

AIA i-learn Manual_ Login Process

Table of contents

Section 1 - Login with Multi-Factor Authentication (MFA).....	2
Section 2 - One Active Session per User.....	4
Section 3 - Password Policy	5



Section 1 - Login with Multi-Factor Authentication (MFA)

Users with the role 'ID Office Focal Admin' must verify their login to the platform using a code sent to their email.

After entering their username and password, the system will request a security code that will be sent to their email, which they must then enter.

1. Log in using 'Non AIA Employee Login'

Welcome to Athens International Airport Training Center!

If you are an employee of AIA, click on the button below to log in to the e-learning platform

[AIA Employees Login](#)

If you are not an employee of AIA, click on the button below to log in to the e-learning platform

[Non AIA Employees Login](#)

English (en) ▾

2. Enter username and password

If you are not an employee of AIA, click on the button below to log in to the e-learning platform

[Non AIA Employees Login](#)

Sign In

[Forgot Password?](#)


[Log in](#)



3. Enter the code received via email

2-step verification


To keep your account safe, we need to check that this is really you.

 **Verify it's you by email**
We've just sent a 6-digit code to your email: f****1@test.gr

Enter code

[Continue](#)

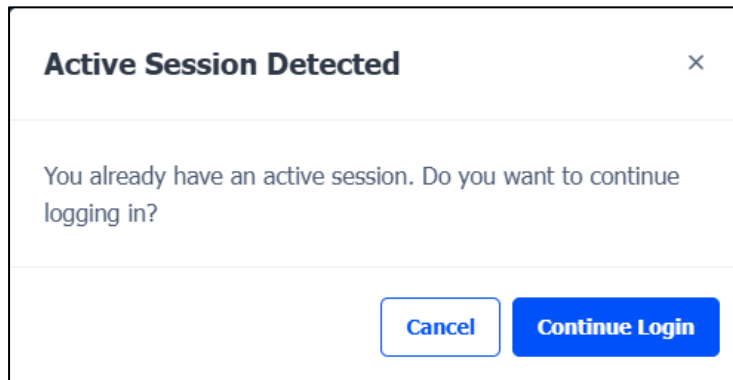
[Cancel login](#)

Need help?

[Contact site support](#)



Section 2 - One Active Session per User

Each user is allowed to have only one active session. This means that if a user is already logged in and attempts to log in from another browser, another device, or in an incognito window—or if someone else tries to log in using their account—the following message will appear:



If the user chooses to continue, the previous session will automatically terminate, and the original user will be logged out from all systems (i-Learn, ID Office, Booking).



Section 3 - Password Policy

The new password must meet the following requirements:

- Length: must be at least 12 characters long
- Complexity: must include at least one (1) uppercase letter, one (1) lowercase letter, one (1) number, and one (1) special character. The use of more than four (4) consecutive characters of the same category (uppercase, lowercase, numbers, and symbols) is not allowed
- Expiration/Validity: passwords must be changed at least every 90 days
- History: must be different from the last 5 passwords
- Security: must not contain the user ID or more than two consecutive identical characters, and must not include dictionary words or personal user information that can be easily guessed (e.g., surname, car license plate number, date of birth, address, phone number, etc.)

Upon the first login after these changes, users will be required to change their password so that it complies with the new password policy, by following the steps below:

1. Log in using 'Non-AIA Employee Login'

Welcome to Athens International Airport Training Center!

If you are an employee of AIA, click on the button below to log in to the e-learning platform

[AIA Employees Login](#)

If you are not an employee of AIA, click on the button below to log in to the e-learning platform

[Non AIA Employees Login](#)

English (en) ▾



2. Enter username and password

If you are not an employee of AIA, click on the button below to log in to the e-learning platform

[Non AIA Employees Login](#)

Sign In

dispatcher

.....

[Forgot Password?](#)

[Log in](#)

3. Continue by clicking 'Continue Login'

Active Session Detected ×

You already have an active session. Do you want to continue logging in?

[Cancel](#) [Continue Login](#)



4. Enter a new password that meets the required specifications

You must change your password to proceed. ×

Change password

Username

The password must have at least 12 characters, at least 1 digit(s), at least 1 lower case letter(s), at least 1 upper case letter(s), at least 1 special character(s) such as *, -, or #, compliance with a custom set of security controls.
Passwords must not contain 4 consecutive characters of the same type (uppercase letters, lowercase letters, numbers or symbols).
Passwords must not contain your username or personal information (name, email, phone, address, custom profile data, etc.).
Passwords can be reused after 5 changes

Current password

New password

New password (again)

Log out all other browser sessions ⓘ

ⓘ Required