



Centers for Medicare & Medicaid Services

# **CMS Enterprise Portal Quick Reference Guide (QRG)**

## **Help Desk Multi-Factor Authentication (MFA) Support**

---

June 8, 2016  
Version 2.1 Final

## Table of Contents

- 1. Introduction \_\_\_\_\_ 2
- 2. Step-by-Step Instructions to Unlock a Registered MFA Device \_\_\_\_\_ 3
- 3. Step-by-Step Instructions to Remove a Registered MFA Device \_\_\_\_\_ 10
- 4. Step-by-Step Instructions to Generate One-Time Security Code \_\_\_\_\_ 16

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## 1. Introduction

This guide provides step-by-step instructions on how Application Help Desks can support their users for the following Multi-Factor Authentication (MFA) related services:

- Unlock MFA device(s)
- Remove MFA device(s)
- Generate a One-Time Security Code

**Note:** This document assumes that the application user has an active CMS Enterprise Portal account, a role in <*Application Name*>, and has registered for MFA in order for the Application Help Desk to provide support.

### Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security mechanism that is implemented to verify the legitimacy of a person or transaction.

MFA requires you to provide more than one form of verification in order to prove your identity. MFA registration is required only once when you are requesting a role, but will be verified every time you log into the CMS Enterprise Portal.

During the MFA registration process, the CMS Enterprise Portal requires registration of a phone, computer, or e-mail to add an additional level of security to a user's account.

You may select from the following options to complete the registration process:

- **Smart Phone:** Download Validation and Identity Protection (VIP) access software on your smart phone/tablet. You must enter the alphanumeric credential ID that is generated by the VIP access client. You will then enter the Security Code generated by the VIP client.
- **Computer:** Download VIP access software on your computer. You must enter the alphanumeric credential ID generated by the VIP access client. You will enter the Security Code generated by the VIP client.
- **E-mail:** Select the e-mail option to receive an e-mail containing a Security Code required at login. You must provide a valid, accessible e-mail address.
- **Short Message Service (SMS):** Use the SMS option to have your Security Code texted to your phone. You must enter a valid phone number. The phone must be capable of receiving text messages. Carrier charges may apply.
- **Interactive Voice Response (IVR):** Select the IVR option to receive a voice message containing your Security Code. You must provide a valid phone number and (optional) phone extension.

For registering MFA devices, refer to the following EIDM Quick Reference Guides:

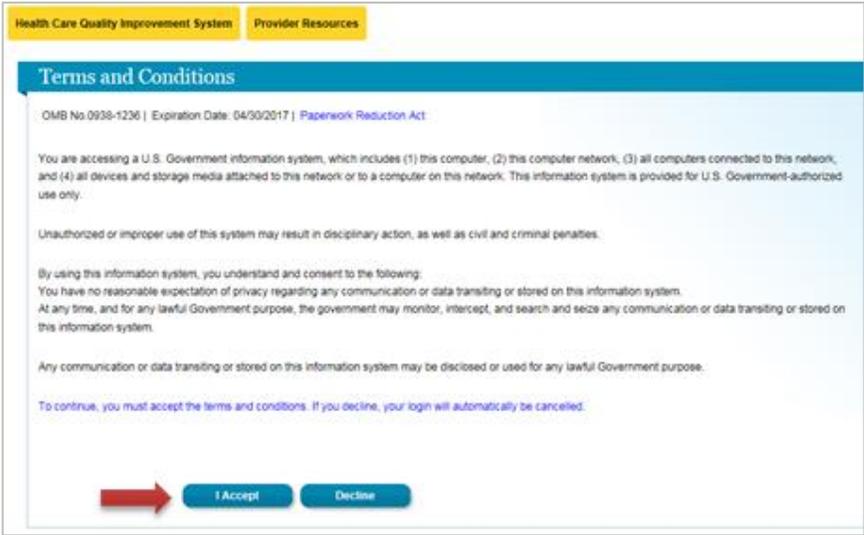
- EIDM QRG – Users Adding MFA to Application Role
- EIDM QRG – User Login

For accessing the 'User Details' page, refer to the following EIDM Quick Reference Guides:

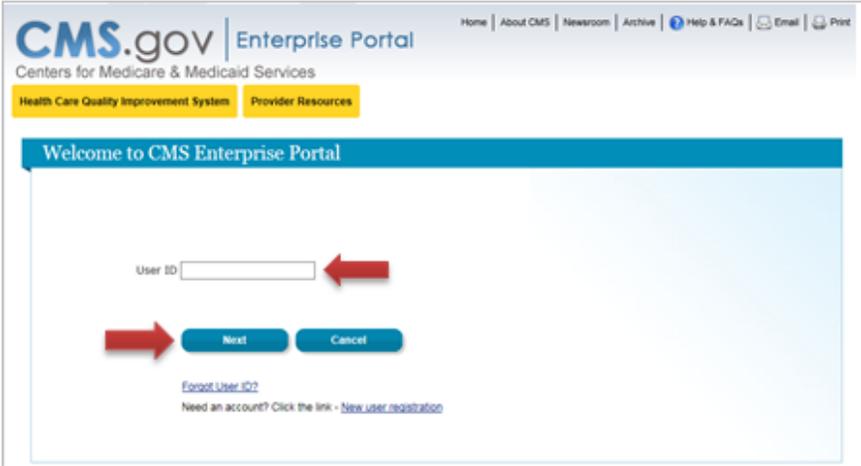
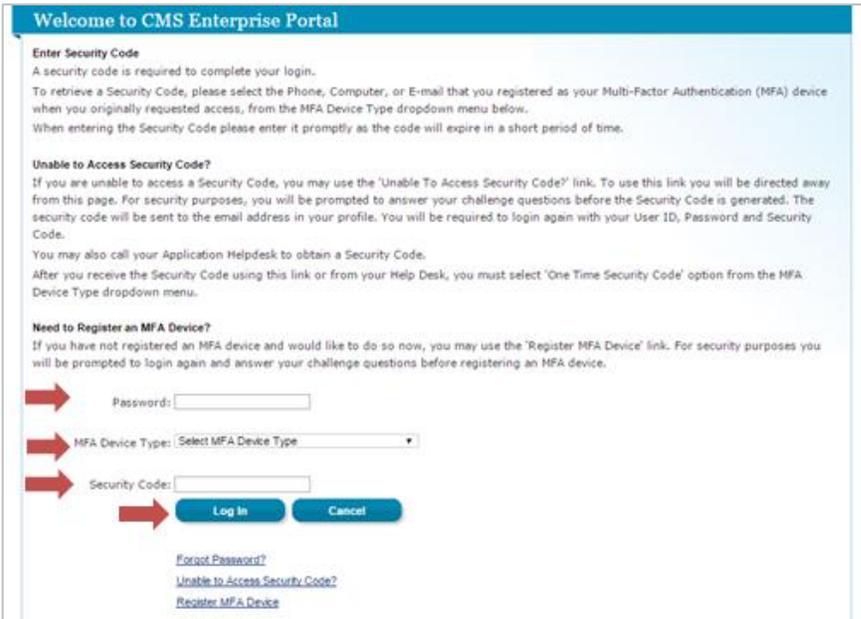
- EIDM QRG – Help Desk Manual LOA Updates

## 2. Step-by-Step Instructions to Unlock a Registered MFA Device

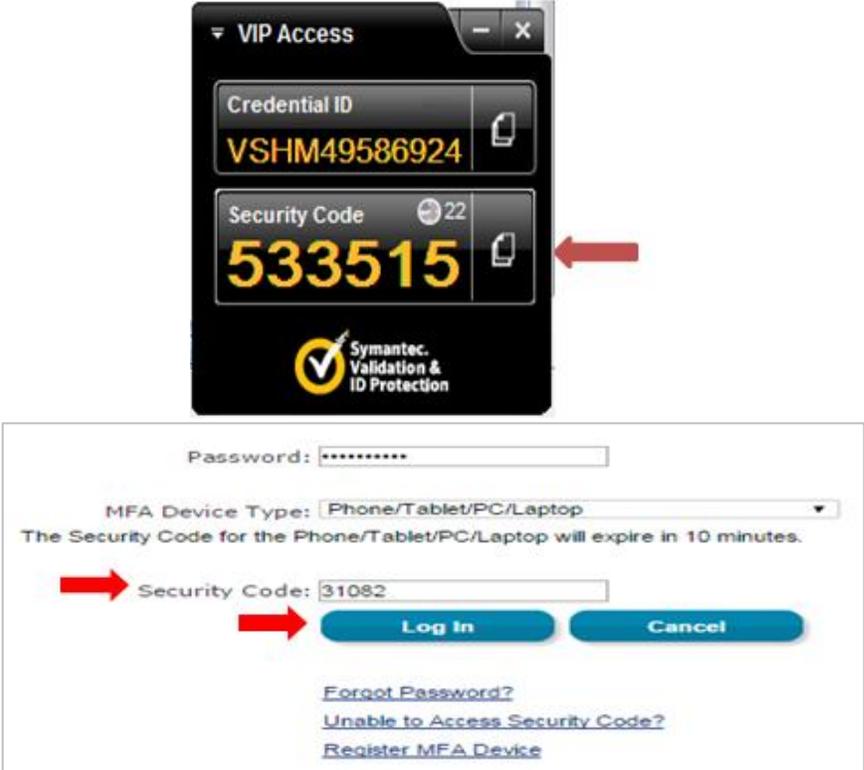
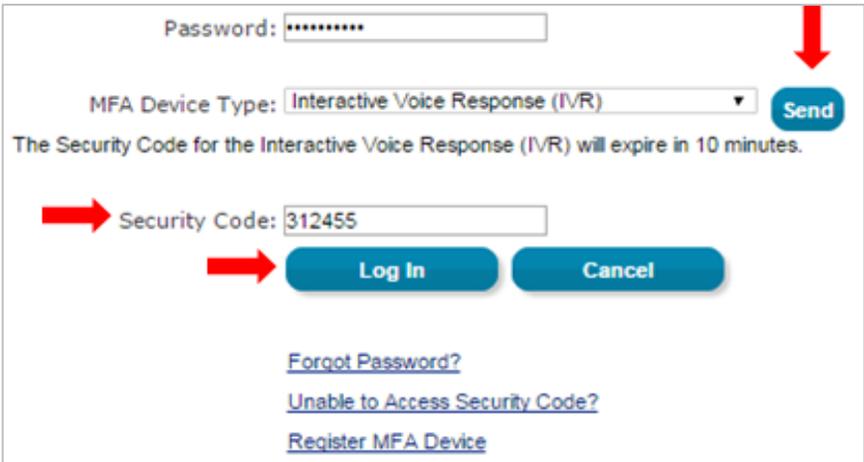
This section outlines the steps Application Help Desk Users, Application Approvers, and EIDM Help Desk Users take to unlock a registered phone, computer, or e-mail address. Please follow each step listed below unless otherwise noted.

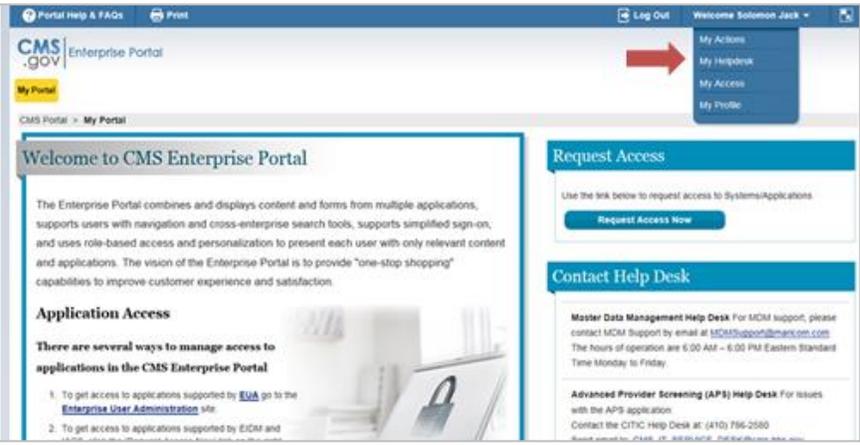
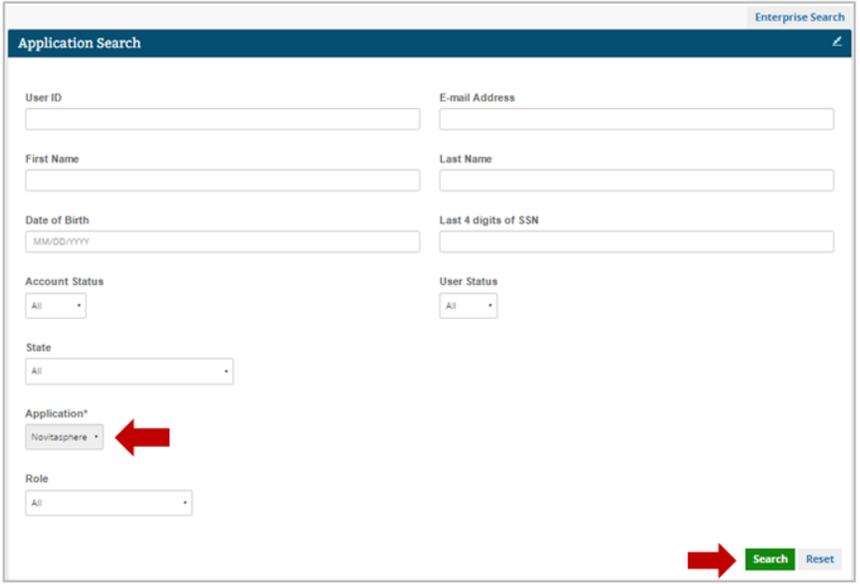
Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following browsers: Internet Explorer 8, 9, 10, and 11, Firefox, Chrome, and Safari.</i></p>	
<p>2. Read the 'Terms and Conditions' page and select <b>I Accept</b> to continue.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

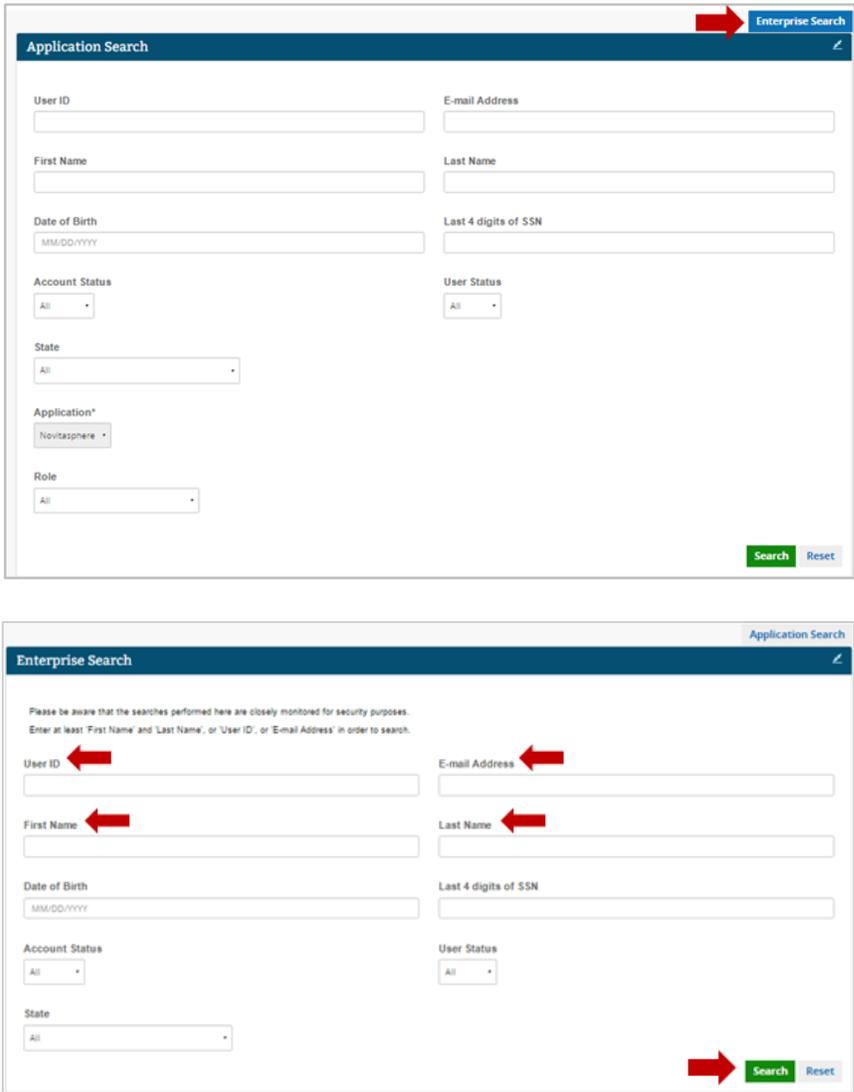
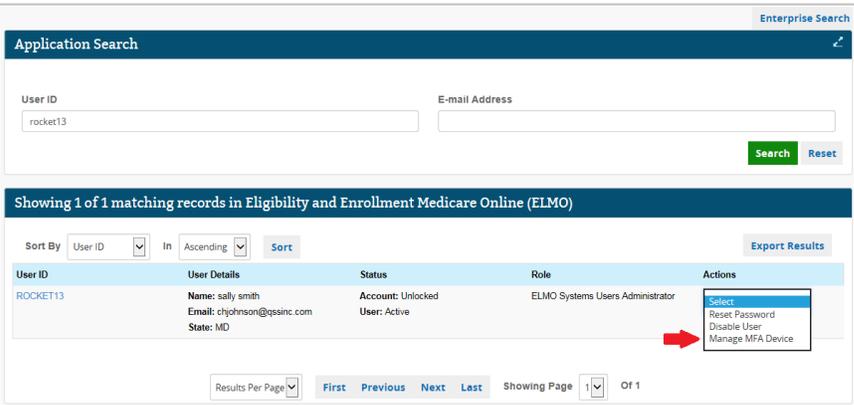
Steps	Screenshots
<p>3. Enter your <b>User ID</b> and select <b>Next</b>.</p>	
<p>4. Enter your <b>Password</b>, select an <b>MFA Device Type</b> from the drop-down, enter the <b>Security Code</b>, and select <b>Log In</b>.</p> <p><i>Note: The 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expires in 30 minutes. The 'Security Code' for the other MFA device types expires in 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.</i></p> <p><i>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.</i></p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

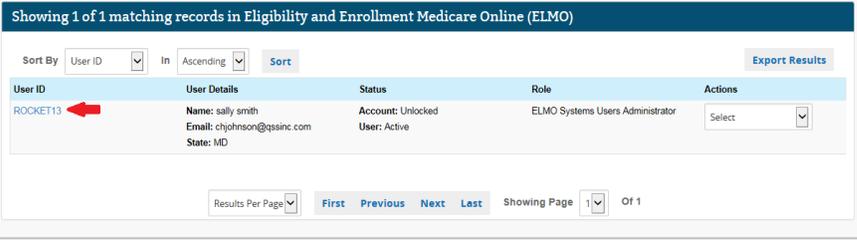
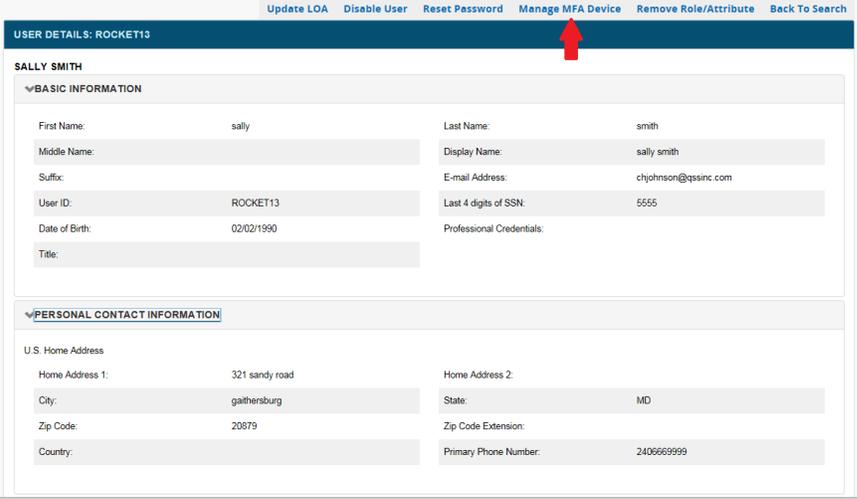
Steps	Screenshots
<p>4a. If you select <b>Phone/Tablet/PC/Laptop</b> as the 'MFA Device Type', enter the VIP Access software's 'Security Code' as the MFA <b>Security Code</b> and select <b>Log In</b>.</p>	
<p>4b. If you select <b>Text Message – Short Message Service (SMS), Interactive Voice Response (IVR), or E-mail</b> as the 'MFA Device Type', select <b>Send</b> to receive the code on the selected MFA device type.</p> <p>Enter the code in the <b>Security Code</b> field and select <b>Log In</b>.</p>	

Steps	Screenshots
<p>4c. If you select <b>One-Time Security Code</b> 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 <b>Security Code</b> field and select <b>Log In</b>.</p>	
<p>5. Locate the ‘Welcome &lt;First&gt; &lt;Last&gt;’ drop-down list in the top-right corner of the page and select <b>My Helpdesk</b>.</p>	
<p>6. Enter the user’s details on the ‘Application Search’ page and select <b>Search</b>.</p> <p><i>Note: Use this to search and manage user accounts under your authority. You must select at least the <b>Application</b> to perform a search. Only the first 1,000 results will display.</i></p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

Steps	Screenshots
<p>6a. If you are unable to locate a user in ‘Application Search’, you can select ‘Enterprise Search’, enter the user’s details, and select <b>Search</b>.</p> <p><i>Note: Use this to search and manage user accounts in the CMS Enterprise Portal. This search option is intended for helping users who may have called the wrong Help Desk or may not have an application role, etc. You must enter at least the <b>User ID</b> (or) <b>E-mail Address</b> (or) a combination of <b>First Name</b> (and) <b>Last Name</b> to perform a search. The results will only display if 10 or fewer results match the criteria.</i></p>	
<p>7. Select <b>Manage MFA Device</b> from the ‘Actions’ drop-down list.</p> <p><i>Note: The option to select ‘Manage MFA Device’ is also available on the ‘User Details’ page.</i></p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

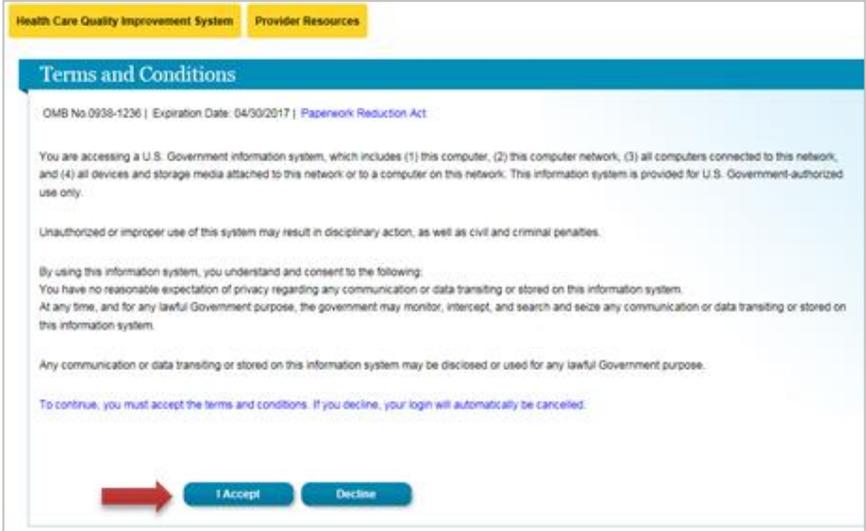
Steps	Screenshots																																								
<p>7a. Select the <b>User ID</b> to go to the ‘User Details’ page.</p>	 <p>Showing 1 of 1 matching records in Eligibility and Enrollment Medicare Online (ELMO)</p> <p>Sort By: User ID In: Ascending Sort Export Results</p> <table border="1"> <thead> <tr> <th>User ID</th> <th>User Details</th> <th>Status</th> <th>Role</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>ROCKET13</td> <td>Name: sally smith Email: chjohnson@qpsinc.com State: MD</td> <td>Account: Unlocked User: Active</td> <td>ELMO Systems Users Administrator</td> <td>Select</td> </tr> </tbody> </table> <p>Results Per Page: First Previous Next Last Showing Page 1 Of 1</p>	User ID	User Details	Status	Role	Actions	ROCKET13	Name: sally smith Email: chjohnson@qpsinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select																														
User ID	User Details	Status	Role	Actions																																					
ROCKET13	Name: sally smith Email: chjohnson@qpsinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select																																					
<p>7b. Select <b>Manage MFA Device</b>.</p>	 <p>Update LOA Disable User Reset Password Manage MFA Device Remove Role/Attribute Back To Search</p> <p>USER DETAILS: ROCKET13</p> <p>SALLY SMITH</p> <p>BASIC INFORMATION</p> <table border="1"> <tr> <td>First Name:</td> <td>sally</td> <td>Last Name:</td> <td>smith</td> </tr> <tr> <td>Middle Name:</td> <td></td> <td>Display Name:</td> <td>sally smith</td> </tr> <tr> <td>Suffix:</td> <td></td> <td>E-mail Address:</td> <td>chjohnson@qpsinc.com</td> </tr> <tr> <td>User ID:</td> <td>ROCKET13</td> <td>Last 4 digits of SSN:</td> <td>5555</td> </tr> <tr> <td>Date of Birth:</td> <td>02/02/1990</td> <td>Professional Credentials:</td> <td></td> </tr> <tr> <td>Title:</td> <td></td> <td></td> <td></td> </tr> </table> <p>PERSONAL CONTACT INFORMATION</p> <p>U.S. Home Address</p> <table border="1"> <tr> <td>Home Address 1:</td> <td>321 sandy road</td> <td>Home Address 2:</td> <td></td> </tr> <tr> <td>City:</td> <td>gaithersburg</td> <td>State:</td> <td>MD</td> </tr> <tr> <td>Zip Code:</td> <td>20879</td> <td>Zip Code Extension:</td> <td></td> </tr> <tr> <td>Country:</td> <td></td> <td>Primary Phone Number:</td> <td>2406669999</td> </tr> </table>	First Name:	sally	Last Name:	smith	Middle Name:		Display Name:	sally smith	Suffix:		E-mail Address:	chjohnson@qpsinc.com	User ID:	ROCKET13	Last 4 digits of SSN:	5555	Date of Birth:	02/02/1990	Professional Credentials:		Title:				Home Address 1:	321 sandy road	Home Address 2:		City:	gaithersburg	State:	MD	Zip Code:	20879	Zip Code Extension:		Country:		Primary Phone Number:	2406669999
First Name:	sally	Last Name:	smith																																						
Middle Name:		Display Name:	sally smith																																						
Suffix:		E-mail Address:	chjohnson@qpsinc.com																																						
User ID:	ROCKET13	Last 4 digits of SSN:	5555																																						
Date of Birth:	02/02/1990	Professional Credentials:																																							
Title:																																									
Home Address 1:	321 sandy road	Home Address 2:																																							
City:	gaithersburg	State:	MD																																						
Zip Code:	20879	Zip Code Extension:																																							
Country:		Primary Phone Number:	2406669999																																						
<p>8. Select the checkbox corresponding to the locked MFA device and select <b>Unlock MFA Devices</b>.</p> <p><i>Note: The option to <b>Unlock MFA Devices</b> is enabled only if there is an MFA device for the user with the locked status.</i></p>	 <p>Manage MFA Device: PVPQRSUSER2</p> <p>MFA ID: pvpqruser2</p> <table border="1"> <thead> <tr> <th>Select All</th> <th>Credential ID/Phone Number/E-mail</th> <th>MFA Device Description</th> <th>MFA Device Type</th> <th>MFA Device Status</th> <th>Registered On</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>12034501169</td> <td>Mobile</td> <td>SMS_OTP</td> <td>LOCKED</td> <td>06/01/2016 1:00 PM</td> </tr> <tr> <td><input type="checkbox"/></td> <td>VSST38826952</td> <td>046137</td> <td>STANDARD_OTP</td> <td>ENABLED</td> <td>05/25/2016 2:49 PM</td> </tr> </tbody> </table> <p>Unlock MFA Devices Remove MFA Devices Generate Security Code Cancel</p>	Select All	Credential ID/Phone Number/E-mail	MFA Device Description	MFA Device Type	MFA Device Status	Registered On	<input checked="" type="checkbox"/>	12034501169	Mobile	SMS_OTP	LOCKED	06/01/2016 1:00 PM	<input type="checkbox"/>	VSST38826952	046137	STANDARD_OTP	ENABLED	05/25/2016 2:49 PM																						
Select All	Credential ID/Phone Number/E-mail	MFA Device Description	MFA Device Type	MFA Device Status	Registered On																																				
<input checked="" type="checkbox"/>	12034501169	Mobile	SMS_OTP	LOCKED	06/01/2016 1:00 PM																																				
<input type="checkbox"/>	VSST38826952	046137	STANDARD_OTP	ENABLED	05/25/2016 2:49 PM																																				
<p>9. Select <b>OK</b> to confirm unlocking the registered MFA device.</p> <p>OR</p> <p>Select <b>Cancel</b> to return to the ‘Manage MFA Device’ page.</p> <p><i>Note: If the selected device(s) is already in Enabled status, an error message will be displayed.</i></p>	 <p>Manage MFA Device: PVPQRSUSER2</p> <p>Are you sure you want to unlock the following MFA Device(s): Credential ID: 12034501169</p> <p>OK Cancel</p>																																								

Steps	Screenshots
10. A success message displays. Select <b>OK</b> to return to the search results.	

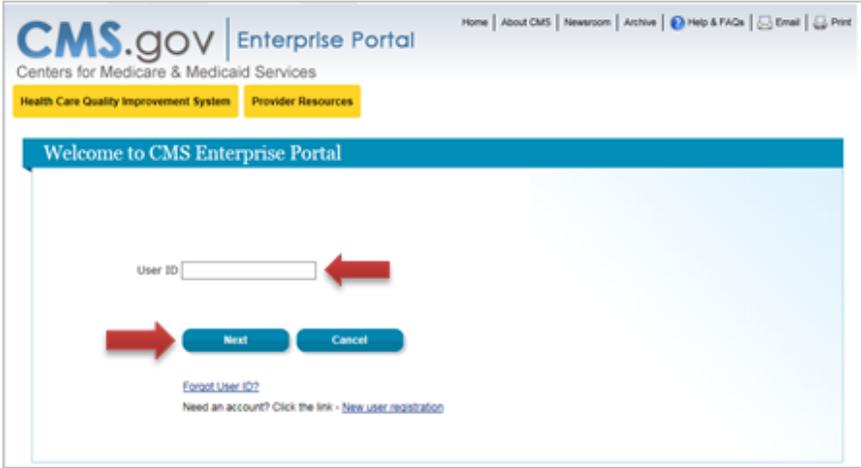
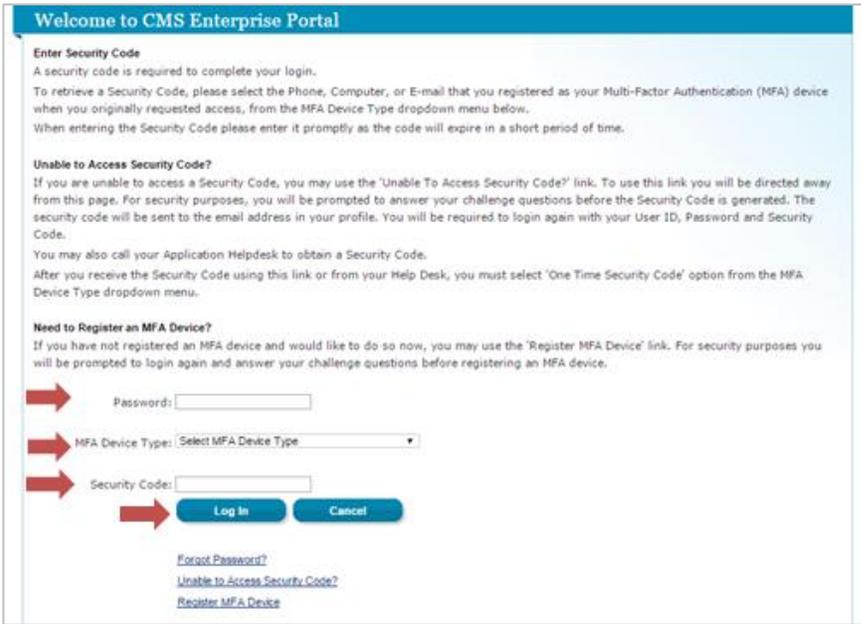
If you have questions or need assistance regarding MFA, please contact your Application Help Desk

### 3. Step-by-Step Instructions to Remove a Registered MFA Device

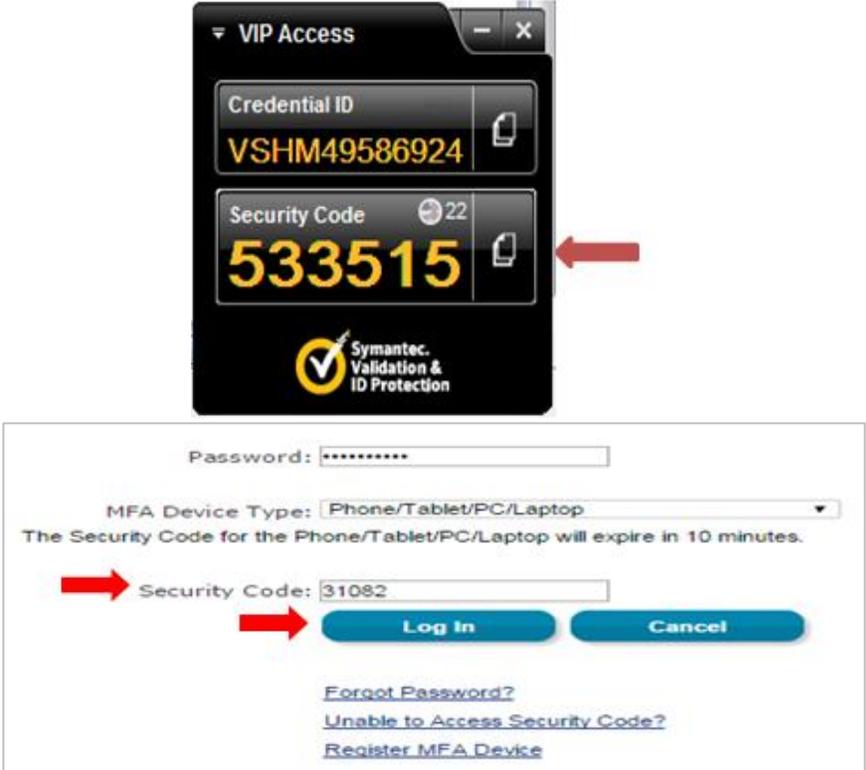
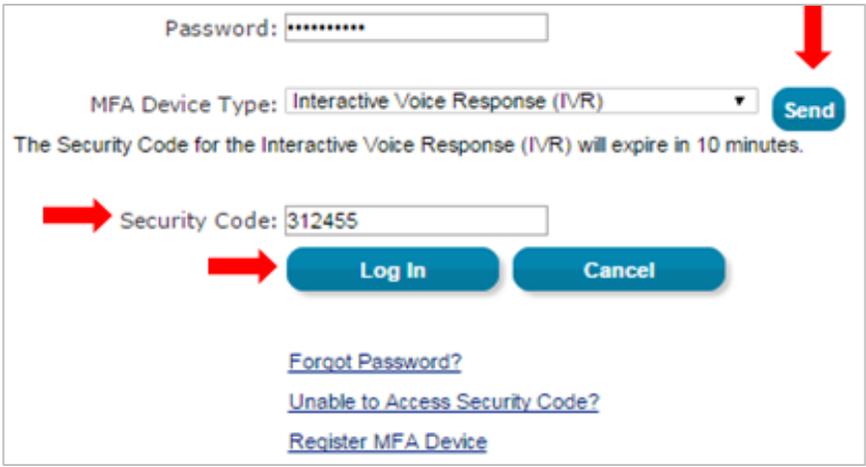
This section outlines the steps Application Help Desk Users, Application Approvers, and EIDM Help Desk Users take to unlock a registered phone, computer, or e-mail. Please follow each step listed below unless otherwise noted.

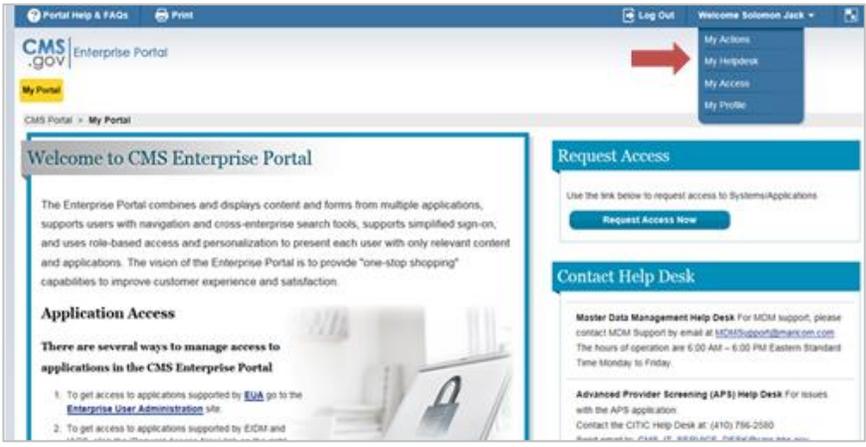
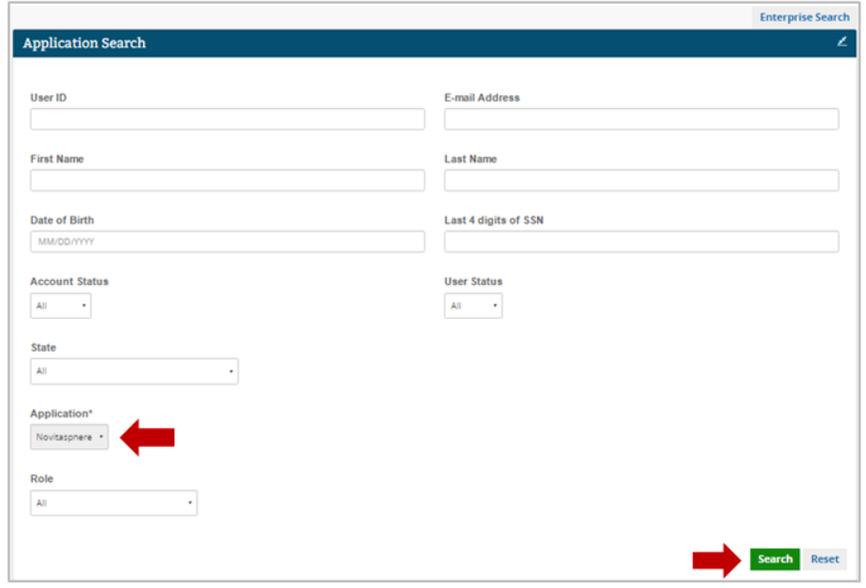
Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following browsers: Internet Explorer 8, 9, 10, and 11, Firefox, Chrome, and Safari.</i></p>	
<p>2. Read the 'Terms and Conditions' page and select <b>I Accept</b> to continue.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

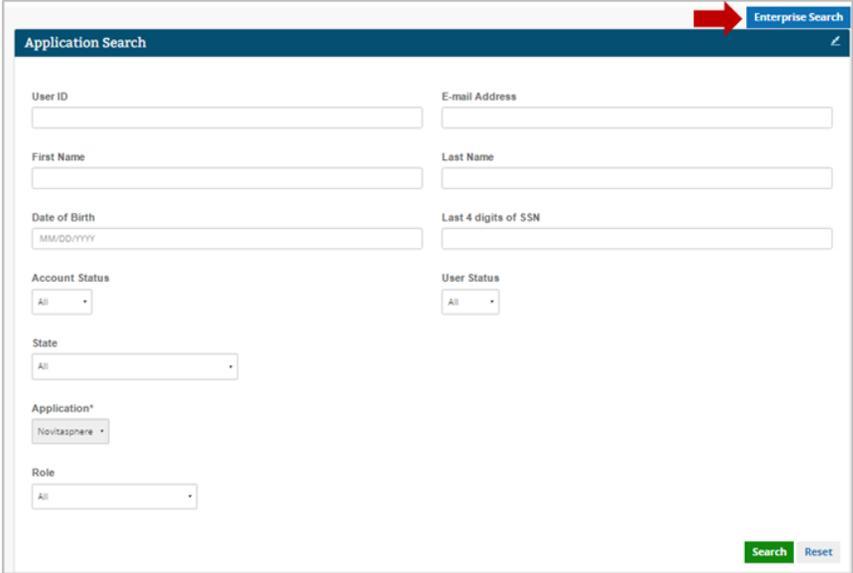
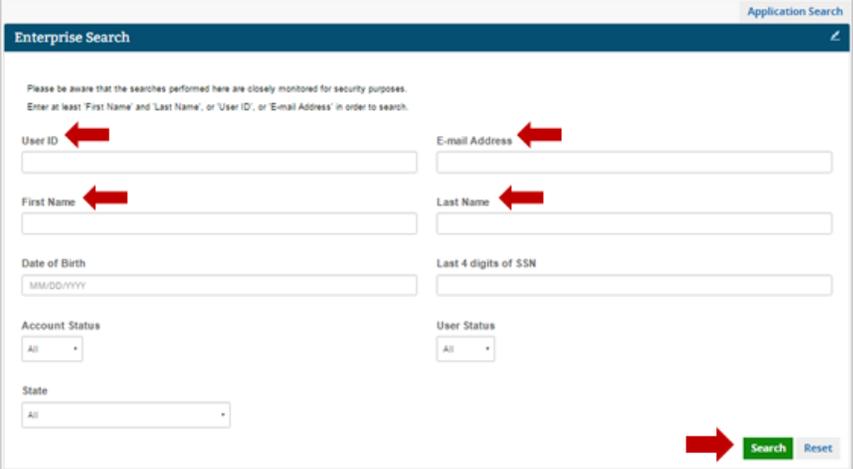
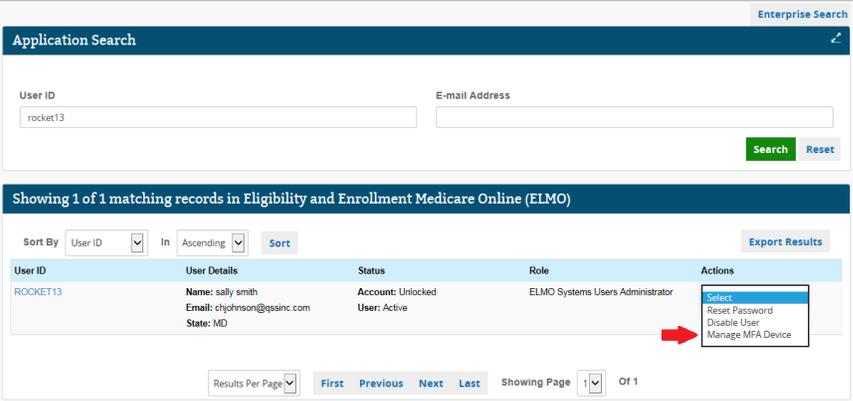
Steps	Screenshots
<p>3. Enter your <b>User ID</b> and select <b>Next</b>.</p>	
<p>4. Enter your <b>Password</b>, select an <b>MFA Device Type</b> from the drop-down list, enter the <b>Security Code</b>, and select <b>Log In</b>.</p> <p><i>Note: The 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expires in 30 minutes. The 'Security Code' for the other MFA device types expires in 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.</i></p> <p><i>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.</i></p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

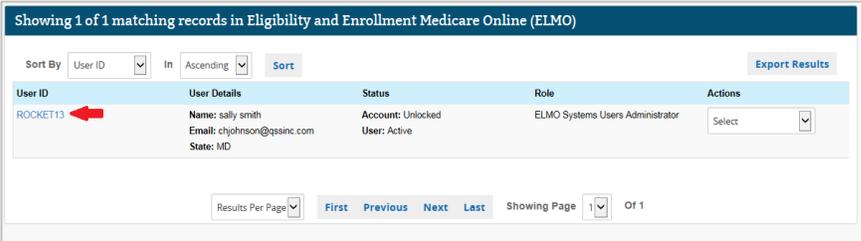
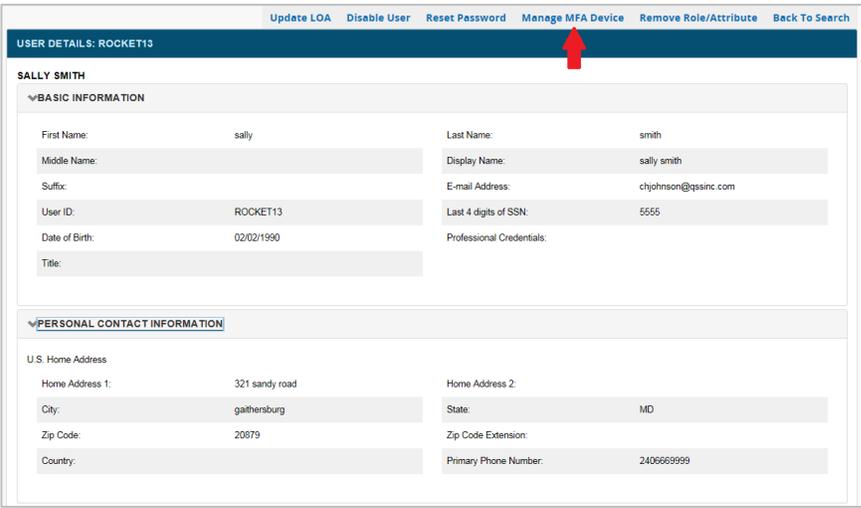
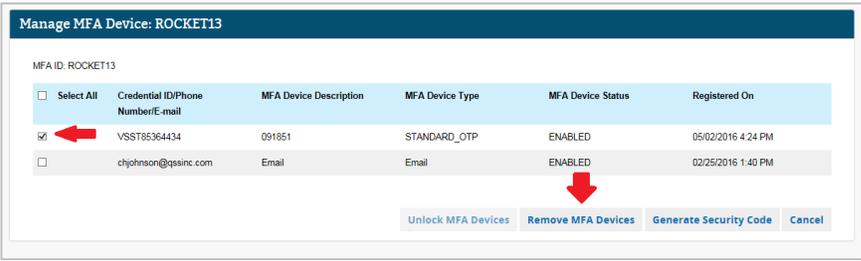
Steps	Screenshots
<p>4a. If you select <b>Phone/Tablet/PC/Laptop</b> as the 'MFA Device Type', enter the VIP Access software's 'Security Code' as the MFA <b>Security Code</b> and select <b>Log In</b>.</p>	
<p>4b. If you select <b>Text Message – Short Message Service (SMS), Interactive Voice Response (IVR), or E-mail</b> as the 'MFA Device Type', select <b>Send</b> to receive the code on the selected MFA device type.</p> <p>Enter the code in the <b>Security Code</b> field and select <b>Log In</b>.</p>	

Steps	Screenshots
<p>4c. If you select <b>One-Time Security Code</b> 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 <b>Security Code</b> field and select <b>Log In</b>.</p>	
<p>5. Locate the ‘Welcome &lt;First&gt; &lt;Last&gt;’ drop-down list in the top-right corner of the page and select <b>My Helpdesk</b>.</p>	
<p>6. Enter the user’s details on the ‘Application Search’ page and select <b>Search</b>.</p> <p><i>Note: Use this to search and manage user accounts under your authority. You must select at least the <b>Application</b> to perform a search. Only the first 1,000 results will display.</i></p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

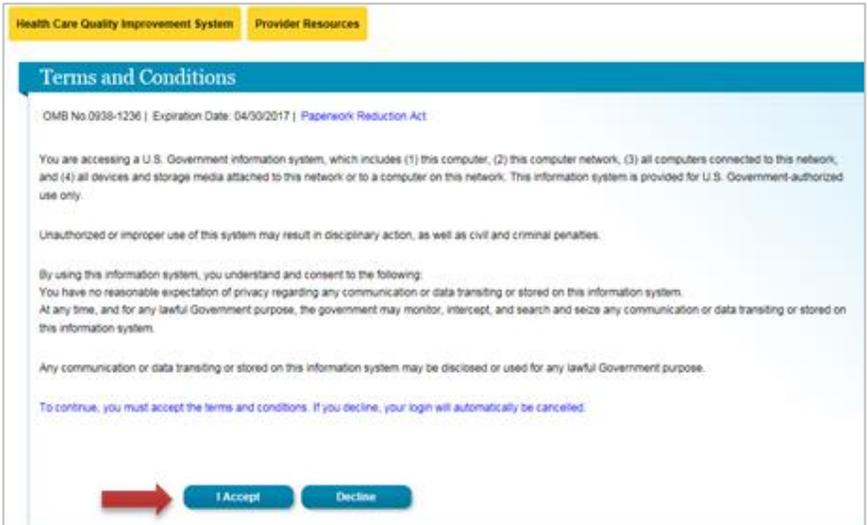
Steps	Screenshots										
<p>6a. If you are unable to locate a user in ‘Application Search’, you can select ‘Enterprise Search’, enter the user’s details, and select <b>Search</b>.</p> <p><i>Note: Use this to search and manage user accounts in the CMS Enterprise Portal. This search option is intended for helping users who may have called the wrong Help Desk or may not have an application role, etc. You must enter at least the <b>User ID</b> (or) <b>E-mail Address</b> (or) a combination of <b>First Name</b> (and) <b>Last Name</b> to perform a search. The results will only display if 10 or fewer results match the criteria.</i></p>	 <p>The screenshot shows the 'Application Search' form. A red arrow points to the 'Enterprise Search' button in the top right corner. The form includes fields for User ID, E-mail Address, First Name, Last Name, Date of Birth, Last 4 digits of SSN, Account Status, User Status, State, Application*, and Role. Search and Reset buttons are at the bottom right.</p>  <p>The screenshot shows the 'Enterprise Search' form with a warning message: 'Please be aware that the searches performed here are closely monitored for security purposes. Enter at least 'First Name' and 'Last Name', or 'User ID', or 'E-mail Address' in order to search.' Red arrows point to the User ID, E-mail Address, First Name, and Last Name fields. The Search and Reset buttons are at the bottom right.</p>										
<p>7. Select <b>Manage MFA Device</b> from the ‘Actions’ drop-down list.</p> <p><i>Note: The option to select ‘Manage MFA Device’ is also available on the ‘User Details’ page.</i></p>	 <p>The screenshot shows the search results for user 'ROCKET13'. The user details are displayed in a table. The 'Actions' column has a dropdown menu with the following options: Select, Reset Password, Disable User, and Manage MFA Device. A red arrow points to the 'Manage MFA Device' option. The table also shows the user's status as 'Active' and their role as 'ELMO Systems Users Administrator'. The search results are sorted by User ID in ascending order.</p> <table border="1"> <thead> <tr> <th>User ID</th> <th>User Details</th> <th>Status</th> <th>Role</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>ROCKET13</td> <td>Name: sally smith Email: chjohnson@gssinc.com State: MD</td> <td>Account: Unlocked User: Active</td> <td>ELMO Systems Users Administrator</td> <td>Select Reset Password Disable User Manage MFA Device</td> </tr> </tbody> </table>	User ID	User Details	Status	Role	Actions	ROCKET13	Name: sally smith Email: chjohnson@gssinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select Reset Password Disable User Manage MFA Device
User ID	User Details	Status	Role	Actions							
ROCKET13	Name: sally smith Email: chjohnson@gssinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select Reset Password Disable User Manage MFA Device							

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

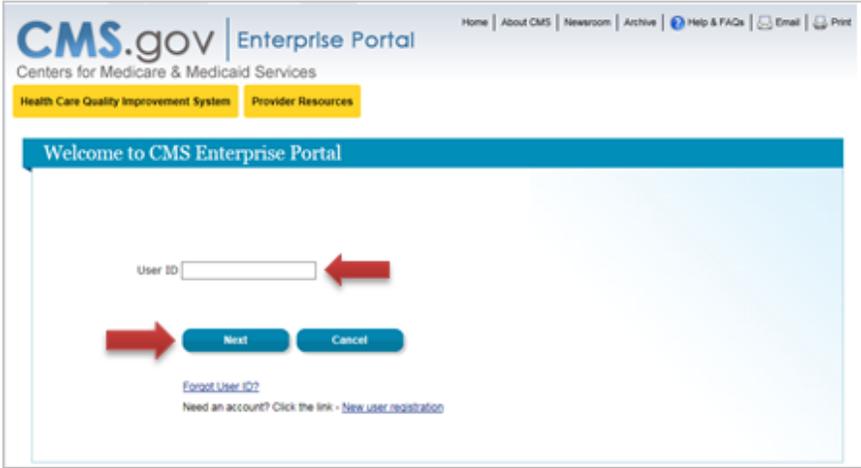
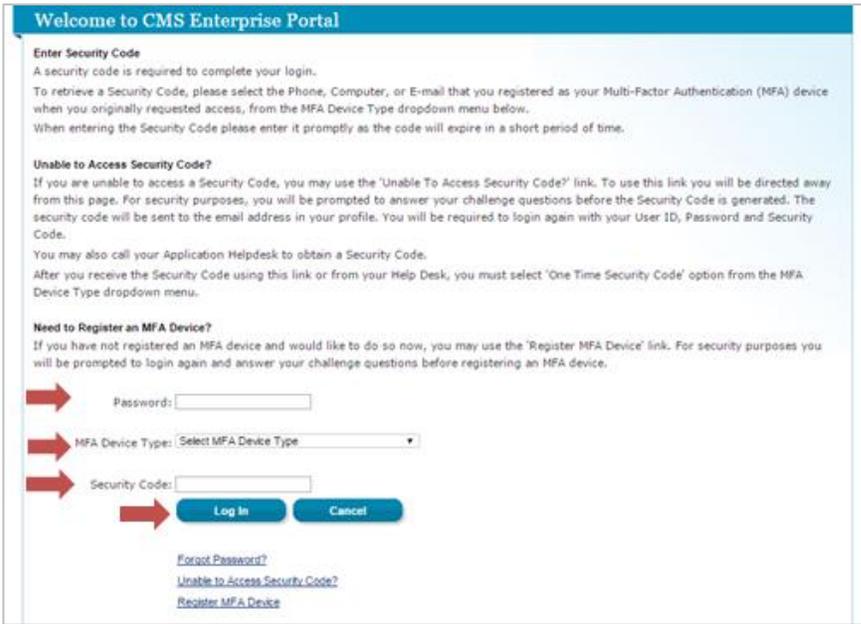
Steps	Screenshots																		
<p>7a. Select the <b>User ID</b> to go to the ‘User Details’ page.</p>	 <p>Showing 1 of 1 matching records in Eligibility and Enrollment Medicare Online (ELMO)</p> <p>Sort By: User ID In Ascending Sort Export Results</p> <table border="1"> <thead> <tr> <th>User ID</th> <th>User Details</th> <th>Status</th> <th>Role</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>ROCKET13</td> <td>Name: sally smith Email: chjohnson@qsinc.com State: MD</td> <td>Account: Unlocked User: Active</td> <td>ELMO Systems Users Administrator</td> <td>Select</td> </tr> </tbody> </table> <p>Results Per Page: First Previous Next Last Showing Page 1 Of 1</p>	User ID	User Details	Status	Role	Actions	ROCKET13	Name: sally smith Email: chjohnson@qsinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select								
User ID	User Details	Status	Role	Actions															
ROCKET13	Name: sally smith Email: chjohnson@qsinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select															
<p>7b. Select <b>Manage MFA Device</b>.</p>	 <p>Update LOA Disable User Reset Password Manage MFA Device Remove Role/Attribute Back To Search</p> <p>USER DETAILS: ROCKET13</p> <p>SALLY SMITH</p> <p>▼BASIC INFORMATION</p> <p>First Name: sally Last Name: smith Middle Name: Display Name: sally smith Suffix: E-mail Address: chjohnson@qsinc.com User ID: ROCKET13 Last 4 digits of SSN: 5555 Date of Birth: 02/02/1990 Professional Credentials: Title:</p> <p>▼PERSONAL CONTACT INFORMATION</p> <p>U.S. Home Address</p> <p>Home Address 1: 321 sandy road Home Address 2: City: gaithersburg State: MD Zip Code: 20879 Zip Code Extension: Country: Primary Phone Number: 2406669999</p>																		
<p>8. Select the checkbox corresponding to the MFA device that needs to be removed and select <b>Remove MFA Devices</b>.</p>	 <p>Manage MFA Device: ROCKET13</p> <p>MFA ID: ROCKET13</p> <table border="1"> <thead> <tr> <th>Select All</th> <th>Credential ID/Phone Number/E-mail</th> <th>MFA Device Description</th> <th>MFA Device Type</th> <th>MFA Device Status</th> <th>Registered On</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>VSST85364434</td> <td>091851</td> <td>STANDARD_OTP</td> <td>ENABLED</td> <td>05/02/2016 4:24 PM</td> </tr> <tr> <td><input type="checkbox"/></td> <td>chjohnson@qsinc.com</td> <td>Email</td> <td>Email</td> <td>ENABLED</td> <td>02/25/2016 1:40 PM</td> </tr> </tbody> </table> <p>Unlock MFA Devices Remove MFA Devices Generate Security Code Cancel</p>	Select All	Credential ID/Phone Number/E-mail	MFA Device Description	MFA Device Type	MFA Device Status	Registered On	<input checked="" type="checkbox"/>	VSST85364434	091851	STANDARD_OTP	ENABLED	05/02/2016 4:24 PM	<input type="checkbox"/>	chjohnson@qsinc.com	Email	Email	ENABLED	02/25/2016 1:40 PM
Select All	Credential ID/Phone Number/E-mail	MFA Device Description	MFA Device Type	MFA Device Status	Registered On														
<input checked="" type="checkbox"/>	VSST85364434	091851	STANDARD_OTP	ENABLED	05/02/2016 4:24 PM														
<input type="checkbox"/>	chjohnson@qsinc.com	Email	Email	ENABLED	02/25/2016 1:40 PM														
<p>9. Select <b>OK</b> to confirm removing the registered MFA device.</p> <p>OR</p> <p>Select <b>Cancel</b> to return to the ‘Manage MFA Device’ page.</p>	 <p>Manage MFA Device: ROCKET13</p> <p>MFA ID: ROCKET13</p> <p>Are you sure you want to remove the following MFA Device(s)? Once removed, the device(s) will no longer be able to receive the Security Code. Credential ID: VSST85364434</p> <p>OK Cancel</p>																		
<p>10. A success message displays. Select <b>OK</b> to return to the search results.</p>	 <p>Manage MFA Device: ROCKET13</p> <p>MFA ID: ROCKET13</p> <p>MFA device(s) has been removed successfully.</p> <p>OK</p>																		

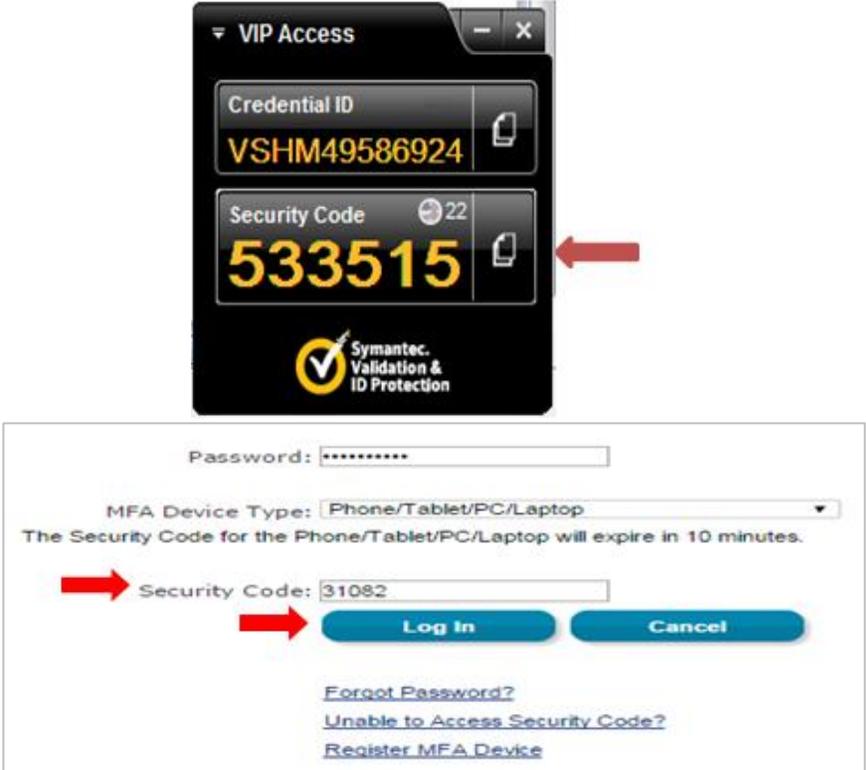
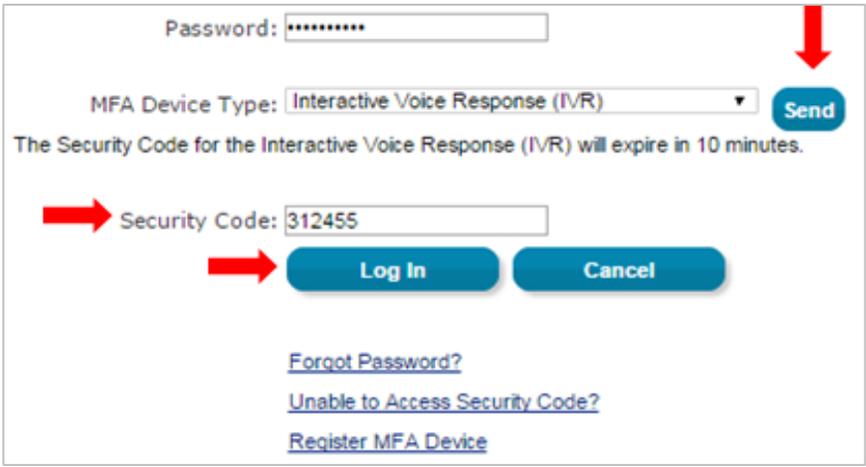
## 4. Step-by-Step Instructions to Generate One-Time Security Code

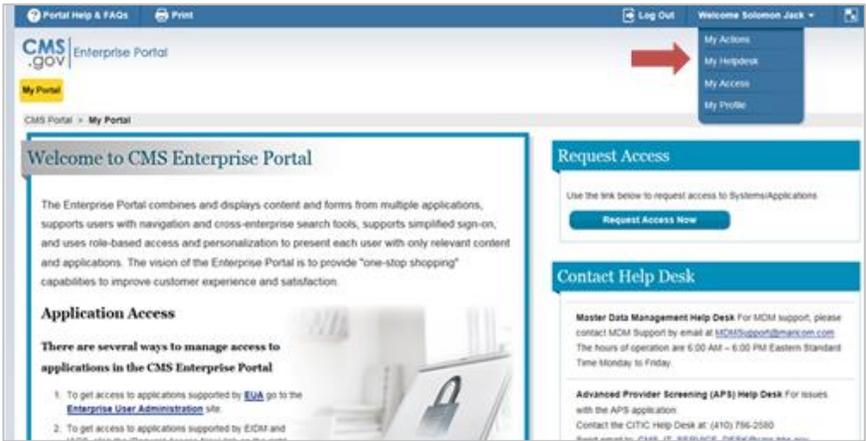
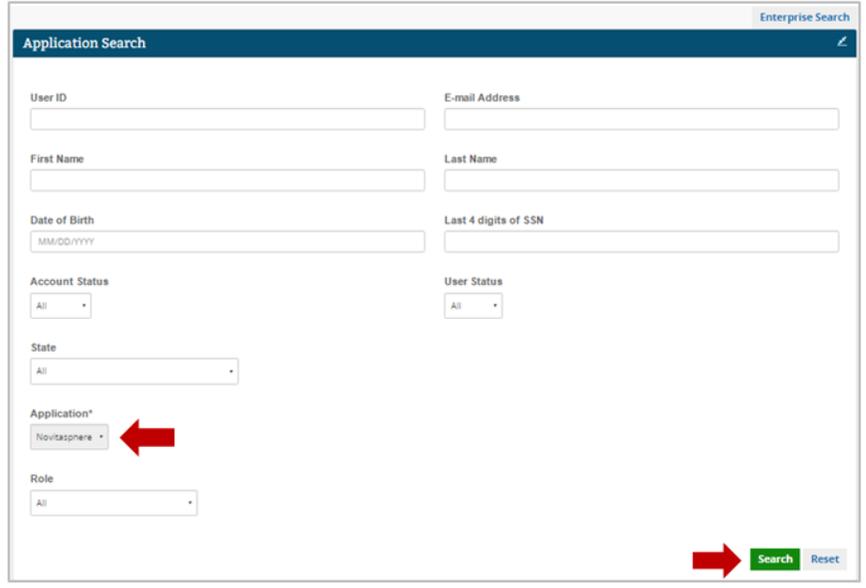
This section outlines the steps Application Help Desk Users, Application Approvers, and EIDM Help Desk Users take to generate a one-time MFA security code. Please follow each step listed below unless otherwise noted.

Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following browsers: Internet Explorer 8, 9, 10, and 11, Firefox, Chrome, and Safari.</i></p>	
<p>2. Read the 'Terms and Conditions' page and select <b>I Accept</b> to continue.</p>	

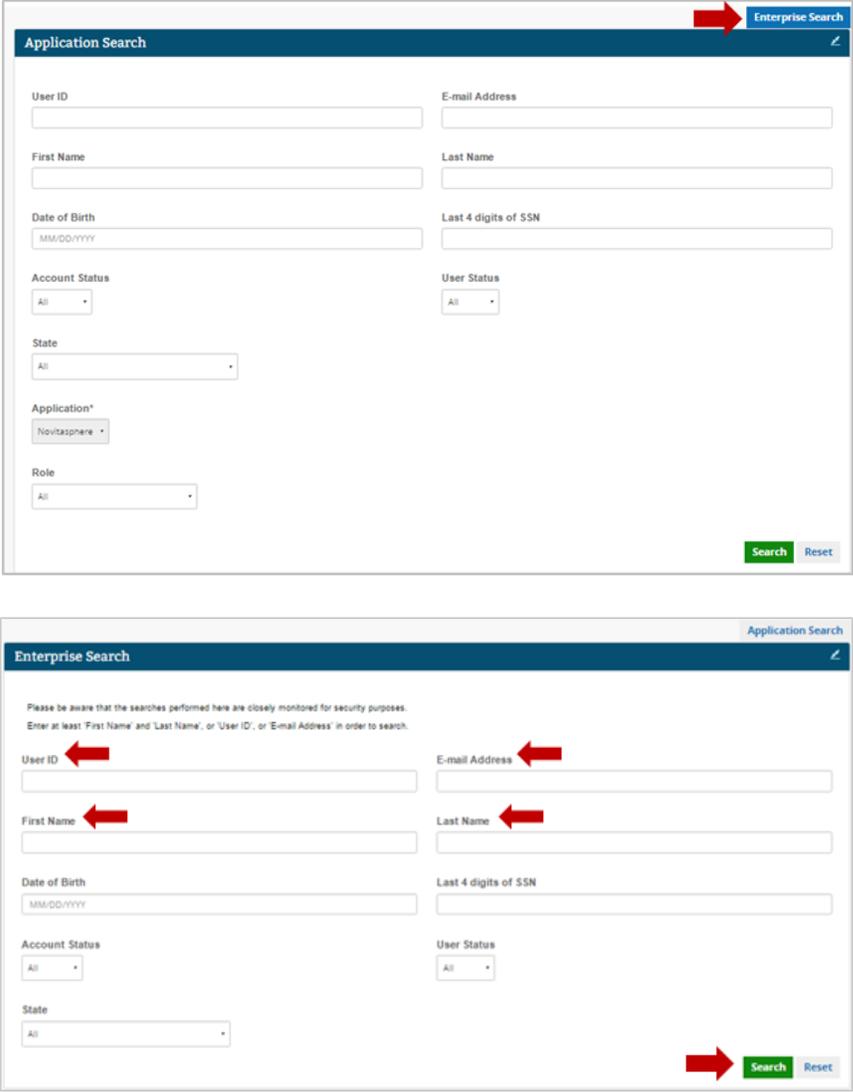
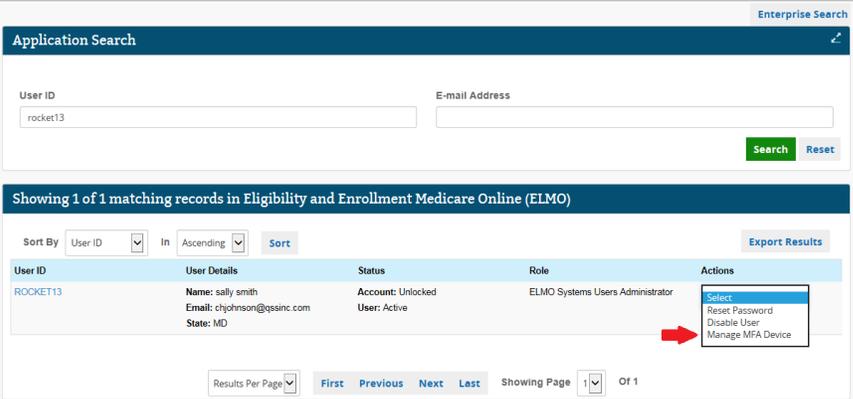
If you have questions or need assistance regarding MFA, please contact your Application Help Desk

Steps	Screenshots
<p>3. Enter your <b>User ID</b> and select <b>Next</b>.</p>	
<p>4. Enter your <b>Password</b>, select an <b>MFA Device Type</b> from the drop-down list, enter the <b>Security Code</b>, and select <b>Log In</b>.</p> <p><i>Note: The 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expires in 30 minutes. The 'Security Code' for the other MFA device types expires in 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.</i></p> <p><i>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.</i></p>	

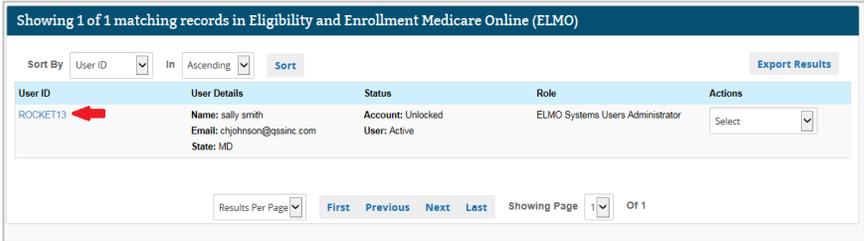
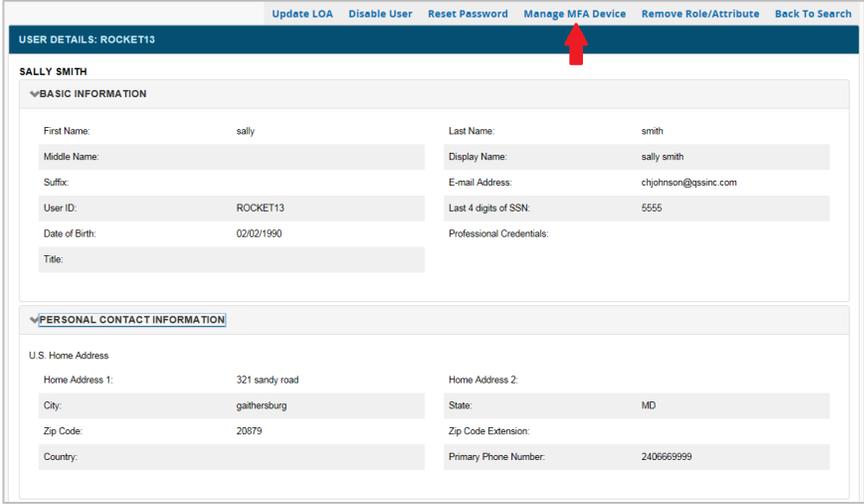
Steps	Screenshots
<p>4a. If you select <b>Phone/Tablet/PC/Laptop</b> as the ‘MFA Device Type’, enter the VIP Access software’s ‘Security Code’ as the MFA <b>Security Code</b> and select <b>Log In</b>.</p>	
<p>4b. If you select <b>Text Message – Short Message Service (SMS), Interactive Voice Response (IVR), or E-mail</b> as the ‘MFA Device Type’, select <b>Send</b> to receive the code on the selected MFA device type.</p> <p>Enter the <b>Security Code</b> and select <b>Log In</b>.</p>	

Steps	Screenshots
<p>4c. If you select <b>One-Time Security Code</b> 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 <b>Security Code</b> field and select <b>Log In</b>.</p>	
<p>5. Locate the ‘Welcome &lt;First&gt; &lt;Last&gt;’ drop-down list in the top-right corner of the page and select <b>My Helpdesk</b>.</p>	
<p>6. Enter the user’s details on the ‘Application Search’ page and select <b>Search</b>.</p> <p><i>Note: Use this to search and manage user accounts under your authority. You must select at least the <b>Application</b> to perform a search. Only the first 1,000 results will display.</i></p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

Steps	Screenshots
<p>6a. If you are unable to locate a user in ‘Application Search’, you can select ‘Enterprise Search’, enter the user’s details, and select <b>Search</b>.</p> <p><i>Note: Use this to search and manage user accounts in the CMS Enterprise Portal. This search option is intended for helping users who may have called the wrong Help Desk or may not have an application role, etc. You must enter at least the <b>User ID</b> (or) <b>E-mail Address</b> (or) a combination of <b>First Name</b> (and) <b>Last Name</b> to perform a search. The results will only display if 10 or fewer results match the criteria.</i></p>	
<p>7. Select <b>Manage MFA Device</b> from the ‘Actions’ drop-down list.</p> <p><i>Note: The option to select ‘Manage MFA Device’ is also available on the ‘User Details’ page.</i></p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

Steps	Screenshots																		
<p>7a. Select the <b>User ID</b> to go to the ‘User Details’ page.</p>	 <p>Showing 1 of 1 matching records in Eligibility and Enrollment Medicare Online (ELMO)</p> <p>Sort By: User ID In Ascending Sort Export Results</p> <table border="1"> <thead> <tr> <th>User ID</th> <th>User Details</th> <th>Status</th> <th>Role</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>ROCKET13</td> <td>Name: sally smith Email: chjohnson@qssinc.com State: MD</td> <td>Account: Unlocked User: Active</td> <td>ELMO Systems Users Administrator</td> <td>Select</td> </tr> </tbody> </table> <p>Results Per Page: First Previous Next Last Showing Page 1 Of 1</p>	User ID	User Details	Status	Role	Actions	ROCKET13	Name: sally smith Email: chjohnson@qssinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select								
User ID	User Details	Status	Role	Actions															
ROCKET13	Name: sally smith Email: chjohnson@qssinc.com State: MD	Account: Unlocked User: Active	ELMO Systems Users Administrator	Select															
<p>7b. Select <b>Manage MFA Device</b>.</p>	 <p>Update LOA Disable User Reset Password Manage MFA Device Remove Role/Attribute Back To Search</p> <p>USER DETAILS: ROCKET13</p> <p>SALLY SMITH</p> <p>▼ BASIC INFORMATION</p> <p>First Name: sally Last Name: smith Middle Name: Display Name: sally smith Suffix: E-mail Address: chjohnson@qssinc.com User ID: ROCKET13 Last 4 digits of SSN: 5555 Date of Birth: 02/02/1990 Professional Credentials: Title:</p> <p>▼ PERSONAL CONTACT INFORMATION</p> <p>U.S. Home Address</p> <p>Home Address 1: 321 sandy road Home Address 2: City: gaithersburg State: MD Zip Code: 20879 Zip Code Extension: Country: Primary Phone Number: 2406669999</p>																		
<p>8. Select <b>Generate Security Code</b>.</p> <p><i>Note: The <b>Generate Security Code</b> button will be displayed only if the user has an MFA ID. It is not required to select the checkbox corresponding to an MFA device in order to generate a Security Code.</i></p>	 <p>Manage MFA Device: ROCKET13</p> <p>MFA ID: ROCKET13</p> <table border="1"> <thead> <tr> <th>Select All</th> <th>Credential ID/Phone Number/E-mail</th> <th>MFA Device Description</th> <th>MFA Device Type</th> <th>MFA Device Status</th> <th>Registered On</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>VSS185364434</td> <td>091851</td> <td>STANDARD_OTP</td> <td>ENABLED</td> <td>05/02/2016 4:24 PM</td> </tr> <tr> <td><input type="checkbox"/></td> <td>chjohnson@qssinc.com</td> <td>Email</td> <td>Email</td> <td>ENABLED</td> <td>02/25/2016 1:40 PM</td> </tr> </tbody> </table> <p>Unlock MFA Devices Remove MFA Devices Generate Security Code Cancel</p>	Select All	Credential ID/Phone Number/E-mail	MFA Device Description	MFA Device Type	MFA Device Status	Registered On	<input type="checkbox"/>	VSS185364434	091851	STANDARD_OTP	ENABLED	05/02/2016 4:24 PM	<input type="checkbox"/>	chjohnson@qssinc.com	Email	Email	ENABLED	02/25/2016 1:40 PM
Select All	Credential ID/Phone Number/E-mail	MFA Device Description	MFA Device Type	MFA Device Status	Registered On														
<input type="checkbox"/>	VSS185364434	091851	STANDARD_OTP	ENABLED	05/02/2016 4:24 PM														
<input type="checkbox"/>	chjohnson@qssinc.com	Email	Email	ENABLED	02/25/2016 1:40 PM														
<p>9. Select a <b>Justification</b> from the drop-down list and select <b>OK</b>.</p> <p><i>Notes: The Justification values are:</i></p> <ul style="list-style-type: none"> <li><b>Unable to access device(s)</b> - Use when the user is unable to access their MFA device.</li> <li><b>No device registered</b> - Use when user does not have any registered MFA devices.</li> <li><b>Issue retrieving Security Code</b> - Use when the user is unable to retrieve the Security Code via any of the registered MFA devices.</li> </ul>	 <p>Manage MFA Device: ROCKET13</p> <p>MFA ID: ROCKET13</p> <p>Are you sure you want to generate a Security Code for this user? User ID: ROCKET13</p> <p>Justification* Select</p> <p>OK Cancel</p>																		

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

Steps	Screenshots
<p>10. Select the <b>Security Code Provided to User by Phone</b> checkbox if you gave the user the code over the phone and select <b>OK</b> to return to the search results page.</p>	