V 07 | 01/20/2021

COMDATA® | Multi-factor Authentication (MFA)

Multi-factor Authentication: Customer Administrator's Setup Guide

As an organization, we are always striving to stay ahead of the curve with our security and IT practices. We are excited to introduce our new approach to enhance the security of the ICD portal. Multi-factor Authentication (MFA) adds a second layer of validation after you input your username and password into the iConnectData (ICD) login page.
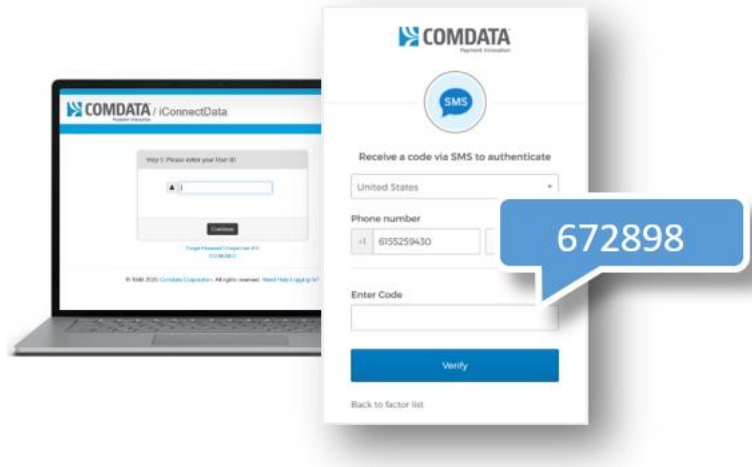
Going forward, as a part of the login process, ICD users who take advantage of Comdata's MFA process will receive a six-digit Access Code. Upon receiving the code, the user enters the code in iConnectData to complete the login process. Using a code is the second level of our new 'multi-factor' login process.

| Content |

Multi-factor Authentication Setup

1. Log into ICD: https://w6.iconnectdata.com/Login/init/ICD. Enter User ID and click "Continue".
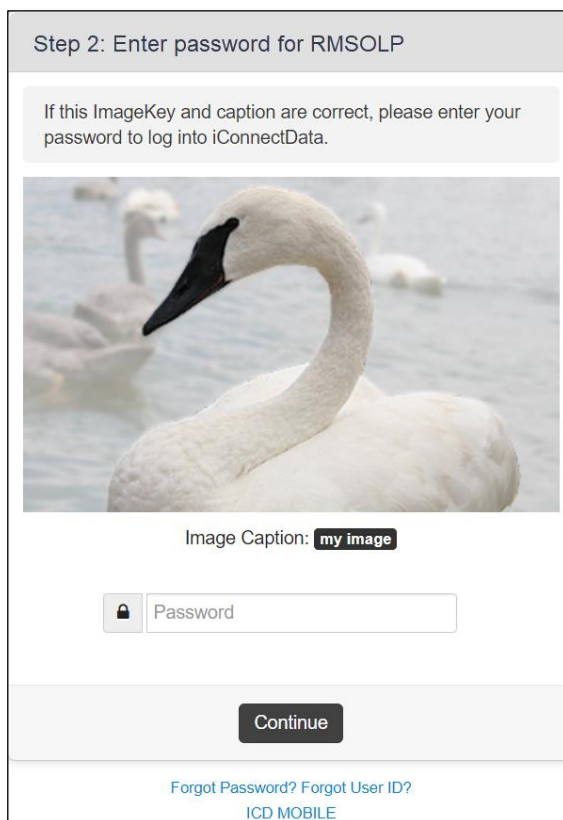
> Step 1: Please enter your User ID
>
> 👤 RMSOLP
>
> Continue
>
> Forgot Password? Forgot User ID?
> ICD MOBILE

2. Check the ImageKey / ImageKey Caption and enter ICD Password and then click Continue.

> Step 2: Enter password for RMSOLP
>
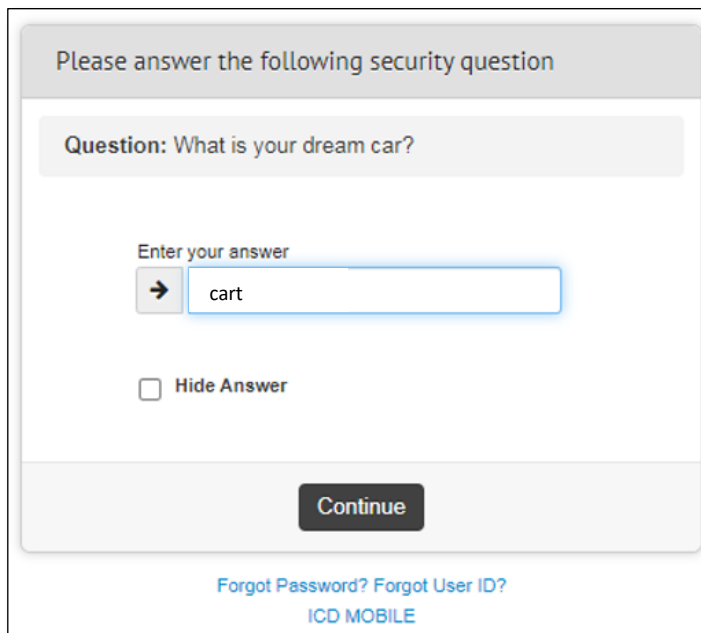> If this ImageKey and caption are correct, please enter your password to log into iConnectData.
>
> Image Caption: my image
>
> 🔒 Password
>
> Continue
>
> Forgot Password? Forgot User ID?
> ICD MOBILE

3. Answer security question. Please note that this security question might be used in the future as your password recovery question.
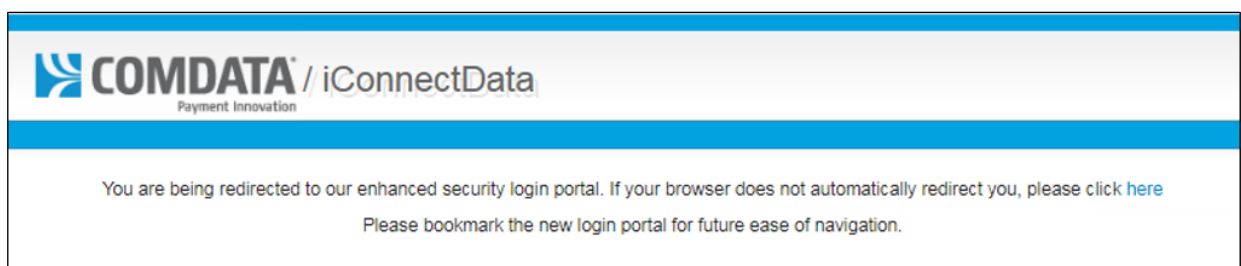
4. The system's enhanced security function immediately registers the user. Once registered, a redirect page displays this message:

    "You are being redirected to our enhanced security login portal. If your browser does not automatically redirect you, please click here*. Please bookmark the new login portal for future ease of navigation."*
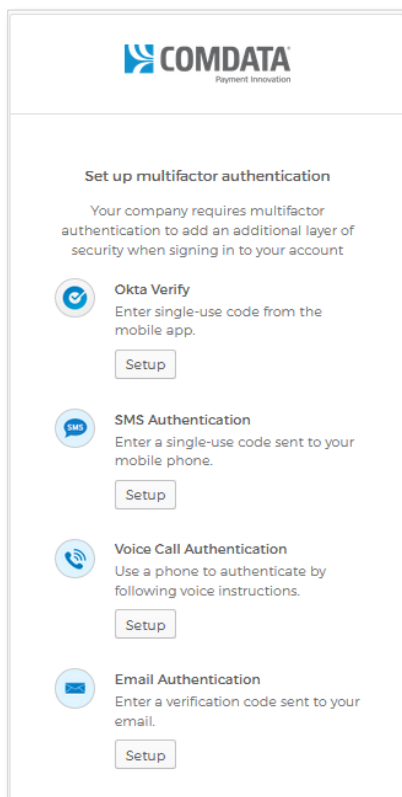
    Note: The system automatically redirects the user to the new login page after 15 seconds, *or* the user can click the 'here' link to go to the new login page.
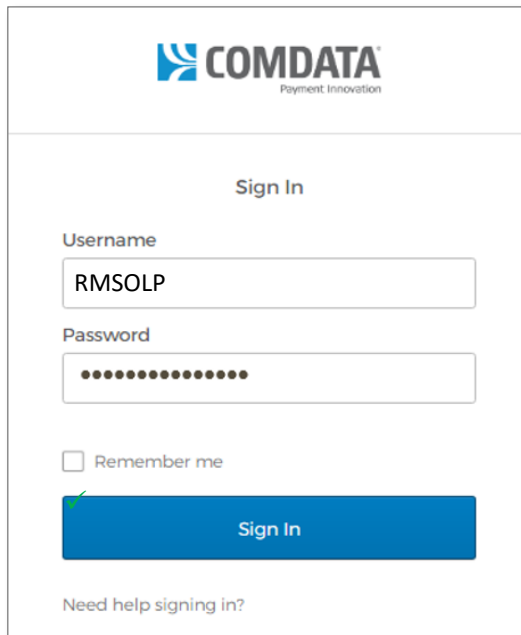
5. Enter your ICD Username and Password on the new **Sign In** dialog box and click "Sign In". "Remember me" retains the Username for future logins.

6. In the **Set up multifactor authentication** dialog box, select your preferred method and click "Setup".

Refer to these steps for setup instructions.

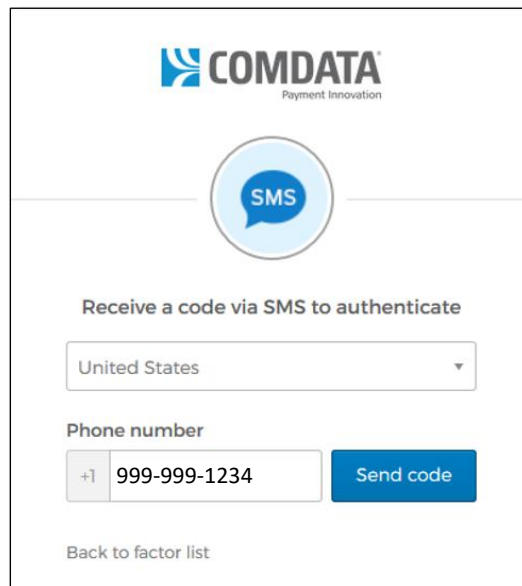**SMS**: Step 7

Email: Step 8

Voice Call: Step 9

Okta Verify (Push Notification - Mobile App): Step 10

7. The **SMS** dialog box displays.

    a. User selects the country from the dropdown and enters the mobile phone number that will be used to receive the SMS text message with the Authentication Code, then clicks "Send code".

        The "Back to factor list" link takes the user back to the "Set up multifactor authentication" dialog box.

    b. The setup process returns a dialog box with a field for the user to enter the single-use code received on their mobile phone. The text message below is sent by Comdata's system to the user's phone.
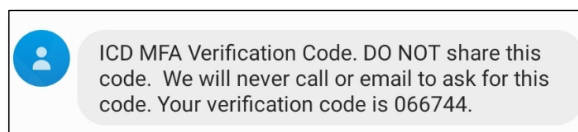
c. User enters the 6-digit code, then clicks "Verify". If, after 30 seconds, the user has not entered the single-use code sent to their mobile phone, the system will give the user an option to "Re-send code" in case the first code was not received. **Remember! Do not share this code with anyone. Comdata will never call or email a user asking for this code.**
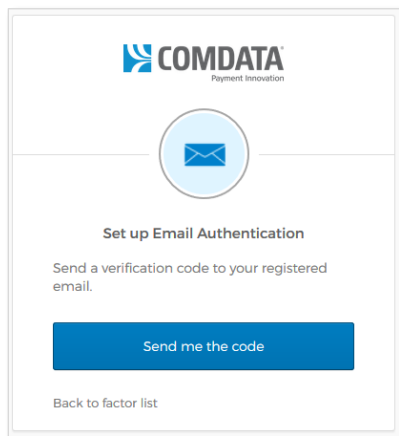

d. After the system completes verification, the user is redirected to the ICD Dashboard, fully logged in, and ready to begin their daily workflow.
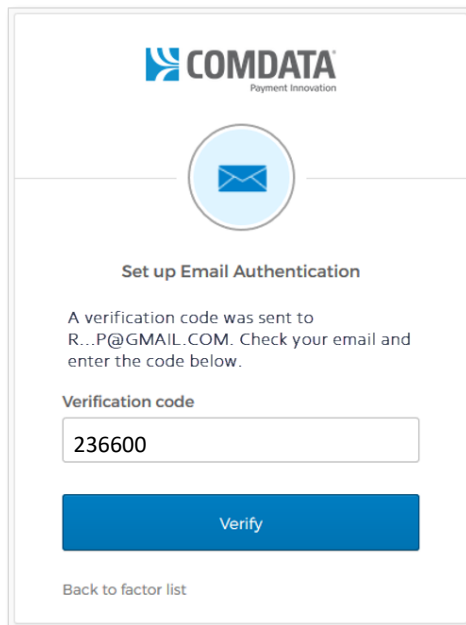
8. The **Email** dialog box displays:

    a. Click "Send me the code". User is sent a 6-digit code to the email address of record.

    b. An email sent confirming your email address. A one-time use code is provided to complete the email address setup process.

c. Key in the 6-digit code received in the email and click "Verify".

d. User is redirected to the ICD Dashboard, fully logged in, and ready to begin their daily workflow.

9. The **Voice Call** dialog box displays:

   a. Enter your mobile phone number and click "Call". After clicking "Call" the button changes to "Calling".
   Note: An "Extension" can be entered for a land line.

   b. User receives a phone call with this message:
   "Hello. Thank you for using our phone verification service. Your code is ######.".
   The phone message will repeat the code again and will end with *"Good bye"*.
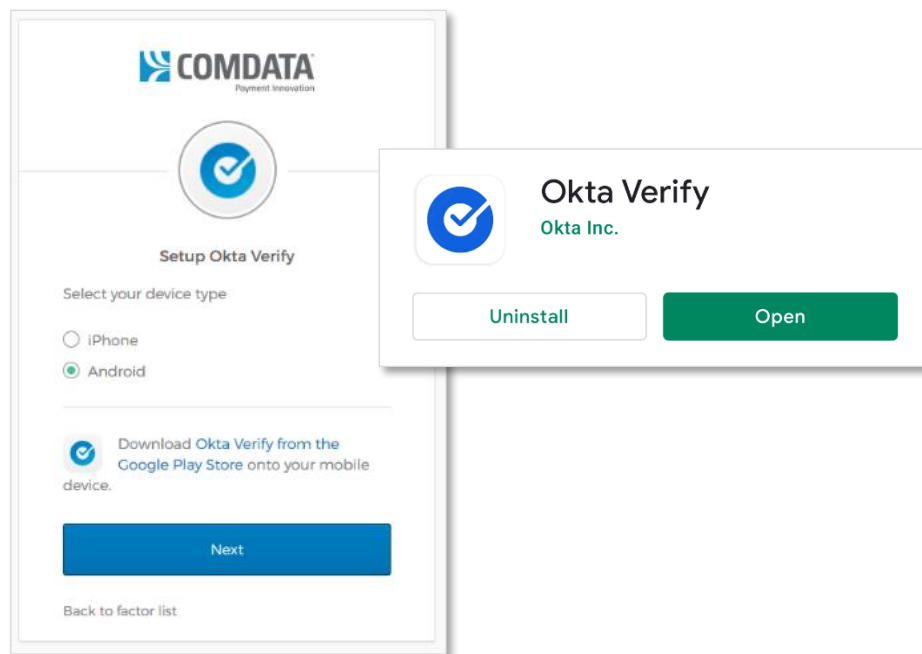
10. The **Setup Okta Verify** dialog box displays.

    a. Select your device type: iPhone or Android.
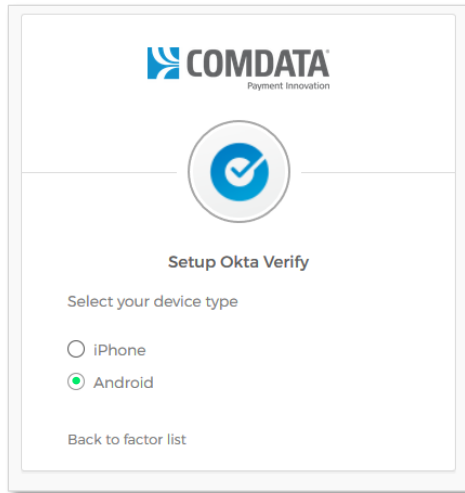
    b. User is asked to download the app. After downloading the app, click "Next" on the **Setup Okta Verify** dialog box.


    c. Launch the application on the mobile device and select "Add an account".

    d. When asked for Account Type, select "Other". "Other" is used for two-factor authentication code for third party services. Note: The app does not allow screenshots for security reasons.

e. After selecting "Other", scan the QR code and click "Next". The account is added and the mobile app automatically displays a 6-digit authentication code.
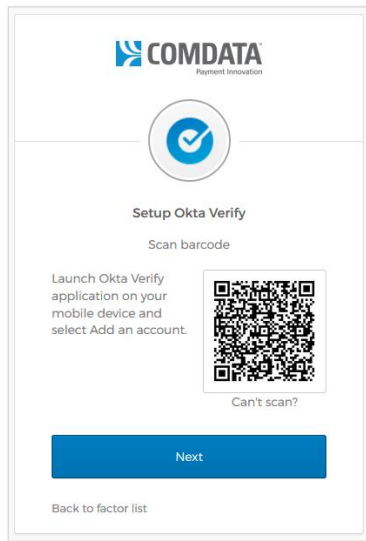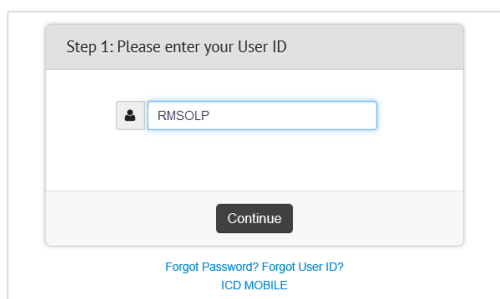

f. Key in the 6-digit code and click "Verify". Going forward, when asked for the 6-digit code, you will open the mobile device app to get the code.
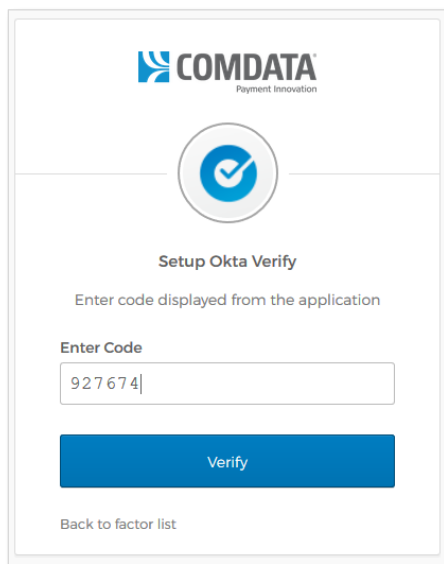
ICD Login *after* MFA Setup – What to Expect

This is the new login experience *after* the user has been set up for Multi-factor Authentication. "What to Expect" steps will differ based on the method that the user has set up. The steps below illustrate what to expect when a user has selected **SMS** as the preferred method for receiving a verification code.
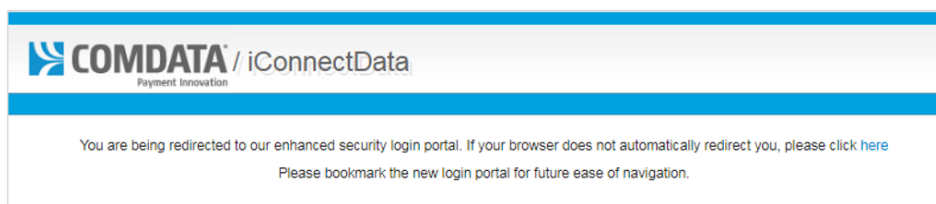
1. Log into ICD: https://w6.iconnectdata.com/Login/init/ICD. Enter User ID and click "Continue".

2. A redirect page displays this message: "You are being redirected to our enhanced security login portal. If your browser does not automatically redirect you, please click here. **Please bookmark the new login portal for future ease of navigation."** *Note:* The system automatically redirects to the new login page after 15 seconds, *or* the user can click the 'here' link to go directly to the new login page.

The redirect message asks you to bookmark the new link for ease of navigation, so you do not get redirected over and over.

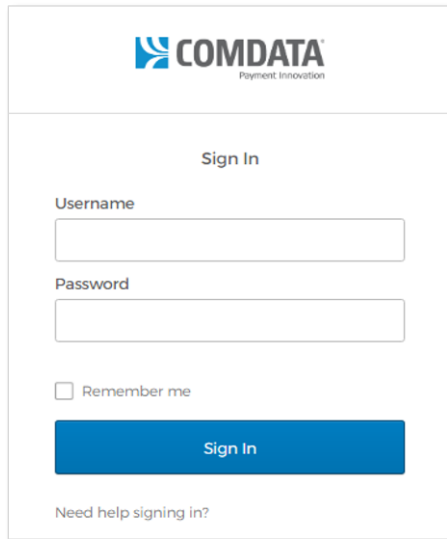The link for the **new ICD MFA** is: https://w6.iconnectdata.com/icd-auth

IMPORTANT! Once you have registered for the ICD MFA, **change your Comdata bookmark to the URL above.** If you log into ICD with the same computer (IP address) and user name and password, you will not be challenged to enter a new 6 digit code for 12+ hours.

If you log in with a different device (say a mobile phone), you will perform the same process that you did for the first device you registered with MFA.
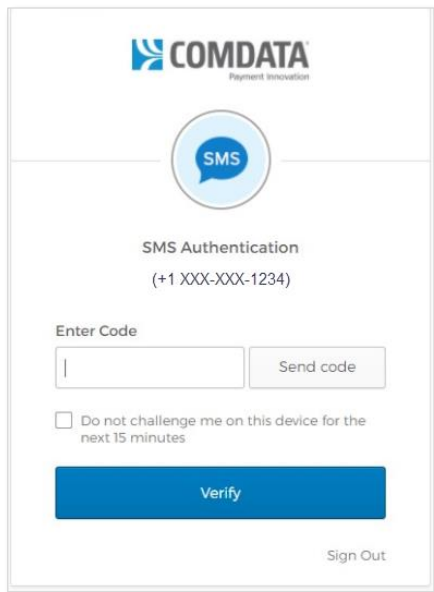
3. New **Sign In** dialog box displays. Enter Username and Password and click "Sign In". *Note:* The user has the option to select "Remember me", which will retain their Username for future logins.

4. The dialog box for the selected Authentication method displays. The example below is SMS – it displays the associated mobile phone number (masked to only show the last four digits). User clicks "Send code".

5. The user will receive the single-use code on their mobile phone, usually within seconds.

6. The user will enter the code into the "Enter Code" field and click "Verify". Note: The user has the option to select to not be challenged again for the next 15 minutes if logging in again from this device.
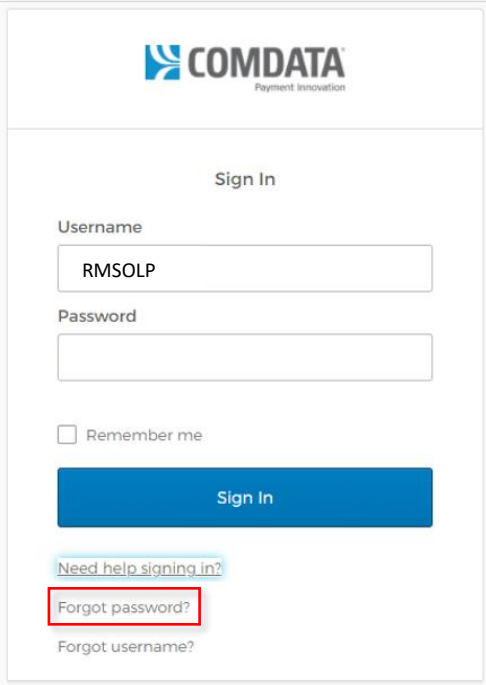
7. Assuming their MFA challenge was accepted, the user is redirected to the ICD Dashboard, fully logged in, and ready to begin their daily workflow.

Reset User Password via SMS

To reset a password the user will need a verification code. SMS can only be selected if a mobile phone number has been set up in the User Profile.

1. On the **Sign In** dialog box, enter the Username, then click "Forgot password?".
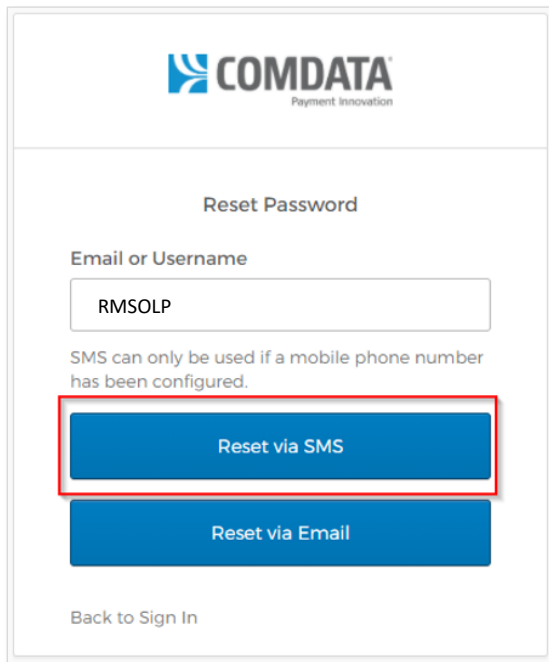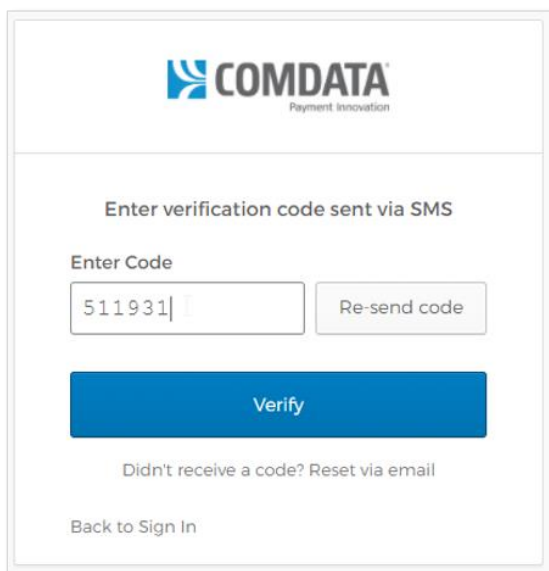
2. The **Reset Password** dialog box displays. Click "Reset via SMS". SMS can only be selected if a mobile phone number has been set up in the User Profile.
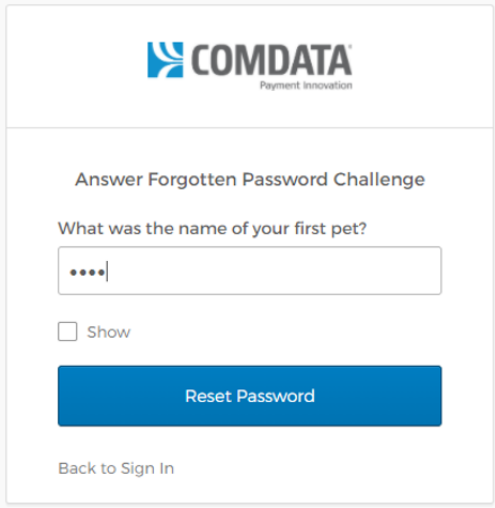
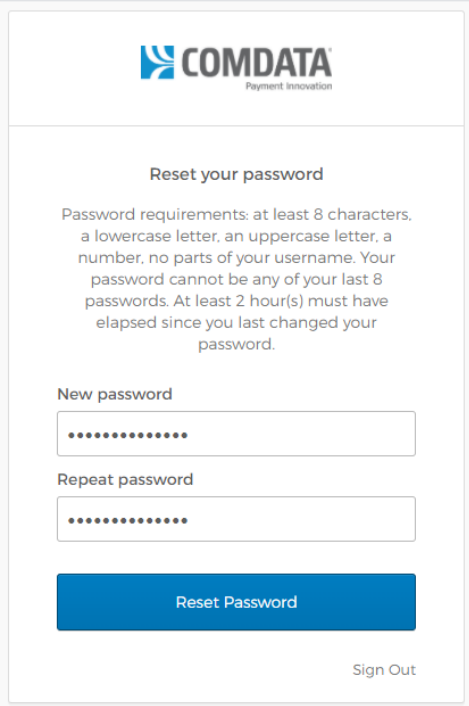3. A verification code will be sent via SMS. Enter the verification code and click "Verify".

4. After successful verification, answer the Forgotten Password Challenge question and click "Reset Password".

5. Using the password character requirements, create a new password and then click "Reset Password".

6. A new verification code is sent via SMS. Enter the verification code and click "Verify".

7. After successful verification, click "Sign In". User is redirected to the ICD Dashboard, fully logged in, and ready to begin their daily workflow.
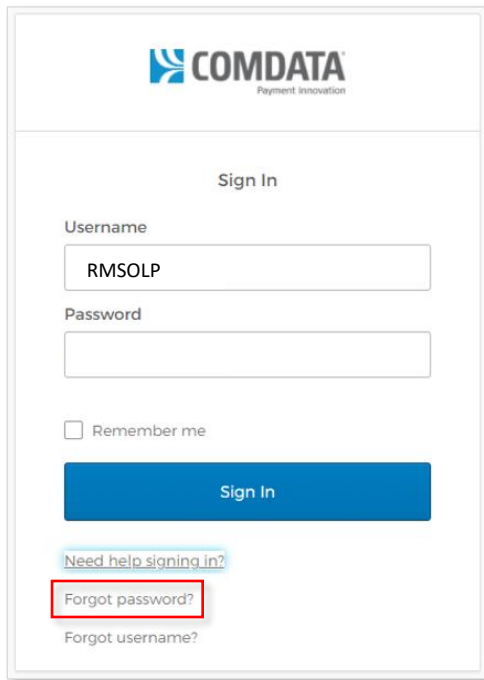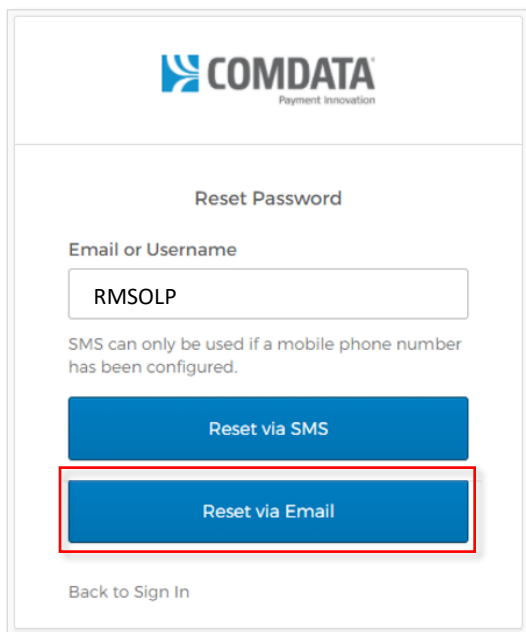
Reset User Password via Email

To reset a password the user will need a verification code. Text here.

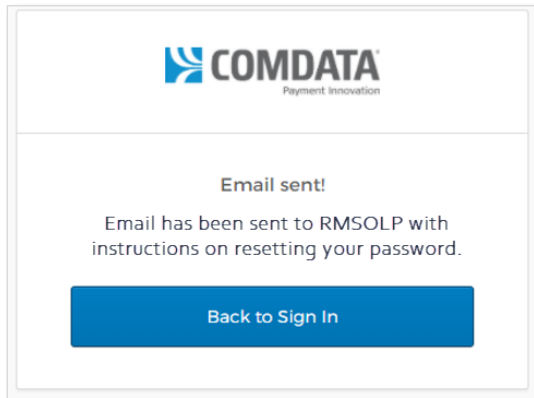1. On the **Sign In** dialog box enter a Username, then click "Forgot password?".

2. The **Reset Password** dialog box displays. Click "Reset via Email".

3. The **Email sent!** dialog box confirms that an email has been sent to the user.
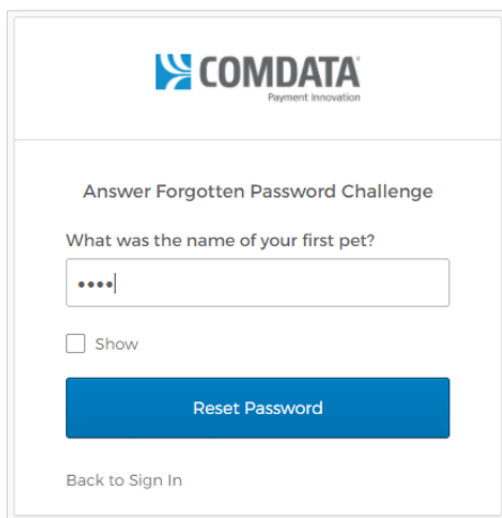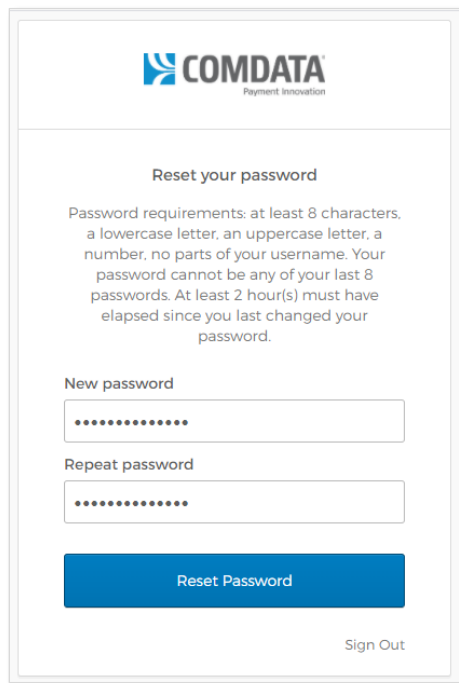

4. The Comdata email provides a link for the Password Reset. Click "Reset Password".
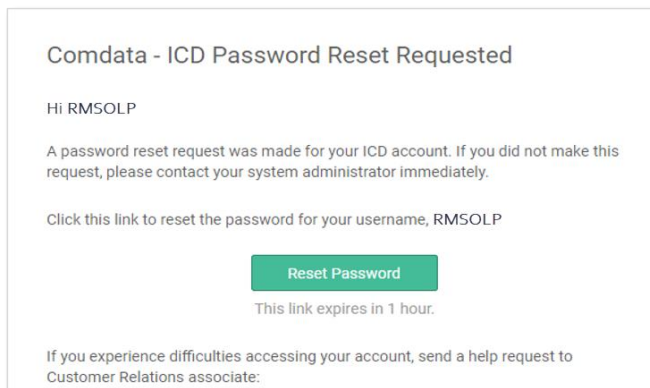
5. Answer the Forgotten Password Challenge question and click "Reset Password".

6. After successfully answering the challenge question, the **Reset your password** dialog box displays. Using the password character requirements, create your new password and then click "Reset Password".
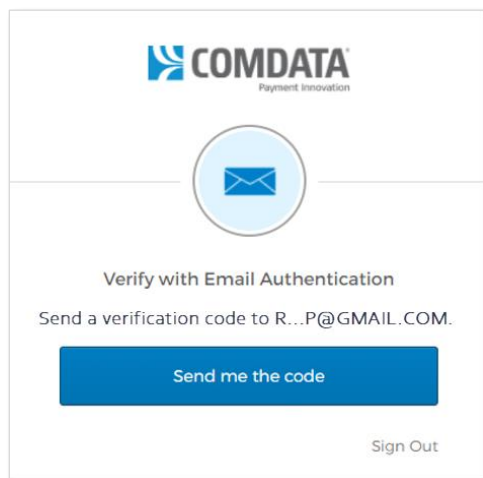
7. Click "Send me the code" to confirm that you are requesting a verification code to be sent to the displayed email address.
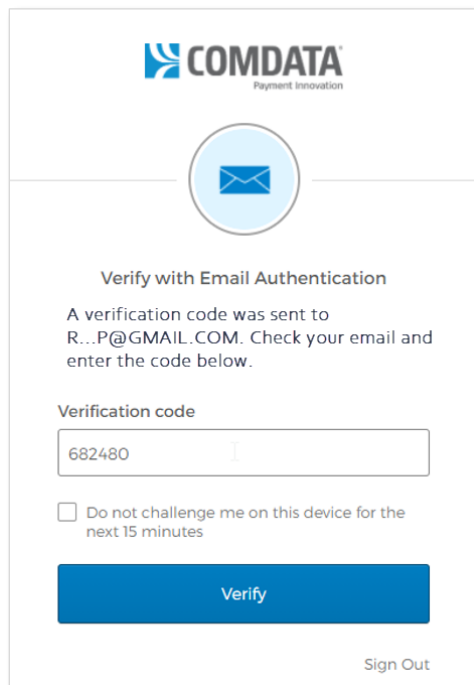
8. You will receive a message confiming that an email has been sent with a verification code. Enter the Verification code and click "Verify".
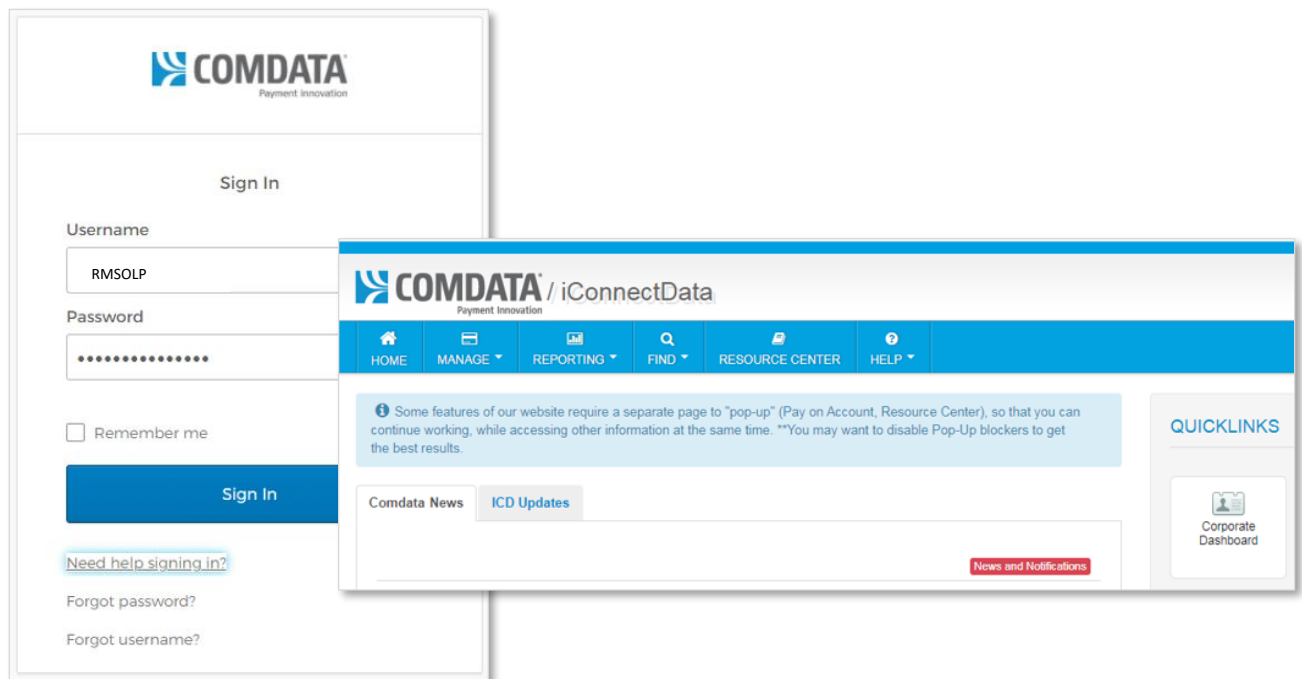
9. After successful verification, the user clicks "Sign In" and is redirected to the ICD Dashboard, fully logged in, and ready to begin their daily workflow.

Retrieve User ID

Only Migrated Users can retrieve a User ID. Migrated users can use the "Need help signing in?" > "Forgot username?" link. The user will be prompted to enter their email, First Name and Last Name. They will receive an email with the User ID.

1.   On the **Sign In** dialog box, click "Forgot username".

2.   On the **User ID Request** dialog box, enter your Email Address, First Name, Last Name and click "Continue".

3. You will receive an email with your iConnectData User ID.

> **User ID Request**
>
> Dear RMSOLP,
>
> Please use the following User ID to log in to iConnectData:
>
> RMSOLP
>
> If you did not initiate this request, please call 1-800-741-2777.
>
> Sincerely,
>
> *iConnectData Support*

Modify User Password

Migrated users can change their password using the **My Profile** screen. The user will need to provide the current password when setting up a new password.

> **Update Password**
>
> **If the password fields are left blank, your password will remain unchanged.**
>
> Passwords are case sensitive and must be 6-20 characters in length with at least 1 letter and at least 1 number.
>
> Current Password: [••••••••••••]
>
> New Password: [••••••••••••]
> Confirm Password: [••••••••••••]

MFA Factor Value Maintenance

Please reach out to your Account Representative if you would like to:

- Change the factor method (Example: switching from SMS to Call)

- Change the factor value (phone number for SMS or call or email address for Email or App).