Accessing PEP data in Salesforce

Overview

In order to access PEP data in Salesforce, several layers of security must be addressed. And once access to Salesforce is obtained, configuration of the Salesforce menu is required. This document identifies the steps required for a user to have access and interact with information in Salesforce. The Appendix provides additional information on the function of the various security elements within Salesforce.

The intended audience for this document are university advisors and PEP central administration

Table of Contents

Chapter 1: Requesting access to Salesforce

Execute the following steps to obtain the appropriate level of access to Salesforce PEP data.

NOTE: The order of the steps is critical to ensure proper access. Each step MUST be completed before starting the next step.

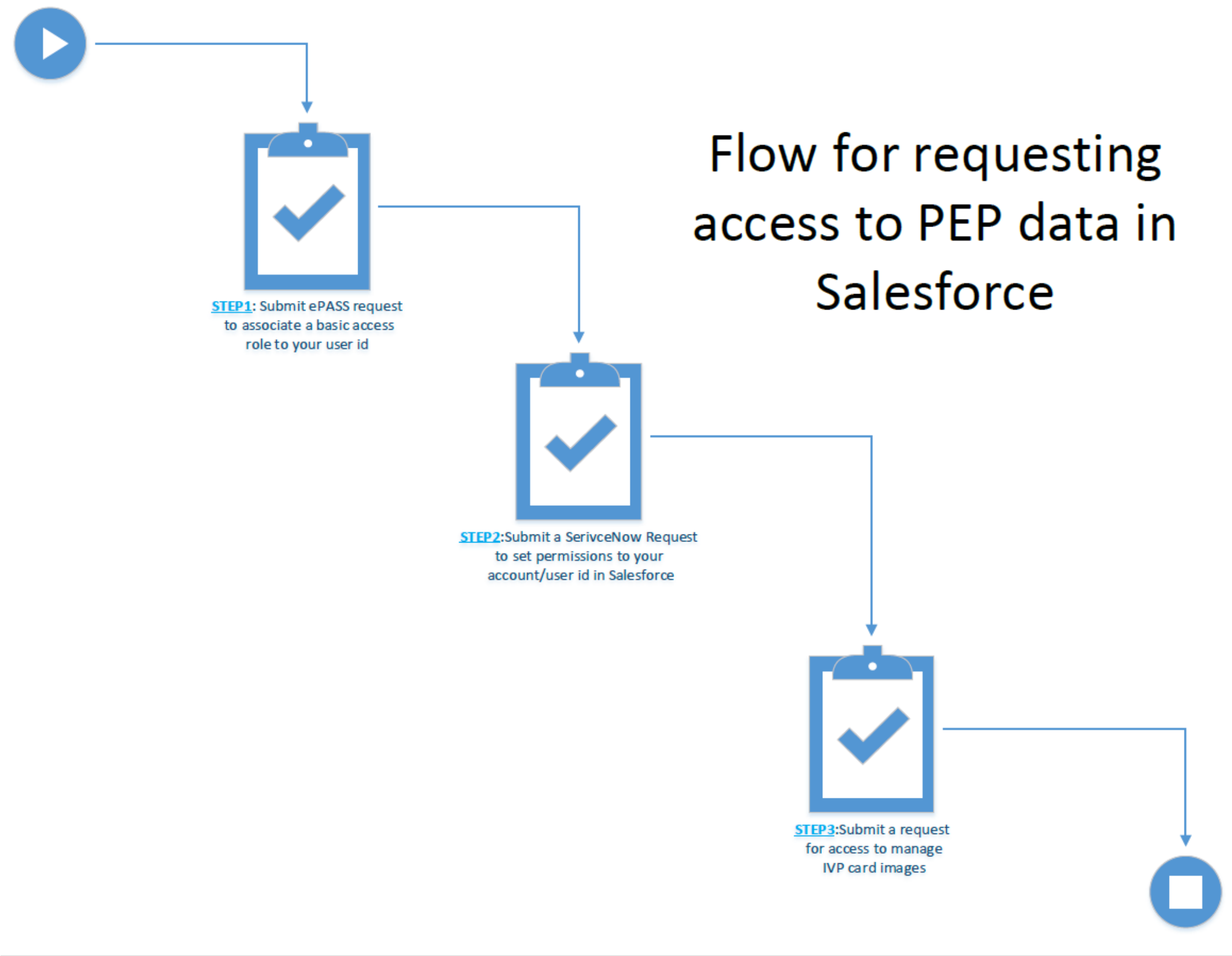
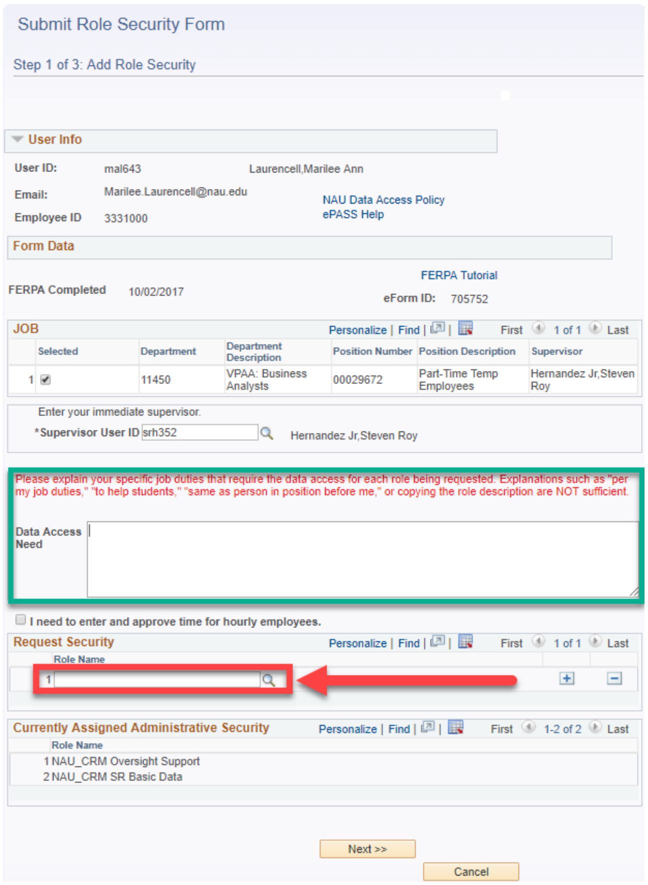


Figure 1: Flow to obtain access to PEP data in Salesforce

STEP 1: Open an ePASS (Electronic PeopleSoft Administrative Security System) request

This action will generate USER record in Salesforce with the requested role

1) Navigate to the Louie self service page
2) Select ePASS Home Page link
3) For additional information, please refer to the NAU Salesforce proxy policy
4) From the ePass Home Page, select the Initiate a Security Request Form link, which will display the request form:

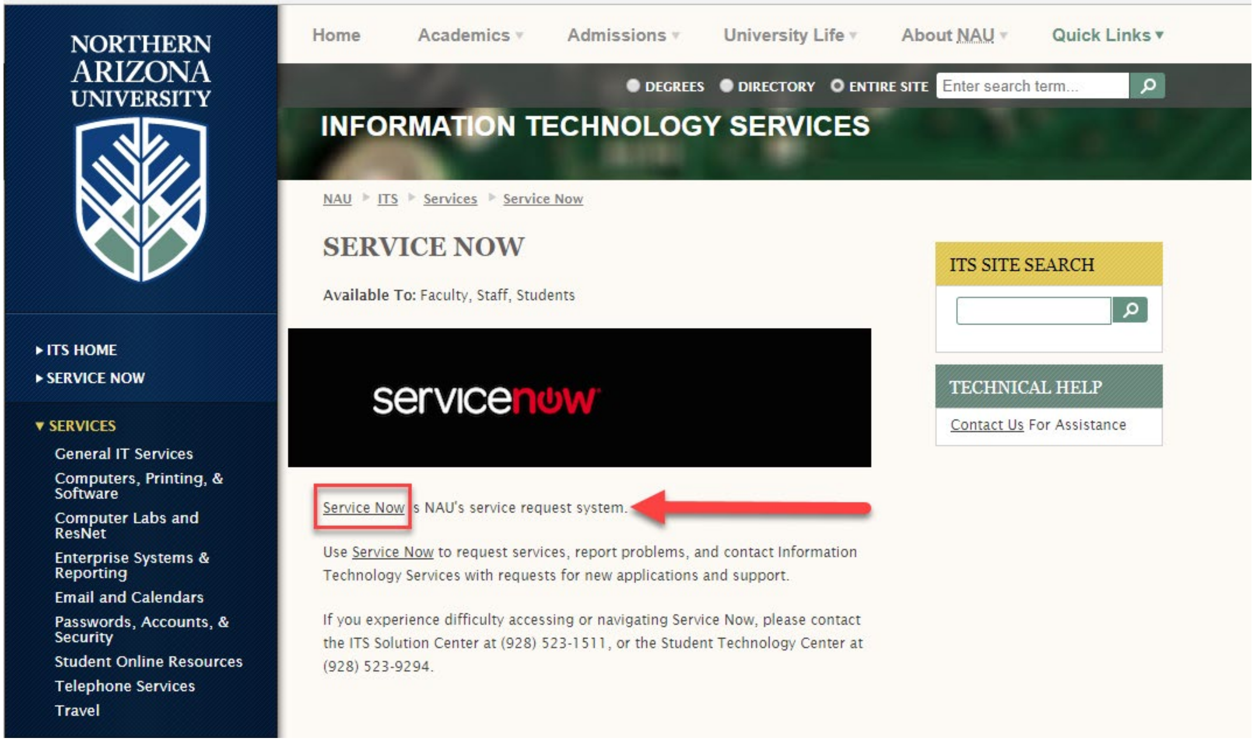


a) On the form, update the "Data Access Need" text box with the reason access is required (see green box in screen shot above)
b) On the form, update the "Role Names" (see red arrow in screen shot above) with the appropriate Role
   i) For Academic Advisors, PEP OFE staff (full-time staff), request inclusion in the following profiles:
      - **NAU_CRM_OVERSIGHT_SUPPORT**
   ii) For GAs supporting OFE, request inclusion in the following profiles:
      - **NAU_CRM_ADVANCED_SUPPORT**

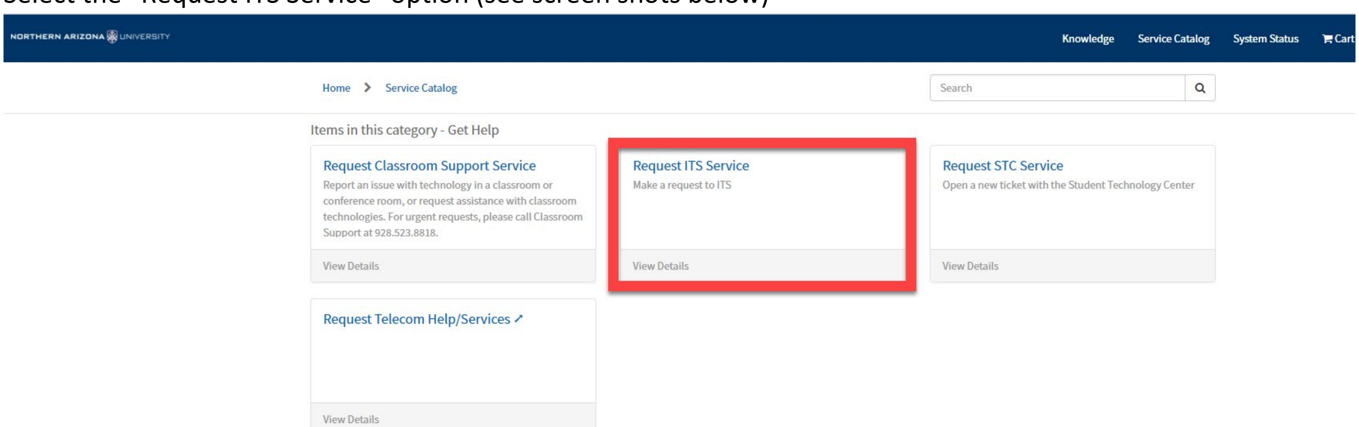
5) For additional information on ePass, click here
6) For additional information on Salesforce proxy roles, click here

STEP 2: Open a ServiceNOW request to set permissions in Salesforce for PEP data

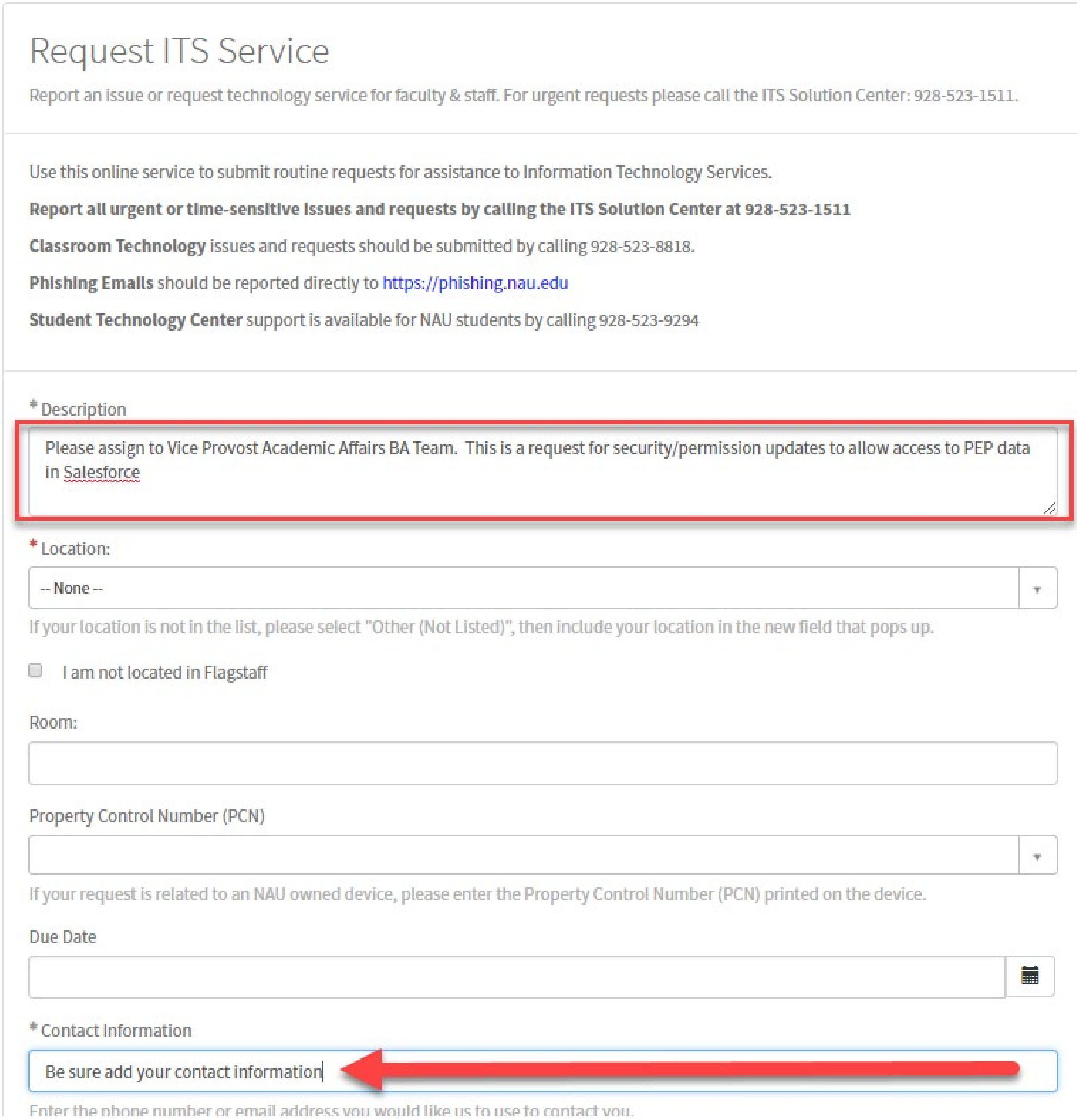
1) Navigate the ITS Service Portal site and select ServiceNow



2) Select the "Request ITS Service" option (see screen shots below)



3) A "Request ITS Service" form will be presented (see screen shot below):



NOTE: Requests must be routed to the Vice Provost Academic Affairs BA Team. This MUST be specifically stated in the description to avoid delays in obtaining access to PEP data in Salesforce.

a) Enter the following information in the description text box:
   i) Requesting inclusion in the permission sets to **access PEP data in Salesforce**. Please route the request to Vice Provost Academic Affairs BA Team for approval
   ii) The request must include the appropriate permission set for your support role. Include one of following, which best aligns with your support role:
      (1) PEP Academic Advisors, for use by Academic Advisors
      (2) PEP Report Manager, for those only needing to review/run reports

(3) PEP Program Manager, typically for PEP administrative staff and GAs supporting OFE
(4) PEP OFE Assistant, if supporting Office of Field Experience

iii) **All PEP requests** must include a request to be added in the Salesforce public group
(1) Request inclusion in the PEP PUBLIC GROUP for the user

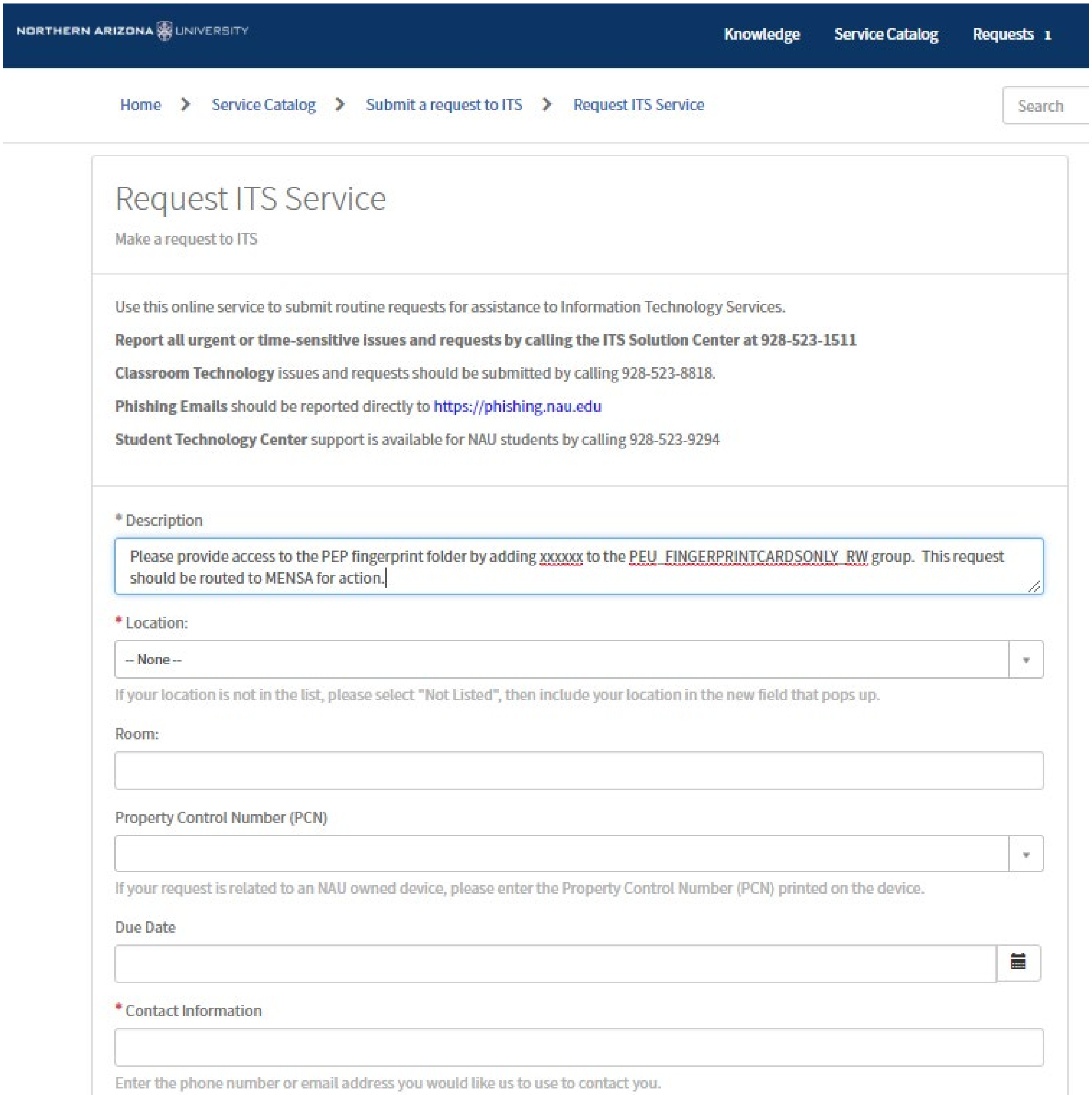
iv) To ensure access via Lightning
(1) Request "Lightning" to be enabled
(2) Request your profile be set to University Advising
(a) NOTE: even if you are not a university advisor, be sure to include request to assure access to PEP data.

b) Requests approved by the Vice Provost Academic Affairs BA Team will be routed to the appropriate ITS group for further action.

STEP 3: Submit a request for access to manage IVP card images

IVP or fingerprint cards are managed in two different repositories: Sharedrive and OnBase. The advisors will upload a copy of the IVP to OnBase, while the OFE uses the sharedrive to send the IVP when requesting student teaching placement at a school.

Step 3a: Open a request for access to the PEU shared drive



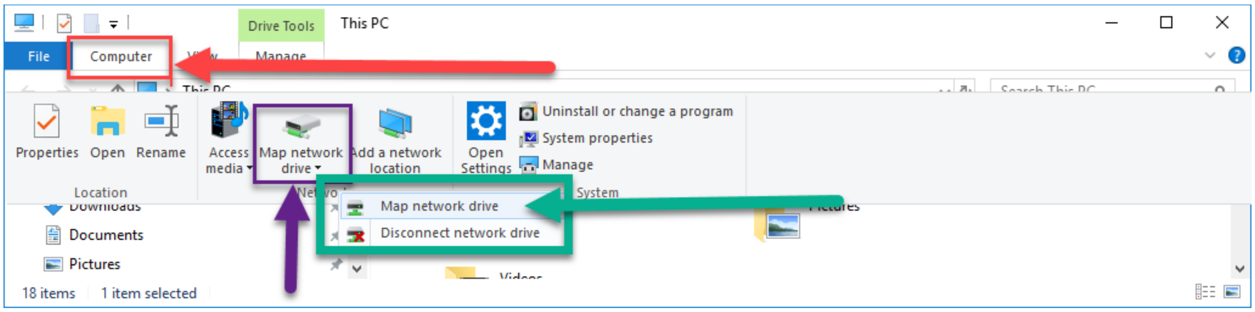
a) Enter the following information in the description text box:

Please provide access to the PEP fingerprint folder by adding *your name and NAU Id* to the PEU_FINGERPRINTCARDSONLY_RW group. This request should be routed to MENSA for action.

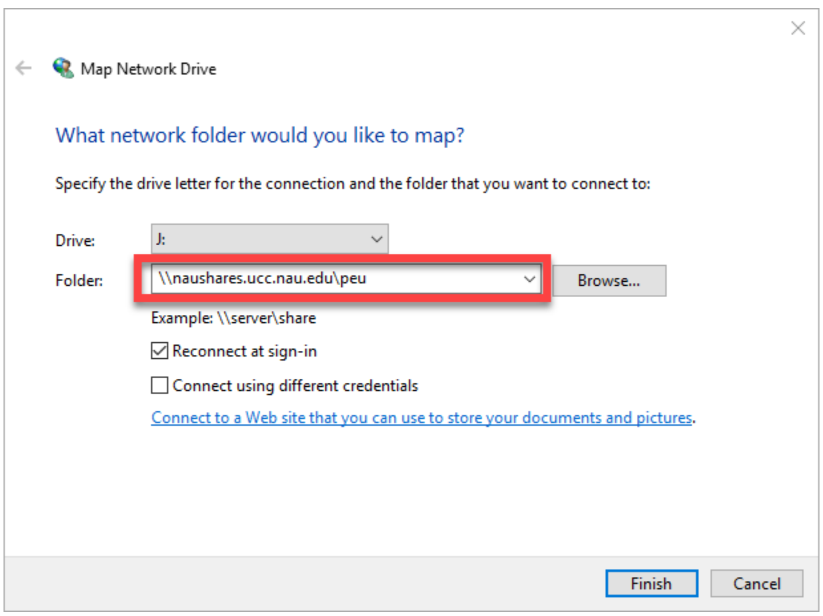
NOTE: xxxxxx should be replaced by your name and NAU id

b) Once added to the PEU group, access to the fingerprint folder will be allowed. To access the fingerprint folder, you must "map" to the sharedrive

i) In Windows Explorer, select the drop down menu for "Computer". From the Computer menu, select Map Network Drive. From the Map Network Drive menu, select Map network drive.



ii) Define the shared drive that will be mapped by selecting a "drive" from the drop down (any unused selection is valid) and entering the folder information: \\naushares\ucc.nau.edu\peu



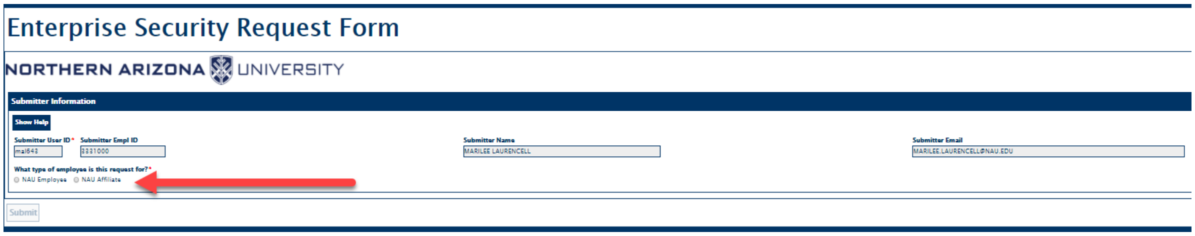
iii) Select the "finish" button to link to the shared drive.

Step 3b: Open a request for access to OnBASE

1) From the NAU OnBase Enterprise page, select the link for the Enterprise Security Request Form
NOTE: The form will be presented in sections. You must select "submit" or input information before the next section of the form will be visible

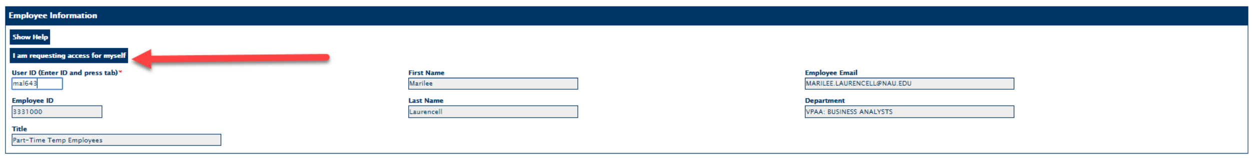
2) Populate the form as follows:

a) Submitter Information Section



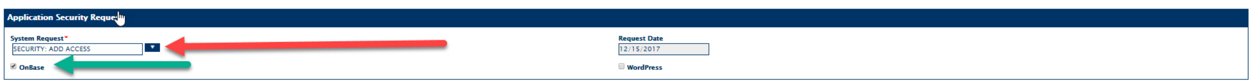
i) Submitter fields will be automatically populated, but update as needed
ii) Select the appropriate radio button for "What type of employee is this request for?" (see red arrow in screen shot above)
iii) Click the "submit" button
    (1) The "Submit" button will not be active until the type of employee is identified

b) Employee Information Section



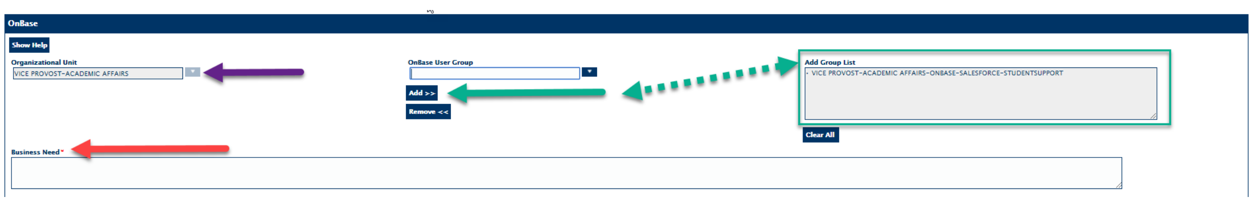
i) If the request is for yourself, select the "I am requesting access for myself" button (see red arrow in screen shot above); otherwise, fill in the employee information

c) Application Security Request Section



i) For "System Request", select "ADD ACCESS" from the dropdown list (see red arrow in screen shot above)
ii) Select the "OnBase" checkbox (see green arrow in the screen shot above)

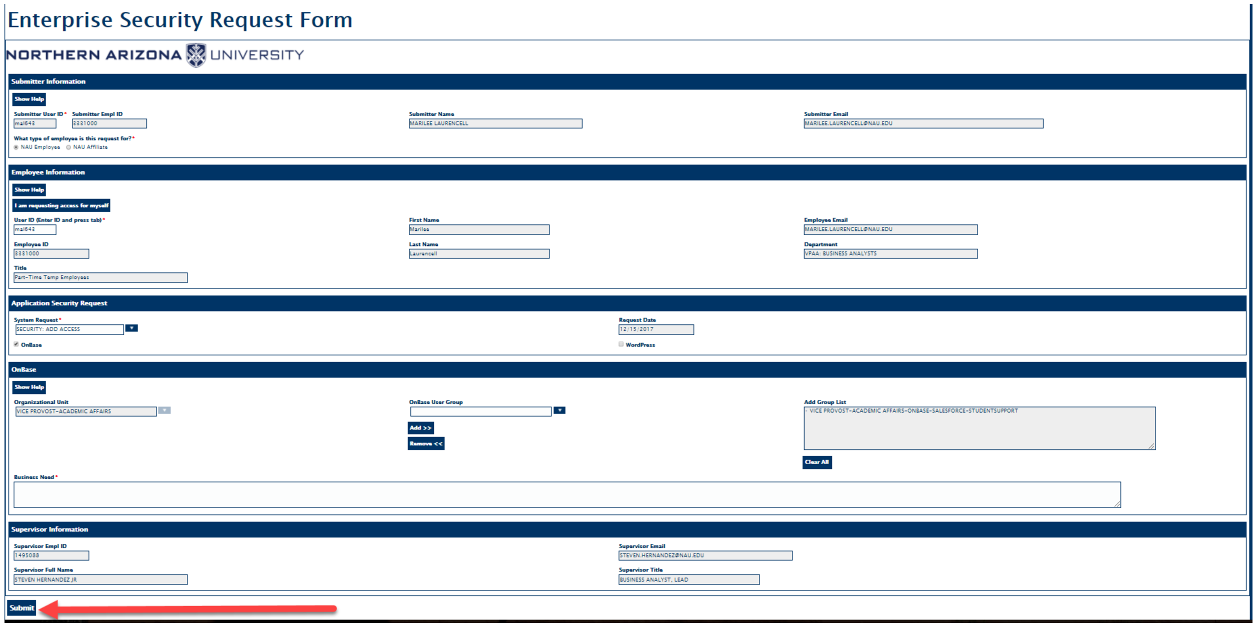
d) OnBase Section



i) For Organizational Unit, select "Vice Provost – Academic Affairs" from the dropdown list (see purple arrow in screen shot above)
ii) For OnBase user Group, select "Vice Provost – Academic Affairs - ONBASE - SALESFORCE – STUDENTSUPPORT" from the dropdown list (see green arrows in the screen shot above)
    (1) Select the "Add>>" button once the OnBase User Group has been selected. This will automatically populate the "Add Group List"
iii) Provide the "Business Need" for the access in the text box provided (see red arrow in screen shot above)

e) Supervisor Information
    i) Supervisor Information will be automatically populated, but update as needed

f) Click the "submit" button (see red arrow on screen shot below):

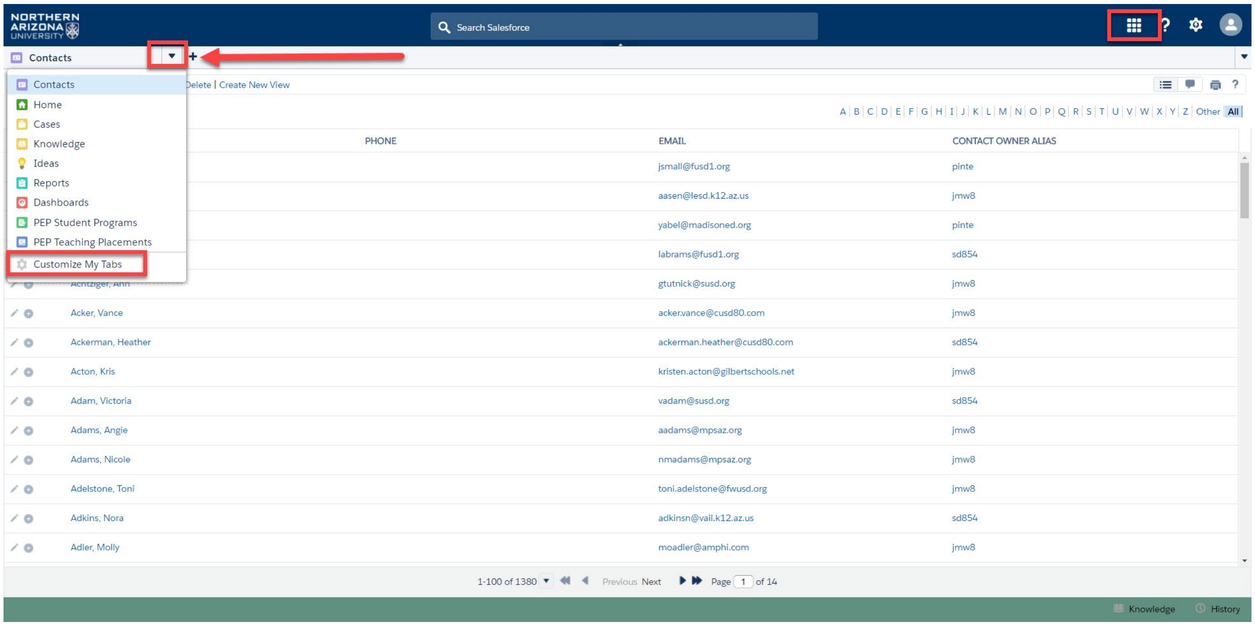


Chapter 2: Configuring the Salesforce Console for PEP

Once access to Salesforce has been obtained, it will be necessary to configure the Salesforce menus for ease of access to PEP information. The following steps detail one method for configuring the access. Please note that access to PEP data is based on the Salesforce role and permission sets. Not all users will have access to all areas of PEP (for example, general access to PEP financials is not allowed).

Step 1: Accessing Salesforce NAU Console

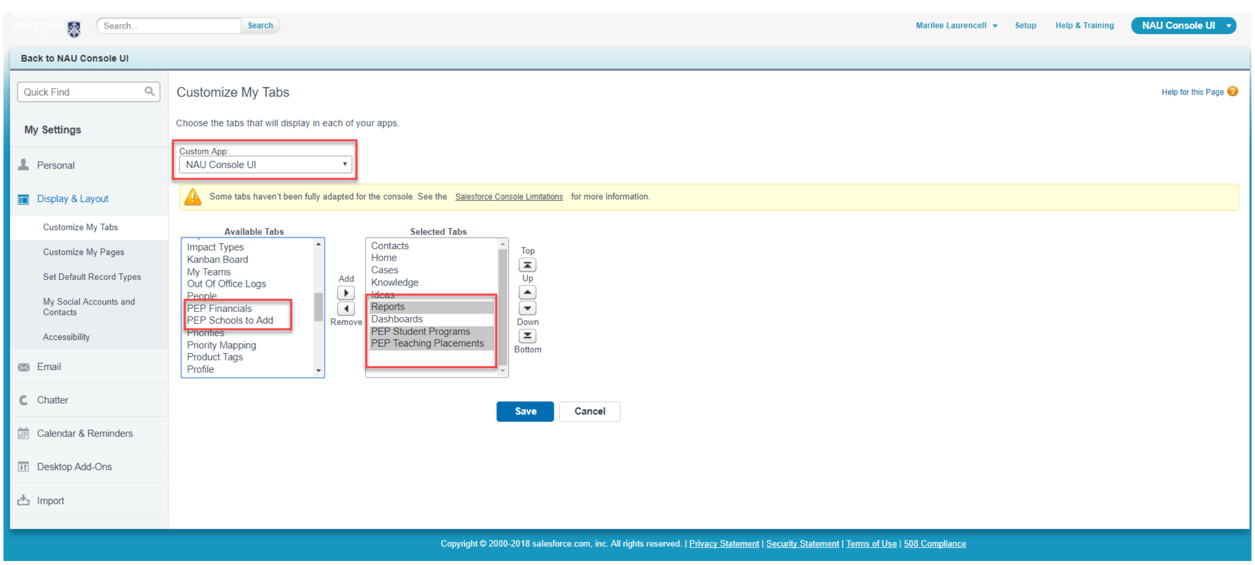
Upon initial access to Salesforce, the user will be presented with the default console (see screen shot below).



1) The grid highlighted in the upper right corner provides a drop down list of the available views
2) The drop down on the left side of the menu (see red arrow in screen shot above) provides a list of Salesforce "areas".
3) Select the "Customize My Tabs" option at the bottom of the drop down list

Step 2: Customizing the tabs

Upon selection of the Customize My Tabs option, the user can select the "tabs" to be displayed on their console (see screen shot below).



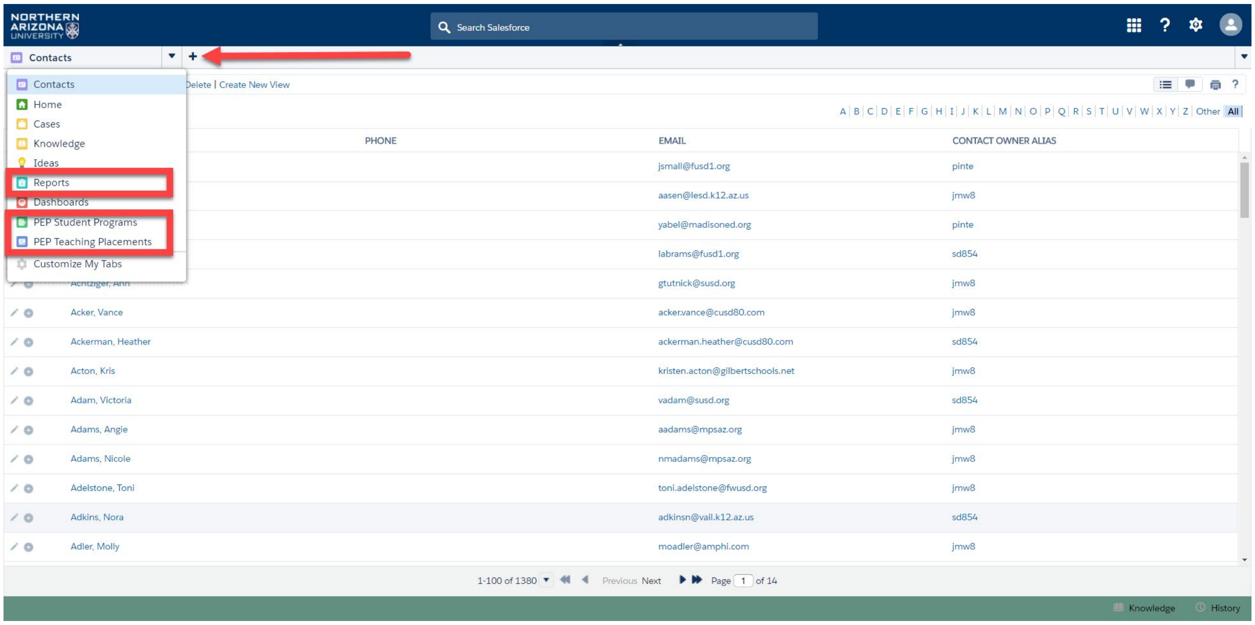
1) Selected the desired tabs from the "Available Tabs" list on the left side and click "add"
   a) For accessing PEP data, the following should be selected:
      i) PEP Student Programs

ii) PEP Teaching Placements

iii) Reports

b) Select the "Save" button to capture the selections and return to the previous screen

2) Selection of the tab drop down button (see red arrow below) will now show the selected tabs



APPENDIX

Security Attributes in Salesforce

Roles

Roles determine user access to objects, regardless of who owns those records. Users at any role level can view, edit, and report on all data that's owned by or shared with users below them in the role hierarchy.

- For example, you can set the contact access so that users in a role can edit all contacts associated with accounts that they own, regardless of who owns the contacts. And you can set the opportunity access so that users in a role can edit all opportunities associated with accounts that they own, regardless of who owns the opportunities.

Profiles

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one. Profiles are used to assign the minimum permissions and access settings for a specific group of users.

Every profile belongs to exactly one user license type.

Permissions

Every user is assigned only one profile, but can have multiple permission sets. Create permission sets to grant access among logical groupings of users, regardless of their primary job function.

- For example, let's say you have several users with a profile called Sales User. This profile allows assignees to read, create, and edit leads. Some, but not all, of these users also need to delete and transfer leads. Instead of creating another profile, create a permission set.

User Permissions

Specify what tasks users can perform and what features users can access.

Object Permissions

Specify the base-level access users have to create, read, edit, and delete records for each object.

Custom Permissions

Allows definition of access checks that can be assigned to users via permission sets or profiles, similar to how you assign user permissions and other access settings.

- For example, one can define access checks in Apex that make a button on a Visualforce page available only if a user has the appropriate custom permission.

Public / Personal Groups

A group consists of a set of users, which can contain individual users, other groups, or the users in a particular role. Everyone in the organization can use public groups.

- For example, an administrator can create a group for an employee carpool program. All employees can then use this group to share records about the program.

Change Log

Version	Date	Author	Description
V1.0		Marilee Laurencell	Initial release
V1.1	5/22/18	Marilee Laurencell	Added sharedrive access for IVP card; added change Log
V2.0	9/10/18	Marilee Laurencell	Added specific permissions for GAs supporting OFE
V2.1	10/17/18	Marilee Laurencell	Added additional roles for the ePass request
V2.2	1/8/2019	Marilee Laurencell	Added details for SF Lightning