

Centers for Medicare & Medicaid Services

|  |
| --- |
| **CMS Enterprise Portal Quick Reference Guide (QRG)**  **EIDM Reports Interface** |
| February 5, 2017  Version 0.2 Final |

**Table of Contents**

[1. Introduction 2](#_Toc470106365)

[2. Requesting Application Access 3](#_Toc470106366)

[3. Accessing the Reports Interface 8](#_Toc470106367)

[APPENDIX A: Report Templates 13](#_Toc470106368)

# Introduction

This guide provides an overview of the Reports Interface within Enterprise Identity Management (EIDM). This document includes step-by-step instructions for using the interface.

***Note:*** *Access to the Reports Interface is restricted to CMS EIDM Team members, Application Business Owners, designated Business Owner Representatives, and the EIDM Help Desk. If you do not have an active CMS Enterprise Portal account, refer to the EIDM QRG: ‘New Users Completing RIDP and MFA’.*

# Requesting Application Access

The Report Interface can be accessed only by users who get the required role in the EIDM Reports application. This section outlines the steps Users take to request access to the EIDM Reports application. Please follow each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 1. Go to <https://portal.cms.gov/>and select **Login to CMS Secure Portal**on the CMS Enterprise Portal.   ***Note:*** *The CMS Enterprise Portal supports the following browsers: Internet Explorer 11, Firefox, Chrome, and Safari*. | Portal Landing Page |
| 1. Read the ‘Terms and Conditions’ pageand select **I Accept**to continue. | I Accept the Terms and Conditions |
| 1. Enter your **User ID** and select **Next**. | Enter User ID |
| 1. Enter your **Password,** select an **MFA Device Type** from the drop-down, enter the **Security Code,** and select **Log In**.   ***Note****: The ‘Security Code’ for the ‘E-mail’ and ‘One-Time Security Code’ options expires after 30 minutes. The ‘Security Code’ for the other MFA device types expires after 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.*  *If you do not have access to your registered MFA device, please refer to the ‘User Login’ QRG for step-by-step instructions on how to register an MFA Device.* | Enter your Password, select an MFA device from the MFA Device Type dropdown, enter the Security Code, and select Log In. |
| 4a. If you select **Phone/Tablet/PC/ Laptop** as the ‘MFA Device Type’, enter the VIP Access software’s ‘Security Code’ as the MFA **Security Code** and select **Log In**. | VIP Access  Enter Security Code |
| 4b. If you select **Text Message – Short Message Service (SMS)**, **Interactive Voice Response (IVR)**,or **E-mail** as the **‘**MFA Device Type’,select **Send** to receive the code on the selected MFA device type.  Enter the code you receive in the **Security Code** field and select **Log In**. | Enter Security Code |
| 4c. If you select **One-Time Security Code** as the **‘**MFA Device Type’, enter the code you receive either in the e-mail sent to your registered e-mail address via the ‘Unable to Access Security Code?’ link or from your Application Help Desk in the **Security Code** field and select **Log In**. | Enter Security Code |
| 1. Select **Request Access Now** on the portal landing page. | Select Request Access Now on the portal landing page.  Arrow |
| 1. Select **Request Access** on the ***EIDM Reports*** access tile. | Select Request Access on the EIDM Reports access tile.  Arrow |
| 1. **Select the Group** for whichyou require access in order to request the corresponding roles in the **Select a Role** drop-down list. Enter your **Reason for Request**. Select **Next** to continue with your role request.   ***Cancel****: Returns you to the* ***View and Manage My Access*** *page.*  ***Note****: The role request will route per the application role approval hierarchy. Business Owner Representative routes to the corresponding Application Business Owner. CMS EIDM only and Application Business Owner route to EIDM Help Desk.* | Select the Group you require access to in order to request the corresponding roles in the Select a Role drop-down list. |
| 1. Select **Submit** to complete the role request. | Select Submit to complete the role request. |
| 1. Select **OK** to continue back to the **View and Manage My Access** view. | Select OK to continue back to the View and Manage My Access view. |

# Accessing the Reports Interface

After obtaining a role within the EIDM Reports application, users can access the EIDM Reports Interface.

To access EIDM Reports, please follow each step listed below unless otherwise noted.

| **Steps** | **Screenshots** |
| --- | --- |
| 1. Go to <https://portal.cms.gov/>and select **Login to CMS Secure Portal**on the CMS Enterprise Portal.   ***Note:*** *The CMS Enterprise Portal supports the following browsers: Internet Explorer 11, Firefox, Chrome, and Safari*. | Portal Landing Page |
| 1. Read the ‘Terms and Conditions’ pageand select **I Accept**to continue. | I Accept the Terms and Conditions |
| 1. Enter your **User ID** and select **Next**. | Enter User ID |
| 1. Enter your **Password,** select an **MFA Device Type** from the drop-down, enter the **Security Code,** and select **Log In**.   ***Note****: The ‘Security Code’ for the ‘E-mail’ and ‘One-Time Security Code’ options expires after 30 minutes. The ‘Security Code’ for the other MFA device types expires after 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.*  *If you do not have access to your registered MFA device, please refer to the ‘User Login’ QRG for step-by-step instructions on how to register an MFA Device.* | Enter your Password, select an MFA device from the MFA Device Type dropdown, enter the Security Code, and select Log In. |
| 4a. If you select **Phone/Tablet/PC/ Laptop** as the ‘MFA Device Type’, enter the VIP Access software’s ‘Security Code’ as the MFA **Security Code** and select **Log In**. | VIP Access  Enter Security Code |
| 4b. If you select **Text Message – Short Message Service (SMS)**, **Interactive Voice Response (IVR)**,or **E-mail** as the **‘**MFA Device Type’,select **Send** to receive the code on the selected MFA device type.  Enter the code you receive in the **Security Code** field and select **Log In**. | Enter Security Code |
| 4c. If you select **One-Time Security Code** as the **‘**MFA Device Type’, enter the code you receive either in the e-mail sent to your registered e-mail address via the ‘Unable to Access Security Code?’ link or from your Application Help Desk in the **Security Code** field and select **Log In**. | Enter Security Code |
| 1. Select **My Reports**in the drop down menu at the top right corner of the Welcome screen. | Select My Reports in the drop down menu at the top right corner of the Welcome screen. |
| 1. Select **Preview/Generate** on the report tile you would like to view.   ***Note****:Use the* ***Search Report*** *box to search for a report using a keyword within the report name.*  *Refer to Appendix A for additional information on report categories and reports available.* | EIDM Reports Interface |

|  |  |
| --- | --- |
| 1. Select the fields to populate the report.   ***Report Date From****: Select a date equal to the current date or prior.*  ***Report Date To****: Select a date no greater than the current date.*  ***Application****: The drop-down displays all applications granted to your role in the EIDM Reports application.*  ***Report Format****: The drop-down displays available formats of CSV, Excel, and PDF.*  ***Note****: Any fields marked with an asterisk (\*) are mandatory.* | Preview/Generate Report |
| 1. Accept the PII Acknowledgement statement and select **Generate Report**.   ***Reset****: Selecting reset will clear your report criteria.*  ***Cancel****: Ends the report generation process and returns the user to the EIDM Reports page.*  ***Note****: The acknowledgement checkbox must be selected in order to enable the* ***Generate Report*** *button.* | Accept the PII Acknowledgement statement and select Generate Report. |

# APPENDIX A: Report Templates

Below are descriptions of the report templates currently available within the Reports Interface.

***Note****: Exporting the report to Excel will provide the ability to format and filter the report information to fit your specific needs.*

|  |  |
| --- | --- |
| **EIDM Application Reports –** These reports provide high level summary counts at the application level. | |
| **Report Name** | **Report Description** |
| Application Summary Report | Use this report to review the user base for your application, including cumulative user count for each role with registered users. The report provides Role Name, count of users for the selected date, and cumulative count of users for your application. |
| Annual Certification Summary Report | Use this report to review your application’s summarized annual certification counts. The report summarizes the counts into groups, for instance the number of users certified, revoked, or due for certification for the last 7 days, last 30 days, last quarter, next 7 days, next 30 days, or next quarter. |
| Pending Certification Report | Use this report to review a list of your application users and roles due for certification within a given time period. The report provides information including user information, Role Name, last review date, and next review date. |
| **EIDM User Reports** – These reports provide more detailed user specific information for an application. | |
| **Report Name** | **Report Description** |
| User Details Report | Use this report to review detailed user and role specific information for your application’s users. The report provides information including user information, Role Name and Attributes, Last Login, and Account Status. |
| User Role Approver Report | Use this report to review role requests for your application and corresponding details of the approvers who took an action on the requests. The report provides information including user information, Request ID, Request Status (approved/rejected), approver information and date the action took place. |
| User Annual Certification Report | Use this report to review annual certification details for application users due for certification within the next sixty (60) days. The report provides user information, Role Name and Attributes, Approver User ID, Last and Next Certification Due Dates. |
| Orphaned Organization Report | Use this report to identify any organizations without an approver for your application. The report provides Organization Name and Organization Identifier (e.g., TIN or PTAN). The User Details Report is a good follow-up report to use to identify users within a particular Orphaned Organization. |
| **EIDM Audit Reports** – These audit reports provide role request and user specific audit data for an application.  ***Note:*** *The reports can be run in sixty (60) day increments as far back as two (2) years from the current run date.* | |
| **Report Name** | **Report Description** |
| Role Request Audit Report | Use this report to review the role request history of users for your applications. The report provides information including User ID, Role Name, Request ID, Request Status, timestamp when the request was modified, and who took the action on the role request. |
| User Audit Report | Use this report to review the history of user specific information for your applications. The report provides information including User ID, Event (e.g., Password Change), who created the event, Old Value, and New Value. |
| **EIDM Aggregate Reports** - These reports provide aggregate counts for all applications integrated with EIDM. These are for users with the CMS EIDM role. | |
| **Report Name** | **Report Description** |
| EIDM User Role Report | Use this report to review the user base by application, including daily (last day prior to report run date) and cumulative count of users by role for all applications in EIDM. A total of users with no application roles and total users for all applications is provided at the end of the report. |
| MAC User Role Report | Use this report to review role details and user specific information for the MAC applications. MAC applications are FCSO, myCGS, and Novitasphere. The report provides information including user information, Role Name, other CMS roles that the user has in other applications, Role Grant Date, and Password Reset Date. |