About the Frequently Asked Questions

These Frequently Asked Questions (FAQ) include information about both the Remote Identity Proofing (RIDP) and Multi-Factor Authentication (MFA) services. The CMS Enterprise Portal and HETS Provider GUI (HPG) will now require that all new HPG Users utilize RIDP. CMS will require all HPG Users (new and existing) to register for and begin using MFA services. These two services will help improve CMS' ability to reduce fraud and ensure system security by implementing security measures that enhance the ability of identifying a given individual and the type of data they are able to access.

Frequently Asked Questions

Remote Identity Proofing

What is Remote Identity Proofing (RIDP)?

What happens to the data submitted for identity proofing?

Will my Social Security Number (SSN) be shared with any federal or private agency?

I already provided my personal information during Registration to set up a CMS Enterprise Portal user account. Why do I have to provide it again to access certain applications?

Will RIDP affect my credit?

What if I have a problem completing Identity Verification? Is there an Experian Help Desk?

What happens if my identity cannot be verified during the online RIDP process?

What happens if my identity cannot be verified during the Experian phone proofing RIDP process?

How do I contact the MCARE Help Desk?

Remote Identity Proofing tips for success

Multi-Factor Authentication

What is Multi-Factor Authentication (MFA)?

When I click on an application, I am directed to the MFA Login Screen. What is this?

Are there any specific MFA service providers? What MFA devices can I link to my CMS user account?

How do we use MFA?

How do I get MFA credentials?

Where can I get the MFA software?

How do I register for MFA if I receive an error when installing the software on my computer?

I cannot download Symantec VIP on my BlackBerry.

I cannot use the desktop MFA software or the mobile phone MFA software.

I am being asked to type a Credential ID. Where do I find the Credential ID?

How do I register additional devices to my user account?

How do I use Multi-Factor Authentication?

What is a Security Code?

If my Credential ID is copied or stolen, can someone else access my CMS Enterprise Portal User account?

Can I access multiple applications if I am multi-factor authenticated?

How many MFA devices can I link to my CMS Enterprise Portal user account?

Will I be charged cell phone time each time I use Symantec VIP MFA on my mobile device?

Do I need to use my MFA device every time I log in? How do I know if I need MFA?

Remote Identity Proofing

1.   What is Remote Identity Proofing (RIDP)?

RIDP is the process of validating sufficient information about you (e.g., credit history, personal demographic information, and other indicators) to uniquely identify you. RIDP is a required service for new HETS Provider GUI (HPG) Users – existing HPG Users will not be required to complete the RIDP process. CMS uses Experian to remotely perform identity proofing.

You may have already encountered RIDP through various interactions with banking systems, credit reporting agencies, and shipping companies. The Experian identity verification service is used by CMS to confirm your identity when you need to access a protected CMS Application. When you log in to the CMS Enterprise Portal and request access to the HETS Provider GUI (HPG), you will be prompted to RIDP if you have not been previously identity proofed to the level of assurance required by the CMS Enterprise Portal. You will be asked to provide a set of core credentials, which include:

- Full **Legal** Name
- Social Security Number
- Date of Birth
- Current **Residential** Address
- Personal Phone Number

The Experian identity verification service will use your core credentials to locate your personal information in Experian and generate a set of questions, referred to as out-of-wallet questions. Experian will attempt to verify your identity to the appropriate level of assurance with the information you provided. Most users are able to complete the ID proofing process in less than five minutes. If you encounter problems with RIDP, you will be asked to contact Experian Support Services via phone to resolve any issues. Please see the Remote Identity Proofing Tips for Success section below for some tips on navigating the ID proofing process successfully.

2.   What happens to the data submitted for identity proofing?

The CMS Enterprise Portal collects your personal information, described as data that is unique to you as an individual, such as name, address, telephone number, Social Security Number, and date of birth. The CMS Enterprise Portal uses this personal information only to verify your identity. Your information will be sent to Experian, an external identity verification provider, to help us confirm your identity. If collected, we will validate your Social Security Number with Experian only for the purpose of verifying your identity. Experian verifies the information you give us against their records and may present you with questions based on your credit profile, called out-of-wallet questions. The out-of-wallet questions and answers, including financial history, are strictly between you and the RIDP service Experian; neither the CMS Enterprise Portal nor the HETS Provider GUI (HPG) will store them. Experian is required by law to securely maintain this data for seven years. For more information regarding how CMS uses the information you provide, please read the CMS Privacy Act Statement.

3.   Will my Social Security Number (SSN) be shared with any federal or private agency?

Your SSN will be used for verification purposes only. Neither the CMS Enterprise Portal nor the HETS Provider GUI (HPG) will share your SSN with any federal or private agency.

4.   I already provided my personal information during Registration to set up a CMS Enterprise Portal user account. Why do I have to provide it again to access certain applications?

Use of RIDP and MFA is required for the HETS Provider GUI (HPG) application. This particular application requires a higher level of security and thus requires these additional services. Utilizing these services will provide additional security for both the User and CMS. In most cases, you may need to provide a few more details (i.e., SSN, Date of Birth) to be able to request access to the selected application or role.

5.   Will RIDP affect my credit?

No, this type of inquiry does not affect your credit score and you will not incur any charges related to this credit score inquiry. When you Identity proof, Experian creates something called a soft inquiry. Soft inquiries are visible only to you, the consumer, and no one else. Soft inquiries have no impact on your credit report, history, or score other than being recorded and maintained for 23 months.

6.   What if I have a problem completing Identity Verification? Is there an Experian Help Desk?

Yes, Experian Help Desk is a dedicated call center for individuals who have failed being proofed online while attempting to obtain a CMS Enterprise Portal credential. The Experian Help Desk can be contacted at 1-866-578-5409. The Experian Help Desk is open Monday through Friday from 8:30 a.m. to 10:00 p.m., Saturday from 10:00 a.m. to 8:00 p.m., and Sunday from 11:00 a.m. to 8:00 p.m., Eastern Standard Time (EST).

For additional information, please see the Experian Consumer Assistance site: [Experian Customer Assistance](#).

7.   What happens if my identity cannot be verified during the online RIDP process?

If Experian cannot identity proof you online, you will be asked to contact either the Experian Help Desk or the MCARE Help Desk, depending on the reason you failed RIDP. The system will provide you with a reference number to track your case. The Experian Help Desk cannot assist you if you do not have the reference number. If you are asked to contact the MCARE Help Desk, you will be given a response code to help the MCARE Help Desk perform the manual identity proofing process with you.

8.   What happens if my identity cannot be verified during the Experian phone proofing RIDP process?

If you contact the Experian Help Desk and your identity cannot be verified, you will be referred to the MCARE Help Desk to complete the manual identity proofing process.

9.   How do I contact the MCARE Help Desk?

The MCARE Help Desk is open Monday through Friday, 7:00 a.m. to 7:00 p.m. EST.

You can contact the MCARE Help Desk using either of the following methods:

- Phone: (866) 324-7315
- Email: mcare@cms.hhs.gov

Remote Identity Proofing Tips for Success

Name

- You must use your full legal name. Refer to your Driver's License or financial account information.
- Your surname **has** to match the surname Experian has for you on file.
- Do not use nicknames.
- If you have a two-part name, enter the second part in the middle name field. (i.e., Billy Bob would have Billy in the first name field and Bob in the middle name field).

Address

- Enter your current **residential** address:

    o Address where you receive financial statements including credit cards and/or utilities
    o Address you most consistently use for billing purposes
    o Address associated with your credit report

- If you have a recent change in address, you can try to identity proof with a prior address.
- Do not enter any extraneous symbols in the address field. If you want to confirm the correct format, visit USPS Look up a Zip Code.

Phone

- Enter a personal landline phone number (if you have one).
- A cell phone can be used, but a residential landline is preferred.

Out-of-Wallet Questions

- You will be asked a series of questions regarding your personal financial transactions/information.
- Try to collect all of your information together before attempting the session.
- Download a free copy of your credit report at Annual Credit Report.

Consent

- You will be asked to give consent to verify your identity information from your credit report.
- The information is utilized only for purposes of **identity proofing** – "you are who you say you are."
- The consent of utilizing the information **does** post as a **soft** inquiry on your credit report. The **soft** inquiry is visible **only** to you.
- The consent/inquiry **does not** affect your credit score.

Exclusions

- If you have a Victim's Statement or a blocked or frozen file, you will **not** be able to complete the identity proofing process online. After attempting online, you will be directed to call Experian's Consumer Services at **1-866-578-5409** to have the alert temporarily lifted so that you can attempt the identity proofing process.
- If you are listed as deceased on the Social Security Administration's (SSA) Death Master File, you will **not** be able to complete the identity proofing process online. You may contact the SSA at **1-800-269-0271**. They will be able to make sure that your information is being reported correctly.

Multi-Factor Authentication

1.   What is Multi-Factor Authentication (MFA)?

MFA is an approach to security authentication that requires you to provide more than one form of a credential in order to prove your identity. CMS is requiring MFA service for CMS Enterprise Portal and HETS Provider GUI (HPG) Users. CMS uses Symantec's Validation and Identity Protection (VIP) service to add a layer of protection for your online identity. Symantec's VIP utilizes government-certified technology and techniques to provide this multi-factor authentication.

2.   When I click on an application, I am directed to the MFA Login Screen. What is this?

The MFA Login screen is displayed when a user attempts to access the CMS Enterprise Portal. If the User has MFA credentials, they will be able to access the application. If the user does not have MFA credentials, they will have to register MFA through their phone or computer.

3.   Are there any specific MFA service providers? What MFA devices can I link to my CMS user account?

Yes, there are various MFA service providers. Symantec is the MFA service provider for CMS Enterprise Portal accounts. Symantec provides validation and identity protection through the computer and smartphone.

4.   How do we use MFA?

CMS uses MFA to grant access to the CMS Enterprise Portal and the HETS Provider GUI (HPG). Users will be asked to enter their CMS Enterprise Portal username, password, and a One Time Password (OTP) that is generated by Symantec VIP software to gain access to the HETS Provider GUI (HPG). The OTP can be generated by a free Symantec application that can be downloaded to your desktop or smartphone, or alternatively, you can receive an OTP via a Short Message Service (SMS) or voice phone call once you have registered your phone in the CMS Enterprise Portal. The "Where can we get the MFA software?" section of the FAQ will provide the necessary information to install the Symantec application on your desktop or smartphone.

5.   How do I get an MFA credential?

The CMS Enterprise Portal will prompt you to register an MFA credential when you request access to the HETS Provider GUI (HPG) and have not already registered an MFA credential in the CMS Enterprise Portal. You will be given a choice of MFA token delivery methods. The primary MFA token delivery method is to download software and install it on your computer or a mobile device. Alternatively, if you require special support, you can set up SMS or voice token to deliver your MFA credential. Where to get the MFA software is discussed below.

6.   Where can I get the MFA software?

You will need MFA software if you choose to receive your MFA credential on a computer or laptop or a mobile device. You will be required to download the MFA software from Symantec and install it in your device of choice.

To download the desktop software for Windows or Mac, navigate to the Symantec VIP Center site at https://idprotect.vip.symantec.com/desktop/home.v and follow the instructions.

If using an iPhone, Android, Blackberry, or other mobile device, use your device to navigate to the Symantec VIP Center mobile site at https://m.vip.symantec.com/home.v and follow the instructions.

SMS OTP and Voice OTP options do not require a software download.

---

7. How do I register for MFA if I receive an error when installing the software on my computer?

If you are having trouble downloading and installing the MFA software on your desktop or laptop, it is possibly due to your company's IT policy that disables users from installing any software on their company-provided machines. Check with your company's IT department for assistance. If your company does not allow you to install MFA software, one alternative is to use a mobile device that you control, or you can also use a voice call to obtain the OTP. You can refer to other instructions in this FAQ for information on cell phone installation and voice token usage.

---

8. I cannot download Symantec VIP on my BlackBerry.

If your Blackberry is a company-provided BlackBerry, your IT department may have locked down your device and disallowed users from loading applications. Check with your IT department to see if you have the required permissions to download an application on your BlackBerry. Some companies have also allowed the download of applications on their BlackBerries but only over Wi-Fi networks. If this is the case, connect your BlackBerry to a Wi-Fi network to download Symantec VIP by typing the following link for the Symantec VIP Center mobile site in the BlackBerry browser: https://m.vip.symantec.com/home.v

---

9. I cannot use the desktop MFA software or the mobile phone MFA software.

The CMS Enterprise Portal allows you to set up a voice or SMS delivery method for your OTP that does not require an MFA software download. You can register a phone number and select SMS or Voice OTP, and then the CMS Enterprise Portal can register your phone number and delivery method with Symantec. After your MFA is activated, when you request access to the CMS Enterprise Portal you will receive either a phone call or text message that contains your OTP, depending on the delivery method that you select.

The SMS and Voice OTP expire within one hour of when they are sent, so please make sure you provide a phone number that will be accessible to you during your typical work hours. For example, do not use a residential phone number if you will normally log in from your place of employment.

---

10. I am being asked to type a Credential ID. Where do I find the Credential ID?

The Credential ID is the 12-digit alphanumeric number on the top of the soft token that was downloaded to your device from Symantec. The Credential ID begins with four letters and ends with eight numbers. In the example below in **Figure 1**, the token displays the Credential ID as VSST57144377.

Figure 1: Credential ID

---

11. How do I register additional devices to my user account?

You can register up to five MFA credentials in your user account. Additional MFA credentials can be added to your account after you have been prompted by the CMS Enterprise Portal to set up the first MFA credential. The "Register your Smartphone or Computer" hyperlink on the "My Profile" page will appear once you have successfully set up your first MFA credential. You can click on the link and add additional MFA devices to your user account.

---

12. How do I use Multi-Factor Authentication?

When you access the CMS Enterprise Portal, the system will display the MFA login screen. You will be required to enter your CMS Enterprise Portal User ID, password, and the VIP security code. If you have registered an MFA token device, enter your CMS Enterprise Portal User ID, password and the security code that is displayed on your MFA token device. In the example below in **Figure 2**, the token displays the security code as 523876.

Figure 2: Security Code

For your protection, an MFA device automatically generates a new security code each time it counts down from a 30-second timer.

If you have registered an MFA SMS token or MFA Voice token, when you access the CMS Enterprise Portal, the system will send you a security code via text message or voice call to the number you registered in your account.

For your protection, a security code sent via SMS or Voice counts down from a 10-minute timer.

13. What is a Security Code?

A Security Code is a numeric code that appears under the label 'Security Code' on your MFA device. This Security Code is mapped to your CMS Enterprise Portal User ID and is used as a second-factor authentication to confirm your identity. Please remember, this Security Code changes every 30 seconds. Make sure you enter and submit the Security Code within 30 seconds.

14. If my Credential ID is copied or stolen, can someone else access my CMS Enterprise Portal User account?

No. A Credential ID cannot solely be used to access a CMS Enterprise Portal User account.

15. Can I access multiple Applications if I'm multi-factor authenticated?

Yes, you can work on multiple applications if you have been Multi-Factor Authenticated. MFA serves as a Single Sign on (SSO) and allows you to work on multiple CMS applications during a valid CMS Enterprise Portal session.

16. How many MFA devices can I link to my CMS Enterprise Portal user account?

CMS Enterprise Portal allows you to link a maximum of five distinct devices, which can either be a computer or a smartphone.

17. Will I be charged cell phone time each time I use Symantec VIP MFA on my mobile device?

It depends on what delivery method you use. The Symantec VIP MFA software is free. Once the Symantec VIP MFA application is downloaded and installed on the phone it does not utilize any cell time to generate the six-digit security code. Cell or network traffic is used to download the application to one's mobile device. There are no recurring charges associated the use of either software option. If you choose not to use the software option and select SMS or Voice OTP, carrier charges may apply.

18. Do I need to use my MFA device every time I log in? How do I know if I need MFA?

MFA is required for specific applications (including the HETS Provider GUI [HPG]) that require a higher level of authentication. Not all applications require MFA for a user. This is decided on the basis of a user's application access. For example, a user has access to App1 and App2. App1 requires MFA and App2 does not. A user logs in using single factor authentication; i.e., the user ID and password. A user is allowed to access App2, but when the user tries to access App1, the CMS Enterprise Portal triggers second-factor authentication. The user must then submit the CMS Enterprise Portal user ID, password and the VIP security code.