Multi-factor authentication troubleshooting guidance

For biodiversity systems

Department of Climate Change, Energy, the Environment and Water

NSW GOVERNMENT

Acknowledgement of Country

Department of Climate Change, Energy, the Environment and Water acknowledges the Traditional Custodians of the lands where we work and live.

We pay our respects to Elders past, present and emerging.

This resource may contain images or names of deceased persons in photographs or historical content.

Artist and designer Nikita Ridgeway from Aboriginal design agency Boss Lady Creative Designs created the People and Community symbol.

Cover photo: Farmland. Beowa National Park. Nick Cubbin/DCCEEW

Published by:
Environment and Heritage
Department of Climate Change,
Energy, the Environment and Water
Locked Bag 5022, Parramatta NSW 2124
Phone: +61 2 9995 5000 (switchboard)
Phone: 1300 361 967 (Environment and Heritage enquiries)
TTY users: phone 133 677, then ask for 1300 361 967
Speak and listen users: phone 1300 555 727, then ask for 1300 361 967
Email info@environment.nsw.gov.au
Website www.environment.nsw.gov.au

ISBN 978-1-923357-10-5
EH 2024/0327
First published in November 2024; reissued December 2024

Find out more at:

environment.nsw.gov.au

Contents

What is multi-factor authentication?

Multi-factor authentication (MFA) is a security measure that enhances login protection by requiring 2 forms of identification – typically a password and a one-time password (OTP) sent to your mobile or email. This additional step helps safeguard your account from unauthorised access.

Why are we introducing multi-factor authentication?

The NSW *Cyber Security Policy* mandates best practices to protect against common cyber security threats.

MFA makes it significantly harder for someone to gain unauthorised access to your accounts. With MFA enabled, even if an attacker has your password, they will not be able to progress further without that second factor of authentication.

How does multi-factor authentication work?

MFA works by requiring 2 steps during login:

- your password
- OTP sent to your email or Australian mobile.

When logging into Biodiversity Accredited Assessor System (BAAS) or Biodiversity Offsets Agreement Management System (BOAMS), you will be prompted to enter your username, password, and the OTP sent to your mobile or email.

Is multi-factor authentication the same as verification of identity?

No. MFA enhances the security of your login process. Identify verification is a separate process where users may need to provide identity documents to prove who they are. The department may ask for such documents if you need to recover access to your account.

What do I need for multi-factor authentication?

To use MFA, you need either or both an :

- Australian mobile number
- email address.

Tip: Ensure your mobile number and email address are up to date in your account.

Who will be impacted by multi-factor authentication?

All assessor applicants, accredited assessors, community users, council members and consent authority members accessing BOAMS or BAAS will be required to use MFA for enhanced security.

Will multi-factor authentication be required for all future system logins?

Yes, once MFA has been rolled out, it will be required each time you log in to ensure your account remains secure.

Can I choose which method (email or mobile) to receive my one-time password?

Yes, you can select either your mobile number or email as your preferred method for receiving OTP each time you log in.

Do I need to install multi-factor authentication?

No, MFA does not require any additional installation. It is integrated directly into your login process.

What type of phone do I need for multi-factor authentication?

MFA works on any phone with SMS capability. You do not need a smartphone, nor specific software versions.

What if I have poor network connectivity?

You will need access to an Australian mobile number or your email to receive the OTP. If mobile network issues are common, choose the email option to receive the OTP.

Can I use an international mobile number for multi-factor authentication?

No, only Australian mobile numbers can be used for the MFA process.

What happens if I have changed my mobile number or lost my phone?

Each time you log in to your BOAMS or BAAS account, you will be prompted to choose the way you want to receive your OTP. So, if you have changed your mobile phone number select the email option to receive the OTP, then update your mobile number in your account settings.

What happens if I lose access to my email account?

Each time you log in to your BOAMS or BAAS account, you will be prompted to choose the way you want to receive your OTP. So, if you have lost access to or changed your email account, choose the mobile option to receive OTP, then update your email address in your account settings.

What happens if I change my job?

As an accredited assessor, your accreditation is assigned to you as an individual. You can consider using your personal mobile number and email address for continuity. You can also easily update the contact details associated with your account as and when needed.

What should I do if I am unable to receive my one-time password via email, even after updating my account with a valid email address?

If you are still unable to receive your OTP via email, even after updating your account with a valid email address, it may be due to your organisation's IT policies or restrictions on certain email domains. In this situation we recommend that you choose to receive OTPs via your Australian mobile phone when logging in.

What should I do if I encounter an error when choosing the method to receive my one-time password?

If you encounter an error when choosing how to receive your OTP, return to the previous page and select an alternate method to receive your OTP. If the error persists, please contact bosdigital@dcceew.nsw.gov.au.

Will the process for assessors adding councils and consent authorities as case parties change with the introduction of multi-factor authentication?

No, the process assessors follow to add councils and consent authorities as case parties will **not change** with the introduction of MFA. Assessors can continue assigning cases as they currently do, and councils and consent authorities will still receive access as usual.

Why are councils and consent authorities being asked to create individual Biodiversity Offsets and Agreement Management System accounts?

Individual Biodiversity Offsets and Agreement Management System (BOAMS) accounts are being introduced to enhance system security, especially with the addition of multi-factor authentication (MFA). Having individual accounts helps ensure that each login is verified and secure, offering better protection for both user information and system data.

Can councils and consent authorities still use their shared login accounts?

Yes, **shared logins will remain active** for the time being. Councils and consent authorities can continue using shared credentials, and they will still have access to

cases assigned to their shared login. We are, however, encouraging individual team members to create their own BOAMS accounts as part of a gradual shift to increased security.

Will users with individual Biodiversity Offsets and Agreement Management System accounts be able to see cases assigned to the shared council/consent authority account?

Yes, council and consent authority users who log in using individual BOAMS accounts will still be able to access cases that have been assigned to the council or consent authority's shared login account.

Is there a plan to eventually phase out shared logins for councils and consent authorities?

While shared logins remain active for now, creating individual accounts is a step towards better security practices. We will provide advance notice and detailed guidance before making any future changes to shared account access.

What are the benefits of using individual accounts over shared logins?

Individual accounts, combined with MFA, offer improved security, accountability, and control over system access. They help ensure that only verified, authorised users access sensitive data, reducing security risks associated with shared credentials.

Can I use a third-party authenticator tool, like Microsoft Authenticator, for multi-factor authentication in Biodiversity Offsets and Agreement Management System?

BOAMS does not support third-party authenticator tools, such as Microsoft Authenticator, for multi-factor authentication (MFA). Instead, BOAMS sends a one-time password (OTP) directly to your registered mobile number via SMS or to your registered email address. This approach ensures that all users can complete MFA without needing to download or set up additional apps, making the process simple and accessible for everyone.

Multi-factor authentication support

For MFA-related technical issues or assistance, please visit our Biodiversity Offsets and Agreement Management System page or email bosdigital@dcceew.nsw.gov.au.

More information

NSW Cyber Security Policy