97 TRS

PLATFORM ONE (P1) ChatOps Setup Guide

Platform One General Overview

Key areas you should know

- What is Platform One (P1) ChatOps?
- Platform One Profile Setup
- Platform One Registration
- Platform One Licensing
- Platform One Access
- Multifactor Authentication Setup
- Login
- Quick-Switch Reference Guide (Mattermost -> P1 ChatOps)
- FAQ
- Troubleshooting

What is Platform One ChatOps? (P1)

- P1 ChatOps is the certified mobile application for Platform One (P1) and its customers. It provides secure chat and collaboration capabilities for mission execution in conjunction with Mattermost
- Mattermost is migrating to P1 ChatOps 14 May 2025 and Mattermost will no longer receive push notifications

Platform One Profile Setup

The first few things you should do

ON A DESKTOP COMPUTER (USE EDGE BROWSER)

Step 1 ACCOUNT REGISTRATION

1.1 New users can create a Platform One (P1) account at **https://login.dso.mil/register** from a computer with a CAC reader. New users must use their military email to register. **Note.** Internet Explorer browser is not supported.

- Profile Details:
- First Name.
- Last Name.
- Affiliation and Paygrade (select from dropdown menu)
- Unit, Organization (US Air Force)
- Username Ex. John.doe.123 →john.doe.123@us.af.mil (use front part of AF email)
- Email. Complete .mil email. **DO NOT USE PERSONAL EMAILS**

Platform One Profile Setup

The first few things you should do

ON A DESKTOP COMPUTER (USE EDGE BROWSER)

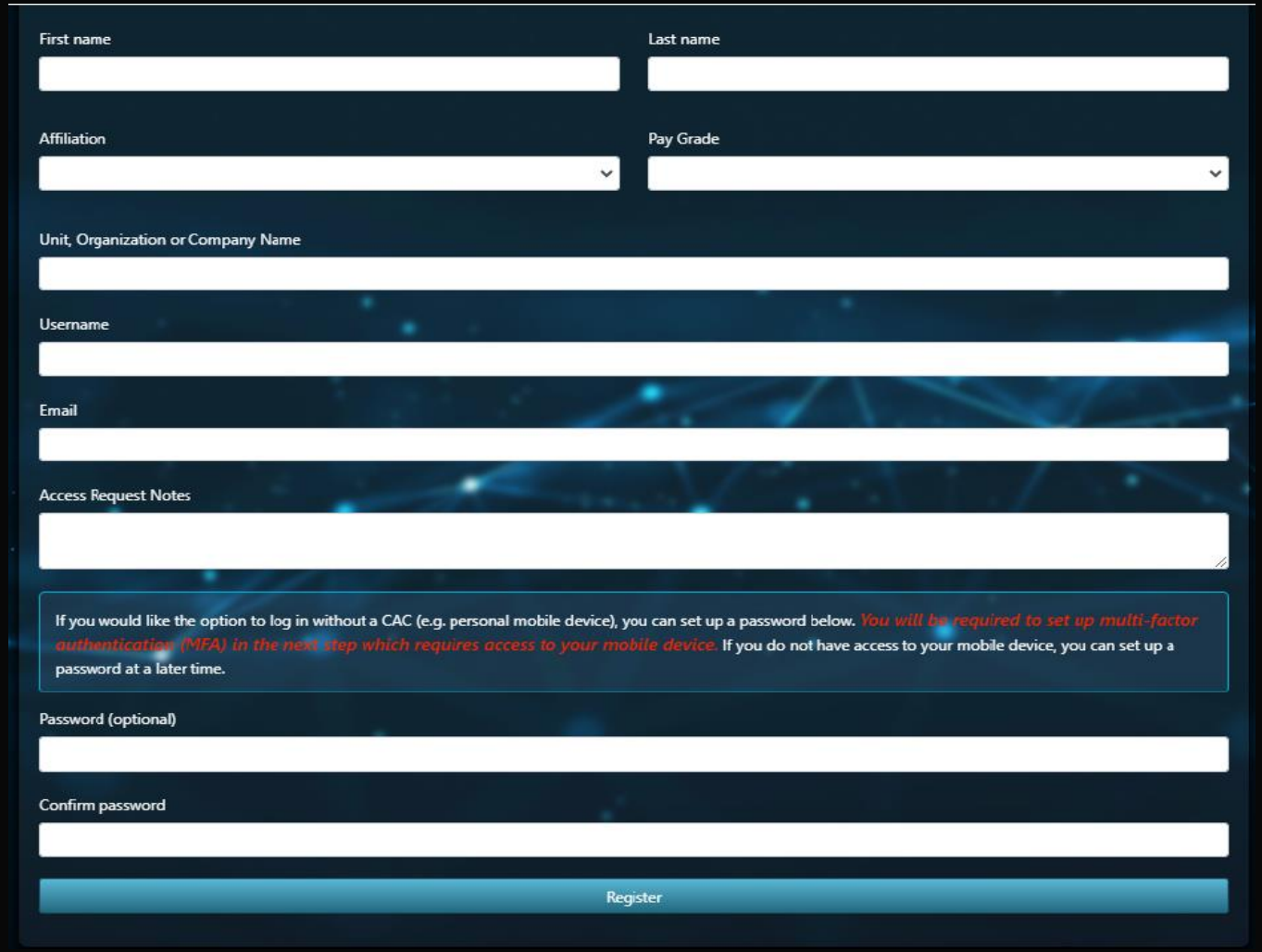
Step 1 ACCOUNT REGISTRATION (continued)

- Password & Confirm Password
  - This is for multifactor authentication which enables users to access P1 ChatOps without their CAC. If a password is entered, it will expect the new user to set MFA up immediately and prevent the user from logging in, even with a CAC, until MFA setup is complete. If a password is entered, the next screen will ask the new user to install an authenticator app (Google authenticator or Microsoft Authenticator) on their mobile device. QR code or navigate to either using the device's app store.

Platform One Registration Page

The first few things you shoulddo

Step 1 (continued)



Platform One Licensing

The first few things you should do

Step 1.2

On-boarding Supervisors Submit New User for Platform One License.

- Altus will onboard individuals 2-3 weeks prior to class start. This is dependent on the individual setting up their account. If account is not setup, we can not onboard you prior to class start

Step 2

- **If your licensing is successful**, Platform One sends the new user an email with a link to activate the license. This sometimes gets filtered to spam so please check your spam folder.

Platform One Access

Step 2.1

New User Activates License

- New user must click link in their email from Platform One to activate the Platform One license. This must occur within 3 days or the link expires and the on-boarding supervisor must resubmit the new user for a license. Check spam folder!

Step 3

Access Platform One Servers

- Once the new user has activated the license, the new user can access the Matermost servers. Server URL for Impact Level (IL) 4 users is https://chat.il4.dso.mil/ . It is authorized for CUI information. DO NOT post classified information on this sever.

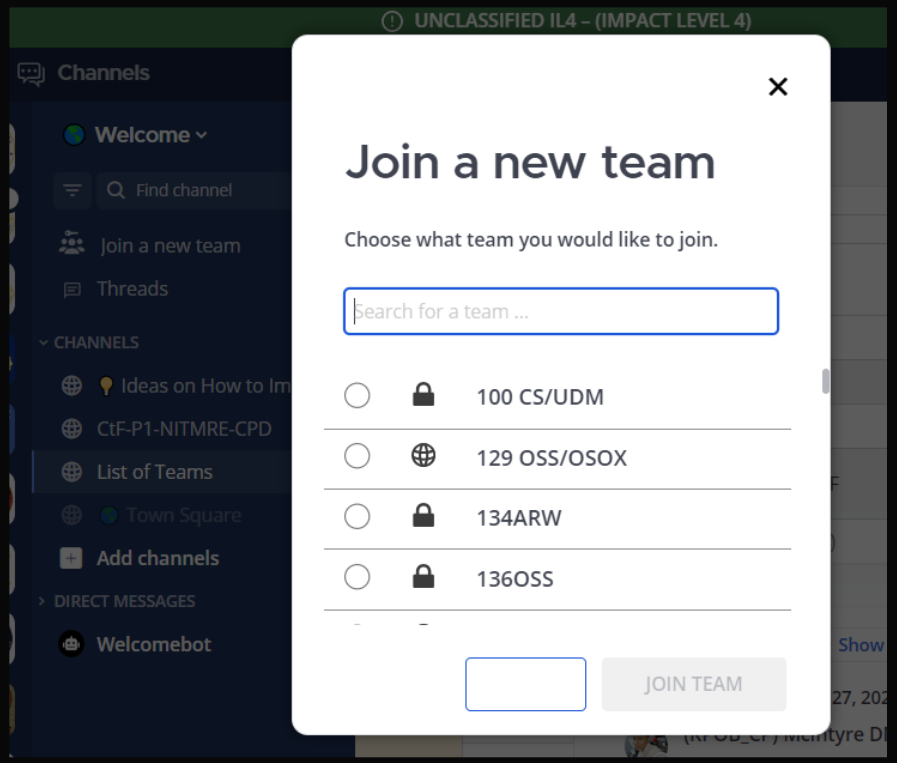
Platform One Access

Step 4 **Join P1 Teams**

- **“Join a new team.”** In the upper left of the mattermost screen, under the team name, select “Join a new team.” Select the applicable team, select join team.

- **Invite Link.** Use a valid invite link. Users can get the invite link from team admins. (See next slides for teams and channels)

- **Slash Command.** Use a slash command. This will send the request to team admins in the P1 ChatOps team. For example, join AFTRANS/MISSION C2 team, use /requestaccess team USAF-618AOC-MOD in any message box and send.

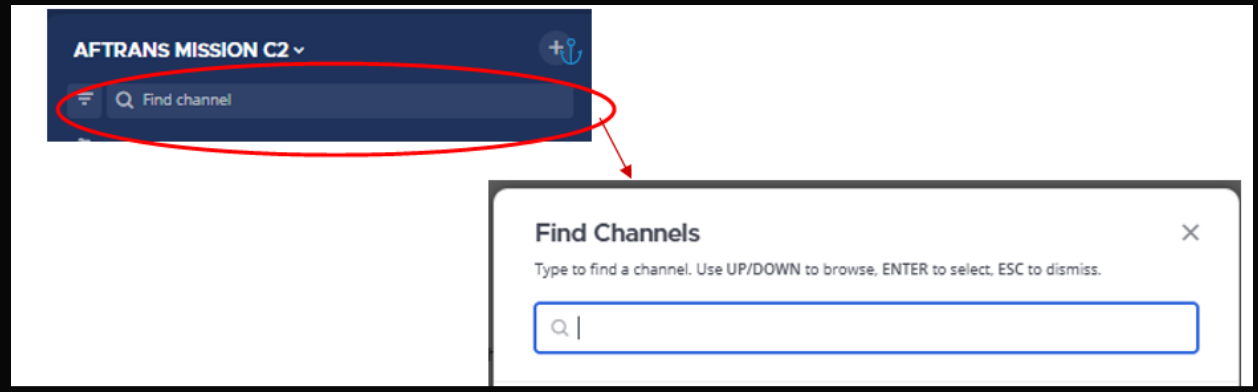


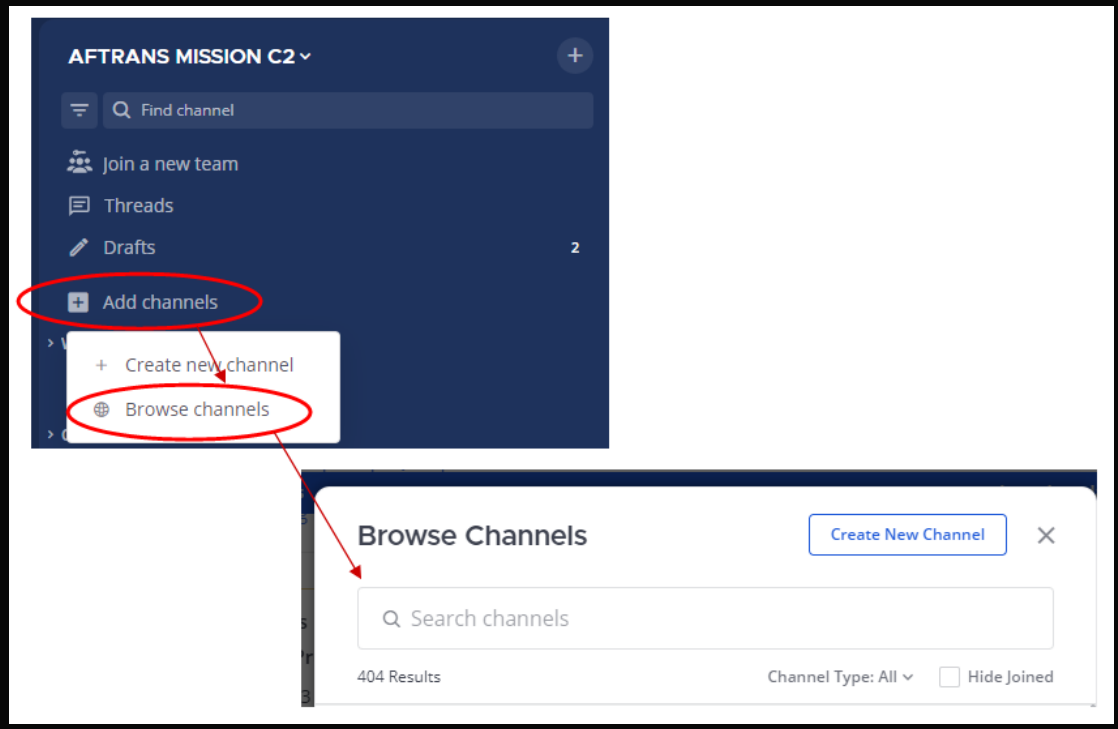
Platform One Access

Step 4.1

Join Mattermost Channels

Mattermost teams are broken into channels (like chat rooms), which can be public or private. Public channels can be joined by selecting “Find channel” and “Add Channels.” Existing channel members can add members to private channels.





Multi Factor Authentication Setup

ON A DESKTOP COMPUTER (USE EDGE BROWERS)

Step 5 **Multi Factor Authentication**

- **What is MFA?** Multi-factor authentication is a method to access P1 Mattermost without needing a CAC, i.e., access from EFB. MFA is like adding an extra lock to your online accounts, where you need your password (the regular key) and something else to prove it's really you trying to access it, like a code sent to your phone, or accessed from an authenticator app. Basically, it's a way to make sure only you can get in, even if someone else figured out your password.

Step 5.1 **Establish P1 Password**

- **Enter a password either during the registration process OR after the initial registration process by going to https://login.dso.mil and clicking Authenticator in the upper right after logging in with a CAC.**

Step 5.1 **Download Microsoft Authenticator OR Google Authenticator App**

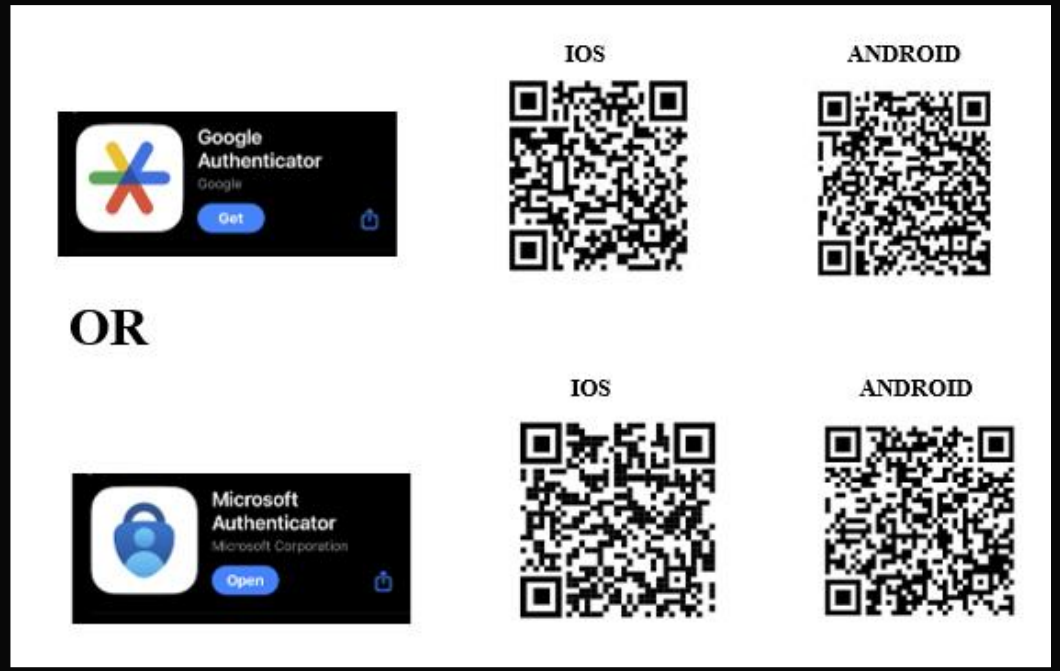
- **Download Microsoft Authenticator OR Google Authenticator App.** If not already downloaded on the device, scan QR code in **Figure A1.7.** to download Google or Microsoft authenticator app on the mobile device or visit app store. Once downloaded, log into the authenticator application.

Multi Factor Authentication Setup

Step 5.2 Link authenticator App with Platform One Account

Open the downloaded authenticator application. User prompts the authenticator app to add a new authentication account (i.e., clicking a plus sign or selecting, “Get Started”). Select “Scan QR Code” > if it asks if for a personal or work account, select work > the application will provide a camera view indicating to scan the QR code for the MFA set-up page. This is the point that the QR code provided at https://login.dso.mil needs scanned.

User will need a new Six Digit Code each time they log in without a CAC.



Scan QR codes to download authenticator

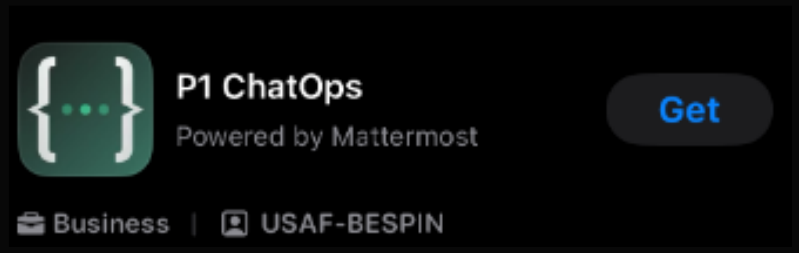
Login

IOS

ANDROID

Step 6

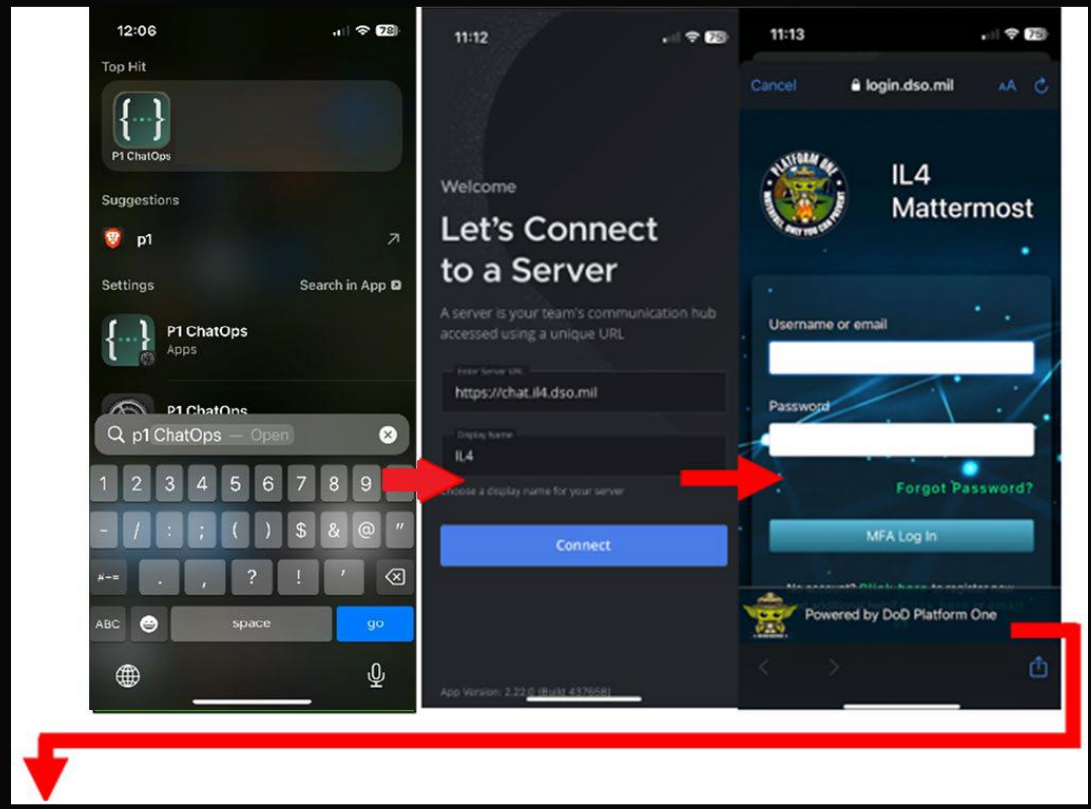
Download P1 ChatOps App



Step 6.1

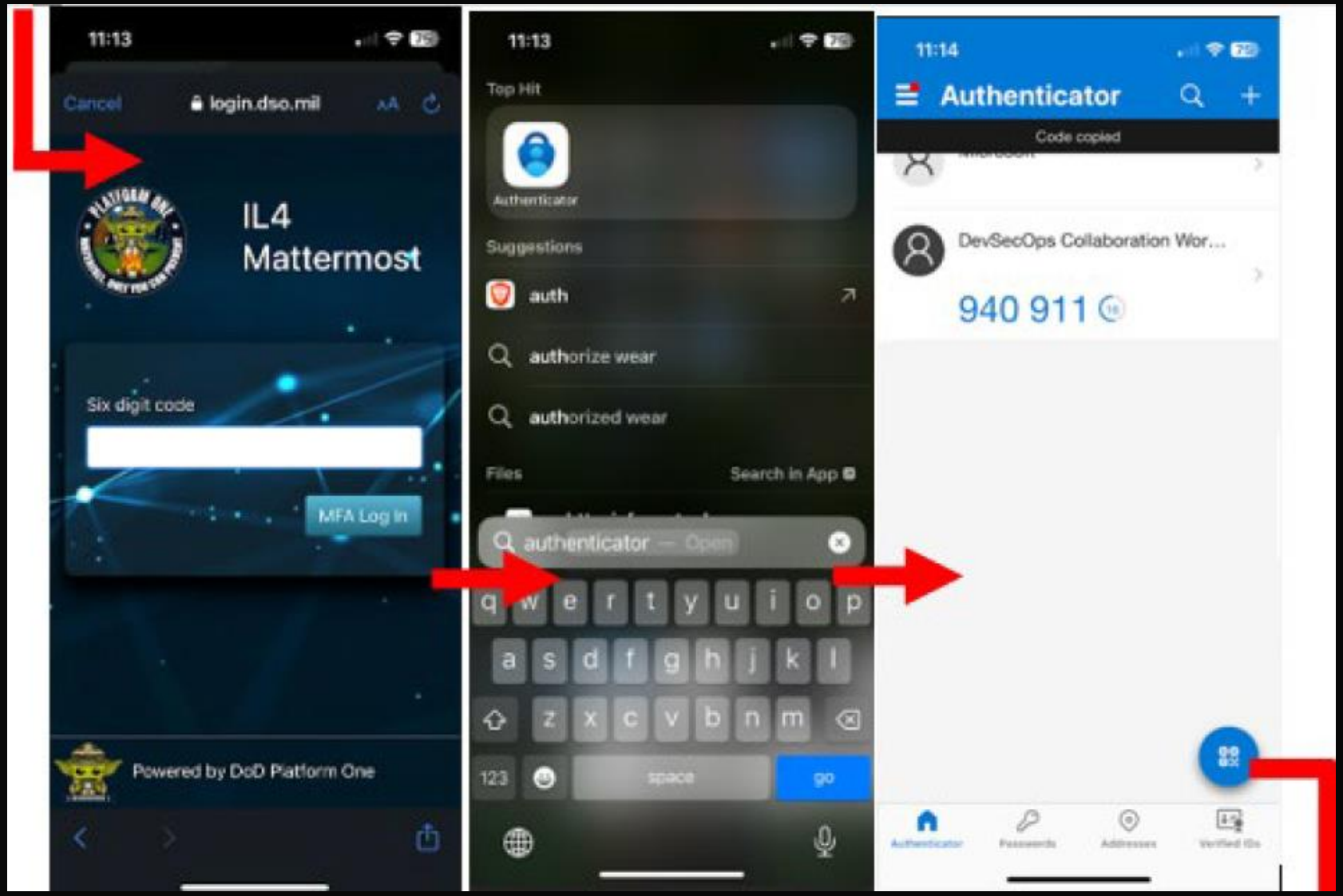
Login to P1 ChatOps App Using Code from Authenticator App (THE MOMENT YOU'VE BEEN WAITING FOR!)

Under server, enter the server URL, such as https://chat.il4.dso.mil . Server name is recommended to be IL4 or CUI. Once *Connect* is selected, the login process will be transitioned into a browers for the user to entere their username and password. (Continue to next slide)



Login

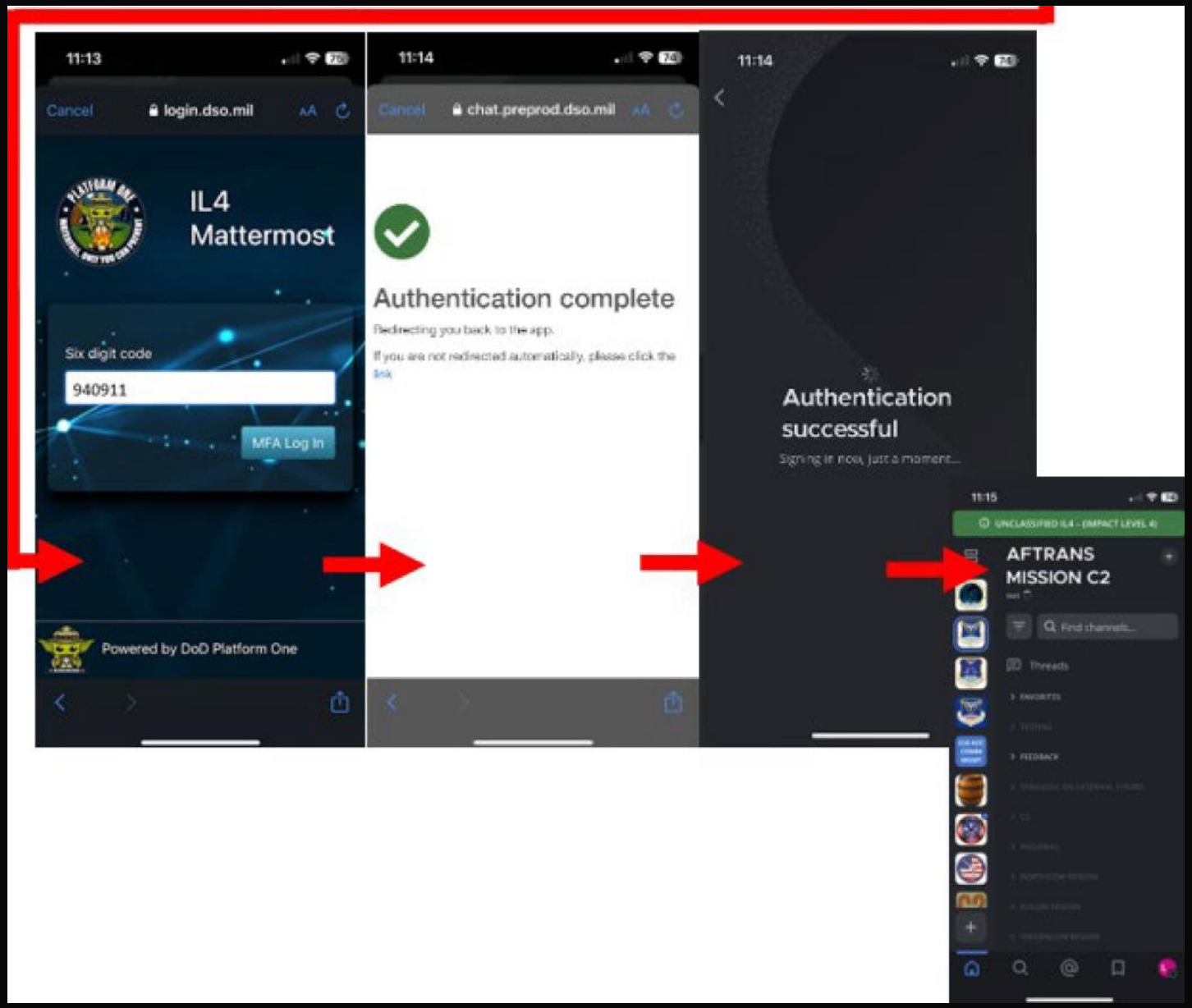
Once MFA Log In is selected, the next screen prompts *Six digit code. Open the downloaded authenticator app. Copy the code from the DevSecOps Collaboration Workspace authentication.*



Login

Switch back to the browser, and paste the code. Select MFA Log In. The next page will indicate “Authentication Successful” and reroute back to the P1 ChatOps App, logged in.

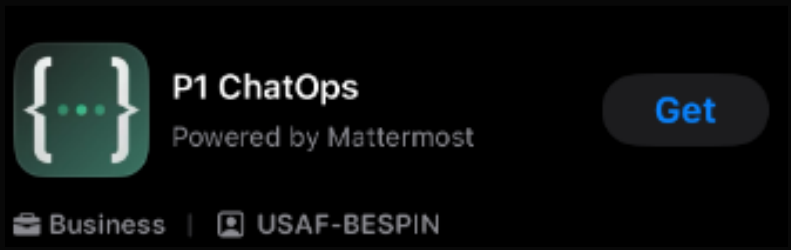
Please see Altus Channels that we would like you in on the next slide. Thank you



Quick-Switch Reference Guide

Legacy Mattermost App -> P1 ChatOps App

- Download P1 ChatOps App



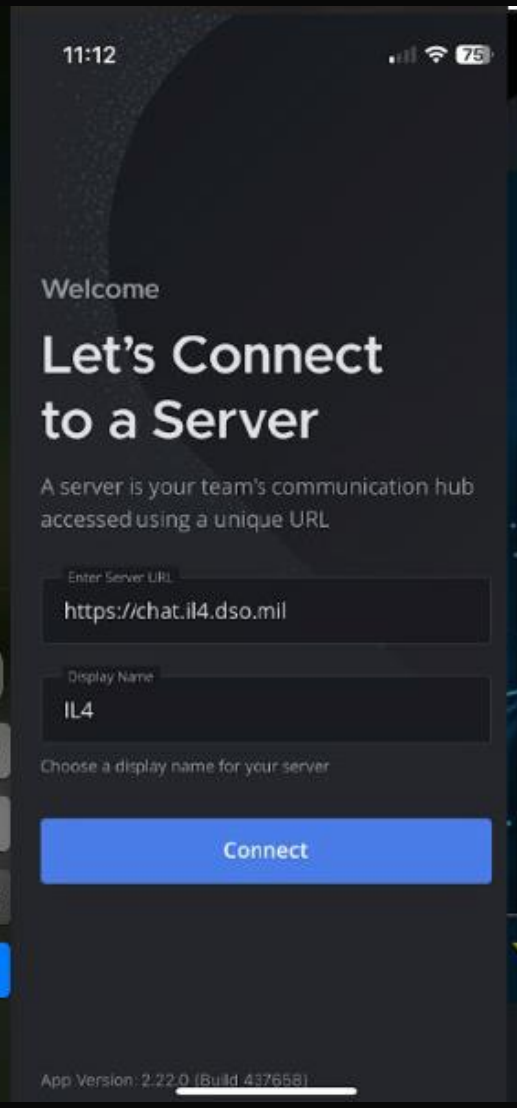
IOS

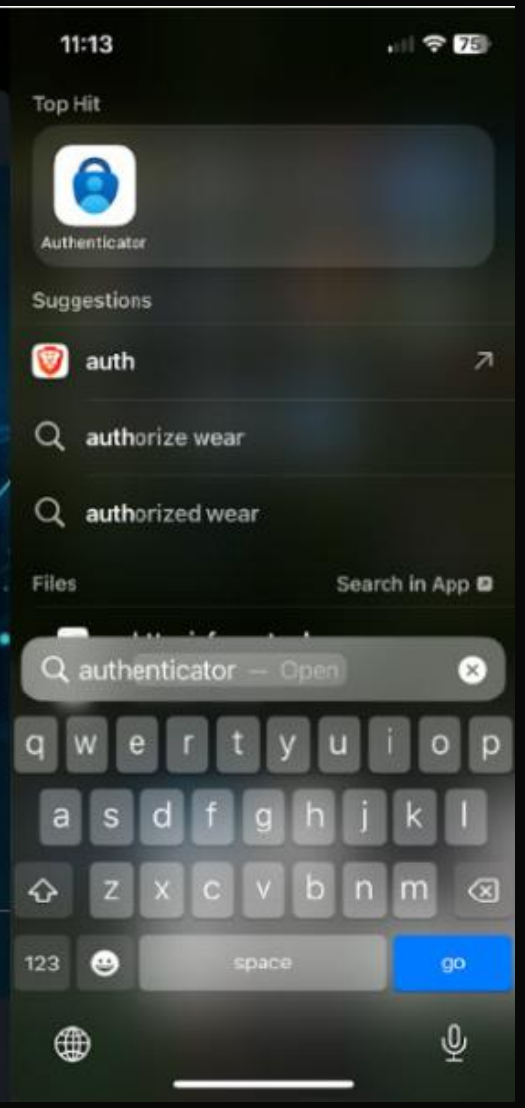
ANDROID

Everything currently done to login will remain the same in exception of using the P1 ChatOps app instead of the legacy Mattermost app.

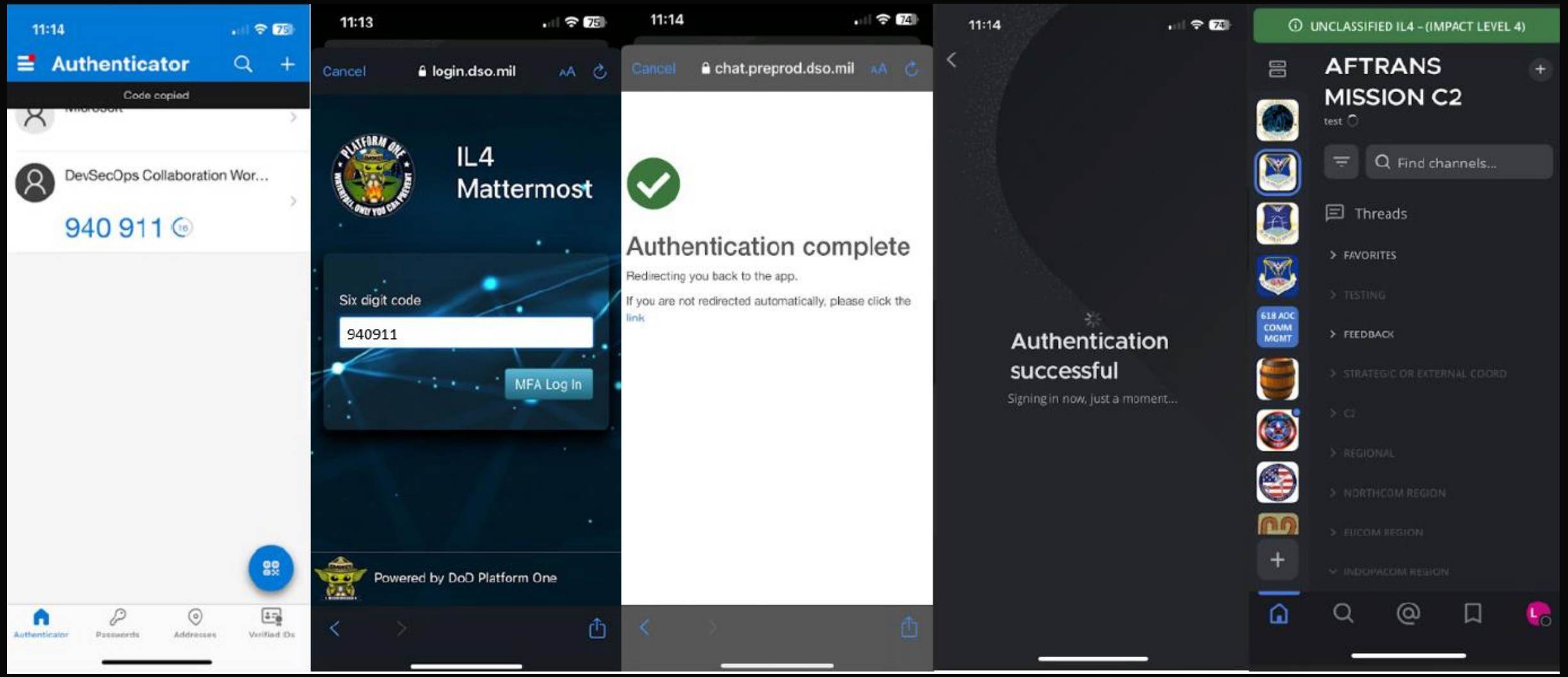
Login to Mattermost P1 ChatOps App Using Code from Authenticator App. User opens the P1ChatOps app on their device. Under server, enter the server URL, such as: https://chat.il4.dso.mil. If IL4 server, server name is recommended to be IL4 or CUI. Once *Connect* is selected, the login process will be transitioned into a browser for the user to enter their username and password. Once *MFA Log In* is selected, the next screen prompts *Six digit code.* Open the downloaded authenticator app. Copy the code from the DevSecOps Collaboration Workspace authentication, switch back to the browser, and paste the code. Select *MFA Log In.* The next page will indicate "Authentication Successful" and reroute back to the Mattermost P1 ChatOps App, logged in.

Quick-Switch Reference Guide





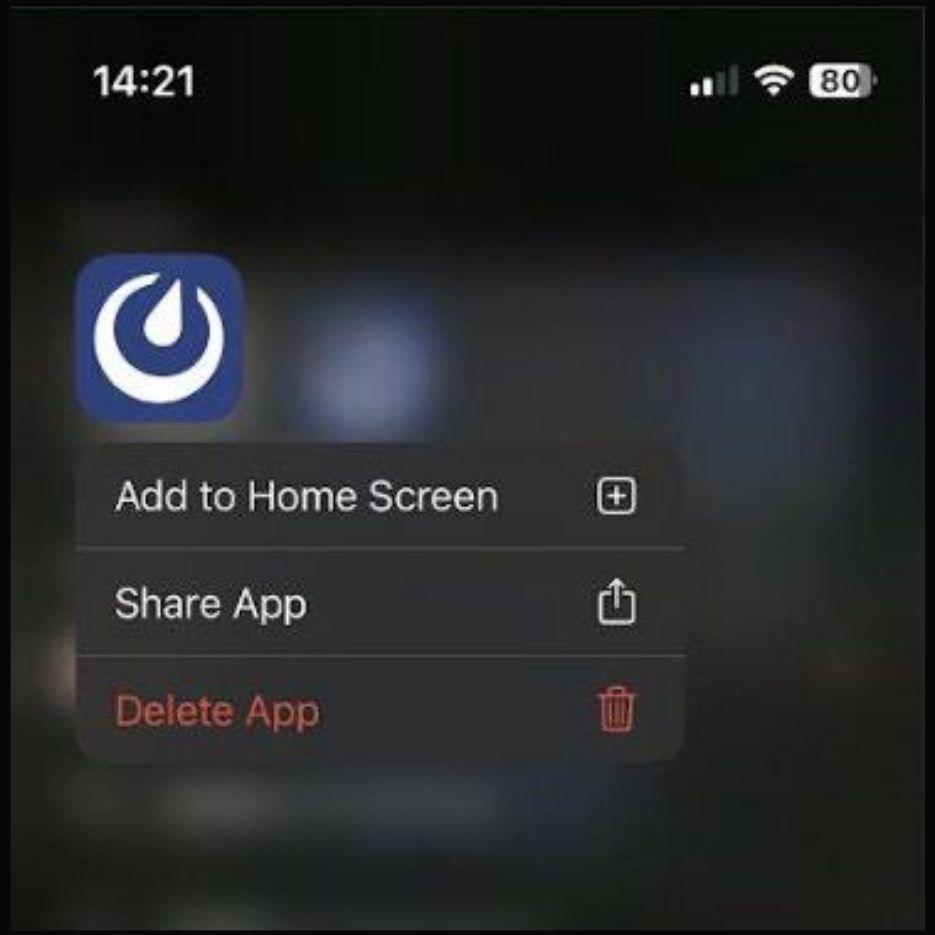
Quick-Switch Reference Guide



Quick-Switch Reference Guide

Remove Legacy Mattermost App from Device

- Locate the Mattermost app previously used to log in and remove it
- from your device.



Troubleshooting

****** MATTERMOST HELP DESK**** START HERE!**

- aflcmc.hncx.p1cst@us.af.mil

Submit trouble ticket:

- https://jira.il2.dso.mil/servicedesk/customer/portal/1/create/36

P1 Support Hub (general help hub)

- https://jira.il2.dso.mil/servicedesk/customer/portal/1/group/7

See 97 Student Admin in building 87 Room 103 or email altus mattermost help orgbox 97trs.tra.altusmmlicensing@us.af.mil

FAQ

“These users could not be found” as a response to On-Boarding supervisor license request. Member did not complete registration and needs to go to https://login.dso.mil to complete. Once they finish the registration, the on-boarding supervisor needs to resubmit the new user for a license.

“You need to verify your email address to activate your account” as a result of new user attempting to log in. Member has a P1 license, but has not activated the link in the email. These links are only valid for 3 days. On-boarding supervisor can resubmit new user for license if the link has expired. If new user is not receiving an email, check spam. If it is not there, submit a ticket to P1.

“Account has been disabled” or **“x509 certificate error”** by an existing user attempting to log in. This can be solved in two ways. An individual with on-boarding supervisor rights must resubmit the member for a license. Once the ticket processes, their login will work again. There will not be another email that they need to activate the license, so the on-boarding supervisor must let the user know they have regained access. Alternatively, the disabled user can email aflcmc.hncx.p1cst@us.af.mil from the email associated to their account with a brief description of the error and one of the following key words in the body: “disabled”, “enable”, or “unlock.” This will prompt an automated system to review the account and reactivate it.

FAQ

“Account has not been granted access to this application group:” Needs a P1 license. Contact someone with On-boarding Supervisor Rights (Mattermost Wing OPR) to submit the individual for a license. Do not submit a ticket to platform one for this; they cannot conduct this function.

You need to verify your email address to activate your account:” Member has P1 license, but has not activated the link in the email. These links are only valid for 3 days. If you are not receiving an email, check your spam.

My email is incorrect. Log into https://login.dso.mil and update the profile. It will send the email a new verification link. Upon next log out and re-login to Mattermost, the email will update. Emails must be the government/military email for gov employees/mil members. Do not use gmail, hotmail, yahoo, aol, etc.

Member did not receive email after licensing ticket processed successfully: They may have already had a Platform One license in the past. The ticket would have reactivated it, which does not send an additional email with a link. The member should try logging in at https://chat.il4.dso.mil to see if they were granted access. If unable to access, try checking their email's spam folder