Time Entry and Security Setup Process

This job aid contains the steps to initiate time entry and approval routing security.

I. Initiate Time Entry Security and Setup
II. Request Security Profiles in the Security Application
III. Review and Modify Time Approval Routing Queue
IV. Situations to Avoid

Position definitions

There are three key unit roles involved in the time entry and approval routing security setup process:

Human Resources/Payroll Contact/Business Manager: Coordinates the approval routing security setup for a unit's human resources and payroll functions

Superuser: Changes or approves all time transactions either in Employee Self-Service or **PHATIME**

Unit Security Contact (USC): Initiates security access requests and changes

I. Initiate Time Entry Security and Setup

The time entry and security setup has several interrelated pieces. Each of these pieces should be coordinated between the USC and Administrative IT Systems and Services (AITS).

New TS-Orgs

The TS-Org is used by the USC in the security profile requests. The individuals in your unit who are being assigned time entry and approval roles will also need security access to the TS-Org. AITS will also use the TS-Org information to set up the time approval routing queue in ***NTRRQUE***. If the unit chooses to create separate time approval routing queues by TS-Org, the unit should identify an unused Banner Org Code related to their department which can be assigned as a new TS-Org.

Adjustment Notification Application Security for the New TS-Org

If your unit decides to add a new TS-Org and time approval routing queue, your USC will need to request the appropriate security related to the ***Adjustment Notification Application (ANA)*** so that any ***ANA*** based transactions (e.g., overpayment adjustments, leave balance requests) for employees moved to the new TS-Org can be processed.

Your USC will submit a request to designate a **Department Workflow Originator** and a **Department Workflow Approver** for each new TS-Org through the ***Security Application***.

If the unit does not have an unused org code, a new Banner Org Code can be requested from University Accounting and Financial Reporting by filling out and submitting Banner Organization Code Request Form to cfoapalmaintenance@uillinois.edu.

PARIS Security for New TS-Org

Your USC will need to request the appropriate security related to ***PARIS***. New ***PARIS*** users need to complete training before your USC can request the ***PARIS PUA*** security profile. More information can be found at the ***PARIS Resource*** page.

1. Search for Unused Banner Org Codes

1) Access the ***Unused FOPAL Codes*** report at https://www.obfs.uillinois.edu/accounting-financial-reporting/reports/foapal-maintenance/.
2) Click the **Unused Organization Codes** link.
3) Type your **ID** and **Password**.
4) Click the **Login** button.
5) Click the **Open** button.
6) Click the **Enable Editing** button.
7) Click the **Chart & Dept** filter button.
8) Select the appropriate Chart & Dept to display the unit's unused organization codes. Write down the org code to be used for a new TS-Org.

    NOTE: If the unit does not have an unused org code, a new Banner Org Code can be requested from University Accounting and Financial Reporting by filling out and submitting Banner Organization Code Request Form to cfoapalmaintenance@uillinois.edu.

9) Close the Unused-Organization-Codes.xlxs file when finished.

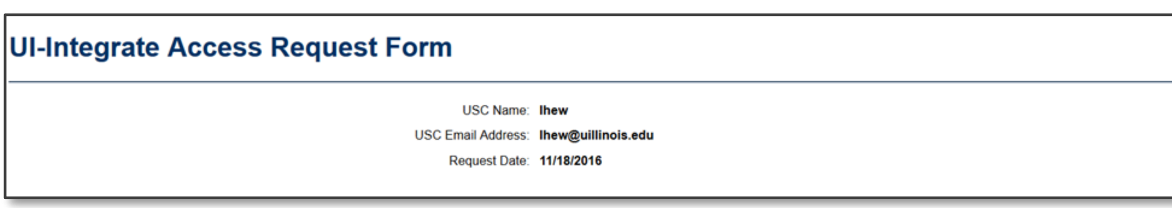
2. Request Security Profiles in the Security Application

Before a time entry routing queue is created, the USC submits the security requests for the time entry roles. If the individual is being granted Banner HR access for the first time, the USC must also request the appropriate organization and employee class (e-class) access. The USC submits these security requests through the ***Security Application*** found on the ***Unit Security Contact (USC) Website***.

1. Login to the Security Application

1) Go to https://www.aits.uillinois.edu/access/usc_website.
2) Type your **ID** and **Password**.
3) Click the **Login** button.

The ***Security Application*** will display the USC name, email address and the request date *(see Figure 23)*.



UI-Integrate Access Request Form

USC Name: **lhew**
USC Email Address: **lhew@uillinois.edu**
Request Date: **11/18/2016**

Figure 23

2. Initiate an Employee Access Request

The USC will provide their department information to direct the security profile request to the appropriate university authorization group and the UIN of the employee *(see Figure 24)*.

1) Select the **Campus**.
2) Select the **College** code.
3) Select the **Department** code.
4) Select the Physical Campus.
5) Type the employee **UIN**.
6) Click the **Retrieve** button.

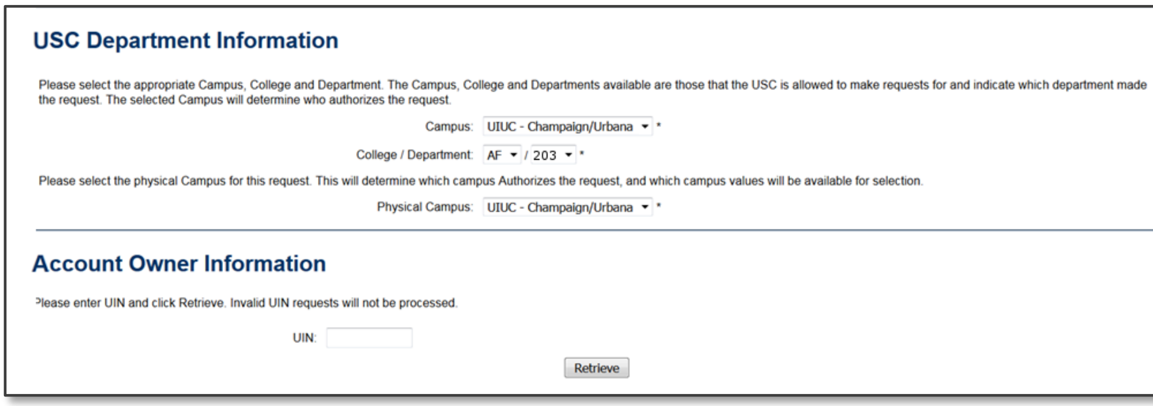


Figure 24

3. Review and Complete the Security Compliance Statements

With every security profile request, the USC must review and complete the security compliance statements *(see Figure 25)*.

1) Select the checkbox to confirm the department has a signed copy of the *Information Security Compliance Form* on file.

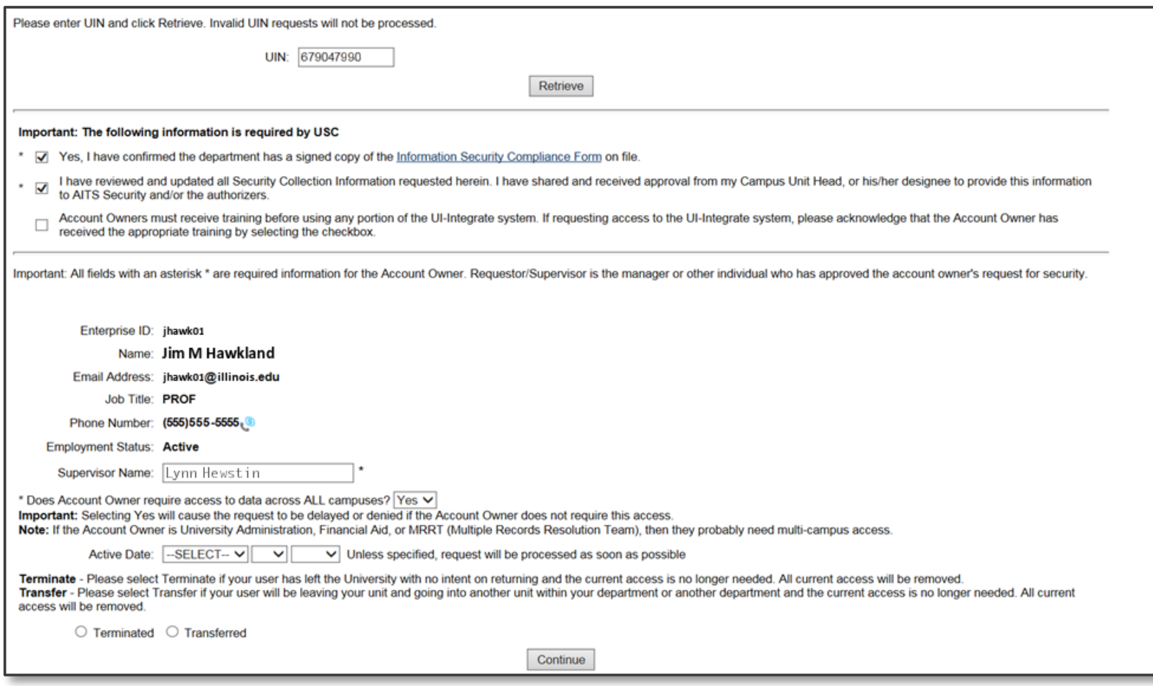
2) Select the checkbox to confirm all of the requested *Security Collection Information* has been updated, and submission of the information has been approved.

3) Type the **Supervisor Name**.

4) Select **Yes** or **No** for Account Owner access across ALL campuses.

5) Select the **Active Date** for the security profile request (Month, Day, Year).

6) Click the **Continue** button to proceed with the **Time Entry** security profile request(s).



Please enter UIN and click Retrieve. Invalid UIN requests will not be processed.

UIN: 679047990

Retrieve

Important: The following information is required by USC

* ☑ Yes, I have confirmed the department has a signed copy of the Information Security Compliance Form on file.
* ☑ I have reviewed and updated all Security Collection Information requested herein. I have shared and received approval from my Campus Unit Head, or his/her designee to provide this information to AITS Security and/or the authorizers.

☐ Account Owners must receive training before using any portion of the UI-Integrate system. If requesting access to the UI-Integrate system, please acknowledge that the Account Owner has received the appropriate training by selecting the checkbox.

Important: All fields with an asterisk * are required information for the Account Owner. Requestor/Supervisor is the manager or other individual who has approved the account owner's request for security.

Enterprise ID: **jhawk01**
Name: **Jim M Hawkland**
Email Address: **jhawk01@illinois.edu**
Job Title: **PROF**
Phone Number: **(555)555-5555**
Employment Status: **Active**
Supervisor Name: Lynn Hewstin *

* Does Account Owner require access to data across ALL campuses? Yes
Important: Selecting Yes will cause the request to be delayed or denied if the Account Owner does not require this access.
Note: If the Account Owner is University Administration, Financial Aid, or MRRT (Multiple Records Resolution Team), then they probably need multi-campus access.

Active Date: --SELECT-- Unless specified, request will be processed as soon as possible

Terminate - Please select Terminate if your user has left the University with no intent on returning and the current access is no longer needed. All current access will be removed.
Transfer - Please select Transfer if your user will be leaving your unit and going into another unit within your department or another department and the current access is no longer needed. All current access will be removed.

○ Terminated ○ Transferred

Continue

Figure 25

4. Request E-class Access

Before requesting an e-class security profile, the USC needs to determine if the individual needs access to Master e-classes (all e-classes) or Restricted e-classes (certain e-classes i.e. BA, CC, etc). An individual cannot have both Master e-class and Restricted e-class access.

Master E-class Access Request Steps

1) Click the **UI HRPay** tab in the ***Security Application***.
2) Click the **Employee Status Access** increment link.
3) Click **Add** from the drop down in ***Action*** column for **Master Employee Class Access**. *(See Figure 26)*.
4) Click the **Save** button.
5) Click the **View/Submit Request** button if finished requesting access for this individual.

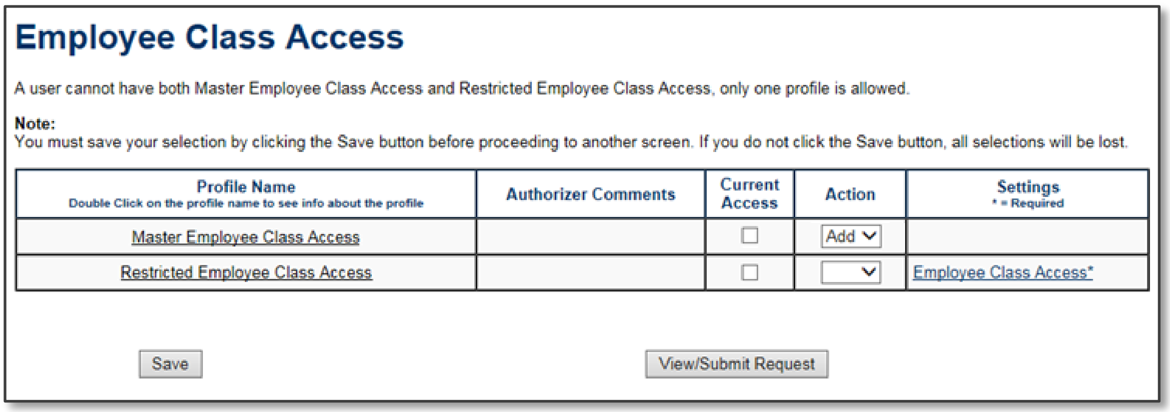


Figure 26

Restricted E-class Access Request Steps

1) Click the **UI HRPay** tab in the ***Security Application***.
2) Click the **Employee Status Access** increment link.
3) Click **Add** from the drop down in ***Action*** column for **Restricted Employee Class Access**. *(See Figure 27)*.
4) Click the **Employee Class Access** in ***Settings*** column for **Restricted Employee Class Access**.
5) Select the appropriate e-class code from the drop down.
6) Click the **Save** button.
7) Click the **View/Submit Request** button if finished requesting access for this individual.

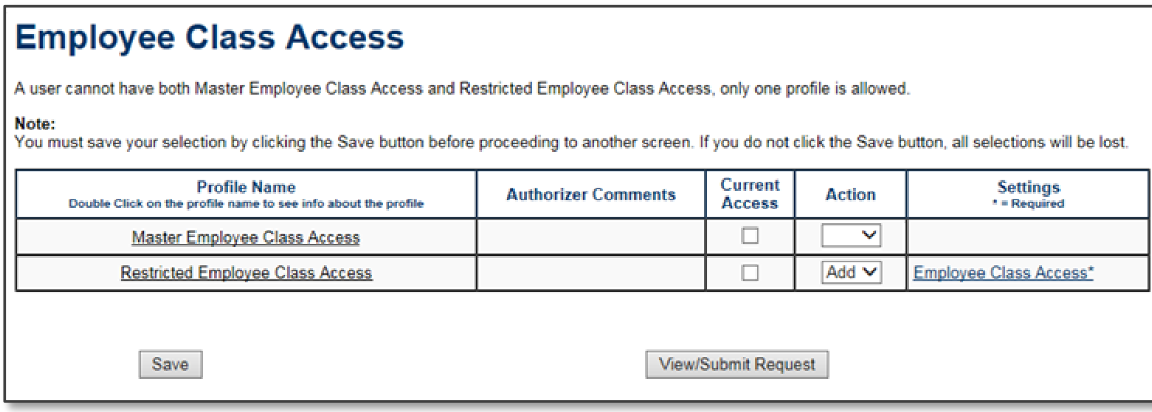


Figure 27

5. Request TS-Org Access

Determine which TS-Org(s) must be accessible to the individuals who will have time entry roles. Remember to include TS-Orgs for proxy roles.

1) Click the **UI HRPay** tab in the ***Security Application***.
2) Click the **HR Org Code Access** increment link.
3) Select **Add** from the drop down in the ***Action*** column for **Department HR Organization Level Access** *(see Figure 28).*
4) Click the **Dept Org Code Access** link in the ***Settings*** column for **Department HR Organization Level Access**.
5) Select the **Chart of Accounts** from the drop down.
6) Select the **From Organization** to choose a beginning point for a range of organization codes.
7) Select the **To Organization** to choose an end point for the range of organization codes.
8) Select **Add** in the ***Action*** column.
9) Click the **Save** button.
10) Click the **View/Submit Request** button if finished requesting access for this individual.

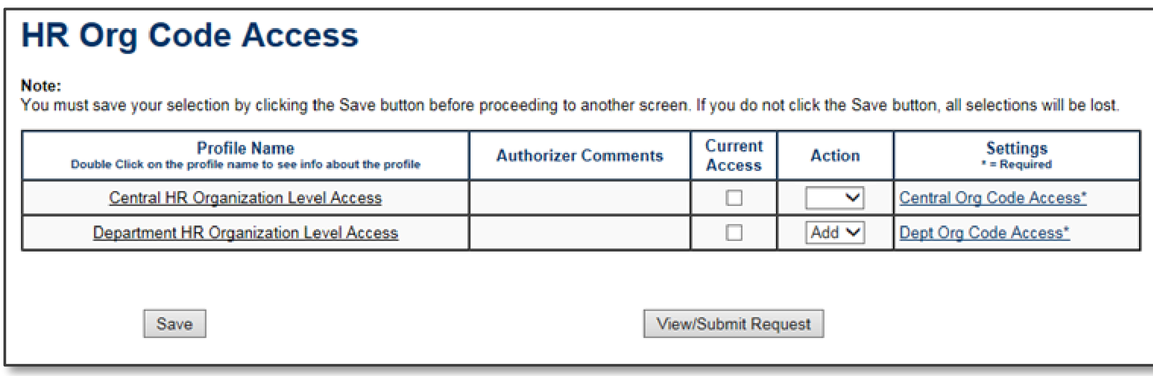


Figure 28

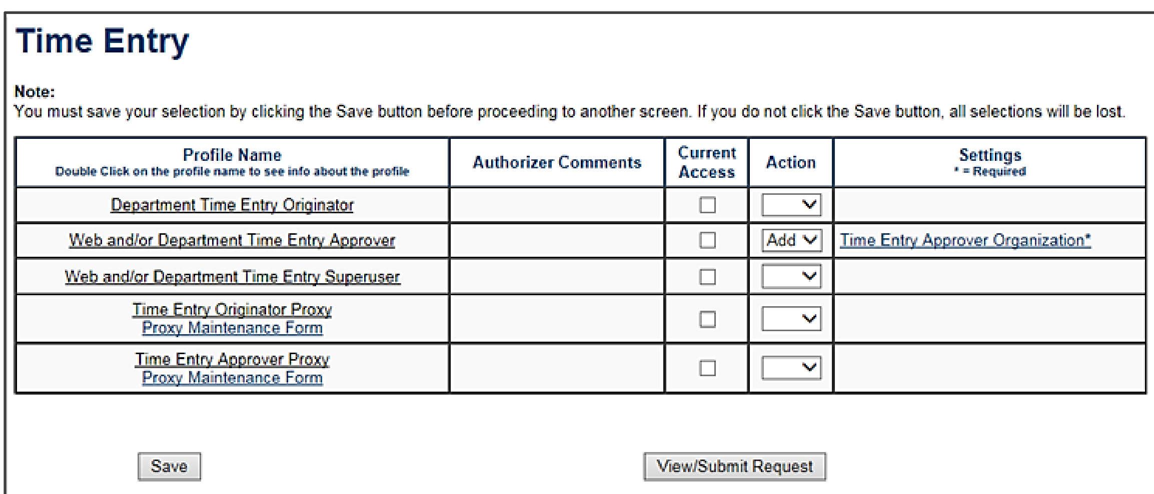
II. Request Time Entry Security Profile

For each individual with a time entry role, determine which time entry security profile is needed for their role (e.g., **Web and/or Department Time Entry Approver** or **Time Entry Approver Proxy**). For each employee with a time entry role, the preceding security steps of *Initiate Employee Access Request*, *Review and Complete Security Compliance Statements*, *Request E-Class Access*, and *Request TS-Org Access* must be completed in that order before the **Time Entry** security profile is requested.

1. Request Web and/or Department Time Entry Approver Security Profile

1) Click the **UI HRPay** tab in the ***Security Application***.
2) Click the **Time Entry** increment link.
3) Select **Add** in the ***Action*** column for **Web and/or Department Time Entry Approver** *(see Figure 29).*
4) Click the **Time Entry Approver Organization** link in the ***Settings*** column.
5) Select the **Chart of Accounts** from the drop down *(see Figure 30).*
6) Select the **Organization** from the drop down.
7) Select the checkbox for the appropriate override approver, if it appears.

   NOTE: If the **Time Approver** is a Civil Service employee who will have approval access to his/her own timesheet, this checkbox for an override approver will appear. **Time Approvers** must not approve his/her own timesheets so an override approver must be set up for the **Time Approver**'s timesheet. AITS will set up the time approval override for a Civil Service employee. The unit **Superuser** can edit the approval override or set up an approval override for a Salaried Non-Exempt Academic Professional in the **Override Routing Queue Form *(NBAJQUE)*** in ***Banner***. See the job aid, *Overriding a Routing Queue*.
8) Click the **Save** button.
9) Click the **Profiles** button.
10) Click the **View/Submit Request** button.


Time Entry

Note:
You must save your selection by clicking the Save button before proceeding to another screen. If you do not click the Save button, all selections will be lost.

Profile Name Double Click on the profile name to see info about the profile	Authorizer Comments	Current Access	Action	Settings * = Required
Department Time Entry Originator		☐		
Web and/or Department Time Entry Approver		☐	Add	Time Entry Approver Organization*
Web and/or Department Time Entry Superuser		☐		
Time Entry Originator Proxy Proxy Maintenance Form		☐		
Time Entry Approver Proxy Proxy Maintenance Form		☐		

Save   View/Submit Request

Figure 29

Time Entry Approver Organization (required)

Chart Of Accounts	Organization	Approver (Posn#-Desc-Name-PosnCoas-Orgn-Start Dt)	Action
1 - University of Illinois - Urbana	203000 - Chemistry	U56852 - PROFESSOR - 1-203000 08/16/2016	Add

Save Profiles

Figure 30

2. Request Web and/or Department Time Entry Superuser Security Profile

1) Click the **Time Entry** increment link.
2) Select **Add** in the ***Action*** column for **Web and/or Department Time Entry Superuser** *(see Figure 31).*
3) Click the **Save** button.
4) Click the **View/Submit Request** button.

Time Entry

Note:
You must save your selection by clicking the Save button before proceeding to another screen. If you do not click the Save button, all selections will be lost.

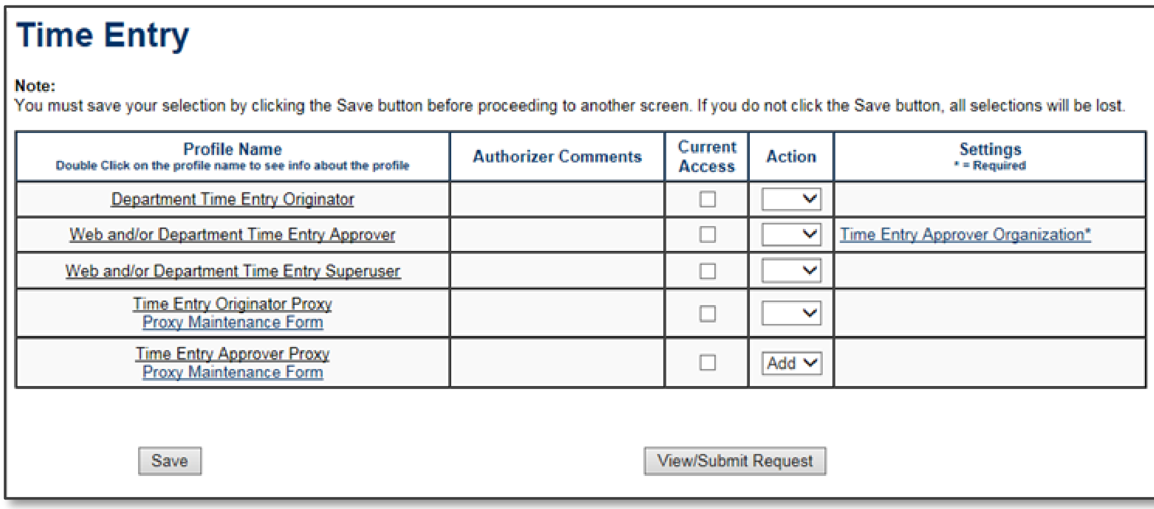
Profile Name Double Click on the profile name to see info about the profile	Authorizer Comments	Current Access	Action	Settings * = Required
Department Time Entry Originator		☐		
Web and/or Department Time Entry Approver		☐		Time Entry Approver Organization*
Web and/or Department Time Entry Superuser		☐	Add	
Time Entry Originator Proxy Proxy Maintenance Form		☐		
Time Entry Approver Proxy Proxy Maintenance Form		☐		

Save View/Submit Request

Figure 31

3. Request Time Entry Originator Proxy Security Profile

1) Click the **Time Entry** increment link.
2) Select **Add** in the ***Action*** column for **Time Entry Originator Proxy** *(see Figure 32).*
3) Click the **Save** button.
4) Click the **View/Submit Request** button.



Time Entry

Note:
You must save your selection by clicking the Save button before proceeding to another screen. If you do not click the Save button, all selections will be lost.

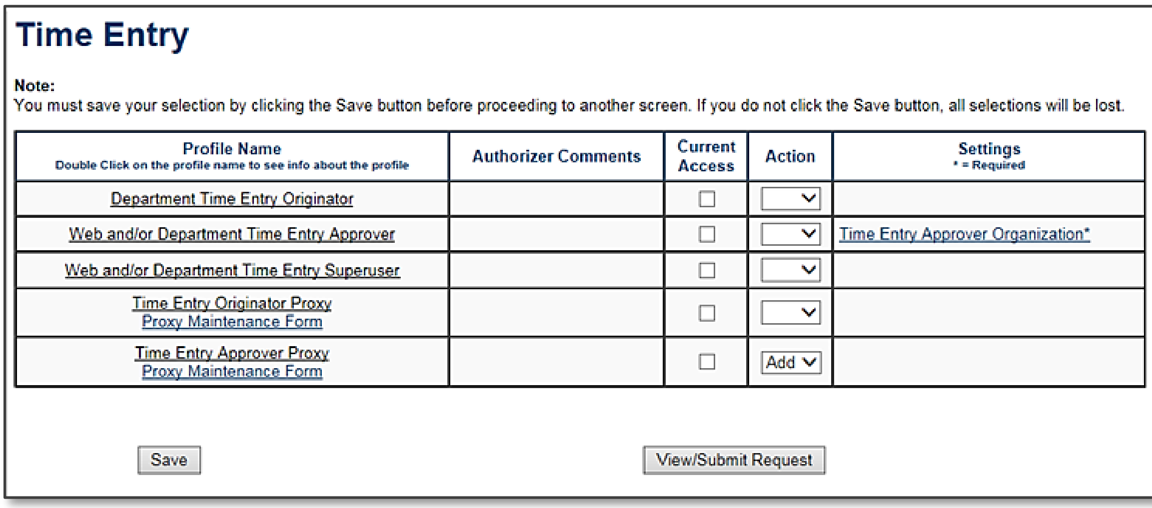
Profile Name Double Click on the profile name to see info about the profile	Authorizer Comments	Current Access	Action	Settings * = Required
Department Time Entry Originator				
Web and/or Department Time Entry Approver				Time Entry Approver Organization*
Web and/or Department Time Entry Superuser				
Time Entry Originator Proxy Proxy Maintenance Form				
Time Entry Approver Proxy Proxy Maintenance Form			Add	

Save   View/Submit Request

Figure 32

4. Request Time Entry Approver Proxy Security Profile

1) Click the **Time Entry** increment link.
2) Select **Add** in the ***Action*** column for **Time Entry Approver Proxy** *(see Figure 33).*
3) Click the **Save** button.
4) Click the **View/Submit Request** button.



Time Entry

Note:
You must save your selection by clicking the Save button before proceeding to another screen. If you do not click the Save button, all selections will be lost.

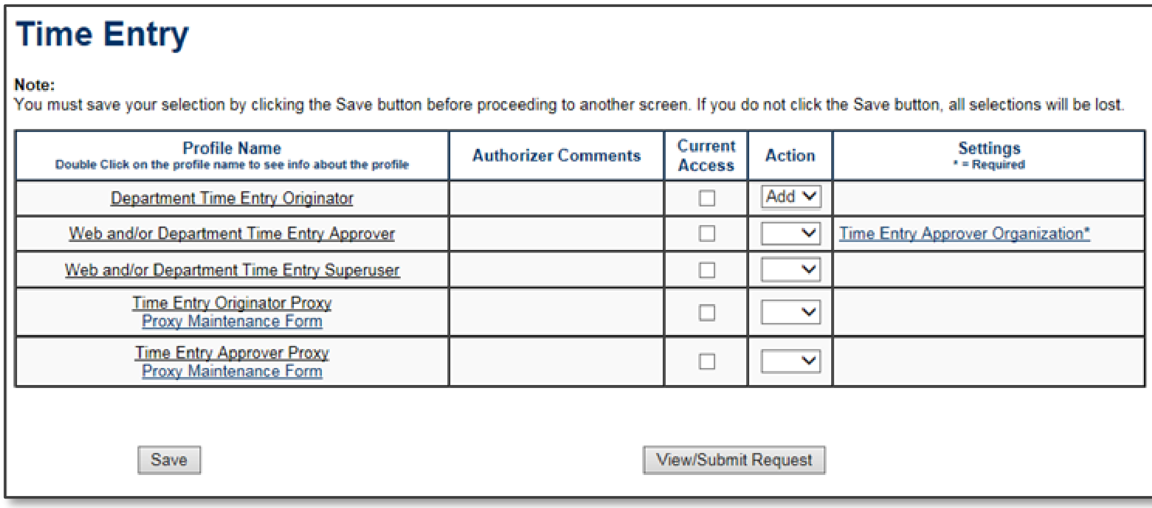
Profile Name Double Click on the profile name to see info about the profile	Authorizer Comments	Current Access	Action	Settings * = Required
Department Time Entry Originator		☐		
Web and/or Department Time Entry Approver		☐		Time Entry Approver Organization*
Web and/or Department Time Entry Superuser		☐		
Time Entry Originator Proxy Proxy Maintenance Form		☐		
Time Entry Approver Proxy Proxy Maintenance Form		☐	Add	

Save   View/Submit Request

Figure 33

5. Submit a Security Profile Request for Department Time Entry Originator

1. Click the **Time Entry** increment link.
2. Select **Add** in the ***Action*** column for **Department Time Entry Originator** *(see Figure 34)*.
3. Click the **Save** button.
4. Click the **View/Submit Request** button.



Time Entry

Note:
You must save your selection by clicking the Save button before proceeding to another screen. If you do not click the Save button, all selections will be lost.

Profile Name Double Click on the profile name to see info about the profile	Authorizer Comments	Current Access	Action	Settings * = Required
Department Time Entry Originator		☐	Add	
Web and/or Department Time Entry Approver		☐		Time Entry Approver Organization*
Web and/or Department Time Entry Superuser		☐		
Time Entry Originator Proxy Proxy Maintenance Form		☐		
Time Entry Approver Proxy Proxy Maintenance Form		☐		

Save   View/Submit Request

Figure 34

III. Review and Modify Time Approval Routing Queue

AITS will grant the requested security and create the time approval routing queues for the TS-Orgs in ***NTRRQUE*** in ***Banner*** based on new time entry and org security profile requests submitted by the USC in the ***Security Application***.

The unit **Superuser** should review and make any necessary changes to the time approval routing queue in ***NTRRQUE*** prior to the time entry period.

If the unit **Superuser** is unknown or unavailable, University Payroll & Benefits Customer Service can provide information on the current time approval queue(s) for the unit. Call UIC (312) 996-7200, UIUC (217) 265-6363, UIS (217) 206-7211 or email payinq@uillinois.edu.

1. Review an Existing Time Approval Routing Queue

1) Open the **Routing Queue Rules Form** (***NTRRQUE***) in ***Banner***.
2) Enter the **COA**.
3) Enter the **Organization**.
4) Click the **Next Block** button.
5) Under **Approval Category**, select **Time Entry and Approval** *(see Figure 35)*.
6) Review the entries in the **Approver Sequence** block. Write down any changes that need to be made.
7) Click the **Exit** button.

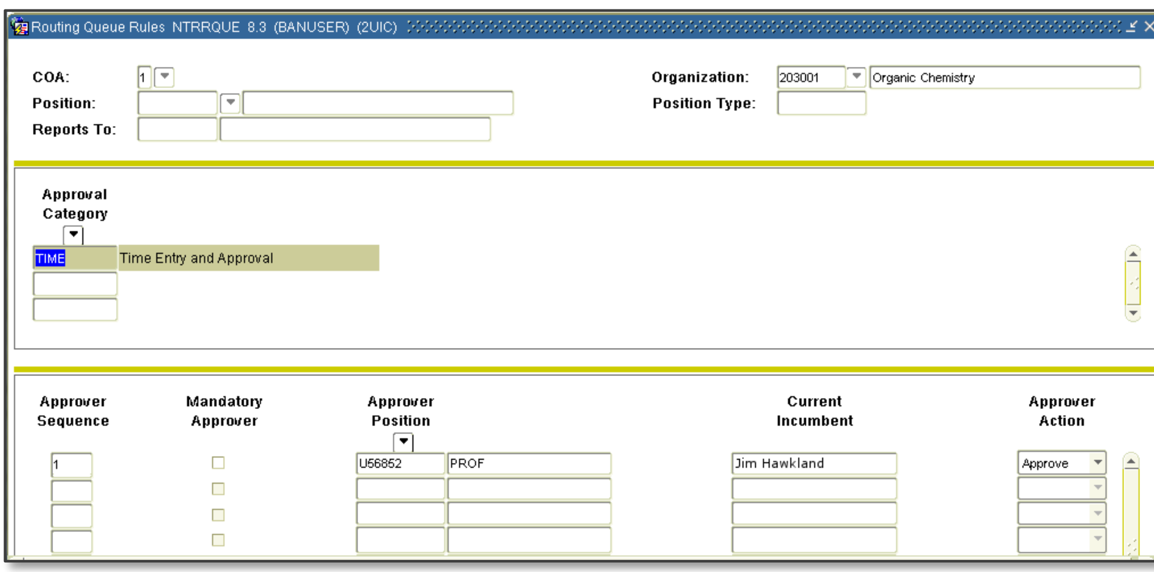


Figure 35

2. Establish Time Approval Routing Queue

If for some reason, the time approval routing queue has not yet been created, but the time entry security has been established for all roles, the unit **Superuser** can set up the time approval queue in ***NTRRQUE***.

1) Open the **Routing Queue Rules Form** (***NTRRQUE***).
2) Enter the **COA**.
3) Enter the **Organization**.
4) Click the **Next Block** button.
5) Under **Approval Category**, select **Time Entry and Approval**.
6) Type *1* in the **Approver Sequence** field, then tab to the **Approver Position** field and type the position number for the Approver.

   NOTE: The **Mandatory Approver** box should **never** be checked. If this box is checked the Routing Queue may become invalid.
7) In the **Approver Action** field, select *Approve*.
8) Click the **Save** button.

IV. Situations to Avoid

	Problem	Solution
1.	**Employee Web Time Entry Originators** or **Department Originators** cannot extract timesheets. **Error:** “Your records cannot be processed at this time. Please contact the Payroll Department.”	Time entry security for one or more individual within the time approval routing queue displayed in the **Routing Queue Rules Form *(NTRRQUE)*** in ***Banner*** is missing or incomplete. The time entry approval routing queue will be “broken” and timesheets will be inaccessible until the security access is granted. *Note: NTRRQUE does not show “VACANT” for the position of the individual who is missing the appropriate security profile/authority. VACANT indicates that there is an issue with the designated position for the corresponding approver or acknowledger (FYI) such as the position is no longer active in NBAJOBS.* The USC must submit the requests for the missing security profiles in the ***Security Application***.
2.	Unit has not established a time approval routing queue. **Error**: “Timesheet records could not be retrieved.”	Units must establish a time approval routing queue in the **Routing Queue Rules Form *(NTRRQUE)*** in ***Banner*** for the TS-Org. After the USC requests the appropriate time entry security profiles for individuals in the time approval process, the unit **Superuser** can establish the time approval routing queue in ***NTRRQUE***. See also Problem 3 regarding Error: Incumbent field will indicate “VACANT”.
3	A position selected for the **Time Approver** is no longer “active”. Common reasons for a position to be no longer “active” are: • **Time Approver** has been terminated • **Time Approver** has on leave • **Time Approver** has been promoted • **Time Approver** has a new job **Error**: Incumbent field will indicate “VACANT”.	Update the time approval routing queue with the new **Time Approver**’s information or the new position information for the **Time Approver**. Remember, the unit **Superuser** must notify the USC to contact AITS to establish security access for new **Time Approvers**.

4.	The **Time Approver** cannot extract their own timesheet. **Error**: "Timesheet records could not be retrieved." Common reasons for a position to be no longer "active" are: • **Override Approver** has been terminated • **Override Approver** has on leave • **Override Approver** has been promoted • **Override Approver** has a new job	The **Override Approvals Queue *(NBAJQUE)*** for the **Time Approver** is "broken". ***NBAJQUE*** will not indicate that the Override Approver's position is no longer "active" like ***NTRRQUE*** with the incumbent field showing "VACANT".. If the **Time Approver** has an Override Approver for their timesheet and cannot extract their timesheet, go to the **Override Approver's** job record(s) in the **HR Front End (HRFE)** and confirm that the Position (job) listed in ***NBAJQUE*** is active in **HRFE** for the pay event in question. Correct the position information in ***NBAJQUE*** for the **Override Approver** or assign a new **Override Approver**.
5.	The **Time Approver**'s position contains more than one employee, e.g., pooled position. **Error**: Incumbent field will indicate "MULTIPLE."	Departments should only designate **Time Approvers** from **non-pooled** positions. The general assumption is that Banner positions will be defined on a one-to-one ratio with the exception of student and extra-help, which may be pooled.
6.	TS-Org code used for a timesheet organization has been deactivated.	A process has been established to ensure a TS-Org code is not tied to a timesheet organization before deactivating. (The possibility of this occurring is extremely unlikely.)