Introduction

KSAMS (new Security Access Management System) is a web-based centralized authorization (role-based access control) system that offers a central point for adding and removing user role membership to other applications and resources. Access is not directly managed by one person, everything is instead requested and approved via workflow with complete audit trail. This offers a consistent interface and process for users requesting access to resources, as well as a single location to give security visibility to audit what people have access to and comprehensively terminate all access when needed.

KSAMS Use Case Diagram

Basic User Features

These are the most common features that the majority of people will use in KSAMS.

Login

To access KSAMS, go to https://systems.oit.uci.edu/kfs/ksams/. If you aren't already logged in, you will be redirected to the WebAuth login page. After successfully authenticating with your UCInetID and password, you will be redirected back to the KSAMS welcome page. The welcome page includes current announcements and a starting point to other menu options. You can click Home at the top of the page at any time to return to the welcome page.
To view your current access, click on the **Reports** tab, then click on **My Access**. All of the roles (and qualifiers) you currently are a member of are listed.
To view your current DSA (Departmental Security Approver)’s contact information, click on the **Access Request** tab, then click on **Contact DSA**. All of the Departmental DSA names and contact information defined at your organization level and its parent levels are listed. They will most often be the first line of approvers for organization-based access so questions specific to any local policies and requirements for access requests should be asked of them. Members of OIT HelpDesk are listed as DSA at the highest organization level to handle questions and approvals when the local organization DSA is not available.

**KSAMS**

<table>
<thead>
<tr>
<th>Access Request</th>
<th>Approval Queue</th>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Request</td>
<td>Contact DSA</td>
<td></td>
</tr>
</tbody>
</table>

**Current DSA’s For JONES, VALERIE (Ricket1D: vjones, Organization: IR: 7234 SUPPORT AND SERVICES)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALVAREZ, DANIEL</td>
<td><a href="mailto:dane@uci.edu">dane@uci.edu</a></td>
<td>(949) 824-2222, 2240</td>
<td>R-9017 OFFICE OF INFORMATION TECHNOLOGY</td>
</tr>
<tr>
<td>MORALLO, MARIA</td>
<td><a href="mailto:mmorallo@uci.edu">mmorallo@uci.edu</a></td>
<td>(949) 824-4114</td>
<td>R-9017 OFFICE OF INFORMATION TECHNOLOGY</td>
</tr>
<tr>
<td>NELSON, CHRISTOPHER</td>
<td><a href="mailto:cnelson@uci.edu">cnelson@uci.edu</a></td>
<td>(949) 824-6404</td>
<td>R-9017 OFFICE OF INFORMATION TECHNOLOGY</td>
</tr>
<tr>
<td>PEREZCASTANEDA, MARIE</td>
<td><a href="mailto:mariperez@uci.edu">mariperez@uci.edu</a></td>
<td>(949) 824-5155</td>
<td>R-9017 OFFICE OF INFORMATION TECHNOLOGY</td>
</tr>
<tr>
<td>ROSAS, GENA</td>
<td><a href="mailto:genaros@uci.edu">genaros@uci.edu</a></td>
<td>(949) 824-4154</td>
<td>R-9017 OFFICE OF INFORMATION TECHNOLOGY</td>
</tr>
<tr>
<td>WATT, CHERYL</td>
<td><a href="mailto:cheryl.watt@uci.edu">cheryl.watt@uci.edu</a></td>
<td>(949) 824-7367</td>
<td>R-9017 OFFICE OF INFORMATION TECHNOLOGY</td>
</tr>
<tr>
<td>CABAN, MICHAEL</td>
<td><a href="mailto:mikedcabi@uci.edu">mikedcabi@uci.edu</a></td>
<td>(949) 824-9177</td>
<td>UC-UNIV UC OFFICE OF THE PRESIDENT</td>
</tr>
</tbody>
</table>

**Add Access Request**

**Watch the Video**

New access can typically be requested three different ways in KSAMS:

1. **Self-service** where a user requests access for themselves via request form
2. **Manager requests access** for their staff via request form
3. **User or manager contacts** DSA (Departmental Security Approver) directly via email (or another local process outside of KSAMS), and DSA submits request form on their behalf

If doing #3, the DSA should paste the original request from user or manager in the reason/justification field of the request form for a complete audit trail.

In all cases, new access can only be granted by submitting a request form. To do this, click on the **Access Request** tab, then click on **Add Request**.
First choose the user you are requesting access for, they are called the Grantee. You can do this by entering a partial name or exact UCInetID in the Grantee Name field and pressing enter or clicking the search icon. If there are multiple matching results a pop-up window will allow you to choose one of the names, otherwise the chosen result will populate the Grantee UCInetID required field. Only identities with a home organization defined can be selected.

Next choose the access you want to grant this individual. You can do this by entering a partial role name or role namespace in the Role Name field and pressing enter or clicking the search icon. If there are multiple matching results a pop-up window will allow you to choose one of the roles, otherwise the chosen result will be added to the requested Access table. If you only want to choose one of the matching roles you can simply click on the role name and be returned to the previous screen with the new role added to the access list. If you want to select multiple of the matching roles you can click on the "+" button for each role you want to add, then close the window to be returned to the previous screen with the new roles added to the access list.

If you would like a longer description of any of the roles you can also click the "?" button.
You can request multiple lines of access in one batch request, simply choose multiple role search results. If you would like to remove an access row from the Requested Access table simply click the " - " button in that row. If you would like to add another row using that row's same role name click the " + " button in that row. Some roles have qualifiers associated with them. Required qualifiers are denoted with a red *. If you have any questions about which roles or qualifier values should be requested to get specific access to another application, please contact your DSA or refer to that application's user documentation.

Next enter in the Reason/Justification field the reason or justification why this access is being requested for this individual.
Lastly, when the request form is complete, click on the **Submit Request** button. That will validate the entire form to ensure all required fields are entered, all qualifier values are valid (that the values exist and/or are the right format), and that the access doesn't already exist for that individual. Once there are no errors from the validation, the form will be submitted to the workflow engine.

KSAMS breaks up your request into multiple workflow documents that get routed individually based on the role and qualifiers requested in each row. A result page is displayed showing the status of each of those individual requests, either an error message or if successful the document identifier of the workflow document it generated. You can click on the **Document #** to see where it got routed to for approval.
To view the status of an access request, or more specifically a KSAMS Request Document in the workflow engine, you can click on the Document # as described in the above add access request process. However, if you would like to check on the status of a KSAMS Request Document at a later time after you’ve navigated away from that page, click on the Approval Queue tab, then click on Document Search. This will bring up the Document Lookup screen for the workflow engine and pre-fill the desired type as KSAMSRequestDocument.

You can further refine your search based on Initiator (UCInetID who submitted the request), Grantee (UCInetID who the requested access was for), Document/Notification ID (Document #), and Date Created range for when the request was submitted. Click the Search button and matching KSAMS Request Documents will be listed.
Click on the Document/Notification ID of the desired result and a new page will pop up that includes all the details of that document. Details include who initiated the document and when, the current status of the document and pending route node / approval role if it is currently still enroute. If you want to see a full audit trail of the workflow route history or the specific members of the approval role it is waiting on, click the show button on the Route Log tab. When finished you can close this pop up window to return to the Document Lookup screen.
When you are finished using KSAMS, you can securely logoff by clicking Logout at the top of the page and closing your window.

### DSA and Approver Features

In addition to the basic user features, DSA (Departmental Security Approver) and other Approvers (trainers, central office, etc) in KSAMS have added responsibilities. These include mainly to approve or deny access requests that get routed to them for approval, but they can also submit remove access requests and other advanced features.

#### Approve/Deny Requests

- Watch the Video (part 1 of 2)
- Watch the Video (part 2 of 2)

DSAs and other Approvers (trainers, central office, etc) can view all of the KSAMS Request Documents that have been routed to them for approval by clicking on the Approval Queue tab, then click on Action List. This will actually display their entire workflow action list, but for KSAMS focus on those where Type is KSAMS Request Document. If the screen is blank, there are no pending action items. Otherwise, click on the Id of any pending documents and it pop up a window showing all of the document details and routing status.
To understand under which context you are being asked to approve the request, look at the **Current Route Node / Approver Role** field. How a DSA or other Approver determines whether a request should be approved is outside the scope of KSAMS and possibly specific to that person and/or role. There may be other processes outside of KSAMS to determine the requirements of access approval (such as having completed training or only approving requests made by managers). Once that decision is made, the DSA or Approver can click on the **Approve** or **Disapprove** button as appropriate. If Disapprove is chosen, a new screen will ask for a reason why, which will be sent back to the initiator to acknowledge. If Approve is chosen, the document is then routed to the next workflow node. Once the document reaches final state with all required approvals the requested access is active and both the initiator and grantee will get a notification email. **Note:** to enforce separation of duties, an approver cannot approve a document for which they are also the grantee, if they do the document will go into an exception state at the end of workflow and access will not be granted.

The **KSAMS Super DSA** role has the ability to override workflow routing and approve/deny any pending **KSAMS Request Document**, but is only to be used in rare and exceptional circumstances. If you have an urgent request and all approvers are unavailable for a long period of time contact the OIT HelpDesk.
Copy Access Request

Watch the Video

Another feature for DSAs and other advanced KSAMS roles is the ability to quickly copy access from one user to another on the Add Request form. In situations where the bulk of access (past or present) from one user should be granted to another, one can use the Copy From User area of the Add Access Request Form. Simply enter the UCNetID of the user to copy access from and optionally a date (if you want to copy access that user had at some specific date in the past) and click the Load Access button. If matching access is found, it will be appended to the Requested Access list on behalf of the Grantee. As with any access on this page, if you want to remove some rows (i.e. copy all except...) simply click the " - " button for each row you don't want to request to add. You can do this as many times as you'd like for different users, the rest of the page works exactly the same way as the Add Access Request form instructions above.

Remove Access Request

Watch the Video

Existing access can only be removed from a user by submitting a request form. To do this, click on the Access Request tab, then click on Remove Request.
First choose the user you are requesting access removal from, they are called the **Grantee**. You can do this by entering a partial name or exact UCInetID in the **Grantee Name** field and pressing enter or clicking the **search** icon. If there are multiple matching results a pop-up window will allow you to choose one of the names, otherwise the chosen result will populate the **Grantee UCInetID** required field.

Next choose the **Remove Type** for this request. You can choose to **Remove Specific Access** if you want to remove just specific rows of access (useful when individual’s job duty changes), or you can choose **Cancel All Access** if you want to remove all access in one approval (useful when individual is separating from the organization).

Once all the required fields are filled click the **Submit Request** button.

If **Remove Specific Access** was chosen, all the existing access for that individual is displayed and you must click the checkbox in the **Remove?** column for each row of access you want to request to remove. The unchecked rows will be ignored. Next enter in the **Reason/Justification** field the reason or justification why this access removal is being requested for this individual. Lastly, when the request form is complete, click the **Submit Request** button. That will validate the entire form to ensure all required fields are entered and submit the form to the workflow engine.
KSAMS may generate multiple workflow documents that get routed individually based on the organization code of the grantee and/or role requested in each row. A result page is displayed showing the status of each of those individual requests, either an error message or if successful the document identifier of the workflow document it generated. You can click on the **Document #** to see where it got routed to for approval.

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Role Name</th>
<th>Qualifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINANCIAL</td>
<td>Campus Credit Card - Department Head/Business Manager</td>
<td>Chart Code=IR, Organization Code=7334</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Campus Credit Card - Refund</td>
<td>Chart Code=IR, Organization Code=7334</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Cost Share Tracking</td>
<td>Chart Code=IR, Organization Code=10600</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Data Warehouse - Payroll Expense</td>
<td>Chart Code=IR, Organization Code=7334, Account Number=GF12096</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Data Warehouse - Payroll Expense</td>
<td>Chart Code=IR, Organization Code=7334, Account Number=GF12096</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Data Warehouse - Payroll Expense</td>
<td>Chart Code=IR, Organization Code=7334, Account Number=GF12096</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Data Warehouse - Payroll Expense</td>
<td>Chart Code=IR, Organization Code=7334, Account Number=GF12096</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Data Warehouse - Payroll Expense</td>
<td>Chart Code=IR, Organization Code=7334, Account Number=GF12096</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Payroll Certification - Central Office User</td>
<td>Chart Code=IR, Organization Code=7332</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>PI Report - Browse</td>
<td>Chart Code=IR, Organization Code=7334</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>PI Report - Browse</td>
<td>Chart Code=IR, Organization Code=7334</td>
</tr>
<tr>
<td>ITSEC</td>
<td>GIT VPN User</td>
<td>Chart Code=IR, Organization Code=7332</td>
</tr>
<tr>
<td>KFS-SYS</td>
<td>User</td>
<td>Chart Code=IR, Organization Code=7332</td>
</tr>
<tr>
<td>KFS-THEM</td>
<td>TEM Organization Profile Arranger</td>
<td>Chart Code=IR, Organization Code=7332, Discards Hierarchy=Y</td>
</tr>
<tr>
<td>KFS-THEM</td>
<td>TEM Organization Profile Arranger</td>
<td>Chart Code=IR, Organization Code=7332, Discards Hierarchy=Y</td>
</tr>
</tbody>
</table>

**Reason / Justification**

Valerie is no longer responsible for FOSS in OS.
If **Cancel All Access** was chosen, you will be prompted to verify you are sure you want to cancel all access. The **Y** es checkbox must be checked otherwise the request will be ignored. Next enter in the **Reason/Justification** field the reason or justification why this access removal is being requested for this individual. Lastly, when the request form is complete, click the **Submit Request** button. That will validate the entire form to ensure all required fields are entered and submit the form to the workflow engine.
Reports and Audit

To access audit and other reports in KSAMS you must be a member of one of the many DSA or Approver roles, or the read-only *KSAMS Inquiry* role.

Lookup Current Access

Watch the Video

To lookup current access of any other individual, click on the **Reports** tab, then click on **Access Lookup**. Enter the UCNetID of the individual to query and optionally an As Of Date to look up access at a point in time in the past in the text boxes, and click the **Submit** button. All of the roles (and qualifiers) that individual is currently (or at the point of time optionally given in the past) a member of are listed.
To lookup the DSA (Departmental Security Approver) contact information of any other individual, click on the Report tab, then click on DSA Lookup. Enter the UCnetID of the individual to query in the text box and click the Submit button. All of the Departmental DSA names and contact information defined at that individual's organization level and its parent levels are listed.
Audit Reports

KSAMS leverages the Cognos reporting engine for various security audit reports. To access them, click on the Reports tab, then click on Audit Reports. When you click on the desired report link as described below, you will be redirected to the OIT Cognos application where you may be required to enter your UCNetID and password again. All data is current as of the previous night.

All reports default to HTML view. If you would like to export the data in a different format, click the HTML dropdown on the top right area of the final report, and then choose from PDF, XML, and various Excel/CSV formats to download.

KSAMS Current Role Membership Report

This report requires you to select the Role Namespace and one or more Role Names under that namespace to report on.
Once that is done, click the Finish button on the bottom of the page. A report will be generated that shows all current user access for the roles you selected, including Role Name, Grantee, Qualifiers (if applicable), Active From Date, and Add Request Document (if applicable). You can also click on the Grantee UCInetID or Add Document ID to get a detailed drill-down report specific to that field.

**KSAMS Current User Access By Home Department Report**

This report requires you to select the Home Department Code(s) to report on. Type in a home department code in the textbox and then click the Insert button to add it to the list, or select one from the list and click the Remove button to remove it from the list.

Once that is done, click the Finish button on the bottom of the page. A report will be generated that shows all current user access for members of the home department(s) you selected, including Grantee, Role, Qualifiers (if applicable), Active From Date, and Add Request Document (if applicable). You can also click on the Grantee UCInetID or Add Document ID to get a detailed drill-down report specific to that field.

**KSAMS User Access History Report**

This report requires you to select the UCInetID(s) to report on. Type in a UCInetID in the textbox and then click the Insert button to add it to the list, or select one from the list and click the Remove button to remove it from the list.
Once that is done, click the Finish button on the bottom of the page. A report will be generated that shows all user access history (current and past) for the users you selected, including Grantee, Role, Qualifiers (if applicable), Active From Date, Add Request Document (if applicable), Active To Date and Remove Request Document (if applicable). You can also click on the Grantee UCInetID, Add Document ID, or Remove Document ID to get a detailed drill-down report specific to that field.

Currently this report is not available for users who is inactive for a long time. Please contact the KSAMS team for those cases.

**KSAMS AdHoc Query**

For seasoned Cognos reporting tool users, you can write your own custom reports using KSAMS data. If you click this option the Cognos advanced workspace application will load and you will be able to query and design your own reports based on the KSAMS data package.

Back to Top

**Approval Workflow Configuration**

Watch the Video

To lookup the current approver workflow routing configuration defined for roles, click on the Reports tab, then click on Approver Config. Enter a partial role name or role namespace (or * to return all roles defined) in the text box and click the Submit button.

The matching defined role(s) is/are displayed, each with different workflow steps for "add" and "remove" request actions. Each workflow can have multiple steps and are ordered by the route node name ascending. For each route node, the Approver Role the document gets routed to is displayed, and you can click on it to get a pop up window to display that role’s details and current membership. Also whether that workflow step is Required or FYI only is displayed. There is also a special workflow defined for "cancel" requests, since that is not role specific.
Manual Update Role Type

KSAMS will send out notification email when the membership of a manual update role is changed (users get added and removed from the role), including from the KSAMS automatic purge process. If it's a cancel action then one notification will be generated per manual update role this person is in. For example, if the person has 3 roles but only 2 of them belongs to the manual update type then when a cancel happens, 2 notifications will be generated with action = "cancel".

Process of Purging Access of Separated Employees

It’s the responsibility of the sponsor/manager of a separated employee to notify / submit a cancel request to DSA so the DSA can nuke all the access of the separated employee.

KSAMS provides a safe net feature, which will send an email to DSA so DSA can remove the employee’s access once the he/she becomes inactive (emailDSAZombieUserJob). The status will change to inactive after the Payroll (PPS) reflects the change. If no action is taken, KSAMS will remove all the access of an inactive employee (purgeEmailNoHomeOrgZombieUsersJob). The auto purge batch job is run once daily and will generate cancel ESB messages to MQ. It will generate a manual update email reminder if a manual update roles is involved.

Scheduled Downtime (Both UI & WS)

Workdays: 8pm - 10pm

Daily: 12:55am - 3:00am

Back to Top