

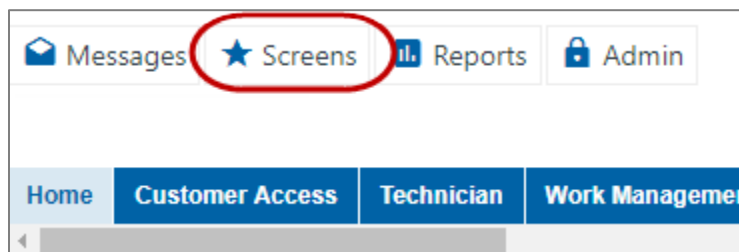
The following information describes how to set up and use your company issued keycards to log into the EAM system.

- ❗ Do not open or use the same instance of the Web Modules in multiple browser windows or tabs. This can cause errors or unexpected performance issues.

1. Set-up

In order to configure the keycard log in, there are two types of data that must be set up and a workstation plug-in must be installed for EAM to validate and log in the user using a keycard.

Data setup is typically done through the system's Enterprise Portal screens that can be accessed by clicking the Screens button at the top, left corner of the Web Modules. .



Setting a Pin

The first type of data is the PIN set for EAM users that will use a keycard. The PIN can be set on a user's record using the Users Screen in the Enterprise Portal.

The PIN field is located under Security Options tab on the Users screen.

- ✔ A user's PIN can be up to 6 numeric digits.

The screenshot shows the 'Users' screen in the Enterprise Portal. The top navigation bar includes 'Users', 'ADMIN MODE', and 'CHANGE REQ'. Below the navigation bar are buttons for 'Search', 'Reload', 'Sort', 'Select Filter', 'Select Sort', 'New', 'Copy', 'Delete', and 'Edit'. The left sidebar contains a list of tabs: 'Basic Info', 'Groups Currently Assigned', 'Comments', 'Security Options' (highlighted in orange), and 'Printers'. The main content area displays the 'Security Options' for a user. It includes fields for 'Date and time password was last changed' and 'Date and time of last login'. There are three checkboxes: 'User must change password at next login', 'Requires external authentication', and 'Password never expires'. Below these is a checkbox for 'Login is disabled' with a 'Reason' field. At the bottom, there is a checkbox for 'Mobile user' and a 'PIN' field, which is circled in red. The 'PIN' field is a text input box.

Setting Keycard Information

The second type of data is for the keycard itself and who it is issued to. This information is edited on the Access Keys screen in Enterprise Portal.

The Access Keys screen allows tracking of keycards, the card information associated to it, and what the card is issued to. The card must be issued to the associated user for keycard sign-in to work, either directly to the user or through the employee record associated to the user.



Note: The card identifier field entered should reflect the identifier read by the keycard holder.

The system will validate to ensure any keycards used here are of ISSUED status and assigned to the same user who is using the keycard when logging in.

Access Keys ADMIN MODE CHANGE REQUEST HELP

Search Reload Sort Select Filter Select Sort New Copy Delete Edit Save Cancel

Access key ID

Basic Info

Key type: HID, MAG, RFID, PHYSICAL KEY, OTHER

Key status: NOT ASSIGNED, **ISSUED**, RETURNED, LOST

Facility code

Card identifier

Card PIN

Assigned to:

Employee ID

Equipment ID

Operator ID

User ID

Part ID Part suffix Serial number

Department ID

Comment

Facility and stationary equipment information

Location ID

Location asset ID

Setting-up Keycard Software

The last requirement to setup keycards is the software for workstations to read the keycard holder. As the system runs as a web application, a plug-in is required to allow a web application to communicate with hardware connected to the workstation. The installer itself is available within a web deployment of the system and can be installed by doing either of the following:

- IT, using group policy to workstations, grabbing from the web deployment files for deployment
- Downloading directly from Web Modules as an administrator to a workstation

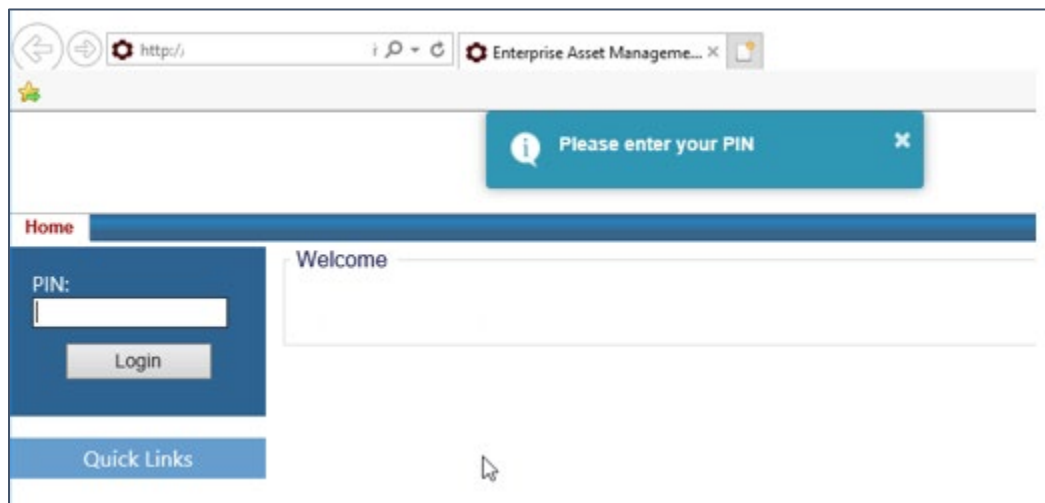


Note: The plug-in is only designed for workstations using Internet Explorer browsers.

2. Logging In

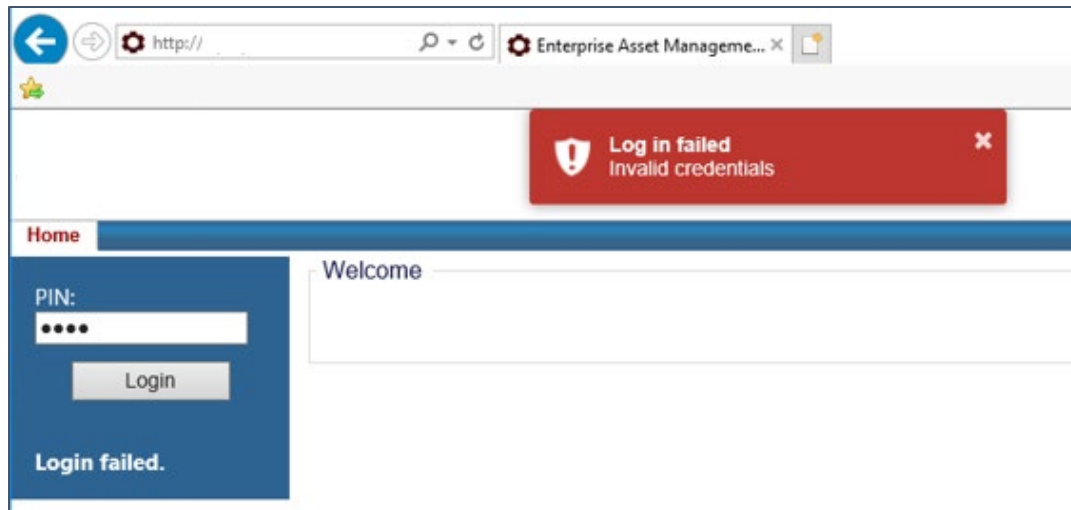
Workstations must be equipped with keycard holders. When EAM Web Modules is opened on the browser, the user will insert their keycard into the keycard holder.

The keycard holder will communicate the card information to the browser and the EAM log in process will prompt the technician for a PIN, putting focus into the PIN field now shown. Note it is by design not to communicate the validity of the card at this point.



If the user enters a PIN that matches their user record and the card identifier matches the issued card to the user, the technician will be logged into EAM with no further input required.

If the technician enters an invalid PIN or the keycard is considered invalid, then the technician will be shown a log in failed message.



Possible reasons for failed logins are as follows:

- Invalid PIN is entered
- Card Identifier is not recognized, meaning the keycard is not registered within EAM
- Keycard must be assigned and ISSUED to a user. If a card is set to another status, such as LOST, the system will not allow for login.

3. Logging Out

While logged into EAM, the system will be aware that the technician logged in using a keycard and PIN. EAM Web Modules will check the card status. When the technician pulls the keycard from the keycard holder, it will trigger Web Modules to log out the technician with no further input required.

This is the same process as if the technician clicked the **Logoff** button.

A log off message is flashed, usually only for a second, before being redirected back to the main page.

Please wait while being logged off.