeping with myDeductions](#)
- [Using myDeductions at tax time](#)

Watch: A quick demonstration of myDeductions

Media: A quick demonstration of myDeductions
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiubgosm84⧉ (Duration: 01:09)

Download the ATO app

Using the ATO makes it easier and more convenient to keep records in one place, including photos of your receipts and invoices. Individuals can record of their expenses. Sole traders can record expenses and income.

To use the myDeductions record-keeping tool:

- download the [ATO app](#) to your smart device
- if you have not logged into the ATO app, myDeductions can be accessed from the quick link on the ATO app home screen, this is the screen you see when you first open the app
- if you have logged into the ATO app, you can find myDeductions by selecting

the More button and then selecting myDeductions
- step through and choose whether you'd like to use the tool as an individual (generally or as an employee), as a sole trader (business) or both.

Records you add are stored locally on your device. You should back up your data to a separate location regularly using the Backup feature in myDeductions in case your device is broken, lost or stolen as this isn't an automatic process.

Record keeping with myDeductions

As an individual or employee, you can:

- use the myDeductions tool to keep records of your
  - work-related expenses (such as vehicle trips you make)
  - general expenses (such as the cost of managing your tax affairs or gifts and donations you make)
- upload these records at tax time to make lodging your tax return easier.

As a sole trader, you can:

- use the myDeductions tool to keep records of your
  - business income
  - business expenses
- upload your records at tax time to make lodging your tax return easier
- share your data by emailing it to your registered tax agent.

If you're a sole trader with a primary production business or personal services income you:

- can record your business income and expenses
- can share your records on myDeductions by emailing it to your registered tax agent
- shouldn't upload your records to prefill your tax return.

To share your records via email using an iPhone or iPad (iOS), you will need to have the Apple Mail app installed on your device.

Using myDeductions at tax time

Whether you lodge your own tax return or use a tax agent, Using myDeductions can help you organise and keep your tax records.

When you are ready to prepare your tax return you can:

- email your records, to either
  - yourself
  - your tax agent
- upload your records to us to be ready to pre-fill your tax return, then either
  - you can lodge your tax return
  - your tax agent can access the records you upload through their practice management software.

If you download the ATO app and use the myDeductions tool:

- Only record your information on a single device throughout the year, because you can't consolidate sets of records and you can only upload once per financial year.
- Multiple people can't use one device.
- Backup your data to a separate location regularly in case your device is broken, lost, stolen, or before you choose to update to a new smart device.

Access Manager

- https://www.ato.gov.au/General/Online-services/Access-Manager/
- Last modified: 01 Dec 2022
- QC 40982

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
How to use Access Manager to notify us of your hosted SBR-enabled software services.

About Access Manager

- https://www.ato.gov.au/General/Online-services/Access-Manager/About-Access-Manager/
- Last modified: 01 Dec 2022

- QC 71002

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

On this page

- [Access Manager for ATO online services](#)
- [Log in to Access Manager](#)
- [Access Manager through RAM](#)
- [Responsibilities when using Access Manager](#)

Access Manager for ATO online services

Access Manager is used to [manage access and permissions](#) for ATO online services, including:

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

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

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 [myGovID](#)
- to be the [principal authority or authorisation administrator](#) in [Relationship Authorisation Manager (RAM)](#) .

Log in to Access Manager

Access Manager through RAM

[Relationship Access 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 myGovID and RAM
- always keep your myGovID 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:

1. Select the user.
2. Select View or Modify
3. 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 do not 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 myGovID and RAM
- always keep your myGovID secure and not share it with others
- not disclose your myGovID password or share it with others.

By providing others with access to secure business information through myGovID 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 the 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 your 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 myGovID
- 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.

Access Manager permissions

- https://www.ato.gov.au/General/Online-services/Access-Manager/Access-Manager-permissions/
- Last modified: 01 Dec 2022
- QC 71003

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

On this page

- Assign and manage permissions
- Permissions for business and tax professionals
- Permissions for superannuation services
- Permissions for government partner agencies

Assign and manage permissions

Assign and manage permissions for our online services.

Assign access and permissions

To assign permissions to authorised users:

1. Select Manage permissions.
2. Select the user.
3. Select the relevant permissions or Select all and Clear all buttons above the list.
4. Select Save.

Copy permissions

To copy permissions from one user to another:

1. Select Manage permissions.
2. Select Copy permissions.
3. Select the user from the drop-down menu that you want to copy the permissions for. Don't copy permissions from an authorised user with full access, as this may cause an error.
4. Select the user that you want to copy the permissions to (you can select one or multiple users).
5. Select Save.

Disable or change user access

To disable or change the status of an account:

1. Select the Active or Disabled button. If Disabled is selected, the user won't be able to log in to Access Manager or any of our online services. A disabled account can be reactivated by selecting the Active button

2. Select Save.

Remove user access

To remove a user's access:

1. Select Manage permissions.
2. Select the user then select Remove account. If removed, the user won't be able to log in to Access Manager or our online services. A removed account can be restored and made active.
3. Select Confirm.

Restore user access

To restore a user's access:

1. Select Manage permissions.
2. Select Past credential holders history.
3. Select Restore for the relevant user.
4. Select Confirm.
5. Select the restored user in the table page.
6. Select Active against the Account status.
7. Select Save.

View user past credentials

To view when a user was removed or restored:

1. Select Manage permissions.
2. Select Past credential holders history.
3. Select the user.
4. Select Close.

View Access history report

The Access history report includes the date and time the user logged in to an online service. You can view one or all authorised users' accesses.

For registered agents, the report also lists the clients who have been accessed.

To view the Access history report:

1. Select Manage permissions.
2. Select either
    1. the user (for one user) then Access history report
    2. Access history report – all users (for all users).

3. Type the date and time range, then select Search.
4. Select Export to download the report as a CSV file.

View Update history report

The 'Update history report' shows when an authorisation was created. This report can only display information for a single user.

To view the Update history report:

1. Select Manage permissions.
2. Select the user.
3. Select Update history report.
4. Type the date and time range then select Search.
5. Select Export to download the report as a CSV file.

Definition of column headings in the permission tables

Category – the category which the permissions are grouped.

Permission/s required – the Access Manager permission required for a user to complete the activity or form in the online service.

Activity or form – the activity or function the permission gives access to. For example, the 'FBT return' form is used in the SBR channel, while 'Update business registration details' is an activity available through Online services for business and the ABR.

Transaction – used to control different levels of access for each transaction. For example, in relation to an activity statement:

- View – view a lodged activity statement
- Prepare – enter data for an activity statement but not lodge
- Lodge – submit an activity statement to the ATO
- Revise – update a previously lodged activity statement.

Online services – the online service the permission applies to. Some permissions give access to multiple online services. For example, 'View business registration details' gives access to that function in both Online services for business and the ABR.

Notes – Described restrictions or special considerations relevant to the permission.

Permissions for business and tax professionals

Permissions that apply to business and tax professionals in Access Manager and which online service they provide access to.

The permissions in the following table apply to:

- business – the business itself
- business to business – a business acting on behalf of another business using the business appointment's function
- registered tax and BAS agents with a client in focus.

Table 1: Category – Accounts and payments

Activity or form	Permissions required	Transaction	Online services	Notes
Account Summary	Account Details	View	OSB OSFA	n/a
Tax Accounts	Account Details	View	OSB OSFA	n/a
Superfund Administration Account	SoA	View	OSB OSFA	Limited to ABNs belonging to SoA with APRA funds, RSA providers, EPSSS or businesses linked to them
Refunds	Refund request Action own mail	Add / Update	OSB OSFA	n/a
Transfer Requests	Transfer request Action own mail	Add / Update	OSB OSFA	Non-BAS agent functionality
Payments	Account Details Make payments Financial and payment details	View Add / Update Add / Update	OSB OSFA SBR	n/a
Payment Arrangements	Payment plans Account Details Make Payments	Add / Update	OSB OSFA SBR	Includes Add / Update financial and payment details

Table 2: Category – Lodgment

Activity or form	Permissions required	Transaction	Online services	Notes
Activity	Activity	View	OSB	n/a

Statements	Statement Registration Account Details	Prepare Lodge Revise View	OSFA SBR	
Annual Investment Income Report	Annual Investment Income Report	Prepare Lodge	OSB OSFA SBR	n/a
Attribution managed investment trust return	Attribution managed investment trust return	Prepare Lodge	SBR	n/a
Certificate of Coverage request	Certificate of Coverage request	View Prepare Lodge Revise	OSB OSFA SBR	n/a
Closely held trust beneficiary reports Includes TFN Report and TFN Withholding report	Closely held trust beneficiary reports	Prepare Lodge	SBR	Non-BAS agent functionality Includes TFN Report and TFN Withholding report
Common Reporting Standard (CRS) statement	Common Reporting Standard (CRS) statement	Prepare Lodge	OSB OSFA SBR	Access is not available using Business Appointments Non-BAS agent functionality
Community Housing Annual Report	Community Housing Annual Report	Prepare Lodge	OSB	Access is not available using Business Appointments
Consolidated group notification	Consolidated group notification	Prepare Lodge	SBR	Non-BAS agent functionality
Country by Country Report	Country by Country Report	Prepare Lodge	OSB OSFA SBR	n/a
Direct Debit	Direct Debit	Prepare Lodge	SBR	Excluding BAS agents

Duty Free Operator return	Excise Forms	View Prepare Lodge Revise	OSB	n/a
Early stage innovation company report	Early stage innovation company report	Prepare Lodge	OSB OSFA	n/a
Electronic Payments systems transaction report	Electronic Payments systems transaction report	Prepare Lodge	OSB OSFA	n/a
Electronic Portability Form	Electronic Portability Form	View	OSFA	n/a
Employee Commencement form	Employee Commencement form	View Prepare Lodge	OSB OSFA SBR	Employee commencement form access is required for stapled super fund requests
Employee Share Scheme annual report	Employee Share Scheme annual report	Prepare Lodge	OSB OSFA	n/a
Excise Claim	Excise Forms	View Prepare, Lodge Revise	OSB	n/a
Excise Duty Return	Excise Forms	View Prepare Lodge Revise	OSB OSFA	n/a
FBT Return	FBT Return	Prepare Lodge	SBR	Fringe benefits tax
Foreign Account Tax Compliance Act (FATCA)	Foreign Account Tax Compliance Act (FATCA)	Prepare Lodge	OSB SBR OSFA	n/a
FTCN	Excise Forms Financial and	View Prepare	OSB OSFA	n/a

	payment details	Lodge Add / Update		
Further Information	Objection and private ruling applications View and action own mail	Prepare Lodge View	OSB OSFA	Access is not available using Business Appointments
General Purpose Financial statements	General Purpose Financial statements	Prepare Lodge	OSB OSFA	Non BAS agent functionality
GST Property credits	Accounts	View	OSB OSFA	n/a
Income tax history and copy of return	Account	View	OSB	n/a
Merchants Point of Sale transactions reporting	Merchants point of sale transactions reporting	View Prepare Lodge	OSB OSFA	n/a
Non-Individual income tax return	Non-Individual income tax return	Prepare Lodge	SBR	Non-BAS agent functionality
Objection and Private Ruling	Objection and private ruling applications View and action own mail	Prepare Lodge View	OSB OSFA	Access is not available using Business Appointments
PAYG Payment Summary	PAYG Payment Summary	Prepare Lodge	SBR	Access is not available using Business Appointments
Petroleum Stewardship of Oil Claim	Excise Forms Financial and payment details	View Prepare Lodge Add / Update	OSB OSFA	n/a
Private Health	Private Health	Prepare	OSB	Available to

Insurance Report	Insurance Report	Lodge	OSFA	ABNs belonging to a private health insurance fund
Reported Transactions	Accounts	View	OSB OSFA	n/a
Statement of Tax	Account	View	OSB OSFA	n/a
Taxable Payment Annual Report	Taxable Payment Annual Report	Prepare, Lodge	OSB OSFA	Access is not available using Business Appointments
Transfer balance Account Report	Transfer balance Account Report	Prepare Lodge	OSB OSFA SBR	Non BAS agent functionality
TFN declaration	TFN declaration	Prepare Lodge	OSB OSFA SBR	Access is not available using Business Appointments
Transfer of shares and units	Transfer of shares and units	Prepare Lodge	OSB OSFA	Non-BAS agent functionality

Table 3: Category – Manage Employees

Activity or form	Permissions required	Transaction	Online services	Notes
STP Reporting	Payroll Event	View	OSB OSFA SBR	n/a
STP Deferrals and Exemptions	Payroll Event	Lodge	OSB OSFA SBR	n/a
Small Business Super Clearing House	Small Business Super Clearing House	View Lodge	OSB OSFA	n/a
COVID-19	Registrations Financial and	View Lodge	OSB OSFA	n/a

	payment details	Add / Update		

Table 4: Category – Communication

Activity or form	Permissions required	Transaction	Online services	Notes
Secure Mail	View and action own mail	View	OSB OSFA	Access is not available using Business Appointments
Secure Mail Admin access	Access other users mail	View	OSB OSFA	Access is not available using Business Appointments
History	Communication History	View	OSB OSFA	n/a
Preferences	Registration	View	OSB	n/a
Your Dealings	n/a	Default view	OSB OSFA	n/a

Table 5: Category – Profile

Activity or form	Permissions required	Transaction	Online services	Notes
Business Details	Registration	View Add / Update	OSB OSFA ABR	n/a
Business Addresses	Registration	View Add / Update	OSB OSFA	n/a
Email addresses	Registration	View Add / Update	OSB OSFA	n/a
Authorised contacts	Registration	View Add / Update	OSB OSFA	n/a

Agent	Registration	View	OSB	n/a
Associates	Registration	View	OSB OSFA ABR	n/a
Financial Institution Details	Registration Financial and Payment Details	View Add/Update	OSB OSFA SBR	n/a
Manage Card Details	Financial and Payment Details	Add/Update	OSB OSFA	n/a
Tax Registration	Tax roles	View Add / Update	OSB OSFA ABR	n/a

Tax practice administration

The permissions in the table below are available if an ABN is associated with a registered agent number (RAN). Access can be granted to:

- the client – give users access to your clients as a registered agent
- a RAN – only applies to users who have been given access to the RAN within Access Manager
- restricted clients – clients can be set as restricted clients in Access Manager and only users with permission to access a restricted client or all restricted clients can access these.

Table 6: Permissions for tax practice administration

Activity or form	Permissions required	Transaction	Online services	Notes
Access to all restricted Clients	Access to all restricted Clients	None	OSFA SBR ABR	n/a
Trust account details	Trust account details	None	SBR	Includes EFT reconciliation reports and lodgement performance reports
View Agent reports including usage reports	View Agent reports	None	SBR	This includes Usage reports

Client List - bulk download	Client List - bulk download	None	OSFA	n/a
Reports	Reports	View	OSFA SBR	Includes client list reports and client lodgment reports
Clients	Clients	View Add Update	OSFA SBR ABR	n/a

Permissions for superannuation services

The permissions in the table below apply to:

- Australian Prudential Regulation Authority (APRA) funds
- government non-regulated funds
- self-managed super funds (SMSFs)
- retirement savings account (RSA) providers
- exempt public sector superannuation schemes (EPSSS)
- life insurance providers (LIP).

Permissions also apply to businesses linked to, or tax agents representing the services above.

Table 7: Permissions for superannuation services

Activity or form	Permissions required	Transaction	Online services	Notes
EmployerTICK	Employer TFN integrity check	Validate	SBR	EmployerTICK Available to employers, or a business linked to an employer
Self-Managed Superfund search and verify members	SMSF – Search and verify members	Verify	SBR	SVS Limited to APRA funds, government non-regulated funds and SMSFs
Self-Managed	SMSF – Verification	Verify	SBR	SVS

Superfund verification service	service for rollovers/contributions			Limited to APRA funds, government non-regulated funds, employers and SMSFs
Superstream FVS FIA template	Super products – List	View	SBR	FVS Limited to APRA funds, RSA providers, EPSSS or businesses linked to them
Superstream FVS	Super products details – View	View	SBR	FVS Limited to APRA funds, RSA providers, EPSSS or businesses linked to them
Superstream FVS	Super products details – Lodge	Lodge	SBR	FVS Limited to APRA funds, RSA providers, EPSSS or businesses linked to them
Superstream SuperTick	Super – TFN integrity check (SuperTICK)	View Validate	SBR	SuperTICK Limited to APRA funds, RSA providers or businesses linked to them
Superstream MATS	Super – Member information service (View)	View	SBR	MATS Limited to APRA funds, RSA providers or businesses linked to them
Superstream	Super – Member	View	SBR	MAAS

MAAS	account services (View)			
Superstream MAAS	Super – Member account services (Lodge and update)	Lodge and Update	SBR	MAAS
Superstream SMAT access	SuperMatch 2 Initiate ATO monies Transfer	View Update	SBR	Limited to APRA funds, RSA providers or businesses linked to them
Superstream	SuperMatch2 Retrieve super details	View	SBR	Limited to APRA funds, RSA providers or businesses linked to them
SMSF Annual Return	SMSF Annual Return	Prepare Lodge	SBR	SMSF
Super Guarantee Charge Statement	Super Guarantee Charge Statement	Prepare Lodge	OSB OSFA	n/a
Super Compassionate Release of superannuation	Super Compassionate Release of superannuation	View	OSB OSFA	n/a
Superannuation Contribution report	n/a	n/a	n/a	Non BAS agent functionality
Member Contribution Statement	Member Contribution Statement	Prepare Lodge	OSB	n/a
Audit Completion Advice	SMSF Auditor reporting	Prepare Lodge	OSB	SMSF Auditors
Auditor Contravention Report	SMSF Auditor reporting	Prepare Lodge	OSB	SMSF Auditors
Transfer balance	Transfer balance Account Report	Prepare Lodge	OSB OSFA	Limited to APRA funds,

Account Report				SBR	SMSFs, RSA providers, EPSSS and LIPs Non BAS agent functionality

Permissions for government partner agencies

The permissions in the following table are available to ABNs which we have set up in Access Manager with access to the phoenix watch list or as a:

- government partner agency
- state and territory government agency.

Table 8: Permissions for government partner agencies

Activity or form	Permissions required	Transaction	Online services	Notes
ABR API Agency	ABRAPIAgency	View	ABR	Govt
Partner Agency	Partner Agency	View	ABR	Govt
Partner Agency Search	Partner Agency Search	View	ABR	Govt
State and Territory government Agency	Gov.State Territory	View Lodge	OSB	Govt

Access Manager for business

- https://www.ato.gov.au/General/Online-services/Access-Manager/Access-Manager-for-business/
- Last modified: 01 Dec 2022
- QC 71004

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

On this page

- [Appoint a business and assign permissions](#)
- [Modify permissions for an appointed business](#)
- [Remove a business appointment](#)
- [Assign access to authorised users for a principal business](#)
- [Modify or remove access to authorised users for a principal business](#)

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 do not 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 do not 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.

Access Manager for tax professionals

- https://www.ato.gov.au/General/Online-services/Access-Manager/Access-Manager-for-tax-professionals/
- Last modified: 01 Dec 2022
- QC 71005

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

On this page

- Assign a RAN
- Assign permissions to access your clients
- Assign permissions to restricted clients
- Manage access to your client list

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
    1. To allow access – select View at Client list – bulk download
    2. To remove access – deselect View at Client list – bulk download.

4. Select Save.

Access Manager for business software users

- https://www.ato.gov.au/General/Online-services/Access-Manager/Access-Manager-for-business-software-users/
- Last modified: 01 Dec 2022
- QC 71006

How to use Access Manager to notify us of your hosted SBR-enabled software services.

On this page

- Notify us of your hosted SBR software
- Remove a notification
- Add or remove a software ID

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 advise of these details when you purchase or subscribe to their service).

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

1. Select My hosted SBR software services.
2. Select Notify the ATO of your hosted service.
3. Search for a digital service provider in the list, or search by typing the ABN or name.
4. Select the ABN link of your digital service provider.
5. Enter the software ID provided to you by your digital service provider and select Next.
6. 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 what was 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 software service:

1. Select My hosted SBR software services. Your current digital service providers will display.
2. Select the ABN link of the digital service provider to modify or remove the notification.
3. Select Remove notification
4. 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 for other users in your business or remove a software ID which is no longer used or is invalid. To do this:

1. Select My hosted SBR software services. Your current digital service providers will display.
2. Select the ABN link of a digital service provider to modify or remove the notification.
3. Type the new or corrected software IDs in the Add Software IDs fields.
4. Select Remove heading to remove unwanted software IDs.
5. Select Next to review your changes.
6. Select Save.

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

ATO digital wholesale services

- https://www.ato.gov.au/General/Online-services/ATO-digital-wholesale-services/
- Last modified: 09 Apr 2020
- QC 62006

Many businesses use software packages to help manage their operations. Some software packages exchange data with us seamlessly via ATO developed application programming interfaces (APIs). For example, APIs allow users to submit business activity statement (BAS) and Single Touch Payroll (STP) information directly to us.

We support DSPs by offering a wide range of digital wholesale services through Standard Business Reporting (SBR). DSPs may provide a wide range of

capabilities within their software, such as:

- accounting
- tax agent practice management
- bookkeeping
- payroll
- STP sending service providers
- superannuation gateways
- SMSF management.

DSPs must meet a set of security requirements before they can use our digital wholesale services. This ensures their systems have adequate security measures in place to protect the confidentially of taxpayer information and integrity of ATO systems.

See also:

- Requirements for digital service providers⬚
- Online services for DSPs⬚
- Your practice – DSPs

Digital service provider Operational Security Framework

- https://www.ato.gov.au/General/Online-services/ATO-digital-wholesale-services/Digital-service-provider-Operational-Framework/
- Last modified: 02 Jun 2022
- QC 62007

The DSP Operational Security Framework⬚ outlines what is required of digital service providers⬚ (DSPs) that access and use our digital wholesale services⬚ via Standard Business Reporting (SBR).

The DSP Operational Security Framework requirements reduce the risk of identity theft, tax refund fraud and system hacks. Controls to protect the confidentiality and integrity of client data, include but are not limited to:

- data encryption
- unique user logins – a requirement of all software products connected to our digital services
- multi-factor authentication – an additional step, using two different types of ID to verify the user account
- audit logging to capture user access and transactions
- entity validation which confirms the registered entity using software is a legitimate entity with legitimate contact details

- data is hosted in Australia by default – limiting risk of unauthorised access or inappropriate disclosure due to cross-jurisdictional policies.

We will update and change the DSP requirements to mitigate any emerging risks in our digital environment.

Users will not notice most of these security controls in their software, except for unique client logins and multi-factor authentication.

Multi-factor authentication is mandatory for most software products, namely cloud-based or online software, and is recommended for all other types.

We are committed to protecting your data, and we will restrict or de-whitelist DSP products (PDF, 303KB) ⬇ that fail to conform to the DSP Operational Security Framework.

A range of services and support to help you stay up to date with the latest news and information can be found at Your practice – DSPs.

AUSid

- https://www.ato.gov.au/General/Online-services/AUSid/
- Last modified: 01 Aug 2022
- QC 52648

Set up AUSid for overseas limited registered entities accessing Online services for non-residents to report and pay GST.

On this page

- About AUSid
- Creating an AUSid account
- Troubleshooting
- Contact us
- Terms and conditions of use
- Privacy notice

About AUSid

AUSid is a secure way to access our Online services for non-residents ↗.

Online services for non-residents is for individuals associated with overseas limited registered entities that use simplified GST registration. It allows them to register, report and pay goods and services tax GST in Australia.

Creating an AUSid account

To use AUSid:

- [Step 1: Download and install AUSid](#) on your desktop.
- [Step 2: Create an AUSid account](#).
- [Step 3: Log in to Online services for non-residents](#) securely on any browser.

Step 1: Download and install AUSid

To download and install AUSid, choose your desktop device's operating system:

- [Windows](#) (EXE, 47.2MB) – Windows users (Windows 8 and above) can also download AUSid directly from the [Microsoft store](#)⬏
- [MacOS](#) (DMG, 61MB).

If you have trouble installing or using AUSid, check with your IT systems administrator that:

- the Windows 10 store is enabled and accessible
- you have the correct permissions to install AUSid on your computer
- you have given 'https://ausid.ato.gov.au' access to your network (whitelisted). You must do this so AUSid can receive and process login requests
- your Wi-Fi or router allows access to 'https://ausid.ato.gov.au'. Look up how to log in and change configuration for your specific router.

Alternatively, you can try installing AUSid on a computer that isn't part of this network and service your login requests from there.

Step 2: Create an AUSid account

To create your AUSid account, open the AUSid application installed on your device and enter the following details:

- username (must be unique)
- password
- given name (first name)
- family name (surname)
- date of birth
- email address (must be unique).

Step 3: Log in to Online services for non-residents

1. Go to [Online services for non-residents](#)⬏ and select Login.
2. Enter your username and select Submit.
3. Open your AUSid application and enter your password to accept the request.

Once you've logged in to Online services for non-residents using your AUSid, you can [register for simplified GST](#).

We recommend that more than one individual has an AUSid and is listed in the simplified GST registration as an authorised user. This ensures you and authorised staff can report and pay GST for your business.

Each individual needs their own AUSid, it must not be shared with others.

Troubleshooting

You can troubleshoot most AUSid issues such as:

- [Forgot your password](#)
- [Use your AUSid on another device](#)
- [Error 31207 (500)](#)
- [Request help](#)
- [How to use Online services for non-residents](#)

Forgot your password

If you have forgotten your password, you can still access your AUSid account:

1. Open AUSid on the original device used to setup your AUSid account.
2. Select Manage your details.
3. Select Forgotten your password.
4. Follow the onscreen instructions to reset your password.

Use your AUSid on another device

To access your existing AUSid on a new device:

1. Open AUSid on the original device used to setup your AUSid account.
2. Select Manage your details.
3. Display the unique Recovery code.
4. Open AUSid on your new device.
5. Select I already have an account.
6. Enter the Recovery code with your account details.
7. Enter your new password.

If you have an older version, you may need to download and install AUSid again to use these functions. Don't uninstall your existing AUSid application.

Error 31207 (500)

If you get 'error 31207 (500) System unavailable':

1. Open AUSid on the original device used to setup your AUSid account.
2. Select Manage your details.
3. Select Forgotten your password.
4. Follow the onscreen instructions to reset your password.

If you don't know the registered AUSid details or don't have access to the email address registered for your AUSid, you must create a new AUSid.

Your new AUSid can be linked to your business by an existing AUSid holder or by contacting us for assistance.

Request help

If you need help accessing your AUSid account or managing authorisations to

access your simplified GST registration, see How to use Online services for non-residents.

If you're still having issues, contact us. Tell us the reason for your request and your AUSid account details, including:

- the reason for your request, for example
  - I need to add or remove AUSid authorised users to access my simplified GST registration
  - I forgot my AUSid password
  - I need to set up my AUSid account on another device
  - I have deleted my AUSid application and want to access my AUSid account on an existing device
  - I can't access my AUSid account.

- your Australian reference number (ARN)
  - If you haven't registered for simplified GST, you won't have an ARN and we can't prove your identity.

- information to verify your registration, or you're an authorised contact for simplified GST registration
  - your AUSid username or email address
  - given name (first name)
  - family name (surname)
  - date of birth
  - business name
  - any 3 of the following details from your simplified GST registration
    - address
    - reference number from an ATO-generated letter
    - date of registration
    - payment details (amount and date of payment).

How to use Online services for non-residents

If you are a non-resident and need more help using functions in Online services for non-residents, you can find more details on simplified GST registration for assistance.

To keep your account up to date and secure, make sure you register for simplified GST and review your authorised contacts to add, remove or link to your AUSid and simplified GST accounts.

Contact us

For AUSid enquiries or technical support:

- email us at AUSidsupport@ato.gov.au. If you need technical support, you must provide

- the step in the process you were trying to action, including the date and time the error occurred, the error code or screen message, screen shots and what you were trying to action
- your contact information, including the email address you used for registration.

- phone us on +61 2 6216 1111. Our business hours are between 8:00 am and 5:00 pm, Monday to Friday (except for national public holidays).

  Tell the operator to connect you to 1300 146 094, then wait until you hear instructions to enter 118#. You will be transferred to an officer who can help you
- phone our free interpreting service on +61 3 9268 8332 and ask to be connected to 1300 146 094.

Terms and conditions of use

The AUSid system terms and conditions may change over time. They are current at the time they are published on this page.

By using the AUSid system, you agree to be bound by the AUSid terms and conditions current at each time of use.

AUSid security credential

An AUSid security credential is all login details and personal information that may be used to access AUSid accounts, for example a username and password.

Access and data security – account-holder responsibilities

To keep your account secure, you must:

- always keep your AUSid security credential secure – don't disclose or share it with others
- ensure that no other person has access to your AUSid security credential
- log out from the AUSid system when you're not using it
- lock or secure your computer or device if its shared, or left unattended
- only use your AUSid account in accordance with the AUSid terms and conditions, for purposes you're authorised for at the relevant time of access
- notify the ATO immediately if you suspect that the security of your AUSid account has been compromised
- not use your AUSid account for any unlawful or improper purpose.

Suspension or cancellation of AUSid account

The ATO retains the right to suspend or cancel your AUSid account at any time where it suspects any of the following has occurred:

- there has been unauthorised access of your AUSid account
- your AUSid account has been used for a purpose for which you weren't

properly authorised at the relevant time of access

- your AUSid account is being used for any unlawful or improper purpose.

Warranties and indemnity

The ATO gives no express or implied warranties in relation to the AUSid system or its use.

All statutory warranties are, to the fullest extent permitted by law, expressly excluded. You warrant that:

- the personal information supplied by you in connection with your AUSid account is true and accurate
- you have read and understood the AUSid terms and conditions
- you have complied with the AUSid terms and conditions current at each time of use
- your use of the AUSid system is properly authorised at the relevant time of access
- agree to indemnify the ATO against any loss or claim arising from either
  - your non-compliance with the AUSid terms and conditions
  - acting in a manner or for a purpose for which you are not authorised at the relevant time of access.

Except that your liability will be reduced to the extent that any wilful, negligent, or unlawful act or omission by the ATO contributed to the loss or claim.

Privacy notice

We collect personal information about you when you use this application. This personal information may include details that identify an individual.

This notice explains how we manage the personal information we collect.

We will collect your name, date of birth, email address and username for the purposes of creating and managing your AUSid account. Your AUSid account can be used as an authentication credential to register for and access your simplified GST registration.

If we don't collect this information you won't be able to create an AUSid account. We may disclose the personal information to other agencies where we're authorised or required to do so by law.

The ATO's privacy policy contains important information about your privacy, including how you can access and seek correction of information we hold about you, how to make a complaint if you think we have breached the Australian Privacy Principles and how we will deal with any privacy complaints.

Identity security and scams

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/
- Last modified: 27 Jul 2021
- QC 49586

Your personal information is an important part of your identity. Make sure you keep it safe.

Scammers might try to trick you into giving your information away or paying out money.

Find out more:

- Verify or report a scam
- Scam alerts
- Scam data
- Protect your information
- Help for identity theft

See also:

- Online security
- IDCARE⬚

Verify or report a scam

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Verify-or-report-a-scam/
- Last modified: 01 Feb 2023
- QC 40945

Check or report an ATO impersonation scam and get to know some warning signs of phone, email and SMS tax scams.

On this page

- Verify a scam
- Report a scam
- Warning signs of phone, email and SMS tax scams

Verify a scam

Scams trick you into paying money or giving out your personal information.

Scammers often pretend to be from trusted organisations like the ATO.

We will sometimes contact you by phone, email, SMS and post. If you're not sure whether it's really us, do not reply. You should phone us on 1800 008 540 to check.

Report a scam

If you have been affected by an ATO impersonation scam, you can report it to us.

This information contains instructions on how to report a scam:

- Phone scams
- Email and SMS scams
- Social media scams

Information about scams and how to report a scam is also available in Easy Read format and other languages.

Phone scams

If you received a scam phone call and you did pay money or provide sensitive personal identifying information to the scammer, phone us on 1800 008 540 to report it.

You should also:

- make an official report to your local police
- contact your bank or financial institution if you provided your credit card or bank details to the scammer
- contact the bank you made the payment to and lodge a fraud report.

If you received a scam phone call and did not pay money or provide sensitive personal identifying information to the scammer, you should still report the scam to us. You can use our online Report a scam form.

Email and SMS scams

If you received a scam email or SMS, do not click on any links, open any attachments or download any files.

If you did pay money or provide sensitive personal identifying information to the scammer, phone us on 1800 008 540 to report it.

You should also:

- make an official report to your local police
- contact your bank or financial institution if you provided your credit card or bank details to the scammer
- contact the bank you made the payment to and lodge a fraud report.

If you did not pay money or provide sensitive personal identifying information to the scammer, you should still report the scam to us. You can either:

- forward the entire email to ReportEmailFraud@ato.gov.au
- take a screenshot of the SMS and email it to ReportEmailFraud@ato.gov.au

Delete the email or SMS after reporting it to us.

You can report other types of scams to Scamwatch⃗, or contact the Australian Cyber Security Centre⃗ to report cybercrime.

Social media scams

We've recently observed several social media accounts impersonating us.

If you are approached by a social media account that is impersonating us, do not engage with it. Take a screenshot of the account or post and email it to ReportEmailFraud@ato.gov.au.

Warning signs of tax scams

Scammers are constantly looking for new ways to trick people.

There are some common warning signs in the information below to help you check if you have been contacted by a scammer or by us:

- Phone scams
- Emails and SMS scams
- Social media scams

You can also find out about current scams we're aware of.

Phone scams

Some of the common features of phone scams are described in the table below. Use this information to help you identify if a phone call claiming to be from us is a scam.

How to identify phone scams

What scammers may do	Our approach
Scammers may threaten you with immediate arrest. They do this to make you afraid or panic and stop you thinking clearly.	We will never threaten you with immediate arrest.
Scammers may: - demand you pay right now and keep you on the phone line until you pay - say that if you hang up there will be a warrant for your arrest.	We will never demand you stay on the line until a payment is made.

They use these threats to make you pay by the end of the call.	
Scammers may: • send unsolicited pre-recorded messages (robocalls) to your phone • leave messages on your voicemail asking you to call back.	We will never send unsolicited pre-recorded messages to your phone. Only phone us on a number you have looked up yourself. Do not call the number given to you in the call or voicemail.
Scammers may use technology to show real ATO or Australian phone numbers in the caller ID or call log.	Calls from the ATO do not show a number. They will show as No Caller ID. Only phone us on a number you have looked up yourself. Do not call the number shown in caller ID or in your call log.
Scammers may tell you that your tax file number (TFN) has been cancelled or suspended due to money laundering or other criminal activity. They will say you either need to: • pay money to avoid being arrested or sent to court • transfer your money to a safe bank account to protect your TFN from future misuse.	We do not cancel TFNs. Always check that you're dealing with a legitimate agency before providing any information. If you're not sure, hang up. You can phone us to check. Only call us on a number you have looked up yourself. Do not call the number given to you in the call or voicemail.
Scammers may refuse to allow you to speak with a trusted adviser or your regular tax agent. They do this to prevent anyone from telling you that it's a scam and stopping you from paying.	We will never prevent you from discussing your tax affairs with your trusted adviser or agent.
Scammers may attempt to make a conference call with a fake tax professional, law enforcement officer or another official. They do this to make the call seem	We will never make a conference call with a third party, such as your tax agent or law enforcement. Know your tax affairs – you can log into ATO online services through myGov to

real and increase your fear, but the second person will be another scammer.	check your tax affairs at any time. You can also contact your tax agent or the ATO.
Scammers may request payment by iTunes, Google Play, STEAM or other vouchers. These vouchers can be easily purchased and sold globally. They are an untraceable form of currency (money).	We will never request payment of a debt through iTunes, Google Play, STEAM or other vouchers. You can find out about legitimate ways to make payments to the ATO.
Scammers may request payment by JB hi-fi, Myer, Woolworths or other retail gift cards. These gift cards can be easily purchased and are an untraceable form of currency (money).	We will never request payment of a debt through JB hi-fi, Myer, Woolworths or other retail gift cards. You can find out about legitimate ways to make payments to the ATO.
Scammers may request payment by Bitcoin or other cryptocurrencies, either directly or deposited into an ATM. This currency is difficult to trace and offers more anonymity.	We do not accept payment in cryptocurrency. You can find out about legitimate ways to make payments to the ATO.
Scammers may request that you pay money into a personal bank account. This could be an Australian-based account established by scammers. The money moves accounts until it is sent offshore.	We will only ever ask you to pay a tax debt into a bank account held by the Reserve Bank of Australia. Check online to see that the Bank-State-Branch (BSB) number is one for the Reserve Bank of Australia. You can find out about legitimate ways to make payments to the ATO.
Scammers may request that you pay through cardless cash ATM withdrawals.	We will never ask you to pay a tax debt through a cardless cash ATM withdrawal. You can find out about legitimate ways to make payments to the ATO.
Scammers may request you pay money through offshore wire transfer (where the scammers are located).	We will not request payment of a debt through offshore wire transfer. You can find out about legitimate ways

	to make payments to the ATO.
Scammers may request that you pay money through a cash delivery either through a courier service or made in person at a pre-determined public location.	We will never ask you to pay through a cash delivery. You can find out about legitimate ways to make payments to the ATO.
Scammers may request that you pay a fee to receive a tax refund. They will usually ask you to pay the fee using your credit card and then steal your credit card details.	We will never ask you to pay a fee to receive a refund. Do not provide your credit card details to anyone unless you trust the person you're dealing with and they genuinely require these details.
Scammers may offer payment arrangements if you can't pay the full amount. This is done to increase instances of payments and the total amount paid.	Before you enter a payment arrangement, contact us or your tax agent using a number you have looked up yourself.

Emails and SMS scams

Some of the common features of email and SMS scams are described in the table below. Use this information to help you identify and respond to scams.

How to identify and respond to email or SMS scams

What scammers may do	Our approach
Scammers may ask you to provide your personal identifying and financial institution details through a return SMS or email to receive a refund.	We may use SMS or email to ask you to contact us, but we will never send an unsolicited message asking you to return personal identifying information through these channels. Protect your personal information. Do not give out your tax file number (TFN), date of birth or bank details unless you trust the person you are dealing with and they genuinely require these details.
Scammers may request that you click on a link in an SMS or email to log on to an online service.	We will never send you an email or SMS with a link to log in to our online services.

Scammers create fake log on pages that look real. They use these sites to steal your credentials (usernames and passwords).	
Scammers may ask you to click on a link in an SMS or email to download forms or attachments.

They may do this to install malicious software on your computer to gain access to your data. Or they may keep your personal identifying or financial information for future misuse. | Be careful when downloading attachments or clicking links, even if the message seems to come from someone you know. |

Social media scams

Some of the common features of social media tax scams are described in the table below. Use this information to help you identify and respond to scams.

How to identify and respond to social media scams

What scammers may do	Our approach
Scammers may create fake social media accounts and send requests to you asking for personal identifying information or payments.

When you comment on our social media posts, they may respond and offer to provide support, asking you to direct message them.

We're actively working to combat these scams as they arise. | We are on Facebook ⤢, Twitter ⤢ and LinkedIn ⤢, but we will never use these social media platforms to ask you to provide personal information or documentation or ask you to make payments.

You can tell it's genuinely our Facebook account as our page has a blue verification tick to the right of our name (Australian Taxation Office). Our Twitter account has a grey tick next to our username (@ato_gov_au).

You can verify us on LinkedIn by ensuring that the account you're engaging with:
- has the official ATO logo and organisational name next to the message. Beware of slight variations of our name, like 'Australia' rather than 'Australian' Taxation Office
- has been posting on LinkedIn actively, and has been doing so for a long time
- only provides you with email addresses that end with '.gov.au'
- doesn't have typos or grammatical errors in its messages |

| | • has a large number of account followers.

We will never interact with you through Whatsapp.

Never [share information](#) such as your TFN, myGov or bank account details on social media, even through private message. |

Authorised by the Australian Government, Canberra.

Scam alerts

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Scam-alerts/
- Last modified: 31 Jan 2023
- QC 53447

Find information and examples on the latest tax and super-related ATO impersonation scams.

On this page

- [Scam advice](#)
- [Latest scam alerts](#)
- [Previous scam alerts](#)

Scam advice

Be wary of emails, phone calls and text messages claiming to be from the ATO.

If you think a phone call, SMS, voicemail, email or interaction on social media claiming to be from the ATO is not genuine, do not engage with it. You should either:

- phone us on 1800 008 540
- go to [Verify or report a scam](#) to see how to spot and report a scam.

Stay up to date on the latest scam alerts by [subscribing to our general email updates](#). You will also receive updates on all new general content on our website.

Latest scam alerts

- [January 2023 – ATO social media impersonation accounts scam](#)
- [July 2022 – tax refund SMS scams](#)

- [June 2022 – 2022 tax lodgment email scam](#)
- [April 2022 – fake TFN/ABN application scams](#)
- [February 2022 SMS and email scams – cryptocurrency](#)
- [November 2021 phone and email scams – superannuation](#)
- [November 2021 phone scam – fake tax debt](#)
- [October 2021 email scam – update your financial information](#)
- [August 2021 phone scam – new payment methods](#)

January 2023 – ATO social media impersonation accounts scam

We're seeing an increase in fake social media accounts impersonating the ATO, our employees and senior executive staff across Facebook, Twitter, TikTok, Instagram and other platforms.

These fake accounts ask users that interact with the ATO to send them a direct message so they can help with their enquiry. The people behind these fake accounts are trying to steal your personal information, including phone numbers, email addresses and bank account information.

Our only official accounts are on [Facebook](#)⬀, [Twitter](#)⬀ and [LinkedIn](#)⬀.

The best way to verify that it's really the ATO is to:

- check how many people follow the account. Our verified Facebook and LinkedIn accounts have over 200,000 followers, and our Twitter account has over 65,000 followers
- check activity on the accounts. Our social media channels have been operating for around 10 years – if it's a newly created account, or only has a few posts, it's not us
- look for the grey tick next to our username (@ato_gov_au) on Twitter and the blue tick next to our name (Australian Taxation Office) on Facebook
- make sure any email addresses provided to you end with '.gov.au'.

The images below show examples of what impersonation accounts might look like.

If you're approached by an impersonation account, do not engage with them. Take a screenshot of the account, email the information to ReportEmailFraud@ato.gov.au and block the account through the social media platform's reporting function.

July 2022 – tax refund SMS scams

We're concerned about a high volume of SMS scams pretending to be from the ATO.

These scams tell you that you're owed an income tax repayment and ask you to click a hyperlink and complete a form.

Clicking the link takes you to a fake ATO webpage that asks for your personal identifying information, including your credit card details.

If you receive an SMS like this, don't click on any links. Report the scam to us.

The image below shows one example of what this scam can look like.
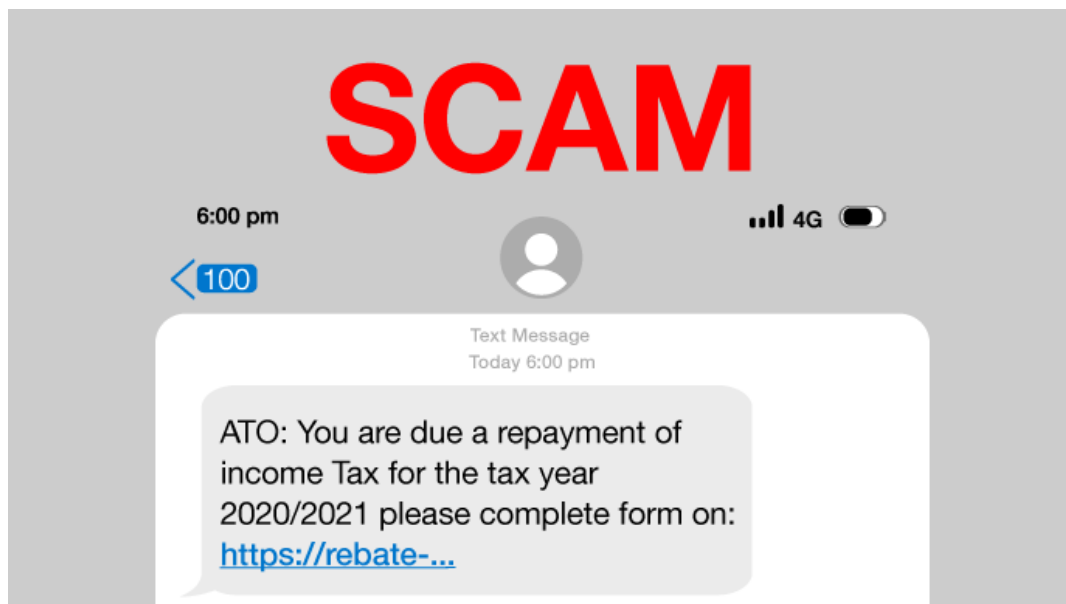
The real ATO will never send you an SMS with a link to log in to our online services. We'll also never ask for your credit card details.

If you're ever unsure whether it's really the ATO, don't reply. Phone us on 1800 008 540 to check.

June 2022 – 2022 tax lodgment email scam

We're seeing an increase in email phishing scams claiming to be from the ATO.

These scams tell people their '2022 tax lodgment' has been received. The email asks them to open an attachment to sign a document and complete their 'to do list details'.

Opening the attachment takes you to a fake Microsoft login page designed to steal your login details. Entering your password could give the scammer access to your Microsoft account, allowing them to reset your passwords for other accounts like banking and online shopping.

If you get an email like this, don't click on any links or open any attachments. Forward the email to ReportEmailFraud@ato.gov.au, and then delete it.

The images below are examples of the format this scam can take.

SCAM

Your 2022 lodgment receipt

Dear Taxpayer,

- Your 2022 lodgment was received on 30 May 2022 at 02.29pm AEST.
- Your receipt number is 7022180418610.

Thanks for your lodgment.

It takes about 3 weeks to process your lodgment. **Please do not call us during this time as we cannot speed up this process.** Check on the to do list to sign on the attached demanded documents in **Section C**.
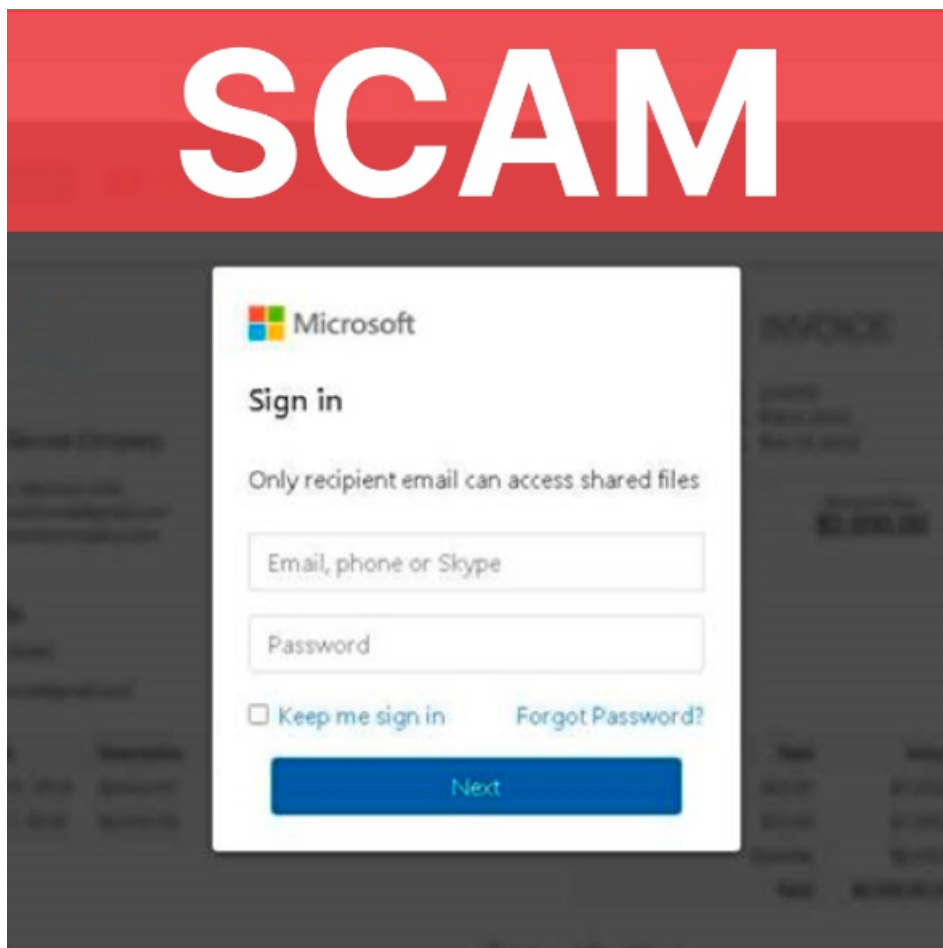
The real ATO will never send you an email or SMS with a link to log in to our online services.

And while we may use email or SMS to ask you to contact us, we will never send an unsolicited message asking you to return personal identifying information through these channels.

Remember to [protect your passwords](#) and update them regularly.

April 2022 – fake TFN/ABN application scams

We're seeing an increase in scams involving fake tax file number (TFN) applications.

These scams tell people they can help them get a TFN for a fee. But instead of delivering this service, these fraudulent websites steal the person's money and personal information.

These scams are often advertised on social media platforms like Facebook, Twitter and Instagram.

Applying for a TFN is free. Find out how you can [apply for a TFN](#).

If you're applying for a TFN through a tax agent, always check they are registered with the [Tax Practitioners Board](#)⬀.

The same goes for Australian business number (ABN) applications – never give out your personal information unless you're sure of who you're dealing with.

February 2022 SMS and email scams – cryptocurrency

We're receiving reports of cryptocurrency scams.

Scammers pretending to be from the ATO are telling people they are suspected of being involved in cryptocurrency tax evasion. They are then asking them to 'connect their wallet' and provide detailed information via a link.

If you receive an SMS or email like this, don't click on the link. It will take you to a fake myGov log on page, designed to steal your personal information.

The image below is one example of the format this scam can take.
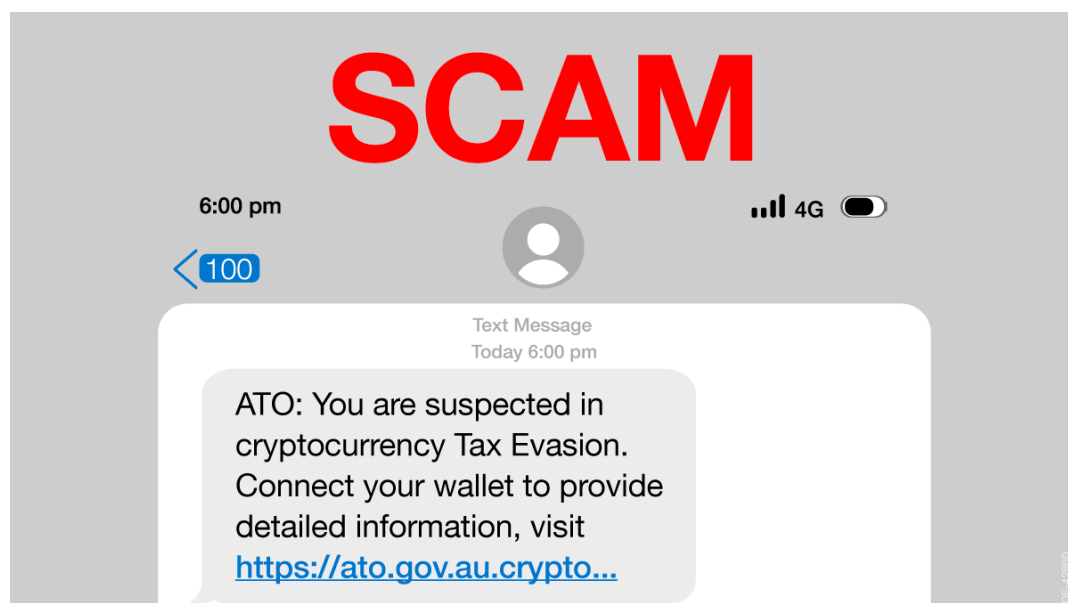
The real ATO will never send you an SMS or email with a link to log in to our online services.

And while we may use SMS or email to ask you to contact us, we will never ask you to return personal information through these channels.

If you're ever unsure whether it's really the ATO, don't reply. Phone us on 1800 008 540 to check.

November 2021 phone and email scams – superannuation

We're concerned about an increase in scams involving fake superannuation investments.

Scammers are phoning and emailing people, pretending to be financial advisers or super experts. They are encouraging people to invest their super in a supposedly high performing self-managed super fund (SMSF).

These scammers will start by asking you for some information and may ask you to do a super comparison online. They are likely to be persistent and may contact you multiple times.

Sometimes, they will fraudulently use the name and Australian Financial Service Licence (AFSL) of a real business and set up a fake website to appear legitimate.

They will tell you there is no need for you to engage directly with the ATO, ASIC or any other tax or super professional.

If you agree to invest, they will transfer your super into bank accounts they control and disappear with it.

Even if you don't agree to invest, if you provide them with enough personal information they may use this to transfer your super from your existing account without you knowing, ultimately stealing your super savings.

Always check who you are dealing with before providing any personal or financial information.

Be cautious about anyone who contacts you with unsolicited financial advice:

1. Check ASIC's [Professional registers](#) to make sure they are licensed professionals.
2. Conduct an online search to independently verify their identity and to see if there are any reviews or indications of scam activity related to their website, email address or phone number.
3. If in doubt check with another registered tax professional.

If you receive an SMS, email or letters from the ATO about an SMSF that you did not establish contact us on 13 10 20 immediately.

ASIC has more information about [how to recognise and report super scams](#).

November 2021 phone scam – fake tax debt

We're reminding people to look out for phone scams about fake tax debts.

Scammers pretending to be from the ATO are calling people and telling them they have a tax debt that they need to pay straight away.

We will use phone, email and SMS to contact you. But we will never:

- send a pre-recorded message to your phone
- threaten you with immediate arrest
- demand payment through unusual methods like gift cards or payments to personal bank accounts
- insist you stay on the line until a payment is made.

Phone calls from the real ATO will show up as 'No caller ID' on your phone.

If you're ever unsure whether it's really the ATO, do not reply. You should phone us

on 1800 008 540 to check.

We have more information on how you can [identify and report tax and super scams](#).

October 2021 email scam – update your financial information

We're receiving reports about a new email scam impersonating the ATO.

Scammers are sending emails telling people they will receive a tax refund. They ask them to update their financial information on an attached form to process the refund.

The image below is an example of the scam email.

Subject: Secure mail from Australian Taxation Office (ATO-1F2N7)

Australian Taxation Office
22-October-2021

According to our calculation, you should receive a refund of $892.80
In order for us to process the refund, you will need to update your financial information.
What to do next:
Fill and submit the attached form.

Thanks,
Customer Services Team

Message ID: ATO2BQ8
Please do not reply to this email as this inbox is not monitored.
You can update your preferences or unsubscribe at any time.

If you receive an email like this, delete it. Don't open the attachment or click on any links.

If you receive a message from the ATO asking for your personal information, phone us on 1800 008 540 to make sure it's legitimate. If you think it's fraudulent, report it by sending an email to reportemailfraud@ato.gov.au.

You should never give out your personal information unless you are sure of who you are dealing with.

August 2021 phone scam – new payment methods

We're receiving reports of scammers demanding money by new methods.

This includes things like:

- 'cardless cash' ATM withdrawals
- retail gift cards, such as JB hi-fi, Myer and Woolworths
- courier services who collect the cash payments
- cash delivery made in person at a pre-determined public location.

Scammers are trying to trick people into making payments by pretending to be from the ATO and other agencies, such as the Australian Federal Police.

They might tell you that your TFN has been suspended or compromised due to money laundering or other illegal activity, or that you owe a debt.

The real ATO will never demand payment by these methods. You should always check legitimate ways to pay a tax debt on our website before making a payment.

If you have paid money to a scammer through one of the methods listed above or are concerned about your personal safety, report it to your local police straight away and specify all the details.

We also strongly encourage you to contact your financial institution immediately. In some cases, they may be able to stop a transaction or close your account if the scammer has your account details.

And remember, if you're ever unsure whether an ATO contact is genuine, hang up and phone us on 1800 008 540 to check.

See How to pay for legitimate ways to pay a tax debt.

Previous scam alerts

- May 2021 email scam – update your myGovID details
- February 2021 phone scam – suspended TFN
- October 2020 email scam – JobKeeper and backing business investment claims
- September 2020 phone and SMS scams – fake tax debt
- July 2020 SMS and email scams– verify your myGov details
- June 2020 phone scam – threatening arrest and requesting personal details

May 2021 email scam – update your myGovID details

We're receiving reports of a new email scam that asks people to update their myGov or myGovID details.

Scammers pretending to be from the 'myGov customer care team' are sending emails telling people they need to verify their identity by clicking on a link.

The image below is one example of the format this scam can take.
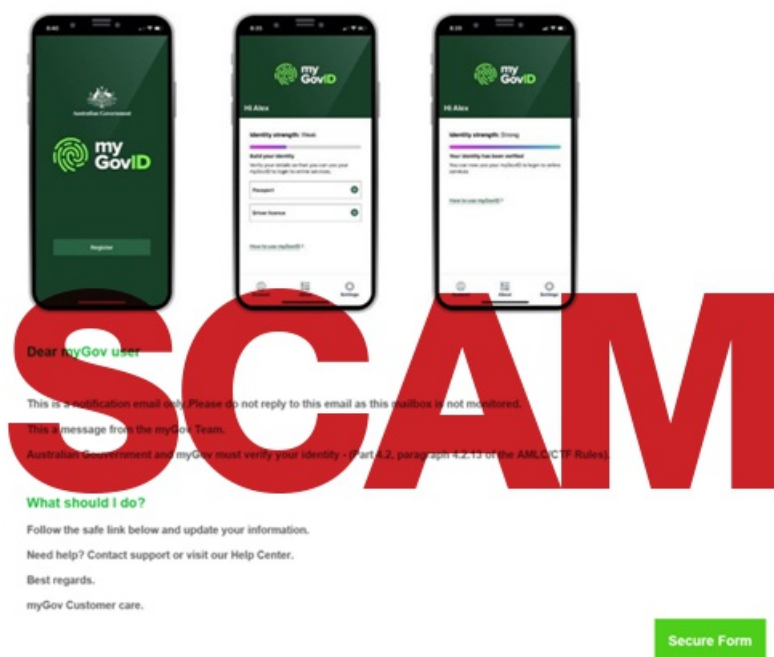
Don't click any links and don't provide the information requested.

The link goes to a fake myGov logon page designed to steal your personal information, including your passport and driver's licence details.

You will get email or SMS notifications from myGov whenever there are new messages in your myGov Inbox. However, these messages will never include a link to log on to your myGov account. Always access our online services directly via one of the following:

- my.gov.au
- ato.gov.au
- the [ATO app](#).

When downloading the myGovID app, make sure it's from either the Apple App Store or the Google Play Store.

If you receive an SMS or email that looks like it's from myGov, but it contains a link or appears suspicious, you can report it to ScamWatch. If you have clicked on a link or provided your personal information, you can contact Services Australia's Scams and Identity Theft Helpdesk on 1800 941 126.

February 2021 phone scam – suspended TFN

We are receiving increasing reports of people losing money to automated phone scams.

Scammers pretending to be from the ATO tell people their tax file number (TFN) has either been:

- suspended due to illegal activity
- compromised by a scammer.

They request the call recipient either pay a fine to release their TFN or transfer all bank funds into a holding account to protect it from future misuse.

We:

- do not suspend TFNs
- will never request you pay a fine or transfer money in order to protect your TFN pending legal action.

Phone calls from us do not show a number on caller ID. We will never send unsolicited pre-recorded messages to your phone.

If you receive a phone call like this, hang up and do not provide the information requested.

If you're unsure whether an ATO contact is genuine, phone us on 1800 008 540 to check.

An example of this type of scam is available below:

- [Audio recording of suspended TFN scam (MP3, 82KB)](#) ⬇

October 2020 email scam – JobKeeper and backing business investment claims

We are receiving reports of email scams about claims for JobKeeper and Backing Business Investment. The fake emails say we are investigating your claims. They ask you to provide valuable personal information, including copies of your driver's licence and Medicare card.

The image below is one example of an email scam currently circulating.

Do not provide the information requested, do not click on any links and delete the email straight away.

Coronavirus JobKeeper Payments

Australian Government
Australian Taxation Office

~~SCAM~~

We are currently checking all claims made through the Coronavirus JobKeeper Payments / Backing Business Incentive Scheme.

In order to complete all checks we kindly ask you to reply to this e-mail with the following information:

- A clear, high-resolution photo (scan) of your driver's licence (front & back)

- A clear, high-resolution photo (scan) of your Medicare Card (front & back)

If you receive a message from the ATO asking for your personal information, phone us on 1800 008 540 to make sure it's legitimate. If you think it's fraudulent, report it by sending an email to reportemailfraud@ato.gov.au.

You should never give out your personal information unless you are sure of who you are dealing with.

September 2020 phone and SMS scams – fake tax debt

We are concerned about the increasing number of people paying fake tax debt scammers.

Scammers pretending to be from the ATO are contacting members of the community, telling them that they have a tax debt and that if they do not pay it straight away they will be arrested.

These scammers will often request payment through unusual methods, such as cryptocurrency, pre-paid credit cards or gift cards. They will try to keep people on the line until they have paid.

If you receive a phone call, text message or voicemail like this, don't send payment or provide any personal information. Hang up and delete the message.

We will never:

- threaten you with immediate arrest
- demand payment through unusual methods.

If you are not sure if it's the ATO contacting you, phone us on 1800 008 540 to check.

It's also a good idea to know your tax affairs. You can:

- log in to ATO online services through myGov to check your individual tax affairs
- log in to Online services for business to check your business tax affairs
- contact your tax or BAS agent
- contact us.

July 2020 SMS and email scams – verify your myGov details

We are receiving increasing reports of several myGov-related SMS and email scams. These scams look like they have come from a myGov or ATO email address. They also might appear in your legitimate ATO or myGov SMS message thread.

The image below is one example of an SMS scam currently circulating.

Don't click any links and don't provide the information requested.
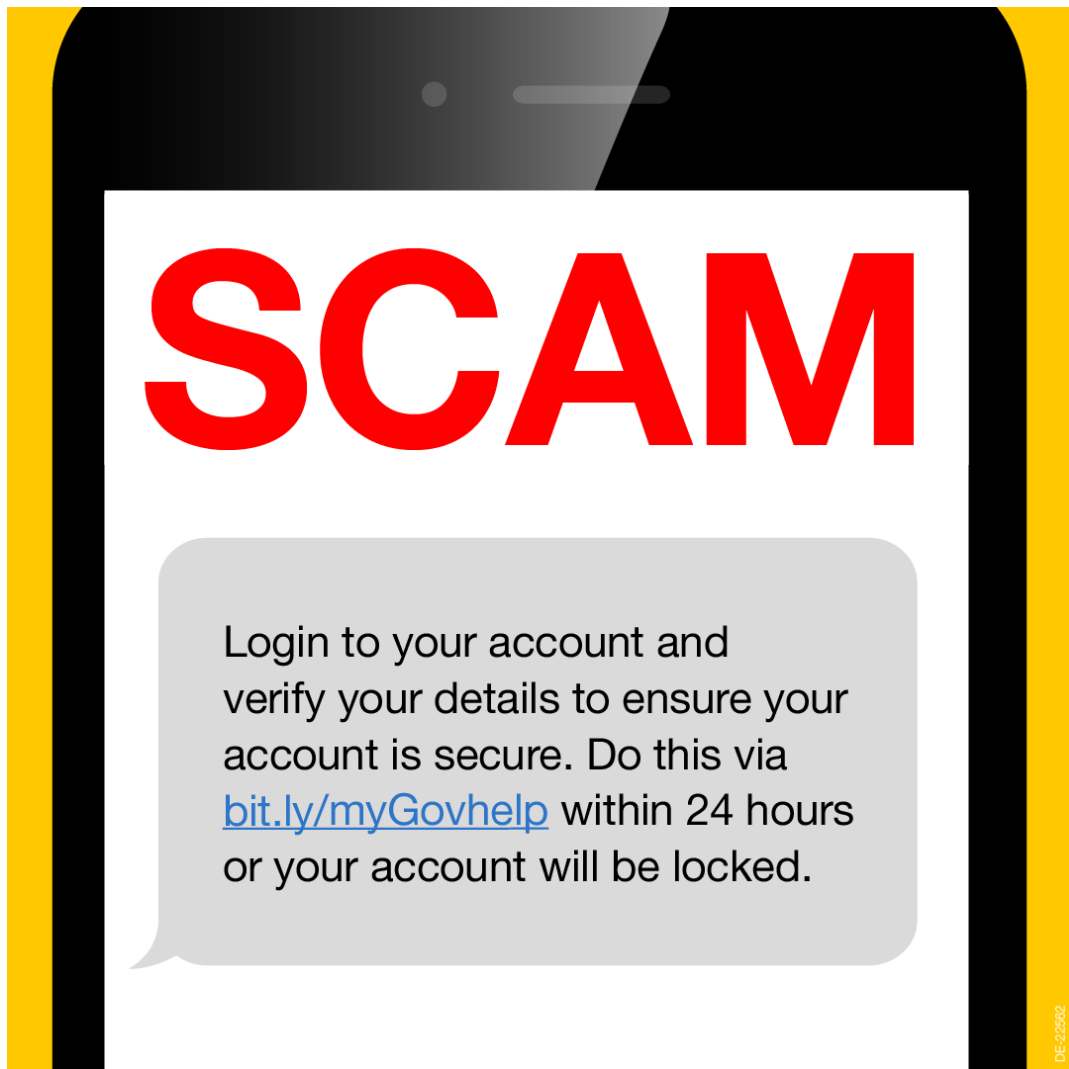
You will get email or SMS notifications from myGov when there are new messages in your myGov Inbox. However, these messages will never include a link to log on to your myGov account. Always access our online services directly via one of the following:

- my.gov.au
- ato.gov.au
- the [ATO app](#).

All online management of your personal tax affairs should be done in ATO online services, accessed through your genuine myGov account. Any communications containing your personal information, such as your tax file number (TFN), will be sent to your myGov Inbox, not your email account.

You can make accessing your myGov account more secure by opting to receive a security code via SMS. It's a quick and secure way to sign in to access ATO online services.

If you receive an SMS or email from the ATO that you think is fraudulent, report it by sending an email to reportemailfraud@ato.gov.au.

If you receive an SMS or email that looks like it's from myGov but it contains a link or appears suspicious, email reportascam@servicesaustralia.gov.au.

If you have clicked on a link or provided your personal information, contact Services Australia on 1800 941 126.

June 2020 phone scam – threatening arrest and requesting personal details

We are receiving reports of scammers sending members of the public automated phone calls pretending to be from the ATO, as well as other government agencies including Services Australia and the Department of Legal Services.

These automated calls claim their TFN has been suspended and that there is a legal case against their name. The call tells people they must contact the caller by pressing '1' or they will be referred to the court and arrested.

If the person presses '1' and makes contact with the scammer they are typically told that their TFN had been suspended due to money laundering or other suspicious or fraudulent activity and that there are several allegations against them. They are then asked to provide:

- the last four digits of their TFN
- their address
- their date of birth
- the name of their bank account
- the approximate amount of money in the account/s.

Sometimes the scammer will 'transfer' the victim to the 'police' where they're told a case has been filed against them and they will be arrested unless they pay.

Sometimes they advise the victim will receive mail to their home or that their bank accounts will be closed.

If you receive this call, hang up and do not provide the information requested. We will never:

- send unsolicited pre-recorded messages to your phone
- threaten you with immediate arrest.

If you are not sure whether an ATO call is legitimate, hang up and phone us on 1800 008 540 to check.

Scam data

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Scam-data/
- Last modified: 23 Jan 2023
- QC 56423

Find the latest data on ATO impersonation scams.

On this page

- Latest scam data
- Monthly comparison
- Payment methods

Latest scam data

In December 2022, we received 1,165 reports of ATO impersonation scams.

We did not receive any reports of payments made to scammers during this month. Find out how to protect your personal information, and verify or report a scam.

Monthly comparison

Table 1: Monthly comparison of reported ATO impersonation scams

Date	SMS	Email	Phone	Social
Dec 22	510	573	66	14
Nov 22	370	1,007	69	22
Oct 22	393	1,191	94	32
Sep 22	548	569	151	3
Aug 22	666	828	80	5

July 22	321	489	197	2
Jun 22	127	460	544	2
May 22	244	288	414	0
Apr 22	293	342	360	1
Mar 22	64	418	479	5
Feb 22	244	1,072	496	3
Jan 22	405	178	357	0
Dec 21	368	184	231	4

The Social category includes scams that occur through platforms like Facebook, Twitter, LinkedIn and WhatsApp.

Payment methods

Table 2: ATO impersonation scammer payment methods, December 2022

Payment method	Bank transfer
Amount paid	$0
People paid	0

For legitimate ways to pay your tax debt, see [How to pay](#).

Protect your information

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Protect-your-information/
- Last modified: 27 Jul 2021
- QC 19354

Your personal information is an important part of your identity. You need to keep it safe.

To commit identity crime, thieves only need some basic details such as your name, date of birth, address, myGov details or tax file number (TFN).

They can use this information to:

- access your bank account and buy things using your credit card
- access your myGov account to steal your tax refund
- steal your superannuation
- make fraudulent self-managed super fund (SMSF) registrations
- apply for a government benefit
- sell your house
- commit refund fraud in your name
- take over your business and submit adjustments for business activity statements (BAS) that you have lodged before
- sell your identity to organised crime groups on the dark web or via other means.

If identity thieves steal your identity, it can take a long time to fix. It may be difficult for you to:

- get a job or loan
- rent a house
- apply for government services or benefits.

If you suspect your personal information, such as your TFN, has been stolen, misused or compromised, phone us as soon as possible on 1800 467 033 between 8.00am and 6.00pm Monday to Friday. We will investigate and can place extra protection on your ATO account.

Watch our video *Be aware of what you share* to see how to identify an illegitimate request for information.

Media: Be aware of what you share
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiub15jkgg (Duration: 1:00)

Our approach to identity crime

We use intelligent systems to automatically detect tax returns suspected of being fraudulently lodged using another person's identity. These systems help us stop incorrect, invalid or fraudulent refunds before they are paid.

Our Client Identity Support Centre supports taxpayers who had their identities stolen, misused or compromised. We provide information, advice and assistance to help taxpayers re-establish their identities.

We are also a partner agency in a whole-of-government approach to reducing identity crime. The National Identity Security Strategy, supported by the Attorney-General's Department, works to combat the misuse of stolen or assumed identities.

Find out about:

- [How to protect yourself](#)
- [How to protect your business](#)
- [Security advice for tax professionals](#)

See also:

- [Help for identity theft](#)
- [Online security](#)
- [Lost or stolen TFN](#)
- [IDCARE](#)↗
- [Australian Cyber Security Centre](#)↗

How to protect yourself

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Protect-your-information/How-to-protect-yourself/
- Last modified: 27 Jul 2021
- QC 50498

Be aware of what you share – your personal information is valuable.

On this page

- [Know what to protect](#)
- [Be aware of what you share](#)
- [Protect your TFN](#)
- [Protect your passwords](#)
- [Protect your computer and phone](#)
- [Only use a registered tax agent](#)
- [Enrol your voiceprint with us](#)
- [Complete our online security self-assessment](#)
- [Data breaches](#)

Know what to protect

Your personal information is the key to your identity. It includes your:

- full name
- date of birth
- current address
- bank account numbers
- credit card details
- tax file number (TFN)
- myGov and ATO online login details

- driver's licence details
- passport details
- passwords.

Watch:

Watch our video *Protect your personal information* to see what you should protect and how.

Media: Protect your personal information
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiubfurqiw (Duration: 1:34)

Be aware of what you share

You should only share your personal information with:

- people you trust
- organisations with a legitimate need for it.

You should treat requests for personal information with caution. Before providing your personal information:

- ask the person who contacts you for some identity credentials
- check the person's credentials by calling their employer using a phone number you have looked up yourself.

Be careful what you discuss in public. Identity thieves can listen to your phone calls and conversations with friends.

Store personal information in a secure place

Avoid carrying your birth certificate or passport in a wallet or handbag unless you need them.

Do not store personal information, such as TFNs, passwords, or personal identification numbers (PINs), in your mobile phone.

Never leave personal papers or spare house keys in the glove box of your car.

Lock your mailbox, and if you receive large volumes of mail consider using a post office box.

Shred or destroy documents that contain any personal information.

Make sure electronic documents containing personal information are secure. Protect these files with passwords and encryption or use a trusted data vault website.

Protect yourself from scams

Scams can trick you into providing either money or personal information.

Scammers can be believable and will sometimes quote personal information to sound authentic.

If someone asks for your bank or personal details, money, refunds or gifts, be cautious. Consider the possibility that it may be a scam – even if you think you know the person well.

See also:

- [Verify or report a scam](#)
- [Scam alerts](#)
- [Scamwatch](#)↗

Social media – be aware of what you share

Scammers can use information you post on social media to steal your identity.

To help protect yourself:

- do not share personal information, such as your TFN, myGov or bank account details, on social media
- understand who can see your information and consider setting your profile to 'private'
- be cautious about which friend requests you accept
- do not post information that would make you or your family vulnerable, such as birth dates, addresses or photos that contain personal identifying information.

We are on Facebook, Twitter, and LinkedIn, but we will never use these social media platforms to ask you for payment or personal identifiable information.

Protect your TFN

We give each taxpayer a unique TFN. You use your TFN and other personal information to lodge tax returns and other tax forms.

To protect your identity:

- Only give your TFN to organisations or people who have a legitimate need for it, such as your tax agent, current employer or bank.
- Destroy or delete your TFN from any documents you are throwing away.
- Don't share your online passwords with others.
- Never send your TFN, password or other sensitive information in emails.

Protect your passwords

Never share your passwords.

You should also consider updating them regularly.

Avoid writing down your passwords and leaving them in your purse, wallet or in a file on your computer.

Consider using a passphrase that includes numbers and symbols which is easy for you to remember but difficult for someone to guess. For example, P!ne@pp1eP!zz@

See also:

- [Online security](#)

Protect your computer and phone

Computer

Scammers can use viruses, malware and programs to access or steal your personal information. To help protect yourself against digital attacks, you should:

- keep your anti-virus, malware, and spyware protection software up to date
- make sure you have a firewall and it is up to date
- avoid entering personal information or passwords into unsecure websites
- be careful when downloading attachments or clicking links in emails, even if the message seems to come from someone you know
- avoid using public computers (for example, in libraries or internet cafés) to access your personal information.

Phone

Stop people from accessing information on your phone by:

- using a password, PIN, or screen lock
- keeping your operating software up to date
- only connecting to secure (encrypted) wireless networks from trusted sources
- considering installing anti-virus software on your phone.

Be aware that older phones can be more susceptible to hacking attempts or other illegal activity.

Only use a registered tax agent

Make sure that any tax agent you use is registered. You can do this by checking the [Tax Practitioners Board](#)⬚ website.

Registered tax agents do not require access to your myGov and ATO online accounts to complete your tax return for you. They have their own systems to do this. Never share your myGov login details with anyone, including your registered tax agent.

And remember, only a registered tax agent can charge you a fee to prepare and lodge your tax return.

Enrol your voiceprint with us

You can now use your voiceprint to verify your identity when you contact us.

Your voiceprint is unique to you. It is the digital representation of the sound, rhythm, physical characteristics and patterns of your voice. Once you've saved it with us, we confirm your identity when you contact us by matching the characteristics of your voice to your voiceprint.

Setting this up will help us to protect your tax account and reduce the chance of scammers accessing it. To enrol, log in to our online services for individuals via the ATO app and follow the prompts.

See also:

- Voice authentication
- ATO app

Complete our online security self-assessment

You can use our online security self-assessment to:

- understand and identify your established online security measures
- identify areas where you can improve your online practices and processes
- get more information and resources to help improve your online security measures.

The assessment is voluntary and anonymous. We do not record your personal information or responses.

Next step:

- Online security self-assessment questionnaire

See also:

- Top cyber security tips for individuals
- Australian Cyber Security Centre

Data breaches

If you are the victim of a data breach and your personal identifying information has been accessed, go to Data breach guidance for individuals.

Find out about:

- How to protect your business
- Security advice for tax professionals
- Help for identity theft

Authorised by the Australian Government, Canberra.

How to protect your business

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Protect-your-information/How-to-protect-your-business/
- Last modified: 27 Jul 2021
- QC 50499

Strong security practices can help you protect your business, staff and client information from identity thieves.

These criminals can get your business and client details by:

- breaking into your business and stealing your records
- taking a photo of your business or employee details
- stealing your passwords, account logins or myGovID details
- obtaining access to your data through legitimate means (for example, an employee targeting vulnerabilities in your systems or security controls)
- using compromised emails with malicious links or programs
- sending emails to phish for information from your business
- exploiting security vulnerabilities in software.

On this page:

- Complete our online security self-assessment
- Know what to protect
- Make sure you have internal controls
- Protect your myGovID

Media: Protect your business against identity crime http://tv.ato.gov.au/ato-tv/media?v=bd1bdiunji3ij9 (Duration: 1:18)

Complete our online security self-assessment

You can use our online security self-assessment questionnaire to:

- understand and identify your established online security measures
- identify areas where you can improve your online practices and processes
- get more information and resources to help improve your online security measures.

The questionnaire is voluntary and anonymous – we don't record any of your personal information.

Next step:

- Online security self-assessment questionnaire

Know what to protect

Identity thieves may target your:

- myGovID
- business activity statements
- employees' personal information
- business records containing personal or business information.

Secure your business premises

It only takes a few moments for thieves to photograph or steal information at your workplace. You can help keep your business, customer and employee information safe by:

- installing physical barriers such as locked doors and windows
- making sure you have appropriate alarm systems in place
- filing documents in lockable storage units.

Secure your systems

To protect yourself and your business from identity thieves, we recommend:

- securing your business files and employee information when they are not in use
- changing all passwords on a regular basis
- making sure all employees log out of systems and lock computers when not in use
- making sure your computers, software and other devices have up-to-date security and anti-virus software.

When sourcing software for your business you may wish to ask vendors how they make sure they are providing secure systems and services. For example:

- Will your data be stored in Australia or overseas?
- What data breach support services do they provide?
- Do they follow the Australian Signals Directorate Essential 8 mitigation strategies ?
- Do they have security certification (ISO27001, iRAP) and what were the outcomes of any assessments?

See also:

- Top cyber security tips for business
- Data breach guidance for businesses
- IDCARE

Make sure you have internal controls

You can protect your business and employees by:

- performing background checks on new employees
- restricting new employees' access to systems and credentials
- being able to track employees' actions when dealing with sensitive and

personal information

- removing access to systems and credentials from employees as soon as they leave your employment.

Protect your myGovID

myGovID uses encryption and cryptographic technology and the security features in your device, such as fingerprint or face, to protect your identity.

If you are aware or suspect that your myGovID has been inappropriately accessed, you need to report this immediately.

Contact the myGovID support line on 1300 287 539 (select option 2 for myGovID enquiries) between 8.00am and 6.00pm Australian Eastern Standard Time (AEST), Monday to Friday.

International callers can contact us by phoning our switchboard on +61 2 6216 1111 between 8.00am to 5.00pm AEST, Monday to Friday, and request your call be transferred to the myGovID support line.

See also:

- [myGovID](#)⤴ for more information and tips about myGovID security and staying safe online

Find out about:

- [Security advice for tax professionals](#)
- [Help for identity theft](#)

Security advice for tax professionals

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Protect-your-information/Security-advice-for-tax-professionals/
- Last modified: 27 Jul 2021
- QC 50500

Criminals may target your practice to steal you or your client's information. They may also use your business to lodge fraudulent claims.

As a tax professional you need to protect your business and client information, including making sure it is safe online.

We recommend you:

- check the proof of identity for all new clients and question any discrepancies
- only lodge for clients whose identity you have confirmed

- make sure your computer security systems are up to date and protected against cyber attacks
- train your staff in the need to, and methods of, securing client information
- make sure your staff understand what is appropriate to discuss on social media or via email.

You should remain vigilant, take precautions, address security, and uphold your client and business privacy by assessing your online practices at least quarterly.

On this page

- Complete our online security self-assessment
- Know what to protect
- Make sure you have internal controls
- Protect your myGovID
- Report fraud
- Data breaches

Complete our online security self-assessment

You can use our online security self-assessment questionnaire to:

- understand and identify your established online security measures
- identify areas where you can improve your online practices and processes
- get more information and resources to help improve your online security measures.

The questionnaire is voluntary and anonymous – we do not record any of your personal information.

Next step:

- Online security self-assessment questionnaire

Know what to protect

Identity thieves may target your:

- myGovID
- business activity statements
- employees' personal information
- business records containing personal or business information.

Secure your business premises

It only takes a few moments for thieves to photograph or steal information at your workplace. You can help keep your business, client and employee information safe by:

- installing physical barriers such as locked doors and windows
- making sure you have appropriate alarm systems in place
- filing documents in lockable storage units.

Secure your systems

To protect yourself and your business from identity thieves, we recommend:

- securing your business files and employee information when they are not in use
- changing all passwords on a regular basis
- making sure all employees log out of systems and lock computers when not in use
- making sure your computers and other devices have up-to-date security and anti-virus software.

When sourcing software for your business, you may wish to ask vendors how they make sure they are providing secure systems and services. For example:

- Will your data be stored in Australia or overseas?
- What data breach support services do they provide?
- Do they follow the [Australian Signals Directorate Essential 8 mitigation strategies](#)?
- Do they have security certification ([ISO27001, iRAP](#)) and what were the outcomes of any assessments?

See also:

- [Fraudulent payment summaries](#)
- [Top cyber security tips for business](#)

Make sure you have internal controls

You can protect your business and employees by:

- performing background checks on new employees
- restricting new employees' access to systems and credentials
- being able to track employees' actions when dealing with sensitive and personal information
- removing access to systems and credentials from employees as soon as they leave your employment.

Protect your myGovID

myGovID uses encryption and cryptographic technology and the security features in your device, such as fingerprint or face, to protect your identity.

If you are aware or suspect someone has inappropriately accessed your personal information in myGovID, you need to report this immediately.

Contact the myGovID support line on 1300 287 539 (option 2) between 8.00am and 6.00pm Australian Eastern Standard Time (AEST), Monday to Friday.

International callers can contact us by phoning our switchboard on +61 2 6216 1111 between 8.00am to 5.00pm AEST, Monday to Friday, and request your call be transferred to the myGovID support line.

See also:

- [myGovID](#)⧉ for more information and tips about myGovID security and staying safe online

Report fraud

Fraud can be the result of many things, including criminals:

- stealing someone's identity to lodge incorrect returns and steal refunds
- obtaining access to your client records to gain information
- impersonating your business to gain a benefit.

To report suspected fraud or criminal activity:

- make a [tip-off](#)
- phone us on 1800 060 062 (between 8.00am and 6.00pm AEST, Monday to Friday).

To reduce the risk of fraud in your practice, we suggest that you:

- always confirm the identity of new clients, especially when they are requesting bulk lodgments or amendments
- restrict access to your systems and records to those with a genuine need
- check existing client records for unusual updates or lodgments
- make sure both the physical and cyber security of your premises is strong, using adequate filing systems and software to protect your client records
- contact the myGovID support line on 1300 287 539 (option 2) between 8.00am and 6.00pm AEST, Monday to Friday if you suspect the misuse of your myGovID.

Data breaches

If you have experienced a data breach in your practice, [data breach guidance for tax professionals](#) outlines the steps you may need to take to secure your client records and protect them against potential refund and superannuation fraud.

See also:

- [IDCARE](#)⧉

Find out about:

- [Help for identity theft](#)

Help for identity theft

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Help-for-identity-theft/
- Last modified: 27 Jul 2021
- QC 49587

If you know or suspect that someone has stolen your tax file number (TFN) or is using your tax-related information illegally, phone us on 1800 467 033 as soon as you can.

Depending on your situation, there are also other actions you can take if you suspect identity theft.

Identity theft – how to get help

Situation	What you should do
You think someone has stolen or misused your TFN, your Australian business number (ABN) or other tax-related information.	Phone us on 1800 467 033, between 8.00am and 6.00pm AEST, Monday to Friday.
You think someone accessed your myGov account, including your linked ATO online services, without your permission.	Phone us on 13 28 61, between 8.00am and 6.00pm AEST, Monday to Friday.
You think someone has inappropriately accessed your personal information in myGovID.	Phone us on 1300 287 539 (select option 2), between 8.00am and 6.00pm AEST, Monday to Friday.
You think someone has inappropriately accessed your business information in Relationship Authorisation Manager (RAM).	Phone us on 1300 287 539 (select option 3), between 8.00am and 6.00pm AEST, Monday to Friday.
You think someone has falsely used your personal information to set up a self-managed super fund (SMSF) under your name or made changes to your existing SMSF to gain access to your superannuation.	Phone us on 1800 467 033, between 8.00am and 6.00pm AEST, Monday to Friday.

You must report all tax-related security issues to us.

You can also report:

- other cybercrime to the Australian Cyber Security Centre via the Cyber Issue Reporting System
- identity theft and fraud to your state or territory police.

On this page

- Help to re-establish your tax identity
- If you hold taxpayer information
- How we respond to identity theft

Help to re-establish your tax identity

If you think someone has stolen or misused your identity, contact our Client Identity Support Centre on 1800 467 033 (between 8.00am and 6.00pm AEST, Monday to Friday).

We will help you establish your tax identity. When you phone us, we'll discuss the identification documents you'll need to provide.

If you think your other personal information was compromised, we recommend you contact IDCARE on 1800 595 160 (between 8.00am and 5.00pm AEST, Monday to Friday). IDCARE provides free advice and confidential support to victims of identity theft.

See also:

- Data breach guidance for individuals

If you hold taxpayer information

If you hold tax or superannuation data (including TFNs) for clients or employees and you are aware (or suspect) the security of this information has been breached, phone our Client Identity Support Centre on 1800 467 033 between 8.00am and 6.00pm AEST, Monday to Friday.

See also

- Data breach guidance for businesses
- Data breach guidance for tax professionals
- Security advice for tax professionals

How we respond to identity theft

The way we respond to identity theft depends on the situation:

- Someone has your TFN
- Monitoring your tax and super account.

Someone has your TFN

If someone has your TFN, you need to tell us and we will check for any unusual or suspicious activity on your account.

If someone uses your TFN, we'll confirm and then correct the details in your account.

This may take longer for more complex tax affairs.

We will then discuss any further action taken with you.

Monitoring your tax and super account

If your TFN has been compromised, we can help protect your tax and super account by monitoring your records before automatic processing of any lodgments or claims.

If an activity looks suspicious, we may contact you to confirm the details before processing commences.

The security measures we apply will remain on your file until we determine that there is no further risk.

See also

- [Protect your information](#)
- [How to protect yourself](#)
- [Lost or stolen TFN](#)
- [Verify or report a scam](#)
- [Online security](#)
- [IDCARE](#)
- [Scamwatch](#)

Authorised by the Australian Government, Canberra

Data breach guidance for individuals

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Help-for-identity-theft/Data-breach-guidance-for-individuals/
- Last modified: 30 Nov 2022
- QC 54174

If you have experienced a data breach that has compromised your tax identity, we have advice to help protect you.

On this page

- [If your personal information is lost or stolen](#)

If your personal information is lost or stolen

If your personal information has been lost or stolen in a data breach, it can lead to identity crime, as well as fraud on your tax or superannuation accounts.

If you have experienced a data breach that has compromised your tax identity, we have advice to help you protect your information and account.

We can take action to identify and protect you against potential tax and super fraud.

How data breaches can happen

You may be impacted by a data breach where your personal information is stolen by an unauthorised third party. Data breaches can include both physical and digital records.

A data breach may be a result of:

- your employer, tax agent or another organisation's accounts being compromised
- a home or office break-in
- someone hacking into your computer systems or using targeted phishing emails to compromise your electronic devices
- your records being accidentally left somewhere.

Criminals can use personal information stolen during data breaches to commit identity crime. If your identity is stolen, it is difficult to recover.

What to do after a data breach

- If you are notified of a breach or suspect you have been a victim of a data breach, contact our Client Identity Support Centre on 1800 467 033 Monday to Friday 8:00 am–6:00 pm AEST. We will discuss with you the level of security safeguards that may need to be applied to your account.
- If you are concerned about the security of your other personal information and the wider impact of identity theft, we recommend you speak with [IDCARE](#)⤢ on 1800 595 160. IDCARE provide free and confidential support to victims of data breaches and identity theft.
- We recommend you take note of our [top cyber security tips for individuals](#) to help make your identity more secure.

How we protect clients affected by a data breach

If fraud has occurred on your tax records, we will work with you to fix your account. We may also apply protective measures to protect it from future identity and refund fraud incidents, such as:

- [Additional proof of identity](#)
- [Additional monitoring processes](#)
- [Additional security measures](#).

Additional proof of identity

If you are the victim of a data breach, we may ask you for additional proof of record ownership before we discuss your tax affairs. This will apply when you interact with us. Even if you use a tax professional, we may request that you contact us directly.

Asking questions only you will know assures us we are dealing with a genuine client, and not an unauthorised third party.

You may also choose to have a secret password created on your record. Secret passwords validate your identity when you deal with us.

You can set up a secret password with our staff over the phone. However, if we are unable to establish your proof of identify, we may request you [visit a shopfront](#) with proof-of-identity documentation. You can also complete the tax file number enquiry form on the [Australia Post](#) website.

Additional monitoring processes

We will continue to monitor your record. If we identify any irregular activity, we may contact you or your registered tax professional to make sure the activity is legitimate. This may delay the processing of tax returns and other forms.

Additional security measures

Depending on your circumstances, we may apply additional security measures within our systems.

If we apply these measures:

- you may not be able to use our online channels or [myGov](#)
- pre-fill data may not be available
- we may need to make extra checks for tax returns and other forms that could delay processing
- we may prevent business activity statements from issuing automatically. You or your tax professional will need to contact us before each lodgment so we can generate these statements.
- your digital identity may be suspended while we investigate if there has been a compromise in our online environment.

Large data breaches

We are aware of [large data breaches](#) such as the Optus data breach and Medibank cyber incident and that people who have been affected might be concerned about their personal information.

We want to assure you that ATO systems have not been affected.

Large data breaches

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Help-for-identity-theft/Data-breach-guidance-for-individuals/Large-data-breaches/
- Last modified: 14 Nov 2022
- QC 70498

Steps to make sure your personal information is safe if it has been lost or stolen in a data breach or cyber incident.

On this page

- Optus data breach
- Medibank cyber incident
- Information for affected customers
- Reminders for the community
- Complaints

Optus data breach

We're aware of the recent Optus data breach and that people who have been affected might be concerned about their personal information.

We want to assure you that ATO systems have not been affected by the Optus data breach.

If you think you've been affected by the Optus data breach⧉, phone Optus Customer Service on 13 39 37.

Medibank cyber incident

We understand that the Medibank private cyber incident⧉ is stressful for those people affected.

If you think you may be affected by the recent Medibank private cyber incident:

- AHM customers can phone 13 42 46
- Medibank Private customers can phone 13 23 31
- visit the Medibank website⧉.

Information for affected customers

We're aware of the potential fraud and identity theft risks with taxpayers' personal information being compromised.

Information for customers affected by large data breaches:

- Australian Cyber and Security Centre (ACSC) advice for people affected by the Optus data breach⧉

- ACSC quiz – Have you been hacked?
- IDCARE Optus Data Breach Response Fact Sheet
- Home Affairs support for victims of identity crime – apply for a Commonwealth Victims' Certificate
- Scamwatch alerts on how to protect your information – Optus data breach and Medibank Private data breach.

The ATO takes data security seriously and we have several safeguards and systems in place to protect taxpayers.

Reminders for the community

It's important to always be vigilant for suspicious activity.

These tips can help protect your accounts and keep your personal information safe:

- Use multi-factor authentication for your accounts where possible.
- Be careful when clicking on links and providing personal information.
- Make sure your contact details are up to date when using online services.

Other websites that can help you protect yourself and stay informed:

- Moneysmart – Identity theft
- Office of the Australian Information Commissioner (OAIC) – Identity fraud
- ACSC – Report cybercrime
- Services Australia – Replacing a Medicare card because of a data breach.

Complaints

If you would like to make a privacy complaint, contact Optus or Medibank Private. If you are unable to resolve your complaint directly, you can lodge a complaint with the Telecommunications Industry Ombudsman or the Office of the Australian Information Commissioner.

Data breach guidance for businesses

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Help-for-identity-theft/Data-breach-guidance-for-businesses/
- Last modified: 30 Nov 2022
- QC 54172

Information security is an important aspect of your business. If your data is lost or compromised, it can be very difficult and costly to restore.

We can take action to identify and protect your business and client accounts against potential tax and superannuation fraud.

On this page

How data breaches can happen

A data breach occurs when confidential taxpayer information has been accessed by an unauthorised third party.

This information may include:

- employee payroll, tax, and super information
- confidential business documents
- banking details.

Examples of data breaches include, but are not limited to:

- unauthorised removal of computers, data, or records in both paper and digital formats
- people with legitimate access to the data using it for fraudulent activity
- accessing taxpayer files using a fraudulently obtained credential, such as myGovID
- criminals exploiting vulnerabilities in your IT security controls, hacking or phishing for information
- accidental disclosure of information, for example, records emailed to an unauthorised third party or hard copies left in a public place
- payroll information for your employees being unlawfully accessed
- unauthorised access to cloud-based services you use to store information.

What to do after a data breach

You should report any data breaches to us so we can place protective measures on client accounts.

If a breach occurs within your business, we recommend you:

- Phone our Client Identity Support Centre on 1800 467 033 Monday to Friday, 8:00 am–6:00 pm AEST, so that we can apply measures to protect your business, staff and clients where necessary.
- If you are a digital service provider or software developer, use the Report data breach form within Online Services for DSPs⬚, or phone the SBR Service Desk on 1300 488 231, available every day, 8:00 am–6:00 pm AEST.
- Review the Office of the Australian Information Commissioner's (OAIC) information about notifiable data breaches⬚ to make sure you comply with your obligations under the *Privacy Act 1988*, including the Notifiable Data Breaches (NDB) scheme.
- Tell affected employees or business associates about the breach. These may include software providers, such as your payroll services, especially if you

suspect the breach originated in one of their service offerings.

- Consider what information was accessed during the breach and take steps to safeguard this where necessary. For example, you may need to report inappropriate access to your myGovID.
- Take steps to secure the information in your business by updating all security software and controls.
- Review systems access and remove it for people who no longer need it.
- Continue to follow security best practices and reinforce these practices with your staff to reduce the risk to your business.

If you, your impacted employees, clients or business associates are concerned about the security of other personal information and the wider impact of identity theft, we recommend you speak with IDCARE on 1800 595 160. IDCARE provide free advice and confidential support to victims of data breaches and identity theft.

Case study: Compromise of business email account

Compromised business email accounts are an increasing risk to business. Fraudsters gain access to corporate email accounts and spoof the business email address. They do this to steal personal identifying information or to defraud the company, its employees or customers of money.

Spoofing is where an email is sent from a fake website or email address disguised as a legitimate website or email address. If you hover the mouse icon over the email address, the true source of the email will be shown.

A recent report advised a tax agent's email address was spoofed by a fraudster. The fraudster sent an email, which seemed legitimate, to the agent's client list asking them to complete a personal data request form. This was an attempt to harvest client identifying information to commit future identity and tax fraud.

We took immediate action and applied protective measures to the affected client, entity and employee accounts.

Cyber and phishing attacks can be very damaging for business and can often lead to further attacks on your client, business and employee data.

Staff education is critical. If you receive a suspected scam phishing email, do not:

- click on any links
- open any attachments
- download any files
- install any applications.

These files may install a virus on your computer to steal identity credentials.

How we protect clients affected by a data breach

If a data breach has occurred at your business, it is important you understand the steps we may take to safeguard taxpayer data and our tax and superannuation systems.

To protect the community we may apply treatment options to any files impacted by the data breach, which may include:

- Additional proof of identity
- Additional monitoring processes
- Additional security measures
- Appointment of a data breach manager.

Additional proof of identity

If your business is the victim of a data breach, we may ask you for additional proof of record ownership before we discuss your tax affairs. This will apply when you interact with us. Even if you use a tax professional, we may request that you contact us directly.

Asking questions only you will know assures us we are dealing with your business and not an unauthorised third party.

You may also choose to have a secret password created on your record. Secret passwords validate your identity when you deal with us.

You can set up a secret password with our staff over the phone. However, if we are unable to establish your proof of identify over the phone we may request you visit a shopfront with proof-of-identity documentation or complete the tax file number enquiry form on the Australia Post website.

Additional monitoring processes

When a breach has occurred we will continue to monitor any impacted ATO records to make sure transactions on these accounts are accurate. If we identify any irregular activity, we may contact you to verify the accuracy of the information provided or the legitimacy of any account activity.

This may delay processing of tax returns and other forms.

Additional security measures

Depending on the circumstances, we may apply additional security measures within our systems.

If we apply these measures:

- you may not be able to use our online channels or myGov
- pre-fill data may not be available
- we may prevent business activity statements from issuing automatically. You

will need to contact us before each lodgment so we can generate these statements.

- we may need to make extra checks for tax returns and other forms that could delay processing.

Appointment of a data breach manager

In some cases, we may assign a data breach manager who will assist you in the management of data breaches within your business. They can provide support to reduce the impact on your business and your client.

Inappropriate access to myGovID

[myGovID](#)⌐ uses encryption and cryptographic technology and the security features in your device, such as fingerprint or face, to protect your identity.

If you are aware or suspect someone has inappropriately accessed your personal information in myGovID, you need to report this immediately.

Contact the myGovID support line on 1300 287 539 (select option 2) between 8:00 am and 6:00 pm AEST, Monday to Friday.

International callers can contact us by phoning our switchboard on +61 2 6216 1111 between 8:00 am to 5:00 pm AEST, Monday to Friday, and requesting your call be transferred to the myGovID support line.

For more information and tips about staying safe online, see [myGovID security](#)⌐.

To help protect your business from a data breach, we recommend you:

- review our [top cyber security tips for business](#).

Data breach guidance for tax professionals

- https://www.ato.gov.au/General/Online-services/Identity-security-and-scams/Help-for-identity-theft/Data-breach-guidance-for-tax-professionals/
- Last modified: 30 Nov 2022
- QC 54173

Information security is an important aspect of your business. If your data is lost or compromised, it can be very difficult and costly to manage.

We can take action to identify and protect your practice and client accounts against potential tax and super fraud.

On this page

How data breaches can happen

A data breach occurs when confidential taxpayer information has been accessed by an unauthorised third party.

Tax professionals hold a large amount of client, staff and business information, which makes them a growing target for identity thieves.

Tax professionals who experience a data breach may discover their clients' identities have been stolen and refund fraud has been committed in the clients' names.

Examples of data breaches include, but are not limited to:

- unauthorised removal of computers, data, or records in both paper and digital formats
- people with legitimate access to the data using it for fraudulent activities
- accessing taxpayer files using a fraudulently obtained credential, such as myGovID
- criminals exploiting vulnerabilities in your IT security controls, hacking or phishing for information
- accidental disclosure of information, for example, records emailed to an unauthorised third party or hard copies left in a public place
- payroll information for your employees being unlawfully accessed
- unauthorised access to cloud-based services you use to store information.

What to do after a data breach

Tax professionals should report data breaches to us to make sure protective measures can be placed on client accounts.

If you have experienced a breach we recommend the following actions:

- Phone our Client Identity Support Centre as soon as possible on 1800 467 033 Monday to Friday, 8:00 am–6:00 pm AEST so that we can apply measures to protect your business, staff and clients.
- Review the Office of the Australian Information Commissioner's (OAIC) information about [notifiable data breaches](#)⊡ to make sure you comply with your obligations under the *Privacy Act 1988*, including the Notifiable Data Breaches (NDB) scheme. Review the Tax Practitioners Board (TPB) information on how the [NDBS can impact your TPB registration](#)⊡.
- Tell affected clients and staff about the data breach. We may also contact your clients or staff directly.
- Contact your software provider, especially if you suspect the breach originated in one of their service offerings.

- Consider what information was accessed during the breach and take steps to safeguard this where necessary. For example, you may need to report inappropriate access to your myGovID.
- Take steps to secure the information in your business by updating all security software and controls.
- Review systems access and remove it for people who no longer need it.
- Continue to follow security best practices ⬈ and reinforce these practices with your staff to reduce the risk in your business.

If you or your clients are concerned about the security of other personal information and the wider impact of identity theft, we recommend you speak with IDCARE ⬈ on 1800 595 160. IDCARE provide free advice and confidential support to victims of data breaches and identity theft.

Case study 1: Stolen equipment

A tax agent reported to us that a laptop and documents were stolen from their car. The items contained confidential information, including business credentials and records for individual and business entities managed by the tax agent.

It was later confirmed that the tax agent's identity had been stolen and used to lodge fraudulent PAYG summaries on their clients' accounts.

We applied protective measures to the client, entity and employee accounts relating to the affected tax agent's business.

Reports of stolen equipment and data used for business occur regularly. There are a number of ways in which the data you hold on behalf of your clients, employees and business can be stolen, such as:

- dumpster diving
- letterbox theft
- paper or electronic files left unattended
- cards stolen from wallets
- stolen briefcases or laptops.

To keep your client and business information safe:

- do not leave your information unattended
- make sure you keep your electronic devices secure
- make sure client and staff data is securely stored at the end of each day
- apply multi-factor authentication to all devices used for your business.

Case study 2: Ransomware

A tax agent reported an incident in which they received an authentic looking email from a large Australian business requesting information. The agent clicked a link in the email, which released a 'crypto virus' that locked their computer systems. Fortunately, their IT specialist was able to recover their systems, but the security of their data was put at risk.

The tax agent has since:

- added additional measures to protect their systems and data holdings from future attacks
- provided training to all staff on how to check for spoofing in emails.

We asked the agent to provide the names of potentially compromised clients and applied protective measures to their accounts, including entity and employee accounts.

There are many variations of ransomware that can affect business systems and data in different ways. At the time of ransomware attacks it's impossible to know precisely what a virus will do.

Some ransomware spreads into computer systems and silently steals information. Other ransomware is used to extort money from businesses by locking their computer files using an unbreakable code that only the criminal knows. If you pay the ransom money, the fraudsters may unlock your systems and release the data, but you could be targeted again.

Staff education is critical. If you receive a suspected phishing scam email, do not:

- click on any links
- open any attachments
- download any files
- install any applications.

Make sure your data is secure by backing it up regularly. Consider using off-site data storage options to effectively back-up your data.

How we protect clients affected by a data breach

We protect the privacy of client records by our proof of record ownership processes. If a data breach occurs within your practice, we may implement a range of additional safeguards.

Understanding what treatments we may apply to protect your clients will help you support them.

Treatment options can include one or more of the following, depending on the severity of the breach and any resulting fraud attempts:

- [Additional proof of identity](#)
- [Additional monitoring processes](#)
- [Additional security measures](#)
- [Appointment of a data breach manager](#)

Additional proof of identity

We may issue an alert to our staff requiring them to seek additional proof of record ownership from your client.

The requirement will apply when your client interacts with us. The alert prompts our staff to ask additional questions when validating your client's identity. This alert does not:

- prevent you from dealing with us on behalf of your client
- change how we will identify you.

Asking questions only the genuine client will know assures us we are dealing with the actual client, and not an unauthorised third party.

Your client may also choose to have a secret password created on their ATO record. Secret passwords validate a client's identity when they deal with us.

The client can create their secret password with our staff over the phone. However, if we are unable to establish proof of identity, we may request your client [visit a shopfront](#) with proof-of-identity documentation. They can also complete a tax file number enquiry form on the [Australia Post](#) website.

Additional monitoring processes

We will continue to monitor your client's ATO records. If we identify any irregular activity, we may contact you or your client to make sure the activity is legitimate. This may delay processing of tax returns and other forms.

Additional security measures

Depending on your client's circumstances, we may also apply additional security measures within our systems.

If we apply these measures:

- your client may not be able to use our online services or [myGov](#)
- pre-fill data may not be available
- we may prevent business activity statements from issuing automatically. You or your client will need to contact us before each lodgment so we can generate these statements.
- we may need to make extra checks for tax returns and other forms that could delay processing.

Appointment of a data breach manager

In some cases, we may assign a data breach manager who will assist you in the management of data breaches within your practice. They can provide support to reduce the impact on your practice and clients.

Inappropriate access to myGovID

myGovID uses encryption and cryptographic technology and the security features in your device, such as fingerprint or face, to protect your identity.

If you are aware or suspect someone has inappropriately accessed your personal information in myGovID, you need to report this immediately.

Contact the myGovID support line on 1300 287 539 (select option 2) between 8:00 am and 6:00 pm AEST, Monday to Friday.

International callers can contact us by phoning our switchboard on +61 2 6216 1111 between 8:00 am to 5:00 pm AEST, Monday to Friday, and request your call be transferred to the myGovID support line.

For more information and tips about staying safe online, see [myGovID security](#)🡵.

To help protect your business from a data breach, make sure you:

- undertake [proof-of-identity checks](#)
- review our [top cyber security tips for business](#).

Online security

- https://www.ato.gov.au/General/Online-services/Online-security/
- Last modified: 27 Jul 2021
- QC 40958

There are many ways you can interact with us online, including lodging your tax returns and other tax-related information.

We take the security and privacy of your personal information very seriously. We have steps in place to make sure your data and online transactions with us are secure and safe.

You can help make sure your online transactions with us are safe by taking some simple steps.

On this page

- [Stay safe online](#)
- [How we protect you](#)
- [Data breach guidance](#)
- [Security for digital services providers](#)

Stay safe online

As a taxpayer you play a big part in protecting your personal information when you interact online.

You should:

- Be careful when downloading attachments or clicking links, even if the message seems to come from someone you know.
- Always access our online services directly via ato.gov.au, my.gov.au or the ATO app, not by following a link.
- Keep your tax file number (TFN) and passwords secure – don't share your password with others.
- Keep your superannuation account details secure – don't share your account details with unknown sources online.
- Never reply to emails with your password or other sensitive information (such as your TFN), including to prospective employers.
- Change your passwords regularly.
- Use multi-factor authentication where possible – using SMS codes as your sign-in option for myGov is a quick and secure way to sign-in to access ATO online services.
- Make sure your digital identity, such as [myGovID](#), is secure. Your digital identity is unique to you and shouldn't be shared. Sharing it gives others access to your personal data across services, such as tax and health.
- Avoid conducting high-risk transactions, such as banking or logging on to online services, over unsecure public Wi-Fi.
- Never share personal information, such as your TFN, myGov or bank account details, on social media.
- Regularly back up your data onto an external hard drive or cloud backup. Secure your backup devices by making sure they are not continuously connected to your main network.
- Keep your software up to date. Protect yourself and your business by installing the latest security updates, running regular anti-virus scans and using a spam filter on your email accounts.
- Disable remote access software until it's needed.
- Make data security an everyday priority – practice good 'cyber hygiene' and constantly review your security habits.
- Make sure you check your myGov Inbox regularly – if you know everything is in order, it will be harder for a scammer to convince you otherwise.

We encourage you to be alert and check your online practices at least quarterly.

Our *Online security self-assessment questionnaire* gives you information to help you improve your online security.

Next step:

- Online security self-assessment questionnaire

See also:

- Protect your information
- Top cyber security tips for individuals
- Top cyber security tips for businesses
- Australian Cyber Security Centre[□]

How we protect you

We keep your personal information safe by:

- confirming your details when you contact us
- having a range of systems and controls in place to make sure your data and transactions with us are secure
- logging access to your personal information (to help us identify any unusual behaviour).

To help you stay safe online, we will not:

- ask you for your TFN or bank details via return email, SMS, or on social media
- give your personal information to anyone without your consent, unless the law permits us to
- communicate with you on behalf of another government agency or ask another government agency to represent us.

See also:

- Verify or report a scam
- Scam alerts
- Scamwatch[□]
- Cyber Issue Reporting System[□]

Data breach guidance

A data breach is when confidential information is accessed, disclosed without authorisation, or lost.

To protect yourself, your business, and your employees and clients against identity crime and fraud, you should take appropriate security precautions.

If you or your business experiences a data breach, there are steps you can take to minimise the impact.

See also:

- Data breach guidance for individuals
- Data breach guidance for businesses
- Data breach guidance for tax professionals

Security for digital service providers

We offer a range of digital services that support the community to interact with us to do business. We place specific security measures around where and how we store, access and transfer data.

The growth of our digital wholesale services increases productivity and connects the community across the digital economy. This presents a range of service opportunities for us and the community. However, there are also business risks and security implications to be managed.

The Digital Service Provider (DSP) Operational Framework addresses these risks. It establishes how we'll provide access to and monitor the digital transfer of data through software.

See also:

- [DSP Operational Framework](#)⧉

Authorised by the Australian Government, Canberra.

Top cyber security tips for individuals

- https://www.ato.gov.au/General/Online-services/Online-security/Top-cyber-security-tips-for-individuals/
- Last modified: 27 Jul 2021
- QC 50562

Do you know how valuable you are? Identity thieves do!

Every year thousands of Australians have their identities stolen.

Criminals use stolen personal information to commit identity crimes. This can leave their victims with a bad credit rating and impact their ability to get a loan, run a business, or access government services.

Once your identity is stolen it can take a long time to recover. We, along with leading industry bodies, have created a list of top identity security tips to help keep you and your information safe.

Next step:

- Download a printable version of *Security tips for individuals* via the [ATO Publication Ordering Service](#)⧉ – search for *Security tips* and select Media – all publications.

Cyber Security Stakeholder Group

We developed these tips in consultation with the Cyber Security Stakeholder Group (CSSG), a group comprising of the ATO, tax practitioner industry groups, government agencies and industry partners. The CSSG are working with us to combat the growing threat of identity theft and cybercrime.

See also:

- How to protect yourself
- IDCARE⊠
- Cyber Issue Reporting System⊠ – to report cybercrime
- Scamwatch⊠
- Cyber Security Stakeholder Group

Make sure your passwords are strong and secure

Use multi-factor authentication where possible. Regularly change passwords, and do not share them.

Multi-factor authentication requires users to provide multiple pieces of information to authenticate themselves – for example, a text message sent to your phone when logging in to a website.

An additional layer of security on your accounts can make it harder for others to access your account.

Using strong passwords, with a mix of upper and lower case letters, numbers, and symbols, also makes your accounts harder to hack.

Make sure all devices have the latest available security updates

Run weekly anti-virus and malware scans and have up-to-date security software.

Instances of malicious software (malware) are increasing. It can be easy to accidently click on an email or website link which can infect your computer.

In some instances, your device may be impacted by ransomware. Ransomware can:

- lock your computer until you pay a fee to criminals
- install software which provides access to your bank accounts, allowing criminals to steal your money.

Use a spam filter on your email account

Always use a spam filter on your email account and do not open unsolicited messages.

Be wary of downloading attachments or opening email links you receive, even if they are from someone you know.

Spam emails can be:

- embedded with malware
- used to trick you into providing information or buying non-legitimate goods.

Do not respond to or click on these emails. This can help you reduce the risk of your personal information being used fraudulently, or your computer being infected with malware.

Secure your wireless network, be careful using public wireless networks

Be vigilant when using public wireless networks. Avoid making online transactions while using public or complimentary wi-fi.

Not all wi-fi access points are secure. By making online transactions (such as online banking) on an unsecure network, you can put your information and money at risk.

Be vigilant about what you share on social media

Keep personal information private and be aware of who you are interacting with.

People are accustomed to sharing personal information on social media. However, before sharing ask yourself if it is information you want strangers to have access to.

It is very easy for information on social media sites to be shared outside of your network, even when your security settings are set to private.

Be sure you know who you are speaking to on social media, and only share information with people you know and trust.

Criminals can use certain combinations of your personal information to impersonate you to access money, apply for credit cards and bank loans, or commit crimes.

Treat your personal information like cash

Do not leave your personal information lying around. If your personal information is stolen, it is very difficult to get back.

Keep your personal information private. Only share it when you are required to, and only share it through authorised processes and to authorised people.

Monitor your accounts for unusual activity or transactions

Check your accounts (including bank accounts, digital portals and social media) for transactions or interactions you did not make, or content you did not post.

If an organisation you deal with sends you an email alerting you to unexpected changes on your account, do not:

- click on included hyperlinks

- open any attachments.

You should immediately:

- check your account
- contact the organisation by phone.

Make sure your mail is secure

Make sure your mail is secure and consider using a secure PO Box.

Mail theft is a leading cause of personal information security breaches.

Do not download programs or open attachments

Some programs contain malware that can infect your computer or be used to harvest your personal information.

Be sure you are downloading authorised and legitimate programs. Unless you know the program is legitimate, do not open attachments or download it.

Do not leave your information unattended

Secure your electronic devices wherever you are. Your personal information can be taken in an instant. In some situations, you won't even know it was stolen.

Make sure you:

- do not leave electronic devices unattended
- secure your electronic devices with passcodes
- securely store portable storage devices (such as thumb and hard drives) when not in use.

See also:

- Top cyber security tips for businesses

Top cyber security tips for businesses

- https://www.ato.gov.au/General/Online-services/Online-security/Top-cyber-security-tips-for-businesses/
- Last modified: 27 Jul 2021
- QC 50563

It is important you keep all your business, staff and client information secure. If your data is lost or compromised, it can be very difficult, time consuming and costly to recover.

We, along with leading industry bodies, have created a list of top identity security tips to help keep you and your information safe.

Next step:

- Download a printable version of *Security tips for business* via the [ATO Publication Ordering Service](#)⬀ – search for *Security tips* and select Media – all publications.

Media: Protect your business against identity crime
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiunji3ij9⬀ (Duration: 1:18)

Cyber Security Stakeholder Group

We developed these tips in consultation with the Cyber Security Stakeholder Group (CSSG), a group comprising of the ATO, tax practitioner industry groups, government agencies and industry partners. The CSSG are working with us to combat the growing threat of identity theft and cybercrime.

See also:

- [How to protect yourself](#)
- [IDCARE](#)⬀
- [Cyber Issue Reporting System](#)⬀ – to report cybercrime
- [Scamwatch](#)⬀
- [Cyber Security Stakeholder Group](#)

Use strong and secure passwords

Regularly change passwords and do not share them.

Use multi-factor authentication where possible. Multi-factor authentication requires users to provide multiple pieces of information to authenticate themselves – for example, a text message to your phone when logging in to a website.

As a business owner, remember:

- multi-factor authentication puts an additional layer of security on your accounts – it can make it harder for others to access your account
- consider using a passphrase that includes numbers and symbols which is easy for you to remember but difficult for someone to guess (for example, P!ne@pp1eP!zz@).

Remove system access from people who no longer need it

Immediately remove access for people who:

- no longer work for your business
- have changed positions and no longer require access.

Unauthorised access to systems by past employees is a common cause of identity security or fraud issues for businesses.

Make sure all devices have the latest available security updates

Run weekly anti-virus and malware scans and have up-to-date security software.

Instances of malicious software (malware) are increasing. It can be easy to accidently click on an email or website link which can infect your computer.

In some instances, your device may be impacted by ransomware. Ransomware can:

- lock your computer until you pay a fee to criminals
- install software which provides access to your bank accounts, allowing criminals to steal your business's money.

Do not use USBs or external hard drives from an unfamiliar source

USBs and external hard drives may contain malware, which can infect your business computers without you noticing.

It can cost your business a lot of money to repair the damage.

Stolen information could be used to commit crimes, often in your business's name.

Use a spam filter on your email account

Always use a spam filter on your email account. Do not open any unsolicited messages.

Be wary of downloading attachments or opening email links you receive, even if they are from a person or business you know. They can infect your computer with malware and lead to your business or client information being used to commit fraud.

Spam emails can be embedded with malware and can be used to trick you into:

- providing information
- paying fraudulent invoices
- buying non-legitimate goods.

Do not respond to or click on these emails.

Secure your wireless network, be careful using public wireless networks

Be vigilant when using public wireless networks. Avoid making online transactions while using public or complimentary wi-fi.

Not all wi-fi access points are secure. By making online transactions (such as online

banking) on an unsecure network, you can put your information and money at risk.

Be vigilant about what you share on social media

Keep your personal information private and be aware of who you are interacting with.

Before sharing, ask yourself if it is information you want strangers to have access to.

Scammers can take information you publicly display and impersonate you or your business. Impersonators may send emails to trick your staff into providing valuable information or releasing funds.

Monitor your accounts for unusual activity or transactions

Check your accounts (including bank accounts, digital portals and social media) for transactions or interactions you did not make, or content you did not post.

If an organisation you deal with sends you an email alerting you to unexpected changes on your account:

- don't click on included hyperlinks
- don't log on to the organisation's website by using links or attachments included in the email.

You should immediately:

- check those accounts
- contact the organisation by phone.

Make sure your mail is secure

Make sure your mail is secure and consider using a secure PO Box.

Mail theft is a leading cause of information security breaches.

Do not download programs or open attachments unless you know the program is legitimate

Some programs contain malware that can infect your computer (including ransomware which locks your files until you pay a criminal). It can also be used to harvest your sensitive personal and business information.

Be sure you are downloading authorised and legitimate programs. Unless you know the program is legitimate, do not open attachments or download programs.

Do not leave your information unattended

Secure your electronic devices wherever you are. Your information can be stolen in an instant. In some situations, you won't even know it's been stolen.

Make sure you:

- do not leave your information unattended
- secure your electronic devices (such as phones or tablets) with passcodes
- securely store portable storage devices (such as thumb and hard drives) when not in use.

Report a system security vulnerability

- https://www.ato.gov.au/General/Online-services/Online-security/Report-a-system-security-vulnerability/
- Last modified: 23 Sep 2022
- QC 66993

Find out about our security vulnerability disclosures policy and how to report potential vulnerabilities in ATO systems.

On this page

- About our security vulnerability disclosure policy
- What the policy covers
- How to report a vulnerability
- People who have disclosed vulnerabilities

About our security vulnerability disclosure policy

The online security of our systems is our top priority. We take every care to keep them secure. But despite our efforts, they may still be vulnerable.

We are keen to engage with the security community. Our security vulnerability disclosure policy allows you to responsibly share your findings with us.

If you think you have identified a vulnerability in one of our systems, services or products, report it to us as quickly as possible.

As an Australian Government agency we can't compensate you for finding potential or confirmed vulnerabilities. However, we can recognise you by publishing your name or alias on this page.

Our policy doesn't authorise you to conduct security testing against the ATO. If you think a vulnerability exists, report it to us. We can test and verify it.

What the policy covers

Our security vulnerability disclosure policy covers:

- any product or service wholly owned by us to which you have lawful access
- any product, service and infrastructure we provide to shared service partners to which you have lawful access
- any services that are owned by third parties but utilised as part of our services that you have lawful access to.

Under this policy, you must not:

- disclose vulnerability information publicly
- engage in physical testing of government facilities
- leverage deceptive techniques, such as social engineering, against ATO employees, contractors or any other party
- execute resource exhaustion attacks, such as DOS (denial of service) or DDOS (distributed denial of service)
- leverage automated vulnerability assessment tools
- introduce malicious software or similar harmful software that could impact our services, products or customers or any other party
- engage in unlawful or unethical behaviour
- reverse engineer ATO products or systems
- modify, destroy, exfiltrate, or retain data stored by the ATO
- submit false, misleading or dangerous information to ATO systems
- access or attempt to access accounts or data that does not belong to you.

Do not report security vulnerabilities relating to missing security controls or protections that are not directly exploitable. Examples include:

- weak, insecure or misconfigured SSL (secure sockets layer) or TLS (transport layer security) certificates
- misconfigured DNS (domain name system) records including, but not limited to SPF (sender policy framework) and DMARC (domain-based message authentication reporting and conformance)
- missing security HTTP (hypertext transfer protocol) headers (for example, permissions policy)
- theoretical cross-site request forgery and cross-site framing attacks.

How to report a vulnerability

To report a potential security vulnerability, send details to VulnerabilityDisclosure@ato.gov.au.

Provide as much information as possible, including:

- an explanation of the potential security vulnerability
- listing the products and services that may be affected (where possible)
- steps to reproduce the vulnerability
- proof-of-concept code (where applicable)
- names of any test accounts you have created (where applicable)
- your contact details.

We may need to contact you for more information to resolve the concern. We will handle your report confidentially in line with our ATO privacy policy.

We ask that you also maintain confidentiality. Don't publicly disclose details of any potential security vulnerabilities without our written consent.

What happens next

When you report a vulnerability, we will:

- respond to you within 2 business days
- recognise your contribution to our program.

We will not:

- financially compensate you for reporting
- share your details with any other organisation, without your permission.

If you have any questions, contact us at VulnerabilityDisclosure@ato.gov.au.

People who have disclosed vulnerabilities

The names or aliases of people who contribute to our security vulnerability disclosure program will be published with their permission and shown below:

- Harrison Mitchell
- Cyril Luk
- Tim McMahon
- Callum Macarthur
- Scott Sturrock

Technical support

- https://www.ato.gov.au/General/Online-services/Technical-support/
- Last modified: 26 May 2022
- QC 40959

If you are having trouble accessing or using our online services, check our troubleshooting for common errors and known system issues.

Help and support for online services - individuals
Technical support for ATO online services, the ATO app, myTax and applying for a TFN using myGovID.

Troubleshooting for businesses and tax practitioners
Check if your error or system issue is a known issue and what you can do to resolve the problem.

Minimum system requirements
Find out if there are system requirements you need to meet to use our online

services.

Related pages

[Technical Helpdesk](#)⬈
Get general authorisation and connectivity support.

Help and support for online services – individuals

- https://www.ato.gov.au/General/Online-services/Technical-support/Help-and-support-for-online-services---individuals/
- Last modified: 11 Nov 2022
- QC 41368

Help if you're having trouble linking to ATO online services, using myTax or the ATO app, or applying for a TFN online.

On this page

- Linking ATO online services to myGov
- Using ATO online services
- Using myTax
- Using the ATO app
- Using myGovID to apply for a TFN
- Using Individuals Auto-Registration to apply for a TFN

Linking ATO online services to myGov

Check your personal details are in the correct format:

- TFN – 9 digit number, no spaces.
- Given name – the first 40 characters.
- Family name – the first 40 characters.
- One name only – enter your name in the family name field only.

If you still get an error message, check the table below for support.

Known issues or errors you may experience when linking to ATO online services

Error message or known issue	What you can do
Unable to link	Check you've entered these details correctly.

Unable to complete link as details do not match customer record.	Find your myGov personal details (name and date of birth): • select My account from the myGov homepage • then select My profile. These details will only appear if you have a link to either Medicare or Centrelink. If these details are incorrect, you'll need to contact either Centrelink or Medicare to update them. If the details displayed are correct, you'll need to contact us to update your ATO record.
Two attempts remaining One attempt remaining	Check the information is entered in the correct format. To find the correct format, check the instructions or click on the help (?) icon for format advice. If you're unable to answer, select another question about information in your tax record. You can find out more about the information you need for linking to us on myGov
Linking lockout This occurs when you've had 3 failed attempts to link to us. For security purposes you won't be able to link for one hour.	Try again after the 1 hour lockout has expired. Check the information is entered in the correct format. To check the correct format, check the instructions or click on the help (?) icon for format advice. If you're unable to answer, select another question specific to you. You can find out more about the information you need for linking to us on myGov
Unable to sign in to myGov You may not be able to sign in to your myGov account if you don't have access to security codes.	See When you can't sign in to your myGov account.
Cannot find link This message appears when attempting to navigate from myGov to ATO online.	You need to link your myGov account to the ATO before you can access ATO online services. For instructions, see Link your myGov account to the ATO. If you have previously linked your account to the

This means myGov is unable to find an active link to the ATO.	ATO, return to the myGov homepage, select View and link services to check your ATO link status. • If not showing as linked, select Link to begin the linking process. • If linked, you'll need to select Unlink. Once you've received confirmation that the ATO has been unlinked, you should select Link to link again.
Unable to verify Ineligible to link	If you receive one of these error messages, you will need to contact us.

See Create a myGov account and link it to the ATO.

Using ATO online services

Known issues or errors when using ATO online services

Error message or known issue	What you can do
An error has occurred (001)	• Ensure your device meets our minimum system requirements. • Try using another device. • Try again later. If the problem persists, contact us.
Your settings are blocking this page from loading (002)	Check your device to see if you have an ad blocker, browser add-on or anti-virus software installed. You may need to update the settings of this software (check your software provider's instructions) to allow our website to display. For example, by allowing content from the ato.gov.au domain which will enable access to onlineservices.ato.gov.au. You can generally find icons for ad blockers and other add-ons near the address bar in your browser. Alternatively, try using another device or browser. If you have followed the above steps and continue to experience this issue, phone our technical helpdesk on 1300 139 373.

A system issue error message is displayed Examples include: • A927.06 – The ATO system has encountered an unexpected error while processing your request • Proxy error • Unknown error • Unexpected system error • Session terminated • Session expiry.	If the problem persists, contact us.

Using myTax

Known issues or errors when using myTax

Known issue	What you can do
There is no 'Prepare' button or link on the ATO online services homepage for a specific year The 'Prepare' button or link will not display on the ATO online services homepage if: • you lodged a non-lodgment advice for the year you're trying to lodge • you indicated that your last lodged tax return was your final return.	Select the Manage tax returns quick link on the ATO online services homepage. If you completed a non-lodgment advice for the tax return you're now trying to lodge, select the History tab on the Income tax page. Then follow the on-screen instructions to start your return. If you previously indicated that your last lodged tax return was your final return, select the Not lodged tab on the Income tax page. Then follow the on-screen instructions to start your return. If a link does not display allowing you to lodge your tax return you will need to contact us.
Lodged return displaying as 'Not lodged' or 'Resume' on the ATO	If you: • have a lodgment receipt number, do not

	attempt to lodge your return again
online homepage	• don't have a lodgment receipt number, try lodging the return again.
Some returns may not display as lodged immediately after lodgment and may still appear in the For action section on the ATO online homepage.	If the lodgment is still displaying as Not lodged or Resume after 3 days, contact us.

Using the ATO app

Table 4: Troubleshoot known issues when using the ATO app

Known issues	What you can do
Unable to view the latest information such as financial year or unable to access a feature within the app	• Backup any myDeductions records (if applicable) before updating. • Update to the latest version of the ATO app. • Close the app, connect to the internet and open the app again.
A system error message displays Examples may include: • an error has occurred • error during set-up • an error code • any other error.	Ensure you have the latest version of the app installed. If the error message: • doesn't specify a timeframe – try again • specifies a timeframe – wait for that time to elapse and then try again. If you continue to receive the same error message, you can contact us to report the issue. Take note of and tell us the error code you receive.
In myDeductions 'Unable to upload your records' This might happen when you are attempting to upload myDeductions records to the ATO.	• Check for any system maintenance. • Check your device is connected to the internet.

	• Ensure you have the latest version of the app – back up your myDeductions records before updating the app.
	• Try again later.
	If you continue to receive this error message, you can [contact us](#) to report the issue.
In myDeductions – error trip recording on OPPO devices

OPPO devices include a setting which prevents apps from running in the background. If you go out of the app or your device goes into standby mode while recording a GPS trip, this setting can cause the ATO app to stop tracking your trip. | To resolve this issue, on your device, select
• Settings
• Battery
• Energy Saver
• ATO app
• Turn off, Background Freeze.

These steps may vary slightly depending on the device you have. |

Using myGovID to apply for a TFN

Table 5: Troubleshoot known issues when applying for a TFN online using myGovID

Known issues	What you can do
'An error has occurred. We are currently experiencing technical difficulties. We apologise for any inconvenience. Try again later.'

Some users are receiving this error message after submitting their online TFN application form. | We're currently investigating this issue.

If the issue persists, consider using an alternative method to [apply for a TFN](#). |

Using Individuals Auto-Registration to apply for a TFN

Table 6: Troubleshoot known issues when applying for a TFN using Individuals Auto-Registration (IAR)

Known issues	What you can do
When applying for a TFN in IAR, you may receive the following error message: Your info entered does not match that held by DIBP

This issue can occur when the time zone on your device is not set to an Australian time zone. | Set your device to an Australian time zone. Then resubmit the application. |

Troubleshooting for businesses and tax practitioners

- https://www.ato.gov.au/General/Online-services/Technical-support/Troubleshooting-for-businesses-and-tax-practitioners/
- Last modified: 23 Jan 2023
- QC 41616

This page contains updates on the availability of ATO systems for businesses and tax practitioners.

On this page

- Online services for agents
- Practitioner lodgment service (PLS) and Standard business reporting (SBR)
- MyGovID
- Online services for business
- Single Touch Payroll
- Other

Further information is available on the following dashboards:

- Online services for agents dashboard
- Practitioner lodgment service dashboard
- Superannuation dashboard
- Online services for business dashboard

Further information for technical assistance:

- Technical helpdesk

Online services for agents

Refer to the Online services for agents user guide for more information on Online services for agents.

Summary	Action required
Error message 'The attachment service is currently unavailable. Try again later' received when attaching an ATO PDF form in Practice Mail Updated 06/09/2022	To prevent this error, use the Save form button that is located in the form. Then attach the PDF to your practice mail message. For further information go to Deferrals forms for registered agents.
Error message received when attempting to update Financial Institution Account (FIA) details Added 28/07/2022	If you receive this error phone 13 72 86 Fast Key Code 1 2 5 2 to update the financial institution account details. This is a known issue that we are working to resolve.
Quick links not responding when clicked Updated 17/05/2022	The quick links redirect you to the Online services for agents menu item, your anti-virus or anti-malware software may be interpreting this as redirecting you to an untrusted location. What you need to do: • Whitelist the ato.gov.au domain in your anti-virus and anti-malware software. Your anti-virus and anti-malware software may also require exceptions specifically for onlineservices.ato.gov.au[↗] If you need further support, contact the technical helpdesk on 1300 139 373 Ensure you have at hand details of the problem, internet browser and anti-virus and anti-malware software you are using.
On-demand income tax lodgment status report missing clients that don't have due lodgments Updated 10/03/2022	Clients not obligated to submit tax returns, are no longer included in this report. For more information go to Client list. To obtain your client list data use Advanced search or View client list. This is a known issue that we are working to resolve.
On-demand activity statement	This is a known issue that we are working to

outstanding lodgment report; not displaying valid withholding payer numbers (WPN's) Updated 10/03/2022	resolve.
Outstanding activity statement on-demand reports return an incorrect withholding payer number (WPN) for some clients Added 04/02/2022	Phone 13 72 86 Fast Key Code 3 2 2 to confirm your clients WPN. This is a known issue that we are working to resolve.
On-demand income tax lodgment status report; missing middle initial in client's names for sole traders and individuals Updated 10/03/2022	This is a known issue that we are working to resolve.
Lodged attribution managed investment trust (AMIT) tax return, not appearing under the income tax 'history' tab Added 03/03/2022	If the trust return does not appear as outstanding under the 'not lodged' tab, you can confirm lodgment has been processed by reviewing the income tax account transactions. The income tax lodgment status report (current year + previous 3 years) will display the status of your clients not lodged, lodged and not necessary Income tax returns including AMIT returns. To download: • go to Agent homepage • select Reports and forms then Reports • scroll to the relevant report type • scroll to 'Income tax lodgment status report' (current year + previous 3 years) • select Request.
Outstanding activity statements On-demand report may provide an incorrect registered agent number (RAN) for some clients Updated 07/03/2022	RANs in the activity statement outstanding lodgment report may display incorrectly. To confirm the registered agent linked to the account, refer to the client level menu 'profile' and then select Maintain authorisations. This is a known issue that we are working to resolve.

Outstanding activity statements on-demand report is providing incorrect payment reference numbers (PRN) for activity statement and income tax instalment for non-ABN clients when opened in excel Updated 21/01/2022	To ensure the PRN displays correctly you will need to Download and then Import the csv file into Excel. If the data is not imported it could provide incorrect PRNs and result in misallocated payments. To import: • Open Microsoft Excel • Select Data menu > Get data > From file > From text or csv • Choose the downloaded report csv file and select Import • Set the data type detection to Do not detect data types • Select the Transform button • When the data has loaded, select Close and load to add the data into an Excel workbook. Refer to your excel help search for instructions on how to use this function by searching import csv. All other fields will appear correctly. Refer to payment options in the client level accounts summary to check the correct activity statement and income tax instalment PRN for non-ABN clients.
Payment reference number displays as a formula on activity statement On-demand report Updated 21/01/2022	To access the correct values for all PRNs in the report: • Open the downloaded report csv via the excel 'get data' import function for txt or csv • Set the data type detection to Do not detect data types • Select the Transform button.
Error message 'no Australian business number (ABN) found' or a login error received when logging into Online services for agents Added 12/11/2021	This may occur if you have verified your identity between 29 October and 3 November 2021. If this occurs, you need to ensure you still have 'standard' myGovID identify strength before Online services for agents can be accessed. To confirm: • Log in to your myGovID app and confirm your identity strength. The identity strength

	is located next to your name
	• If the identity strength is 'basic' you will need to verify 2 documents to uplift the identity strength to 'standard'.
New and existing clients that are entering and re-entering into PAYG instalments are automatically defaulted to a digital channel preference Added 13/08/2021	If no channel preference exists or for new and returning PAYG instalment clients, the paper channel preference will be applied. If you have a paper channel preference, we will reissue the paper instalment notices for the period ending June 2021. All PAYG instalment notices with a 28 July 2021 due date will be deferred until 30 August 2021. You will need to vary or pay by the new due date. All previously issued PAYG instalment notices with a due date after 30 August 2021 that went to the incorrect channel will be cancelled and re-issued to the correct channel unless they have already been finalised. Penalties or interest applied for missed payments or lodgments because of this error will be removed or remitted. We apologise for the inconvenience caused. Phone 13 72 86 Fast Key Code 2 1 1 for further information or to discuss your client's circumstances. This is a known issue that we are working to resolve.
Family trust elections (FTE) and interposed entity elections (IEE) report The FTE and IEE report may not be displaying for some clients as expected Added 04/03/2021	Some client FTE and IEE elections or revocations may not be displaying as expected on the FTE and IEE report in Online services for agents. You should continue to lodge these forms. Elections and revocations will continue to process as expected against the intended client record. If you need to confirm the FTE and IEE request has been received due to information not present on the FTE and IEE report, phone

	13 72 86 Fast Key Code 2 1 3. ATO operatives can validate the receipt and statues of an election or revocation received by checking internal systems.
On-demand income tax lodgment status report Added 10/08/2020	If, after we have updated the current year lodgment dates, your client has a 'not lodged' status for the current year and does not have a lodgment due date displayed, they may no longer have an obligation to lodge. Refer to the 'for action 'screen to determine if lodgments are up to date.
5A and T9 instalment amount on activity statement adjusted Online services for agents and PLS and SBR Added 25/03/2020	This occurs when the varied amount at label T9 does not equal the system calculated value that is based on the amount you have provided at label T8. You may be required to report an amount at label T9 that is greater than 25%, 50% or 75% of the estimated tax for the income year. To ensure accurate reporting of PAYG, review the instalment amount before lodging or resubmitting the form. To work out the correct T8 amount to use in each quarter refer to the information below: • For the first quarter in the income year that you are liable to pay an instalment, multiply T9 by 4 • For the second quarter in the income year, add quarter 1 and 2 instalment amounts then multiply by 2 • For the third quarter in the income year, add quarter 1, 2 and 3 instalment amounts, divide by 3 then multiply by 4 • For the fourth quarter in the income year add quarter 1, 2, 3 and 4 instalment amounts. This does not take into account any 5B credits that may have been claimed in previous quarters. For assistance phone 13 72 86 Fast Key Code 1 4 1.
Practice mail – Unable to	Each myGovID has its own mailbox. When

access the practice mail in my old AUSkey mailbox Updated 27/08/2021	you log in you will only see the mail for the myGovID you have logged in with, unless you have been given access to other users mailbox in access manager, or you are an administrator. If you have access to other mailboxes you can transfer the mail yourself. If you do not have access to other mailboxes, your Access Manager administrator or someone with the permission will need to allocate the mail for you. Items transferred to the myGovID mailbox will appear as unread. To transfer the mail: • Navigate to practice mail from the communication drop-down menu • Select the Inbox tab. If required, expand the list using the 'results per page' drop-down menu at the bottom right of the screen: • Select records to allocate • Select Allocate button from the bottom left of the screen • Select myGovID name from the Allocate to drop-down box • Press Allocate button on the bottom right of the screen • If you are an administrator you may find it useful to have Access Manager open at the same time to assist you to distinguish between the different credential names and types (AUSkey or myGovID). It is good practice to end date the AUSkey in Access Manager once all the mail has been moved from the old AUSkey mailbox.
Error received when sending mail attachments with '.xlsx' file type Added 18/02/2020	Some users may receive an error message when attempting to send attachments with '.xlsx' file type via practice mail. This may include deferral requests. We suggest that you save the file as 'Excel 97-2003 Workbook (*.xls)' before attaching to your practice mail message.

General interest charge (GIC) null display on statement of account debit and credit

Updated 29/12/2019 | If a GIC charge has been applied and reversed, a null result is displayed on the activity statement account transaction screen under the debit and credit headers.

To review the debit and credit transactions, simply expand the transaction. Sighted users can do this by clicking on the chevron at the end of the transaction line.

Note: This is the same for the print friendly version of this report. |
| Unable to view lodgment program data

Known issue impacting agents that operate under a trust to trustee structure

Updated 27/05/2019 | This is a known issue that we are working to resolve.

We will provide more information once more information is known. |
| Error message displayed after selecting 'submit' when removing a client using a unique identifier

You have errors in the following fields:
- Search clients
- Select a client

Updated 07/02/2019 | To resolve:
- with your cursor in the search field press 'enter', or
- click the search icon to the right-hand side of the identifier entered.

This will display the client's information to proceed with removing the client. |
| 'Enter letters only' error when attempting to enter a country into the other field when updating addresses

Updated 18/03/2019 | Users may experience an error when attempting to update addresses. If you select 'Other' in the Country* field you will be asked to input a country in the 'If other, specify here*' field.

An issue exists with validating the value input in this field which will return an error. If you receive the error:
- return to the 'country*' field and select the relevant country, or
- if the country is not in the list, phone 13 72 86 Fast Key Code 3 3. |
| Predictive search is only | Predictive search only returns ten matches in |

displaying ten matches when more than ten are expected Updated 07/02/2019	the drop-down box. To view the full list of results: • with the cursor in the search box, press 'enter', or • click the search icon to the right-hand side of the quick search field. This will navigate you to the advanced search screen to display the full list of the predictive search results.
Authorisation issues – client account Do not have authorisation to act on behalf of a client for all relevant accounts Updated 07/02/2019	To update the client accounts that you are currently authorised for, go to: • the client's client summary page • select Profile then Maintain authorisations • select appropriate account.
Authorisation issues – income tax account • Using an ABN as the unique client identifier, can only access specific accounts, not including the income tax accounts • Receive error message 'This client is already in your client list' when attempting to add the client again using the TFN • How do I add the client for income tax? Updated 07/02/2019	To update the accounts that you are currently authorised for, go to: • the Client's Client summary page • select Profile then Maintain authorisations • select Income tax. This will allow you to view and act on behalf of your client for all accounts. Note: Tax agents who are authorised to act on behalf of the client for all accounts must use the TFN as an identifier when adding the client in Online services for agents.
No response when selecting 'print friendly version' on some pages. Updated 07/02/2019	This issue may be related to your browser, browser settings or add-ons. Try using an alternative browser such as Chrome or Firefox. Turn off or disable browser ad blockers or add-ons that may be blocking this function.

[Back to top](#)

Practitioner lodgment service (PLS) and Standard business reporting (SBR)

Refer to the [PLS user guide](#) for more information on PLS.

- [Authentication errors](#)

List of PLS and SBR issues

Summary	Action required
CMN.ATO.IITR.EM000378 received when attempting to electronically lodge Individual income tax return Added 04/11/2022	This error is received when a WPN is provided as an identifier at either employment termination payment (ETP) or Australian Superannuation Lump sum payments. To resolve: • Remove the WPN • Enter '10000000001' in the ABN • Submit the return.
Notice of assessment 'Other information relevant to your assessment' section shows labels being adjusted from 0 to 0. Added 27/05/2022	No further action required; this is a display issue only and does not impact the clients tax assessment.
How to lodge loss carry back for 2022 future year returns with substituted accounting period (SAP) to enable amendments post 30 June 2022 Added 20/05/2022	Labels to enable 2023 losses to be carried back using the 2022 service are not available in SBR and PLS electronic lodgments. Agents will need to amend by using the 2022 service or lodge on paper.
Medicare Levy Surcharge commencement and finalisation dates for client health funds (multiple funds within the financial year) are not available via SBR pre-fill service Updated 29/03/2022	This information is available in pre-fill that is accessible through Online services for agents.
Unable to electronically	If you receive this error lodge a paper income

progress income tax returns for client's aged between 35–39 years old, who received 'working holiday maker' income Added 24/03/2022	tax return. This is a known issue that we are working to resolve.
Error CMN.ATO.CTR.428057 received when attempting to electronically lodge company tax return Added 15/02/2022	This error occurs when the total salary and wages expense at 'financial and other information' (label 8D) is greater than 'total expenses at profit and loss' (6Q) due to negative cost of sales (label 6A). If you receive this error lodge a paper Company tax return.
Error message received when managed fund distribution values at item 13 are left blank Added 21/01/2022	To resolve this error input zero into the values at item 13.
I have received refunds in my trust account but I have not received an electronic funds transfer (EFT) reconciliation report via my practitioner lodgment service (PLS) Added 10/12/2021	If you have received refunds and you have not received your EFT reports phone 13 72 86 Fast Key Code 3 1 2.
Duplicate checking error message 'CMN.ATO.GEN.DUPLICATE ENTRY' received when lodging company tax returns (CTR) with substituted accounting period (SAP) Added 27/09/2021	If you receive this error remove the ABN from the return and attempt to lodge again. If you have attempted to relodge and still receive the error phone 13 72 86 Fast Key Code 3 1 2.
Validation error VR.ATO.IITR.300101 received when attempting to lodge individual income tax return Added 16/07/2021	It has been identified that this validation rule incorrectly includes assessable first home super saver (FHSS) released amount – Category 3. Ensure any of these assessable account released amount – Category 3 income is included in the total entered at estimated total income.

	Including the assessable account release amount in the estimated total income will not affect the calculation or determination of a client's entitlement to government super contributions. This is determined internally, based on the income information provided in the individual income tax return including responses to A3 government super contributions.
Validation errors VR.ATO.IITR.730259 and VR.ATO.IITR.730260 received when attempting to lodge individual income tax returns Updated 08/09/2022	These errors can occur when income from a financial investment has not been included elsewhere in the return. If you receive these errors, and you believe the errors are incorrect, we suggest that you lodge the return by paper. Then send a message through Online services for agents with supporting information. To do this: • select Practice mail • select New • choose Topic 'debt and lodgment' • choose Subject 'managed lodgment program'. In the message, you must include the following: • advice that a deferral is required and the reason why you are unable to lodge • the client name and their TFN • the date the return was posted to the ATO. Note: You can't lodge a tax return via practice mail. This is a known issue that we are working to resolve.
When pre-lodging the individual income tax return you are returned with error message 'CMN.ATO.GEN.0002 Lodgment failed. Contact the ATO. Error code 50137'	Determine if the return contains exempt foreign income in the income details schedule. If so, ensure that foreign income deductible expenses are not greater than exempt foreign income and attempt to lodge the return again.

Delay in processing of tax return if inputting an amount at 'Net foreign rent from a managed fund' Added 01/03/2021	This will create an error in ATO systems which will require manual intervention and delay the processing of an individual tax return. To ensure that this error does not occur do not input any figures at 'Net foreign rent from a managed fund'. If the 'Net foreign rent from a managed fund' amount is known then record the information in 'Total other foreign income from managed fund' and 'Your share of other foreign income from managed fund' at label 20M on the tax return.
CMN.ATO.IITR.730053 and CMN.ATO.IITR.730061 Agents completing individual client tax returns. Error specifically relates to taxpayers: • who are in receipt of a capped defined benefit income stream (reported at label 7M of the main IITR) • who are over 60 years old • where the benefit is made up only of taxed elements, they have had tax withheld. Updated 08/09/2022	Validation rule VR.ATO.INCDTLS.000014 requires a value greater than 0 at any of the fields: • Superannuation income stream taxable component taxed element • Superannuation income stream taxable component untaxed element • Superannuation income stream tax-free component • Superannuation income stream lump sum in arrears taxable component taxed element • Superannuation income stream lump sum in arrears taxable component untaxed element • Superannuation income stream lump sum in arrears tax-free component. In this specific scenario agents should: • include a single dollar ($1) in the 'superannuation income stream tax-free component' field, and • place a $0 in all other fields identified in validation rule VR.ATO.INCDTLS.000014. On the main IITR agents should ensure the correct amount is reported at label 7M.
5A and T9 instalment amount on activity statement adjusted	This occurs when the varied amount at label T9 does not equal the system calculated value that is based on the amount you have provided at Label T8.

Online services for agents and PLS and SBR Added 24/03/2020	You may be required to report an amount at label T9 that is greater than 25%, 50% or 75% of the estimated tax for the income year. To ensure accurate reporting of PAYG, review the instalment amount before lodging or resubmitting the form. To work out the correct T8 amount to use in each quarter: • For the first quarter in the income year that you are liable to pay an instalment, multiply T9 by 4 • For the second quarter in the income year, add quarter 1 and 2 instalment amounts then multiply by 2 • For the third quarter in the income year, add quarter 1, 2 and 3 instalment amounts, divide by 3 then multiply by 4 • For the fourth quarter in the income year add quarter 1, 2, 3 and 4 instalment amounts. This does not take into account any 5B credits that may have been claimed in previous quarters. For assistance phone 13 72 86 Fast Key Code 1 4 1.
CMN.ATO.IITR.000224 – Tax withheld from Australian Government pensions and allowances incorrect Tax withheld amounts from Australian Government pensions or allowances are greater than or equal to the amount of Australian Government pensions. Both amounts must be correct Updated 02/08/2019	There are circumstances where Centrelink clients may have payment summaries that include a tax withheld amount greater than the taxable amount. This can be the result of changing payment types during the year or repaying payments that had tax withheld. If you experience this issue, phone 13 72 86 Fast Key Code 3 1 2 for further support.
Unable to lodge company tax return due to incorrect duplication error	Some users may receive an incorrect duplication error when lodging company returns using practitioner lodgment service (PLS). This is occurring in limited

Updated 16/10/2018	circumstances. We have found in many cases removing the ABN from the return you are trying to lodge will resolve this error.
CMN.ATO.AS.EM005 – .is a mandatory field When attempting to lodge activity statement, 'CMN.ATO.AS.EM005 - .is a mandatory field' error is returned that does not specify which field is mandatory Updated 15/08/2018	'Does G1 include GST' Y/N indicator at field G1 is mandatory if entry exists at G1. Update Y or N indicator and resubmit.
Non-individual income tax return (ITR) produces error: 'GENERALERRORINCORE' and/or 'CMN.ATO.GEN.200001'	Determine if the ABN being used has a status of cancelled. If: • yes, remove the ABN and resubmit the ITR, or • no, contact your software developer.

CMN.ATO.AUTH.007
 	
You do not have the correct permission to submit this request or retrieve this file.
 	
Updated 30/03/2020
	Desktop software users:
	• review your permissions in Access Manager, or
	• contact your authorisation administrator.
	
	Desktop and cloud software users:
	• check that the client ABN has not been cancelled. If cancelled
	  ○ remove the ABN from the form for lodgment and resubmit, or
	  ○ remove the ABN from your practice management software and the form for lodgment and resubmit.
	• Check that the client identifiers in your practice management software are correct
	
	  ○ Is the ABN correct for the TFN?
	  ○ Is the TFN correct for the client name?
	  ○ Is the ABN correct for the client name?
	
	If necessary set up your permissions in Access Manager.
	
	If you have confirmed your Access Manager

	settings are correct but the error persists, phone 13 72 86 Fast Key Code 3 1 2.

Authentication errors

List of authentication errors

Summary	Action required
SBR.GEN.AUTH.001 Mandatory information missing from the transmission. Contact your software provider Added 27/08/2021	Inform your digital service provider that the following element or attribute {AttributeName} was not found in the transmission.
SBR.GEN.AUTH.002 Mandatory information provided in the transmission is invalid. Updated 27/08/2021	Check that you have correctly entered identifiers in your software (as examples, the ABN and TFN.). Contact your digital service provider for assistance.
SBR.GEN.AUTH.003 Reporting party identifier information is missing from the lodgment. Updated 27/08/2021	Check that you have included the reporting party identifier (TFN or ABN) in the lodgment.
SBR.GEN.AUTH.004 Check the credential details match the details of the business/agent submitting the information Updated 27/08/2021	Check the ABN in the credential matches the business or registered agent details (for example, ABN or RAN) in the transmission. If necessary, contact your authorisation administrator. If you still need help, phone the technical help desk on 1300 287 539.
SBR.GEN.AUTH.005	Check that the client identifiers (TFN or ABN) entered into the practice software match the

Misalignment of identifying information Updated 19/07/2019	client identifiers used for the lodgment.
SBR.GEN.AUTH.006 A notification does not exist for your software provider for sending your online (cloud) transactions Updated 27/08/2021	A notification must exist in Access Manager for your digital service provider before attempting to transact. Phone 1300 852 232 or use Access Manager to notify us of a hosted SBR software service. You will need to provide the following details: • digital service provider name • their ABN and software ID. See Cloud software authentication and authorisation for more information on hosted SBR services.
SBR.GEN.AUTH.007 Contact your software provider. Updated 27/08/2021	The digital service provider has not been accredited as an online (cloud) software provider. Contact your digital service provider.
SBR.GEN.AUTH.008 Your notification for the online (cloud) software provider does not contain the correct software ID. Updated 27/08/2021	Check and update your hosted SBR software ID through Access Manager or by phoning us on 1300 852 232.
SBR.GEN.AUTH.009 You may not have the correct permission to submit this lodgment. Updated 27/08/2021	You may not have the correct permission for this transaction. Contact the authorisation administrator for your business or practice to update your permissions in Access Manager and then try again.
SBR.GEN.AUTH.010 Your transaction failed due to a problem with the online (cloud) software provider's system.	The credential used by the digital service provider for securing online (cloud) transmissions made by the business is not enabled for these services. To resolve, contact your digital service provider.

Updated 27/08/2021	
SBR.GEN.AUTH.011 Contact your software provider. Updated 27/08/2021	The digital service provider has disabled your nomination. Contact your digital service provider or nominate a new hosted software service on 1300 852 232.
SBR.GEN.AUTH.012 Intermediary identifier information is missing from the lodgment. Updated 27/08/2021	Ensure that the TFN, ABN or ARN of the intermediary is in the appropriate field.
SBR.GEN.AUTH.013 The ABN of the business being acted on behalf of is required. Updated 27/08/2021	Attempt to correct the field.
SBR.GEN.AUTH.014 A client's Australian business number, withholding payer number or ATO reference number is required for this request. Updated 27/08/2021	Attempt to correct the field.
SBR.GEN.AUTH.015 You are not authorised to submit this request. Review permissions in Access Manager and try again. Updated 27/08/2021	You may not have the correct permission for this transaction. Contact the authorisation administrator for your business or practice to update your permissions in Access Manager and then try again.
SBR.GEN.AUTH.016 Mandatory information missing from the lodgment. Added 27/08/2021	Information required for authorisation processing is missing from the lodgment. Review and update required information.

MyGovID

List of myGovID issues

Summary	Action required

Some users are experiencing issues when using myGovID and they may receive an error
 	
Added 18/03/2021
	If you receive CLR000001 error:
	• Upgrade to the latest version of the app on all devices
	• When prompted to create a myGovID, set up your myGovID again using your latest myGovID email address and the same identity documents that you used previously.
	
	Slowness or STA000001 error when verifying an identity document:
	• Leave your app open as it verifies your identity document – allow 5–15 minutes for the document to verify
	• If presented with the error, force quit the app and wait 20 minutes before logging back in
	• When you log in again, check if your identity document verified
	  ◦ if successful, the document will no longer appear in the list of identity documents that can be verified
	  ◦ if unsuccessful, try verifying it again following the advice above.

A user has been granted full access in relationship authorisation manager (RAM)	A principal authority or authorisation administrator will

allowing them to access all restricted clients for the practice, all registered agent numbers (RAN) and all business level permissions. However, the practice wants to customise the user's permissions and cannot with the full access level myGovID authentication Updated 21/11/2019	need to log in to RAM to edit the users' authorisation and change the level of access for Australian Taxation Office from full to custom. After making the change, a link is provided to the user's authorisation in Access Manager where they can re-setup the user's permissions (the user will have no Access Manager permissions by default after the change in RAM).

[Back to top](#)

Online services for business

List of Online services for business issues

Summary	Action required
Error message received when attempting to update Financial Institution Account (FIA) details Added 28/07/2022	If you receive this error [Contact the ATO](#) directly to update these details. This is a known issue that we are working to resolve.
Errors are experienced when accessing online services Added 23/12/2021	[Accessing online services with myGovID and RAM](#) [Clear cookies and cache in browser](#)⬏ then try and log in again or try a different browser.
I receive the error message 'No Australian Business Number (ABN) found' when logging into Online services for business Added 27/08/2021	If you have recently transferred your myGovID app from an old device to a new device, you will need to re-verify your identity. If your identity strength is 'standard' you will need to: • go to the Settings menu within the myGovID app • choose to Reset the app • recreate your myGovID using the latest email and original ID

documents until a standard ID is
achieved.

Single Touch Payroll

List of Single Touch Payroll issues

Summary	Action required
Single Touch Payroll (STP) troubleshooting for employers and intermediaries Updated 15/08/2018	STP troubleshooting
Lodgment of duplicate amounts in Single Touch Payroll (STP) and payment summary annual reports (PSAR) are creating duplicates. This may impact employee's pre-fill Updated 16/07/2018	If you finalise your employees via STP do not send a PSAR or file generated from your software with the same information. Only additional disclosures that are not captured in STP, should be reported via PSAR or file generated from your software. Lodgment of duplicate amounts may impact the employee's pre-fill.

Other

List of other issues

Summary	Action required
Superannuation guarantee charge (SGC) statement Online services for business	In order to be able to successfully submit the SGC statement or statements you will need to: • delete the quarter that previously included a late payment offset amount • re-enter the quarterly period and late payment information • ensure that you do not select 'Save and exit' before

If you have resumed a saved SGC statement and are experiencing issues with the OTR and/or late payment offset fields Updated 09/09/2021	submitting. If this is unsuccessful you will need to lodge using the [Spreadsheet version (XLS, 747KB)](#) ⬇ and attach it to a new secure mail message. To do this: • select Communication from top menu • then Secure mail • select New message • choose Superannuation as the mail topic • choose Lodge SGC statement as the mail subject.
Superannuation guarantee charge (SGC) statement Online services for business If you are lodging an amendment for 31 or more employees, use the spreadsheet Updated 09/09/2021	If you intend to lodge an amended SGC statement for 31 or more employees , lodge using the [spreadsheet version (XLS, 747KB)](#) ⬇ and attach it to a new secure mail message. To do this: • select Communication from top menu • then Secure mail • select New message • choose Superannuation as the mail topic • Lodge SGC statement as the mail subject.
Departing Australia superannuation payment (DASP) – unable to confirm identity	When entering the DASP online system you must enter the client's current passport number however if your client has used the DASP online system previously you need to ensure you use the same passport number that was used in the original application. Ensure your client gives you details of their current passport number in addition to any old passport numbers that may have been used previously to access DASP.
Departing Australia superannuation payment (DASP) – unable to claim unclaimed super money on behalf of a client	When accessing DASP online on behalf of a client, a search for unclaimed super money (USM) will only be conducted where the client's temporary visa has been cancelled and the client is no longer in Australia. Intermediaries are unable to claim USM via DASP online if these conditions are not currently true. Individual clients can access DASP Online or tax agents can lodge a paper claim form.

Unable to open forms from ato.gov.au – for example, objection form
 	
Updated 13/09/2022
	Try any of the following:
	• Update to the latest PDF viewer version
	• Follow prompts provided by browser to move past warning messages or to open in an alternate viewer
	• Download the form to your device by right clicking the form hyperlink and selecting Save link as
	  ○ Open file directly from saved file location (do not run or open from browser prompt)
	  ○ Click OK to close any java script warning messages and open form.
	
	IOS devices will not support downloads containing java script.

Unable to see the early stage innovation companies (ESIC) report Updated 20/01/2023	Users must have the correct permissions set by their administrator in Access Manager to view and lodge the form. To set the required permissions in Access Manager: • under My Business select Manage permissions • select the user to be modified • select the Client tab • under ATO Transactions tick both the Prepare and Lodge check boxes next to 'Early stage innovation companies reporting form' • save changes. The ESIC report is located under Client forms, which are in the Lodgments drop-down menu.
General purpose financial statements (GPFS) How to update and revise a lodged GPFS form Online services for agents and Online services for business Updated 09/09/2021	To update or revise a lodged GPFS form: • navigate to Lodgments menu • select General purpose financial statements • select Update for the year that you want to update • select the 'X' next to the link and answer Yes to delete the statement • attach the updated and revised GPFS.
General purpose financial statements (GPFS)	The only method to lodge a GPFS is via the form located in the lodgments drop-down menu in Online services for agents, or Online services for business.

How to lodge Online services for agents and Online services for business Updated 09/09/2021	If you are unable to access the report, ensure that: • you have the correct permission in Access Manager to prepare and lodge a GPFS • your administrator can grant you permission • the ABN of the entity is valid and has not been cancelled.
Email not delivered – Microsoft office 365 user	In some limited instances you may have an issue with new Microsoft office 365 installations where some emails sent to an official and current ATO email address may not have been delivered. The problem could be related to the configuration of the sender policy framework (SPF) and domain key identified mail (DKIM) services. If you suspect this problem is impacting emails sent from your practice, it will require a correction to your Office 365 configuration (unfortunately there is nothing the ATO can do to fix this). Consult your software service provider or contact your software vendor for more information and guidance.

Back to top

If you cannot find a reference for the system issue you are experiencing, contact us.

Minimum system requirements

- https://www.ato.gov.au/General/Online-services/Technical-support/Minimum-system-requirements/
- Last modified: 21 Apr 2022
- QC 56067

For the best experience when using our online services, your device should meet our minimum system requirements.

These minimum system requirements apply to our online services for:

- individuals and sole traders (accessed via myGov)
- business
- tax and BAS agents
- non-resident businesses using our simplified online GST registration system.

On this page

- [Check your system](#)
- [Supported browsers](#)
- [Other system requirements](#)

Check your system

You can quickly check your system and settings using our online services minimum requirements system check.

When accessing our online services using [myGovID and Relationship Authorisation Manager (RAM)](#) or [AUSid](#), additional requirements may apply.

Check your system

Supported browsers

For the best experience and improved online security, we recommend using one of the supported browsers:

- [Table 1 – for supported desktop browsers](#)
- [Table 2 – for supported mobile browsers](#).

If you use another browser, you may experience issues or be prevented from accessing our online services.

Changes to supported browsers

From 15 June 2022, Internet Explorer 11 is being retired by Microsoft and not supported. You will need to switch to another browser.

Table 1: Online services – supported desktop browsers

Browser	Version
[Google Chrome](#)	Current stable version and current Extended Stable Release (ESR) version
[Firefox](#)	Current stable version and current Extended Stable Release (ESR) version
Internet Explorer	Version 11 (retiring 15 June 2022)
Safari	Current public version and prior two versions

Microsoft Edge	Current stable version and current Extended Stable Release (ESR) version

Table 2: Online services – supported mobile browsers

Browser	Version
Mobile Safari (iOS)	Current public version and prior two versions
Chrome for Android	Current public version and prior two versions

Other system requirements

You may also need to check the following settings on your device when accessing our online services.

Table 3: Online services – other system requirements

Setting	Requirement	Notes
JavaScript	Enabled	Update this in your browser settings.
Cookies	Enabled	Update this in your browser settings.
Internet speed	Download > 0.5Mbps	Slow internet speeds may result in services running slowly or timing out.
Ad-blocker software Anti-virus software Browser add-ons	You may need to adjust the settings of your software or browser add-ons to allow our online services to load correctly.	This may involve whitelisting or adding an exception for the ato.gov.au domain.
Network settings (for example, firewalls)	Ensure the ato.gov.au domain is not blocked.	If you don't have access to update these settings (for example, you're using a public computer or wi-fi network), try a different device or a different network.

Contact our [Technical Helpdesk](#)⬈ – for help meeting these minimum requirements.

Using browser add-ons

Browser add-ons that block ads or trackers may have an unintentional impact on our online services.

For example, some ad-blockers block content based on certain key words (such as 'ad' or 'advertising'). MyTax references occupation types that contain these words for example, 'advertising manager'. This means that the ad-blocker may misinterpret 'advertising manager' as advertising content and prevent myTax from loading.

Your browser add-on may also identify components of our online services as trackers. Common components we use include:

- Google analytics/Google tag manager – we use Google analytics to understand how our online services are being used so we can make improvements as needed. No identifying information is collected (see [Web browsing records – ATO privacy policy](#)).
- Qualtrics Site Intercept – we use this to ask you to complete surveys and submit feedback about our online services.
- Atoonlinecdnstream.azurenet.net – this is not a tracker and is required for our online services. You won't be able to use our online services if this is blocked.
- Omnichannel.ato.gov.au – this is used to support the webchat feature in myTax.

Online services help

- [https://www.ato.gov.au/General/Online-services/Technical-support/Online-services-help/](#)
- Last modified: 07 Mar 2022
- QC 40970

If you are experiencing difficulty accessing or using our online services, check the following links:

- [Technical support](#) – for known system issues.
- [System maintenance](#) – for scheduled and unscheduled outage information.

If you are still experiencing difficulties, you can [Contact us](#).

System maintenance

- https://www.ato.gov.au/General/Online-services/System-maintenance/
- Last modified: 07 Feb 2023
- QC 40990

This page contains up-to-date information on ATO systems maintenance.

On this page

- Weekly system maintenance
- Systems maintenance
- ATO online systems
- Troubleshooting, technical help and performance dashboards
- Staying informed

Weekly system maintenance

ATO online systems may be impacted in part or in full for scheduled weekly maintenance at the following times.

Weekly systems release – start and finish times

Start time	End time
Tuesday 11:30 pm AEDT	Wednesday 7:00 am AEDT
Thursday 11:30 pm AEDT	Friday 7:00 am AEDT
Saturday 11:30 pm AEDT	Sunday 7:00 am AEDT

Systems maintenance

ATO online systems may be impacted in part or in full at the following times. Full or limited functionality may be returned earlier if maintenance is proceeding ahead of schedule.

Systems maintenance – start and finish times

Start time	End time	Maintenance type
Saturday 18 February 2023 10:00 pm AEDT	Sunday 19 February 2023 10:00 am AEDT	Standard release
Saturday 4 March 2023 10:00 pm AEDT	Sunday 5 March 2023 10:00 am AEDT	Monthly maintenance

Saturday 1 April 2023 10:00 pm AEDT	Sunday 2 April 2023 10:00 am AEST	Monthly maintenance
Saturday 22 April 2023 10:00 pm AEST	Sunday 23 April 2023 10:00 am AEST	Standard release
Saturday 6 May 2023 10:00 pm AEST	Sunday 7 May 2023 10:00 am AEST	Monthly maintenance
Saturday 3 June 2023 10:00 pm AEST	Sunday 4 June 2023 10:00 am AEST	Monthly maintenance
Friday 16 June 2023 11:30 pm AEST	Monday 19 June 2023 7:00 am AEST	Integrated release
Saturday 5 August 2023 10:00 pm AEST	Sunday 6 August 2023 10:00 am AEST	Monthly maintenance
Saturday 12 August 2023 10:00 pm AEST	Sunday 13 August 2023 10:00 am AEST	Standard release
Saturday 2 September 2023 10:00 pm AEST	Sunday 3 September 2023 10:00 am AEST	Monthly maintenance
Saturday 23 September 2023 10:00 pm AEST	Sunday 24 September 2023 10:00 am AEST	Standard release
Saturday 30 September 2023 9:00 pm AEST	Sunday 1 October 2023 10:00 am AEDT	Monthly maintenance
Saturday 4 November 2023 10:00 pm AEDT	Sunday 5 November 2023 10:00 am AEDT	Monthly maintenance
Friday 10 November 2023 11:30 pm AEDT	Monday 13 November 2023 7:00 am AEDT	Integrated release
Saturday 2 December 2023	Sunday 3 December 2023	Monthly maintenance

10:00 pm AEDT	10:00 am AEDT	
Saturday 16 December 2023 10:00 pm AEDT	Sunday 17 December 2023 10:00 am AEDT	Standard release

ATO online systems

List of ATO online systems:

- Access Manager
- ato.gov.au
- ATO app (some features)
- ATO Online Services for Agents
- ATO Online Services for Business
- ATO Online Services for Individuals and Sole traders
- ATO Online Services for Non-residents
- ATO Online Services Simulator
- AUSid
- Australian Business Register
- Bulk data exchange
- Data transfer facility
- Departing Australia Superannuation Payment
- EmployerTICK
- Online TFN application
- Progress of return
- Practitioner Lodgment Service
- Single Touch Payroll
- Small Business Superannuation Clearing House
- Standard Business Reporting
- SuperTICK

System maintenance pages for related systems:

- Australian Business Register scheduled site maintenance⧉
- Australian Business Registry Services system maintenance⧉
- myGovID system maintenance⧉
- Relationship Authorisation Manager system maintenance⧉
- Standard Business Reporting status and availability⧉

Back to top

Troubleshooting, technical help and performance dashboards

Troubleshooting – if you are experiencing a system issue or error message.

Technical helpdesk⧉ – assistance with technical log-on, connection, firewall and virtual private network (VPN) issues.

[Online Services for Agents dashboard](#)⧉ – availability and performance of Online services for agents.

[Practitioner Lodgment Service dashboard](#)⧉ – availability and performance of the practitioner lodgment service.

[Superannuation dashboard](#)⧉ – availability and performance of superannuation enabling service.

[Online Services for Business dashboard](#)⧉ – availability and performance of Online services for business.

Staying informed

[Subscribe to email updates](#) to be alerted when this page is updated.

Subscribe to [tax professionals alerts](#) to receive email notification for unplanned Online services for agents or practitioner lodgment service maintenance windows and functionality issues.

Follow us on [Facebook](#)⧉ or [Twitter](#)⧉ for updates and reminders of major system maintenance.

[Back to top](#)

Voice authentication

- https://www.ato.gov.au/General/Online-services/Voice-authentication/
- Last modified: 29 Jun 2021
- QC 52543

Voice authentication is a fast and easy way to confirm your identity when you phone us.

You just need to save your voiceprint with us. Your voiceprint is unique to you.

It is the digital representation of the sound, rhythm, physical characteristics and patterns of your voice.

Once you have saved it with us, we confirm your identity by matching the characteristics of your voice to your voiceprint.

On this page:

- [Benefits of saving your voiceprint](#)
- [How to enrol](#)

- [Secure authentication](#)
- [It differs from voice recognition](#)
- [Delete your voiceprint](#)

Benefits of enrolling your voiceprint

Benefits to saving your voiceprint include:

- you save time confirming your identity when you phone us
- you do not need to answer security questions every time you phone us
- it is a secure way of confirming your identity.

How to enrol

Enrolling your voiceprint is optional. You can choose to enrol your voiceprint the next time you phone us.

The next time you [phone us](#) you will be asked to enter your tax file number (TFN) before being invited to enrol your voiceprint.

1. When prompted, you will be asked to repeat the phrase 'In Australia, my voice identifies me' 3 times. This recording is used to create your voiceprint.
2. You will then need to establish your identity by providing details of information currently on our records.
3. Once you have successfully answered these questions, your voiceprint enrolment is complete. You can then use your voiceprint to confirm your identity in future.

If you do not want to register a voiceprint, you can decline.

Secure authentication

Voice authentication is both a reliable and secure way of confirming your identity.

Voice authentication accounts for a variety of factors, such as background noise and changes in a voice.

When you phone us, the voice authentication system we use can verify you even if:

- you have a cold
- your voice has aged since your last contact
- you have an altered emotional state.

We are able to do this by analysing up to 120 characteristics in your voice, such as pitch and tone and how you speak.

By matching these characteristics against the voiceprint you have enrolled with us, we can then accurately confirm your identity.

These, and other additional security elements of voice authentication, make it very difficult for someone else to mimic your voiceprint and access your personal information.

It differs from voice recognition

Voice recognition tries to work out what you have said. Voice authentication analyses the unique characteristics of your voice to confirm who you are.

Delete your voiceprint

You can delete your voiceprint at any time after you enrol. For security reasons, you will need to phone us on 13 28 61 and speak to a customer service representative who can help you.

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