



Centers for Medicare & Medicaid Services

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

## **Help Desk Manual Level of Assurance (LOA) Updates**

---

June 8, 2016  
Version 1.0 Final

## Table of Contents

1. Introduction	2
2. Step by Step Instructions to Manually Update an Application User's LOA	3

## 1. Introduction

The CMS Enterprise Portal provides three methods, in succession, of determining identity:

1. The first method is online Remote Identity Proofing (RIDP) using Experian's Identity Verification service.
2. If a user fails RIDP, then the second method is Experian Phone Proofing.
3. If a user subsequently fails Phone Proofing, they may go through a documented Manual Identity Proofing (IDP) procedure to update their Level of Assurance (LOA). Manual IDP by the Application Help Desk is, thus, the last resort for identity proofing after a user has failed RIDP and Phone Proofing.

This document provides step-by-step instructions for Application Help Desk users to manually update the LOA of a user's identity after the user has successfully passed the Application's Manual IDP procedure. This document does not specify the content of a Manual IDP procedure.

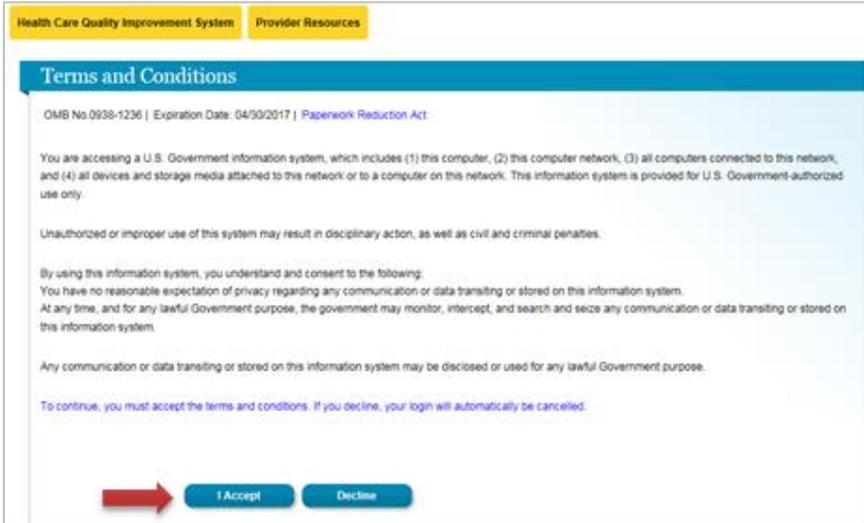
The Help Desk interface is accessed by logging into the CMS Enterprise Portal and is used for all Help Desk functions, including resetting passwords, unlocking accounts, and disabling users.

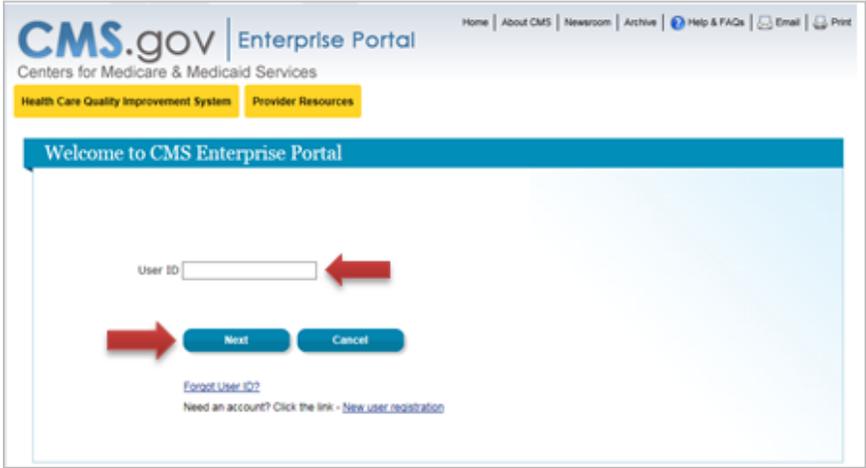
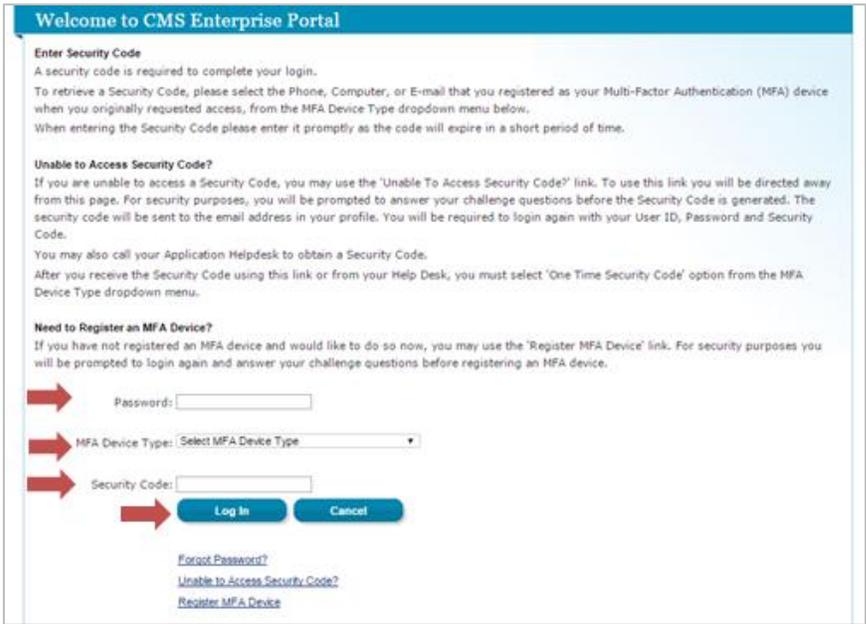
**Note:** The steps for registering for a CMS Enterprise Portal account and adding a Help Desk role can be found in the 'CMS EIDM User Guide'. This document is located on the Frequently Asked Questions (FAQ) page before logging into the CMS Enterprise Portal.

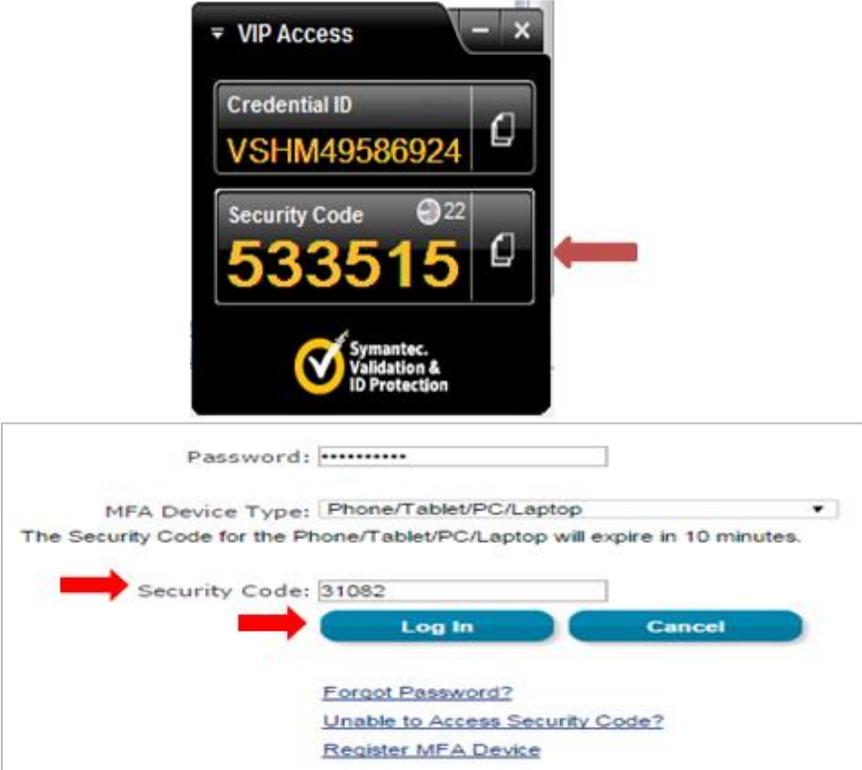
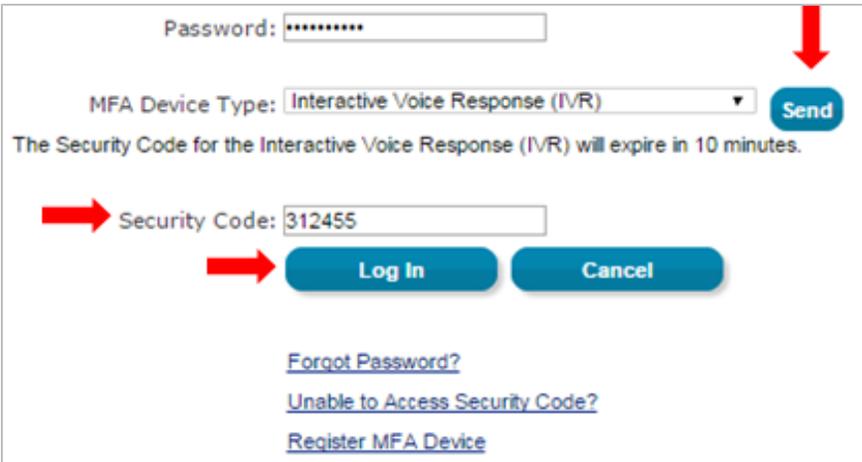
## 2. Step by Step Instructions to Manually Update an Application User's LOA

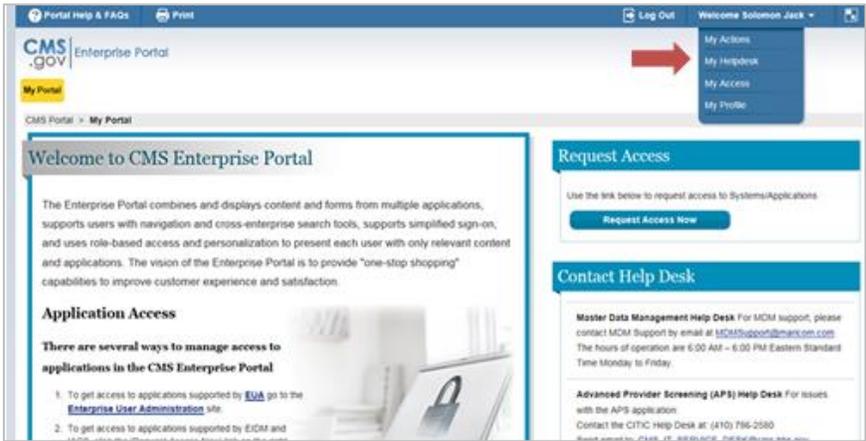
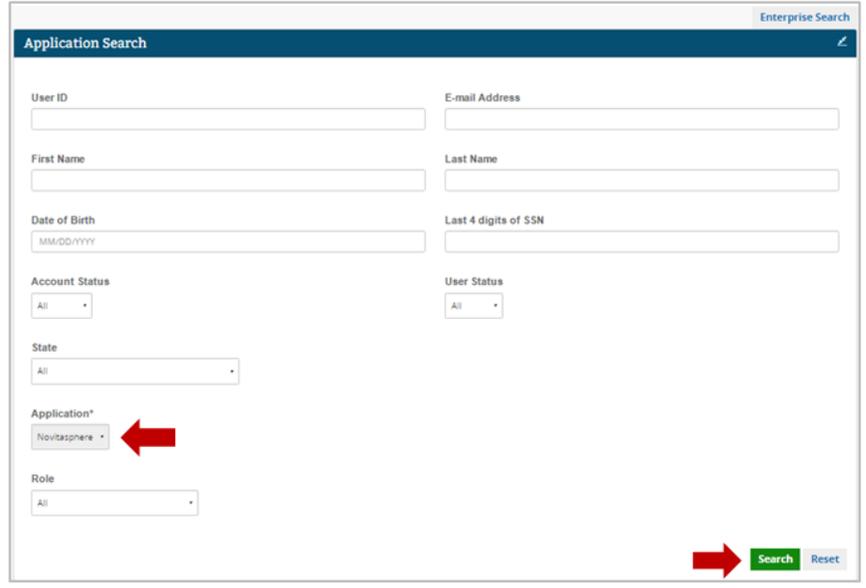
This section outlines the steps Application Help Desk Users follow to update a user's LOA. Please follow each step listed below unless otherwise noted.

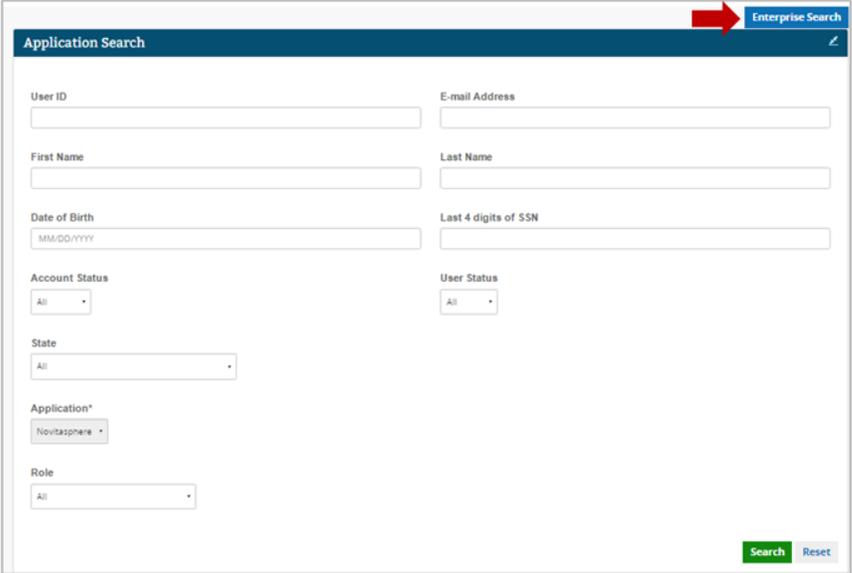
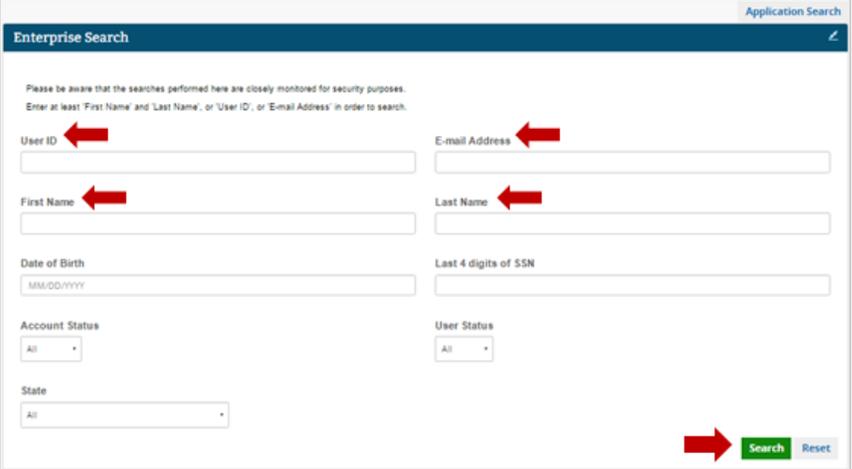
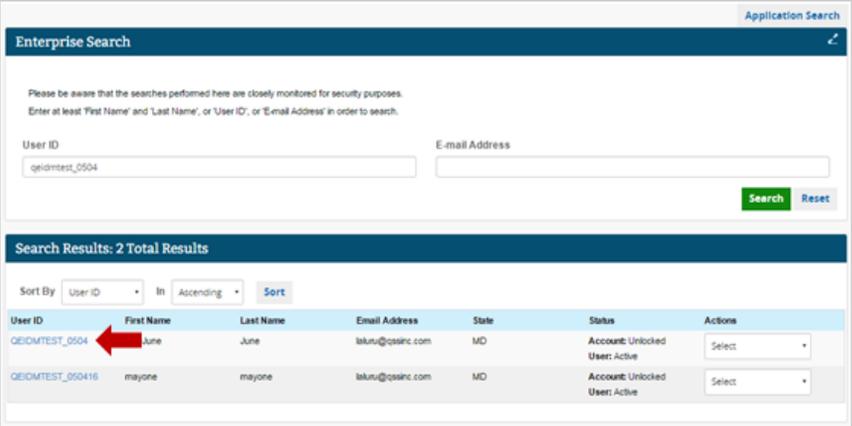
**\*\*\*To be performed only after the CMS-approved vetting process has been completed.\*\*\***

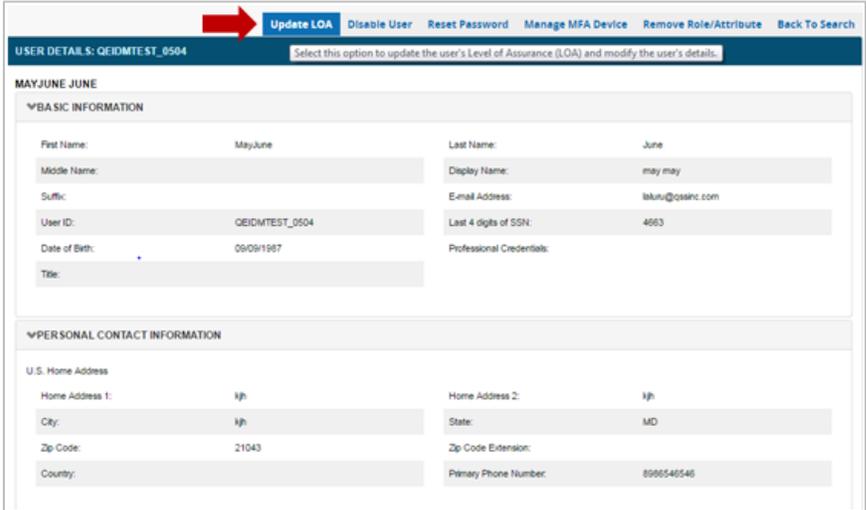
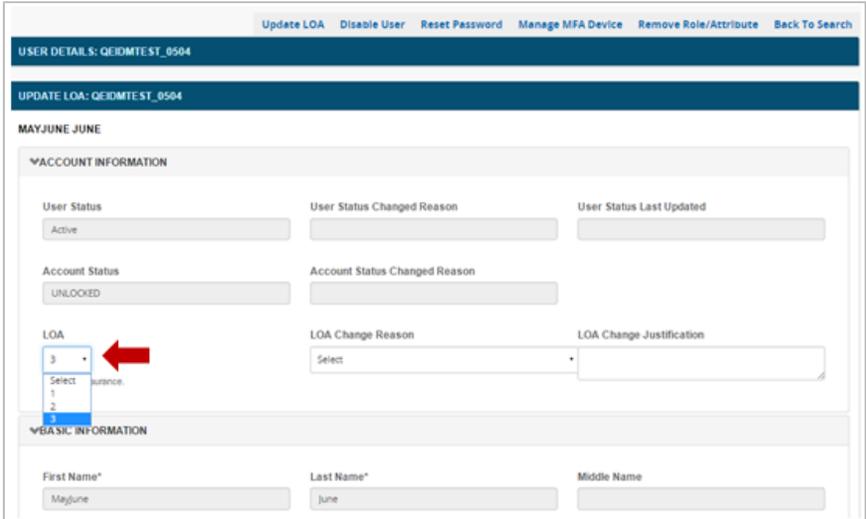
Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following browsers: Internet Explorer 8, 9, 10, and 11, Firefox, Chrome, and Safari.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

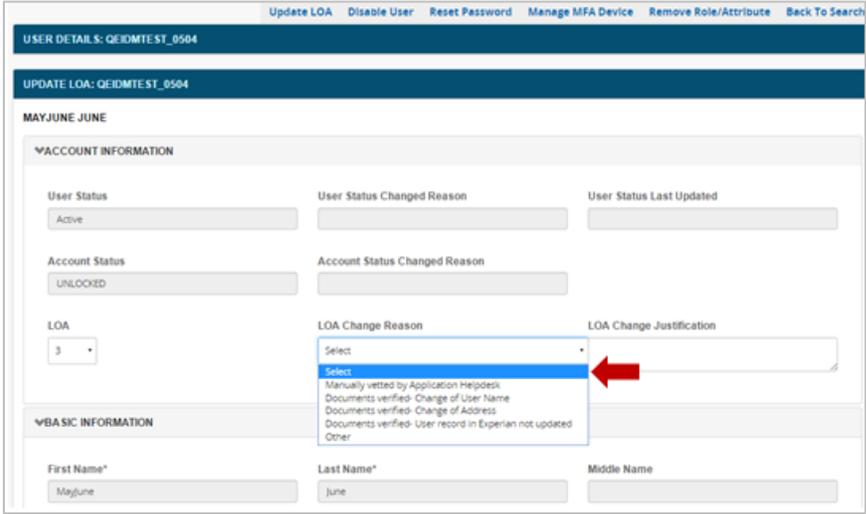
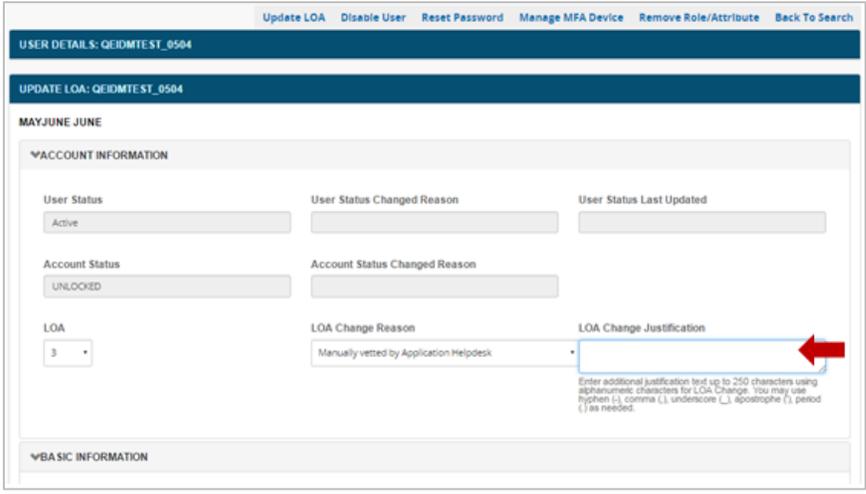
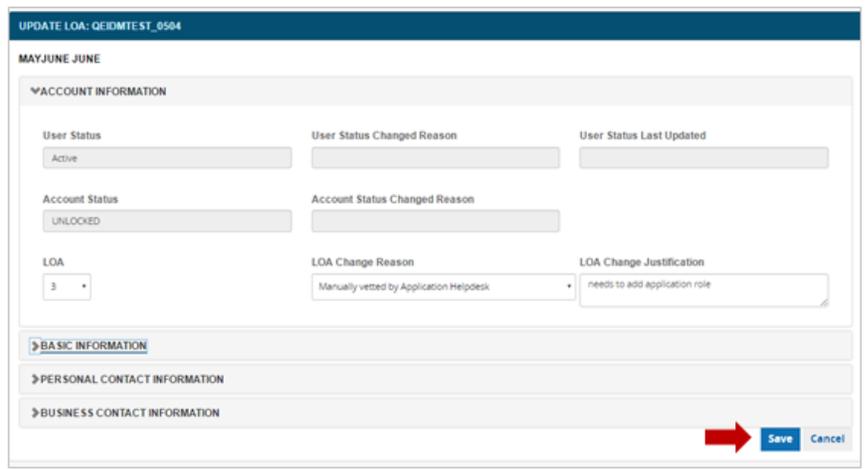
Steps	Screenshots
<p>3. Enter your <b>User ID</b> and select <b>Next</b>.</p>	
<p>4. Enter your <b>Password</b>, select an <b>MFA Device Type</b> from the drop-down list, enter the <b>Security Code</b>, and select <b>Log In</b>.</p> <p><i>Note: The 'Security Code' for the 'E-mail' and 'One-Time Security 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>The screenshot shows two parts. The top part is a mobile app interface titled 'VIP Access' with a Credential ID of 'VSHM49586924' and a Security Code of '533515'. A red arrow points to the Security Code field. The bottom part is a web form with a password field, an 'MFA Device Type' dropdown set to 'Phone/Tablet/PC/Laptop', and a Security Code field containing '31082'. A red arrow points to the Security Code field, and another red arrow points to the 'Log In' button. Below the form are links for 'Forgot Password?', 'Unable to Access Security Code?', and 'Register MFA Device'.</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>	 <p>The screenshot shows the login web form with the 'MFA Device Type' dropdown set to 'Interactive Voice Response (IVR)'. A red arrow points to the 'Send' button. Below the form, the Security Code field contains '312455', and a red arrow points to it. Another red arrow points to the 'Log In' button. The same links for 'Forgot Password?', 'Unable to Access Security Code?', and 'Register MFA Device' are visible at the bottom.</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>The screenshot shows a login form with a 'Password' field, an 'MFA Device Type' dropdown menu set to 'One-Time Security Code', and a message: 'The Security Code for the One-Time Security Code will expire in 30 minutes.' Below this is a 'Security Code' field containing '234211', with a red arrow pointing to it. To the right of the field are 'Log In' and 'Cancel' buttons, with a red arrow pointing to the 'Log In' button. At the bottom, there are links for 'Forgot Password?', 'Unable to Access Security Code?', and 'Register MFA Device'.</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>The screenshot shows the CMS Enterprise Portal home page. In the top right corner, there is a user profile dropdown menu with the text 'Welcome Solomon Jack'. A red arrow points to this menu, which is open and shows options: 'My Actions', 'My Helpdesk', 'My Access', and 'My Profile'. The 'My Helpdesk' option is highlighted. The main content area includes a 'Welcome to CMS Enterprise Portal' message, an 'Application Access' section, and a 'Request Access' section with a 'Request Access Now' button. There is also a 'Contact Help Desk' section with contact information for MCM and APS help desks.</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>	 <p>The screenshot shows the 'Application Search' page. It features several search criteria fields: 'User ID', 'E-mail Address', 'First Name', 'Last Name', 'Date of Birth' (MM/DD/YYYY), 'Last 4 digits of SSN', 'Account Status' (All), 'User Status' (All), 'State' (All), 'Application*' (Novitasphere), and 'Role' (All). A red arrow points to the 'Application*' dropdown menu. At the bottom right, there is a 'Search' button (highlighted with a red arrow) and a 'Reset' button.</p>

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><b>Note:</b> Use this to search and manage user accounts in 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 the <b>User ID</b> on the ‘Search Results’ page.</p>	

Steps	Screenshots
<p>8. Select <b>Update LOA</b> on the ‘User Details’ page.</p>	 <p>The screenshot shows the 'User Details' page for user QEIDMTEST_0504. At the top, there are navigation links: Update LOA (highlighted with a red arrow), Disable User, Reset Password, Manage MFA Device, Remove Role/Attribute, and Back To Search. Below the navigation is a sub-header 'USER DETAILS: QEIDMTEST_0504' and a note: 'Select this option to update the user's Level of Assurance (LOA) and modify the user's details.' The main content area is titled 'MAYJUNE JUNE' and contains two sections: 'BASIC INFORMATION' and 'PERSONAL CONTACT INFORMATION'. The 'BASIC INFORMATION' section includes fields for First Name (MayJune), Last Name (June), Middle Name, Display Name (may may), Suffix, Email Address (lakun@osinc.com), User ID (QEIDMTEST_0504), Last 4 digits of SSN (4663), Date of Birth (09/09/1967), and Title. The 'PERSONAL CONTACT INFORMATION' section includes fields for U.S. Home Address, Home Address 1 (1jh), Home Address 2 (1jh), City (1jh), State (MD), Zip Code (21043), Zip Code Extension, and Primary Phone Number (866546546).</p>
<p>9. Select a new <b>LOA</b> from the drop-down list.</p>	 <p>The screenshot shows the 'Update LOA' page for user QEIDMTEST_0504. At the top, there are navigation links: Update LOA, Disable User, Reset Password, Manage MFA Device, Remove Role/Attribute, and Back To Search. Below the navigation is a sub-header 'UPDATE LOA: QEIDMTEST_0504' and the user name 'MAYJUNE JUNE'. The main content area is titled 'ACCOUNT INFORMATION' and contains several sections: 'User Status' (Active), 'User Status Changed Reason', 'User Status Last Updated', 'Account Status' (UNLOCKED), 'Account Status Changed Reason', 'LOA' (dropdown menu with options 1, 2, 3, and a red arrow pointing to it), 'LOA Change Reason' (Select), and 'LOA Change Justification'. Below the 'ACCOUNT INFORMATION' section is the 'BASIC INFORMATION' section, which includes fields for First Name* (MayJune), Last Name* (June), and Middle Name.</p>

Steps	Screenshots
<p>10. Select an <b>LOA Change Reason</b> from the drop-down list.</p>	
<p>11. Enter an <b>LOA Change Justification</b>.</p> <p><i>Note: For LOA 3 updates, verify that the user’s Social Security Number (SSN) is entered in the SSN field under ‘Basic Information’. If it is not entered, enter their SSN.</i></p>	
<p>12. Select <b>Save</b> to save the changes.</p>	

Steps	Screenshots
13. An acknowledgement message displays to confirm that the update was successful. Select <b>OK</b> to return to the search page.	 A screenshot of a web application interface showing a confirmation message. At the top, there is a navigation bar with links: "Update LOA", "Disable User", "Reset Password", "Manage MFA Device", "Remove Role/Attribute", and "Back To Search". Below this, there are two dark blue header bars. The first one says "USER DETAILS: QEIDMTEST_0504". The second one says "UPDATE LOA: QEIDMTEST_0504". The main content area displays the message "User profile has been updated successfully." To the right of this message is a red arrow pointing to a button labeled "OK".