Sharma, Abhinav - (abhinavsharma)

Arizona Research Labs

ilab: Software Interlock Guide

Table of Contents

[Accessing the Sassafras Server 4](#_Toc501373243)

[Sassafras Server Access Permissions 4](#_Toc501373244)

[Connection Settings 4](#_Toc501373245)

[Connecting to the Sassafras Server 4](#_Toc501373246)

[Installing the VPN Client 4](#_Toc501373247)

[Setting up Sassafras 4](#_Toc501373248)

[Installation of Sassafras Server 4](#_Toc501373249)

[Setting up KeyConfigure (i.e. Sassafras Admin): 5](#_Toc501373250)

[Login 5](#_Toc501373251)

[Setup iLab communications in Sassafras 5](#_Toc501373252)

[Installation of Sassafras Client: 9](#_Toc501373253)

[Setting up a software interlock: 9](#_Toc501373254)

[Locate Computer ID in Sassafras 9](#_Toc501373255)

[Software Interlock Creation in iLab: 10](#_Toc501373256)

[Create new software interlock for each piece of equipment to be managed: 11](#_Toc501373257)

[Configuring Applications and Policies in Sassafras 11](#_Toc501373258)

[Create a Product 11](#_Toc501373259)

[Create Policies in Sassafras 14](#_Toc501373260)

[Create a Sassafras Group 14](#_Toc501373261)

[Create the Deny Policy 15](#_Toc501373262)

[Create the Allow Policy 17](#_Toc501373263)

[Disabling the Software Interlock 20](#_Toc501373264)

[Disabling the Software Interlock within iLab 20](#_Toc501373265)

[Disabling the software interlock within Sassafras 21](#_Toc501373266)

[Disabling the software interlock in case of Network Outage: 21](#_Toc501373267)

[Enabling a disabled software interlock policy 21](#_Toc501373268)

[Enabling a disabled software Interlock policy within iLab 21](#_Toc501373269)

[Enabling a disabled software interlock within Sassafras 23](#_Toc501373270)

[Enable the software interlock after a Network Outage: 23](#_Toc501373271)

[iLab Settings and Software Interlock Behavior 23](#_Toc501373272)

[Access the iLab Setting for Core: 24](#_Toc501373273)

[Settings for the core (Time and duration settings): 25](#_Toc501373274)

[Minimum reservation time: 25](#_Toc501373275)

[Maximum reservation time: 25](#_Toc501373276)

[Time Steps: 25](#_Toc501373277)

[Time when reservation is considered a no-show: 25](#_Toc501373278)

[How much in advance can a reservation be started: 26](#_Toc501373279)

[Time when reservation is considered a walk-out: 27](#_Toc501373280)

[Time when to notify user about walk-out 27](#_Toc501373281)

[Settings for the core (Common Settings): 27](#_Toc501373282)

[Allow walk ups: 27](#_Toc501373283)

[Strict payment information: 28](#_Toc501373284)

[Allow multiple logons per reservation: 29](#_Toc501373285)

[Shut off equipment when terminating walk outs 30](#_Toc501373286)

[Ending an Active Session in iLab 30](#_Toc501373287)

[As a PI or Customer 30](#_Toc501373288)

[As a Core or Institutional Admin 31](#_Toc501373289)

[Additional Resources 31](#_Toc501373290)

Sassafras Setup:

File location:<Quick-Books Path and Snapshots>

# Accessing the Sassafras Server

## Sassafras Server Access Permissions

Access to this server can be granted by Jason Pototsky, Manager, Information Technology. He may be contacted via Email [jpototsk@email.arizona.edu](mailto:jpototsk@email.arizona.edu) or via phone: 520-621-5523.

## Connection Settings

Sassafras Server

Host URL: sarsaparilla.arl.arizona.edu

Host IP address: 10.130.165.32

## Connecting to the Sassafras Server

You will need to connect to the network via the UA’s VPN Client regardless of whether or not you are using an on-campus computer to access the Sassafras Server. Currently UA uses Cisco AnyConnect Secure Mobility Client. If you do not know how to install the VPN Client go [here](http://applewebdata://15E6B889-AA5A-44C9-A60D-F8085A60BDC1#_Installing_the_VPN).

1. Open the VPN Client Software.
2. Connect to the network via the VPN by either of the following: (i) selecting UA SSL VPN from the drop down or (ii) by entering **vpn.arizona.edu** manually.
3. Open Microsoft Remote Desktop and enter the Sassafras Server URL: sarsaparilla.arl.arizona.edu. The server will require you to login using your official UA email (i.e. [net\_id@email.arizona.edu](mailto:net_id@email.arizona.edua)) and NetID password.

## Installing the VPN Client

1. Go [here](https://it.arizona.edu/service/ua-virtual-private-network-vpn) to download and install the UA’s VPN Client. Go [here](https://it.arizona.edu/documentation/ua-vpn-download-and-installation-instructions-windows) for help with this process.
2. You will need to be enrolled in NetID+ to use the VPN Client. You can enroll [here](https://webauth.arizona.edu/netid-plus/). If you need assistance with the Duo Mobile App for two factor authentication you can find it [here](https://it.arizona.edu/documentation/connect-ua-vpn-using-duo-mobile-app).

# Setting up Sassafras

## Installation of Sassafras Server

This has already been done for the U of A on sarsaparilla.arl.arizona.edu.

After following the connection process mentioned in [Connecting to the Sassafras Server](#_Connecting_to_the), these simple installation steps need to be followed:

1. Install the KeyServer on the designated server will all the default settings.

Note: It is a background service and no Program Window would be opened.

1. Install the Windows Admin on the designated server with all the default settings. The software KeyConfigure is now installed on the machine.

# Setting up KeyConfigure (i.e. Sassafras Admin):

## Login

The Sassafras Server and Admin run on the same virtual machine (i.e. sarsaparilla.arl.arizona.edu). The following credentials must be entered:

**Server:** localhost

**Name:** Administrator

**Password:** See stache

Note 1: In case of a fresh installation, the password is reset to “Sassafras” by default.

Note 2: If you are installing Sassafras Admin on a computer other than the designated server, use the Server’s IP Address instead of “localhost,” in this case 10.130.165.32.

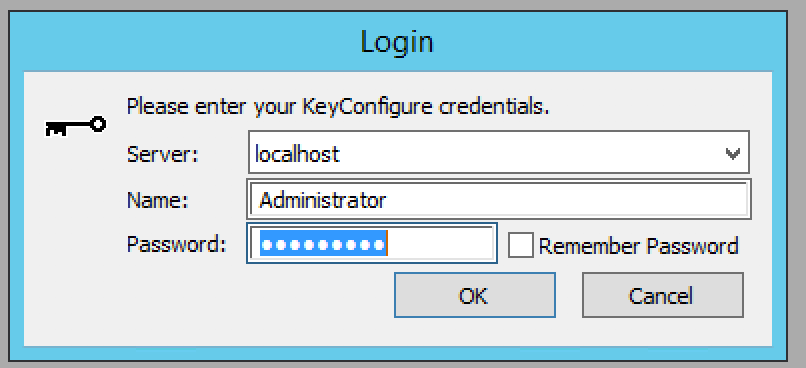


Figure 1 Sassafras Admin Login

Setup iLab communications in Sassafras:

Add iLab Authentication within the KeyServer

1. In Sassafras, open Config > Client Authentication as seen below

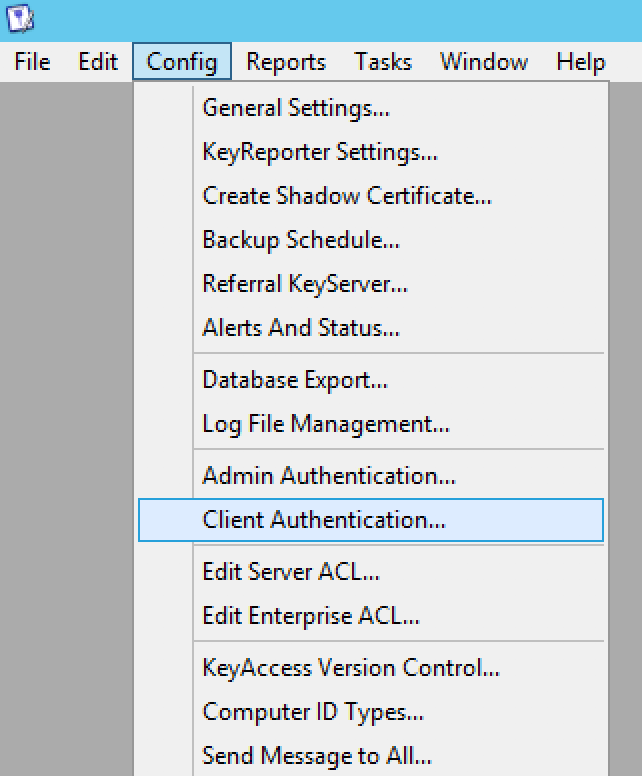


Figure 2 iLab in Sassafras setup: Client Authentication

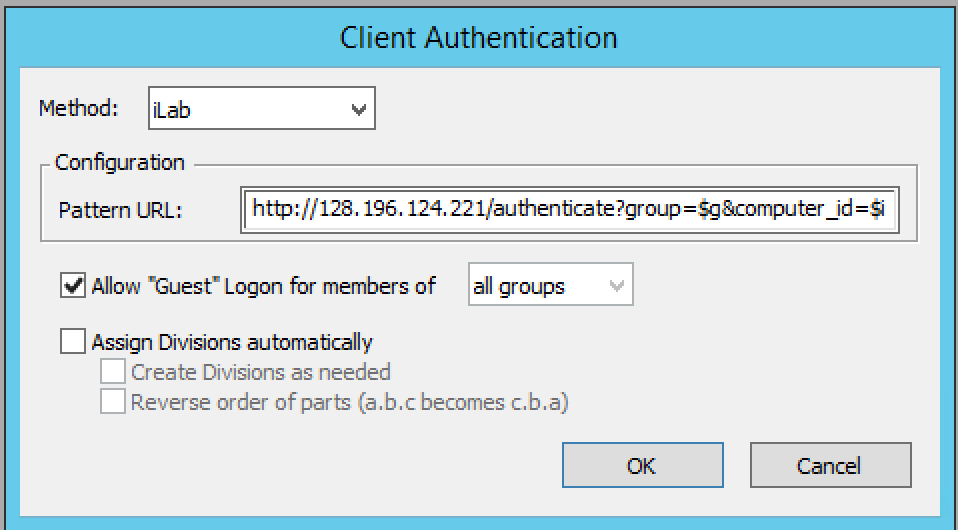
1. Choose method: iLab, and set the Pattern URL to the following:

http://<bridgeIPaddress>/authenticate?group=$g&computer\_id=$i

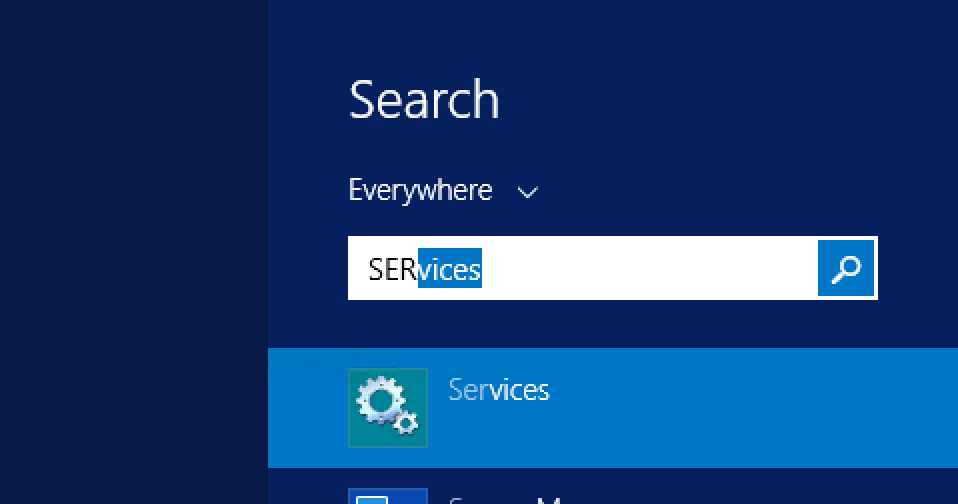
where “<bridgeIPaddress>” is the static IP address of the iLab Bridge. In our case the Pattern URL is:

<http://128.196.124.221/authenticate?group=$g&computer_id=$i>

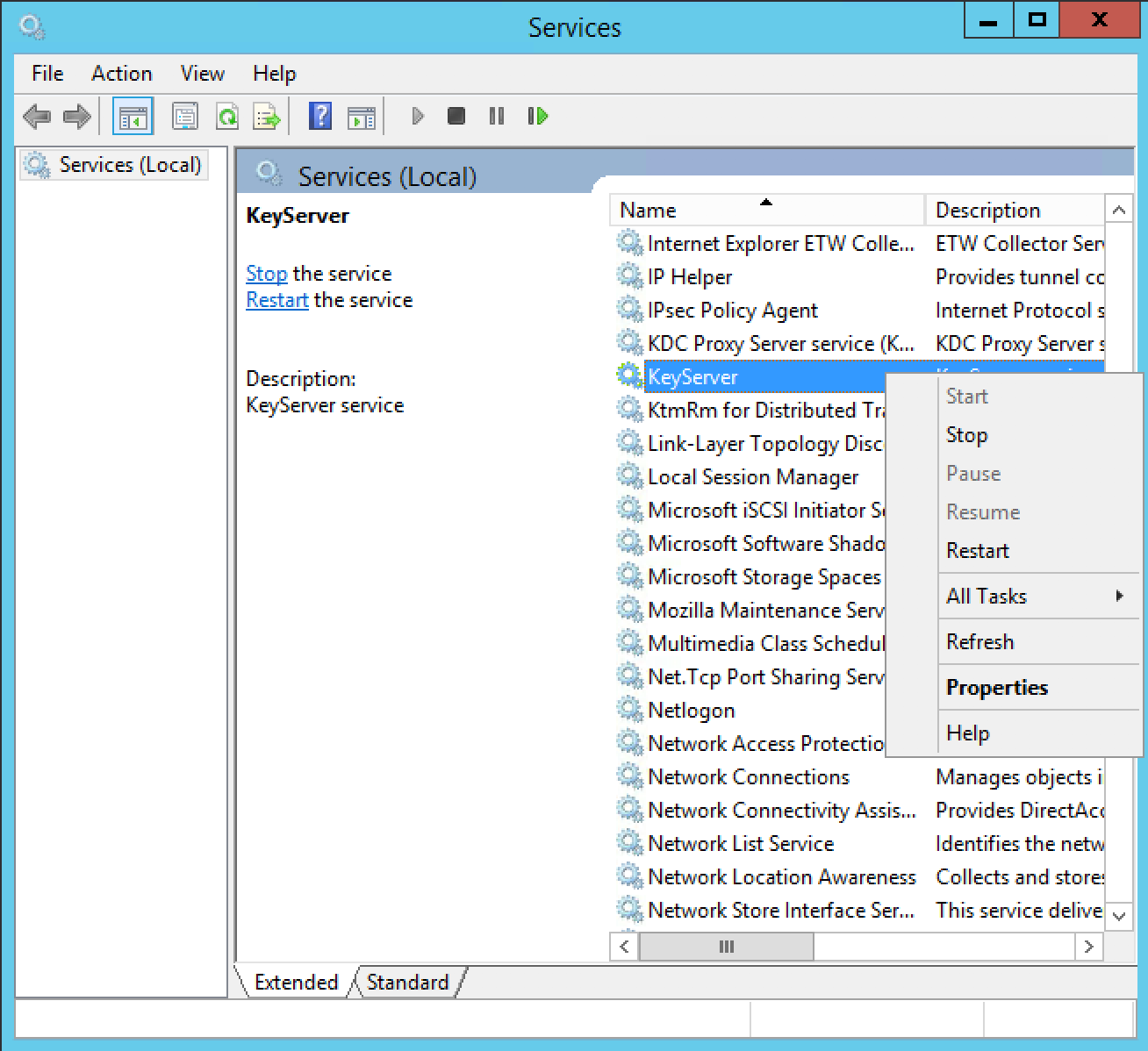
Note: <bridgeIPaddress> *must* be the IP address of the iLab Bridge. Use of its masked URL will cause the integration to fail.



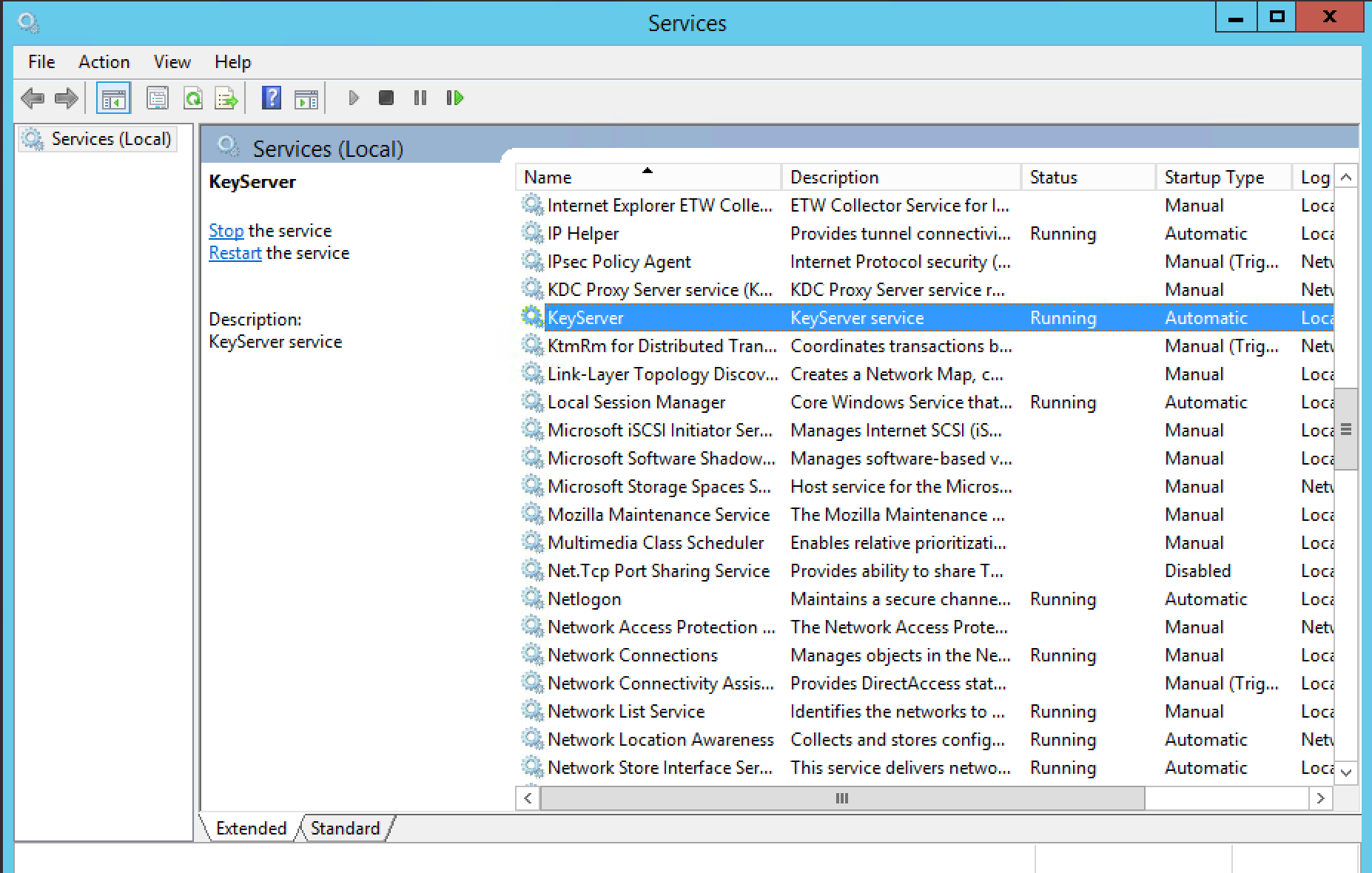
1. Check “Allow “Guest” login for members of” and select “all groups” within the dropdown box. Press the OK button to save these changes.
2. Restart the Sassafras Server from the Services utility in Windows (called KeyServer)
   1. For restarting the service, On the sassafras software interlock server, click on the start button and start typing services as seen below.



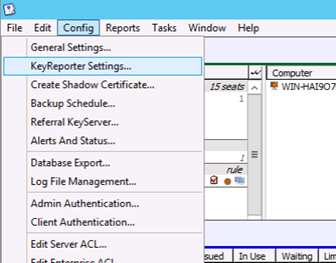
* 1. In the Services window, look for the service named “Key Server” and right click on the service.



* 1. Hit Restart and wait for the service to be in a Running state again.

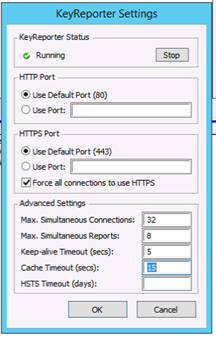


1. Go to Config-> KeyReporter Setting



1. In the popup window, check “Force all connections to use HTTPS” and make sure that the cache timeout is low (< 20 seconds). Then click on Run and OK.

If the KeyReporter Status fails (i.e. does not go into “Running” status), contact the Server Manager with the designated information to help in freeing HTTPS port 443.



## Installation of Sassafras Client:

The Sassafras client software interlock needs to be installed on the following set of computers:

1. Computers that are connected to and used to operate the schedulable equipment on iLab, provided they are connected to the internet/internal network of the university.
2. Computers that are used to operate any additional proprietary software used at the core facility, and for which an interlock is required or desired.

The Computer on which Sassafras Client is installed needs to have two User Accounts:

* + - 1. Administrator Account – This would be used by the core manager to perform maintenance and install/uninstall desired software.
      2. Standard User Account – The Account would be primarily used by users to use the equipment with restricted rights to install/ uninstall software.

Make sure you are logged in administrative rights on the machine, and based on the OS, install the appropriate client software with the default settings by following the instructions.

Note: A restart will be required for the client installation to be complete.

# Setting up a software interlock:

Once the KeyAccess Client is installed on the core facility’s computer, allow a few minutes for KeyServer to:

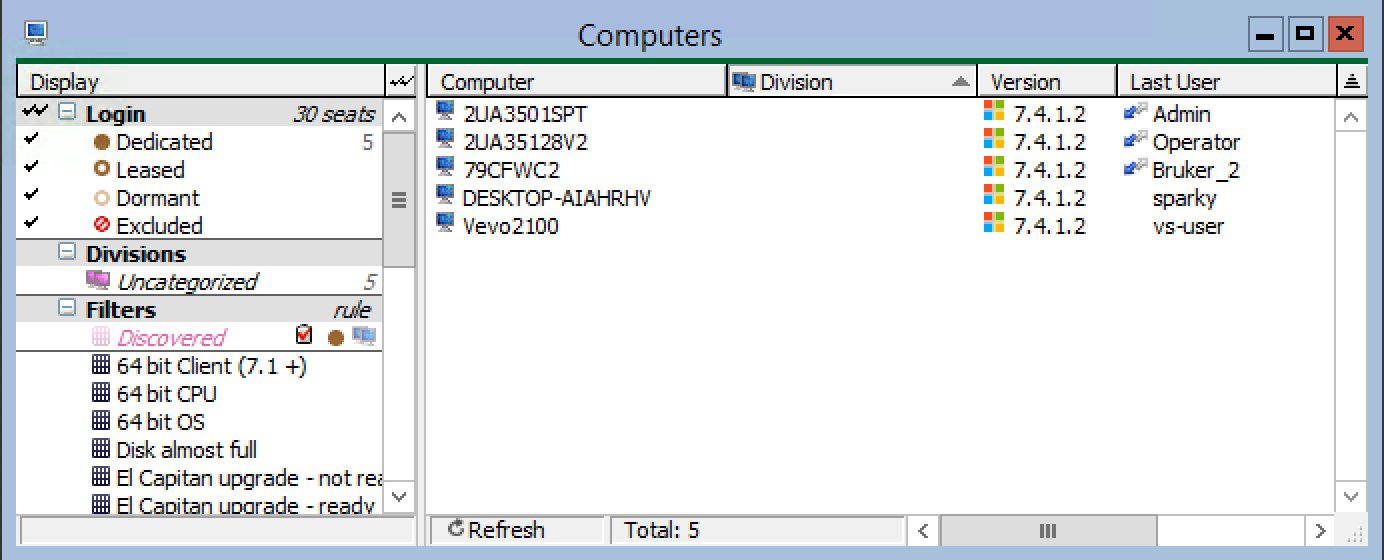
a) sync with the newly installed client, and

b) register the workstation and its installed software programs.

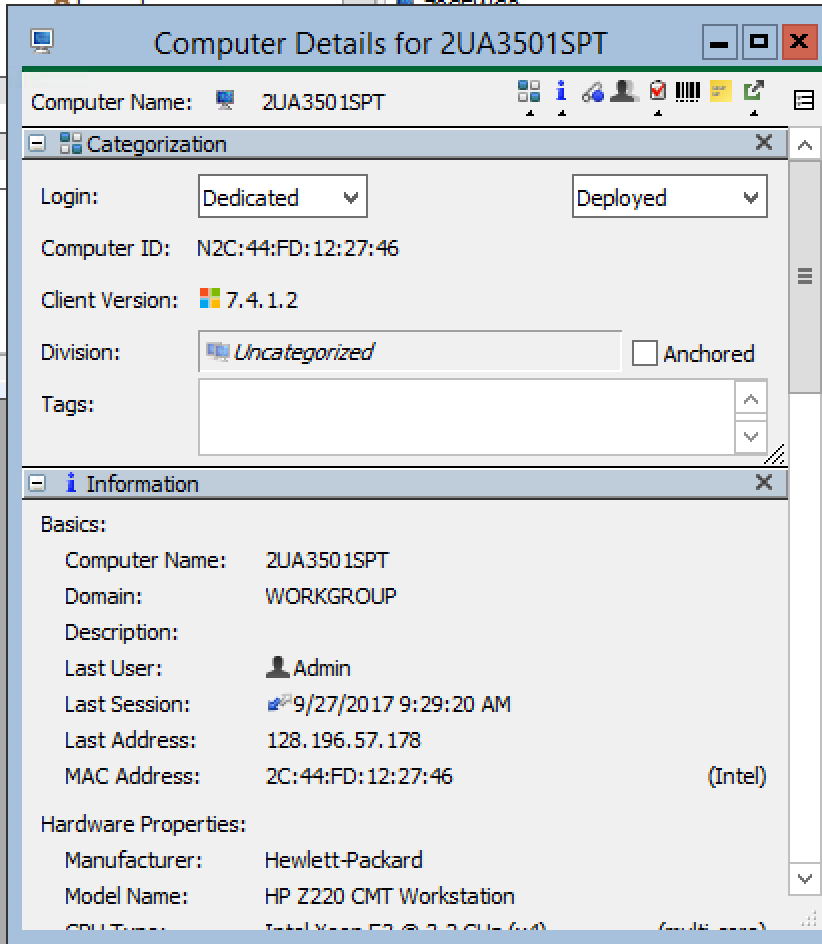
## Locate Computer ID in Sassafras

1. Within the KeyConfigure (Admin) interface, open the Computer’s window by going to the Window option in the top navigation menu and selecting Computers. A window named Computer will popup.
2. Next, locate the workstation that hosts the target software (i.e. Product) you wish to control via the interlock within the Computers list.

Note: the computer name of the interlocked machine can be used to identify the correct computer within the Computers window in Sassafras.

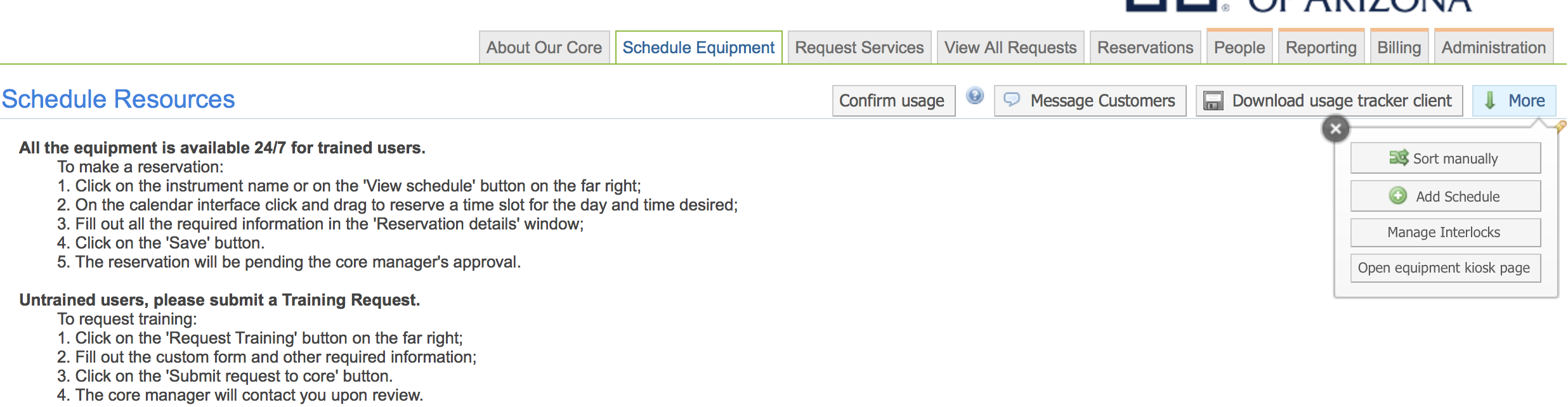


1. Right-click on the computer’s name and note its **Computer ID,** as assigned by Sassafras.



## Software Interlock Creation in iLab:

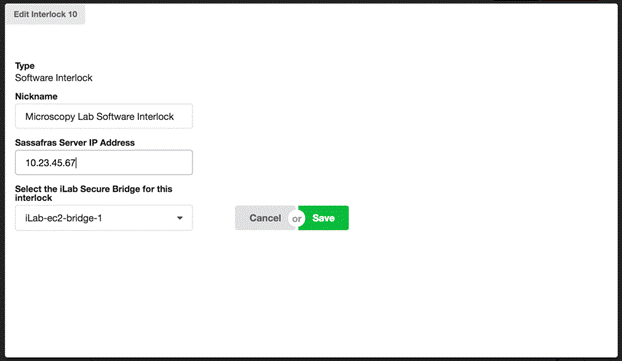
1. Login to iLab (<https://ua.ilab.agilent.com/account/login>). You will need to have Core Admin or Institutional Admin permissions to access the necessary settings.
2. Go to the core for which you are setting up the interlock, and choose the “Schedule Equipment” tab.
3. Click the ‘More’ drop-down, and then click on ‘Manage Interlocks.’



Note: It is important to create a new Software Interlock for each instrument to be managed via the interlock. This will prevent having one set of policies impact another within Sassafras.

### Create new software interlock for each piece of equipment to be managed:

1. Click on ‘Add New’ and select the Type of Interlock as ‘Software Interlock.’
2. Give the new interlock a Nickname
3. Enter the hostname of the Sassafras Server (sarsaparilla.arl.arizona.edu)
4. Choose the appropriate iLab bridge to associate to the software interlock and click ‘Save.’



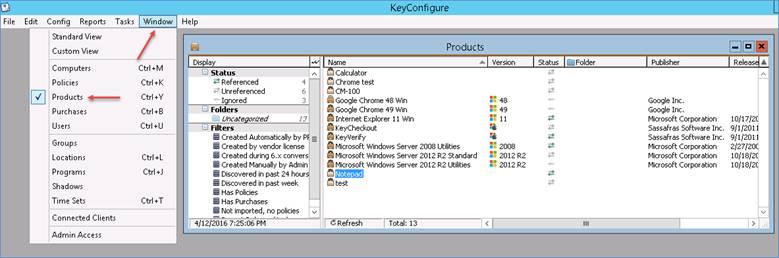
## Configuring Applications and Policies in Sassafras

### Create a Product

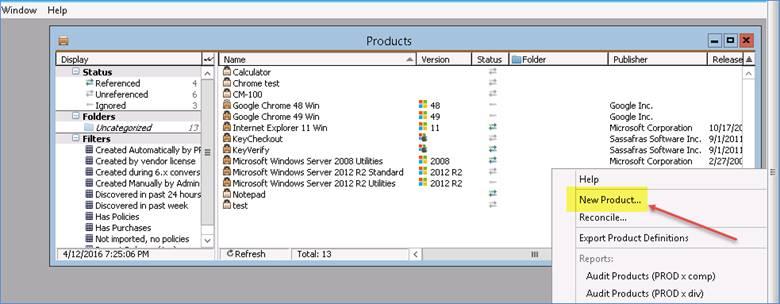
You will then need to create a new product in Sassafras. A product will need to be created in Sassafras for each iLab calendar using the software interlock.

Note: These directions represent the basic setup of a product in Sassafras for use in iLab’s software interlock feature. For any additional details, please refer to Sassafras documentation or contact their technical support team.

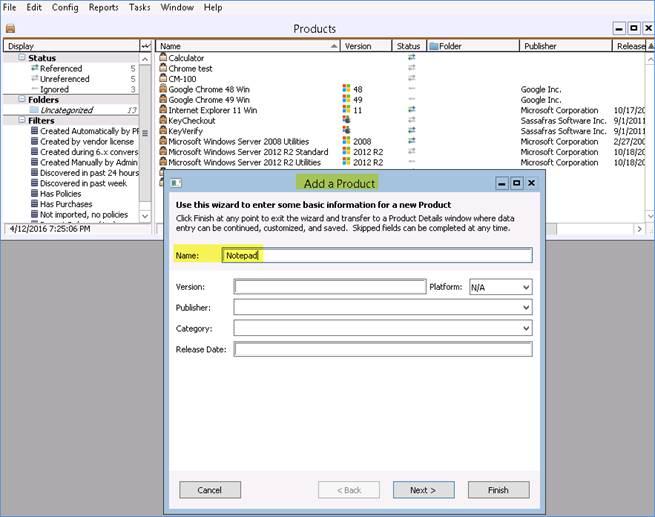
1. Access the Sassafras KeyConfigure (Admin) interface. Open the Products window by going to the Window option in the top navigation menu and selecting Products:



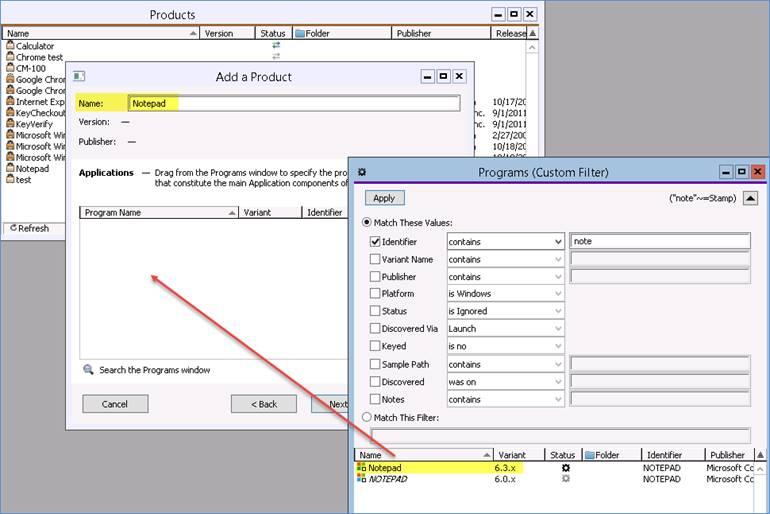
1. Right-click anywhere in the Product window and choose New Product…



1. Follow the steps in the basic product creation wizard:
   1. Give your Product a name and then click ‘Next.’



* 1. Now, associate the software program you'd like to control by adding it to this product, using the Search by Programs window magnifying glass:



* 1. Click ‘Next.’ You can generally skip the previous product step for this setup process. Click ‘Next’ again.
  2. Click ‘Finish.’

## Create Policies in Sassafras

Naming Convention for the policies:

[Facility]-[Hardware]-[Software]-[Allow/Deny]

Allow Policy example: HRUF-VEVO-VEVO-Allow

Deny policy example: HRUF-VEVO-VEVO-Deny

For example, please use FCSR-CANTO-DIVA-Allow as the name for the allow policy on the FACS-CantoII for the software DIVA in the Flow Cytometry Shared Resource.

Naming for facilities are:

Flow Cytometry (FCSR), High Resolution Ultrasound Facility (HRUF) and the Molecular Structures Core (MSC)

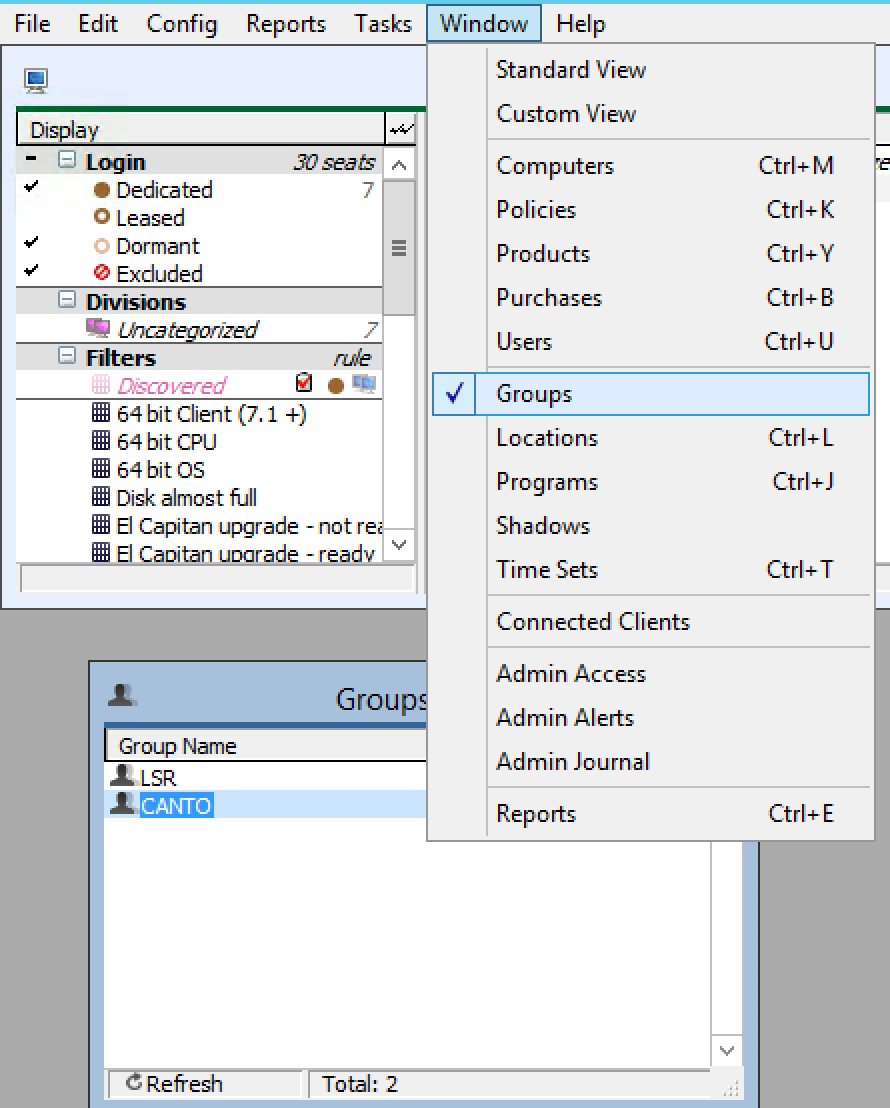
For every [Facility]-[Hardware]-[Software] combination that is to be controlled by the interlock, there must be two policies - a deny policy and a control policy. Please follow the naming convention for naming these policies to allow easy identification and troubleshooting.

### Create a Sassafras Group

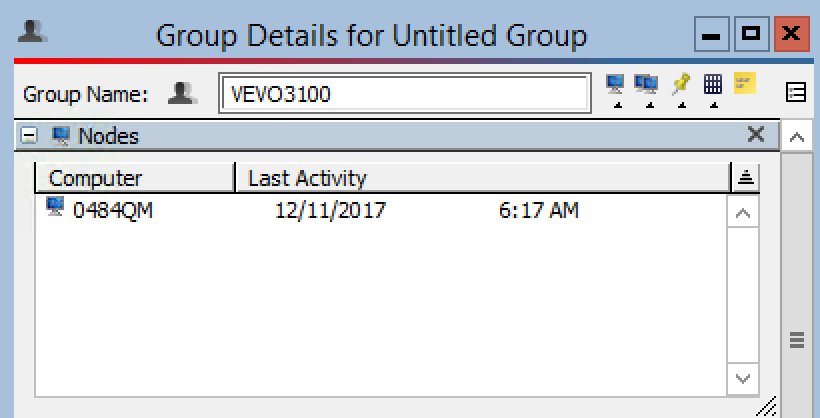
Groups in Sassafras are established to limit a deny policy to only one specific computer, or a specific group of computers. If a group is not established and applied to the scope of a deny policy (i.e. it is left as a Universal policy), every computer with the Sassafras Client installed will be prevented (i.e. denied) from running the target software (i.e. Product), unless there is an active iLab session to release the key, or the override has been engaged.

* + - 1. In the Sassafras Admin, open Window, then right-click Groups, and make a new group.

Note: Please use the naming convention [Facility]-[Hardware]-[Software]-[iLab Group] for naming Groups in Sassafras.



* + - 1. Then, from the Computers window, drag the computer that needs to be covered by the policy into the group.

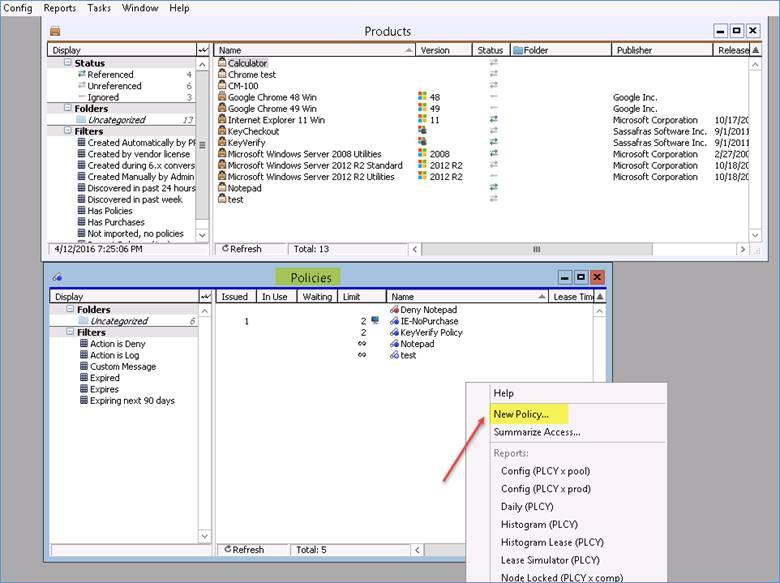


* + - 1. Save the group for use in defining the scope of the deny policy below.

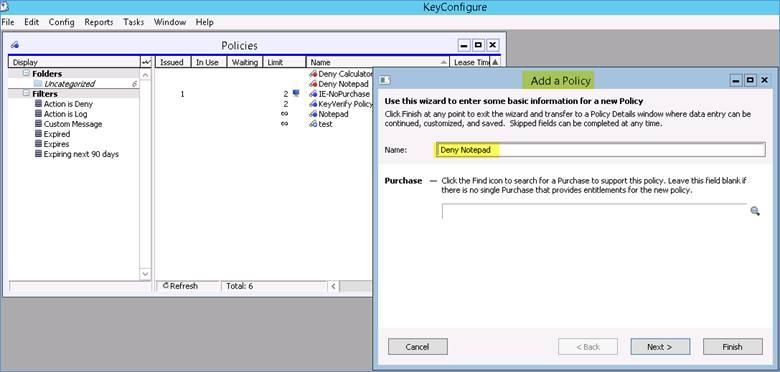
### Create the Deny Policy

The deny policy functions by denying access to the target software (i.e. Product) an active session in iLab.

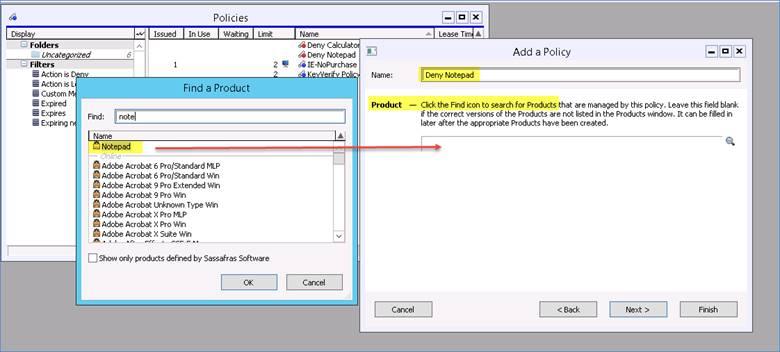
1. Open the Policies window (go to Window in top menu, choose Policies). Right-click anywhere in the Policies box and select New Policy...



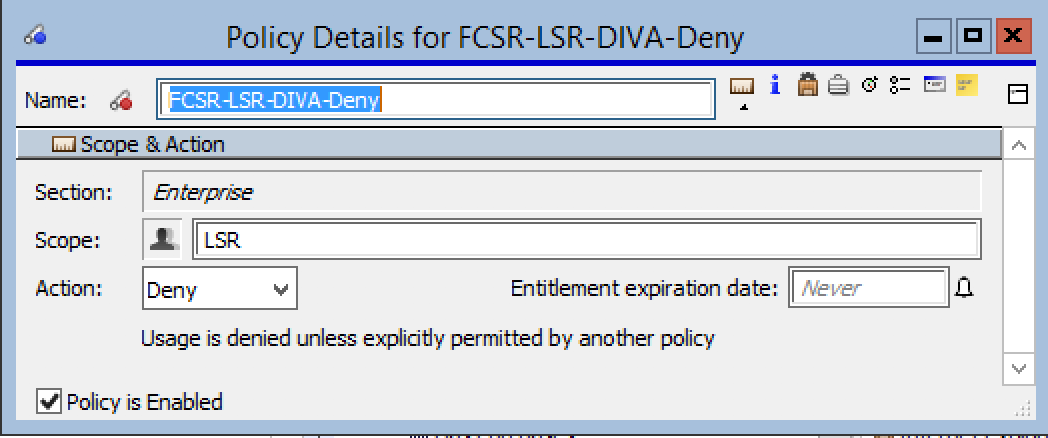
1. Give the deny policy a name by following the naming convention [Facility]-[Hardware]-[Software]-[Deny] (Go to Naming Convention for the policies for more).
2. Click Next.



1. Associate the Product you created previously by adding it to this policy using the ‘Search by Products’ magnifying glass:



1. Set the Action option to ‘Deny.’
2. Drag and drop the appropriate Sassafras Group into the ‘Scope’ field.



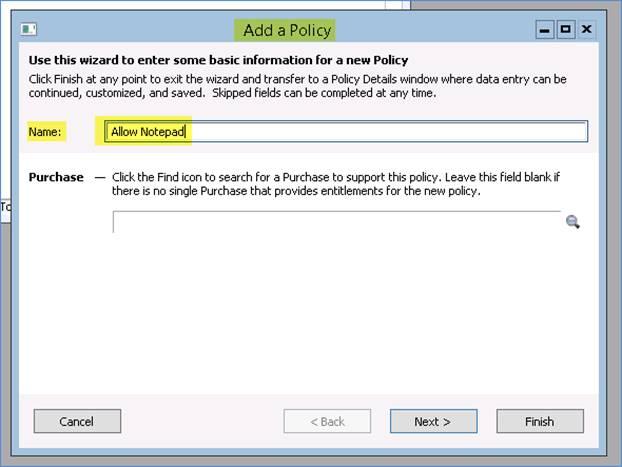
1. Click ‘Next.’
2. Click ‘Finish.’

You can confirm your final deny policy configuration by opening the policies window, locating your deny [Facility]-[Hardware]-[Software] policy and double-clicking on it.

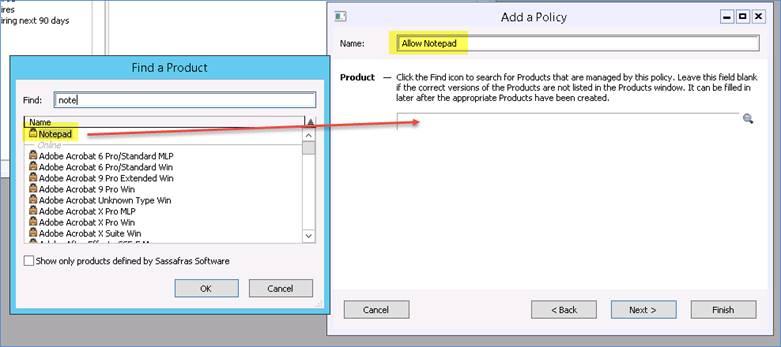
### Create the Allow Policy

The allow policy functions by allowing access to the target software (i.e. Product) when there is an active session in iLab.

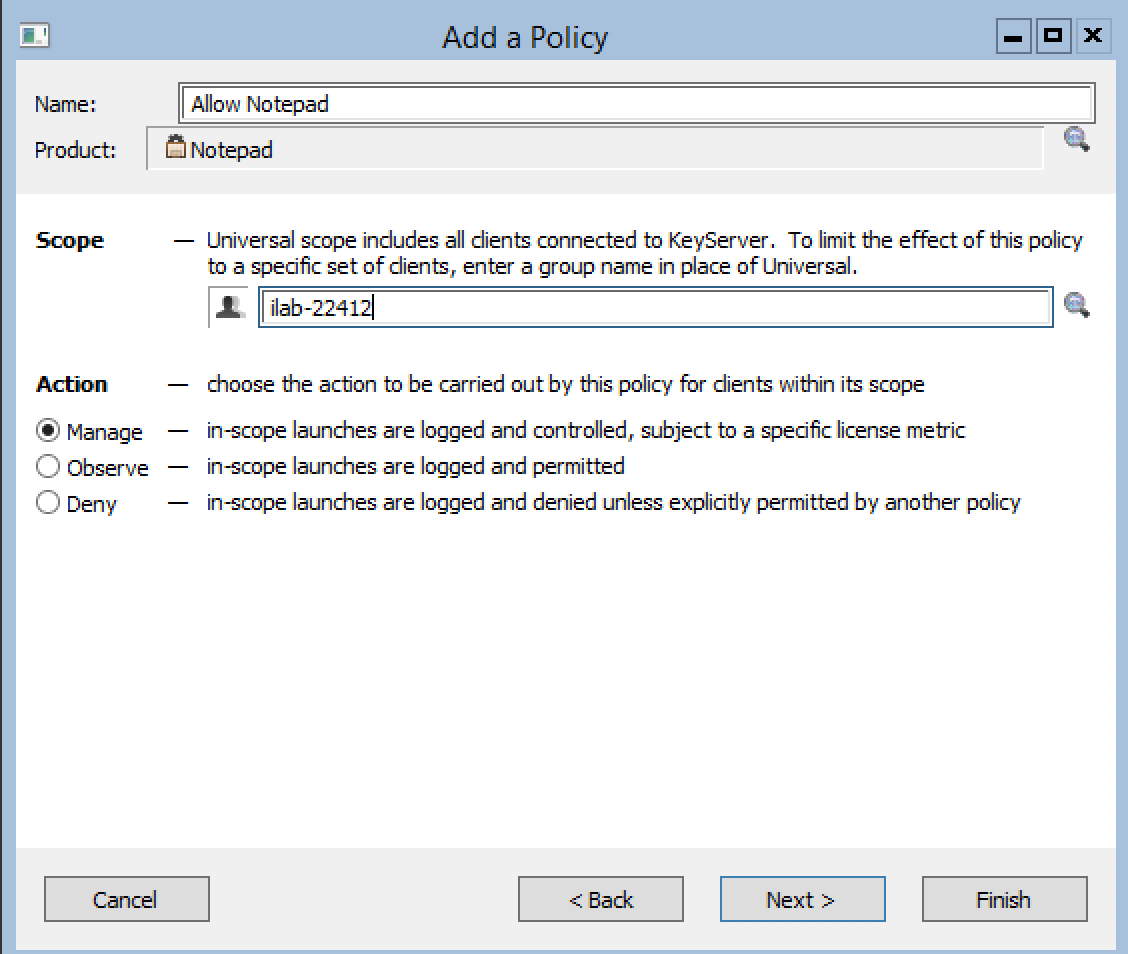
1. Create another new policy by following the naming convention [Facility]-[Hardware]- [Software]-[Allow]. For more details go to [Naming Convention for the policies.](#NamingConvention)



1. Search for and add the product to this policy. Click Next.

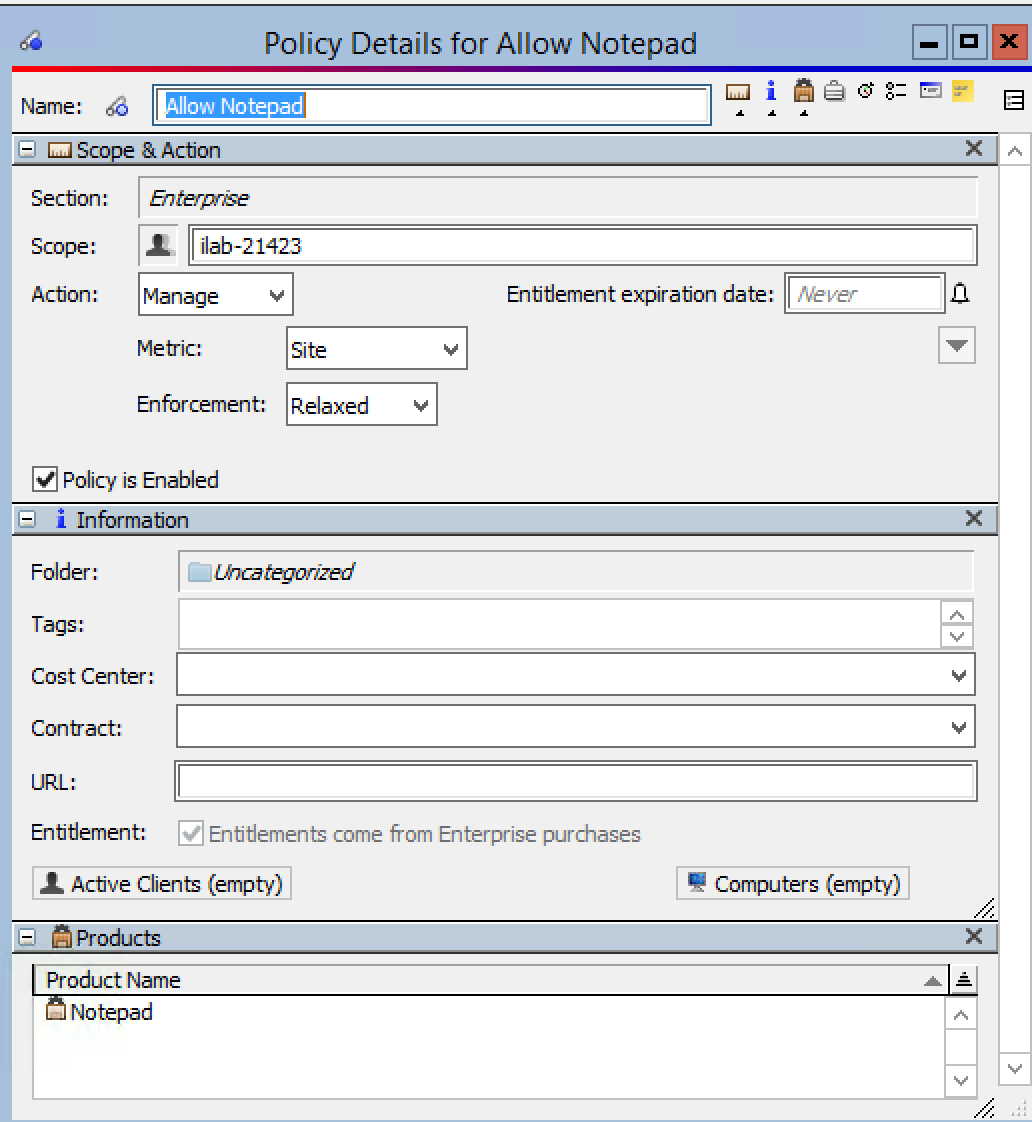


1. Enter the Group ID name from iLab (located in the Software Interlock calendar setting) into the ‘Scope’ field. Do not confuse this with the [Sassafras Group](#_Create_a_Sassafras). Set the Action option to ‘Manage.’



1. Click Finish.

Confirm your allow policy configuration by opening the policies window, locating your [Facility]-[Hardware]-[Software]-Allow policy and double-clicking on it.



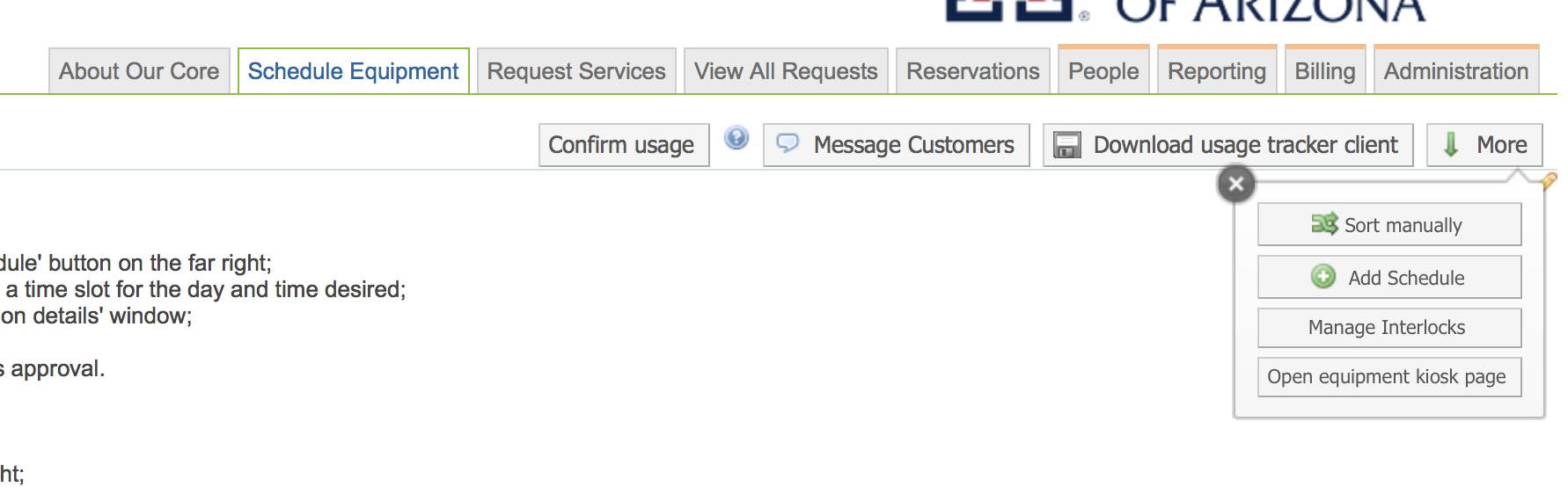
This completes the process of setting up a software interlock.

# Disabling the Software Interlock

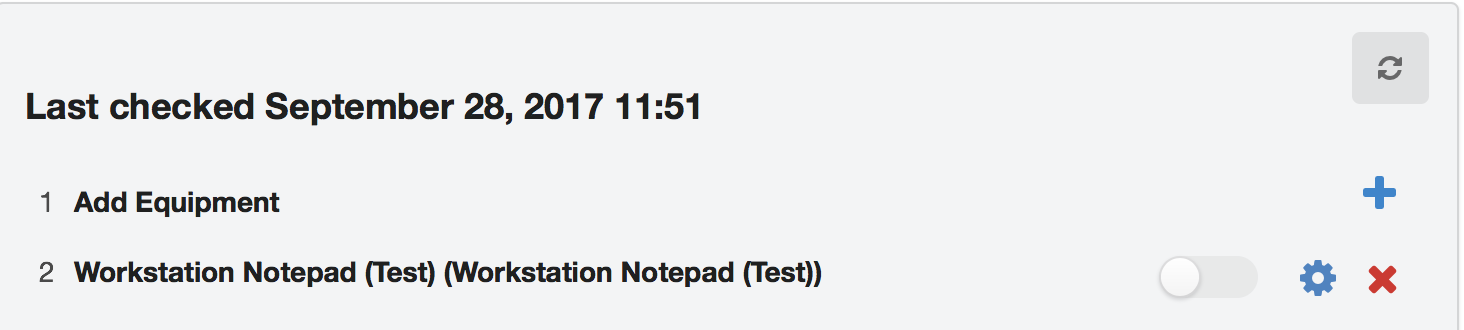
## Disabling the Software Interlock within iLab

It is important to note that activating the interlock override within iLab via this process only disables the interlock for one instance/session. After that the override will automatically turn off, re-engaging the software interlock.

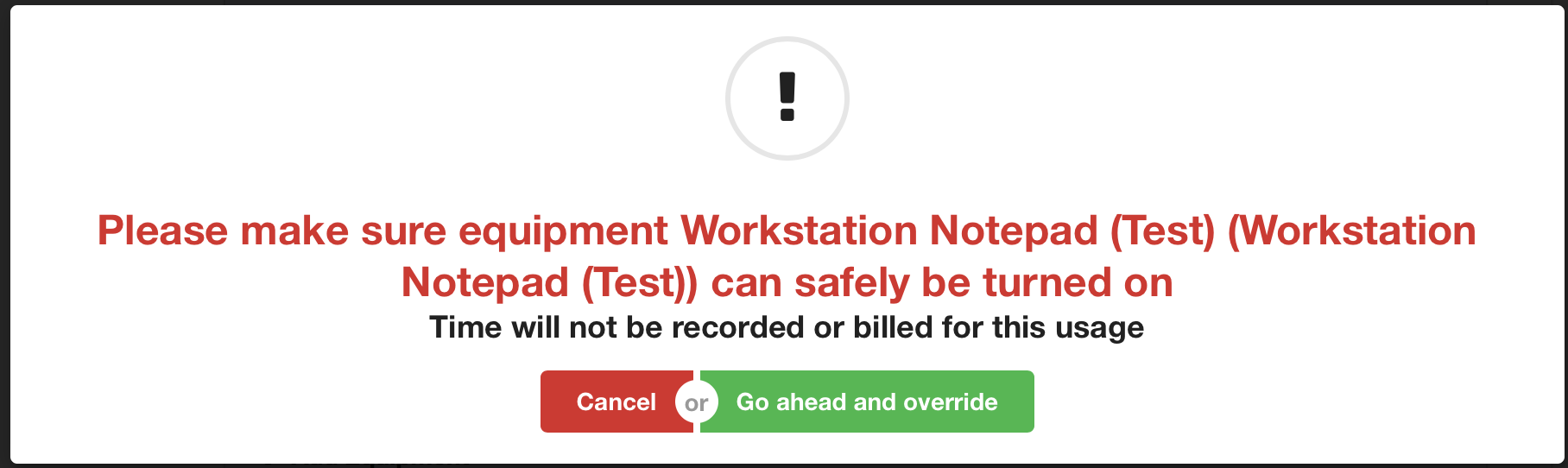
* + - 1. Log in to iLab using an administrative account.
      2. Go to the facility-> Schedule Equipment-> Click on ‘Manage Interlocks’



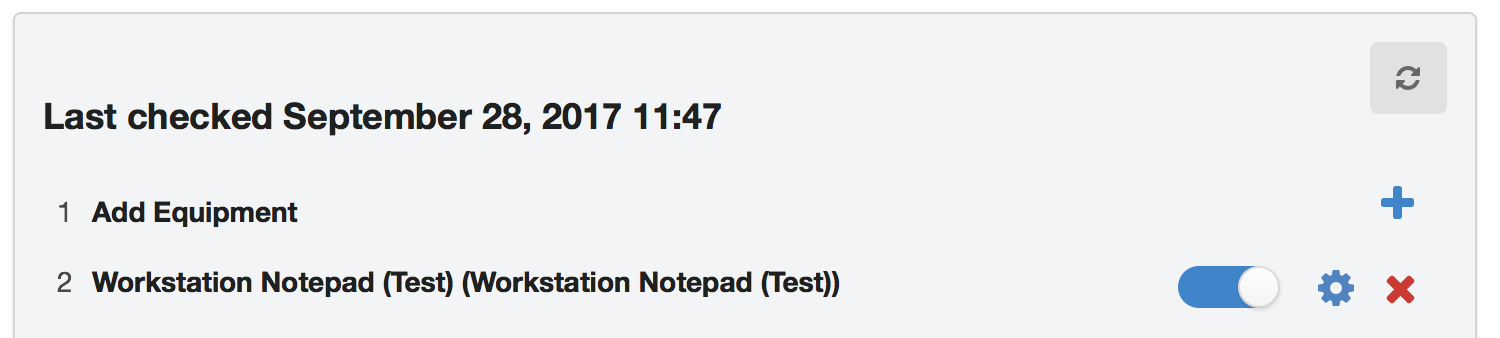
* + - 1. In the below screen turn the required equipment’s software interlock toggle to the right.



* + - 1. The follow message will be displayed. Click on “Go ahead and override.”



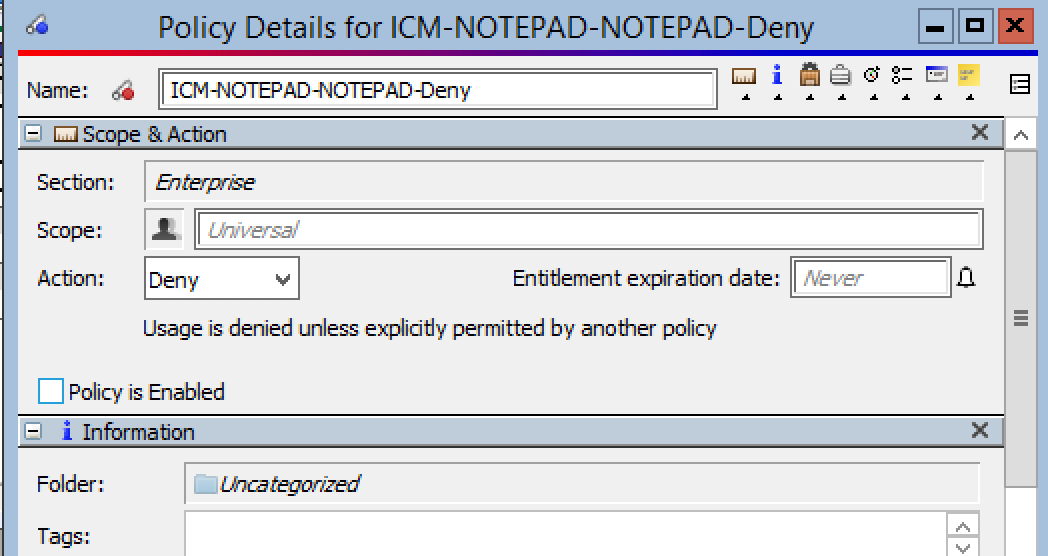
* + - 1. The following screen confirms that the software interlock for that equipment is disabled (the toggle has turned blue).



## Disabling the software interlock within Sassafras

To disable a software interlock within Sassafras you should double click on the Deny policy associated with the [Facility]-[Hardware]-[Software]-Deny combination you want to turn off.

In the policy detail window that pops up uncheck the “Policy is enabled” check box and save the policy. This would disable the policy.



## Disabling the software interlock in case of Network Outage

In case of network outage, login to the equipment computer as an Administrator via the login provided to the core manager.

1. Press Ctrl + Alt + Delete for a windows computer to start the task manager and open the services tab.
2. Search for the “KeyAccess” service which would be currently running on the computer and disable it by right clicking on the service and clicking disable.

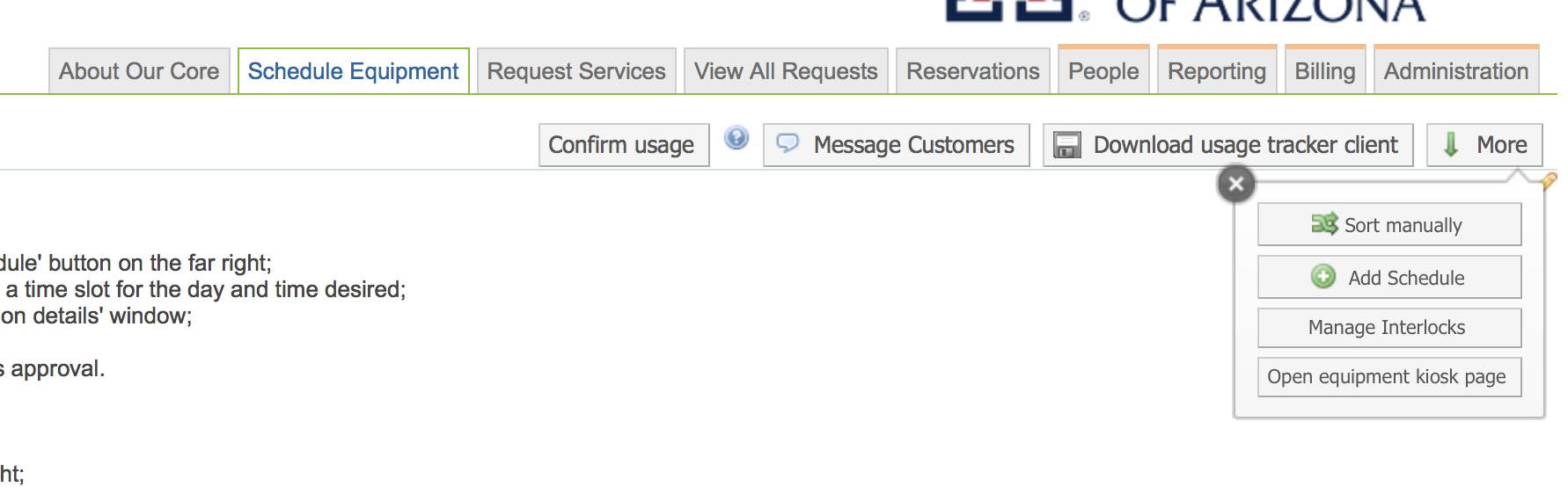
This would disable the interlock till the next restart of the computer.

# Enabling a disabled software interlock policy

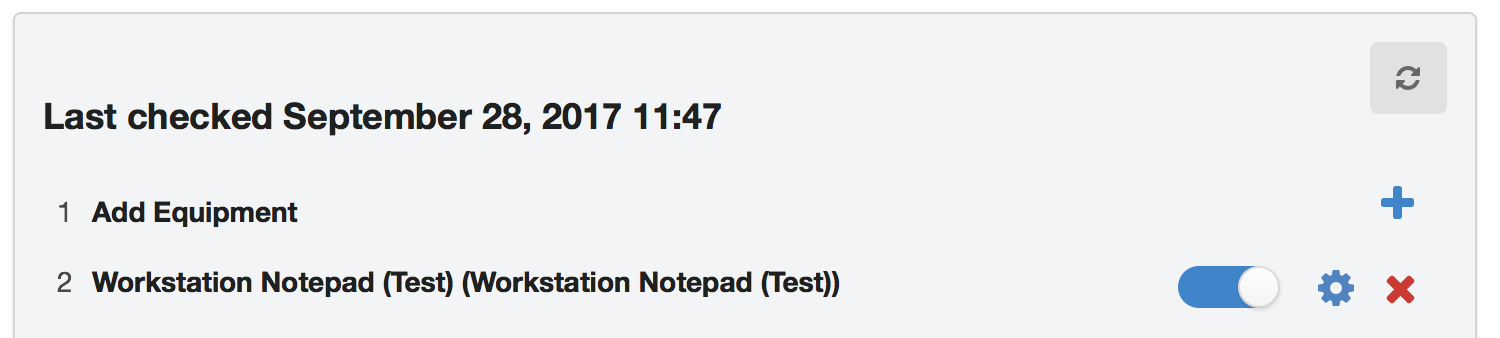
## Enabling a disabled software Interlock policy within iLab

There are two ways that an interlock policy will be enabled in iLab after having been disabled via the override switch in iLab:

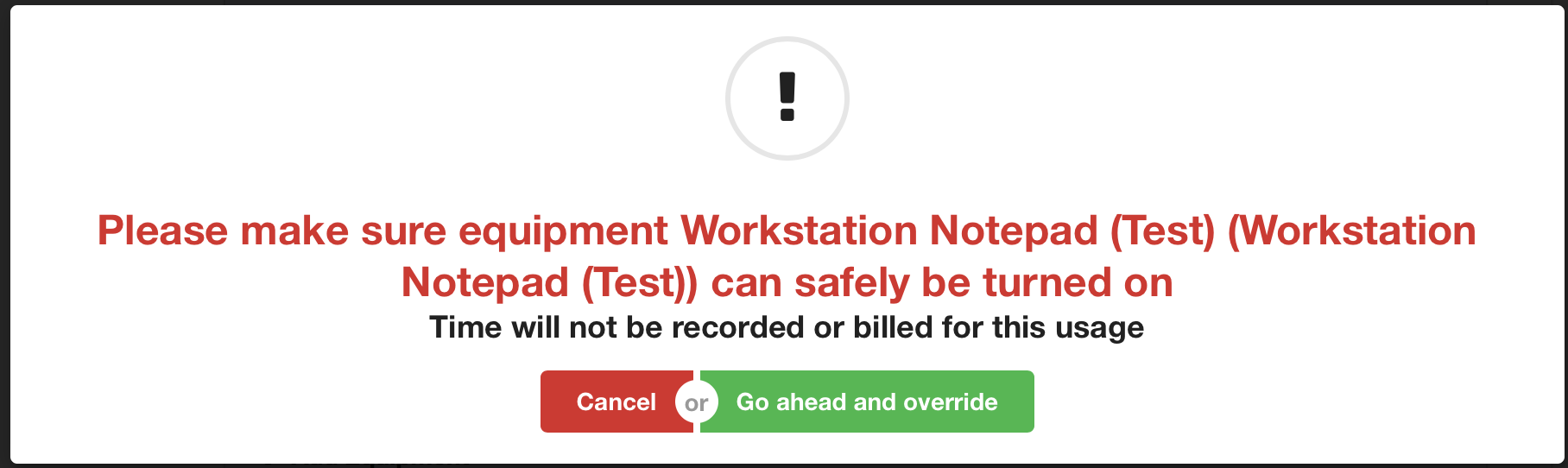
1. The override switch will automatically turn itself off after a session for the instrument targeted by the interlock has been initiated and ended *within iLab*.
2. An interlock override can be manually reversed via the following process:
3. Log in to iLab using an administrative account.
4. Go to the facility-> Schedule Equipment-> Click on Manage Interlock as seen in the SS below



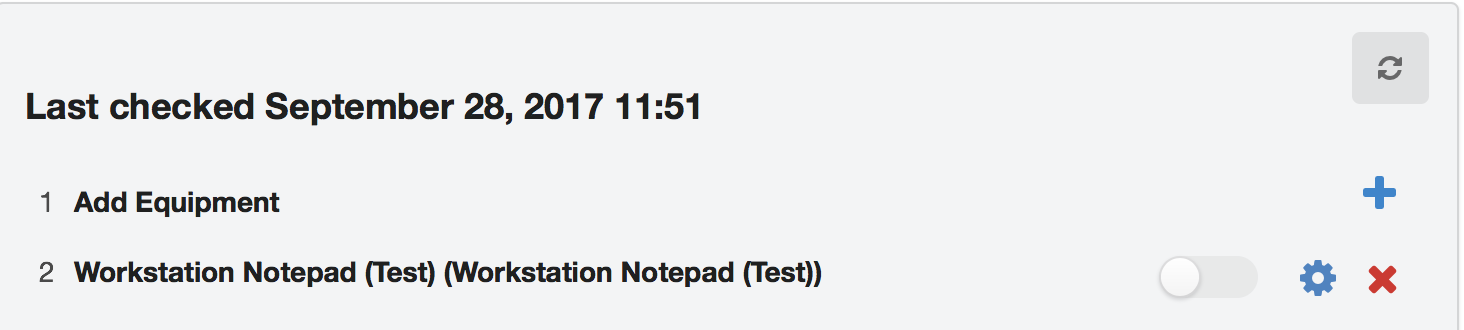
1. In the below screen turn the required equipment’s software interlock toggle to the left.



1. The follow message will be displayed. Click on “Go ahead and override.”



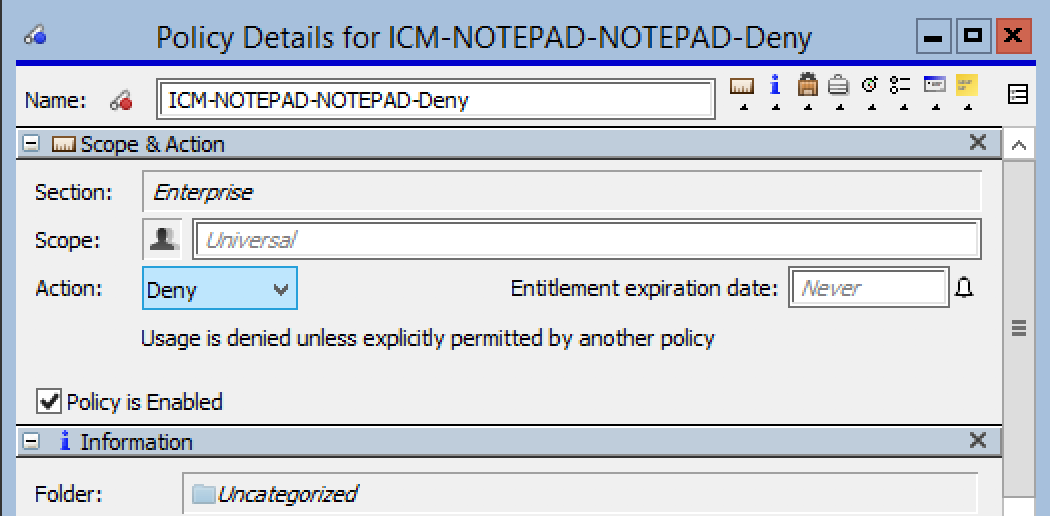
1. The following screen confirms that the software interlock for that equipment is enabled (the toggle has turned gray).



## Enabling a disabled software interlock within Sassafras

To enable a software interlock within Sassafras you should double click on the Deny policy associated with the [Facility]-[Hardware]-[Software]-Deny combination you want to turn on.

In the policy detail window that pops up check the “Policy is enabled” check box and save the policy. This would enable the disabled policy.



## Enable the software interlock after a Network Outage

In order to restore the software interlock after network outage, login to the equipment computer as an Administrator via the login provided to the core manager.

1. Press Ctrl + Alt + Delete for a windows computer to start the task manager and open the services tab.
2. Search for the “KeyAccess” service which would be currently disabled on the computer and enable it by right clicking on the service and clicking enable.

This would reinstate the software interlock as before the network outage.

# iLab Settings and Software Interlock Behavior

Terminology:

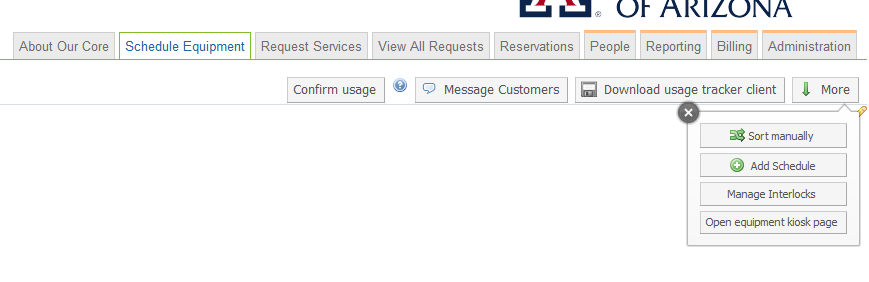
1. Session- The session time in iLab corresponds to the time from when the scheduled calendar time is initiated by clicking the “Start” button using the iLab kiosk till the “Finish” button is clicked or a walk-out is deemed.

2. States of Hardware:

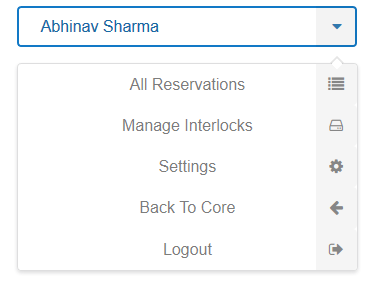
1. Green tick: The Hardware is running and currently not running any session.
2. Orange tick: The Hardware is running and currently running a session
3. Blue tick: The Hardware is running and which booked but the user did not show up.
4. Red tick: The Hardware is under maintenance and is not available for operation

## Access the iLab Setting for Core:

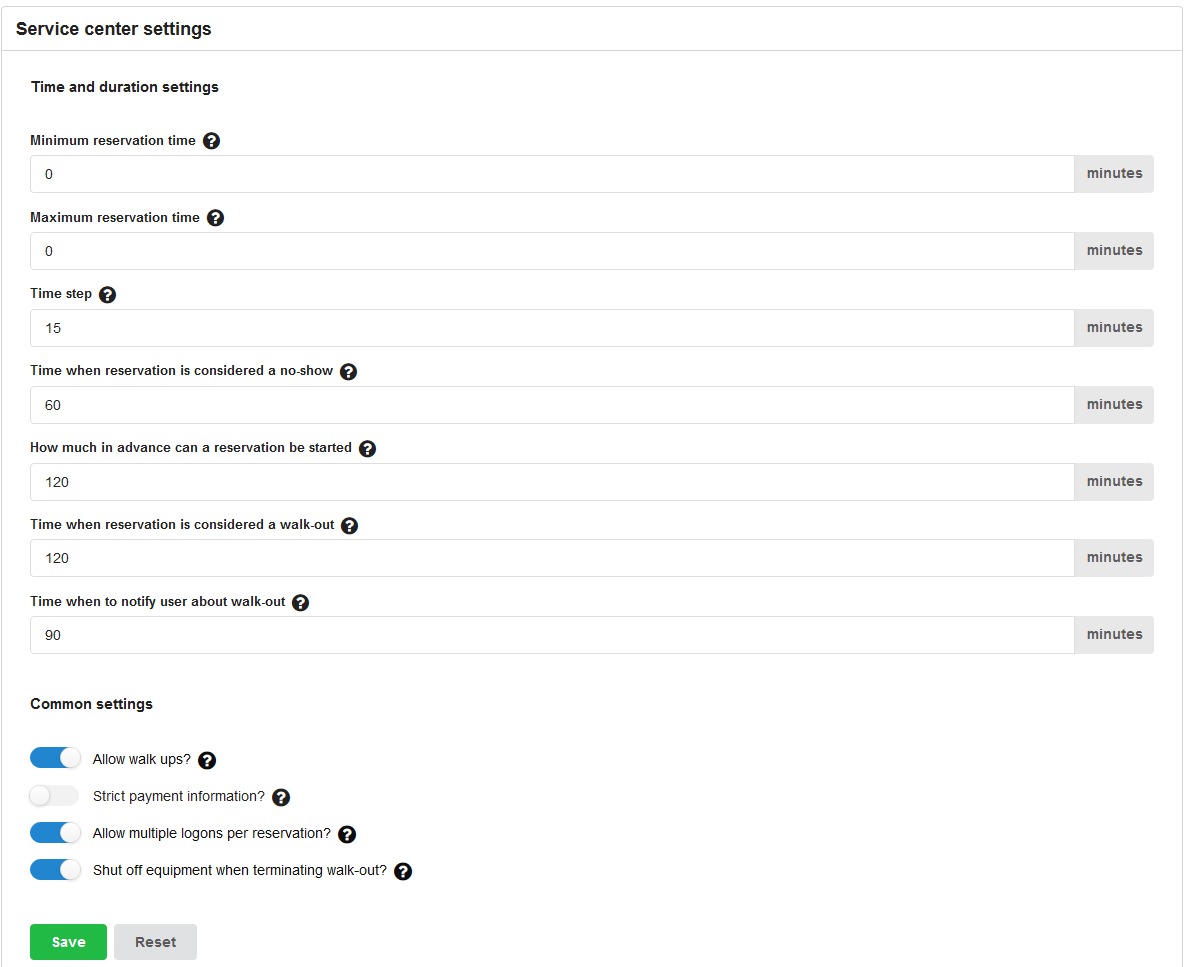
1. Log in as an Admin in the iLab's website.
2. Go to the ‘Schedule Equipment’ tab, and in the ‘More’ drop-down click ‘Open Equipment Kiosk page.’



1. On the Top-Right, click on your name and go to ‘Settings.’



1. The page will display the following screen and all the settings changes made would be the default setting for all the equipment's at the core. The benefit of setting the default setting is that you will simply have to check the "Use core default" when setting up the equipment.



## Settings for the core (Time and duration settings):

Minimum reservation time:

The minimum allowed duration for a reservation.

Maximum reservation time:

The maximum allowed duration for a reservation.

Time Steps:

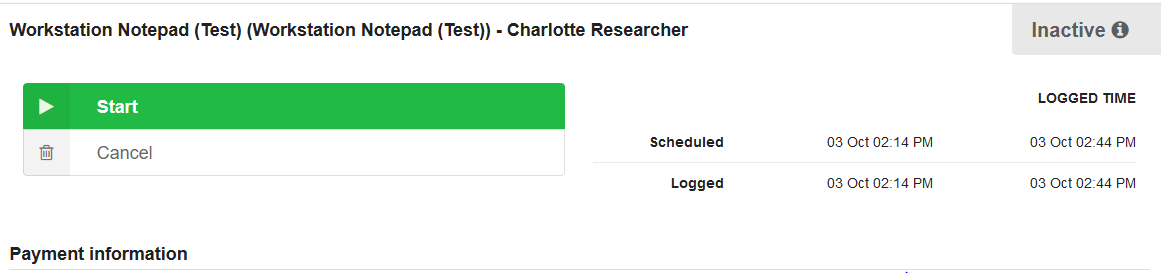
The base increment of time that a reservation can be increased or decreased by (Minimum to be set at 15 mins).

### Time when reservation is considered a no-show:

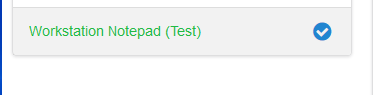
The duration after a session’s start time when the reservation is automatically cancelled and equipment is made available to other users via schedule or walk-up.

Example: Time when reservation is considered a no-show set to 15mins.

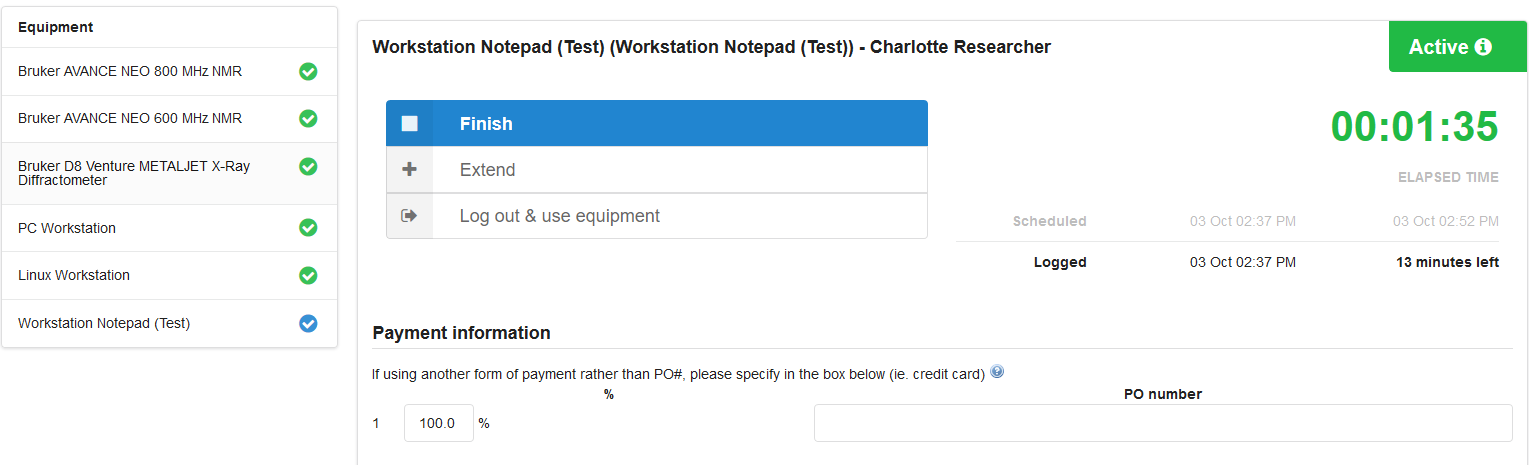
Reservation made for 30 mins.



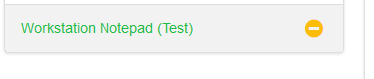
Reservation was not started via the kiosk. After 15 mins the equipment is open to other users, and shows the Blue-Tick.



Even after starting of new session after a no-show, the blue-tick remains



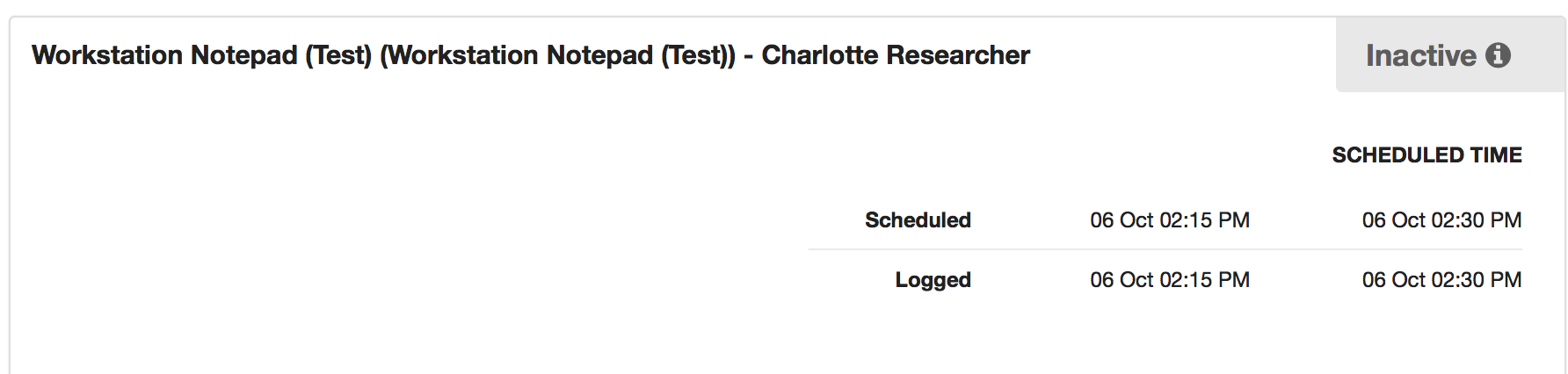
However, it remains blue only till the previous reservation was valid and then turns yellow.



### How much in advance can a reservation be started:

How long after the end of the scheduled session is a user considered to have left without ending their session in iLab. An email is sent to the user once a session is deemed a walk-out.

If a researcher accesses his/her appointment in advance, the reservation would not display the start button before the time mentioned in the field.



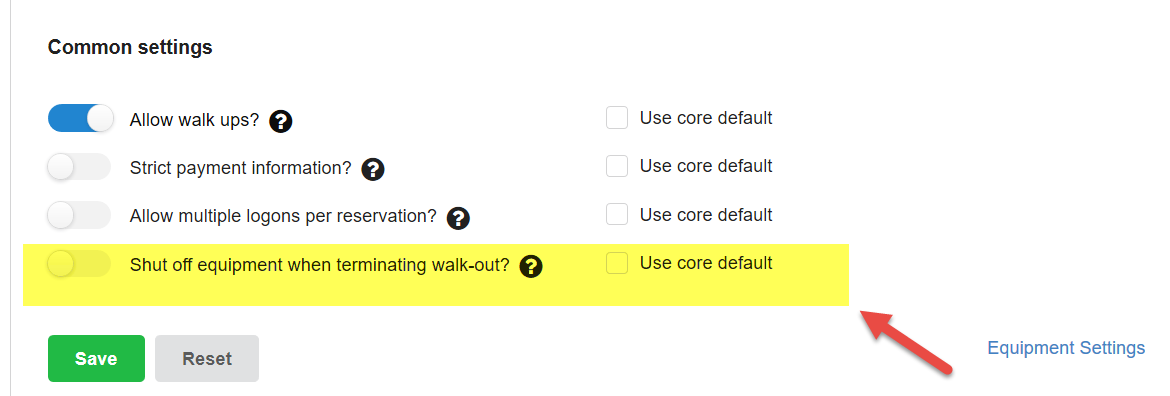
### Time when reservation is considered a walk-out:

How long after the end of the reservation is a user considered to have walked away. An email is sent to the user once the walk-out has happened.

### Time when to notify user about walk-out

An Email is sent to the user at the given number of minutes before the reservation is determined as a walk out (see prior setting).

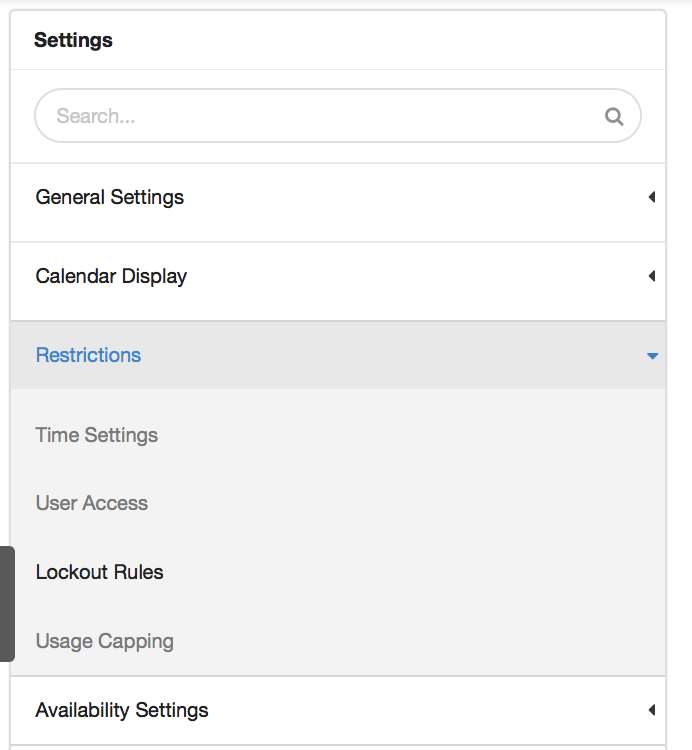
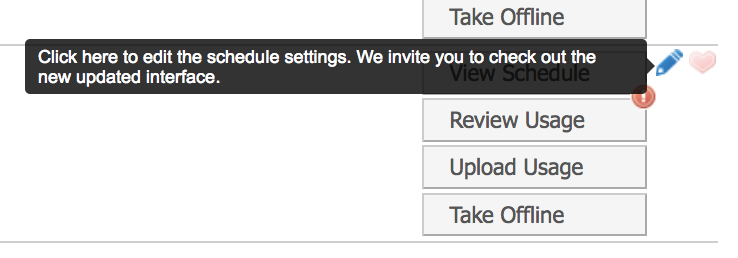
## Settings for the core (Common Settings):



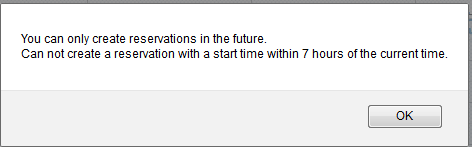
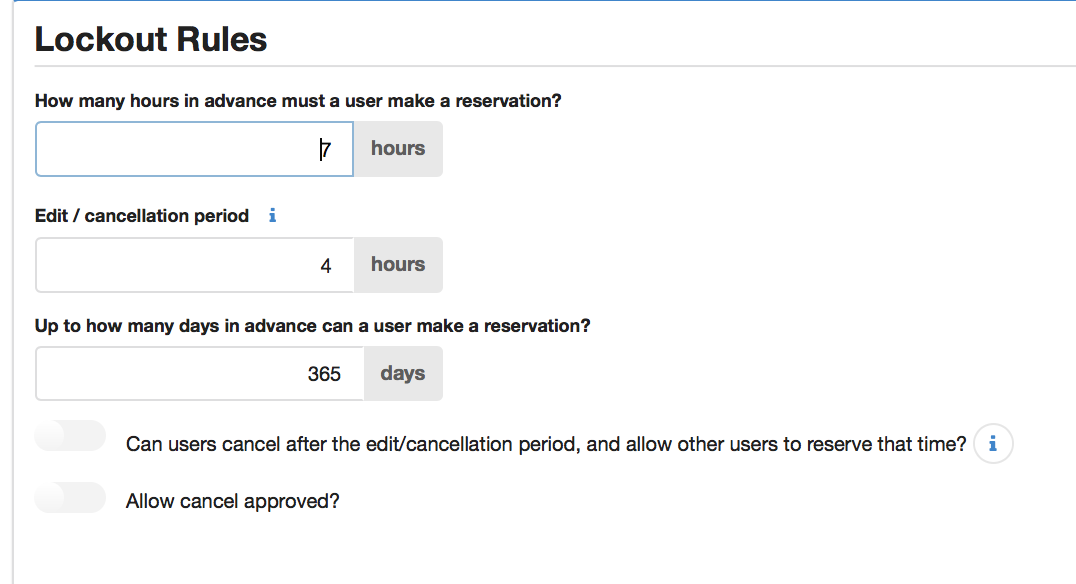
### Allow walk ups:

Setting this switch on (Blue) allows reservations to be made from the Kiosk

If turned off, user cannot create a session based on the policy set in the Schedule Equipment -> Equipment Schedule Setting -> Reservation-> Lookout Setting. A reservation can only be created by the administrator using his account credentials.



1. Schedule Equipment -> b) Restrictions -> Lockout Rules  
   Equipment Schedule Setting



1. Change “How many hours in advance d) Message while creating reservation if changes  
    must a user make a reservation” to 0. not made.

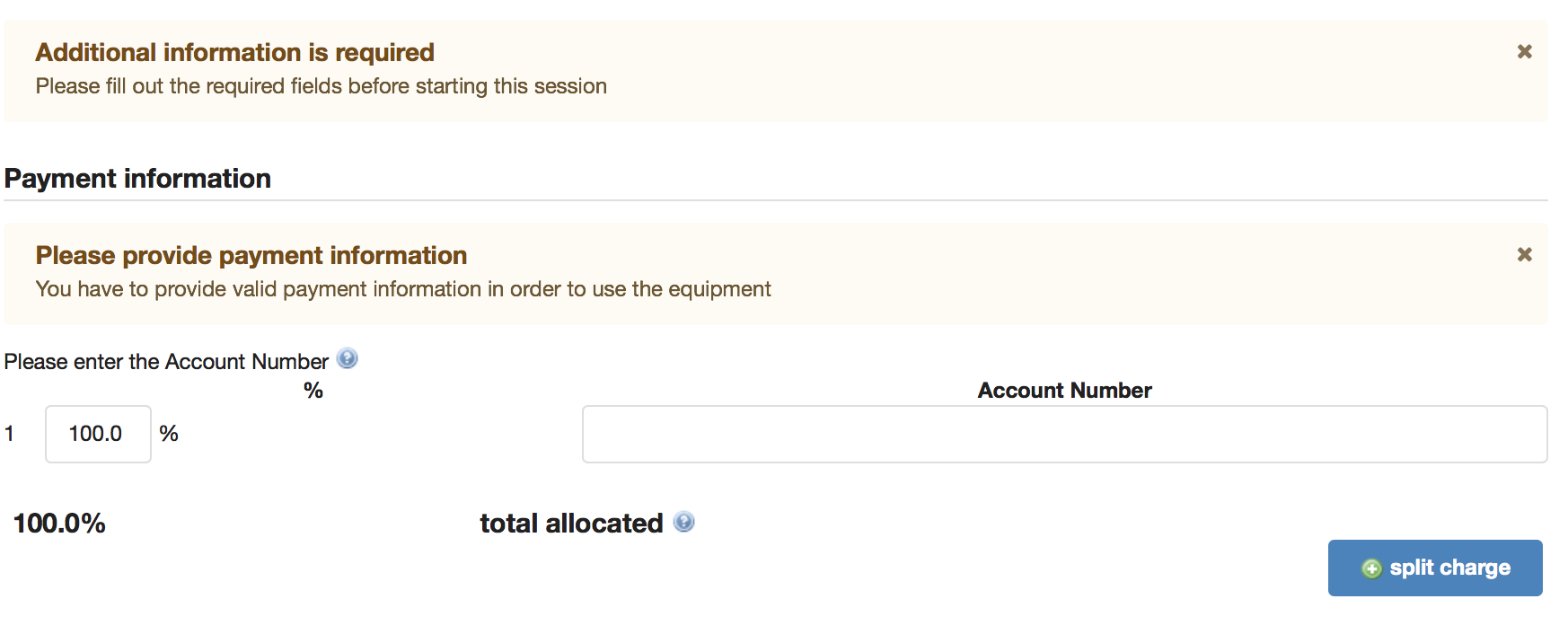
### Strict payment information:

Set to active by turning the knob Blue.

#### Logged on as a Core or Institutional administrator

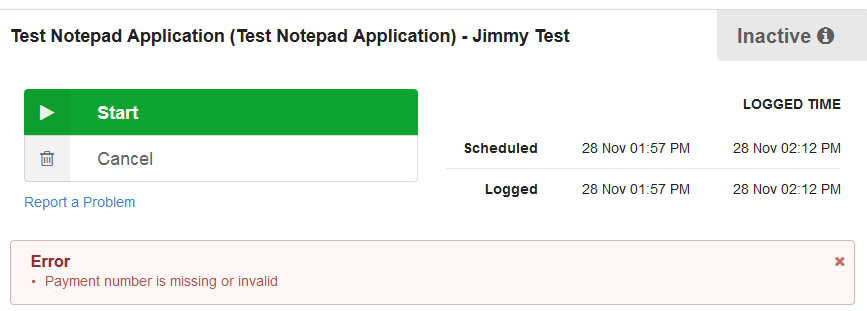
If set to Yes, warning messages would be introduced into the kiosk for the user to complete payment information.

Note: Not entering the details would not stop the user from starting and finishing the session.



#### Logged on as a PI or Customer

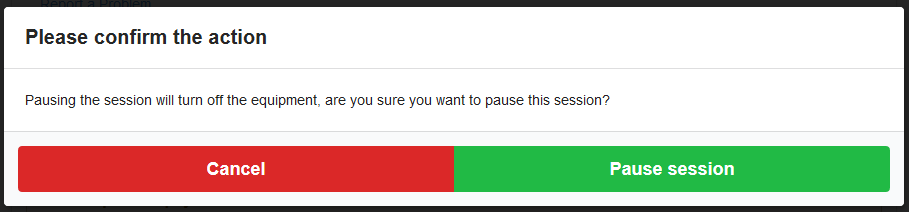
If set to Yes (Blue), the User needs to put the required payment method if none has been specified on his user profile. The session will not start until the required information is added to the scheduled reservation.



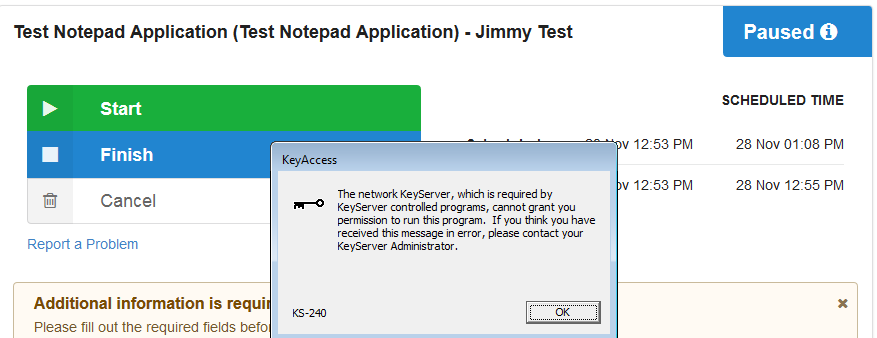
### Allow multiple logons per reservation:

Setting this switch on (blue) allows users to pause the session.

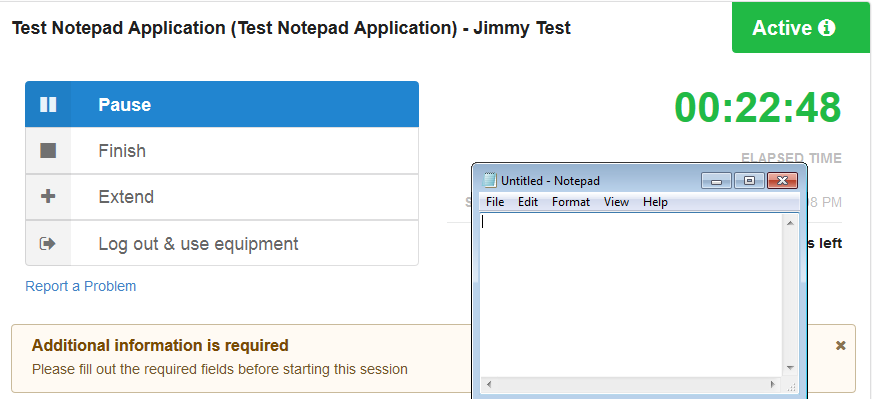
* + - 1. If User has closed the application:
         1. A confirmation screen appears, where user needs to confirm his choice as seen in the snapshot below.



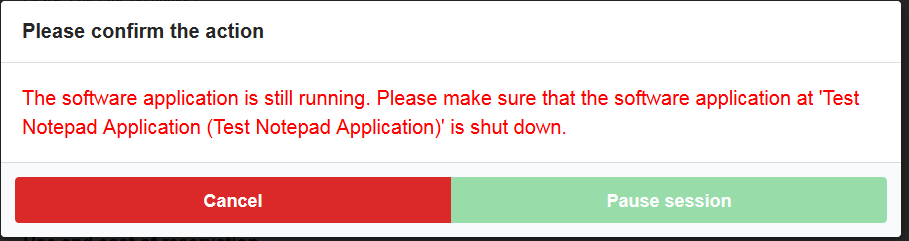
* 1. Once the session is paused, User cannot open the software without Starting the session again.



* 1. The user would be able to work smoothly after starting his session again.



1. If the User has not closed the application:
   1. The user would not be able to pause the session and would be displayed the following screen with the disabled “Pause Session”.



### Shut off equipment when terminating walk outs

Needs to be turned on (Blue) for sassafras to reactivate the deny policy once the software is closed. If turned off, the facility manager needs to manually reset the session by doing the following each time a walk out occurs:

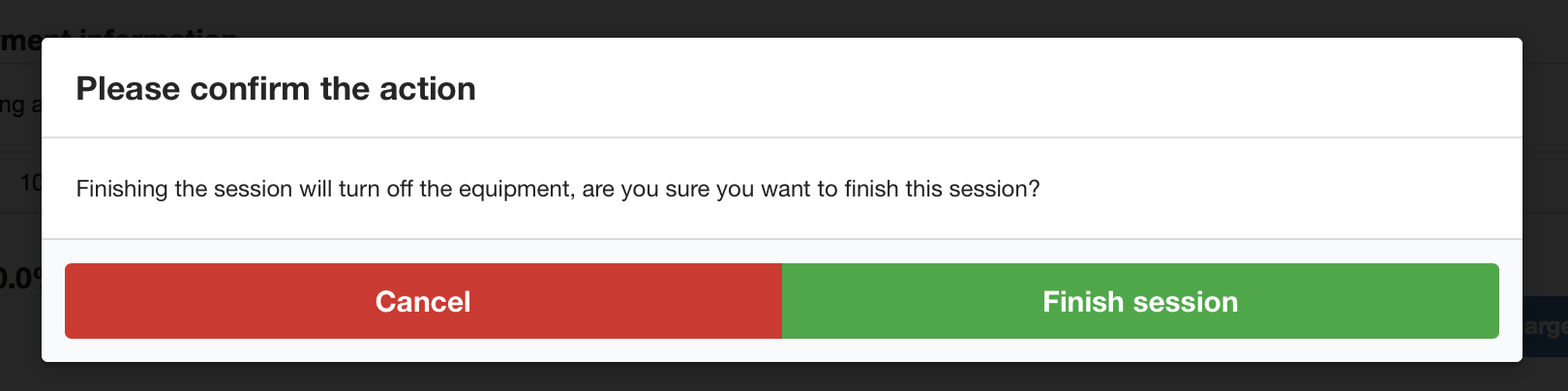
1. Disabling the Software Interlock within iLab followed by enabling a disabled software Interlock policy within iLab

Note: The software is not turned off/closed, it would simply not reopen once closed.

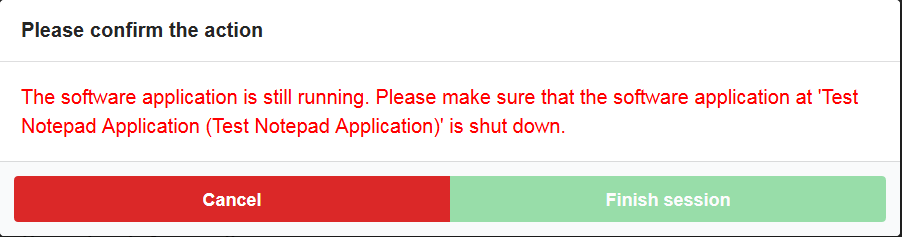
## Ending an Active Session in iLab

### As a PI or Customer

* + - 1. **When the User has closed the designated application** before finishing the session the following screen allows him to finish his session.

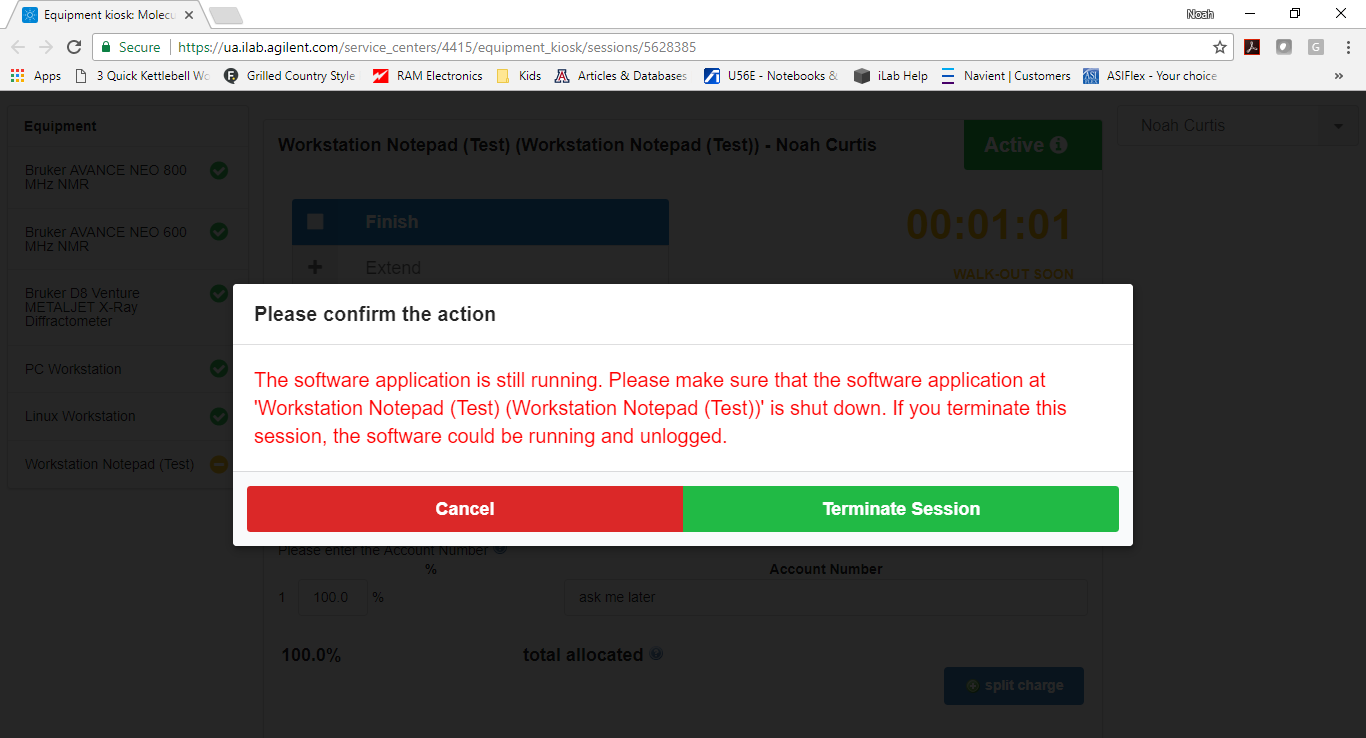


* + - 1. **When the User has NOT closed the designated application** before finishing the session the following screen informs him that the session can only be closed after closing the application.



### As a Core or Institutional Admin

Teminating the session does not necessarily require closing the iLab session. This can be seen from the snapshot below.



# Additional Resources

Sassafras

<http://www.sassafras.com/>

Sassafras Sales

[sales@sassafras.com](mailto:sales@sassafras.com) (Mike Witthaus has been our contact)

Sassafras Support

[support@sassafras.com](mailto:support@sassafras.com)

Phone: (603) 643-3351

Sassafras K2 product

<http://www.sassafras.com/features/>