



Obtaining Access to CIMOR and Referral Database for DD TCM Entities August 2014

Content:

PART I:	Page 1: Essential information for CIMOR users
PART II:	Page 2: New TCM Provider Contract: Establishing a Local Security Coordinator/Officer (LSO) after contract is in place
PART III:	Page 4: Granting additional TCM Entities employee's access to CIMOR once the contract and LSO have been established
PART IV:	Page 5: Requesting CIMOR roles through Access Request Application (ARA) – All staff
PART V:	Page 10: Tracking ARA Requests and List of Current Roles
PART VI:	Page 11: Accessing CIMOR once access is granted
PART VII:	Page 11: Revoking User Access
PART VIII:	Page 11: Password Requirements
PART IX:	Page 12: Changing Your Password
PART X:	Page 14: Browser – Compatibility Settings

PART I: Essential information for CIMOR users.

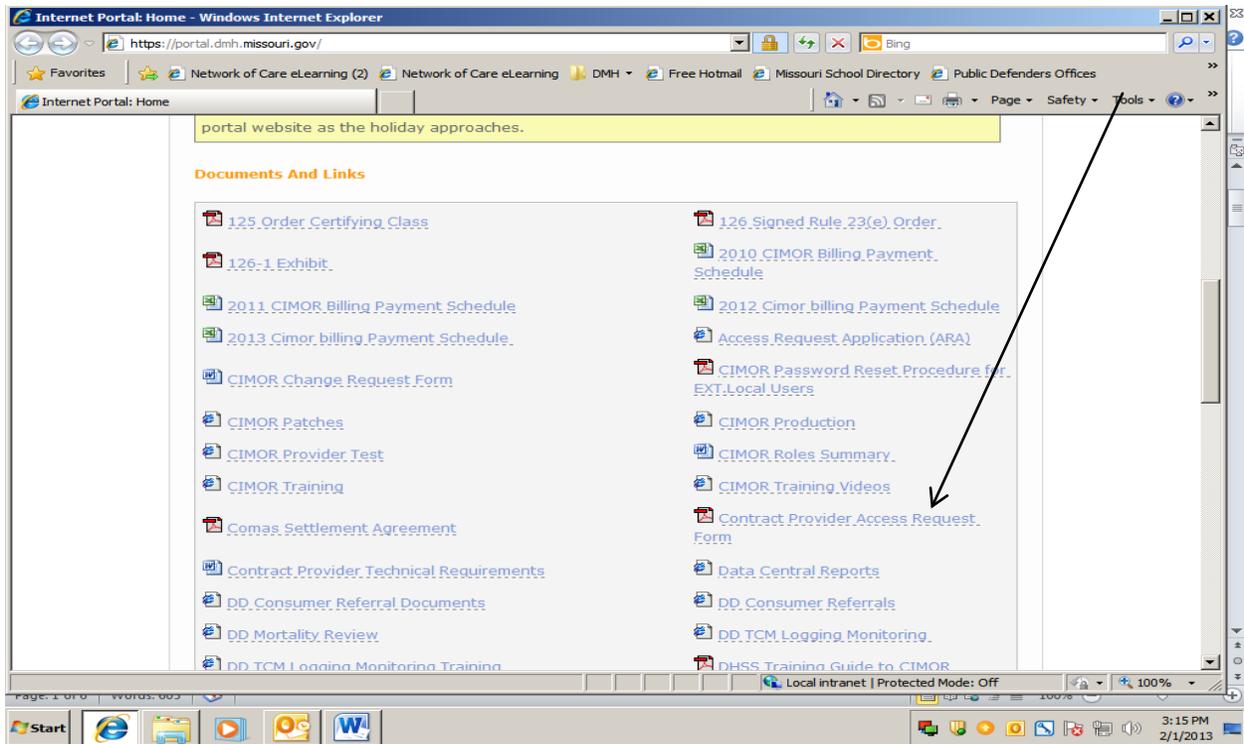
- When you obtain a User ID and Password, log onto CIMOR and change your password prior to any further action. If you skip this step, you must call the helpdesk and reset your password.
- Your password is only good for 60 days. You will not receive any reminders.
 - **This is the #1 reason why users are not able to access CIMOR.**
 - If you forget to change your password in a timely manner or enter an incorrect password too many times (3 or 4) you will be locked out of your account.
 - If you try to sign on and receive the message “invalid user credentials” or “contact your local security officer” this is usually related to a password no longer being valid.

- If this happens, contact Customer Support Center at 573-526-5888 or toll free at 888-601-4779 between 7:00a - 5:30p Monday thru Friday. The Customer Support Center also provides on-call coverage after hours for password resets. A technician will respond to your request with 2 hours of receiving the request. On-call coverage is available from 5:30 p.m. to 8:00 p.m. Monday through Friday, and 8:00 a.m. – 5:00 p.m. on Saturday/Sunday. The After Hour Help Number is 573-690-9924.
- DMH user IDs that have not been used for 90 or more days will be deleted. Please sign on a minimum of every 90 days in order to keep your user ID from being deleted. The user will have to resubmit a Contract Provider Access Form and go through the ARA process again.
- LSO needs to maintain access to CIMOR at least 1x every 60 days and update email address if it changes (update in Profile at top of portal.) LSO has to approve other user’s access request after receipt of notification through the email system. If email is not current, LSO will not receive notification.
- When an email is sent to the Local Security Coordinator/Officer (LSO) only the LSO should respond to that email.
 - Having someone else answer the email will result in loss of access to CIMOR due to a potential security breach. This will be extremely inconvenient if it occurs during billing periods.
- Do not share your user ID and Password. This will also result in loss of access to CIMOR due to a potential security breach.
- If an employee with access to CIMOR leaves the agency you need to IMMEDIATELY revoke their access. See Part VII.
- **Internet Explorer is the only browser that can access CIMOR.** If you have Internet Explorer version 9 or newer, you will have to add the website to the compatibility view of your computer. See “Contract Provider Technical Requirements” Document on the portal under documents and links for more computer requirements.

PART II: New TCM Provider Contract: Establishing a Local Security Coordinator/Officer (LSO) after contract is in place.

The first part of the process requires submitting required documentation to obtain a User ID and password.

- Step 1:** Complete the Contract Provider Access Request Form at <https://portal.dmh.missouri.gov>
- Under Part 4, all DD TCM Entities need to indicate “add” to Consumer Referral DB in second section
 - Under Part 5, if the LSO also has TCM supervisor responsibilities, indicate “add” for Data Entry and Reviewer Roles



Step 2: Draft a letter with the below components onto provider letter head. Example:

Provider Name
 Address
 City, State Zip
 Phone:
 Fax:

Date

Attention: (Provider Relations Liaison), (Local Regional Office Name)
 (Local Regional Office Address)

(Provider Relations Liaison):

RE: LSO and Provider Staff w/ Access to CIMOR

Our Local Security Officer (HIPAA) is: Name of Staff e-mail address

Sincerely,
 Executive Director Signature

Step 3: Fax completed documents to your local Regional Office. They will forward to OA for Assignment.

OA will provide the LSO a user ID and password. You will receive this information back from your local regional office.

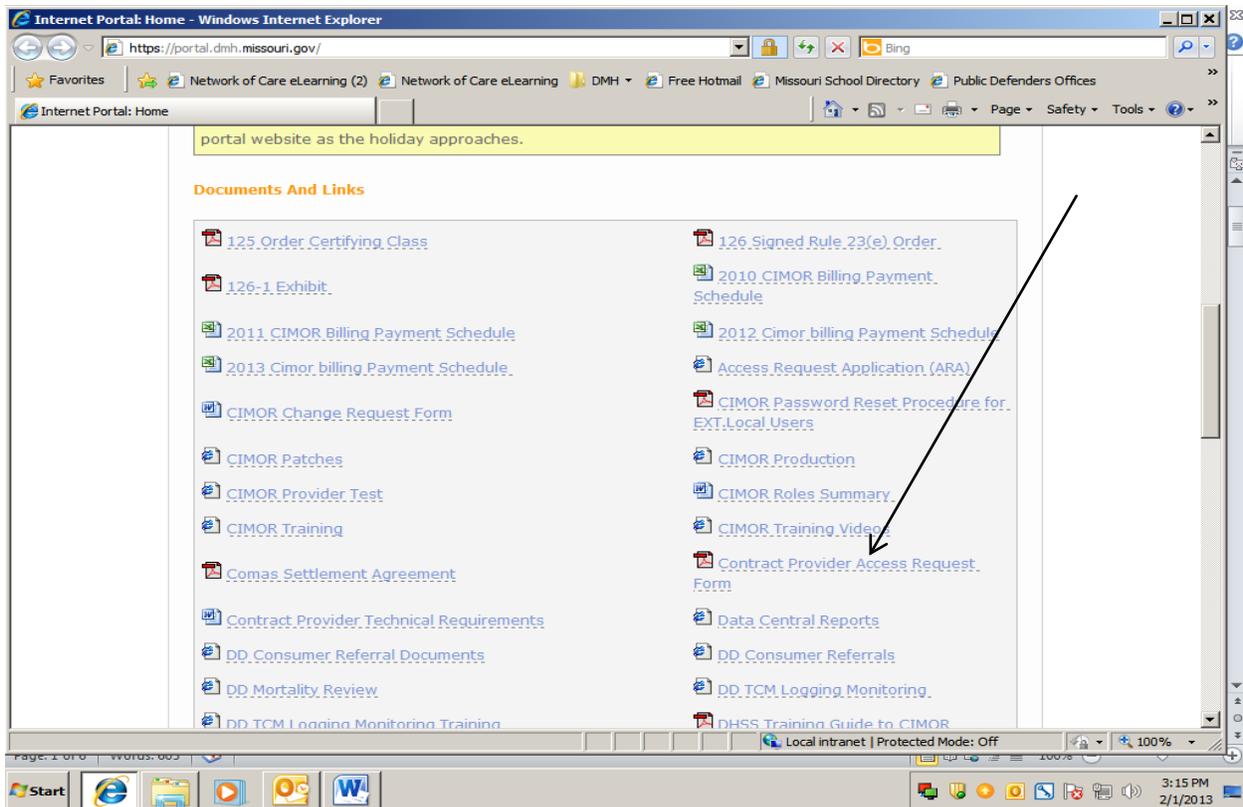
Once the LSO has received their new user ID and password, they will obtain CIMOR access by completing an ARA as described in Part IV, if additional access is needed.

Note: if LSO leave the agency, immediately revoke and reassign a new LSO. The LSO grants additional provider employee's requests for access. Without an LSO identified, requests cannot be processed.

PART III: Granting additional provider employee's access to CIMOR once the contract and LSO have been established.

Step 1: Complete the Contract Provider Access Request Form at <https://portal.dmh.missouri.gov>.

- Under Part 4, all DD TCM Entities need to indicate "add" to Consumer Referral DB in second section
- Under Part 5, if the employee will have TCM supervisor responsibilities, indicate "add" for Data Entry and Reviewer Roles
- Under "Additional Data Request" indicate "Create User ID and Password"



Step 2: Fax completed document to your local Regional Office TCM TAC who will forward to OA.

OA will provide the employee a user ID and password....you will receive this information from your local RO PR liaison. (Be sure your LSO signed the form)

OA will provide the employee a user ID and password....you will receive this information from your local TCM TAC liaison.

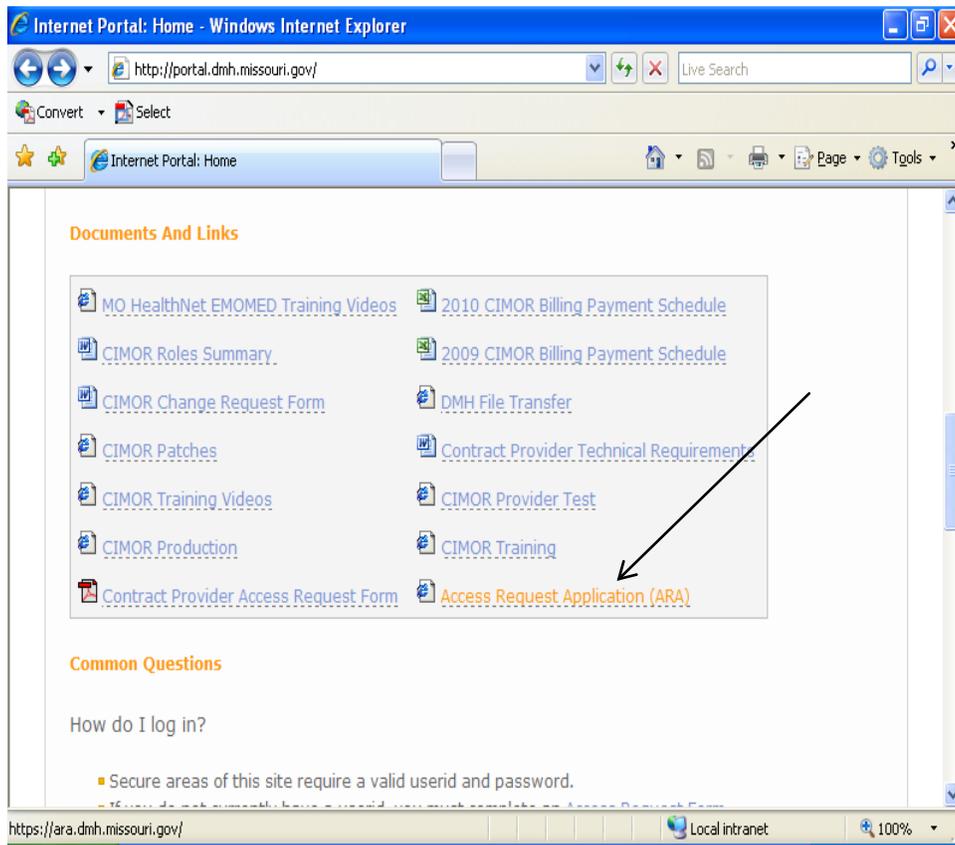
Once the employee has received their new user ID and password, they will proceed through the Part IV to obtain CIMOR access by completing an ARA.

PART IV: Completing an Access Request Application for CIMOR roles

Step 1: Completing an Access Request Application (ARA) is necessary to add provider roles in CIMOR, such as billing access and Health Inventories (HI is required for residential providers.)

To complete the Access Request Application (ARA) the new user will go to the DMH Portal web site at <https://portal.dmh.missouri.gov>.

In the Documents and Links section, click on the Access Request Application (ARA) link.



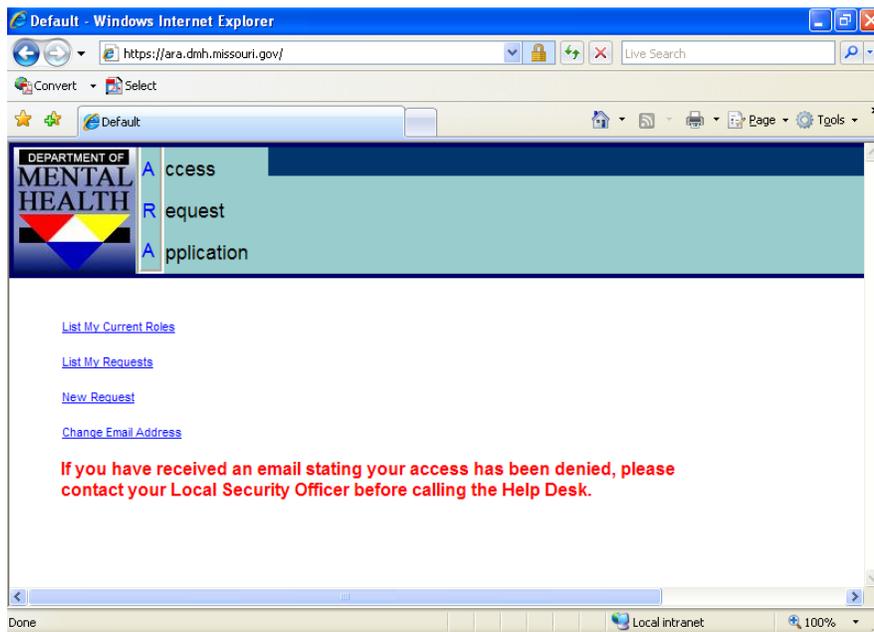


A log-in box will appear.

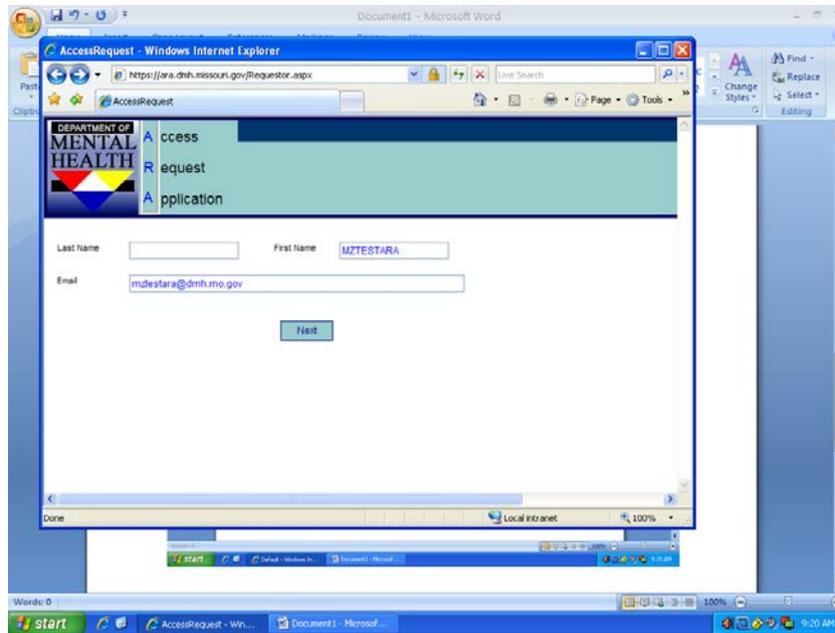
In the User name box, the user must enter their Domain Name, i.e. EXTLCL and a backslash \ (This is the slash mark above the Enter key). For example: extlcl\mytesta. Tab to the second box and enter the password the user was provided.

Note: It is only when accessing the ARA that entering the Domain Name is necessary. For CIMOR access, users will be able to enter their user ID and password only.

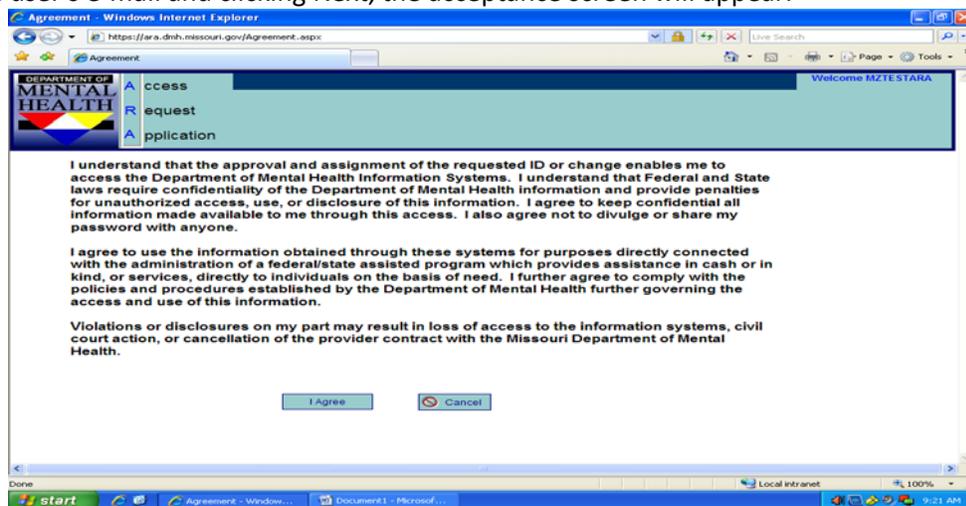
The main portal page will appear. Click New Request.



The next screen that appears will prompt the user to enter their e-mail address.

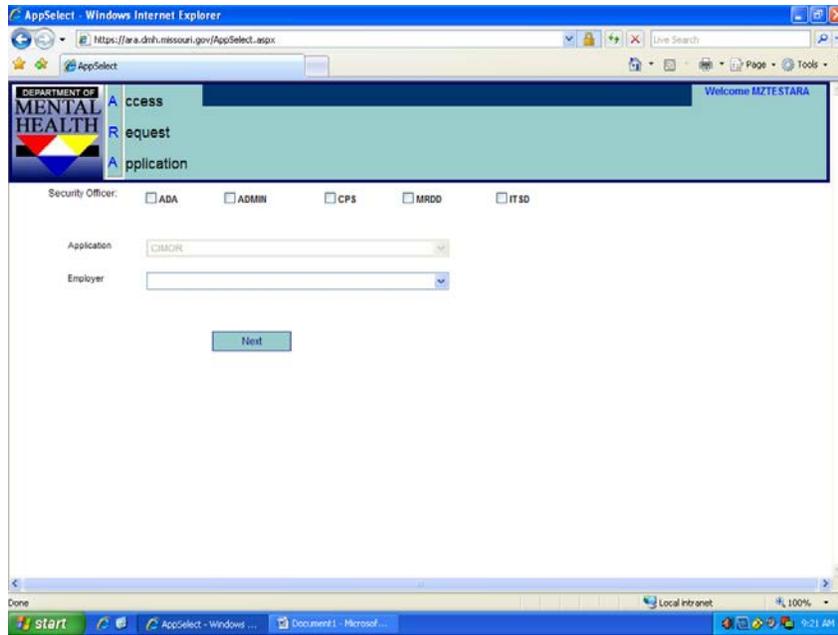


After entering the user's e-mail and clicking Next, the acceptance screen will appear.

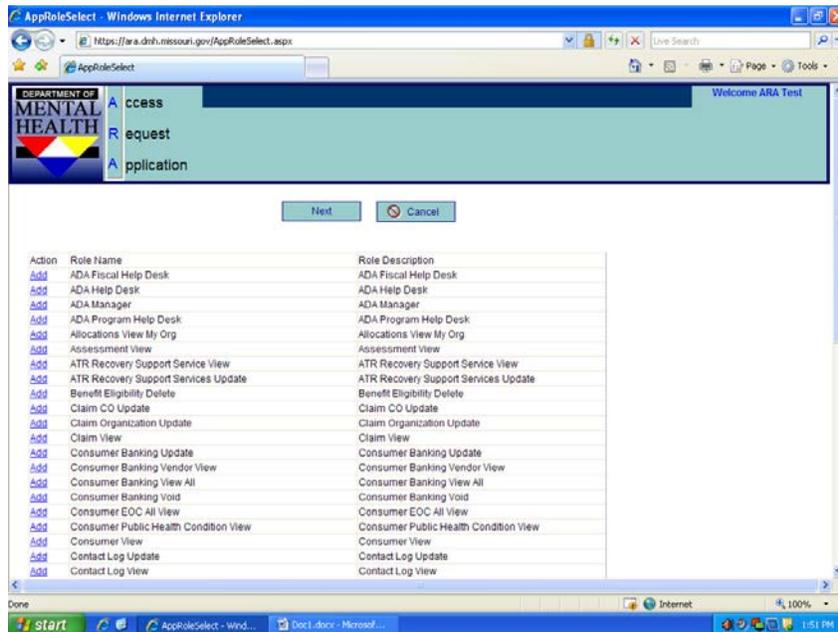


Click I Agree.

In the next screen that appears, the user needs to select the appropriate division, i.e., ADA, CPS, MRDD and the click the arrow in the **LOCAL REGIONAL OFFICE** as their organization.



In the next screen after choosing the provider's name for Employer, the list of CIMOR roles appears.



The user will click Add for each role they need to access.

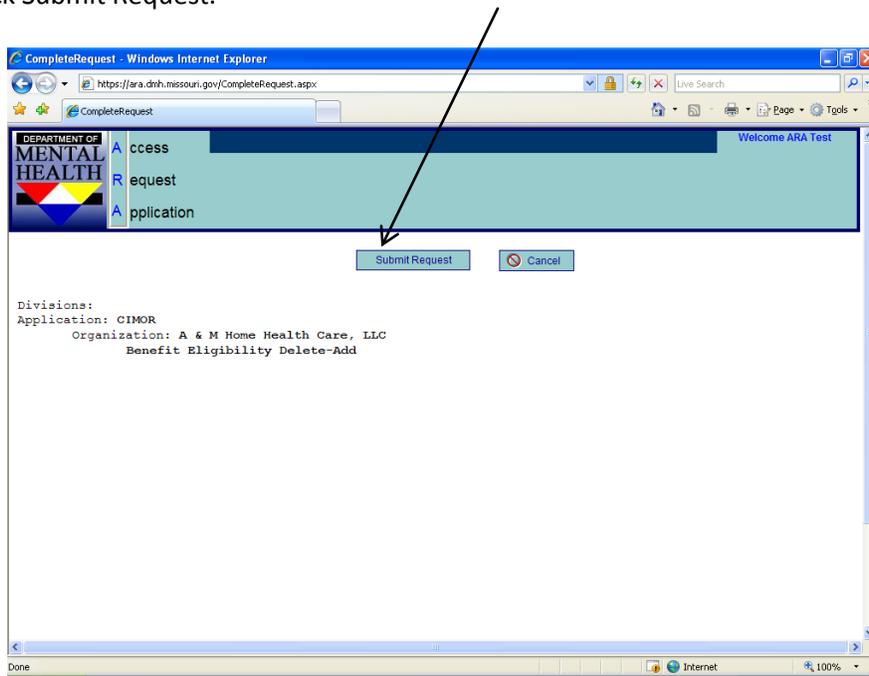
Note: Please refer to the CIMOR Security Roles Document available in the Documents and Links Section of the Portal Home Page for guidance in choosing roles. Not all roles are available for providers. If a request is submitted for a role a provider is unable to have, the entire request will be

denied and a new request must be submitted. Review roles document to decide which ones you want each employee to have.

Roles for DD TCM Entities are:

- DD Private TCM Provider Regional Office User
- DD Provider Profile Update (for staff responsible for maintaining Provider Profile on DD website)

Select “Add” next to the first role and wait for the role to be highlighted, then select the next role and wait for highlight and so on. After selecting the necessary roles, the user will click Next at the top of the screen. A review screen appears. Please review the selected roles and make any corrections if necessary. Click Submit Request.



A screen will appear indicating the request has been submitted.

The request will electronically route to the provider Local Security Coordinator to the email address on file with DMH. After the Local Security Coordinator has approved roles by clicking on the link and signing with their user id and password, the ARA will route electronically to the ITSD Provisioning for final approval.

If roles have been selected correctly and the LSO has approved, CIMOR access granted within 48 hours. If, however, any roles have been chosen that are not available to providers, the ARA will be denied and the user and Local Security Coordinator will receive an e-mail indicating why the request was denied. The request will then need to be resubmitted for approvals.

IF YOU ARE A TCM ENTITY BILLING TCM LOGGING THROUGH CIMOR – SEE NEXT PAGE.

TCM ENTITIES THAT BILL THROUGH CIMOR AND HAVE THEIR OWN EOC FOR TCM LOGGING:

Staff must also request an ARA under the TCM Organization through the same process indicated in this section.

In first screen shot, page 9, you would select your organization as the employer.

Additional Roles for TCM's billing through CIMOR

- MRDD TCM Provider Consumer and Services
- MRDD TCM Provider Financial (administrative in nature and optional for SC's)

PART V: Tracking ARA Requests and List of Current Roles

1. Tracking ARA Requests

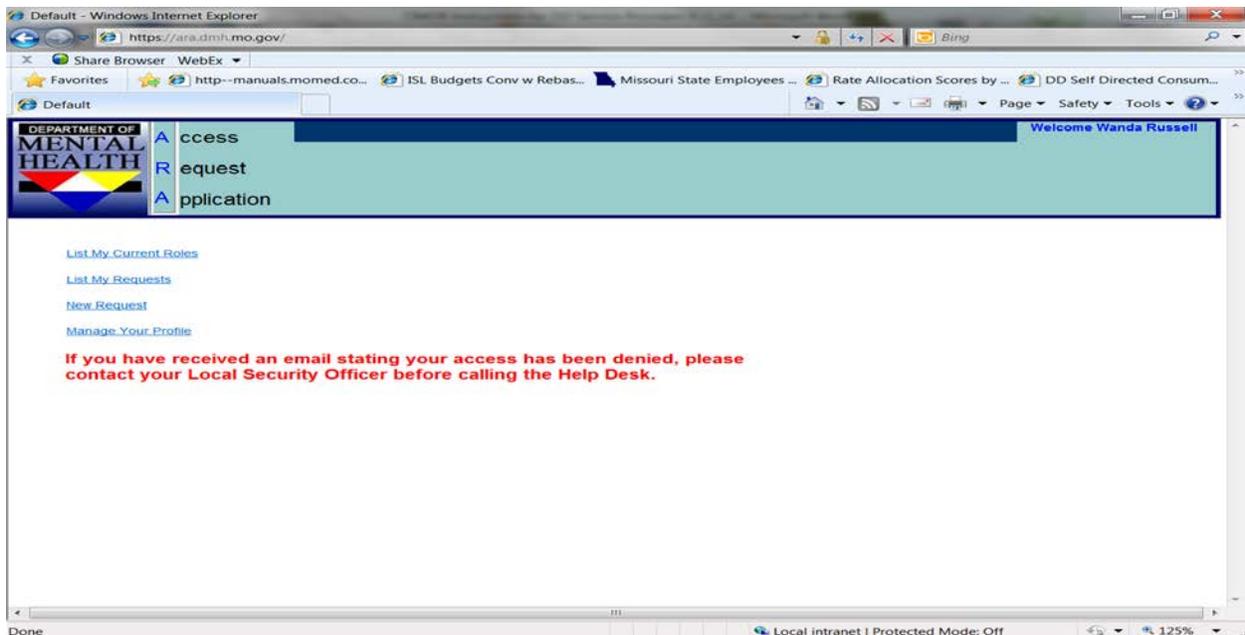
After an ARA has been submitted, the employee can track where the request is in the process.

Go to portal and select "Access Request Application (ARA)" from Forms and Documents. Select "List My Requests" from the following Screen. See screen shot below.

2. Obtaining a list of current approved roles or access.

At any time, an employee can review the roles or accesses in CIMOR that they have been granted.

Go to portal and select "Access Request Application (ARA)" from Forms and Documents. Select "List My Current Roles" from the following Screen. See screen shot below.



PART VI: Accessing CIMOR once access is granted

To access CIMOR after you have been given security clearance, please following these instructions:

- Type in the following url: <https://portal.dmh.missouri.gov>
- Scroll down to Documents and Links
- Click “CIMOR Production”
- Click on Login
- Log in with your user id and current password. **Make sure the Domain is EXTLCL**

The confidentiality statement should display. Accept and then CIMOR home page will display.

PART VII: Revoking User Access

When an employee who has access to CIMOR leaves an agency:

- IMMEDIATELY submit the Contract Provider Access Request Form indicating “Revoke” and the employee’s name. Fax the form to your local Regional Office Provider Relations liaison for processing.
- Remember, if the employee was a DD Provider Representative for the Health Inventory process, you will need to follow the directions in Part IV to assign a new DD Provider Representative.
- If the employee is the LSO, the provider will need to identify a new LSO by completing Steps 1 and 2 in Part 1 in addition to revoking access to the previous LSO.

Revoking user access is essential to an agency for security purposes. The ex-employee is able to access CIMOR from any location as long as they still have access approval.

As the person is no longer employed, it is a violation of confidentiality to have access to consumer information. The person’s access could create errors in billing information.

PART VIII: Password Requirements

Your new password must be at least 7 characters in length.

You must change your password prior to it expiring.

Your password will expire every 60 days.

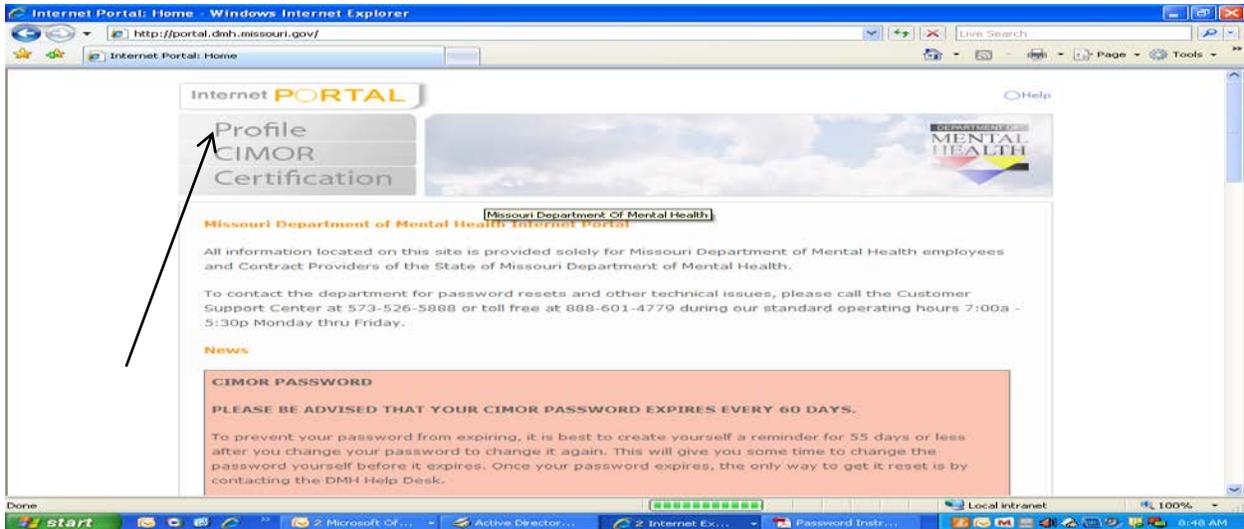
You cannot reuse your last 24 passwords.

Your new password must contain at least 3 of the following 4 character groups:

- 1) English uppercase (A through Z)
- 2) English lowercase (a through z)
- 3) Numerals (0 through 9)
- 4) Non-alphabetic (such as !, \$, #, %)

PART IX: Changing user password.

On your computer, open Internet Explorer and type: <https://portal.dmh.missouri.gov/> into the address bar. The following screen will display.



Click on Profile, a sign on screen will display.



Type in your user-id in the following format: EXTLCL\MYXXXX (replace X's with your user id) Nothing else should be in this box. Type in current password, click OK The following screen will display:

/// Profile

Manage Your Profile

Update Profile	
First Name:	<input type="text" value="Kathy"/>
Last Name:	<input type="text" value="Williams"/>
Organization:	<input type="text" value="Rolla Regional Center"/>
Email:	<input type="text" value="kathy.williams@oa.mo.gov"/>
Telephone:	<input type="text" value="573-368-2511"/>
<input type="button" value="Update"/>	

Manage Your Account

- Your password was last set on 5/17/2011 at 8:11:43 AM and is 28 days old.
- Your password will expire 31 days from today on 7/16/2011. 📅

⌵

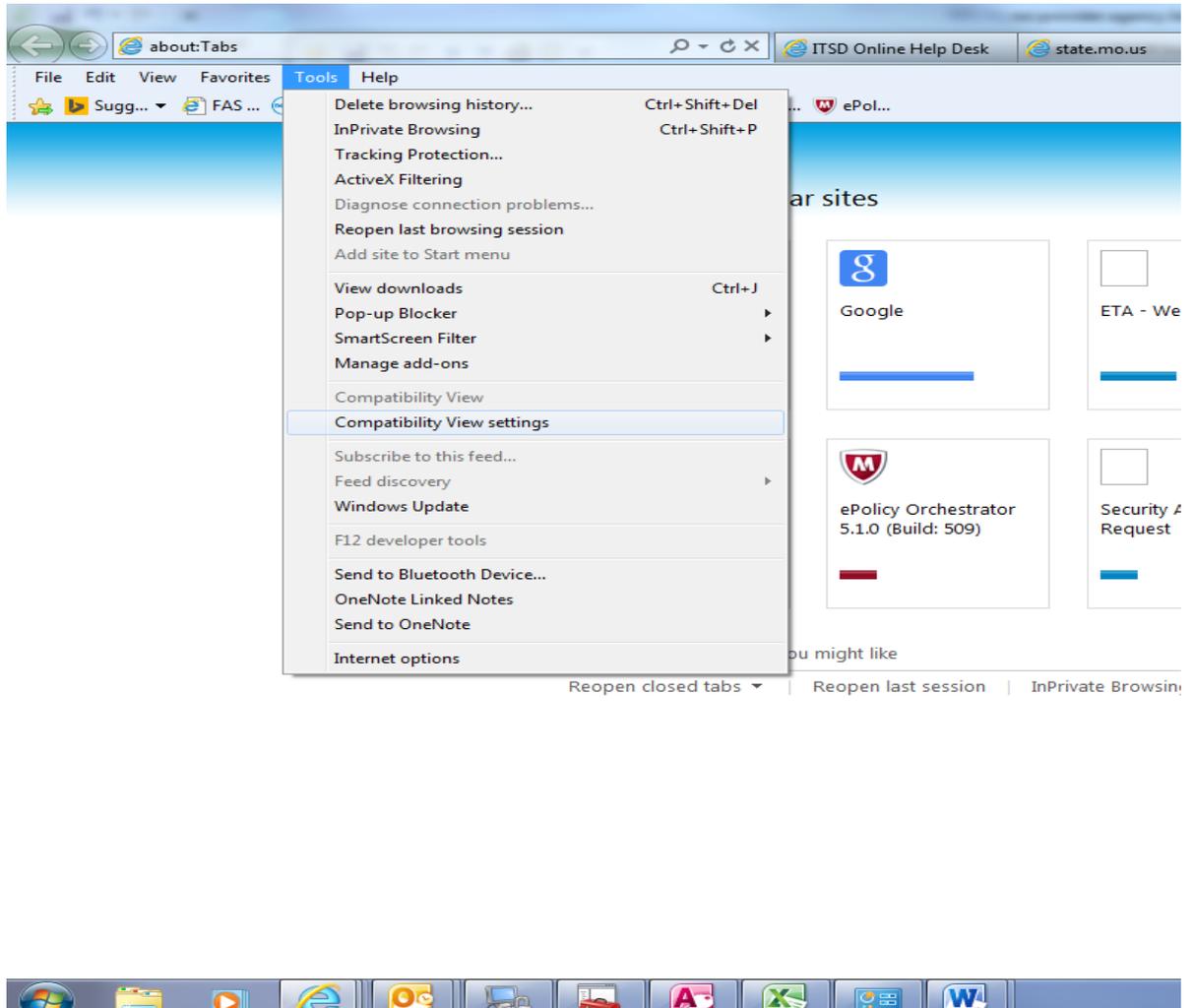
Update Password	
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>
<input type="button" value="Change Password"/>	

Here is where you can change your password.
Click the Back Arrow on your browser to return to the Portal.

REMEMBER: If your password has expired, contact customer support at 573-526-5888 or toll free at 888-601-4779 between 7:00a - 5:30p Monday thru Friday. The Customer Support Center also provides on-call coverage after hours for password resets. A technician will respond to your request with 2 hours of receiving the request. On-call coverage is available from 5:30 p.m. to 8:00 p.m. Monday through Friday, and 8:00 a.m. – 5:00 p.m. on Saturday/Sunday. The After Hour Help Number is 573-690-9924.

PART X: Browser – Compatibility Settings

1. Open up Internet Explorer 9, 10, or 11.
2. Press the “Alt” key on your keyboard to bring up the top menu with File, Edit, View, Tools. Then go to Tools, Capability View Settings,



3. Add CIMOR web site to view in compatibility mode and click on the checkbox that has all to view in capability mode, click Close.

