



Commercial Virtual Remote (CVR) Environment

User Log-on Guide for DoD's Commercial Virtual Remote Environment Using Microsoft Teams

Published: 04/08/2020 Version: 3.7

This guide has three sections to help you set up your Commercial Virtual Remote (CVR) Environment account.

[Section 1: Account Set-Up on Your Desktop.](#) Section 1 of this guide will help you set up your CVR Environment account on your government-issued or personal computer or device.

[Section 2: Multi-Factor Authentication \(MFA\) Set-up using the Microsoft Authenticator App.](#) Section 2 will help you set up MFA on the Microsoft Authenticator App.

- If possible, please use the Microsoft Authenticator (in this Section) to set up MFA, NOT the phone option in Appendix 1 because we have limited licenses for phones and are trying to reserve these for people who can't use the Authenticator option.
- You only need to choose one MFA option; you do NOT need to set up MFA on your phone and on the Microsoft Authenticator App.

[Section 3: Change your Password.](#) Section 3 will help you change your password from the temporary password provided in the Welcome Email to a permanent password. Your temporary password must be changed when you establish your account.

[Additional Resources.](#) This Section has training and onboarding resources to help you learn how to use the CVR Environment within your office.

[Appendix 1: MFA Set-up using Your Phone](#) (only for Users who are unable to set-up Microsoft Authenticator in Section 2). If you are unable to access the Authenticator App and need to set up MFA on your DoD issued or personal phone, use this section. You do NOT need to set up MFA on your phone if you have set up the Microsoft Authenticator app.

[Appendix 2: Common Issues for CVR Users.](#) This section includes known issues and troubleshooting that impact users across DoD.

[Appendix 3: Organization-Specific Issues.](#) This section includes issues and troubleshooting for organization-specific issues within [Army](#), [Navy/USMC](#), [Air Force](#), and [Other Defense Agency](#) systems.



Commercial Virtual Remote (CVR) Environment

Before You Get Started:

You should have received a Welcome Email to your DoD email account with your username and temporary password. You will need this Welcome Email to get started. Please have it ready as you complete the steps below.

- 💡 *Tip 1: You may experience a simpler set-up on a non-NIPR Net computer, such as your personal computer. It is acceptable to use a personal computer or device to set-up your account.*
- 💡 *Tip 2: Users may need to contact their organization's Help Desk for support if they experience issues with Virtual Private Networks (VPNs) or other organization-specific configurations.*

Remember that the **Standard Mandatory DoD Notice and Consent Banner** applies to the CVR Environment; you can review the banner here: <https://www.cloud.mil/cvr/dodnoticeandconsentbanner>



Commercial Virtual Remote (CVR) Environment

Section 1: Set-up Your CVR Environment Account on Your Desktop or Laptop Computer

STEP 1: Open your supported **Web Browser**. (Due to local network settings and configurations, certain browsers are more functional than others. Please try all available browsers on your workstation.)

Supported Microsoft Teams Web Browser:

- Microsoft Edge (use with JSP provided equipment)
- The latest version of Chrome
- The latest version of Firefox

STEP 2: Enter the URL https://teams.microsoft.com/?domain_hint=cvr.mil

STEP 3: On the **sign in** page, enter your [@cvr.mil](#) **Username** provided in the Welcome Email, then select **Next**. **DO NOT CREATE A NEW ACCOUNT.**

A screenshot of the Microsoft Teams sign-in page. At the top left is the U.S. Department of Defense logo. Below it is the heading "Sign in". A text input field contains the placeholder text "username@cvr.mil". Below the input field are three links: "No account? Create one!", "Can't access your account?", and "Sign-in options". A blue "Next" button is positioned to the right of the input field. At the bottom of the page, there is a grey box containing the text: "Don't create a new account, use the @cvr.mil username that was sent via email. I've read & consent to terms in the Information Systems user agreement."



Commercial Virtual Remote (CVR) Environment

STEP 4: On the **Enter password** page, type in the **password** from your welcome email, and then select **Sign in**.

This is a screenshot of the "Enter password" login page. At the top left is the US Department of Defense logo. Below it is the email address "testcharlie7@cvr.mil" with a back arrow. The main heading is "Enter password". Below this is a password input field containing ten dots, highlighted with an orange border. To the left of the field is a link "Forgot my password". To the right is a blue "Sign in" button, also highlighted with an orange border. At the bottom, a grey box contains the text: "Don't create a new account, use the @cvr.mil username that was sent via email. I've read & consent to terms in the Information Systems user agreement."

STEP 5: The DoD has enabled enhanced login capabilities using (MFA) when using your mobile device. Select **Next** to continue.

This is a screenshot of the "More information required" page. At the top left is the US Department of Defense logo. Below it is the email address "testcharlie7@cvr.mil". The main heading is "More information required". Below this is the text: "Your organization needs more information to keep your account secure". There are two links: "Use a different account" and "Learn more". At the bottom right is a blue "Next" button, highlighted with an orange border. At the bottom, a grey box contains the text: "Don't create a new account, use the @cvr.mil username that was sent via email. I've read & consent to terms in the Information Systems user agreement."



Section 2: Set up the Microsoft Authenticator App on Your Device for MFA



Remember! You have two MFA options; you can use the Authenticator app or your phone. For instructions to use your phone click [here](#). If possible, please use the Microsoft Authenticator App in this section, NOT the phone option in Appendix 1 because we have limited licenses for phones and are trying to reserve these for people who can't use the Authenticator option. You must have physical access to your mobile device to configure and use the Mobile App for Authentication.

STEP 1: Download and install the app

Install the latest version of the Microsoft Authenticator App, based on your operating system. You can download the app onto your work or personal device:

- **Google Android.** On your Android device, go to Google Play to download and install the Microsoft Authenticator app. (https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US)
- **Apple iOS.** On your Apple iOS device, go to the App Store to download and install the Microsoft Authenticator app. (<https://apps.apple.com/us/app/microsoft-authenticator/id983156458>)

STEP 2: Set up the Microsoft Authenticator App to send notifications

1. On the **Additional security verification** page, select **Mobile app** from the '**Step 1: How should we contact you**' scroll box. You can use your DoD-issued or personal device for security verification. The mobile number you input here will be used to send you text or voice messages in the future to provide a verification code to access your account, **so make sure to use a phone that you have access to remotely.**
2. Next, select **Receive notifications for verification** from the **How do you want to use the mobile app** box, and then select **Set up**.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up

Next




Commercial Virtual Remote (CVR) Environment

The **Configure mobile app** page appears and go to **Step 3** to continue.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



[Configure app without notifications](#)

If you are unable to scan the image, enter the following information in your app.
Code: 857 634 999
Url: <https://co1pfpad16.phonefactor.net/pad/648069390>

If the app displays a six-digit code, you are done!

[Next](#) [cancel](#)

STEP 3: On your **Mobile** device, Open the Microsoft Authenticator app, select **Add account** from the **Customize and control** icon in the upper-right portion of the screen, and then select **Work or school account**.



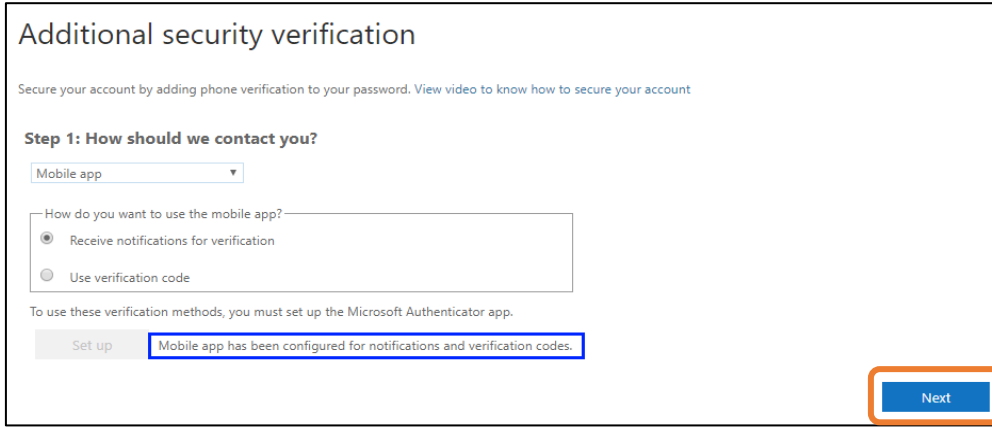
*If this is your first time setting up the Microsoft Authenticator app, you might receive a prompt asking whether to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You must select **Allow** so the authenticator app can access your camera to take a picture of the QR code in the next step (this may not be possible on a Government issued mobile device).*

STEP 4: Use your device's camera to scan the QR code from the **Configure mobile app** screen on your computer and then choose **Next**.



Commercial Virtual Remote (CVR) Environment

STEP 5: Return to your **computer** and the **Additional security verification** page. Make sure you **received** the message **stating** your configuration was successful, and then select **Next**. If you are not successful, return to STEP 2 and try again.

A screenshot of the "Additional security verification" page. The title is "Additional security verification". Below it is a subtitle: "Secure your account by adding phone verification to your password. View video to know how to secure your account". The main heading is "Step 1: How should we contact you?". There is a dropdown menu with "Mobile app" selected. Below that is a question: "How do you want to use the mobile app?". There are two radio button options: "Receive notifications for verification" (which is selected) and "Use verification code". Below the options is a note: "To use these verification methods, you must set up the Microsoft Authenticator app." At the bottom left is a "Set up" button. To its right is a blue box containing the text "Mobile app has been configured for notifications and verification codes." At the bottom right is a blue "Next" button, which is highlighted with an orange border.

The authenticator app will send a notification to your mobile device as a test.

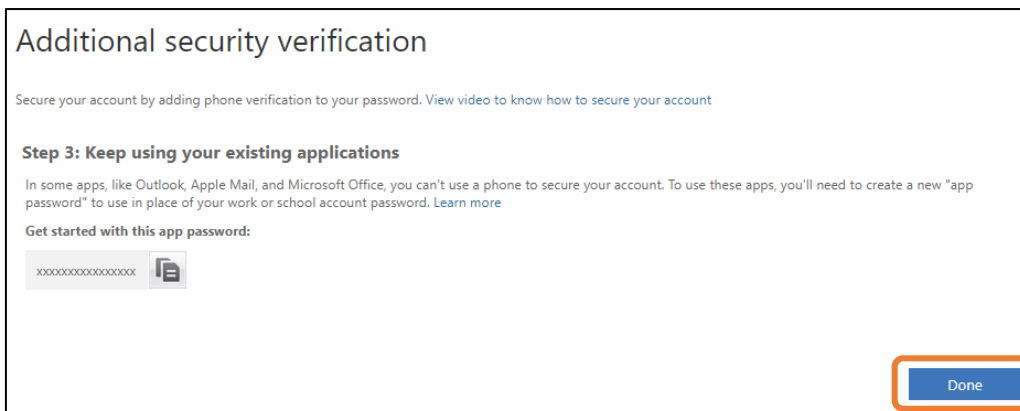
STEP 6: On your **mobile** device select **Approve**.

STEP 7: On your **computer**, add your mobile device phone number to the **Step 3: In case you lose access to the mobile app** area, and then select **Next**.



We strongly suggest adding your mobile device phone number to act as a backup if you're unable to access or use the mobile app for any reason.

STEP 8: From the **Step 4: Keep using your existing applications** make sure that you remember this app password for future use.

A screenshot of the "Additional security verification" page. The title is "Additional security verification". Below it is a subtitle: "Secure your account by adding phone verification to your password. View video to know how to secure your account". The main heading is "Step 3: Keep using your existing applications". Below that is a paragraph: "In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new 'app password' to use in place of your work or school account password. Learn more". Below that is a section: "Get started with this app password:". There is a text input field containing "xxxxxxxxxxxxxxxx" and a copy icon. At the bottom right is a blue "Done" button, which is highlighted with an orange border.

STEP 9: Select **Done**. Validate your phone by **re-verifying** and select **Finish**

STEP 10: Click **Finish**



Section 3: Change Your Password (Required)

STEP 1: Enter your **old password** (the password provided in the Welcome Email) and then type in a **new password**.

Microsoft
xctestuser02@cvr.mil

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

.....

.....

.....

Sign in

STEP 2: Select **Yes** to stay signed-in. It is acceptable under DoD's policies to stay signed in.

Microsoft
xctestuser02@cvr.mil

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

Don't show this again

No **Yes**

Congratulations! You now have access to the CVR Environment. Please go to <https://dodtelework.sharepoint.com/sites/TeamsLearning> to learn more about this collaboration tool.



Commercial Virtual Remote (CVR) Environment

Additional Resources:

- The most recent version of this **User Log-on Guide** can be accessed here: <https://go.usa.gov/xv3tc>
- Visit the **CVR Environment's public website** for up-to-date resources and information: <https://www.cloud.mil/CVR>
- Discover **resources for using the CVR Environment at work** here: <https://dodtelework.sharepoint.com/sites/TeamsLearning>
- **Download and install the full desktop version of Microsoft Teams** on your personal computer or mobile device here: <https://teams.microsoft.com/downloads>. For **DoD-issued** computers and mobile devices, please contact your local IT Help Desk Support for assistance downloading the desktop version of Microsoft Teams.
- Remember that the **Standard Mandatory DoD Notice and Consent Banner** applies to the CVR Environment; you can review the banner here: <https://www.cloud.mil/cvr/dodnoticeandconsentbanner>
- For information on **Teams accessibility under Section 508 of the Rehabilitation Act**, visit this website: <https://support.office.com/en-us/article/office-accessibility-center-resources-for-people-with-disabilities-ecab0fcfd143-4fe8-a2ff-6cd596bddc6d>
- **Records Retention Reminder:** The CVR Environment is not an approved records retention environment, as it is a temporary capability that will only be active throughout the duration of the COVID-19 National Emergency. All users are responsible for managing their records, and must forward or upload records into an approved records retention environment within 20 days of record creation. If you have questions about your schedule or proper records management.
 - View the Records Management brochure: https://www.cloud.mil/Portals/96/Documents/CVR/RM_brochure_2019-3-7.pdf
 - Contact your Records Officer: <https://www.archives.gov/records-mgmt/agency/departments/defense.html>
- You can always contact your **local IT Help Desk Support** for assistance.



Appendix 1: Set-up Multi-factor Authentication using SMS on Your Phone



Remember! You have the two MFA options; you can use the Authenticator app or your phone. If possible, please use the Microsoft Authenticator app in section 2, NOT the phone option in this section because we have limited licenses for phones and are trying to reserve these for people who can't use the Authenticator option.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone
Office phone
Mobile app

Method

Send me a code by text message
 Call me

[Next](#)

STEP 1: Set up your phone for MFA

- **Select your Country or region** (e.g., United States)
- **Select Method** to be contacted on the Phone (Text Message or Call me) and then select **Next**. Begin with the Text Message option (SMS message): however, if you work in a location that does not allow access to devices that can receive text messages, then use the call me option. Be sure to only use a phone to which you will have access while you are working remotely because you will need to access this phone to login to your account.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone
United States (+1)

Method

Send me a code by text message
 Call me

[Next](#)



Commercial Virtual Remote (CVR) Environment

STEP 2: Type in the *verification code* you received on your phone and then select **Verify**.

A screenshot of the "Additional security verification" screen. The title is "Additional security verification". Below the title is a subtitle: "Secure your account by adding phone verification to your password. View video to know how to secure your account". The main heading is "Step 2: We've sent a text message to your phone at +1 2025551212". Below this is a sub-heading: "When you receive the verification code, enter it here". There is a text input field. At the bottom right, there are two buttons: "Cancel" and "Verify". The "Verify" button is highlighted with an orange border.

STEP 3: Select **Done**

A screenshot of the "Additional security verification" screen. The title is "Additional security verification". Below the title is a subtitle: "Secure your account by adding phone verification to your password. View video to know how to secure your account". The main heading is "Step 3: Keep using your existing applications". Below this is a sub-heading: "In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new 'app password' to use in place of your work or school account password. Learn more". Below this is a sub-heading: "Get started with this app password:". There is a text input field containing the app password "nxfytdwckycrzwq" and a copy icon. At the bottom right, there is a "Done" button highlighted with an orange border.

STEP 4: Validate your phone by selecting **Verify** and then select **Finish**

A screenshot of the "don't lose access to your account!" screen. The title is "don't lose access to your account!". Below the title is a subtitle: "To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. You'll need to set up at least 1 of the options below." Below this are two items: "Authentication Phone is set to +1 2025551212 Verify" and "Authentication Email is not configured. Set it up now". At the bottom, there are two buttons: "finish" and "cancel". The "finish" button is highlighted with an orange border.

STEP 5: Select **Finish**

A screenshot of the "don't lose access to your account!" screen. The title is "don't lose access to your account!". Below the title is a subtitle: "Thanks! We'll use the info below to recover your account if you forget your password. Click 'finish' to close this page." Below this are two items: "Authentication Phone is set to +1 2025551212 Change" and "Authentication Email is not configured. Set it up now". At the bottom, there are two buttons: "finish" and "cancel". The "finish" button is highlighted with an orange border.

STEP 6: Return to Section 3 to update your password, then your set-up will be complete.



Appendix 2: Common Issues for CVR Environment Users

As new issues are discovered we'll continue to update this Appendix. Please check back for newer versions published with additional information. The most recent version will be published here: <https://go.usa.gov/xv3tc>

Known Issues and Troubleshooting Steps:

1. **Poor performance or audio video issues while using Teams:** Users on DoD networks or who are using VPNs may experience issues with performance or audio/video in Teams. Generally, this manifests itself in poor performance or an inability to use voice or video for meetings or one-on-one calls or video chats.

Resolution: Most of the Teams functionality can be achieved by disconnecting the VPN. If your organization allows this, then we recommend accessing the CVR Environment outside of a VPN. Additionally, DoD leadership is evaluating other solutions to address this issue.

2. **Audio and/or Video not working:** In addition to known issues with VPNs and DoD network-based connections, some users have reported that their microphones and speakers are disabled on their machines, or the machines that they are using do not have speakers, microphones, or cameras.

Resolution:

- When working remotely consider using a personal machine or mobile device that has audio/video capabilities when needed for these activities.
- If authorized by your organization, connecting external speakers/microphone/webcam, etc., into the audio and microphone jack may alleviate this issue. We recommend you contact your organization's security officer prior to plugging in any external devices into your government issued machine or device.

Features that will may NOT work in CVR Teams:

1. Some users have reported that they are **unable to add stickers or meme's** to chats but are able to send Giphys. This is likely based on the web browser or version of Teams you are using.
2. **Sharing your desktop or an application using the browser app.** Screen sharing may not work with the web version of Teams and requires the Teams desktop app.
3. **Inviting external participants to a meeting.** When you invite external recipients to a meeting, they do not receive the invite. We are aware of this issue and are working on a solution.
4. **Recording.** Users have reported being able to record but not able to view the recording. We are aware of this issue and are working on a solution.



Commercial Virtual Remote (CVR) Environment

Appendix 3: Organization-Specific Guidance

Army: Known issues and troubleshooting

Authenticator Application and/or the Microsoft Teams application installation issue on Government-issued Mobile Device:

Resolution: This is a known issue and solutions are being evaluated. At this time, you cannot use the authenticator application on government-issued mobile devices until the app is made available through the government mobile device management system. Consider using your personal mobile device to install the Authenticator app. You can also reference [Appendix 1](#) to enable MFA through message or voice calls.

Navy/USMC: Known issues and troubleshooting

There are no unique known issues at this time. Please refer to the Common Issues Section for known issues impacting all CVR users.

Air Force: Known issues and troubleshooting

There are no unique known issues at this time. Please refer to the Common Issues Section for known issues impacting all CVR users.

Other Defense Organizations and Agencies: Known issues and troubleshooting

There are no unique known issues at this time. Please refer to the Common Issues Section for known issues impacting all CVR users.