

IMPORTANT INFORMATION

- » You must use your **CMS credentials** (e.g., EUA, HARP, or EDIM) to access your Model's Portal.
- » If you **do not have** compatible **CMS credentials**, you will need to **register for CMS Identity Management (IDM) credentials**.
- » **Remote Identity Proofing (RIDP)** is now **required** for access to Model tools. This is a one-time process that all users will need to complete.
- » Note: If you have access to **multiple CMS tools**, you will access a **centralized landing page** where you can **access all applications**.

ADDITIONAL RESOURCES



Connect users who have an [existing CMS OKTA IDM account](#) should follow the link for guidance. OKTA is a cloud based identity and access management platform used by CMS.

Connect users who need to [create an OKTA IDM account](#) should follow the link for guidance.






Follow the link for a [live demo](#) of the process.

BEST PRACTICES

REMOTE IDENTIFY PROOFING

- ✓ RIDP is the process of validating sufficient information that **uniquely identifies you**.
- ✓ Be prepared to input **legal first, middle, and last name**, personal address, date of birth, personal phone number, and social security number.
- ✓ Ensure you are using your **personal, not business**, information.
- ✓ You will be presented with a **list of questions** that only you should know and will have **ten minutes to answer**.
- ✓ **You can go through this process more than once if necessary**.
- ✓ If you are not comfortable completing this process online, you may request a **manual version from the HelpDesk**. Note that this process takes longer.

MULTIFACTOR AUTHENTICATION (MFA)

- ✓ MFA is an approach to security authentication that requires you to **provide more than one form of a credential** to prove your identity. **You only need to select one option**.
- ✓ Options include:
 -  OKTA – Use a push notification sent to the mobile application
 -  Google Authenticator – Enter single-use code from the mobile application
 -  SMS Authenticator – Enter a single-use code sent to your mobile phone
 -  Voice Call Authenticator – Use a phone to authenticate by voice instructions
 -  Email Authenticator – Enter a verification code sent to your email
- ✓ Follow the link to setup an [alternate MFA factor\(s\)](#).

ONGOING SUPPORT

- » If you have additional questions, be on the lookout for **Office Hours**.
- » Contact the **CMMI Salesforce Help Desk** at 1-888-734-6433, option 5
- » Contact the **CMMI Salesforce Email** at CMMIForceSupport@cms.hhs.gov