



WEBER STATE
UNIVERSITY

Using Area Access Manager

Revised 06/28/17

Thank you for being a member of our Area Access Management Team!

Area Access Managers (AAMs) are a crucial part of ensuring that our students, employees and visitors are able to access the spaces needed to learn, teach, and connect. AAMs hold a high level of responsibility in their respective areas by granting and removing access as required by PPM 5-44a.

This training & reference guide will walk you through the your responsibilities as a Area Access Manager (AAM), including the basic steps of assigning electronic access rights to authorized WSU personnel. Cardholders you have granted access rights to will be able to use their credentials to enter assigned spaces that are otherwise secured in a Card Only status.

Only authorized individuals who have received training are authorized to use OnGuard Area Access Manager program.

By the end of this course, AAMs will be able to verify access for cardholders on campus, grant authorized access, and remove access in accordance with PPM 5-44a.

Training Objective Include an Understanding of:

- Electronic Access
- Personal Identification and Access Credentials Used on Campus
- [PPM 5-44a Electronic Access Policy](#)
- Requirements & Responsibilities
- Access Levels
- OnGuard Area Access Manager

Should you have any questions regarding the use of Area Access Manager, contact the Central Access Manager at CardAccess@weber.edu or the Facilities Management Key & Lock Shop at the numbers below:

Key & Lock Shop.....x8095
Manager.....x8042
FM Help Desk.....x6331
Afterhours.....x6693

Definitions:

Electronic Access: Any access rights that are granted through the use of Weber State University credentials and administered through the Central Electronic Access Control System.

Stand-Alone Electronic Access: Electronic access locks that are not administered through the Central Electronic Access Control System. Stand-alone locks are departmentally owned equipment. Departments individually maintain and program stand-alone locks.

Credentials: Any technology that is supported and authorized by Weber State University to be utilized with the electronic access system. Common credentials currently used at WSU include MAG and/or PROX cards.

MAG cards: Standard issue Wildcards with a magnetic strip on the reverse side. MAG cards are used by swiping them at a reader (similar to swiping a credit card).

PROX cards: Proximity cards look similar to standard issue Wildcards and they include embedded circuitry and technology that allows a reader to recognize cards presented to a reader within a designated proximity. Holding a PROX card in front of a reader for approximately one second allows the credential to be scanned for recognition.

Area Access Manager (AAM): Person responsible for administering electronic access rights to approved cardholders in specific areas. The appropriate Vice President or Dean will determine the AAM position.

Approvers: The employees responsible for authorizing access to be granted. A separation of duties is required between those who are Approvers and those who are AAMs. Always maintain documentation of who approved an access request.

Access Level: Any reader or combination of readers combined with a Timezone. Access Levels are created and managed by the Central Access Manager.

Timezone: A predetermined schedule of days of the week and times of the day when an attached action will occur.

Deactivation: A scheduled date and time upon which an access level will deactivate.
Student access must be scheduled to deactivate each quarter per PPM 5-44A.

OnGuard Area Access Manager

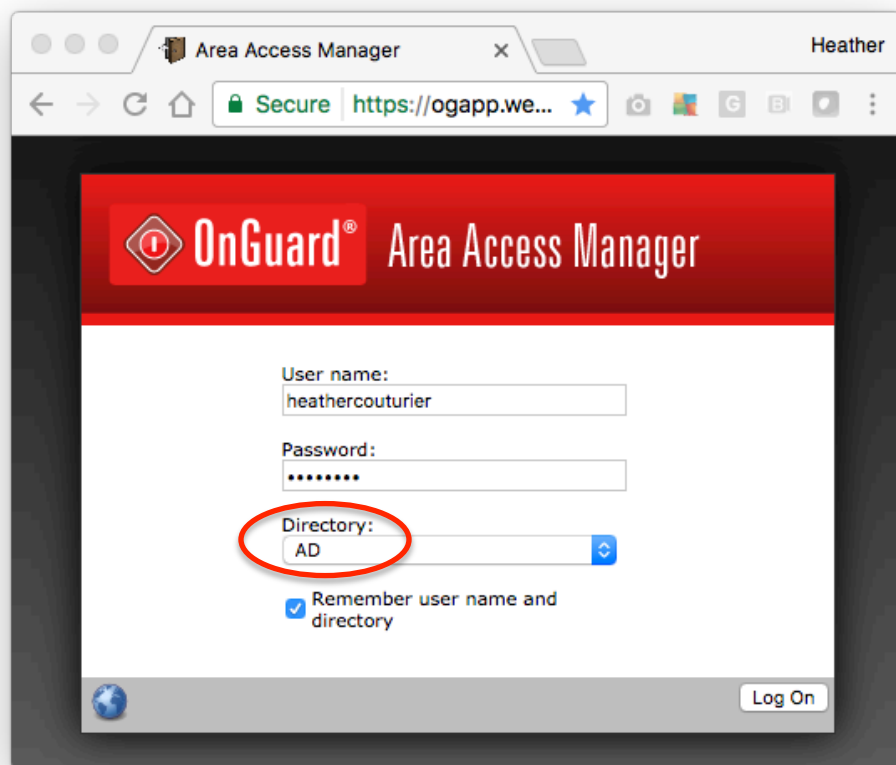
OnGuard Area Access Manager is a web application you can use to assign and remove access levels to an individual's credentials. You must be logged on to the secure server in order to access the program. This means you will be accessing the program while on campus.

A link to OnGuard Area Access Manager is maintained on the Facilities Management Key & Access website at http://weber.edu/facilities/Keys_and_Access.html

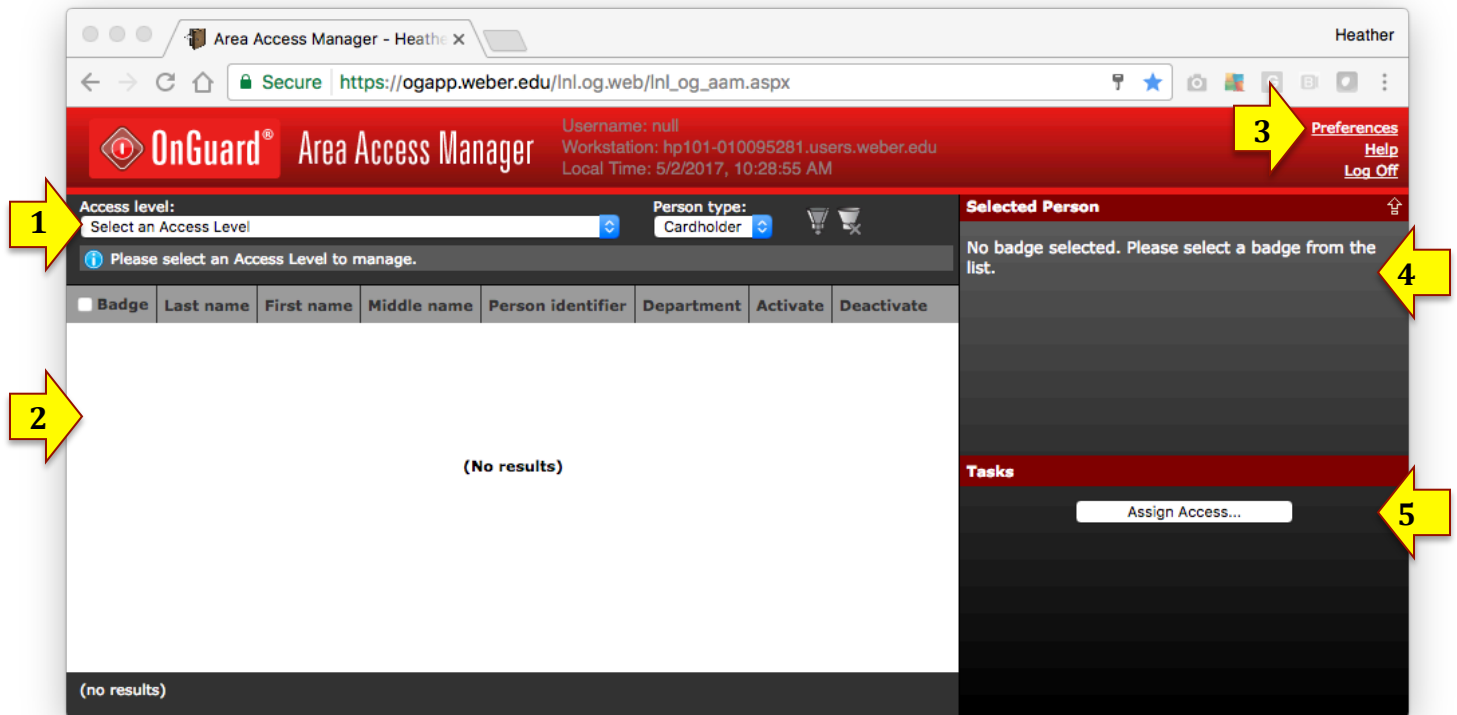
NOTE: Weber State University has a limited number of licenses available for OnGuard Area Access Manager. If you have difficulties logging in, please try again later. If you continue to have difficulties, contact the Central Access Manager at CardAccess@weber.edu or call the Lockshop at x8042 or x8095.

Logging In to Area Access Manager

Step 1: Log on to [Area Access Manager](#) with your eWeber user name & password. Make sure to set your directory to 'AD' (See circle below).



Review of OnGuard Area Access Manager Window



1. The **Access Level** dropdown menu allows you to select and view any access level currently assigned to you.

2. The **Badge Results panel** will populate when you choose one to see all currently assigned individuals in that access level.

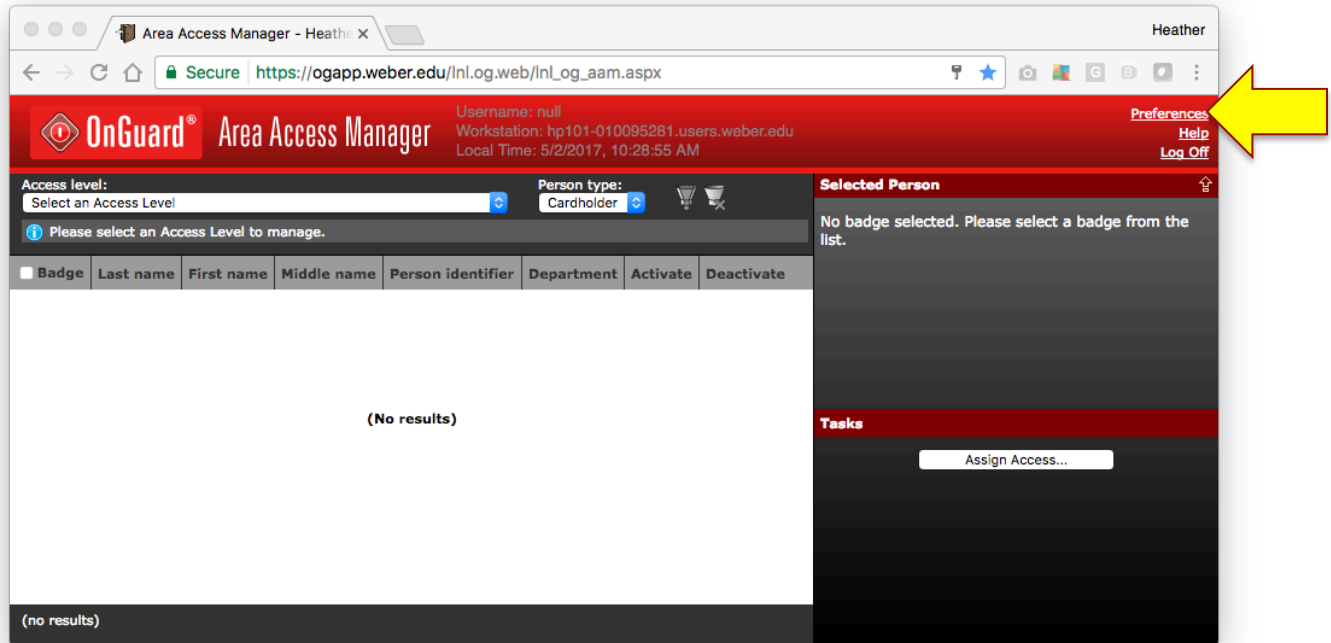
3. The **Preferences** link allows you to ensure you will be able to see all badges assigned to an individual.

4. The **Selected Person panel** will populate with information when you have selected an individual badge.

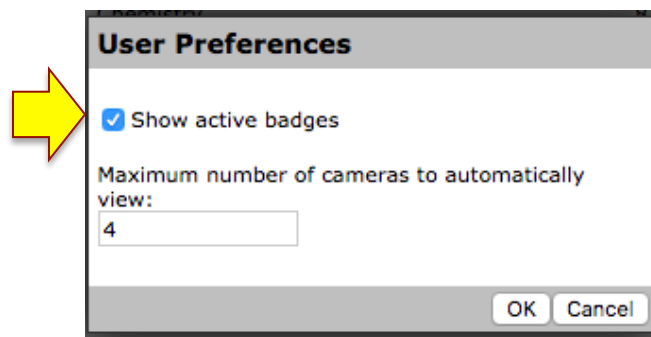
5. The **Tasks panel** shows the currently available tasks and actions available.

Getting Started

Step 1: Click **Preferences** in the upper right corner of the OnGuard Area Access Manager window.



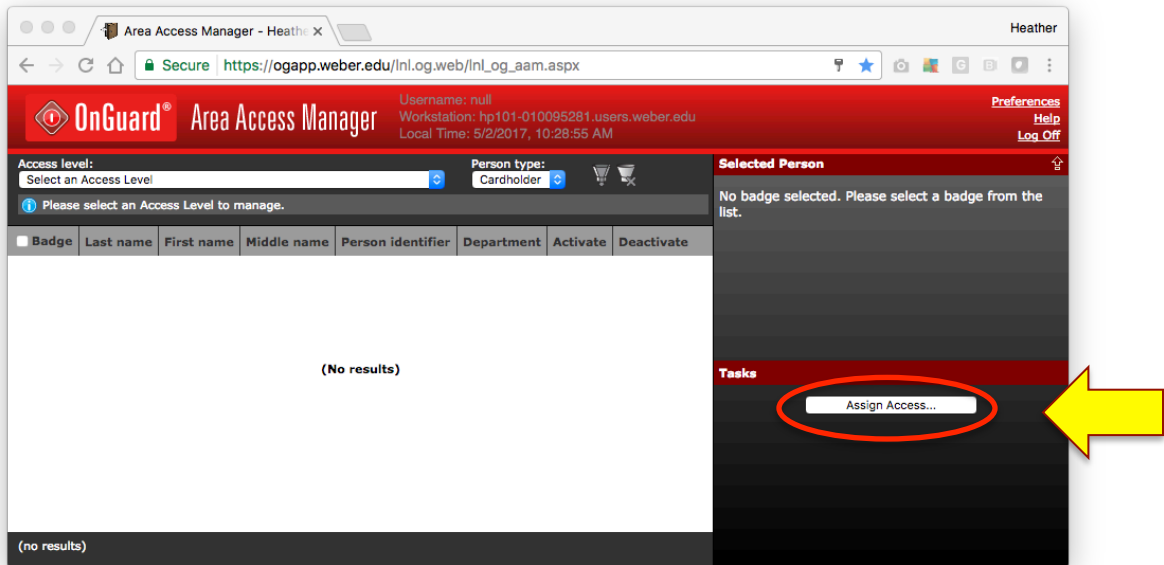
Step 2: Verify the checkbox next to **Show active badges** is selected. Then click **OK**.



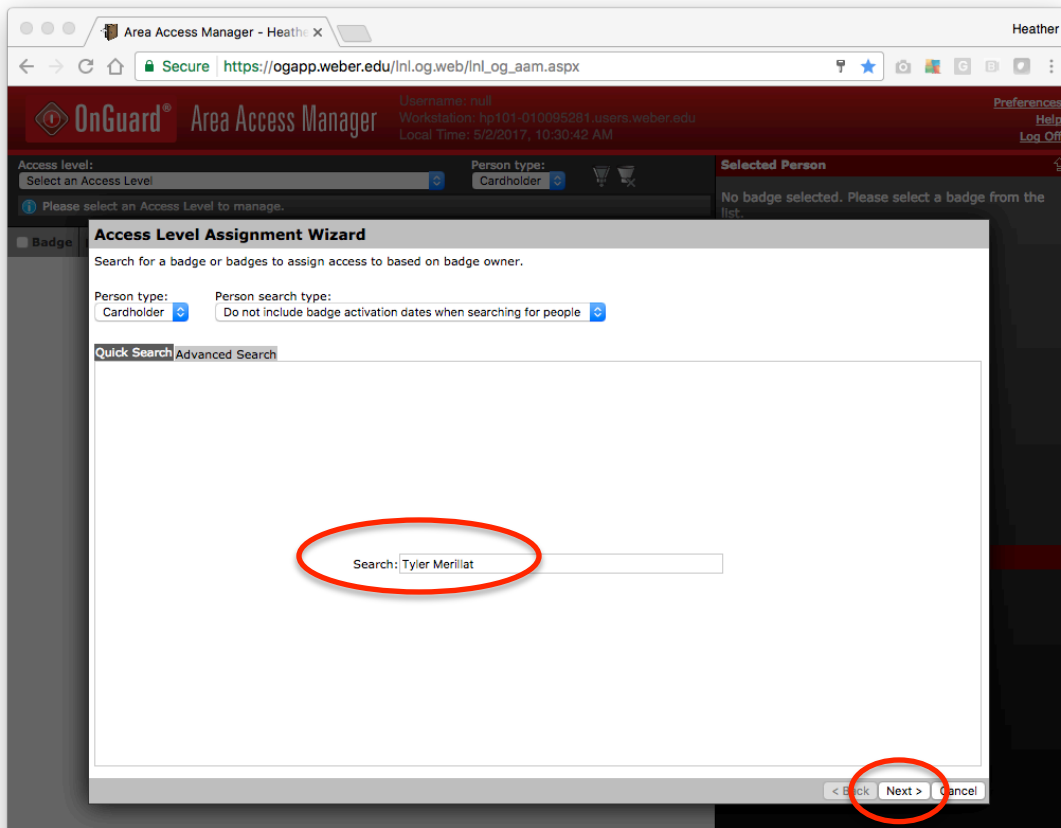
*If you aren't able to see a person's badge type (MAG, PROX, or both), this checkbox has **not** been selected. This is important when considering what reader types are within your access levels!*

Assigning Access in Area Access Manager

Step 1: Click **Assign Access** in the Tasks panel



Step 2: Enter the individual's name and click **Next** (or press [Enter]).



Step 3: Select the appropriate check box(es) next to the appropriate individual.

Area Access Manager - Heather X

Secure https://ogapp.weber.edu/inflog/web/inflog_aam.aspx

Username: null
Workstation: hp101-010095201 users.weber.edu
Local Time: 5/2/2017, 10:31:46 AM

Preferences
Help
Log Off

Access level: Select an Access Level
Person type: Cardholder

Please select an Access Level to manage.

Access Level Assignment Wizard
Select the badges to assign access to.

View

Search results:

Badge	Last name	First name	Middle name	Person
<input type="checkbox"/> ID: 6013160004510552 (Type: MAG STRIPE)	MERILLAT	TYLER		W0131
<input type="checkbox"/> ID: 7299 (Type: PROXIMITY)	MERILLAT	TYLER		W0131

View

Selected:

No badge selected. Please select a badge from the list.

Results: 1-2 of 2 badges (viewing active badges)

< Back Next > Cancel



You can verify what access a cardholder already has by clicking the **View** button above the checked box next to their ID. Using this method, you can view tabs containing the information about the cardholder, the badges issued to them, and the access levels already assigned.

Access Level Assignment Wizard
Select the badges to assign access to.

View

Search results:

Badge	Last name	First name	Middle name	Person
<input checked="" type="checkbox"/> ID: 6013160003465535 (Type: MAG STRIPE)	WILDCAT	WALDO		

WALDO WILDCAT

Cardholder Badges Access Levels

Last name: WILDCAT First name: WALDO Middle name:

Cardholder W or Z#: W01141394

Address:

City:

State:

Zip code:

Phone:

Birth date:

E-mail: waldowilcat@mail.weber.edu

Record last changed: 5/15/2017 1:30:09 pm

Title: none

Department:

Division: Current Student

Location:

Building:

Floor:

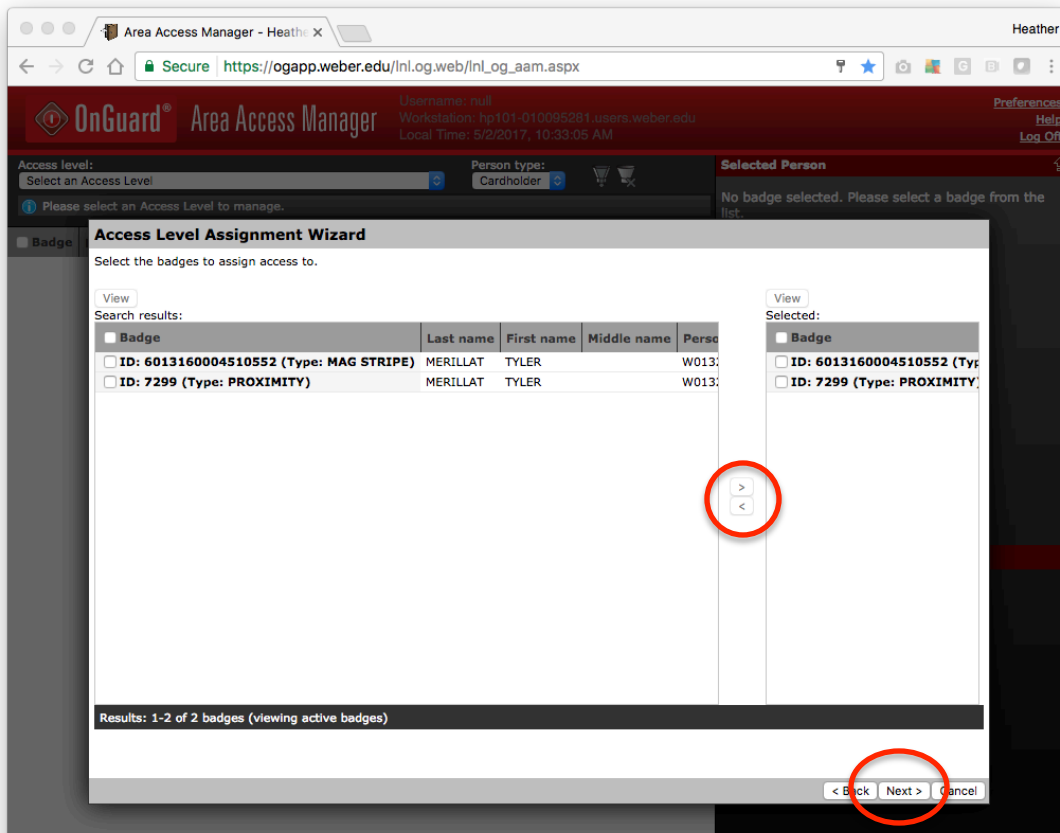
Office phone:

Extension:

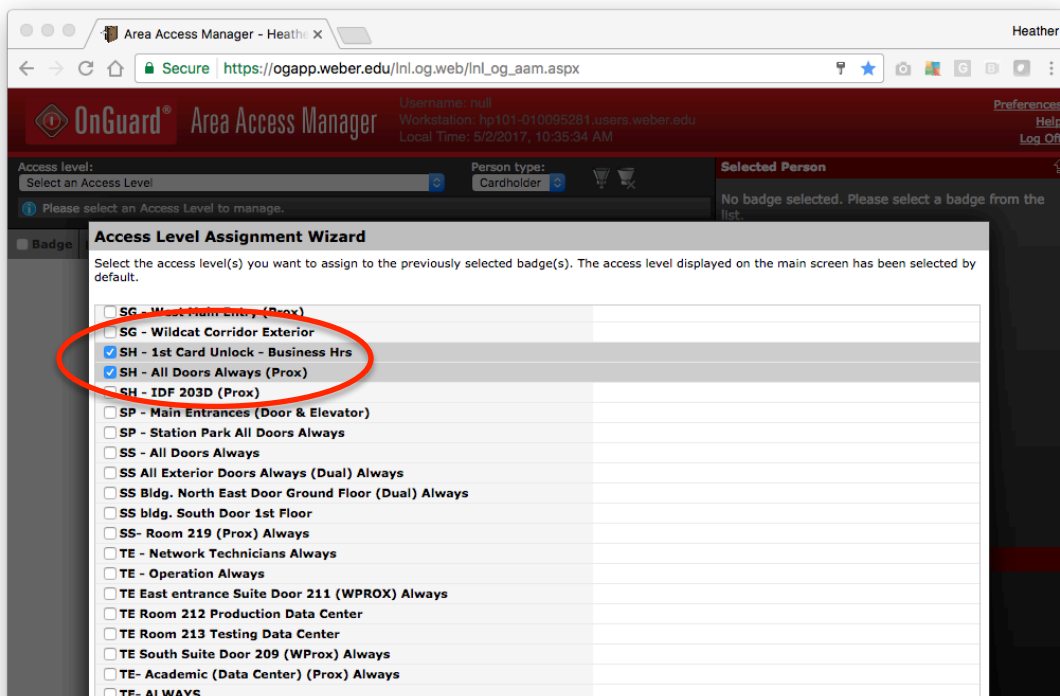
*This is extremely useful, as **each card type cannot have more than 6 access levels.** More than 6 access levels assigned to a card will cause the card to not work properly.*

Contact CardAccess@weber.edu or call us at x8042 with any questions on specific cardholders. We're happy to help.

Step 4. Use the [>] right arrow to add the individual to the Selected list. Click **Next**.



Step 5: Select the appropriate access level for the individual using the checkboxes.





Remember: All Student Access must be set to expire each semester.

Set up your deactivation times for students or other short-term access (such as adjunct faculty) in advance to avoid forgetting them later.

1. Select the **Deactivation date checkbox** to activate the option

Deactivation date: ☒

2. Click the **calendar icon** and select the appropriate date for deactivation.

3. Verify the time at which the deactivation will take effect. The default is 12:00 am (Midnight at the beginning of the selected date)

4. Click the **Set Date/Time** button

5. Verify the deactivation date and time is displayed in the wizard before proceeding. An example is circled for you below. When ready, click **Next**.

Area Access Manager - Heather X

Secure https://ogapp.weber.edu/lnl/og.web/lnl_og_aam.aspx

Username: null
Workstation: hp101-010095281.users.weber.edu
Local Time: 5/2/2017, 10:38:58 AM

Access level: Select an Access Level

Person type: Cardholder

Selected Person: No badge selected. Please select a badge from the list.

Please select an Access Level to manage.

Access Level Assignment Wizard

Select the access level(s) you want to assign to the previously selected badge(s). The access level displayed on the main screen has been selected by default.

Access Level	Deactivation date:
<input type="checkbox"/> SG - West Main Entry (Prox)	
<input type="checkbox"/> SG - Wildcat Corridor Exterior	
<input checked="" type="checkbox"/> SH - 1st Card Unlock - Business Hrs	8/26/2017 12:00:00 am
<input checked="" type="checkbox"/> SH - All Doors Always (Prox)	8/26/2017 12:00:00 am
<input type="checkbox"/> SH - IDF 203D (Prox)	
<input type="checkbox"/> SP - Main Entrances (Door & Elevator)	
<input type="checkbox"/> SP - Station Park All Doors Always	
<input type="checkbox"/> SS - All Doors Always	
<input type="checkbox"/> SS All Exterior Doors Always (Dual) Always	
<input type="checkbox"/> SS Bldg. North East Door Ground Floor (Dual) Always	
<input type="checkbox"/> SS bldg. South Door 1st Floor	
<input type="checkbox"/> SS- Room 219 (Prox) Always	
<input type="checkbox"/> TE - Network Technicians Always	
<input type="checkbox"/> TE - Operation Always	
<input type="checkbox"/> TE East entrance Suite Door 211 (WPROX) Always	
<input type="checkbox"/> TE Room 212 Production Data Center	
<input type="checkbox"/> TE Room 213 Testing Data Center	
<input type="checkbox"/> TE South Suite Door 209 (WProx) Always	
<input type="checkbox"/> TE- Academic (Data Center) (Prox) Always	
<input type="checkbox"/> TE- ALWAYS	

Activation date:

Deactivation date: ☒ 8/26/2017 12:00:00 am

Set Date/Time Clear Date/Time

< Back Next > Cancel

Final Step: Verify the access level assignments for individual, access level, and any activation or deactivation information.

If incorrect, click **Back** and correct the error(s). Otherwise, click **Finish**.

Area Access Manager - Heather X

Secure | https://ogapp.weber.edu/lnl.og.web/lnl_log_aam.aspx

Username: null
Workstation: hp101-010095281.users.weber.edu
Local Time: 8/18/2017, 5:19:25 PM

Access level: Select an Access Level
Person type: Cardholder
Selected Person: No badge selected. Please select a badge from the

Access Level Assignment Wizard

Badge(s) to receive the access level assignment(s):

Badge	Last name	First name	Middle name	Person identifier	Department
ID: 6013160003465535 (Type: MAG STRIPE)	WILDCAT	WALDO		W01141394	

Access level(s) to assign:

Name	Activate	Deactivate
TY - Biochem Student Research		8/14/2017 12:00:00 am

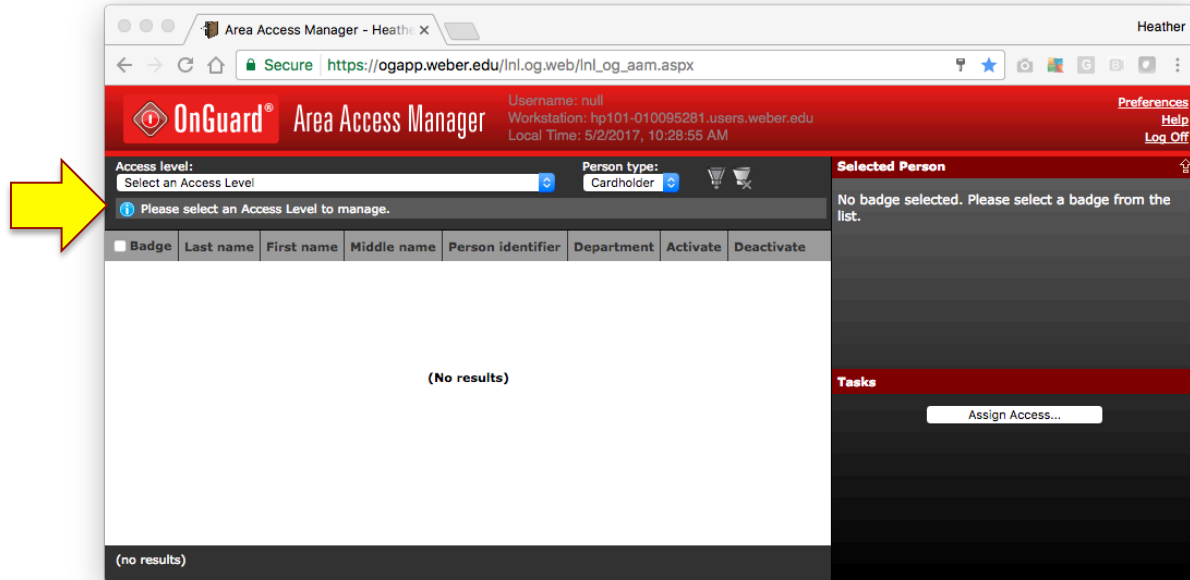
< Back Finish Cancel

In the above example, Waldo is being granted access to the Biochem Student Research access level in Tracy Hall until 12:00 am on August 14, 2017.

If we click finish, the access will be added and we will be able to view him in the access level as shown in the next section.

Reviewing Access Levels in Area Access Manager

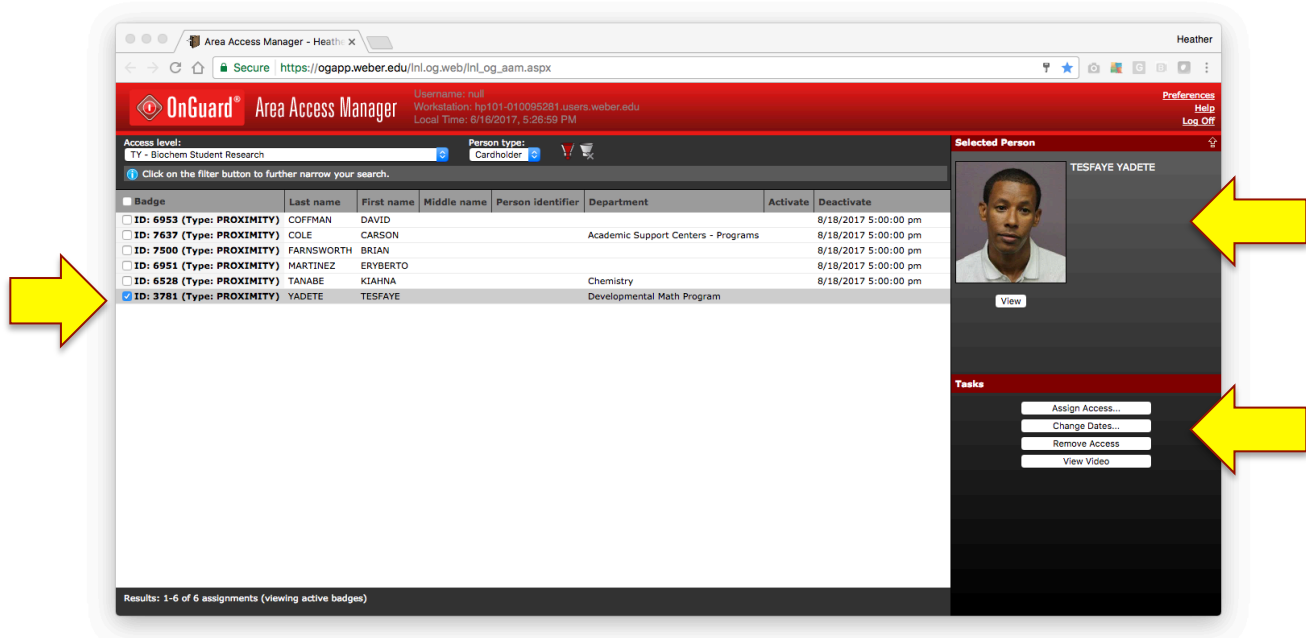
Step 1: Click **Select an Access Level** dropdown menu and select an access level to review.



The Badge Results area of the page will populate with all badges currently assigned the selected access level.



Clicking on a checkbox allows you to see the Wildcard photo for the selected individual & opens additional actions in the Task panel, allowing you to change activation or deactivation dates, or to remove the person's access immediately.





The following actions will only affect the single access level you are reviewing. If an individual has more than one access level under your management, you'll need to perform this action in each access level.

Adjusting Activation/Deactivation Dates

Step 1: Click **Select an Access Level** dropdown menu and select an access level to review (as shown on the previous page).

Step 2: Click the **Change Dates** button.

Step 3: Click the checkbox for the desired date change to activate the option.

Step 4: Click the calendar icon.

Step 5: Click the date for the desired activation or deactivate, then click **Select**.

The screenshot shows a 'Change Dates' dialog box. It contains two rows of controls. The first row is for 'Activation date:' and the second row is for 'Deactivation date:'. Each row has a checkbox on the left and a date input field with a calendar icon on the right. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Step 6: Verify or update the time of the selected day for the desired action.

Step 7: Click **OK**

Step 8: Verify the activation/deactivation is displayed on the access level list for the selected individual(s)

Deactivating Access Levels Immediately

Step 1: Click **Select an Access Level** dropdown menu and select an access level to review (as shown on the previous page).

Step 2: Click the **Remove Access** button.

Step 3: Read the warning message. Click **Yes** to confirm or **No** to cancel.

Notes:

Building/Area: _____

Area Access Manager: _____

Backup Area Access Manager: _____

[illegible]