This page intentionally left blank.
## Revision Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Changed by</th>
<th>Revisions</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2024</td>
<td>K. Pandullo</td>
<td>• Updated new password policy with the change to ARS 5.10</td>
<td>1.6</td>
</tr>
</tbody>
</table>
| August 2023  | A. Hummers | • Transferred to the new template  
• Updated screenshots and instructions to reflect Version 1.5 upgrades. Added Self-Serve section  
• Added updated VMware Horizon Client login screenshot in the Login Using the Virtual Desktop Infrastructure (VDI) section. Updated the name “Self Service” to “CCW Self-Service Account Management (SSAM)” | 1.5     |
| April 2019   | K. Pandullo| Updated screenshots in section 4.2                                                                                                                                                                        | 1.4     |
| October 2019 | K. Pandullo| Updated screenshots for to include updated User Agreement                                                                                                                                               | 1.3     |
| July 2019    | K. Pandullo| Updated screenshots for VDI upgrade                                                                                                                                                                     | 1.2     |
| June 2019    | K. Pandullo| Updated screenshot on page 22                                                                                                                                                                           | 1.1     |
| May 2019     | K. Pandullo| Removed personal information from screenshots                                                                                                                                                           | 1.0     |
| April 2019   | K. Pandullo| Added Change Password screens                                                                                                                                                                          | .05     |
| April 2019   | K. Pandullo| Added note on “Forgotten Password Questions” section                                                                                                                                                    | .04     |
| March 2019   | K. Pandullo| Updated screenshot at top of page 4                                                                                                                                                                      | .03     |
| March 2019   | K. Pandullo| Changes made after initial review                                                                                                                                                                       | .02     |
| March 2019   | K. Pandullo| Created initial document                                                                                                                                                                                | .01     |
Table of Contents

1.0 Things to Know Before Starting.................................................................................................................................................. 1

2.0 Enroll in a Factor for a New CCW Account............................................................................................................................... 1
  2.1 Enroll in Okta Verify Factor.................................................................................................................................................. 3
    2.1.1 Address QR Scanning Issues............................................................................................................................................. 8
  2.2 Enroll in SMS Authentication Factor..................................................................................................................................... 10
  2.3 Enroll in Voice Call Authentication Factor............................................................................................................................. 12

3.0 Login Procedures...................................................................................................................................................................... 14
  3.1 Login Using the Virtual Desktop Infrastructure (VDI) ............................................................................................................... 14
  3.2 Login Using the CCW VPN..................................................................................................................................................... 15
  3.3 Login Via the CCW Website ................................................................................................................................................. 17
    3.3.1 Login with Okta Verify Factor........................................................................................................................................ 17
    3.3.2 Login with SMS Text Factor............................................................................................................................................ 19
    3.3.3 Login with Voice Call Factor.......................................................................................................................................... 20

4.0 Manage Factor Enrollments.................................................................................................................................................... 21
  4.1 Enroll in Multiple Factors ..................................................................................................................................................... 23
    4.1.1 Enroll in Okta Verify Factor............................................................................................................................................ 23
    4.1.2 Enroll in SMS Authentication Factor............................................................................................................................... 25
    4.1.3 Enroll in Voice Call Authentication Factor..................................................................................................................... 27
    4.1.4 Choose from Multiple-Enrolled Factors........................................................................................................................... 29
  4.2 Remove Enrollment in a Factor............................................................................................................................................. 30

5.0 CCW Self-Service Account Management (SSAM).................................................................................................................. 31
  5.1 Forgot Password ..................................................................................................................................................................... 31
  5.2 Unlock Account......................................................................................................................................................................... 34
  5.3 Forgot CCW User ID .............................................................................................................................................................. 37

6.0 Where to Get Assistance....................................................................................................................................................... 38
1.0 Things to Know Before Starting

Multi-factor authentication (MFA) applications within the Chronic Conditions Warehouse (CCW) website enable users to securely access the CCW and Virtual Research Data Center (VRDC). Three types of Okta® MFA applications, or factors, are available for enrollment. It is best practice to enroll in at least two factors in the event a factor malfunctions. Users need to complete an initial enrollment in an authentication factor application before accessing the secure pages of the CCW Website. All three factors are compatible with Apple iOS and Android devices.

The three authentication factors are:

1. **Okta Verify Application** — this factor sends authentication alerts through the Okta Verify application on a mobile device, such as a smart phone, with a password and a “Push” feature that sends an alert to the mobile device to accept the login request. The Okta Verify application is available on Apple iOS and Android devices.
2. **SMS Text Messaging Authentication** — this factor sends authentication codes in a Short Message Service (SMS) text message to a mobile device.
3. **Voice Call Authentication** — this factor sends authentication in a voice mail via a valid phone number that the Okta software can call for verification.

2.0 Enroll in a Factor for a New CCW Account

This section outlines the process of an initial enrollment in a factor.

NOTE: For information about managing additional factors, refer to section 4.0.

1. Navigate to [https://www.ccwdata.org](https://www.ccwdata.org) and select **My CCW Login (Authorized Users Only)**.
2. Enter your CCW User ID and password in the corresponding fields and select the **Sign In** button.

3. The **Sign In** screen displays. Select an Okta authentication factor(s) for the initial setup.
2.1 Enroll in Okta Verify Factor

Follow the steps to set up, or enroll in, the Okta Verify application with a mobile device.

1. Select the **Setup** button under “Okta Verify.”
2. Select the type of mobile phone device you wish to setup.

   a. When selecting the Apple device type, instructions display to download the Okta Verify application from the App Store on your mobile device.
b. When selecting the Android device type, instructions display to download the Okta Verify application from the Google Play Store on your mobile device.

3. After downloading the Okta Verify application on your mobile device, open the application and follow instructions to add an account.
4. Enrollment in Okta Verify requires a Quick Response (QR) code scan from a source. In the Sign In: screen, select the Next button.

5. A QR code displays in the Sign In: screen.
6. Allow the Okta Verify Application to access the camera on your mobile device.

7. Scan the QR code on the Sign In: screen with your mobile device’s camera.

8. The system enrolls the user in the Okta Verify factor. The system indicates a successful enrollment with a check mark next to the **Okta Verify** factor in the Sign In: screen.

   If you are configuring the additional option, SMS Authentication, refer to [section 2.2](#) or for Voice Call Authentication refer to [section 2.3](#).
9. Select the **Finish** button to complete enrollment.

The system will prompt new CCW users to change their password. Enter the temporary password provided by CCW Help in the **Old Password** field. Create a new password using the guidelines detailed on the screen and select **Change Password**.

2.1.1 Address QR Scanning Issues

If issues arise while scanning the QR code of Okta Verify with a mobile device, use the following troubleshooting steps:

1. Select the **Can’t scan?** link in the Setup Okta QR screen.
2. The Setup Okta Verify/Can’t scan QR Code? screen displays. Choose another option for setting up Okta Verify in the Setup Options dropdown menu.

3. Enter the required information in the selected option and select the **Send** button. Follow additional provided instructions depending on the selected option.

4. The system approves the Okta Verify authentication factor enrollment.
2.2 Enroll in SMS Authentication Factor

Follow the steps to set up, or enroll in, the SMS Authentication Factor.

1. Select the **Setup** button under “SMS Authentication.”

2. Enter the mobile number (including the three-digit area code) to receive the SMS text message with a verification code. Select the **Send Code** button.
3. Enter the code received in a text message in the **Enter Code** field. Select the **Verify** button.

4. The system enrolls the user in the SMS Authentication factor. A successful verification displays a checkmark next to **SMS Authentication** factor in the Sign In: screen.

5. Refer to **Step 9** in section 2.1 for instructions for finishing authentication enrollment.
2.3 Enroll in Voice Call Authentication Factor

Follow the steps to setup the Okta Voice Call Authentication service to call a mobile or landline phone and provide a verification code via an audible recording.

1. Select the **Setup** button under Voice Call Authentication.

2. Enter the phone number (including the three-digit area code) to receive a phone call with the verification code. Select the **Call** button.
3. The user receives a voice message with the code on the phone. Enter the received five-digit code in the **Enter Code** field and select the **Verify** button.

4. The system enrolls the user in the Voice Call Authentication factor. A successful verification displays a checkmark next to **Voice Call Authentication** factor in the Sign In: screen.

5. Refer to **Step 9** in section 2.1 for instructions for finishing authentication enrollment.
3.0 Login Procedures

This section outlines the different options for logging into the CCW environment with the new Okta software.

3.1 Login Using the Virtual Desktop Infrastructure (VDI)

Access a VDI desktop via the Okta Verify factor(s) with these steps. Once connected and logged into the virtual desktop session, the new single sign-on feature does not require the user to enter any credentials to access the CCW web applications.

**NOTE:** The CCW username is the same as the CCW User ID.

1. From the VMware Horizon Client, enter your CCW username in the **User name** field.

2. Enter your CCW password in the **Passcode** field.

3. Select the **Login** button.
3.0 Login Procedures

4. In the multi-factor authentication window that displays, do one of the following to enter a code/option number in the **Enter your next code** field:

   a. Open the Okta Verify app on a mobile device and enter the current code from the Okta Verify screen in the **Enter your next code** field.

   b. Enter one of the available options that display in the window in the **Enter your next code** field. In this example, enter option “1” to receive a voice call, option “2” to receive a push notification on a mobile device, option “3” to receive a short message service (SMS) message on the mobile device, or option “0” to abort. The displayed option numbers vary depending on the factors selected during enrollment. Be sure to read the screen prior to entering an option number.

![Login Window](https://vrdc.ccwdata.org)

5. Select the **Login** button again. The user has access to the CCW environment.

3.2 Login Using the CCW VPN

Connect to the CCW VPN with these Okta Verify factor(s) steps.

1. Open Cisco AnyConnect and select the **Connect** button.
2. Enter your CCW User ID and password in the corresponding **Username** and **Password** fields. Select the **OK** button.

![Username and Password fields](image1)

3. Enter which Okta factor you would like to use in the **Answer** field. This example’s options are to enter an Okta Verify passcode, enter “1” to receive a voice call, “2” to receive a push notification to your mobile device, “3” to receive SMS text or “0” to abort. The option number selection will vary depending on the factors in which you have enrolled. Please be sure to read the screen prior to entering an option number. Select the **Continue** button.

![Answer field](image2)

4. Once verification is complete, select the **Accept** button to complete the VPN login process.

![Accept button](image3)
3.3 Login Via the CCW Website

Use the Okta factor(s) when accessing the CCW website or web-based applications.

3.3.1 Login with Okta Verify Factor

1. Enter your CCW User ID and password in the corresponding fields. Select the **Sign In** button.
2. Do one of the following:
   a. Select the **Send Push** button to confirm access on the mobile device
   b. Enter the passcode from the Okta Verify application on the mobile device in the **Or enter code** field.
3. An alert displays in the mobile device to verify that the user has requested access to the CCW Website. Confirm the request. The CCW Website Home page displays.

3.3.2 Login with SMS Text Factor

1. Enter your CCW User ID and password in the corresponding fields. Select the Sign In button.
2. The Sign In: screen displays, including the last four digits of the phone number enrolled with your CCW User ID. Select the **Send Code** button.

3. The system sends a six-digit code via text to the mobile device. Enter the code received in the **Enter Code** field. Select the **Verify** button. The CCW Website Home page displays.

3.3.3 Login with Voice Call Factor

1. Enter your CCW User ID and password in the corresponding fields. Select the **Sign In** button.
2. The Sign In: screen displays, including the last four digits of the phone number enrolled with the CCW user ID. Select the Call button.

3. A voice message delivers a five-digit code on the mobile device or land-line telephone. Enter the code in the Enter Code field and select the Verify button. The CCW Website Home page displays.

4.0 Manage Factor Enrollments

The Manage Multi-Factor Authentication screen allows users to 1) set up more than one Okta factor and 2) remove an enrollment to a factor. CMS CCW recommends registration with at least two Okta factors in the event a factor malfunctions.

**NOTE:** Users must log into the CCW website with an Okta factor from the internet or a CMS Net connection to add or remove a factor enrollment.

1. Login to the CCW website following the log in procedures in section 3.0.
2. Select the **Manage Multi-Factor Authentication** link in the top-right corner of the CCW website home page.

3. The Account screen displays. Users can enroll in multiple MFAs or remove MFA enrollment in the Extra Verification section.

   **NOTE:** A Remove button will display next to the current active factor since the user must enroll in at least one factor to access the CCW webpage and the account screen.
4.1 Enroll in Multiple Factors

Enroll in, or set up, multiple authentication factors by selecting the Set up button opposite the factor name. A factor name associated to a “Remove” button indicates that the user has enrolled in the factor. Reference section 4.2 to remove enrollment to the factor.

**NOTE**: The Set up interface in this process is slightly different from the process in the Sign In: screen in the CCW Website, but required steps are the same.

4.1.1 Enroll in Okta Verify

1. In the Extra Verification section, select the Set up button to the right of “Okta Verify.”

![Extra Verification Interface](image)

2. In the CMS.gov|IDM screen that displays, choose the type of device you will be using to install the Okta Verify Mobile App as described in section 2.1.

![CMS.gov|IDM Setup Interface](image)

3. Open the downloaded application on your mobile device and follow instructions to add an account.

4. Allow the Okta Verify application to access the camera on the mobile device.
5. Scan the QR code on the screen.

6. A successful QR code scan enrolls the user’s new account to the Okta Verify MFA. A notification displays that the set up was successful. In the Extra Verification section, a **Remove** button displays next to “Okta Verify”.

![QR Code Scan](image)
4.1.2 Enroll in SMS Authentication

1. In the Extra Verification section, select the **Set up** button to the right of “SMS Authentication.”

![Extra Verification](image)

2. In the CMS.gov|IDM screen that displays, enter the mobile number to receive the SMS text message with a verification code. Select the **Send Code** button.

![CMS.gov|IDM SMS](image)
3. The system sends a text message containing a six-digit code. Enter the code received in the **Enter Code** field and select the **Verify** button.

4. A notification displays confirming the setup was successful. In the Extra Verification screen, a **Remove** button displays next to “SMS Authentication.”
4.0 Manage Factor Enrollments

4.1.3 Enroll in Voice Call Authentication

1. In the Extra Verification section, select the **Set up** button below “Voice Call Authentication.”

2. Enter the phone number (including three-digit area code) to receive a phone call with the verification code. Select the **Call** button.
3. An audible recording delivers a five-digit code on the mobile device or land-line telephone. Enter the code in the **Enter Code** field. Select the **Verify** button.

4. A notification displays that confirms the setup was successful. In the Extra Verification screen, a **Remove** button displays next to “Voice Call Authentication” for when the user wants to remove enrollment from this authentication process.
4.1.4 Choose from Multiple-Enrolled Factors

If the user has enrolled in more than one factor, he or she can select a preferred factor to use.

1. On the Sign In: screen, enter your CCW User ID and password in the corresponding fields and select the **Sign In** button.

2. The Sign In: screen displays an MFA interface. Select the dropdown next to the factor icon. The multiple Okta factors in which the user has enrolled display.

3. Select a different MFA method to access the CCW website.
4.2 Remove Enrollment in a Factor

Use the Remove function to unenroll in a factor.

1. In the Extra Verification screen, select the **Remove** button to the right of factor to remove enrollment.

2. Select the **Yes** button in the confirmation pop-up window.

3. The system removes the user’s factor enrollment.
5.0 CCW Self-Service Account Management (SSAM)

Users can also reset their passwords and user IDs, as well as unlock their accounts, without having to call the CCW Help Desk for assistance with the CCW Self-Service Account Management (SSAM) tool.

- Select the My CCW Login (Authorized Users Only) link in the upper-right portion of the CCW website home page, the Sign In: screen displays. The Login Assistance section displays in the lower-left portion.

5.1 Forgot Password

1. In the Sign In: screen, under Login Assistance, select the Forgot Password/Unlock Account link to create a new password. The Verify Account Information screen displays.
2. Type in the CCW User ID and email address to confirm your account information. Select the **Submit** button. The system sends an email with a link to reset your password.

3. Select the link within the email received. The link will expire within 24 hours, and users can only use it once.

   ![Email Confirmation Link](https://www2.cwdata.org/self-service/validate?token=8c71077b7b7e3e4628923217355e56e9b51b29b3829f6665d53785b541e46285d)

   A request has been made to reset your Chronic Conditions Warehouse (CCW) password or unlock your CCW account. If this request was initiated by you, please select the link below to proceed. This link will expire on 12/12/23 4:10 PM ET and you may select the link only once.

   If you did not submit this request or need additional help, contact the CCW Help Desk at *ccwhelp@ccwdata.org* or 1-866-766-1915. Hours of operation are Monday through Friday, 8:00 am-5:00 pm ET (excluding most federal holidays).

   As a reminder, please note that the Centers for Medicare & Medicaid Services (CMS) strictly prohibits sharing CCW user login credentials. Any sharing of your CCW credentials will result in the immediate suspension of your account while CMS investigates the incident.

   Thank you,

   **CCW Help Desk**
   
   *ccwhelp@ccwdata.org*
   
   1-866-766-1915 | Toll Free
   1-515-440-3159 | Fax
   
   [www.cwdata.org](http://www.cwdata.org)

4. Once the user selects the link, the **Verify Your Identity** screen will display. Select the **Send Push** button or select the **Or enter code** field.
5. The Self Service Options screen displays.

6. Select the **Change Password** button to create a new password. The Change Password screen displays.

7. Type in a new password that meets the password policy in the **New Password** and **Confirm New Password** fields. Select the **Submit** button.
5. The password changes successfully.

5.2 Unlock Account

1. In the Sign in: screen, under Login Assistance, select the **Forgot Password/Unlock Account** link to unlock an account. The Verify Account Information screen displays.
2. Type in the CCW User ID and email address to confirm your account information. Select the **Submit** button. The system emails the user a link to reset your password.

3. Select the link within the email received. The link expires within 24 hours and users can only use it once.

```
Hello,

A request has been made to reset your Chronic Conditions Warehouse (CCW) password or unlock your CCW account. If this request was initiated by you, please select the link below to proceed. This link will expire on 12/12/23 4:10 PM ET and you may select the link only once.

https://www2.ccndata.org/self-service/validate/token?token=b8c7107b7c73ed62892817355c5beab5b629b385298654c5785b34c1e6285d

If you did not submit this request or need additional help, contact the CCW Help Desk at ccwhelp@ccndata.org or 1-866-766-1915. Hours of operation are Monday through Friday, 8:00 am-5:00 pm ET (excluding most federal holidays).

As a reminder, please note that the Centers for Medicare & Medicaid Services (CMS) strictly prohibits sharing CCW user login credentials. Any sharing of your CCW credentials will result in the immediate suspension of your account while CMS investigates the incident.

Thank you,

CCW Help Desk
ccwhelp@ccndata.org
1-866-766-1915 | Toll Free
1-515-440-3359 | Fax
www.ccndata.org
```

4. Once the user selects the link, the **Verify Your Identity** screen will display.
5. Select the Send Push button or select the Or enter code field. The Self Service Options screen displays. Select the Unlock Account button.

6. The Unlock Process begins and can take up to 15 minutes to complete.
5.3 Forgot CCW User ID

1. In the Sign In: screen, under Login Assistance, select the Forgot CCW User ID link. The Retrieve CCW User ID screen displays.

2. Enter your CCW email address and select the Submit button.
6.0 Where to Get Assistance

The CCW Help Desk staff provides assistance between 8:00 am to 5:00 pm ET, Monday through Friday (excluding most federal holidays). Contact the CCW Help Desk at ccwhelp@ccwdata.org or 1-866-766-1915.