



JNET Automated Registration & User Provisioning System

JTAC USER GUIDE

April 8, 2010, Version 1.2

Revision History

Version	Date	Author(s)	Revision Notes
1.0	11/24/2009	Monika Ross	Initial version.
1.1	03/01/2010	Monika Ross	Add Functionality
1.2	03/12/2010	Monika Ross	Title Change → JTAC Administration

Table of Contents

TABLE OF FIGURES	III
1 INTRODUCTION	1
2 JTAC ROLE	1
2.1 Accessing the JTAC Dashboard.....	1
2.1.1 JTAC Agreement Form.....	2
2.2 JTAC Dashboard	3
2.3 Viewing Your Profile	4
3 CRIMINAL HISTORY ACCESS REQUESTS	6
3.1 Requesting Criminal History Access	6
3.2 Requests & Approvals.....	7
3.3 Request Timeouts	7
3.4 Claim the Request.....	7
3.5 Attestation.....	10
4 JTAC ADMINISTRATIVE TOOLS	10
4.1 JTAC Administration	11
4.1.1 Downgrading Users	12
4.1.2 User Reinstatement	13
4.2 Re-certification CH Role	18
5 JNET HELP DESK	19

Table of Figures

Figure 1 - JTAC Hierarchy.....	1
Figure 2 – JNET User Provisioning System	2
Figure 3 - JTAC Agreement Form.....	3
Figure 4 – JTAC Dashboard.....	4
Figure 5 - Edit Profile.....	5
Figure 6 - JTAC Notification	6
Figure 7 - My Tasks.....	7
Figure 8 - Request Details	8
Figure 9 - Request Claimed & Approved	9
Figure 10 - Request Approved.....	10
Figure 11 - Request Resource Links	11
Figure 14 - NEW JTAC UI	12
Figure 15 - Person Lookup.....	12
Figure 16 – User Downgrade	13
Figure 17 - Roles Tab	14
Figure 18 - View Assignments Icons	14
Figure 19 - View User's Roles.....	15
Figure 20 - Removal Confirmation	15
Figure 21 - Role Assignment Removal Script	15
Figure 22 - User Assignments	16
Figure 23 - Role Assignment Form.....	16
Figure 24 - Search for Role(s).....	17
Figure 25 - User Role Assignments	18
Figure 12 – User Re-certification Request	19
Figure 13 - Re-certification Notification	19

1 Introduction

Under JNET Policy and Procedure every county or agency that desires to use JNET to gain access to Computerized Criminal History Record Information (CCHRI) through CLEAN must designate an individual as a JNET Terminal Agency Coordinator (JTAC). Under the new automated registration, all JTAC's will have the ability to approve or deny a JNET user within their agency/department for Criminal History (CH) access via the computer using JNET's secure infrastructure.

2 JTAC Role

Every County, State and Federal Agency is required to have a JTAC. This person is known as the JTAC Administrator. The JTAC is the Agency point of contact concerning all criminal history information accessed by JNET CH users.

JTAC Administrators, also known as Level 20 JTACs, are responsible for administering and managing CLEAN certification with respect to JNET CH users in their County or Agency. Approvals and denials are managed via the JTAC User Interface (JTAC UI).

Assistant JTACs, Level 10 JTACs, are individuals designated and trained within an agency or subunit. The Assistant JTAC supports the JTAC Administrator and is authorized to perform the same duties and functions as the Level 20 JTAC.

Through the JTAC UI, the JTAC can view and manage roles of every user within that county/agency. Level 10 JTACs can only view Criminal History users within their department. Level 20 JTACs can view all Criminal History users within the County or State/Federal agency.

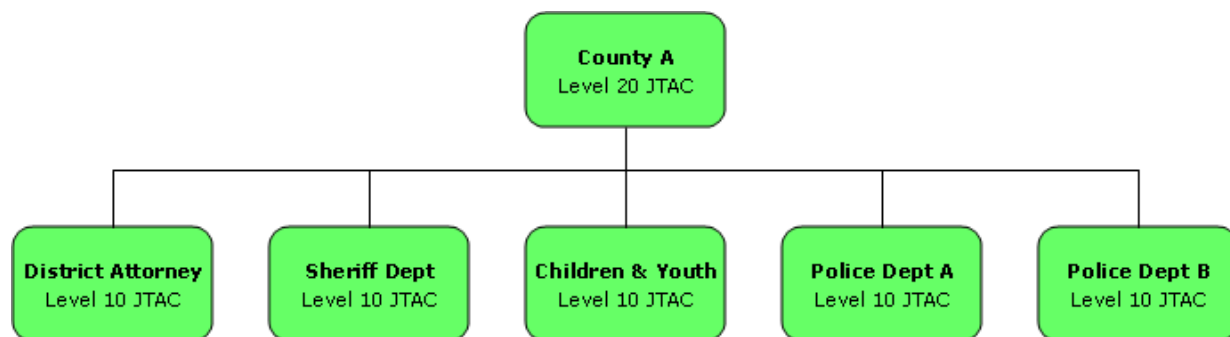


Figure 1 - JTAC Hierarchy

2.1 Accessing the JTAC Dashboard

You can access your dashboard directly from JNET Portal or from within any email notification. To access from the JNET Portal, click on Administration Tools → JNET User Provisioning System.

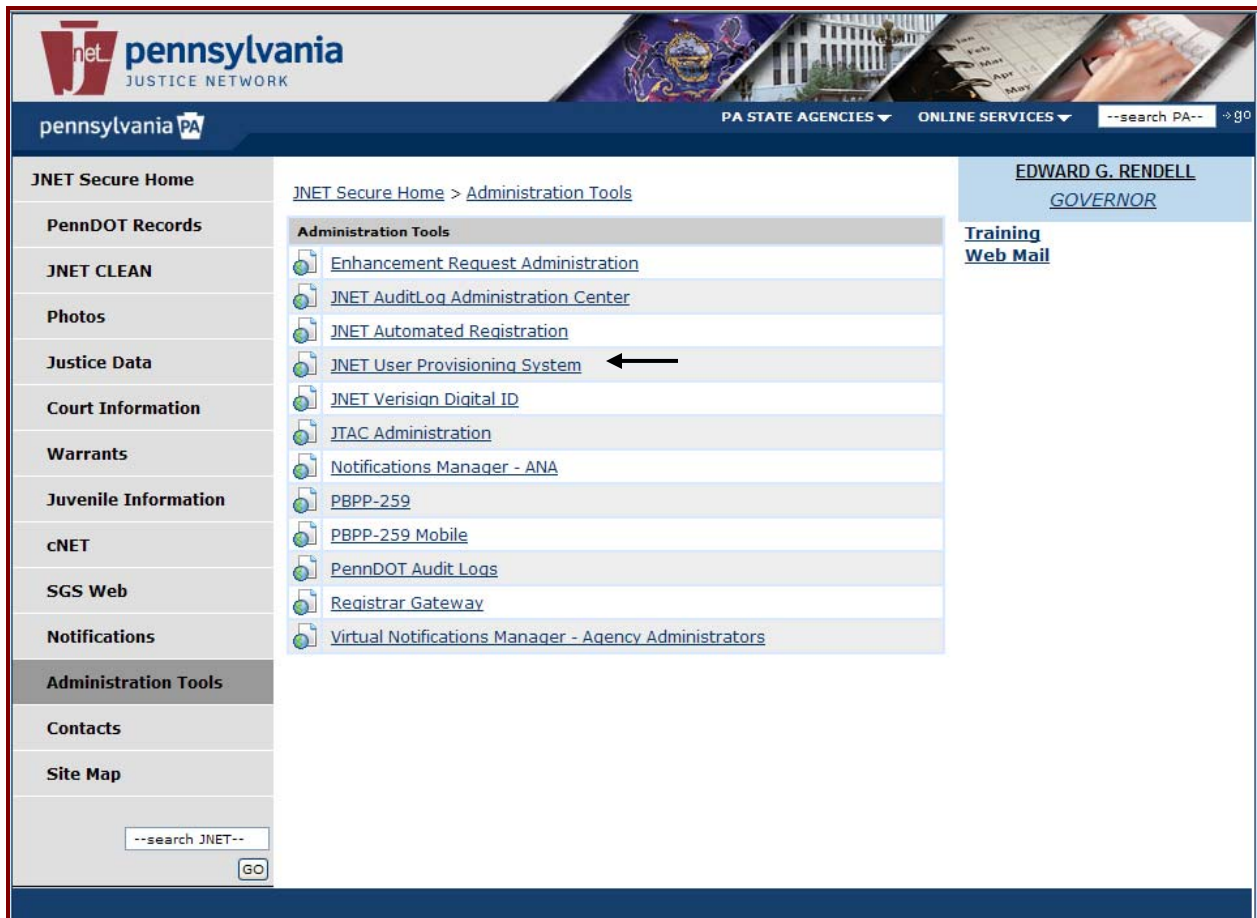


Figure 2 – JNET User Provisioning System

2.1.1 JTAC Agreement Form

In order to access the System, all JTACs must digitally sign a JTAC Agreement Form upon initial entry of the application. When you sign this form, you agree to abide by the requirements set forth by JNET Management.

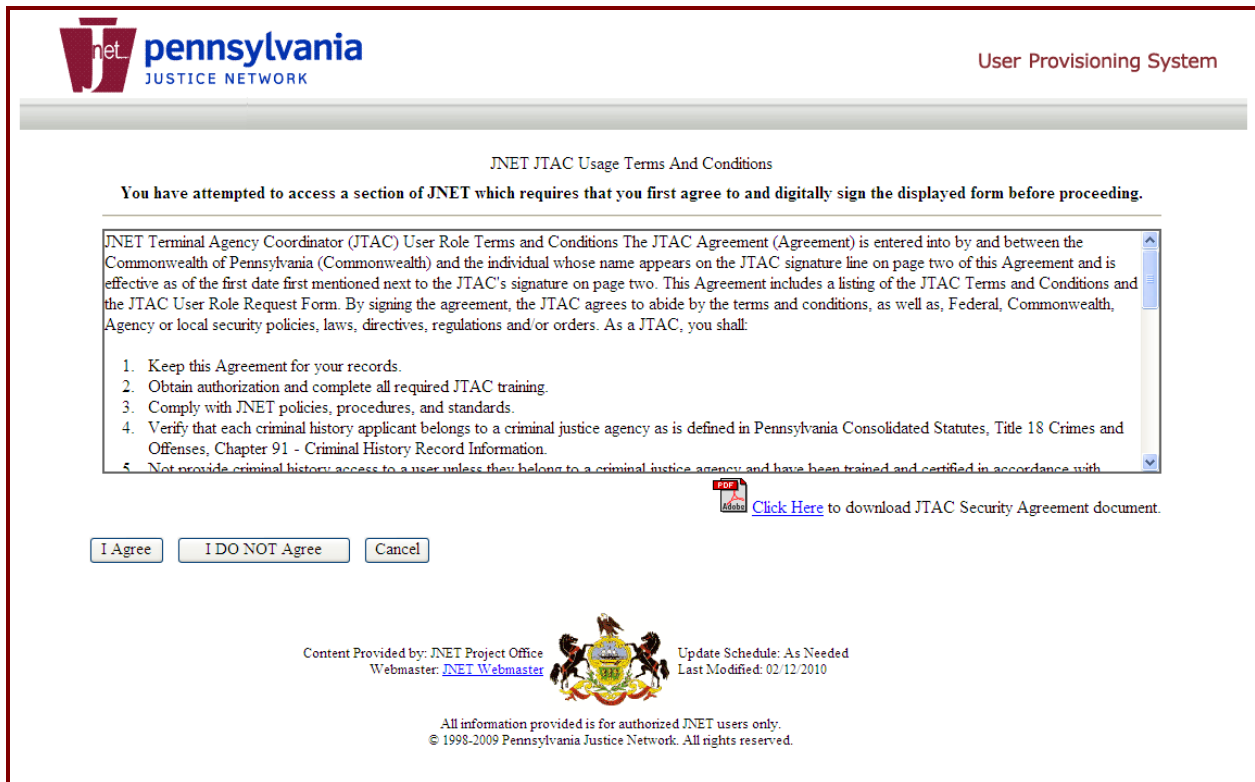


Figure 3 - JTAC Agreement Form

Read the Terms and Conditions and click the “I Agree” button to continue. Clicking the “I DO NOT Agree” or the “Cancel” buttons will exit you from the application.



Note: After signing the form, you will need to close all internet browsers and log in again. If you are also a Sponsor and/or Registrar, you will need to repeat this process for each role.

2.2 JTAC Dashboard

The JTAC dashboard is where you will go to view all your tasks or request from JNET users. The dashboard is also where you can make requests and view your own profile as well.



Figure 4 – JTAC Dashboard

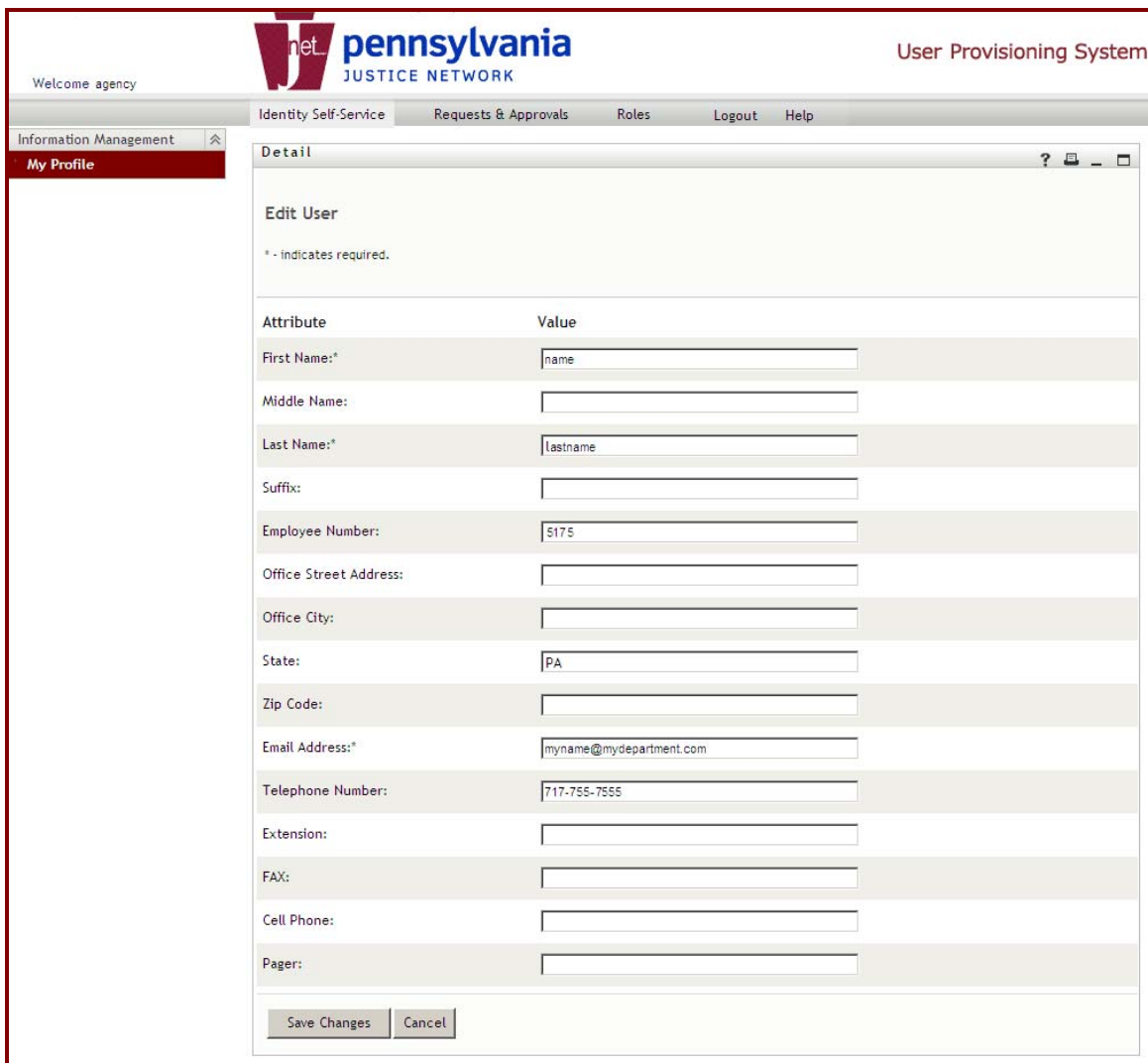
At the top of the dashboard is a menu bar: Identity Self Service, Requests & Approvals, Roles, Logout and Help.

- **Identity Self Service:** This window will display your user profile. It will list your Sponsor, department address, your email and telephone number. You can update your agency address, email and phone number at any time by clicking on [Edit Your Information](#).
- **Requests & Approvals:** This tab allows you to view your tasks, request additional JNET resources, and review the status of those requests. We will discuss this section in more detail.
- **Roles:** The Roles tab allows you to view your current level of access in JNET as well as other applications you have been granted permission to access by your sponsor. Each role assignment shows the effective date (the date you were granted permission) and the expiration date. The expiration date is only displayed for those applications that require recertification, like Criminal History; otherwise this field will be blank.

2.3 Viewing Your Profile

When the dashboard opens you will see your profile on the Identity Self Service Tab. This tab will show your full name, title, department, sponsor, email address and phone number. You can use this screen to update your profile information at any time. To update your information, click on the [Edit Your Information](#) link.

In the new window, enter or update your information. When you are done, click the Save Changes button located at the bottom of the screen.



Welcome agency

Information Management

My Profile

Identity Self-Service | Requests & Approvals | Roles | Logout | Help

User Provisioning System

Detail

Edit User

* - indicates required.

Attribute	Value
First Name:*	<input type="text" value="name"/>
Middle Name:	<input type="text"/>
Last Name:*	<input type="text" value="lastname"/>
Suffix:	<input type="text"/>
Employee Number:	<input type="text" value="5175"/>
Office Street Address:	<input type="text"/>
Office City:	<input type="text"/>
State:	<input type="text" value="PA"/>
Zip Code:	<input type="text"/>
Email Address:*	<input type="text" value="myname@mydepartment.com"/>
Telephone Number:	<input type="text" value="717-755-7555"/>
Extension:	<input type="text"/>
FAX:	<input type="text"/>
Cell Phone:	<input type="text"/>
Pager:	<input type="text"/>

Save Changes | Cancel

Figure 5 - Edit Profile

After your changes are saved, the Cancel button will change to a Return button. Click the Return button go back to the Identity Self Service Tab.

3 Criminal History Access Requests

The Requests & Approvals Tab will show you any Criminal History (CH) requests made by a JNET user which has been approved by their sponsor. This section will cover how to approve a request for Criminal History access.

3.1 Requesting Criminal History Access

In order for an individual to request Criminal History access, they must already have access to JNET. All users should go through an automated process to request this role.

After a user has access to JNET and determines they need Criminal History access, the user must take the following steps:

- Complete the JNET Criminal History training (on-line through the Learning Management System (LMS) or an Instructor-Led training) or
- Complete the PSP CLEAN training and
- Request approval from their Sponsor.

Upon sponsor approval, you will receive a notification. The notification will tell you who is making the request and have a link embedded that will take you to the application to view the details of the request. From there you will be able to approve or deny the request.

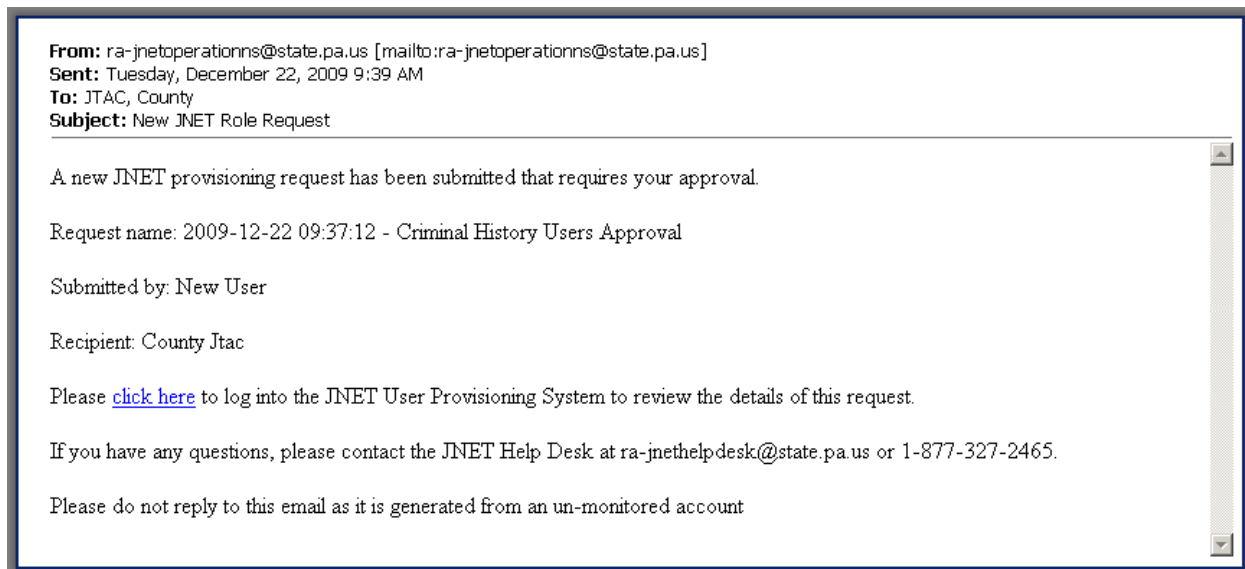


Figure 6 - JTAC Notification

Click on the link in the email notification to access the User Provisioning System. You may also access the System directly from JNET Portal → Administration Tools.

3.2 Requests & Approvals

To view new requests, click on the Requests & Approvals tab. Your menu options on the right side of your screen will change. This tab will allow you to view your tasks, request new resources (JNET applications) and view the status of your requests.



Note: The Request Resources link is a function every JNET user has, which allows you to request additional applications (or entitlements) within JNET. To learn more, read the Auto Registration and User Provisioning System guide.

In the center of your screen you will see high level information regarding new requests waiting for your review and approval. The information includes the date and time of the request and the timeout value. The timeout value is the amount of time the system gives you to approve or deny the request before a notification is escalated to the County Sponsor or the JNET Office.



The screenshot shows the JNET Pennsylvania JUSTICE NETWORK User Provisioning System interface. The 'Requests & Approvals' tab is selected and circled. The 'My Tasks' section displays a table with the following data:

Task	Request	Recipient	Type	Claimed	Timeout	Priority
JTAC Approval	2009-12-22 09:47:12 - Criminal History Users	New A User			0 Days 0 Hours 56 Minutes	

Below the table, it indicates '1 - 1 of 1' and a 'Refresh' button is visible.

Figure 7 - My Tasks

3.3 Request Timeouts

Every request is given a timestamp. This ensures that all requests are reviewed within a timely fashion. The normal timeout for any request is 15 days. As an agency JTAC you have 15 days to respond to a user's request for new resources. If for some reason you do not respond, the request is escalated to the County JTAC who would then contact you to offer assistance should you require it. Ultimately the responsibility to approve or deny a user would start at the agency level.

3.4 Claim the Request

In order to respond to a request, you must first claim it. Claiming the request allows you to take action on the request. To claim, click on the **JTAC Approval** link within the window. The task will open and display detail information about the request.

By claiming the task, the system gives you the authority to approve or deny the request. All requests are handled using the same procedure. Claim the request, review and verify the information, attest the information is correct and then approve or deny the request.

Welcome agency jtac

Identity Self-Service | Requests & Approvals | Roles | Logout | Help

My Work

- My Tasks
- Request Resource
- My Requests
- My Settings
- Enter Proxy Mode
- Edit Availability
- My Proxy Assignments
- My Delegate Assignments

My Tasks

Task Detail

* - indicates required.

Request: 2009-12-22 09:47:25 - Criminal History Users Approval Recipient: New A User

Requested By: New A User Task: JTAC Approval

In Queue since: 12/22/2009 09:37:12 PM Timeout on: 01/22/2010 03:55:15 PM

Assigned To: agency jtac Claimed By:

Claim **Release** **Reassign** **Print Form** **Back**

JTAC Claim

Form Detail

JTAC Role Approval
Please select the button to approve or deny this request.

Request Number: 37e78a69168a44ba94d0108d9db3a7d7 CurrentStatus: Processing

Role: Criminal History Users Location: 1101 S. Front St. Suite 5400

Recipient: Agency Jtac

Department: Central Office Date of Birth: 02/02/1985

Soc. Sec. No.: 111-22-3333 CLEAN Cert. Date: 08/24/2009 CLEAN Expiration: 08/24/2011

Agency ORI: CLEAN: I certify that this individual is JNET Criminal History or PSP CLEAN certified and that the CLEAN certification expiration date above is accurate (two years from the CLEAN exam date).

Fingerprints: I confirm that this individual has been fingerprinted in compliance with CLEAN Administrative Regulations and JNET Policies and Procedures.

Criminal History: I confirm that I have completed a criminal background check on the above recipient and there are no violations as defined by the CLEAN administrative regulations or the JTAC manual that would prohibit access to CHRI.

Comment:

Attestation: By approving this request, I hereby certify, to the best of my knowledge, the above information is true and accurately reflects the individual's status on the date of this approval.
 I am affirming that the above request is valid and complies with the policies and procedures of the Pennsylvania Justice Network.

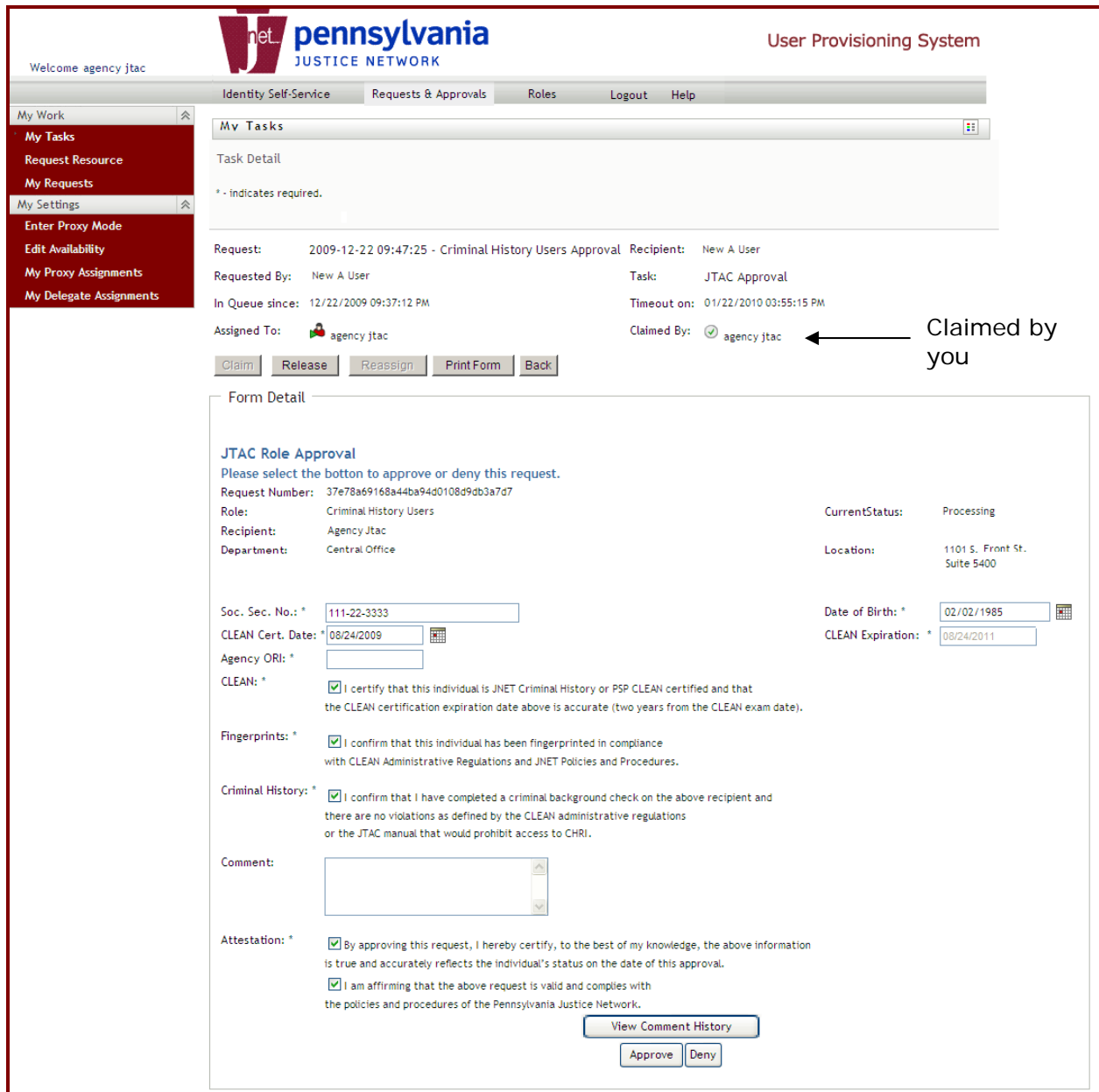
View Comment History

Approve **Deny**

Applicant Information

Figure 8 - Request Details

At the top of the form, click the Claim button to take ownership of the request. You will notice that the status of the request will change to show the request has been claimed by you.



Welcome agency jtac

Identity Self-Service | Requests & Approvals | Roles | Logout | Help

My Work

- My Tasks
- Request Resource
- My Requests
- My Settings
- Enter Proxy Mode
- Edit Availability
- My Proxy Assignments
- My Delegate Assignments

My Tasks

Task Detail

* - indicates required.

Request: 2009-12-22 09:47:25 - Criminal History Users Approval Recipient: New A User

Requested By: New A User Task: JTAC Approval

In Queue since: 12/22/2009 09:37:12 PM Timeout on: 01/22/2010 03:55:15 PM

Assigned To: agency jtac Claimed By: agency jtac ← Claimed by you

Claim Release Reassign Print Form Back

Form Detail

JTAC Role Approval

Please select the button to approve or deny this request.

Request Number: 37e78a69168a44ba94d0108d9db3a7d7

Role: Criminal History Users CurrentStatus: Processing

Recipient: Agency Jtac Location: 1101 S. Front St. Suite 5400

Department: Central Office

Soc. Sec. No.: * 111-22-3333 Date of Birth: * 02/02/1985

CLEAN Cert. Date: * 08/24/2009 CLEAN Expiration: * 08/24/2011

Agency ORI: *

CLEAN: * I certify that this individual is JNET Criminal History or PSP CLEAN certified and that the CLEAN certification expiration date above is accurate (two years from the CLEAN exam date).

Fingerprints: * I confirm that this individual has been fingerprinted in compliance with CLEAN Administrative Regulations and JNET Policies and Procedures.

Criminal History: * I confirm that I have completed a criminal background check on the above recipient and there are no violations as defined by the CLEAN administrative regulations or the JTAC manual that would prohibit access to CHRI.

Comment:

Attestation: * By approving this request, I hereby certify, to the best of my knowledge, the above information is true and accurately reflects the individual's status on the date of this approval.

I am affirming that the above request is valid and complies with the policies and procedures of the Pennsylvania Justice Network.

View Comment History

Approve Deny

Figure 9 - Request Claimed & Approved

In the Form Details you can review the applicant's information, enter notes and approve/deny the request. Since this is a request for criminal history, the user has already entered in their social security number, date of birth and training certification date. As the JTAC, you will need to do the following before approving the request:

- Enter the user's JNET derivative ORI,
- Verify the user's DOB, SSN and training,
- Confirm the user has been fingerprinted,
- Complete a criminal background check.

3.5 Attestation

The final step for the approval process is to attest to the request. This is considered your digital signature and your assurance that all JNET policies and procedures have been followed.

Place a check in the box by clicking inside the box to confirm that the information has been verified. You can also add any notes in the comments box if you desire. These notes are stored in the audit database and can be viewed by you only. Once you are done, click **Approve**.

If for any reason a user is denied CH access, comments should always be entered. For reasons to deny a user access, please refer to your JTAC manual. Click **Deny** to deny the user's access.

Upon approval or denial, you will receive a confirmation page and then be allowed to go back to your tasks to view any remaining requests or exit the application.



Figure 10 - Request Approved

4 JTAC Administrative Tools

The JNET User Provisioning System includes tools that give you the ability to manage your Criminal History users. Level 20 JTACs will be able to view and manage all CH users within the County or State/Federal Agency. Level 10 JTACs will only be able to view and manage those users within their department.

To access the JTAC UI, login to the JNET User Provisioning System and click on the **Requests & Approvals** tab → **My Requests**. You will see four links available to you:

- **JNET Application Access Request:** This link is available to all JNET Users. It allows a user to request access additional resources and roles.
- **JTAC Administration:** This link will allow level 10/20 JTACs to manage Criminal History user's certifications and roles within their county/agency.

- **Re-Certification CH Role:** This link is available to all Criminal History users. After a user passes the CLEAN recertification exam, the user will use this link to request recertification from the JTAC.
- **View My Location:** This link is available to all JNET users after the migration process. View my location will allow user to correctly identify and set their agency after the migration process. This will ensure all their requests are routed to the appropriate Sponsor, Registrar and JTAC.

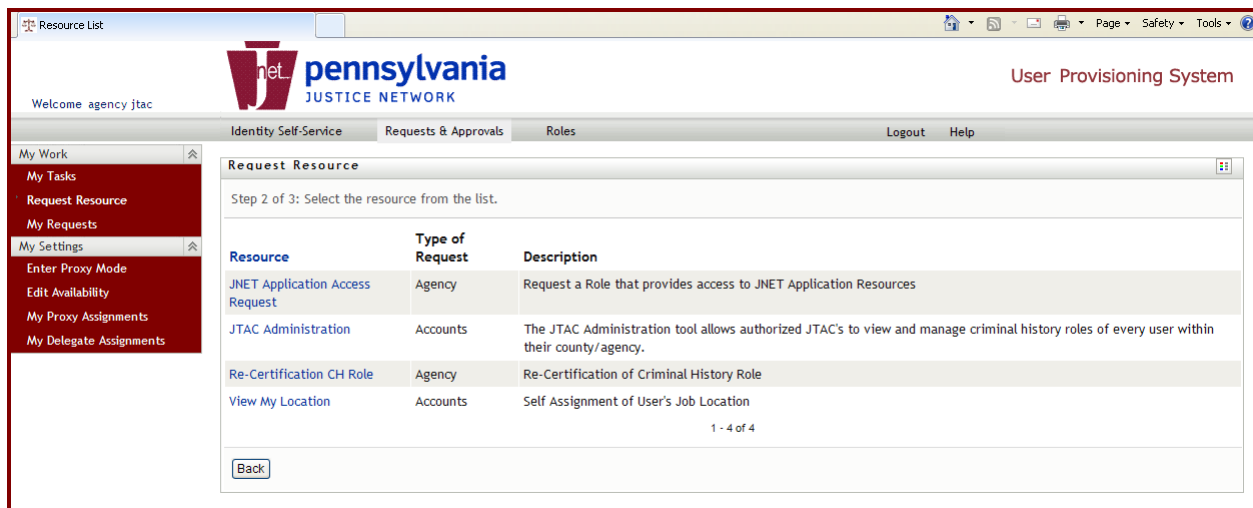


Figure 11 - Request Resource Links

4.1 JTAC Administration

The JTAC Administration function is the JTAC User Interface (UI). It will allow you to manage user's roles. As a JTAC, you will be able to downgrade a user security clearance role from Criminal History to any of the following roles:

- Criminal Justice
- Non-Criminal Justice
- None

To access the tool, click **JTAC Administration** from the **Requests & Approvals** tab → **Request Resource**.

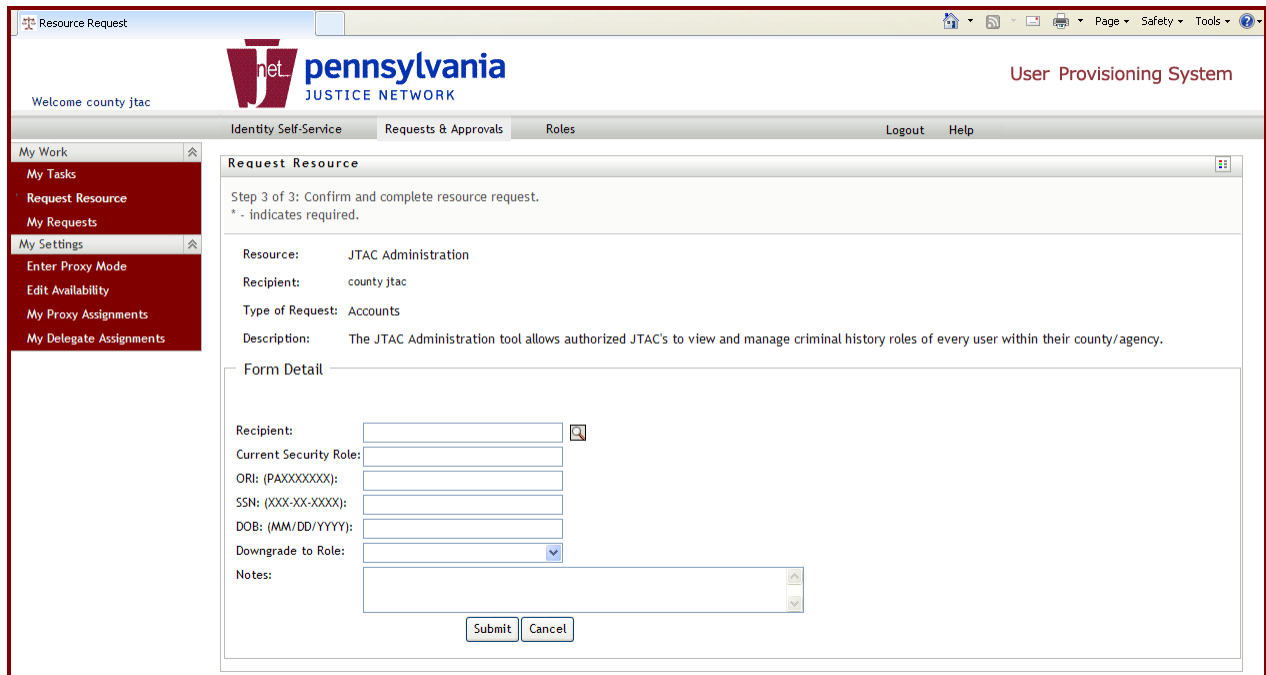


Figure 12 - NEW JTAC UI

4.1.1 Downgrading Users

To downgrade, search for the user by clicking the magnifier located at the end of the Recipient field. A small window will open.

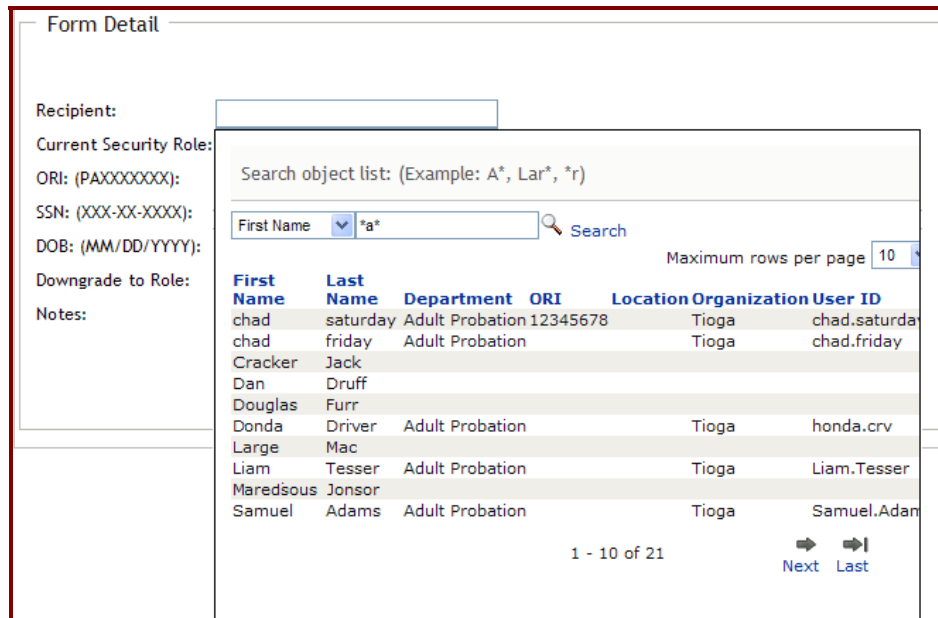
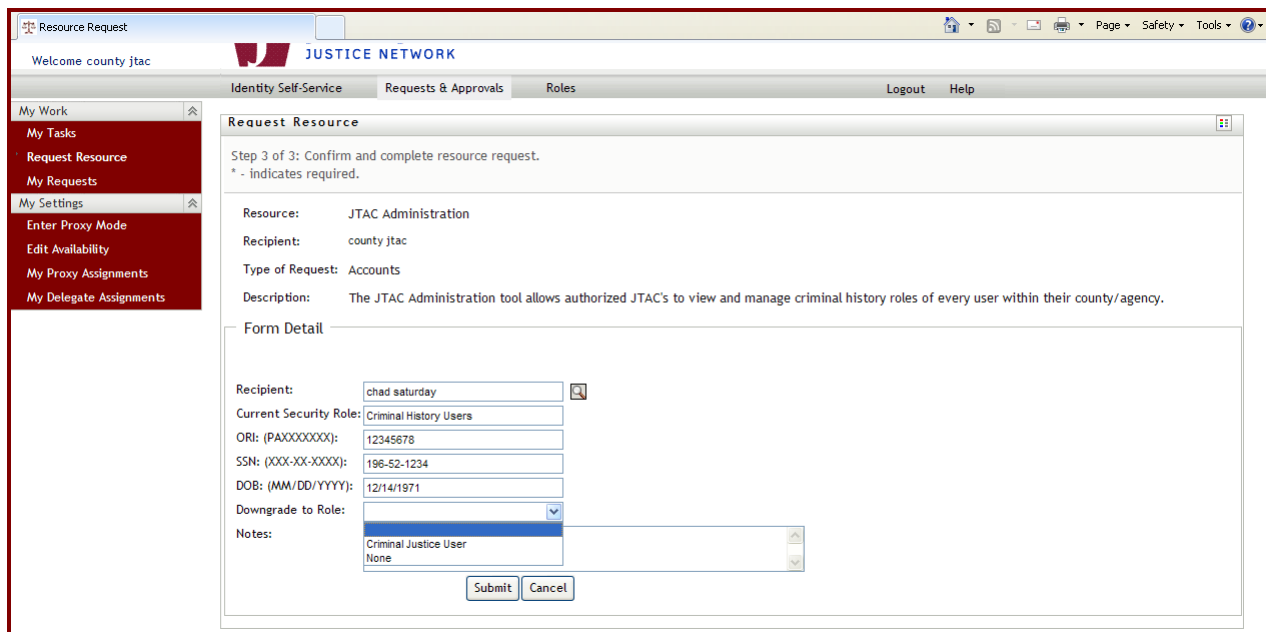


Figure 13 - Person Lookup

By default the window asks for the First Name of the user, however you can also search by Last Name, Department, ORI, Location, Organization or User ID. To select one of these options, click the drop down menu and choose the desired search criteria. If you are not

sure how to spell a name, you can use the "*" as a wildcard. Click on the name of the person you wish to manage. The user's information will populate the fields. Choose the role you want to downgrade and click **Submit** to make the changes.



The screenshot shows a web browser window titled "Resource Request" with the "JUSTICE NETWORK" logo. The page content includes a navigation menu on the left with options like "My Work", "Request Resource", and "My Settings". The main area is titled "Request Resource" and shows "Step 3 of 3: Confirm and complete resource request." The form fields are as follows:

- Resource: JTAC Administration
- Recipient: county jtac
- Type of Request: Accounts
- Description: The JTAC Administration tool allows authorized JTAC's to view and manage criminal history roles of every user within their county/agency.
- Form Detail:
 - Recipient: chad saturday
 - Current Security Role: Criminal History Users
 - ORI: (PAXXXXXXX): 12345678
 - SSN: (XXX-XX-XXXX): 196-52-1234
 - DOB: (MM/DD/YYYY): 12/14/1971
 - Downgrade to Role: Criminal Justice User
 - Notes: Criminal Justice User

Figure 14 – User Downgrade



Note: In the JTAC UI you also have the ability to update or correct a user's information (ORI, SSN, or DOB) without downgrading the user. To achieve this function, leave the Downgrade to Role field should blank.

4.1.2 User Reinstatement

If a user needs to be reinstated, you will need to remove the role of "None" and add the appropriate role. For example, if the user works for a Criminal Justice agency, you should assign the role of cj user. Likewise, if the user works for a Non-Criminal Justice agency, then non-cj user should be assigned.

If the user requires Criminal or PA Criminal History, the user must go through the process of requesting the role. As the JTAC, you are required to verify the users CLEAN certification date and run another background check. If the user's certification is expiring in 90 days or less, the user should re-certify before approving their access. If you have additional questions on reinstatement, please contact your MTAC at the JNET Office.

4.1.2.1 Removing and Assigning Roles

As a JTAC you also have the entitlement of "Role Manager". Role management gives you the ability to manage your user's security clearances. You can view, add and remove a security clearance. The options are selectable by Role and User. The Group and Container options are restricted and are only accessible to the JNET Role Module Administrator.

Because you are a Role Manager, you will be able to see all roles within the system for your county/agency; however you are only authorized to manage Criminal History users for

purpose of downgrading and reinstating. Any other usage would be a violation of policy and you may be subject to termination of access by the JNET MTAC.

To reinstate a user, click on the Roles tab in the User Provisioning System. By default the system will automatically show all of your roles.

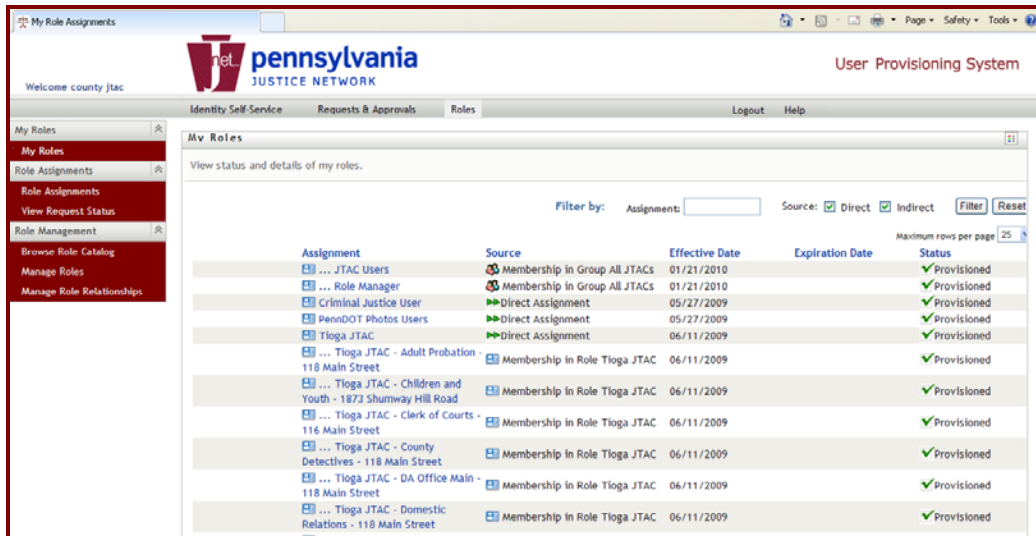


Figure 15 - Roles Tab

From the right side menu, click **Role Assignments** then click on the **User** icon.

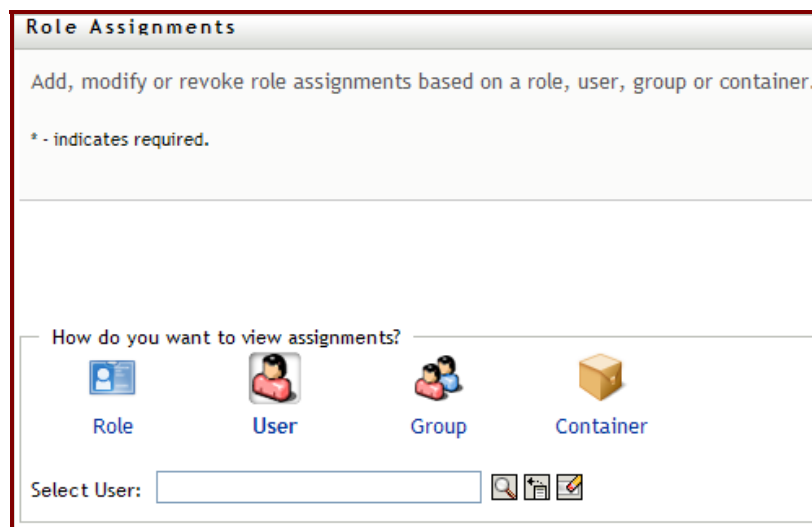


Figure 16 - View Assignments Icons

Click the magnifier icon to search for your user. Enter the user's first name and click search. Click on the user's name for the list. All the roles currently assigned to the user will be displayed.

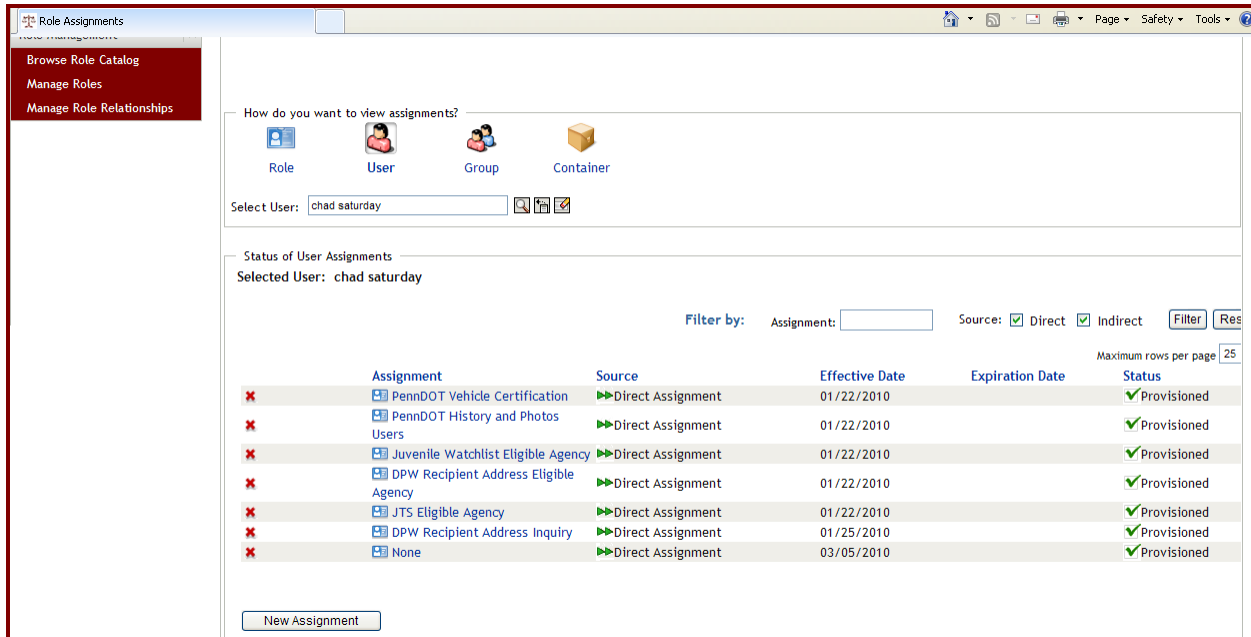


Figure 17 - View User's Roles

This user has been downgraded to None. To remove the role, click the red **X** located at the beginning of the row. Since this removal is permanent, you will be presented with a confirmation alert.

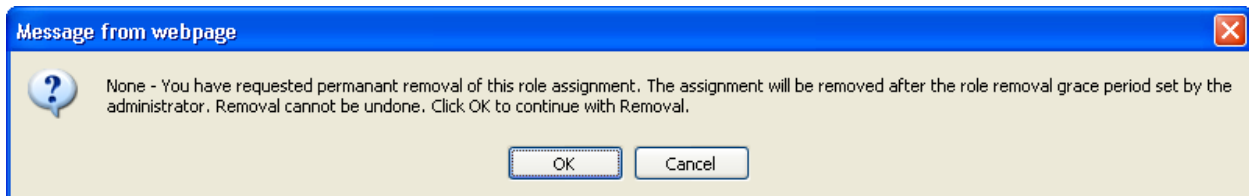


Figure 18 - Removal Confirmation

To confirm, click **OK**; otherwise click **Cancel**. When you click OK, a script will run to remove the role. Click OK to run the script.

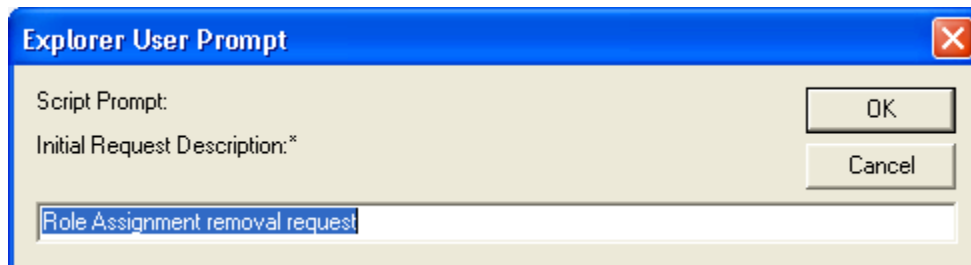


Figure 19 - Role Assignment Removal Script

Now that you have removed the role of 'None', you must assign another security clearance role to give the user access. Click the New Assignment button located below the list of roles.

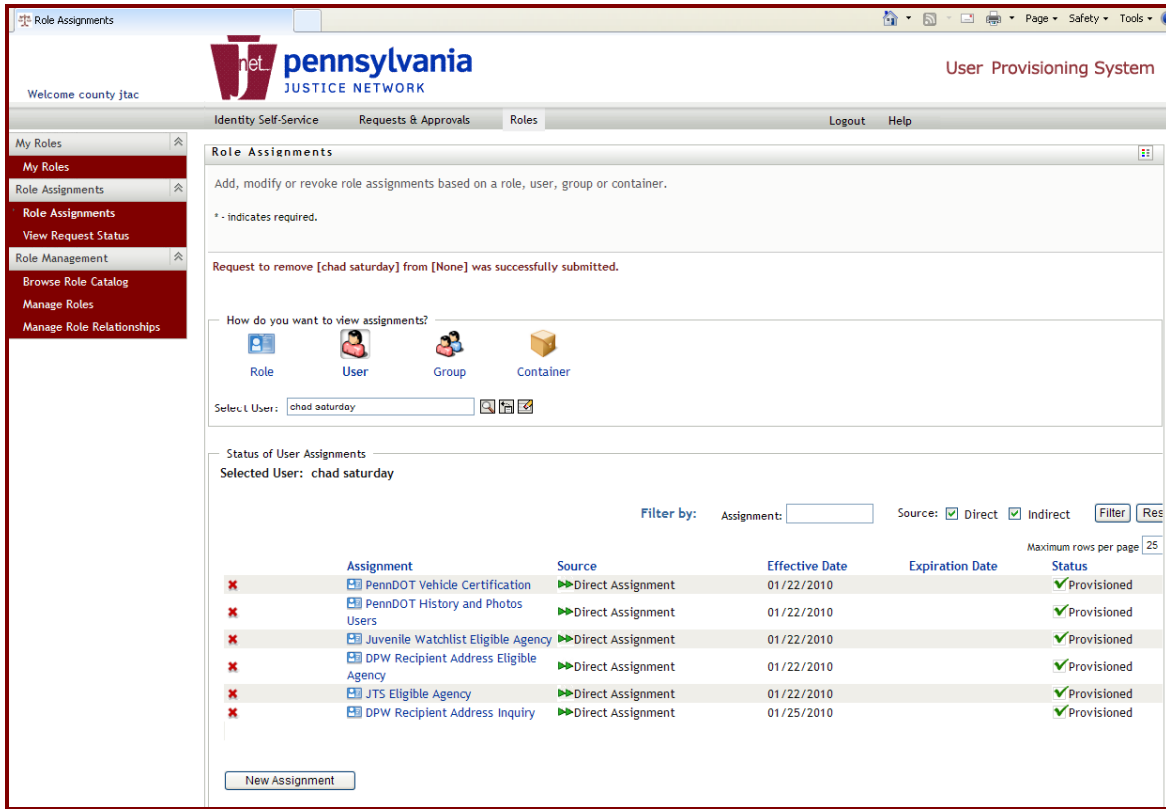


Figure 20 - User Assignments

A new form will appear directly below it. Enter the reason for the request. To assign the role click the magnifier icon located next to the Select Role(s) field. A search window will appear.

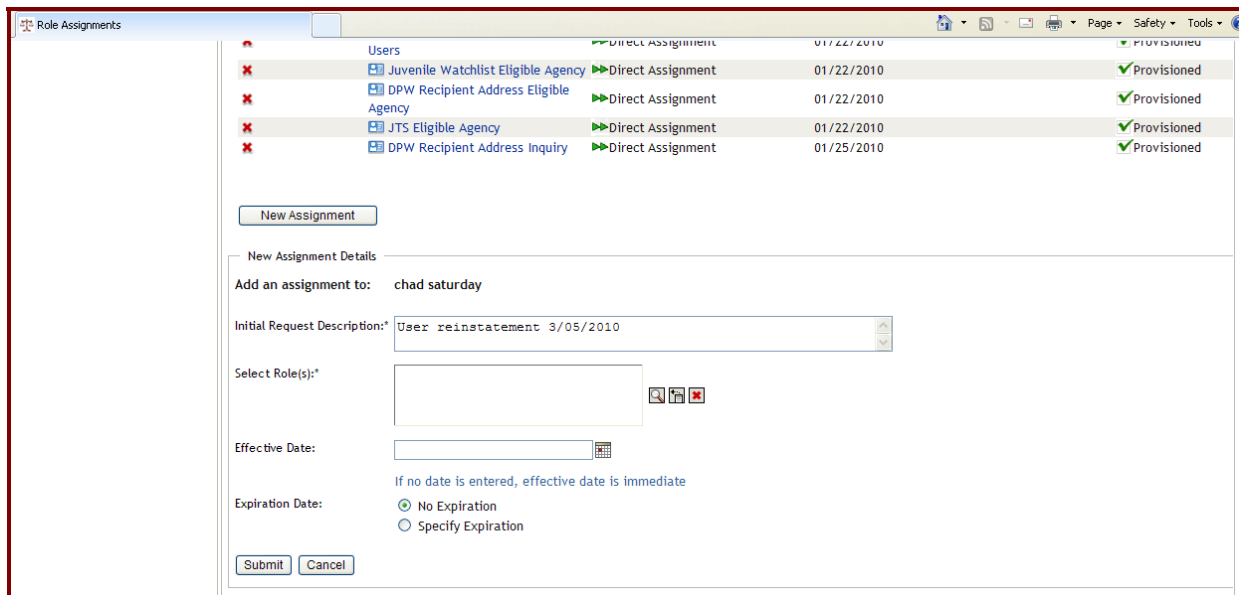


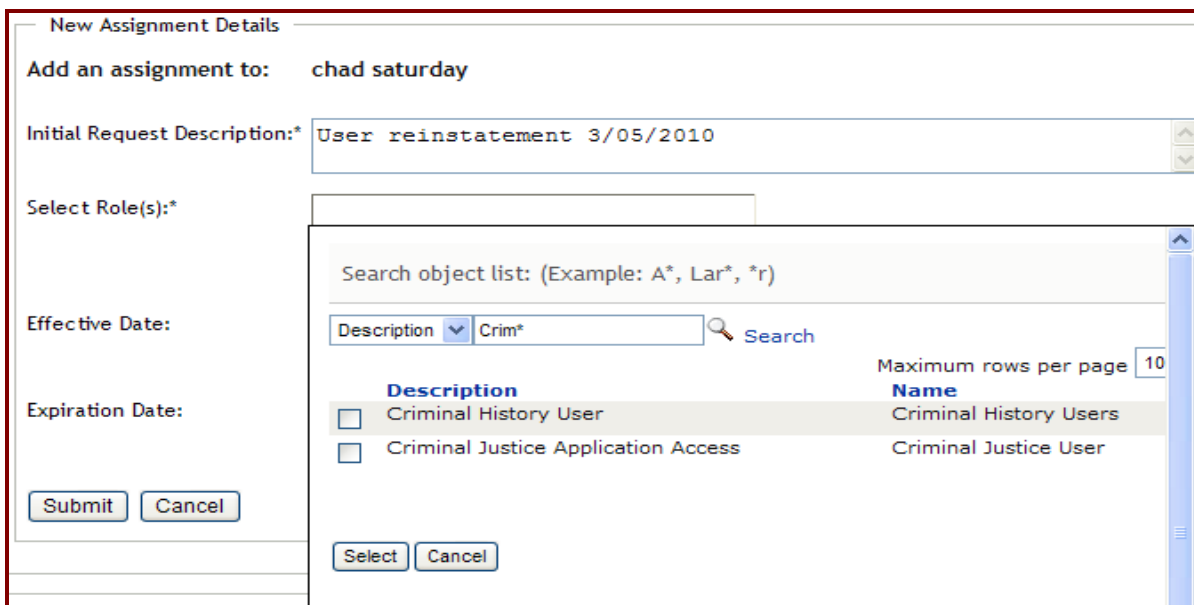
Figure 21 - Role Assignment Form

Enter the role you are assigning. Description is the default search criteria when searching by role; however you can also search by the Name (of the role). The search options allow for multiple wildcards (*) to help you find roles more easily.



Note: the search fields for Roles **ARE** case sensitive. For reference, it may be helpful to print out a role report so the exact naming can be easily identified.

Enter the first few letter of the role and use the wildcard (*) simplify the search. Check the Criminal Justice Application Access role and click Select. The role Criminal Justice User is added to the form.



The screenshot shows a web form titled "New Assignment Details". The "Add an assignment to:" field contains "chad saturday". The "Initial Request Description:" field contains "User reinstatement 3/05/2010". The "Select Role(s):" field is empty. The "Effective Date:" and "Expiration Date:" fields are empty. There are "Submit" and "Cancel" buttons at the bottom left. A search modal is open, showing a search object list with the criteria "Crim*". The search results are as follows:

Description	Name
<input type="checkbox"/> Criminal History User	Criminal History Users
<input type="checkbox"/> Criminal Justice Application Access	Criminal Justice User

At the bottom of the search modal are "Select" and "Cancel" buttons. The "Maximum rows per page" is set to 10.

Figure 22 - Search for Role(s)

User the calendar option to enter the date effective (or type it in directly) and click **Submit**. The role Criminal Justice User is added to the user's profile.

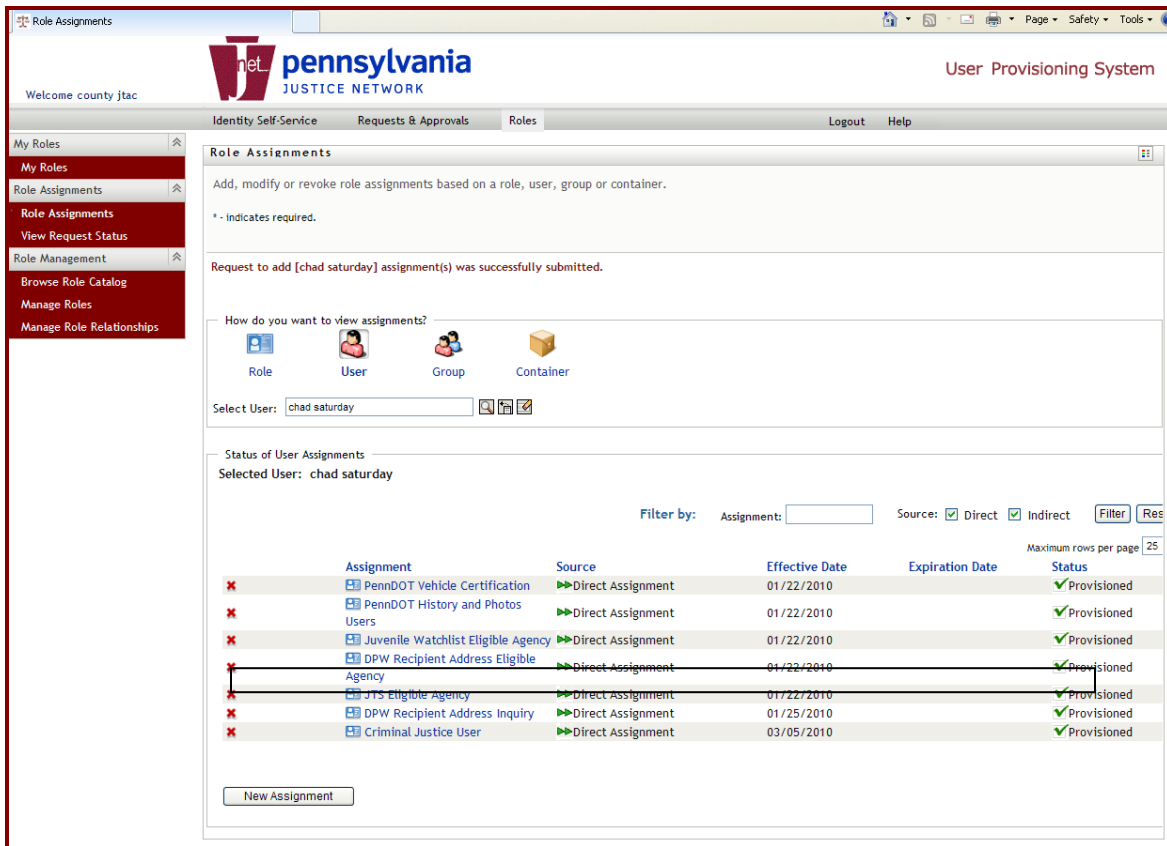


Figure 23 - User Role Assignments

4.2 Re-certification CH Role

All CH users must recertify every two years to retain access to JNET CLEAN. Once users complete the Criminal History Recertification exam in the LMS, they apply for recertification using the JNET User Provisioning System.

To apply your user will click on the Re-Certification CH Role and enter their CLEAN certification date and comments. The CLEAN certification date will be the date they passed the Re-certificate exam in the LMS.

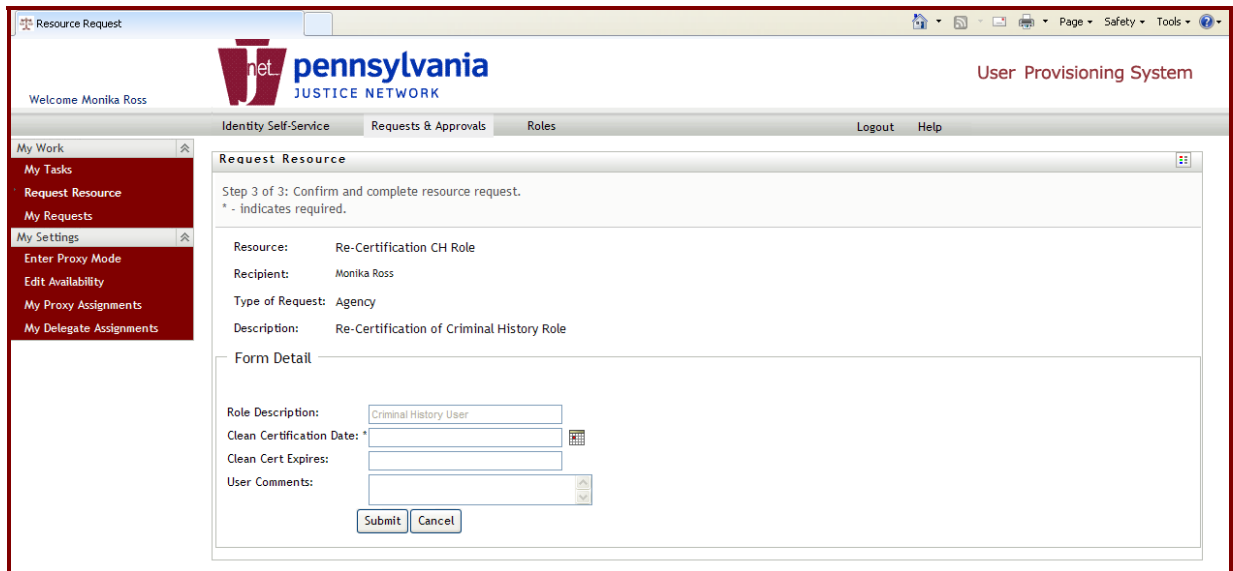


Figure 24 – User Re-certification Request

Once they submit the request, you will be notified of the request through email. Click on the embedded link to access the JNET User Provisioning System and view the user's information.

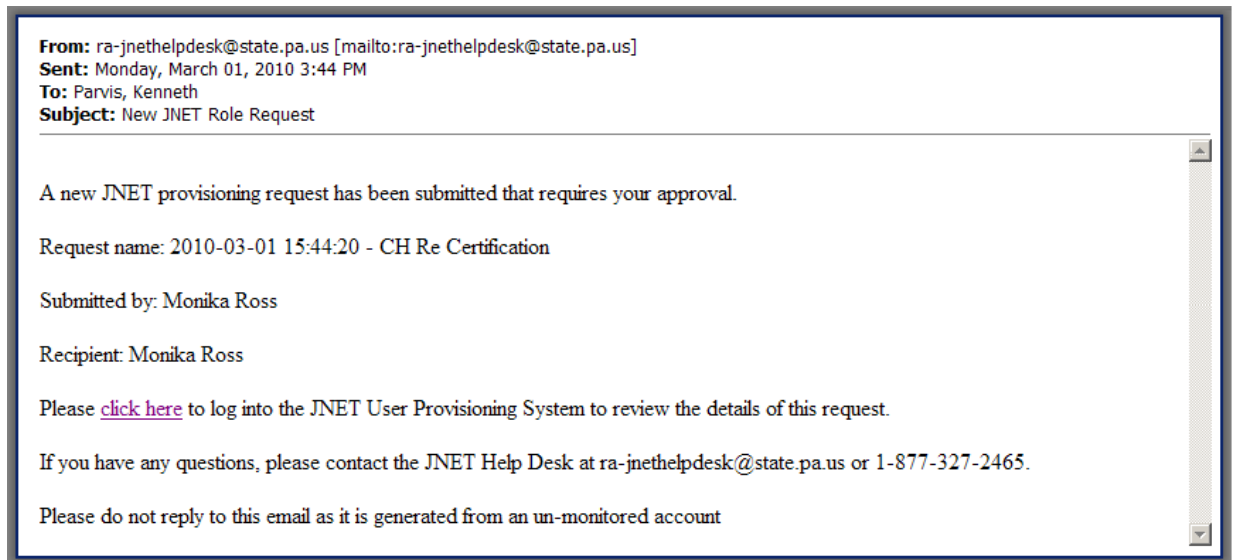


Figure 25 - Re-certification Notification

Follow the same steps in Section 3 to review and approve/deny the request.

5 JNET Help Desk

Should you need further assistance, please contact the JNET Help Desk toll free at (877) 327-2465, locally at (717) 783-5164 or by e-mail at: ra-jnethelpdesk@state.pa.us. The Help Desk is available Monday - Friday from 7:00 AM - 4:00 PM, excluding Commonwealth holidays.