

## Agency Admin Training – Resetting Passwords

- When a user gets locked out due to 3 consecutive bad logins, the login page looks like this:

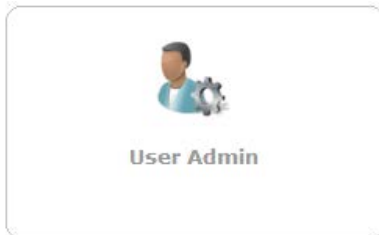


- To reset the password, login to HMIS/Servicepoint yourself.

- Click on the Admin button on the menu

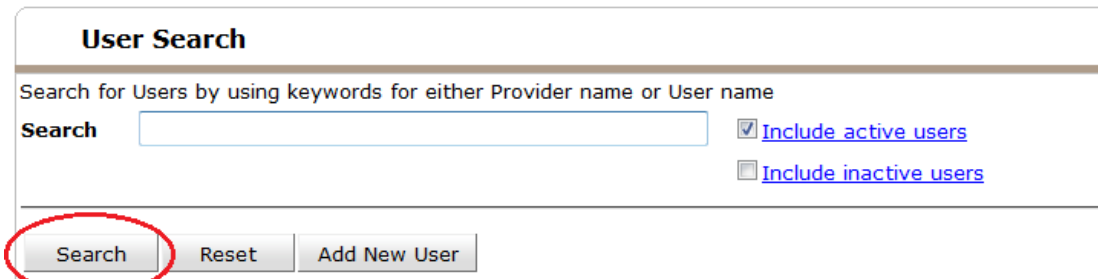


- Click on the User Admin button from the Admin Dashboard



- Click the Search button to populate a list of all your employees/users.

*(Optional, you may search by individual employee name, but it is faster to just click Search)*



## Agency Admin Training – Resetting Passwords

- Choose the user that needs the password reset by clicking the edit pencil icon to the left of their name.



**User Search Results**

	User	Name	Provider	Access Level	Active Status	SP License	ART License
	 ██████████ <b>User Name</b>	██████████ <b>Full Name</b>	Catholic Charities - Flagstaff (6)	Case Manager II	Active		
	 ██████████	██████████	Catholic Charities - Flagstaff (6)	Case Manager II	Active		
	 ██████████	██████████	Catholic Charities - Flagstaff (6)	Case Manager II	Active		
	 ██████████	██████████	Catholic Charities - Flagstaff (6)	Case Manager II	Active		

- First, click the Reset button next to the red **3** consecutive bad logins; it will change back to a green **0**.
- Second, click the Generate Password button. The system will generate a password automatically and this can be given to the user, but you may also type over the system generated password and insert your own generic password that will be easier to manage.

*Whatever password you give them will immediately expire when they use it to login and they will be forced to create another new password only they know. This is why the HMIS support desk always uses the generic "monkey123" password for password resets; you are welcome to use it as well.*

- Lastly, click the Save & Exit button and notify user of new password.

<b>User Name *</b>	<input type="text" value="htrainer2"/>	
<b>Password *</b>	<input type="password" value="*****"/>	<input type="button" value="Generate Password"/> <span style="color: red;">← 2. Click here to generate new password. You may give the user the generated one, or you may type over it with something generic like we use at HMIS support, such as monkey123.</span>
<small>Password must be 8-50 characters long with at least two numbers or symbols.</small>		
<b>Password Expiration</b>	Monday, May 25, 2015	
<b>Role *</b>	Case Manager II	
<b>User Expiration</b>	<input type="text"/> / <input type="text"/> / <input type="text"/>   <b>Current</b>	
<b>Status</b>	<input checked="" type="radio"/> <b>Active</b> <input type="radio"/> <b>Inactive</b>	
<b>Consecutive Bad Logins</b>	3 <input type="button" value="Reset"/> <span style="color: red;">← 1. Click here to "reset" bad logins</span>	
<b>Last Login</b>	Thursday, April 30, 2015	
<b>Has Accepted EULA</b>	Yes	
<span style="color: red;">3. Click Save &amp; Exit</span> <input type="button" value="Save"/> <input type="button" value="Save &amp; Exit"/> <input type="button" value="Exit"/>		

### HMIS Contact Info

**Helpdesk Phone: 602-908-3605**

**Helpdesk Email: HMIS-Support@crisisnetwork.org**