Enterprise Privacy Policy Engine (EPPE) FAQs

Enterprise Identity Management (EIDM)
EPPE Registration (ER)
Multi-Factor Authentication (MFA)
EPPE Roles (ERO)
EPPE General Questions (EGQ)
Modify Your DUA (MYD)
COR (COR)
Requester (REQ)
Extractor (EXT)
Shipper (SHP)
MicroStrategy Reports (MSR)
Browsers (BRO)
Errors (ERR)
Enterprise Identity Management (EIDM)

EIDM001 - What is EIDM?
EIDM002 - How can a CMS employee access EIDM?
EIDM003 - How can I view the EIDM User Guide?
EIDM004 - How can I get my User ID if I forgot it?
EIDM005 - What should I do if I forget my password?
EIDM006 - How can I view my profile?
EIDM007 - How can I change my password?
EIDM008 - How can I change my email address?
EIDM009 - How can I change my security challenge questions and answers?
EIDM010 - How can I change my phone number?
EIDM011 - How can I change my home address?
EIDM012 - When I try to login, I get an error message stating, “Your information cannot be verified. Please try again.” What should I do?
EIDM013 - When I try to login, I get the error message stating, "Your account is disabled. Contact the Help Desk to enable your account." Why does this happen?
EIDM014 - When I try to login, I get the error message stating, “Your account has been locked. Please try again later.” Why did this happen and how can I get my account unlocked?
EIDM015 - When I try to login, I am directed to the 'Unlock My Account' view. Why is this and how do I unlock my account?
EIDM016 - Why do I need to answer challenge questions when unlocking my user account?
EIDM017 - Who is eligible to have a CMS EIDM User Account?
EIDM018 - What is an EIDM User account?
EIDM019 - I am new to the CMS Enterprise Portal; how should I create my user account?
EIDM020 - Why should I submit personal information at the time of registering my user account, and how safe is it?
EIDM021 - What will you do with my personally identifiable information?
EIDM022 - Will my Social Security Number (SSN) be shared with any federal or private agency?
EIDM023 - How long does my information stay with Experian?
EIDM024 - Why does Experian require my personal information?
EIDM025 - Does verifying my identity by Experian affect my credit score?
EIDM026 - What if I have problems? Is there an Experian Help Desk?
EIDM027 - What happens if the Experian Help Desk cannot proof my identity?
EIDM028 - Why am I unable to change my User ID?
EIDM029 - Why do I need to answer all three challenge questions during the unlocking of my user account?
EIDM030 - How long does it take to get approved for access to a requested application or role?
EIDM031 - What is Remote Identity Proofing (RIDP)?
EIDM032 - Where can I find information on who has the right to request an SSN?
EIDM033 - What happens to the data submitted for identity proofing?
EIDM034 - I already provided my personal information during registration to setup an EIDM user account. Why do I have to provide it again to access certain applications?

EIDM035 - What happens if my identity cannot be verified during the online Remote Identity Proofing process?

EIDM036 - Why do I need to provide my SSN?

EIDM037 - Why am I getting an access denied message when requesting access to the EPPE application?

EPPE Registration (ER)

ER001 - How can a CMS employee access EPPE?
ER002 - I was already approved for EPPE access, why am I being asked to request a role again?
ER003 - How long does it take for my role to be approved within the EPPE system?

Multi-Factor Authentication (MFA)

MFA001 - Where can I get the Symantec Validation & ID Protection (VIP) software for Multi-Factor Authentication?
MFA002 - What is Multi-Factor Authentication?
MFA003 - Will CMS pay contractors for the costs to implement Multi-Factor Authentication (e.g., the cost of getting RSA Tokens for employees)?
MFA004 - How do I register my Multi-Factor Authentication device?
MFA005 - What is the Credential ID?
MFA006 - How do I use my Multi-Factor Authentication device to Log into my CMS EIDM User account?
MFA007 - How do I add my Multi-Factor Authentication device to my CMS EIDM User Account?
MFA008 - If my credential ID is copied or stolen, can someone else access my CMS EIDM User account?
MFA009 - Why does the security code keep changing on a Multi-Factor Authentication device?
MFA010 - Why is Multi-Factor Authorization required?
MFA011 - How do I use Multi-Factor Authentication?
MFA012 - How do I download the Multi-Factor Authentication software if I receive an error in installing the software?
MFA013 - Is a Mac OS version of the software available?
MFA014 - I am being asked to type the credential ID. Where do I find the credential ID?
MFA015 - What cell phones are supported?
MFA016 - Will I be charged cell phone time each time I use Symantec VIP Access MFA on my cell phone?
MFA017 - How do I download the MFA software on a cell phone?
MFA018 - Why can’t I download Symantec VIP Access on my Blackberry?
MFA019 - Why can’t I use the desktop software or the mobile phone software?
MFA020 - When will I need to use my Symantec VIP credential ID?
MFA021 - How do I update my VIP Credential ID when I receive a new computer?
EPPE Roles (ERO)
ERO001 - Who is a DUA Requester?
ERO002 - Who is a Custodian?
ERO003 - Who is a CMS Contracting Officer’s Representative (COR)?
ERO004 - Who are the Data Use Agreement (DUA) Management Team?
ERO005 - Who is an EPPE Administrator?
ERO006 - Who is an Extractor?
ERO007 - Who is a Shipper?
ERO008 - How do I request a role in the EPPE system?
ERO009 - Is it possible to request multiple roles on the EPPE system?
ERO010 - How can I switch between roles?
ERO011 - How do I remove EPPE access and make role(s) inactive for my organization?

EPPE General Questions (EGQ)
EGQ001 - What is EPPE?
EGQ002 - Why am I unable to do anything when I access EPPE?
EGQ003 - Why is my organization suspended?
EGQ004 - I receive a ton of EPPE email notifications. Can I turn off notifications?
EGQ005 - Why didn’t my DUA status switch to “Closed?”
EGQ006 - How can I request an additional role?
EGQ007 - How can I change my email preferences?
EGQ008 - How do I log out of EPPE?
EGQ009 - How do I contact the EPPE Help Desk?
EGQ010 - What are the file types that can be uploaded into EPPE?
EGQ011 - Do I need to enter any job codes to request access to EPPE?
EGQ012 - What does the data extraction percentage mean?
EGQ013 - How can we re-use data files if additional year(s) are needed and how can we utilize the “Apply all” feature when adding new year(s)?

Modify Your DUA (MYD)
MYD001 - What is a DUA?
MYD002 - I receive a ton of EPPE email notifications. Can I turn off notifications?
MYD003 - Why didn’t my DUA status switch to “Closed?”
MYD004 - My DUA expired. Why can’t I find it immediately after extending it?
MYD005 - How can I search for a DUA?
MYD006 - Where can I find the recipient information on a DUA?
MYD007 - How can I contact the DUA Management Team?

COR (COR)
COR001 - As a COR, why can’t I see my DUAs in any of my queues?
COR002 - At the Proxy end date, will the COR or DUA Requester need to go in and end the Proxy assignment or will the system automatically end the assignment?
**COR003** - How can the COR identify updates on the DUA?
**COR004** - How do I get a list of my DUAs?
**COR005** - How can a COR access a previously approved DUA?
**COR006** - If the existing COR needs to be changed, will that COR need to approve the COR change?
**COR007** - Does the COR receive notifications from EPPE about DUA Change Contact requests?

**Requester (REQ)**
**REQ001** - As a Requester on a CMS DUA, why am I unable to request or assign certain DUAs through the Change Contact function?
**REQ002** - How can the DUA Requester update the COR on a Contractor DUA?
**REQ003** - What would happen with the DUA if both the DUA Requester and COR are no longer active?
**REQ004** - Should the DUA Requester create a DUA for each year of a contract Period of Performance (PoP)?
**REQ005** - Once a DUA is submitted, does it go to the COR for approval?
**REQ006** - Will there be any email notifications when a DUA is expiring?
**REQ007** - At the Proxy end date, will the COR or DUA Requester need to go in and end the Proxy assignment or will the system automatically end the assignment?
**REQ008** - When will OEDA stop accepting paper DUA forms?
**REQ009** - Do you have to be a DUA Requester to be designated as a Proxy?
**REQ010** - How do I get a list of my DUAs?
**REQ011** - When would the DUA Requester use the Ad Hoc Request?
**REQ012** - How are documents provided by the DUA Requester? Do they need to scan and send them via email?
**REQ013** - If the existing COR needs to be changed, will that COR need to approve the COR change?
**REQ014** - What is the guidance on adding sub-contractors to the DUA?
**REQ015** - Does the CEO of a company have to be the DUA Requester on the DUA?
**REQ016** - What is a Data Extract System (DESY) User? Do we have to add these users?

**Extractor (EXT)**
**EXT001** - As an Extractor, how can I track partially extracted orders within EPPE?
**EXT002** - As an Extractor, how can I create an order?
**EXT003** - As an Extractor, where can I view unfinished orders?
**EXT004** - As an Extractor, where can I view finished orders that haven’t been shipped?
**EXT005** - As an Extractor, where can I view orders that have been shipped?

**Shipper (SHP)**
**SHP001** - As a Shipper, where can I view orders that are ready to be shipped?
**SHP002** - As a Shipper, where can I view orders that have been shipped?
MicroStrategy Reports (MSR)

MSR001 - How do I gain access to MicroStrategy Reports within EPPE?
MSR002 - When a user has multiple roles within EPPE, how does MicroStrategy know for what role you are requesting reports?
MSR003 - In MicroStrategy, can the fields/columns on the report result screen be expanded?
MSR004 - In MicroStrategy, can filters be applied to the report result screen?

Browsers (BRO)

BRO001 - Which browsers are supported by the CMS Enterprise Portal?
BRO002 - What browser mode is supported?
BRO003 - What document mode is supported?
BRO004 - Is JavaScript required for the CMS Enterprise Portal?
BRO005 - How do I clear my browser’s cache using Internet Explorer (IE) 9, 10, and 11?
BRO006 - How do I clear my browser’s cache using Google Chrome?
BRO007 - How do I clear my browser’s cache using Mozilla Firefox?
BRO008 - How do I enable pop-ups in Internet Explorer?
BRO009 - How do I enable pop-ups in Google Chrome?
BRO010 - How do I enable pop-ups in Mozilla Firefox?

Errors (ERR)

ERR001 - What do I do when I receive a “Portlet not Available” error?
ERR002 - What do I do when I receive a “Request Failed” error?
**EIDM001 - What is EIDM?**

EIDM is the acronym for CMS' Enterprise Identity Management service, which includes Remote Identity Proofing, Access Management (Multi-Factor Authentication), Authorization Assistance Workflow Tools, and Identity Lifecycle Management functions (i.e., password reset, recertification, forgotten User ID, etc.).

[Back To Top]

**EIDM002 - How can a CMS employee access EIDM?**

To access the EPPE system you first have to register for a User ID and password for the Enterprise Identity Management (EIDM) system.

1. If you are accessing the CMS Enterprise Portal from the Internet, please navigate to [https://portal.cms.gov](https://portal.cms.gov). If you are accessing the CMS Enterprise Portal from the Intranet, please navigate to [https://portal.cms.cmsnet](https://portal.cms.cmsnet).
2. On the CMS Enterprise Portal page, select the **<New User Registration>** link.
3. In Step #1, click on **<Choose Your Application>** and select the appropriate application.
4. Read and agree to the Terms and Conditions by checking the box and clicking **<Next>** at the bottom of the page.
5. In Step #2, provide the information requested on the **<Register Your Information>** page and click **<Next>** at the bottom of the page.
6. Create a User ID, Password and Challenge Questions on the **<Create User ID, Password & Challenge Questions>** page and click **<Next>** at the bottom of the page.
7. Review the information on the **<Registration Summary>** page and click on **<Submit User>** on the bottom of the page. You will receive an email acknowledging your successful registration.

[Back To Top]

**EIDM003 - How can I view the EIDM User Guide?**

The following are step-by-step instructions on how to access the EIDM User Guide.

2. Click on the **<Help>** link in the upper right-hand corner.

[Back To Top]

**EIDM004 - How can I get my User ID if I forgot it?**

The following are the basic step-by-step instructions on how to use the **<Forgot User ID?>** feature.

2. Select the **<Forgot User ID?>** link on the CMS Secure Portal.
3. Provide the information required on the <Forgot User ID> page and select <Submit> to continue.
4. The acknowledgement page is displayed and informs the user that the information entered has been successfully verified and an email, with your User ID, has been sent to the email address on record.

Back To Top

EIDM005 - What should I do if I forget my password?
The following are the basic step-by-step instructions on how to use the <Forgot Password?> feature to create a new password.

2. Select the <Forgot Password?> link on the CMS Secure Portal page.
3. Enter your User ID and select <Next> to continue.
4. Provide the answers to the challenge questions.
5. Enter a password in the <Create New Password> box.
6. Re-enter the same password for <Confirm New Password> and select <Submit>.
7. The acknowledgement page is displayed and informs the user that the password has been successfully changed and an email has been sent to the email address on record.

Back To Top

EIDM006 - How can I view my profile?
The following are the basic step-by-step instructions on how to <View My Profile> information.

2. After you are logged in, click on your name in the upper right-hand side of the CMS Secure Portal page.
3. Select <My Profile> from the dropdown menu to continue, and the <My Profile> page displays.

Back To Top

EIDM007 - How can I change my password?
The following are the basic step-by-step instructions on how to <Change Your Password>.

2. After you are logged in, click on your name in the upper right-hand side of the CMS Secure Portal page.
3. Select <My Profile> from the dropdown menu to continue, and the <My Profile> page displays.
4. Select <Change Password> from the <Manage Profile> menu on the left-hand side, and the <Change Password> page displays.
5. Enter your old password.
6. Create and enter a new password of your choice for <Enter New Password>.
7. Re-enter the same password for <Confirm New Password> and select <Submit> to continue.
8. The <Change Password> is acknowledged and the portal returns to the login page.

**EIDM008 - How can I change my email address?**

The following are the basic step-by-step instructions on how to <Change Email Address>.

2. After you are logged in, click on your name in the upper right-hand side of the CMS Secure Portal page.
3. Select <My Profile> from the dropdown menu to continue, and the <My Profile> page displays.
4. Select <Change Profile> from the <Manage Profile> menu on the left-hand side, and the <Change Profile> page displays.
5. Provide the answers to your security questions.
6. Scroll to the <Email Address> and provide your new email address.
7. Provide the same email address in the <Confirm Email Address> box.
8. Scroll to the bottom of the page and click on <Submit>.
9. The email address change is confirmed and the <View My Profile> displays.

**EIDM009 - How can I change my security challenge questions and answers?**

The following are the basic step-by-step instructions on how to use the <Change Challenge Questions and Answers> feature.

2. After you are logged in, click on your name in the upper right-hand side of the CMS Secure Portal page.
3. Select <My Profile> from the dropdown menu to continue, and the <My Profile> page displays.
4. Select <Change Profile> from the <Manage Profile> menu on the left-hand side, and the <Change Profile> page displays.
5. Select <Change Challenge Questions> and the <Change Challenge Questions> page displays.
6. Provide your <User ID> and <Password> and click on <Next>.
7. Select a question and then provide the answer of your choosing.
8. Continue to select a question and provide an answer until all three challenge questions have been selected and answered.
9. Select <Submit> to continue.
10. The change to the challenge questions is confirmed and the <View My Profile> displays.

**Back To Top**

**EIDM010 - How can I change my phone number?**
The following are basic step-by-step instructions on how to <Change Phone Number> feature.

2. After you are logged in, click on your name in the upper right-hand side of the CMS Secure Portal page.
3. Select <My Profile> from the dropdown menu to continue, and the <My Profile> page displays.
4. Select <Change Profile> from the <Manage Profile> menu on the left-hand side, and the <Change Profile> page displays.
5. Provide the answers to your security questions.
6. Scroll to the <Phone Number> and provide your new phone number.
7. Scroll to the bottom of the page and click on <Submit>.
8. The phone number change is confirmed and the <View My Profile> displays.

**Back To Top**

**EIDM011 - How can I change my home address?**
The following are the basic step-by-step instructions on how to <Change Home Address> feature.

2. After you are logged in, click on your name in the upper right-hand side of the CMS Secure Portal page.
3. Select <My Profile> from the dropdown menu to continue, and the <My Profile> page displays.
4. Select <Change Profile> from the <Manage Profile> menu on the left-hand side, and the <Change Profile> page displays.
5. Provide the answers to your security questions.
6. Scroll to the address boxes and provide your new home address.
7. Scroll to the bottom of the page and click on <Submit>.
8. The home address change is confirmed and the <View My Profile> displays.

**Back To Top**

**EIDM012 - When I try to login, I get an error message stating, “Your information cannot be verified. Please try again.” What should I do?**

Please check the User ID and password that you entered. An incorrect combination of these will result in such an error message.
**EIDM013 - When I try to login, I get the error message stating, "Your account is disabled. Contact the Help Desk to enable your account." Why does this happen?**

A user's account can be disabled by application help desks or EIDM Administrators for possible reasons linked to security violations or fraud detection. In order to enable your disabled account, you are required to contact the application helpdesk.

**EIDM014 - When I try to login, I get the error message stating, "Your account has been locked. Please try again later." Why did this happen and how can I get my account unlocked?**

After three unsuccessful attempts to login, your account will be locked. Your account will be unlocked after 60 minutes have elapsed since your third consecutive failed authentication attempt. You are required to enter valid credentials associated with your user account to unlock the account.

**EIDM015 - When I try to login, I am directed to the 'Unlock My Account' view. Why is this and how do I unlock my account?**

EIDM locks your user account if no account activity is reported for 60 days. When you login after 60 days the system will display the ‘Unlock my Account’ view; enter your User ID and correctly answer all challenge questions on the next page; enter your new password in the input fields of ‘New Password’ and ‘Confirm New Password’ to unlock your account.

**EIDM016 - Why do I need to answer challenge questions when unlocking my user account?**

EIDM needs to verify your identity. Your response to the challenge questions will enable EIDM to confirm your identity and help you proceed in getting your account unlocked. This also protects you from identity theft.

**EIDM017 - Who is eligible to have a CMS EIDM User Account?**

All U.S. citizens who are over 18 years of age and have a current or previous valid U.S. residential address are eligible to have a CMS EIDM User Account.
EIDM018 - What is an EIDM User account?
EIDM is an acronym for Enterprise Identity Management. An EIDM account verifies the identity of the user and ensures that only authorized/registered users can access protected information and systems through the CMS Enterprise Portal.

EIDM019 - I am new to the CMS Enterprise Portal; how should I create my user account?
Once you are on the CMS enterprise portal at https://portal.cms.gov, select the <New User Registration> link. You are required to enter your personal information and answer the knowledge-based questions. Choose desired user ID / Password as per the guidelines provided. Once the details have been successfully updated in EIDM, the system will display a message confirming the creation of the user account.

EIDM020 - Why should I submit personal information at the time of registering my user account, and how safe is it?
EIDM needs your personal information to verify your identity. During the registration process, EIDM initiates a remote identity proofing call with one of the identity service providers and, based upon the information provided, allows you to create a user account.

For security level information please visit: http://www.cms.gov/About-CMS/Agency-Information/Aboutwebsite/Privacy-Policy.html

EIDM021 - What will you do with my personally identifiable information?
EIDM uses an external authentication service provider, Experian, to help us verify your identity based on the information that you have provided. Experian verifies your information against its records to successfully identify you.

CMS provides, on the public-facing Web sites, the Terms & Conditions of how your information will be handled when registering for a CMS EIDM user account.

EIDM022 - Will my Social Security Number (SSN) be shared with any federal or private agency?
Your SSN will be shared with Experian, the authentication service provider, to verify your identity. EIDM does not share your SSN with any other federal or private agency.
EIDM023 - How long does my information stay with Experian?
Experian will only keep the information we share for seven years as required by federal laws, regulations, or guidelines.

Back To Top

EIDM024 - Why does Experian require my personal information?
Experian may use credit information to help verify your identity; this may result in what is known as a “soft inquiry” on your Experian credit report.

Back To Top

EIDM025 - Does verifying my identity by Experian affect my credit score?
No. These kinds of inquiries are termed as “soft inquiry.”

Soft inquiries:

- do not affect your credit score, and you do not incur any charges related to them;
- are displayed in the version of the credit profile viewable only to consumers and are not reported to lenders.

If you order a credit report from Experian, you will see an entry of inquiry by the Centers for Medicare & Medicaid Services with our address and the date of request.

Back To Top

EIDM026 - What if I have problems? 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 EIDM 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.

Back To Top

EIDM027 - What happens if the Experian Help Desk cannot proof my identity?
If you contact the Experian Help Desk and your identity cannot be verified, you will need to contact the respective application help desk to complete the manual identity proofing process.

Back To Top

EIDM028 - Why am I unable to change my User ID?
The User ID identifies you uniquely to EIDM; therefore, you cannot change your User ID.

Back To Top
EIDM029 - Why do I need to answer all three challenge questions during the unlocking of my user account?
EIDM needs to verify your identity. Your response to the set of three challenge questions will enable EIDM to confirm your identity and help you proceed in getting your account unlocked. This also protects you from identity theft.

Back To Top

EIDM030 - How long does it take to get approved for access to a requested application or role?
It can take up to 30 days to be granted access to an application or role. After 30 days, your request will expire. In the unlikely event that this happens, please contact the respective Application Help Desk.

Back To Top

EIDM031 - 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. If you are requesting electronic access to protected CMS information or systems, you must be identity proofed to gain access. CMS uses Experian, an external identification verification provider, 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 system and request access to EPPE, you will be prompted to RIDP if you have not been previously identity proofed to the level of assurance required by the EPPE. You will be asked to provide a set of core credentials that include:

• Full Legal Name
• Social Security Number (may be optional)
• 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.

Back To Top
EIDM032 - Where can I find information on who has the right to request an SSN?

Specific laws require a person to provide his or her SSN for certain purposes. Federal law mandates that state Departments of Motor Vehicles, tax authorities, welfare offices, and other governmental agencies request your SSN as proof that you are who you claim to be. However, the Privacy Act of 1974 requires that government agencies at the local, state, and federal level disclose to each person whether submitting your Social Security number is required, details on the use of this information, and what law or authority requires its use.

For information on who has the right to request your SSN, see [http://www.identityhawk.com/Who-Can-Lawfully-Request-My-Social-Security-Number](http://www.identityhawk.com/Who-Can-Lawfully-Request-My-Social-Security-Number)

The text of the Privacy Act can be found at [http://www.justice.gov/opcl/privstat.htm](http://www.justice.gov/opcl/privstat.htm)

Back To Top

EIDM033 - What happens to the data submitted for identity proofing?

The EPPE application collects 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. 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 Experian; neither the EPPE application nor CMS can access or store this information. For more information regarding how CMS uses the information you provide, please read the CMS Privacy Act Statement.

Back To Top

EIDM034 - I already provided my personal information during registration to setup an EIDM user account. Why do I have to provide it again to access certain applications?

When you have selected an application or role that requires a higher level of security, you are required to complete identity verification. 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.

Back To Top

EIDM035 - What happens if my identity cannot be verified during the online Remote Identity Proofing process?

If Experian cannot identity proof you online, you will be asked to contact either the Experian Verification Support Services Help Desk or the respective application 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
EPPE FAQs Version 2.0

are asked to contact the application help desk, you will be given a ticket number to help the application help desk perform the manual identity proofing process with you.

Back To Top

EIDM036 - Why do I need to provide my SSN?
The Enterprise Identity Management (EIDM) system is a public government website, allowing any U.S. citizen over the age of 18 to open an account. EIDM is designed to use your SSN to verify your identity. Since you are applying for access to a Federal application that is housed behind the EIDM portal, your SSN is required to complete the verification.

Back To Top

EIDM037 - Why am I getting an access denied message when requesting access to the EPPE application?
You might be attempting to log into the CMS Enterprise Portal with an incorrect User ID. The CMS Enterprise Portal User ID is created when first setting up your portal account and is not used by any other CMS system (such as EUA). If you do not have an account on the CMS Enterprise Portal, you will first need to set one up before accessing EPPE. This process can be started by clicking the “New User Registration” button located on the login screen at https://portal.cms.gov/wps/portal/unauthportal/home/.

Back To Top

ER001 - How can a CMS employee access EPPE?
To request access to the EPPE application and a role follow the instructions below.

1. If you already have a User ID and password, navigate to https://portal.cms.gov.
2. Log in with your User ID and password.
3. On the <My Portal> click on <Request/Add Apps>.
4. After the <Access Catalog> page is displayed, select <Request Access> for the EPPE application.
5. Provide your business contact information, if it is not already on file (EIDM will prompt you if this is needed).
6. Select the <Role> you are registering for (EPPE User) from the <Select the Role> dropdown menu.
7. Enter and select the appropriate information needed to complete your request for access (EIDM will prompt on what is needed).
8. Click on <Submit>.
9. You will now be asked to provide information for the Remote Identity Verification.

Back To Top
ER002 - I was already approved for EPPE access, why am I being asked to request a role again?
EPPE requires a two-step approval process. The first approval grants you access to the EPPE application as an EPPE User. The second approval is for a specific role within the EPPE application (i.e.: COR or Requester roles).

Back To Top

ER003 - How long does it take for my role to be approved within the EPPE system?
Approvals are handled by the EPPE Administrator. Generally, they are processed within 2 business days. You will receive an email notifying you when the Administrator approves your role.

Back To Top

MFA001 - Where can I get the Symantec Validation & ID Protection (VIP) software for Multi-Factor Authentication?
In order to utilize Multi-Factor Authentication, you will be required to download the VIP Access software to the device (i.e., desktop or mobile phone) that you will be using to access EPPE. This software can be found at the following link: https://idprotect.vip.symantec.com/. Once the software has been downloaded to the device, it will be assigned a “Credential ID.” You will then be required to activate each Credential ID that will be used to access EPPE.

Back To Top

MFA002 - What is Multi-Factor Authentication?
Multi-Factor Authentication is generally required to access CMS sensitive data. Multi-Factor Authentication uses a combination of two (or more) different token attributes (also known as factors), to authenticate the user.

- The first is what users know. This is usually a password, but this can also include a user response to a secret challenge question. (This is generally known as Knowledge Based Authentication and, by itself, is insufficient for authentication to most CMS sensitive information.)
- The second is what users have. This could be a physical object (hard token), for example, a smart card, or hardware token that generates one-time-only passwords. It might also be some encrypted software token (soft token) installed on an individual’s system (usually with very limited functional parameters for use).
- The third is who users are, as indicated by some biometric characteristic, such as a fingerprint or an iris pattern.
Two-factor authentication means that instead of using only one single type of authentication token or factor, such as only things a user knows (passwords, shared secrets, solicited personal information, etc.), a second token or factor, something the user has or something the user is, must also be supplied in order to complete the authentication process.

MFA003 - Why is there a long delay receiving the MFA Security Code email?
The email may be delayed by a firewall or virus scans. To bypass this issue, you have the option of downloading the VIP Access application to your laptop or mobile device. Please follow this link to download the application [https://vip.symantec.com/](https://vip.symantec.com/).

MFA004 - How do I register my Multi-Factor Authentication device?
Once your identity is verified at a high level, EIDM will display the ‘Register Device’ screen. You need to enter the Multi-Factor Authentication type (Desktop/ Smartphone/ Smart Card/ VIP Security Token), Credential ID and Security Code (VIP Security Token).

MFA005 - What is the Credential ID?
The Credential ID for the Multi-Factor Authentication device is a security credential that contains a unique 12-character alphanumeric ID.

MFA006 - How do I use my Multi-Factor Authentication device to Log into my CMS EIDM User account?
Once you have registered your Multi-Factor Authentication device, you must enter the 6 digit security code that is displayed on the device in the ‘Security Code’ field.

MFA007 - How do I add my Multi-Factor Authentication device to my CMS EIDM User Account?
You add the Multi-Factor Authentication device by selecting your MFA Device Type from the dropdown list after entering your password.
MFA008 - If my credential ID is copied or stolen, can someone else access my CMS EIDM User account?
No, a Multi-Factor Authentication device alone cannot be used to Sign In to your CMS EIDM User account. Multi-Factor Authentication is used in addition to your EIDM user ID and password.

MFA009 - Why does the security code keep changing on a Multi-Factor Authentication device?
For your protection, Multi-Factor Authentication device automatically generates a new security code each time it counts down from a 30-second timer.

MFA010 - Why is Multi-Factor Authorization required?
As more and more information is being made available and transacted online, new and improved processes and technologies are required to assure that individuals are provided appropriate access to information and only the access that they are authorized to have. Symantec’s VIP Access utilizes government certified technology and techniques to provide this Multi-Factor Authentication. This type of authentication security is being used for many online systems across industries that require this greater level of assurance. These systems also support the government’s initiatives, leveraging the same technology, for a safer and secure Internet in which a common online identity can be used.

MFA011 - How do I use Multi-Factor Authentication?
When logging into the system, the individual will be asked to enter their username, password and then a onetime password that is generated by Symantec VIP Access. This onetime password can be generated by one of several media that are available. The onetime password can be generated by a free Symantec application that can be downloaded to your desktop or smartphone or received via an SMS or voice phone call if your phone is properly registered.

MFA012 - How do I download the Multi-Factor Authentication software if I receive an error in installing the software?
If you are having trouble downloading and installing the MFA software, it is probably due to your IT policy that disables users from installing any software on their machines. A different type of token will need to be used in this case. If you have access to a cell phone, please use the cell phone. There will also be the option to use a voice call to obtain the token. You can refer to
MFA013 - Is a Mac OS version of the software available?
Yes, a Mac version of the desktop token is available for Mac desktop users at https://idprotect.vip.symantec.com/desktop.

MFA014 - I am being asked to type the credential ID. Where do I find the credential ID?
The credential ID is the 12-digit alpha-numeric number on the top of the soft token; it begins with four letters and ends with 8 numbers.

MFA015 - What cell phones are supported?
Symantec VIP Access is supported on over 900 different cell phones. A list of all the supported phones are shown on the Web site http://m.verisign.com under the ‘Supported Phones’ tab.

MFA016 - Will I be charged cell phone time each time I use Symantec VIP Access MFA on my cell phone?
No. Once the Symantec VIP MFA application is loaded on the phone it does not utilize any cell time to generate the six-digit code. Cell or network traffic is used to download the application to one’s cell phone.

MFA017 - How do I download the MFA software on a cell phone?
For the different cell phone devices refer to the links or applicable app stores. Search for Symantec VIP Access.

- iOS (iPhone, iPad) - Download on iTunes. Link with more information is: https://itunes.apple.com/us/app/vip-access/id307658513?mt=8
- Blackberry - Go to http://m.verisign.com on phone’s browser to download.
- Windows Mobile - Go to http://m.verisign.com on phone’s browser to download.
- Older Phone - Go to http://m.verisign.com on phone’s browser to download.
MFA018 - Why can’t I download Symantec VIP Access on my Blackberry?
If your Blackberry is a company provided Blackberry, the company’s IT department may have the device locked down, which will disallow users from loading applications. Check with your IT department to see if you are able to download an application on your Blackberry. Some companies have allowed the download of applications on their Blackberries only over Wi-Fi networks. If this is the case, connect your Blackberry to a Wi-Fi network to download Symantec VIP Access by typing w.verisign.com in the Blackberry browser.

Back To Top

MFA019 - Why can’t I use the desktop software or the mobile phone software?
An option is available to use a voice or SMS based soft token delivery method. This would require that you provide a phone number to receive either a phone call or text message. When that number is registered with EIDM you will be presented with the option to receive a phone-based token delivery during your login process. Upon requesting token delivery, you will receive either a phone call or text message from Symantec with your six-digit one-time password.

These SMS and voice tokens expire within 1 hour of when they are sent to a user. Please make sure you provide a phone number that will be accessible to you during your typical work hours; i.e., do not use a residential phone number if you will normally login from your place of employment.

Back To Top

MFA020 - When will I need to use my Symantec VIP credential ID?
During the EPPE access request process you will need to register your device using the Symantec VIP credential ID.

Back To Top

MFA021 - How do I update my VIP Credential ID when I receive a new computer?
The steps are outlined below:

1. Log into EIDM.
2. In the upper right-hand corner click on your name.
3. Select <My Profile>.
4. On the left-hand side click on <Register MFA>
5. Select <Phone/Tablet/PC/Laptop> from the <Chose MFA Device> dropdown list.
6. Copy the VIP Credential ID from the Symantec VIP Access software to the <Enter Credential ID> field.
7. Enter a meaningful <Enter MFA Device Description>.
8. Click on <Submit>.
**ERO001 - Who is a DUA Requester?**
The person authorized to legally bind their organization to the terms specified in the DUA. This is a required role on the Data Use Agreement (DUA).

**ERO002 - Who is a Custodian?**
Individuals who will have actual possession of the CMS data files, and who will be responsible for observance of all conditions of use, including the establishment and maintenance of security arrangements to prevent unauthorized use. This is a required role on the DUA and in rare instances may be the same individual as the Requester.

**ERO003 - Who is a CMS Contracting Officer’s Representative (COR)?**
A COR is an employee of CMS responsible for ensuring that their contractors meet the commitments of their contracts.

**ERO004 - Who are the Data Use Agreement (DUA) Management Team?**
The DUA Team are within the Data and Information Dissemination Group/Office of Enterprise Data & Analytics at CMS and are responsible for overseeing the EPPE system and the tracking of CMS disclosures of PII/PHI.

**ERO005 - Who is an EPPE Administrator?**
A member of the Data and Information Dissemination Group/Office of Enterprise Data & Analytics at CMS, who is responsible for approving roles, changing reference data, and making high-level decisions in EPPE.

**ERO006 - Who is an Extractor?**
An employee or contractor of CMS responsible for gathering the specific data indicated in the Data Use Agreement (DUA) for dissemination to the requesting entity.

**ERO007 - Who is a Shipper?**
An employee or contractor of CMS responsible for the physical and/or digital delivery of the requested data files to the requesting entity.
ERO008 - How do I request a role in the EPPE system?
Once your access to the EPPE system has been approved, you will need to log on to EPPE. On the EPPE Welcome page there will be a blue link "Request Access". Click on the blue link to start the EPPE role request process.

ERO009 - Is it possible to request multiple roles on the EPPE system?
Yes, you can request multiple roles in the EPPE system. During the initial request, you can continue to add additional roles to the “Your Selection” portion of the screen. Once all necessary roles are requested, click on "Submit". Users can also request additional roles at any time from the “Request Additional Role” option under the “My Organizations” tab.

ERO010 - How can I switch between roles?
To switch roles, click on the "Switch To" dropdown list in the upper right-hand side and choose the appropriate role to activate.

ERO011 - How do I remove EPPE access and make role(s) inactive for my organization?
To remove your access or make your role(s) inactive in the EPPE application, please submit a request to the EPPE Help Desk at EPPE@cms.hhs.gov. If you are making the request on behalf of another user associated with your company, the user’s supervisor would need to email the request to remove the access to the EPPE Help Desk. Once completed, the EPPE Help Desk will confirm that the access has been removed.

EGQ001 - What is EPPE?
The Enterprise Privacy Policy Engine (EPPE) system automates the process of submitting Data Use Agreement (DUA) requests and tracking their status through the approval and data receipt stages. End user requesters and all CMS approvers can interactively use the system to manage the workflow. For those requests that require supporting documentation, it allows documents to be uploaded and then later downloaded for review.

EGQ002 - Why am I unable to do anything when I access EPPE?
Did you receive a message that your organization has an expired DUA? If you have an expired DUA the only DUA functions, you may perform are to extend or close the expired DUA. Until the
expired DUA is extended or closed, you will not be allowed to do anything else in the EPPE system.

Back To Top

**EGQ003 - Why is my organization suspended?**
An organization is suspended if it has one or more expired DUAs that have not been remedied (either extended or closed). Any organization that has an expired CMS DUA will not receive authorization to obtain any new data until their expired DUA has been resolved.

Back To Top

**EGQ004 - I receive a ton of EPPE email notifications. Can I turn off notifications?**
On the bottom left-hand side of the menu items you will find *<My Preferences>*. Within that there is a link for *<Email Preference>*. Once you click on the link you will be able to disable or enable email notifications. Even if you disable email notifications, you will still receive email notifications for certain DUA actions that are required.

Back To Top

**EGQ005 - Why didn't my DUA status switch to “Closed?”**
All data files on the DUA *<DUA Number>* must be closed in order for the DUA to have a status of “Closed.” If all the data files on the DUA selected to be closed are not closed, the DUA status will reflect “Open.”

Back To Top

**EGQ006 - How can I request an additional role?**
On the navigation menu, under the *<My Access>* tab, click on *<Request Additional Role>*.

Back To Top

**EGQ007 - How can I change my email preferences?**
On the navigation menu, under the *<My Preference(s)>* tab, click on *<Email Preferences>*.

Back To Top

**EGQ008 - How do I log out of EPPE?**
On the navigation menu click on the *<Exit EPPE>* tab or click *<Log Out>* in the upper right-hand corner to log out of EPPE.

Back To Top
EGQ009 - How do I contact the EPPE Help Desk?
You may contact the EPPE Help Desk via phone at 844-EPPE-DUA (844-377-3382) or via email at eppe@cms.hhs.gov. The EPPE Help Desk operating hours are Monday through Friday 9 AM through 6 PM (EST).

Back To Top

EGQ010 - What are the file types that can be uploaded into EPPE?
The application will accept doc, .pdf, and .txt files that are 2 MB or smaller. If the file type is invalid, the user will receive an error message and the file will not be uploaded successfully.

Back To Top

EGQ011 - Do I need to enter any job codes to request access to EPPE?
No. To access EPPE, users must have current EIDM credentials to request access to the EPPE application. Once access is granted, the user must request a specific role for the EPPE application e.g. CMS Contact (COR) or DUA Requester.

Back To Top

EGQ012 - What does the data extraction percentage mean?
The data extraction percentage indicates the number of records provided for a specific file.

Back To Top

EGQ013 - How can we re-use data files if additional year(s) are needed and how can we utilize the “Apply all” feature when adding new year(s)?
You may use the re-use feature for years of data that you currently have on other active DUAs. If you also need additional years of data for the file, you would have to request the new year(s) under a new file on the DUA. The “Apply-all” feature works for the new files listed on the DUA, but it will not work for the re-use files.

Back To Top

MYD001 - What is a DUA?
The Centers for Medicare & Medicaid Services (CMS) makes data files available to certain stakeholders as allowed by federal laws and regulations as well as CMS policy. CMS enters into Data Use Agreements (DUAs) with most data requesters for disclosures of protected health information (PHI) and/or personally identifiable information (PII) to ensure that data requesters adhere to CMS privacy and security requirements and data release policies.

Back To Top
MYD002 - I receive a ton of EPPE email notifications. Can I turn off notifications?
On the bottom left-hand side of the menu items you will find <My Preferences>. Within that there is a link for <Email Preference>. Once you click on the link you will be able to disable or enable email notifications. Even if you disable email notifications, you will still receive emails notifying you that certain actions are required of you on a DUA(s).

MYD003 - Why didn’t my DUA status switch to “Closed?”
All data files on the DUA <DUA Number> must be closed in order for the DUA to have a status of “Closed.” If all the data files on the DUA selected to be closed are not closed, the DUA status will reflect “Open.”

MYD004 - My DUA expired. Why can’t I find it immediately after extending it?
The system will process the DUA extension request when the nightly processing job is run. The DUA will be available for use the following day. This instance will not occur if the DUA is extended prior to expiring.

MYD005 - How can I search for a DUA?
On the navigation menu, under the Search tab, click DUA Search to pull up the search functionality.

MYD006 - Where can I find the recipient information on a DUA?
The recipient information is part of the data file attributes. The below steps will assist you in finding the recipient information.

1. Click on DUA Search.
2. Enter DUA# in the DUA# field and click on Search.
3. Once the DUA displays in the search result screen, click on View.
4. When the DUA displays, scroll down to the data file section.
5. Click on the radio button next to each file to expand the file attributes.
6. The recipient information is part of the expanded data.

MYD007 - How can I contact the DUA Management Team?
You may contact the DUA Management Team via email at datauseagreement@cms.hhs.gov.
**COR001 - As a COR, why can't I see my DUAs in any of my queues?**

DUAs will appear in your queues when you have actions to approve or deny. As a COR you may view all of your DUAs through the DUA search function.

**COR002 - At the Proxy end date, will the COR or DUA Requester need to go in and end the Proxy assignment or will the system automatically end the assignment?**

The system will automatically end the COR or Requester Proxy assignment at the end of the specified end date.

**COR003 - How can the COR identify updates on the DUA?**

The COR can identify updates on a DUA by accessing the DUA lifecycle. When the DUA lifecycle is expanded it will display and track the updates made on the DUA. A DUA Requester can enter comments detailing the updated information which will also display in the lifecycle.

**COR004 - How do I get a list of my DUAs?**

The DUA Requester and CORs can use the DUA Search function to review/export a list of DUAs to Excel.

**COR005 - How can a COR access a previously approved DUA?**

The COR that is listed on specific DUA(s) can access these DUAs through the DUA Search. The COR can search by a specific DUA number, status or various other attributes to view DUA(s).

**COR006 - If the existing COR needs to be changed, will that COR need to approve the COR change?**

Once the existing COR is changed on the DUA, the new COR will receive the update to approve. After the DUA update is approved by the new COR, it will then go to the DUA Management Team (DMT) for certification.
COR007 - Does the COR receive notifications from EPPE about DUA Change Contact requests?
The COR will receive a notification if a Change Contact Request lists them as the COR on the DUA.

Back To Top

REQ001 - As a Requester on a CMS DUA, why am I unable to request or assign certain DUAs through the Change Contact function?
For a Requester from a CMS contractor to work with a DUA, the COR listed on the DUA needs to be active in the EPPE application. If the COR listed on the DUA does not have a role in EPPE yet, the application will display a message informing you that the COR is not registered. Please reach out to the COR and encourage them to register in the EPPE application. Once the COR is in the system, you will be able to request or assign the DUA through the Change Contact function.

Back To Top

REQ002 - How can the DUA Requester update the COR on a Contractor DUA?
The DUA Requester can update the COR on any Contractor DUA through the Update/Amend action.

Back To Top

REQ003 - What would happen with the DUA if both the DUA Requester and COR are no longer active?
If there is no one to register in EIDM to request the role as the DUA Requester, a point of contact from the DUA's organization would need to email the DUA Management Team (DMT) at datauseagreement@cms.hhs.gov for assistance.

Back To Top

REQ004 - Should the DUA Requester create a DUA for each year of a contract Period of Performance (PoP)?
The DUA Requester should create a single DUA for the entire contract Period of Performance (POP). The DUA will need to be extended every year within the contract period.

Back To Top

REQ005 - Once a DUA is submitted, does it go to the COR for approval?
Yes, when the DUA is submitted by the DUA Requester, it is then waiting for the COR that is listed on the DUA to approve it. The COR will receive an email notification for pending DUA action(s).
REQ006 - Will there be any email notifications when a DUA is expiring?
Yes, the COR, DUA Requester and Custodians will receive an email notification. Email notifications are sent at 60 days, 30 days, 15 days and everyday thereafter until the DUA is either extended or closed.

REQ007 - At the Proxy end date, will the COR or DUA Requester need to go in and end the Proxy assignment or will the system automatically end the assignment?
The system will automatically end the COR or Requester Proxy assignment at the end of the specified end date.

REQ008 - When will OEDA stop accepting paper DUA forms?
OEDA will no longer accept DUA forms for Contractor DUAs through the datauseagreement@cms.hhs.gov mailbox after April 15, 2019. You can still submit paper DUA forms and updates for Limited Data Sets and Research DUAs via the mailbox (DataUseAgreement@cms.hhs.gov).

REQ009 - Do you have to be a DUA Requester to be designated as a Proxy?
Yes, you must be registered as a DUA Requester before you can be selected by another DUA Requester as a DUA Requester Proxy.

REQ010 - How do I get a list of my DUAs?
The DUA Requester and CORs can use the DUA Search function to review/export a list of your DUAs to Excel.

REQ011 - When would the DUA Requester use the Ad Hoc Request?
A DUA Requester would utilize the Ad Hoc Request function if they are requesting assignment of a DUA from an outside organization. If the DUA Requester is associated with or was previously associated to another organization and does not see their DUA, they can request for the assignment of the DUA to themselves through the Ad Hoc request process, which will need EPPE Admin approval.
REQ012 - How are documents provided by the DUA Requester? Do they need to scan and send them via email?

The DUA Requesters will now have the ability to upload supporting documentation via the EPPE application. These documents are downloadable for viewing by both the COR and DUA Management Team (DMT).

Back To Top

REQ013 - If the existing COR needs to be changed, will that COR need to approve the COR change?

Once the existing COR is changed on the DUA, the new COR will receive the update to approve. After the DUA update is approved by the new COR, it will then go to the DUA Management Team (DMT) for certification.

Back To Top

REQ014 - What is the guidance on adding sub-contractors to the DUA?

If the contract holder is working with any sub-contractors, then the sub-contracting organizations should be listed on the DUA. If individuals from the sub-contracting organizations will be receiving data directly from CMS or accessing data through a CMS system, then they should also be listed as custodians on the DUA.

Back To Top

REQ015 - Does the CEO of a company have to be the DUA Requester on the DUA?

No. A DUA Requester is defined as “The person authorized to legally bind their organization to the terms specified in the DUA. This is a required role on the Data Use Agreement (DUA).”

Back To Top

REQ016 - What is a Data Extract System (DESY) User? Do we have to add these users?

A Data Extract System (DESY) User is not a user role within EPPE but rather users who need access to data files within the DESY data dissemination system. If a custodian will be accessing files directly through DESY, their 4 digit EUA ID will need to be provided in EPPE.

Back To Top

EXT001 - As an Extractor, how can I track partially extracted orders within EPPE?

That functionality does not currently exist in EPPE. The extractor has to manually track partial orders.
EXT002 - As an Extractor, how can I create an order?
On the extractor navigation menu, under the <Order(s)> tab, click on <Create Orders(s)> to create a new order.

EXT003 - As an Extractor, where can I view unfinished orders?
On the extractor navigation menu, under the <Order(s)> tab, click on <Unfinished Order(s)> to see unfinished orders.

EXT004 - As an Extractor, where can I view finished orders that haven't been shipped?
On the extractor navigation menu, under the <Order(s)> tab, click on <Finished Order(s)> to see orders extracted but not shipped.

EXT005 - As an Extractor, where can I view orders that have been shipped?
On the extractor navigation menu, under the <Order(s)> tab, click on <Shipped Order(s)> to see orders that have been shipped.

SHP001 - As a Shipper, where can I view orders that are ready to be shipped?
On the shipper navigation menu, under the <Shipping> tab, click <Pending Order(s)> to see orders that are waiting for processing to be shipped.

SHP002 - As a Shipper, where can I view orders that have been shipped?
On the shipper navigation menu under the <Shipping> tab click <Shipped Orders(s)> to see orders that have been shipped.

MSR001 - How do I gain access to MicroStrategy Reports within EPPE?
If you require access to custom reports created for you by the EPPE team, you will need to get the <MicroStrategy User> role in order to view them. To request access to the MicroStrategy Reports within EPPE follow the steps outlined below.

1. If you already have a User ID and password, navigate to https://portal.cms.gov
2. Log in with your User ID and password.
3. On the <My Portal> page, click on <Request/Add Apps>.
4. After the <Access Catalog> is displayed, on the right-hand side under the My Access portion you should see EPPE.
5. Click on <Add Role> within the Available Actions box under the EPPE application.
6. Provide your business contact information, if it is not already on file (EIDM will prompt you, if this is needed)
7. The “Request Additional Role In EPPE” page displays.
8. Select the <EPPE MicroStrategy User> from the Select a Role dropdown menu.
9. Enter any notes to the Approver.
10. Click <Submit>.
11. Review your request information on the review page and then submit the request.
12. EIDM provides you with a tracking number and emails you when the request has been processed.

MSR002 - When a user has multiple roles within EPPE, how does MicroStrategy know for what role you are requesting reports?
MicroStrategy is aware of the roles that are assigned to a user within EPPE, and those roles are displayed and selectable by the user within MicroStrategy.

MSR003 - In MicroStrategy, can the fields/columns on the report result screen be expanded?
In MicroStrategy, the field/column width can be adjusted by placing the cursor in between two columns. The cursor will change to arrows pointing to the left and right. Click and drag to the desired width.

MSR004 - In MicroStrategy, can filters be applied to the report result screen?
Yes, MicroStrategy allows for filters to be applied on the report result screen. Right mouse click on any column heading and select <Edit View Filter…>. Follow the instructions on the screen.

BRO001 - Which browsers are supported by the CMS Enterprise Portal?
The CMS Enterprise Portal supports the following browsers:

1. Internet Explorer
2. Mozilla Firefox
3. Chrome
4. Safari

**BRO002 - What browser mode is supported?**

There are different browser modes that can be specified by you, the user. Only the native browser mode is supported. For example, if you are using Internet Explorer 8, the supported browser mode is IE8. If you are using IE9, the supported browser mode is IE9. To find out what browser mode you are using, hit the F12 key while in IE. The top of the resulting window/panel will show the browser mode being used.

**BRO003 - What document mode is supported?**

There are different document modes that can be specified by you, the user. Only the native document mode is supported. For example, if the user is using Internet Explorer 8, the supported document mode is IE8 standards. If the user is using IE9, the supported document mode is IE9. To find out what document mode is being used, hit the F12 key while in IE. The top of the resulting window/panel will show the document mode being used.

**BRO004 - Is JavaScript required for the CMS Enterprise Portal?**

JavaScript needs to be enabled for successful use of the Enterprise Portal.

**BRO005 - How do I clear my browser's cache using Internet Explorer (IE) 9, 10, and 11?**

Sometimes it is necessary to clear your browser’s cache. The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded in case they are needed again. To clear your Internet Explorer (IE) cache:

- Select Tools on the menu bar, then select Delete browsing history (or select Tools via the Gear Icon, then Safety and Delete browsing history).
- Make sure to uncheck Preserve Favorites Web site data and check both Temporary Internet Files and Cookies then click okay.
- You will receive a confirmation at the bottom of the window once it has successfully cleared your cache and cookies.
BRO006 - How do I clear my browser’s cache using Google Chrome?
Sometimes it is necessary to clear your browser’s cache. The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded in case they are needed again. To clear your cache using Google Chrome:

- While in Google Chrome hit Ctrl+Shift+Del.
- In the Clear browsing data window select “Beginning of Time” to delete everything.
- Be sure to select “Cookies and other site and plug in data” as well as “Cached images and files.”
- Click on “Clear browsing data.”

Back To Top

BRO007 - How do I clear my browser’s cache using Mozilla Firefox?
Sometimes it is necessary to clear your browser’s cache. The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded in case they are needed again. To clear your cache using Mozilla Firefox:

- While in Mozilla Firefox hit Ctrl+Shift+Del.
- In the Clear Recent History window, select “Everything” for Time range to clear.
- Click the drop down by Details and check the boxes for Cookies and Cache.
- Click on “Clear Now”.

Back To Top

BRO008 - How do I enable pop-ups in Internet Explorer?
Sometimes it is necessary to allow certain pop-ups from an application. To allow pop-ups in Internet Explorer, follow the below steps:

- Select Tools on the menu bar (or select Tools via the Gear Icon.
- Click on “Internet Options.”
- Click on the “Privacy” tab.
- Click on “Settings” in the Pop-up Blocker section.
- Add https://portal.cms.gov to the “Address of website to allow” field.
- Click on “Add.”
- Click on “Close.”
- Click on “OK.”

Back To Top

BRO009 - How do I enable pop-ups in Google Chrome?
Sometimes it is necessary to allow certain pop-ups from an application. To allow pop-ups in Google Chrome, follow the below steps:
• Click on customize Google Chrome button (icon with three horizontal black lines).
• Click on “Settings.”
• On the very bottom of that screen, click on “Show advanced settings.”
• Under the “Privacy” title click on “Content settings.”
• Scroll to the “Pop-ups” section and click on “Manage exceptions.”
• In the “Hostname pattern” field type https://portal.cms.gov.
• Ensure that “Allow” is selected in the “Behavior” field.
• Click on “Done.”
• Click on “Done.”
• Close the “Settings” tab.

**Back To Top**

**BRO010 - How do I enable pop-ups in Mozilla Firefox?**

Sometimes it is necessary to allow certain pop-ups from an application. To allow pop-ups in Mozilla Firefox, follow the below steps:

• Click on customize Firefox button (icon with three horizontal black lines).
• Click on “Options.”
• On the left-hand side click on “Content.”
• Under the “Pop-ups” section click on “Exceptions.”
• Type https://portal.cms.gov in the “Address of website” field.
• Click on “Allow”.
• Click on “Save Changes.”
• Close the “Options” tab.

**Back To Top**

**ERR001 - What do I do when I receive a “Portlet not Available” error?**

When receiving the Portlet is Unavailable error, use the back button followed by the refresh button, and attempt your action again. If the error persists, clear your browser’s cache and cookies, log out and in again, and attempt your action again. If you still receive the error, please take a screenshot including the clock on the bottom right-hand side and send it to the EPPE Help Desk with detailed information as to what you were doing when the error was received.

**Back To Top**
ERR002 - What do I do when I receive a “Request Failed” error?
When receiving the Request Failed error, use the back button followed by the refresh button, and attempt your action again. If the error persists, clear your browser’s cache and cookies, log out and in again, and attempt your action again. If you still receive the error, please take a screenshot including the clock on the bottom right-hand side and send it to the EPPE Help Desk with detailed information as to what you were doing when the error was received.