Australian Government
Department of Education, Skills and Employment

Questions raised at the Provider Consultation Forum on 20 October 2021

myGovID, Provider Experience, Right Fit for Risk

Category of Questions

myGovID: timing

1. Any exceptions to the deadline of 25 March 2022? Will CDP providers in remote locations need to switch over by that date too?

There is no exception to 25 March 2022. The key message here is to start the transition now (to setup myGovID) and test your connection to departmental systems from 1 February 2022 when myGovID authentication is switched on. Any users who do not have a myGovID account post 25 March 2022, will be required to do so before they can access departmental systems such as ESS Web.

myGovID: set up and troubleshooting

2. A lot of the problems we have with access can be solved at a provider level, which means that if we've got issues, we can use our OSCs and other people to solve those problems. How responsive is the Department going to be to support authentication issues with myGovID, particularly for providers in remote areas?

myGovID has been in production for over two years, and it is the only way any tax agent or bookkeeper can access online services with the Australian Taxation Office (ATO). The key learning from rolling out myGovID to these users was early adoption of myGovID by the individual is crucial to iron out any onboarding issues. This includes rectifying mismatched identity documents, or any other issues users might encounter.

If anyone needs support setting up their myGovID, they should call the myGovID helpline. This helpline is run by the ATO, who built and administer myGovID for Government.

Once an individual has a myGovID account, it is easy to maintain and there are very few issues with reinstalling it on a new device or reasserting on a new device.

Some of the issues observed to date, which can be resolved by adopting the technology as early as possible, are:

- an entity not using a staff member's full legal name in the Relationship Authorisation Manager (RAM) authorisation (causing a mismatch with the user's myGovID account when accepting the authorisation),
- not setting up the RAM authorisation correctly (e.g. didn't give access to the government agency needed), or
- forgetting to offboard somebody and that person continues to have access.

So, the big focus for all Providers is two-fold: firstly, encourage your staff to setup their myGovID account with Standard identity strength as early as possible, and secondly, connect them to your business through the RAM.

This ensures your organisation is in the best position to immediately use myGovID to authenticate to departmental systems from 1 February 2022 onwards.

The department will also develop additional guidance and task cards between now and February 2022 to streamline user onboarding and offboarding processes within RAM.

3. If I forget to bring my phone into work, or it gets stolen, I won't be able to log into ESS Web? It might be an issue asking staff to use their personal mobile phones.

Correct, from 25 March 2022 onwards your staff will not be able to access departmental systems without a mobile device with their myGovID account. However, users can install and set up the myGovID app on multiple devices (e.g. on a mobile phone and an Android/iOS tablet).

When setting up your myGovID again, either on a new device or on the same device, select 'I am an existing user' from the myGovID app. Note that you will need to prove your identity for each device so that we can be assured it is really you accessing its service and it will automatically connect to existing authorisations. You can get more help from: https://www.mygovid.gov.au/need-help#mygovid-on-multiple-or-new-devices.

With regards to asking staff to put a myGovID on their personal devices, this was identified as a key issue when myGovID was rolled out to tax agents, however we found that when the time came to implement the change, the issue disappeared quickly as the technology was better understood by users. In cases where a Provider issues mobile devices to staff, this may offer choice, however, staff may still choose to install myGovID on their personal devices to access their individual government services. Respective situations may be resolved through updating your organisational policies accordingly.

During the session, there were also questions how myGovID aligns with requirements of the Right Fit For Risk (RFFR) program. The RFFR requires that all Providers satisfy at the very least Maturity Level One of the Australian Cyber Security Centre Essential Eight. See here: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

There is nothing in the RFFR that expressly prevents the use of mobile devices in your workplaces. MFA is now in fact required for all internet-facing government systems according to Maturity Level One, so myGovID is bringing departmental systems such as ESSWeb to satisfy these very same requirements. With these standards now placed on all Government digital platforms, myGovID and other types of MFA will be the accepted norm.

4. How does someone resolve mismatching personal documents when verifying their myGovID identity?

Users facing issues in verifying their identity though myGovID should call the myGovID Help Line. The Help Page is: https://www.mygovid.gov.au/need-help.

5. What considerations are there for people with vision impairments accessing MyGovID on their phone?

Accessibility options are supported through the user's mobile device (iPhone or Android). There is additional clarification through the myGovID Help Page here: https://www.mygovid.gov.au/need-help#mygovid-accessibility-features.

6. Under our RFFR requirements we do not allow staff to use their personal phones to connect to our systems. By a staff member having access to myGovID on their personal phone doesn't this pose a risk as they are accessing ESS from an app on their personal phone?

The myGovID account on the mobile device is only used to authenticate the user's login into departmental systems. The mobile device itself does not access ESSWeb or other departmental systems; all interactions with departmental systems remain on the user's computer, laptop or workstation. Once logged in, the mobile device is no longer needed until the next time the user is required to re-authenticate.

There were also questions how myGovID aligns with requirements of the Right Fit For Risk (RFFR) program. The RFFR requires that all Providers satisfy at the very least Maturity Level One of the Australian Cyber Security Centre Essential Eight. See here: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

There is nothing in the RFFR that expressly prevents the use of mobile devices in your workplaces. MFA is now in fact required for all internet-facing government systems according to Maturity Level One, so myGovID is bringing departmental systems such as ESSWeb to satisfy these very same requirements. With these standards now placed on all Government digital platforms, myGovID and other types of MFA will be the accepted norm.

7. Does myGovID apply to GovTeams?

No, this won't apply to GovTeams. There may be decisions that the GovTeams team will look at in relation to MFA in the future, but those decisions are not at the department's discretion.

8. Can multiple users register on the same mobile device using the same email address?

No. The myGovID app on a specific device can only support one myGovID account at a time. Think of it like a Driver's Licence (albeit digital) — the Licence will only verify your identity, not someone else's.

myGovID: logging onto ESS Web

9. When I log into ESS Web using myGovID, do I only have to enter the login code when I logon for the very first time, or do I have to enter the code every time I logon?

From 25 March 2022 onwards, every time you log into departmental systems such as ESSWeb, you will be given a login code (four digit PIN) on the screen. When the user enters this PIN into their myGovID app on the mobile device, it will verify their identity and grants access into departmental systems.

It is similar to a Security code sent by text message, but with a higher grade of identity verification. Once you're in ESSWeb, you won't be asked to log in with your myGovID again for the remainder of the session. However, if you logoff or close your browser, you will need to log in again in the manner described above.

10. Does this mean I now have to access ESS Web through my phone?

The myGovID account on the mobile device is only used to authenticate the user's login into departmental systems. The mobile device itself does not access ESS Web or other departmental systems; all interactions with departmental systems remain on the user's computer, laptop or workstation. Once logged in, the mobile device is no longer needed until the next time the user is required to re-authenticate.

11. Given the mobile device requirement it's safe to assume this can't be linked to a hardware key, like yubi or other?

Correct, myGovID cannot be connected to other MFA devices like yubi or Duo.

12. What is the time out duration?

myGovID does not change the existing login duration you currently get from respective departmental systems such as ESSWeb.

myGovID: onboarding and offboarding staff

13. What's the process for bringing that initial administrator on board who can then go into RAM and authorise staff access to DESE agency services ESS Web?

It is likely that your organisation already has an administrator set up in RAM for accessing Government online services for tax purposes. If your organisation does not have RAM set up, the Principal Authority of the business will need to set up their myGovID and link the business in RAM. Once the business is linked, they can set up authorisations for others to work on behalf of the business. Further information on how to get started in RAM can be found at the Relationship Authorisation Manager website (see: https://info.authorisationmanager.gov.au/get-started). Linking staff's myGovID accounts to RAM can be set up at any time, and we encourage Providers to do so as early as possible in preparation for the transition to myGovID in early 2022.

14. What is the process to migrate staff accounts over to myGovID?

Getting a myGovID itself does not require a migration process. For staff members who have existing accounts to access departmental systems, they will need to be invited through eSAM to link their myGovID account to their eSAM account. This will allow a staff member to retain their existing eSAM account. This will also ensure continuity of logs and training completion history from before and after myGovID is linked to their eSAM account.

Further guidance and task cards will be issued by the department between now and February 2022 to help clarify the linking steps required.

15. If people will now login to ESS Web using their new myGovID, will provider businesses lose user information and activity stored in eSAM that is associated with legacy ID's?

All eSAM identities will continue to be used, thus information currently in eSAM will continue to be in use. If staff members link their myGovID to their existing eSAM account (through invitation from their administrators in eSAM), then they will retain their ESSWeb user information and roles to access functions. All myGovID will do is provide a secure key for an individual to authenticate and use their eSAM identities.

16. When staff leave an organisation, what is the process of notifying you the staff member has left work? How do you decouple the permissions assigned to what is a personal credential?

Just like the OSC role today, there is an Authorised Administrator for myGovID in your organisation. The Authorised Administrator is the official who should be removing departing staff members, which should be performed in RAM. See help page on RAM: https://info.authorisationmanager.gov.au/.

Access to departmental systems can also be disabled in eSAM as it does today, however, this only applies to DESE systems such as ESSWeb and CDP.

17. I have myGovID already. Will I be able to access the Provider Portal without a business authorisation via RAM or do we need to get RAM completed as well?

Yes you will need RAM completed as well. This help page about RAM will help clarify how to link a myGovID account to RAM: https://info.authorisationmanager.gov.au/.

However, this authorisation cannot be used to access departmental systems until 1 February 2022 onwards.

Right Fit for Risk (RFFR) Accreditation

18. Is there any timeframe yet for Essential 8 maturity level 3

We ask that Maturity Level One is the minimum that you get to gain Accreditation. We are not mandating any timeframe or requirements to get to Maturity Level Three, unless you believe that is important for your organisation.

You can click here to get more information about Maturity Level One: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

19. We are a micro-business is there any way we can access assistance to gain RFFR accreditation?

Small Providers (servicing less than 2,000 clients) must gain RFFR accreditation by 1 December 2021. Email SecurityComplianceSupport@dese.gov.au if you are experiencing significant challenges preparing your RFFR submission.

20. Does RFFR apply equally with contracts with DSS?

If you have any contracts with DESE today (jobactive, NEIS, etc), these will take primacy and there will be an expectation for you to complete RFFR accreditation in accordance with the communicated timeframes. If you are a Provider to other departments such as DSS or NIAA, and you are not contracted with DESE, we encourage you to contact DSS regarding their RFFR expectations and timeframes.

It is not mandatory to use the DESE Scheme, that is something that is being worked through with JAS-ANZ and the auditing community. The scheme is something that has been published purely for the certifying bodies to upskill themselves to the departmental expectations. You do NOT need to use the DESE scheme to gain accreditation. The quickest

way to gain accreditation today — if you are a medium and large provider — is to complete the customised ISO 27001 certification.

For small organisations servicing less than 2,000 clients, you can complete that on self-assessment as well. If you would like further assistance in this area, please contact SecurityComplianceSupport@dese.gov.au.