Duke@Work Security Tab – Travel Initiators

Overview

Using the Duke@Work Security Tab, SAP Security Administrators can take the following actions:

- Grant an employee rights as a travel initiator which allows the initiator to create expense reports on behalf of other Duke employees.
  - Initiators can be given rights to create expense reports for all employees in an organizational unit (org unit access); or
  - Initiators can be given rights to a specific list of employees (Duke Unique ID access).
- Remove an employee’s rights as a travel initiator.
- Change an employee’s rights from org unit access to Duke Unique ID access.
- Change an employee’s rights from Duke Unique ID access to org unit access.
- Add organizational units or specific employees accessible to an initiator.

On the travel tab, color coding is used to better explain the action being taken as outlined below:

- Org unit highlighted in dark blue on the organizational unit tab – Eligible org unit that is being requested (will workflow and requires approval for it to be available to assign to an initiator).
- Org unit highlighted in gold on the organizational unit tab – Ineligible org unit that is being requested (will workflow and requires approval for it to be available to assign to an initiator).
- Org unit/NetID of newly added employee highlighted in light green on the travel tab – org unit/NetID being added to the initiator (will workflow and requires approval for it to be added to the initiator).
- NetID access highlighted in light purple on the travel tab – a person was added as a request and then removed during editing of the current request. If the tab is saved, closed, and reopened, the information and purple highlighting will no longer display.
Duke@Work Security Tab – Travel Initiators

Points to Remember

- All employees (including student employees) have access to create their own expense reports. No action is required by the department.
- Initiators can either have org unit access or Duke Unique ID access. The initiator cannot have both simultaneously.
- If a travel initiator is given org unit access to create expense reports and also has a payroll role assigned to his/her position, the initiator will see payroll data for all employees in all organizational units assigned to them. Be aware of this access to confidential information. If this access creates problems within the department, the initiator will need to be given Duke Unique ID access.
- If an initiator has org unit access, the access applies to all organizational units assigned to the position.
  - Ex. If an initiator has three organizational units assigned, he/she cannot be given rights to create travel expense reports for just one of the organizational units.
- Org Unit access is position based.
- Duke Unique ID access ties to the person. When hires occur new access will need to be established. When transfers occur, access will need to be stopped.
Duke@Work Security Tab – Travel Initiators

Grant Travel Rights – New

Follow the steps outlined below to establish rights for an employee.

1. Log into Duke@Work – work.duke.edu and go to the “Security Admin” tab.
2. Enter in the name of the employee who will be given access as a travel initiator, click “Go”. Once the employee’s name displays, click the hyperlink associated with the employee’s Duke Unique ID.

3. Once the security page opens, select “Edit”.

****Please note: prior to selecting “Edit”, data is only being “displayed”; therefore, the “Travel” tab is not displayed since this person is not currently an initiator.
Duke@Work Security Tab – Travel Initiators

Grant Travel Rights – New (continued)

4. Select the “Travel Tab”. Notice the first two sections, “Initiator For Org” and “Initiator For Pernr”.

5. If establishing org unit access, “check” the white box beside the first organizational unit listed. This will automatically highlight in green all the organizational units associated with the initiator. Remember: Access must be given to ALL the organizational units assigned to the position. If the initiator needs access to additional organizational units, go to the “Organizational Unit” tab and request access to the appropriate organizational units.
6. If establishing Duke Unique ID access, enter the Duke Unique ID for the employee who should be assigned to this initiator. Once the Duke Unique ID is in the box, select “Enter” on the keyboard and the employee’s name will appear.

****Notice a search box is available when the mouse is placed on the right side of the Pers. No box. If the Duke Unique ID is not available, search for the person by name. Remember that an * is a wildcard for searches in SAP and may be helpful when searching for an employee by name.

7. Continue adding Duke Unique IDs until all appropriate employees have been added to the initiator. The checked box indicates this person is going to be added. If a person is added in error, uncheck the box beside the employee’s name.
8. When the appropriate access has been added to the initiator, either “Save” the information to review and/or submit later or “Submit” the change which will both save and submit the changes into workflow for approval. As with all functions in the Security tool, “Submit” will display the workflow associated with the changes being requested. If you would like additional information on viewing workflow in the Security Tool, please watch the [SAP Security Maintenance – Viewing Workflow Video](#) available in Duke’s [Learning Management System](#). Once workflows have routed and are approved, the initiator will be able to create expense reports for either all employees in the org unit(s) requested or by NetID for all the employees listed.

![Screen capture of Security tool interface](#)

****Please note: As with all workflow in the Security tool, different workflow objects will be approved at different times; therefore, initiators may get access to some employees more quickly than others. For example: If org unit access is being added for three org units the initiator does not have access to, the approval for each org unit will happen individually; therefore, the initiator will get access to each org unit as the approval occurs. Additionally, changes cannot be made to the same user while a previously initiated change is still moving through workflow approval.
Duke@Work Security Tab – Travel Initiators
Change Current Access

Follow the steps outlined below to make changes to established rights for an employee.

1. Log into Duke@Work – work.duke.edu and go to the “Security Admin” tab.
2. Enter in the name of the employee who will be given access as a travel initiator, click “Go”. Once the employee’s name displays, click the hyperlink associated with the employee’s Duke Unique ID.

3. Once the security page opens, select “Edit”.

![Security Admin Tab](image_url)
4. Select the “Travel Tab”. Notice the first two sections, “Initiator for Org” and “Initiator for Pernr”. The current initiator access can be determined by looking at the checkbox display. A checked box beside an org unit in the “Initiator for Org” section or a checked box beside a person in the “Initiator for Pernr” section indicates whether the initiator has org unit or NetID access.

5. To change from UniqueID access to org unit access, select the white check box that corresponds to the first org unit listed. Selecting this check box will automatically “uncheck” all the names listed under the “Initiator for Pernr” section.

****Please note: Once the boxes beside a list of employees is “unchecked” the box beside each employee has to be “checked” one at a time in order to reestablish UniqueID access.
Duke@Work Security Tab – Travel Initiators
Change Current Access (continued)

To remove initiator access for specific employees, “uncheck” the box beside the names of the employees whom the initiator should no longer access in the online expense report tool.

OR

To change from org unit access to NetID Access, enter in the Duke Unique ID of an employee whom the initiator will access.
Duke@Work Security Tab – Travel Initiators

Change Current Access (continued)

Once the employee’s Duke Unique ID is in the box, select “Enter” on the keyboard. The employee’s name will appear and the box beside the name will be “checked”. The box beside the org units listed will be automatically “uncheck” changing the initiators access from org unit to Duke Unique ID. Continue adding DUIDs until all appropriate employees have been added to the initiator.

6. When the appropriate access has been added to the initiator, either “Save” the information to review and/or submit later or “Submit” the change which will both save and submit the changes into workflow for approval. As with all functions in the Security tool, “Submit” will display the workflow associated with the changes being requested. If you would like additional information on viewing workflow in the Security Tool, please watch the SAP Security Maintenance – Viewing Workflow Video available in Duke’s Learning Management System. Once workflows have routed and are approved, the initiator will be able to create expense reports for either all employees in the org unit(s) requested or by NetID for all the employees listed.
****Please note: As with all workflow in the Security tool, different workflow objects will be approved at different times; therefore, initiators may get access to some employees more quickly than others. For example: If org unit access is being added for three org units the initiator does not have access to, the approval for each org unit will happen individually; therefore, the initiator will get access to each org unit as the approval occurs. Additionally, changes cannot be made to the same user while a previously initiated change is still moving through workflow approval.
Duke@Work Security Tab – Travel Initiators

Delete Initiator Access

Follow the steps outlined below to remove rights for an employee.

1. Log into Duke@Work – work.duke.edu and go to the “Security Admin” tab.
2. Enter in the name of the employee who will be given access as a travel initiator, click “Go”. Once the employee’s name displays, click the hyperlink associated with the employee’s Duke Unique ID.

3. Once the security page opens, select “Edit”. 
Duke@Work Security Tab – Travel Initiators

Delete Initiator Access (continued)

4. Select the “Travel Tab”. Notice the first two sections, “Initiator for Org” and “Initiator for Pernr.” Uncheck the boxes under either the “Initiator for Org” or the “Initiator for Pernr” section determined by the initiator’s access. All initiator access has been removed when no boxes are checked in either the “Initiator for Org” or the “Initiator for Pernr” sections.

5. When the appropriate access has been deleted from the initiator, either “Save” the information to review and/or submit later or “Submit” the change which will both save and submit the changes into workflow for approval. As with all functions in the Security tool, “Submit” will display the workflow associated with the changes being requested. If you would like additional information on viewing workflow in the Security Tool, please watch the SAP Security Maintenance – Viewing Workflow Video available in Duke’s Learning Management System. Once workflows have routed and are approved, the initiator will no longer be able to create expense reports for other Duke employees.