
MANAGING USER SECURITY

Organization Administration

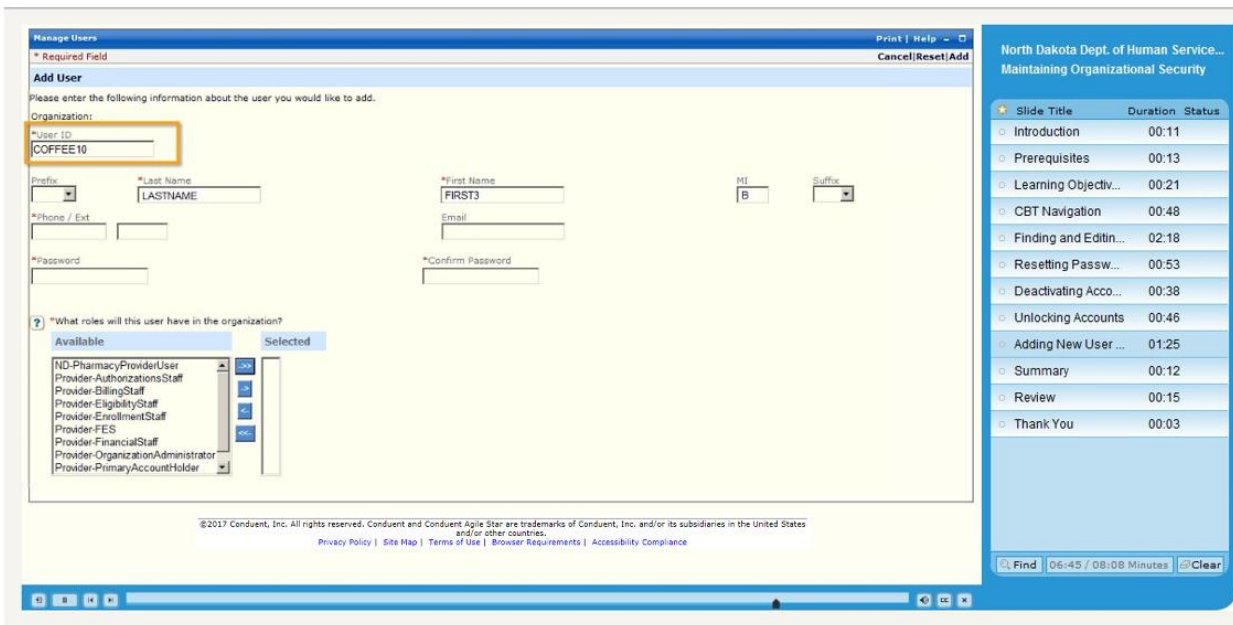
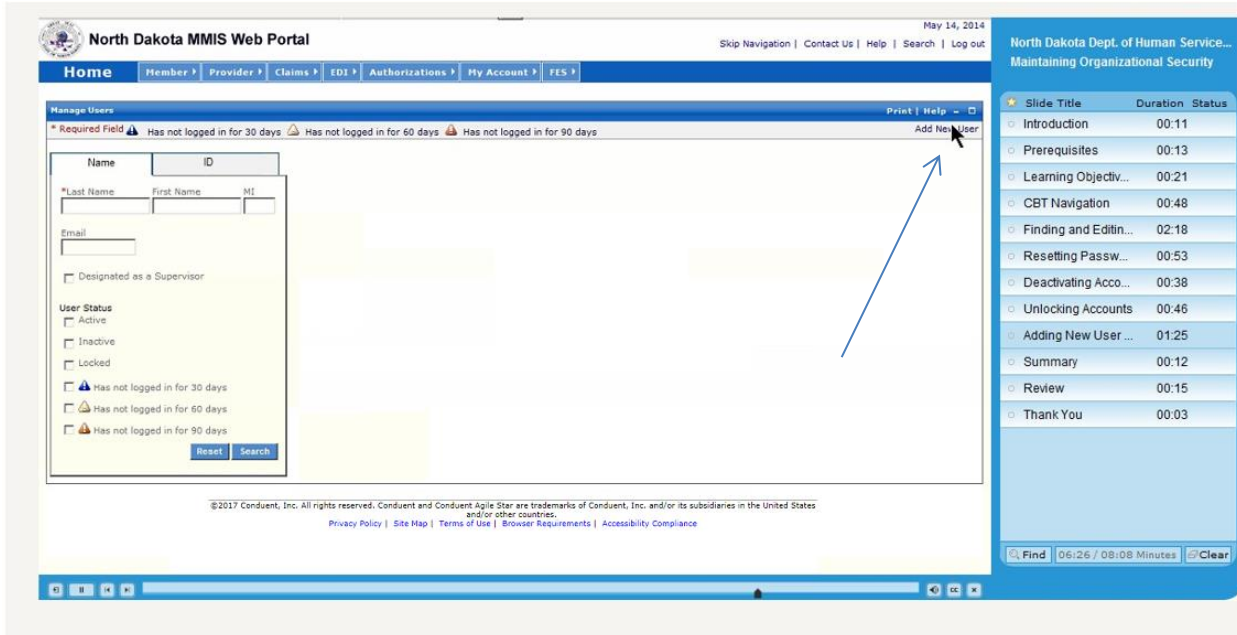
The Organization Administrator is the designated person with the primary responsibility and authority to establish accounts and passwords for access to provider specific secure information in ND Health Enterprise MMIS.

This instruction shows how an Organization Administrator works with security accounts for users within their organization. User has the ability to add, edit, reset passwords and delete user accounts.

Important: The Organization Administrator should set their profile to include Provider-Organization Administrator and Provider-Primary Account Holder.

1. Add a user
2. Search for a user
3. Reset a user's password
4. Deactivate a user
5. Unlock a user account

1. Add a user



*Any field with an asterisk requires data

Provider Accounts Security Role Options

Provider Staff Role	Functionality
Provider-Organization Administrator	Ability to create and configure other Provider organizational users and define their role(s) (Security only)
Provider-Primary Accountholder	Has full access (view/add/update) to all provider functions and privileges (including Security)
Provider-Authorizations Staff	Ability to request/edit/view service authorization requests
Provider-Billing Staff	Ability to submit claims via the web portal; check claims status
Provider-Eligibility Staff	Ability to verify member/patient Medicaid eligibility information
Provider-Enrollment Staff	Ability to view/add/update provider enrollment data
Provider-Financial Staff	Ability to view Remittance Advice and other provider accounting information
Provider-FES	Ability to view/add/update the Submit Payment Alert/Hospice Election Form (Functional Eligibility System)
Provider-Trading Partner Enrollment	Ability to view/add/update Trading Partner details

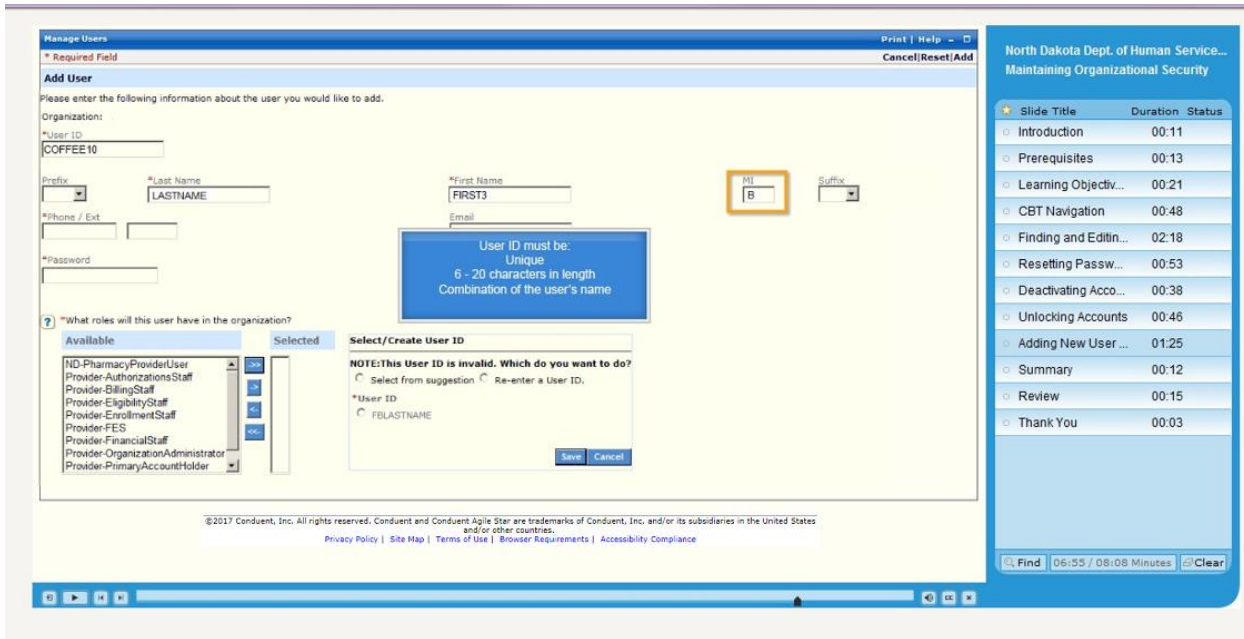
Important: The Organization Administrator should set their profile to include Provider-Organization Administrator and Provider-Primary Account Holder.

Special Considerations

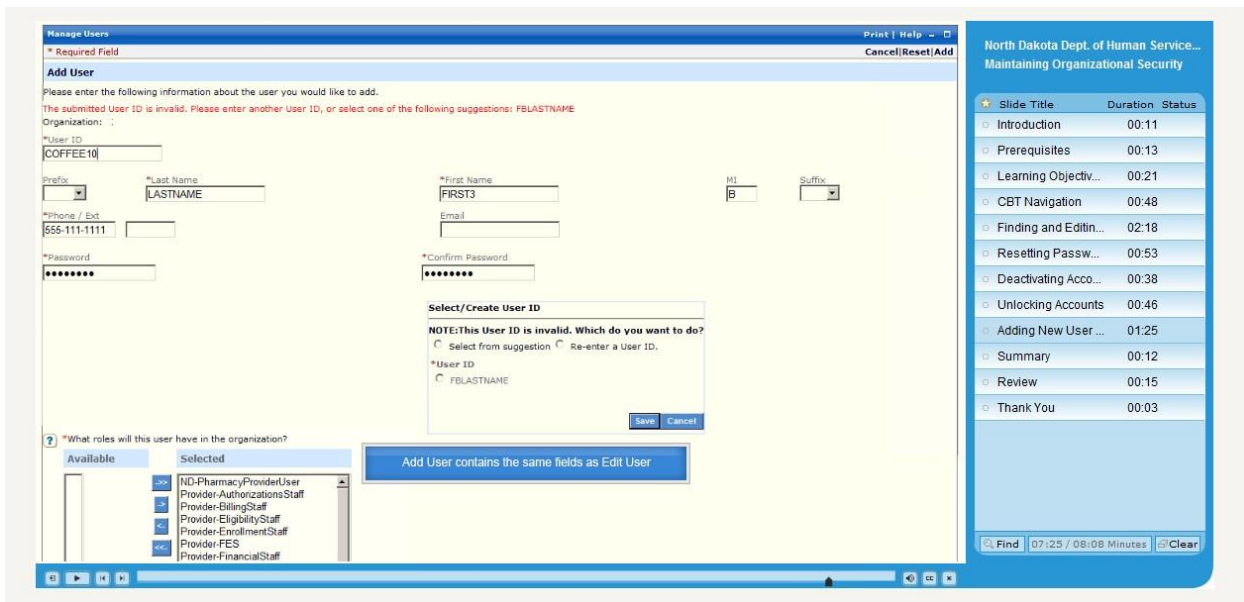
Complex Functional Organizations - For organizations where Medicaid processing is assigned to several individuals or departments we recommend the Organization Administrator create at least one Backup Organization Administrator. In addition, create additional accounts for individuals in the functional areas noted above (Provider Roles) and also create backups for each role in the event of staff absences, job change, or turn over.

Moderate Functional Organizations – For organizations where individuals perform two or more business functions we recommend the Organization Administrator create a Backup Organization Administrator and create additional accounts assigning functional areas, as appropriate for work organization and processes.

Simple (single person) - For organizations where one person performs all business and security functions, the single provider Organization Administrator account also has the Primary Accountholder role assigned and can perform all functions.

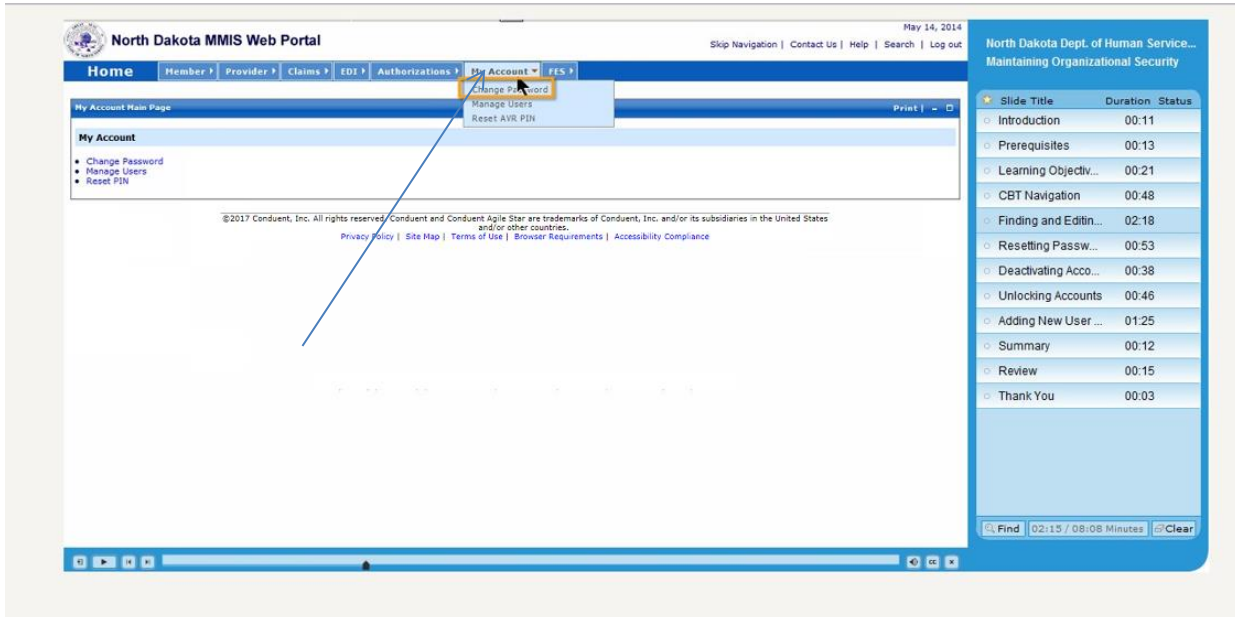


If the user ID is invalid or already used by another provider, the system will suggest alternate user ID's:

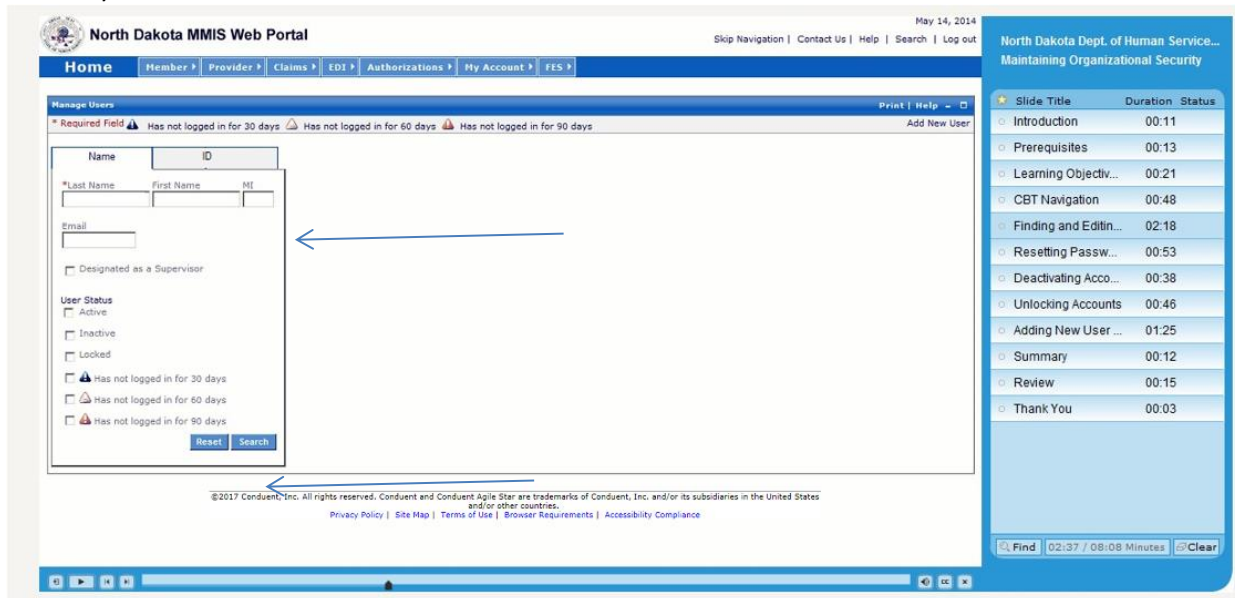


Select Add to save to the database.

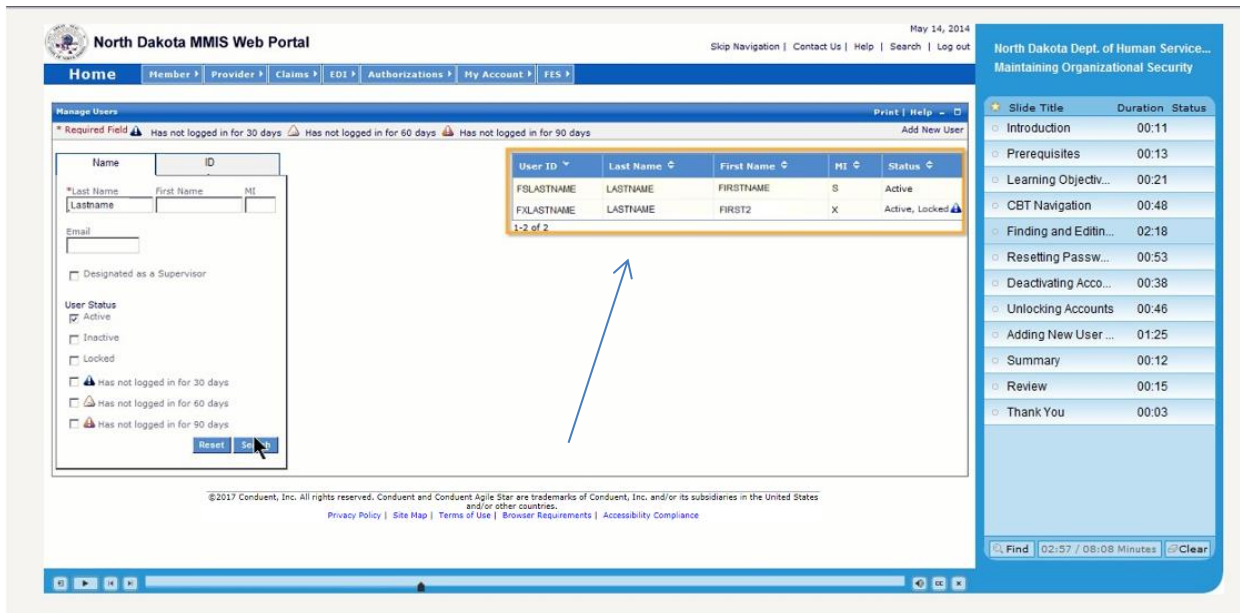
2. Search for a user



Select My Account



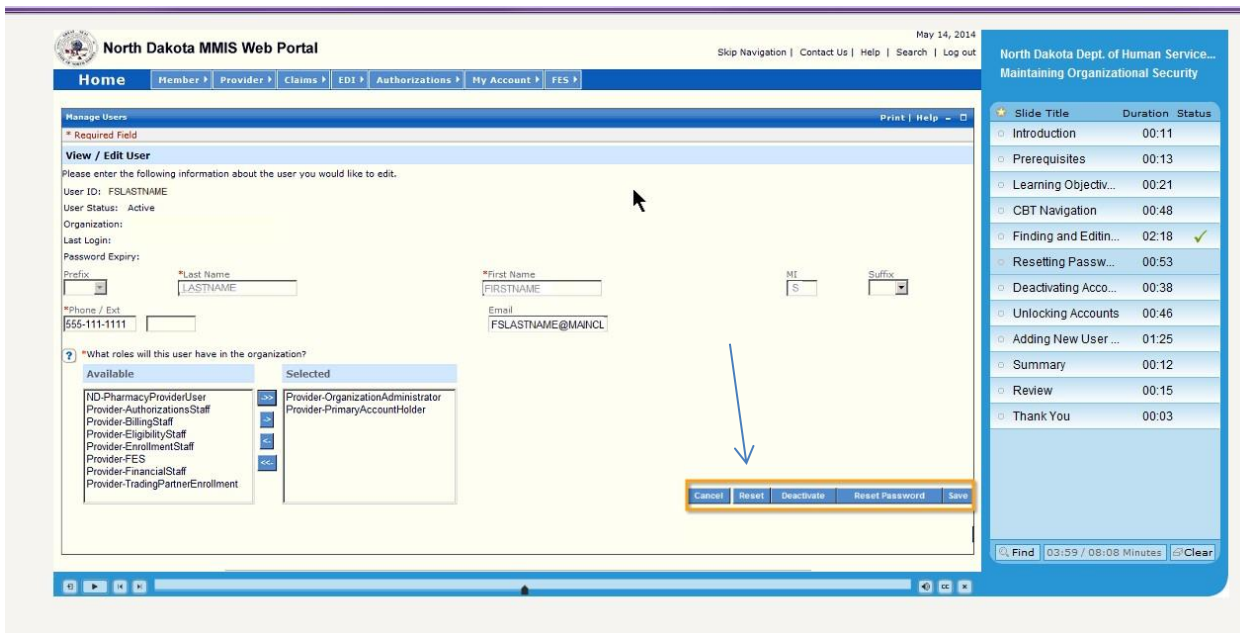
Search for the user by entering first name, last name or by User ID



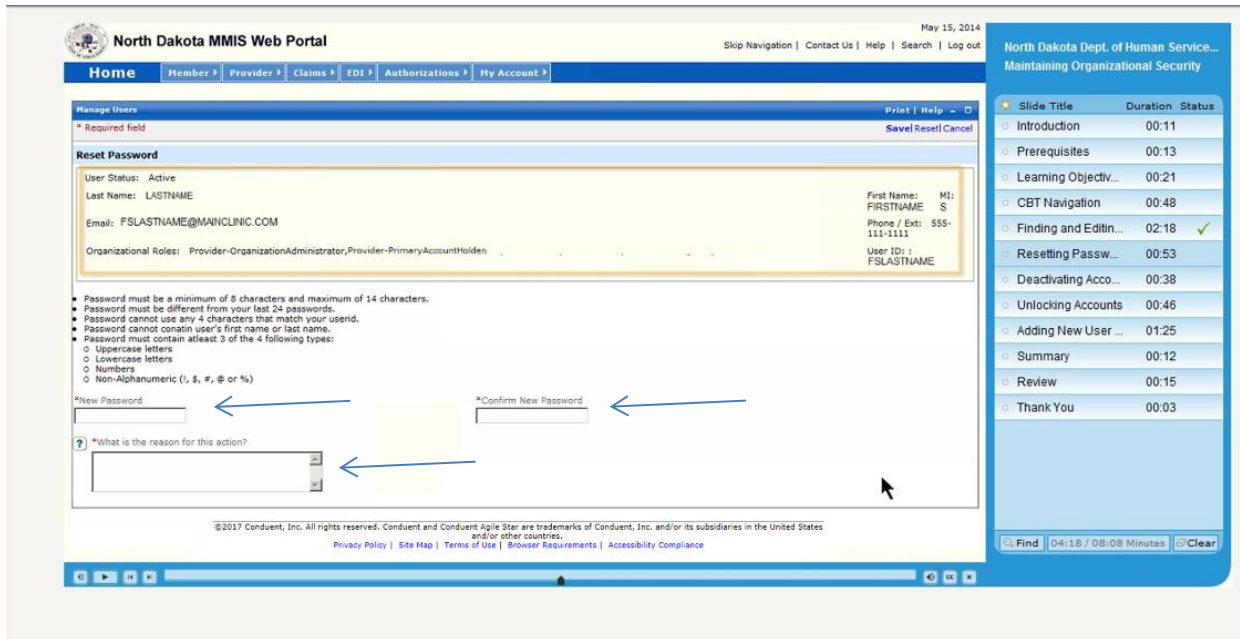
Results will present in highlighted box

3. Reset a user's password

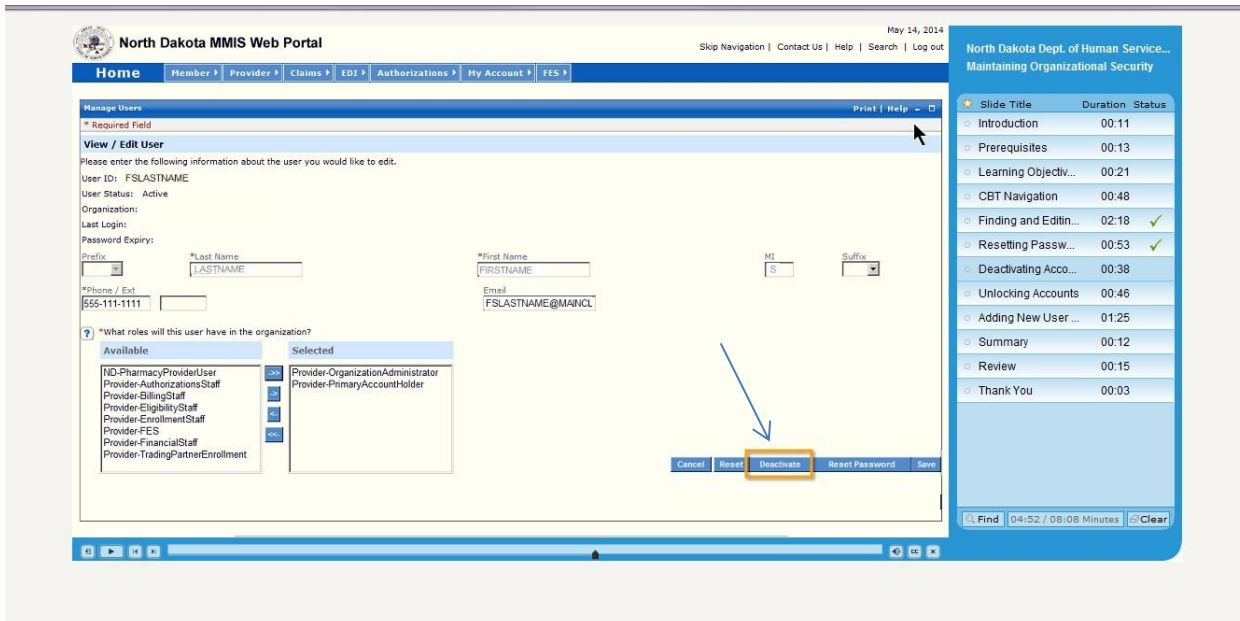
- a. Use step 2 above to search for a user
- b. Follow steps below to reset a user's password



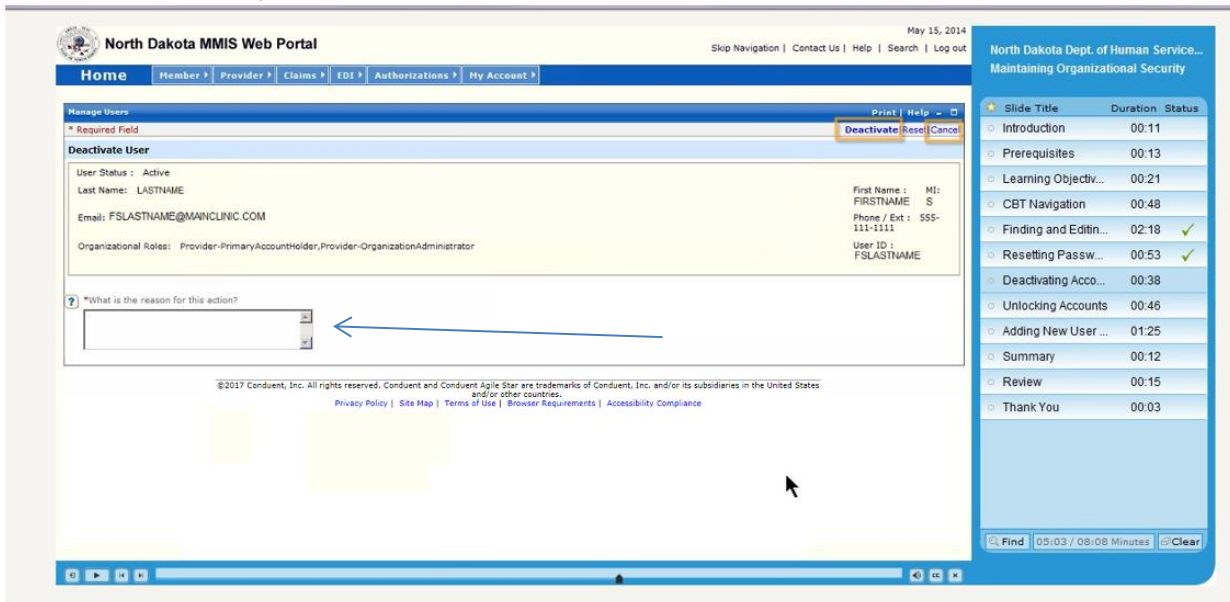
The provider has the option to reset the password; this password is for a one time use only



4. Deactivate a user



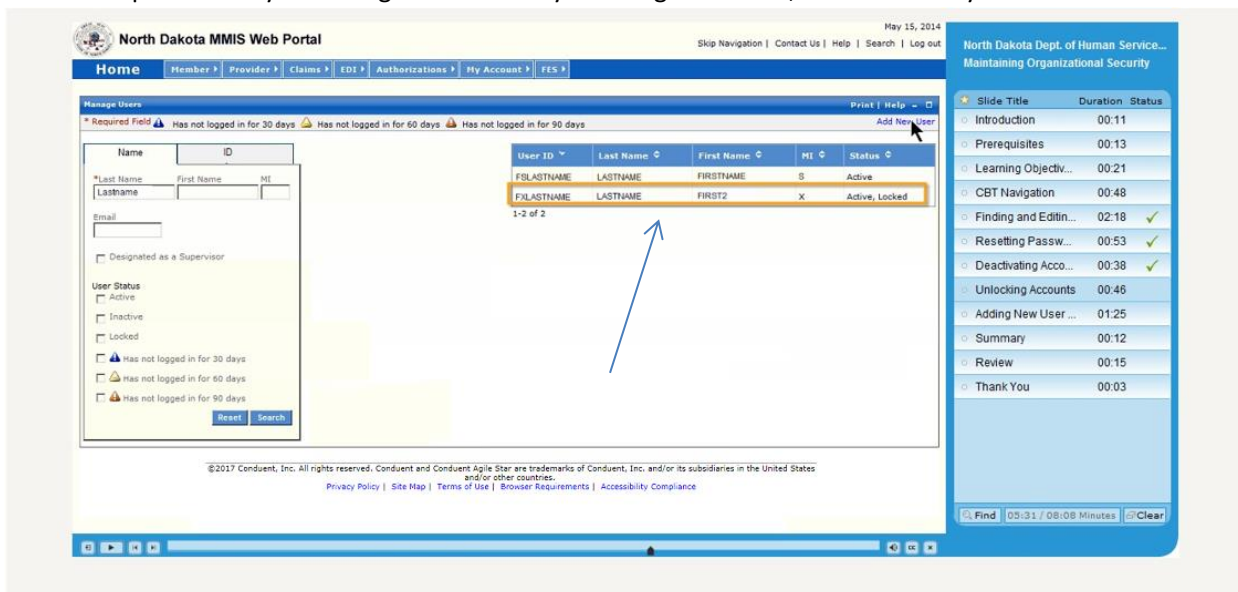
Select the deactivate option



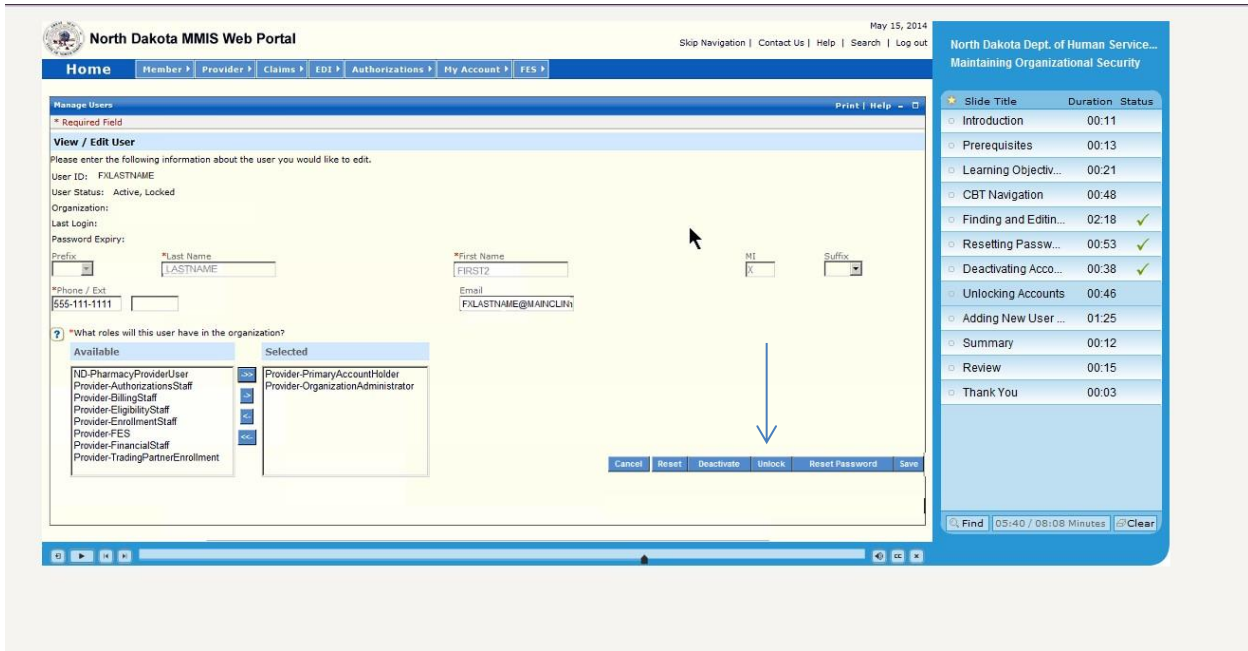
Enter the deactivation reason in the box asking *What is the reason for this action?

5. Unlock a user account

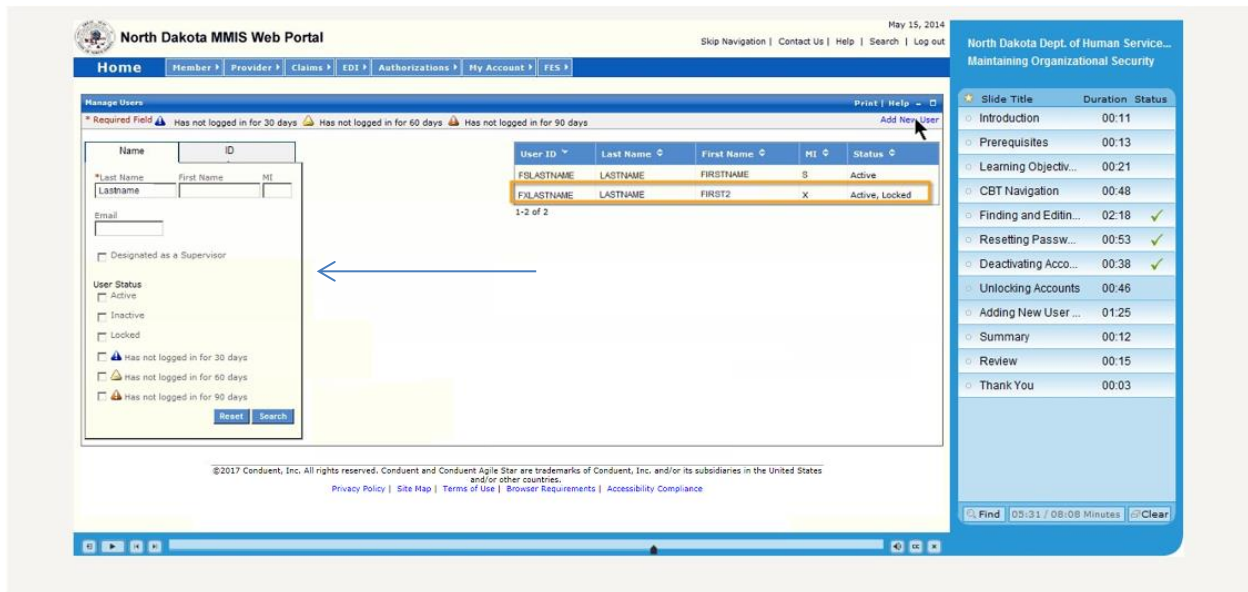
*Follow Step 2 above by searching for the user by entering first name, last name or by User ID



Select user from user list



Select the unlock option



Enter the unlock reason in the box asking *What is the reason for this action?

North Dakota MMIS Web Portal May 15, 2014

Skip Navigation | Contact Us | Help | Search | Log out

Home | Member | Provider | Claims | EDI | Authorizations | My Account | FES

Manage Users Print | Help

* Required Field Unlock | Reset | Cancel

Unlock User

User Status: Active, Locked

Last Name: LASTNAME First Name: FIRST2 MI: X

Email: FXLASTNAME@MAINCLINIC.COM Phone / Ext: 555-111-1111

Organizational Roles: Provider-PrimaryAccountHolder, Provider-OrganizationAdministrator User ID: FXLASTNAME

? *What is the reason for this action?

to unlock

Unlocking an account does NOT reset the user's password

North Dakota Dept. of Human Service...
Maintaining Organizational Security

Slide Title	Duration	Status
Introduction	00:11	
Prerequisites	00:13	
Learning Objectiv...	00:21	
CBT Navigation	00:48	
Finding and Editin...	02:18	✓
Resetting Passw...	00:53	✓
Deactivating Acco...	00:38	✓
Unlocking Accounts	00:46	
Adding New User ...	01:25	
Summary	00:12	
Review	00:15	
Thank You	00:03	

Find 05:56 / 08:08 Minutes Clear

The Organization Administrator can determine if the password should be reset. Otherwise, the user can resume using the password that is in current use.