Software Interlock

Contents

Overview

Core facilities, regulated labs, and cleanrooms often maintain expensive and sophisticated instrumentation and software to support scientific research and other technical work. They would often like to manage, and sometimes restrict, user access to these valuable resources. Currently, iLab has a kiosk and hardware interlock solution whereby instrumentation access can be physically controlled using the iLab Hardware Access Control approach.

However, there are scenarios where certain pieces of equipment may be too sensitive to be administered in such a fashion or when a facility does not have easy access to the necessary IT and/or electrical support staff needed to implement a hardware interlock.

To address these scenarios, Agilent and Sassafras Software, a software license management provider, have collaborated to develop a unique method to manage access to the software that controls the instrument rather than controlling access to the instrument directly.

This functionality controls user access to specific software programs, governed using a combination of Agilent's iLab Operations Software (iLab) scheduling functionality and Equipment Kiosk interface, and the Sassafras K2-KeyServer.

K2-KeyServer is an IT software asset management product from Sassafras Software. Generally, Sassafras KeyServer can keep track of both hardware and software, discover what software you have, track who is using it and how often, and report on usage. Specifically, when used with iLab, K2 is able to enforce policies, which will either allow or disallow the use of software, after consulting with the iLab database. Therefore, software usage can be tied to trained usage or scheduled events booked on iLab calendars.

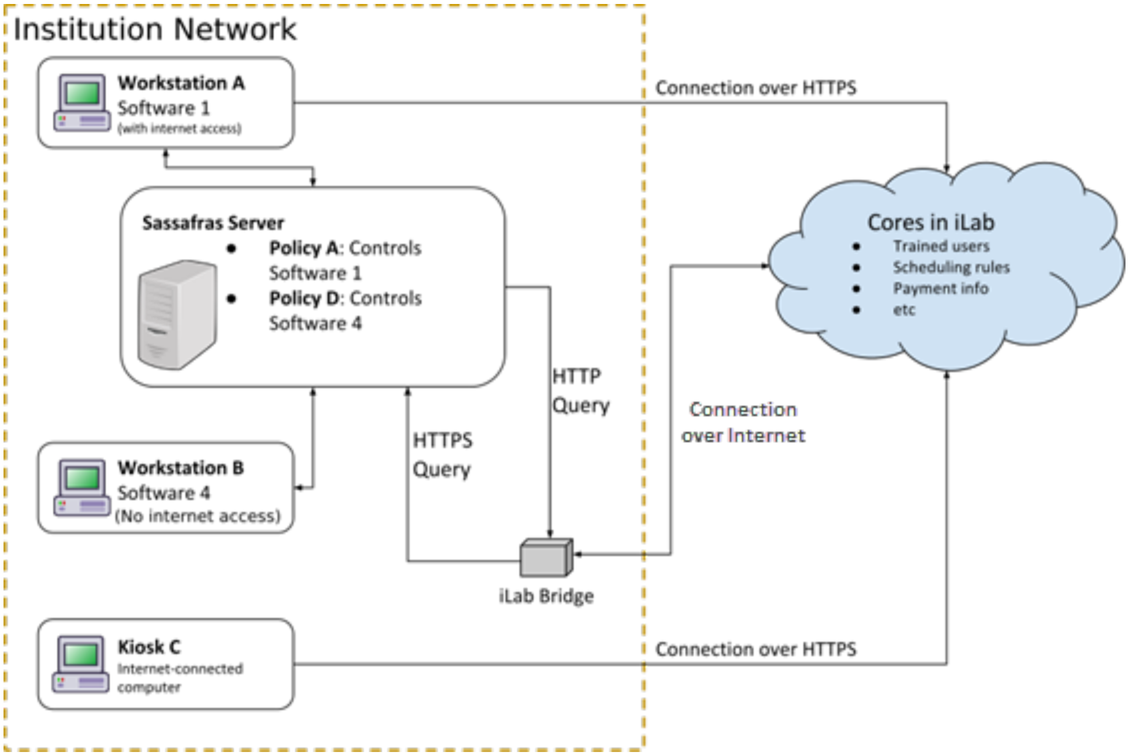
Please note the following:

1. The iLab Operations Software and Sassafras's K2-Key Server are two individual software products that are purchased separately and, initially, separately configured. Once the initial implementation and

configuration of each is complete, the two products can then be linked together via Sassafras software control policies and iLab calendar and interlock management settings.

2. Due to the wide variety of specific software configurations, operating systems and technical requirements utilized by different instrumentation vendors, Agilent cannot guarantee that every software program can be controlled by the Sassafras-iLab Software Interlock feature. However, because of the robustness of both systems and their respective technical support teams, we anticipate scenarios like this will be infrequent.

Schematic of Software Interlock Components



Prerequisites - Sassafras

1. A unique Sassafras *K2-KeyServer* needs to be installed within the Institution's network for each core facility. This *KeyServer's*

responsibility will be to govern any computers that will need to use the Software Interlock functionality within that core facility.

   a. If an institution already has an installation of Sassafras, a separate, unique instance of KeyServer will be required to support each core facility.

   b. iLab recommends there be a central point of contact(s) at the institution to work with iLab to configure and manage the Software Interlock *KeyServer* installation and configuration. It is recommended that this POC(s) be from the Institution's IT Department.

2. Each computer that hosts controlled software will need to have a Sassafras Client (*KeyAccess*) installed on it. The *KeyAccess* client allows Sassafras's *KeyServer* to recognize the computer and identify all software programs installed on it.

   a. Institutions and/or cores will need to purchase enough client licenses to accommodate the total number of computers that will host controlled software programs (not the total number of software programs).

3. Provide local administrative access to the Sassafras *KeyConfigure* interface.

   a. *KeyConfigure* is the interface that allows a local administrator to view computers and installed software, and will be the access point for configuring software Control and Deny Policies[R(1]

4. Any computer on the Institution network that wants to use the Software Interlock solution will need to have network connectivity to this KeyServer (but not necessarily internet access) and controlled applications will be governed by this new Sassafras server.

Prerequisites - iLab

1. iLab *Bridge* configured for Software Interlock will need to be installed.
    a. Note: If an institution already has an iLab *Bridge* for Hardware Interlock, it can be configured to work with Software Interlock
2. An iLab *Calendar* which has been set up and configured for appropriate user access to the controlled software (set up scheduling rules, trained users, etc).

Example User Scenarios for Software Interlock

(Use the above diagram as a reference)

Our existing *Kiosk* interface will be used as an entry point for all Software Interlock interactions.

1. iLab and Sassafras Configurations
    a. In Sassafras *KeyServer*
        i. Workstations A and B are registered
        ii. Software 1 and 4 are registered
    b. In Sassafras *KeyServer*
        i. Policy A is configured to govern Software 1 and the Group ID for Workstation A is entered
        ii. Policy D is configured to govern Software 4 and the Group ID for Workstation B is entered
        iii. Note: There are at least two policies created for each piece of Software (deny and control); however, Sassafras has a lot of flexibility in how policies can be

defined, so there may be further discussion to refine policy definitions.

c. In iLab

   i. Core manager configures Software 1 on Workstation A as a piece of equipment or “resource”, sets up the scheduling rules, training etc. and enters the unique Workstation A ID in iLab

   ii. Core manager effectively associates Software 4 on Workstation B as a piece of equipment or “resource”, sets up the scheduling rules, training etc. and enters the unique Workstation B ID in iLab

2. End-user (researcher) workflow - Workstation A IS connected to the Internet

a. In iLab, researcher clicks Start session through Kiosk interface on the Core page that references Software 1 on Workstation A

b. iLab records that Policy A on Workstation A should be allowed

c. On Workstation A, researcher launches Software 1

d. On Workstation A, Software 1 asks the Sassafras KeyServer if Software 1 can be opened

e. Sassafras KeyServer asks iLab if Policy A on Workstation A is allowed to be launched

f. iLab responds Yes

g. Sassafras KeyServer responds Yes to Workstation A

h. Software 1 launches on Workstation A

i. On Workstation A, researcher uses software 1

j. On Workstation A, researcher finishes their work and closes the controlled software.

k. In iLab, researcher clicks End+ session through the Kiosk interface and the event/time is recorded

l. iLab records that Policy A is no longer active for Workstation A

m. On Workstation A, the next time Software 1 is opened, it cannot be opened unless the next user has a valid reservation to use the software program.

3. End-user (researcher) workflow - Workstation B IS NOT connected to the Internet

a. In iLab, from Kiosk C (which is connected to the internet), researcher clicks Start session through Kiosk interface on the Core page that references Software 4 on Workstation B.

b. iLab records that Policy D on Workstation B should be usable.

c. On Workstation B, researcher launches Software 4

d. Remaining steps from 2.c. to 2.j. (above)

e. On Workstation B, researcher finishes their work and closes the controlled software.

f. On Kiosk C, in iLab, researcher clicks End session through the interface and the event/time is recorded

g. iLab records that Policy D is no longer active for Workstation B

h. On Workstation B, the next time Software 4 is opened, it cannot be opened unless the next user has a valid reservation to use the software program.

4. Software Usage Billing

   a. The user, event and time spent during the session will be recorded as logged time in the Confirm Usage panel associated with the controlled software in iLab.

   b. Once usage is confirmed, a core administrator will then be able to generate invoices and bill for these events.

   c. iLab provides different ways of tracking the billed time: (1) scheduled, (2) logged, (3) maximum of the two

Additional Implementation Instructions

Within Sassafras

Install Sassafras KeyServer
KeyServer can be downloaded from this URL:
https://www.sassafras.com/download/
The first time you access this URL on a specific computer you will be prompted to fill for your email address to gain access to the downloads page. The first time you will then complete a form - subsequently your email alone will be enough to reach this page on other computers. When filling out the form, please include the text “iLab” in the Primary interest/concerns field.

Installation is very easy and is described here:
https://www.sassafras.com/hrl/8.0/tour01.html

Install KeyConfigure and connect to KeyServer using either the IP address, or preferably a DNS name.

Set Client Authentication to “iLab” within the KeyConfigure

1. In Sassafras, open Config > Client Authentication.

2. Set the *Method* to iLab

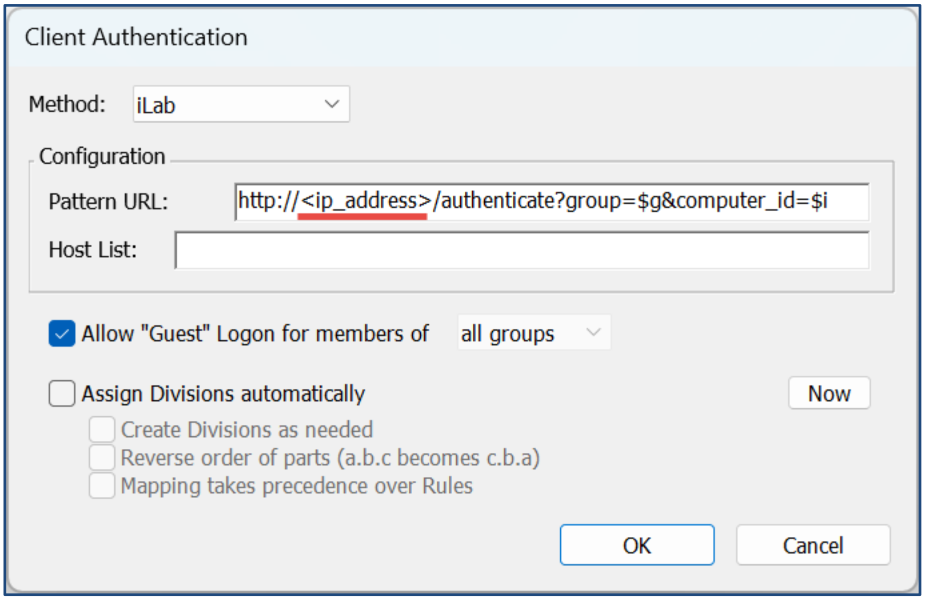
3. Set the *Pattern URL* to the following:

4. http://<bridgeIPaddress>/authenticate?group=$g&computer_id=$i

5. where *ip_address* is the static IP address of the iLab Bridge as provided by the network administrators at the host institution

6. Check *Allow "Guest login for members* and select *all groups*.

7. Click OK.



Client Authentication

Method: iLab

Configuration

Pattern URL: http://<ip_address>/authenticate?group=$g&computer_id=$i

Host List:

☑ Allow "Guest" Logon for members of all groups

□ Assign Divisions automatically

□ Create Divisions as needed

□ Reverse order of parts (a.b.c becomes c.b.a)

□ Mapping takes precedence over Rules

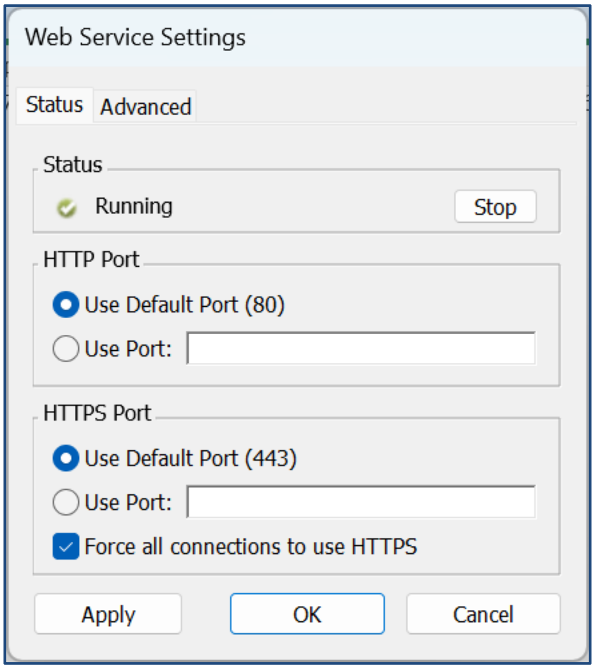
Ensure that Sassafras Web Service is turned on

1. In Sassafras, open Config > Web Service Settings

2. Select default ports for both HTTP (80) and HTTPS (443). Optionally, for increased security, select "Force all connections to use HTTPS"

3. If Status says running, skip to step 5

4. If Status says “Not Running” click on “Start”. If it fails to start, make sure there is no other application serving content on port 443 on the same server.

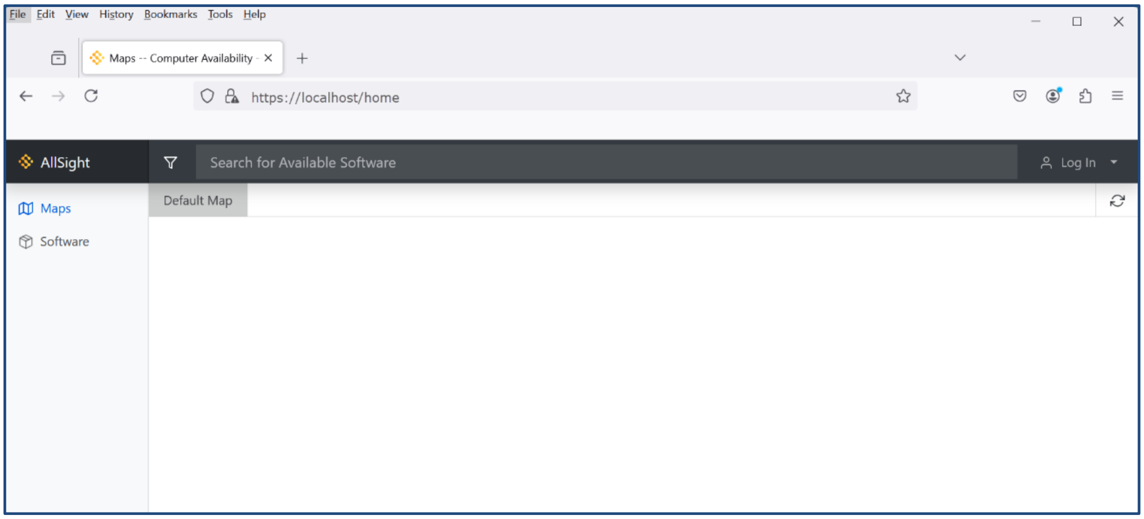


Status
Running

HTTP Port
● Use Default Port (80)
○ Use Port:

HTTPS Port
● Use Default Port (443)
○ Use Port:
☑ Force all connections to use HTTPS

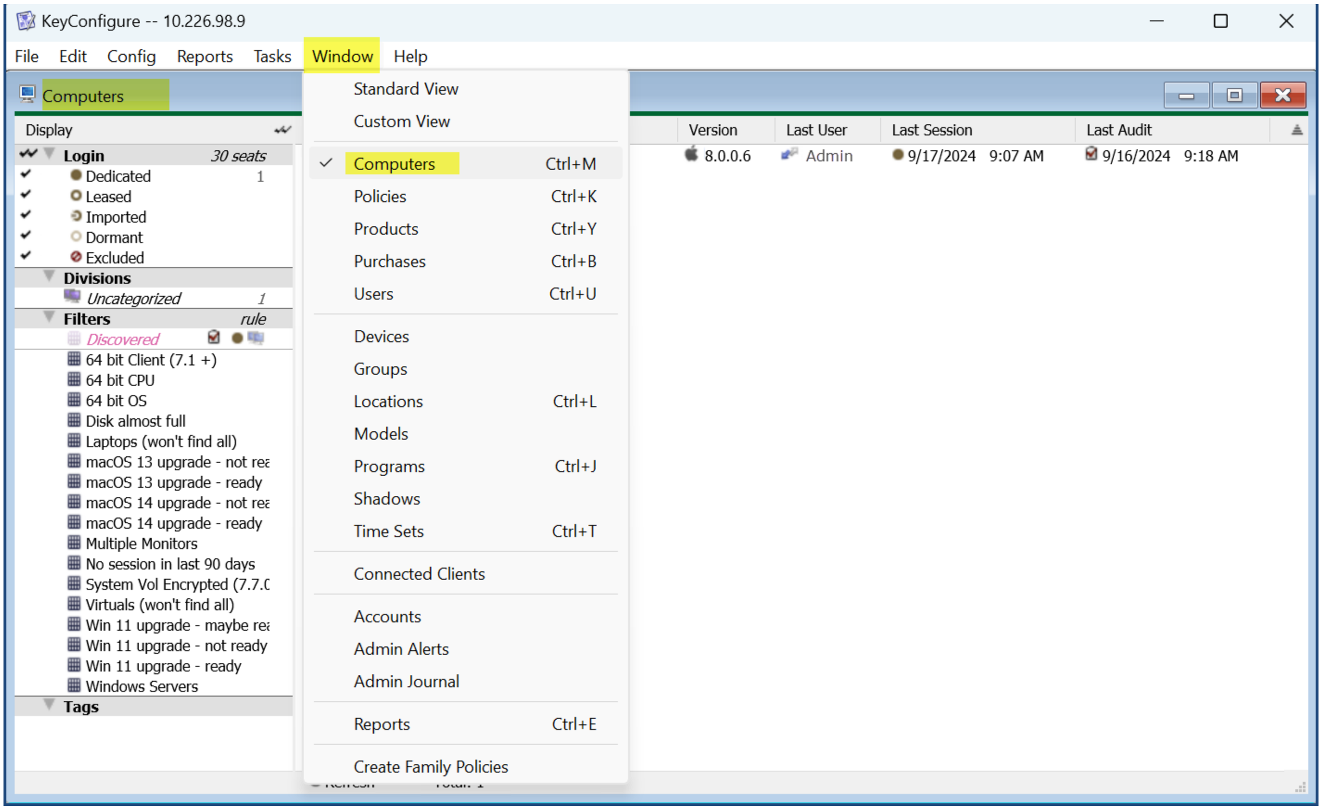
5. Confirmation step – using a browser on the Sassafras server visit https://localhost/ - you should see the Web Service dashboard:


File Edit View History Bookmarks Tools Help
Maps -- Computer Availability
https://localhost/home
AllSight
Search for Available Software
Log In
Default Map
Maps
Software

Install Sassafras KeyAccess Client
Install *KeyAccess* on the computers where the controlled software is installed. This allows the Sassafras *KeyServer* to recognize the computer and identify all software programs installed on it. All computer and software names will then be visible in the *KeyConfigure* interface in their respective windows. The client can be downloaded from: https://www.sassafras.com/client-download/
You will need to enter the address (IP or DNS) of the KeyServer during installation.

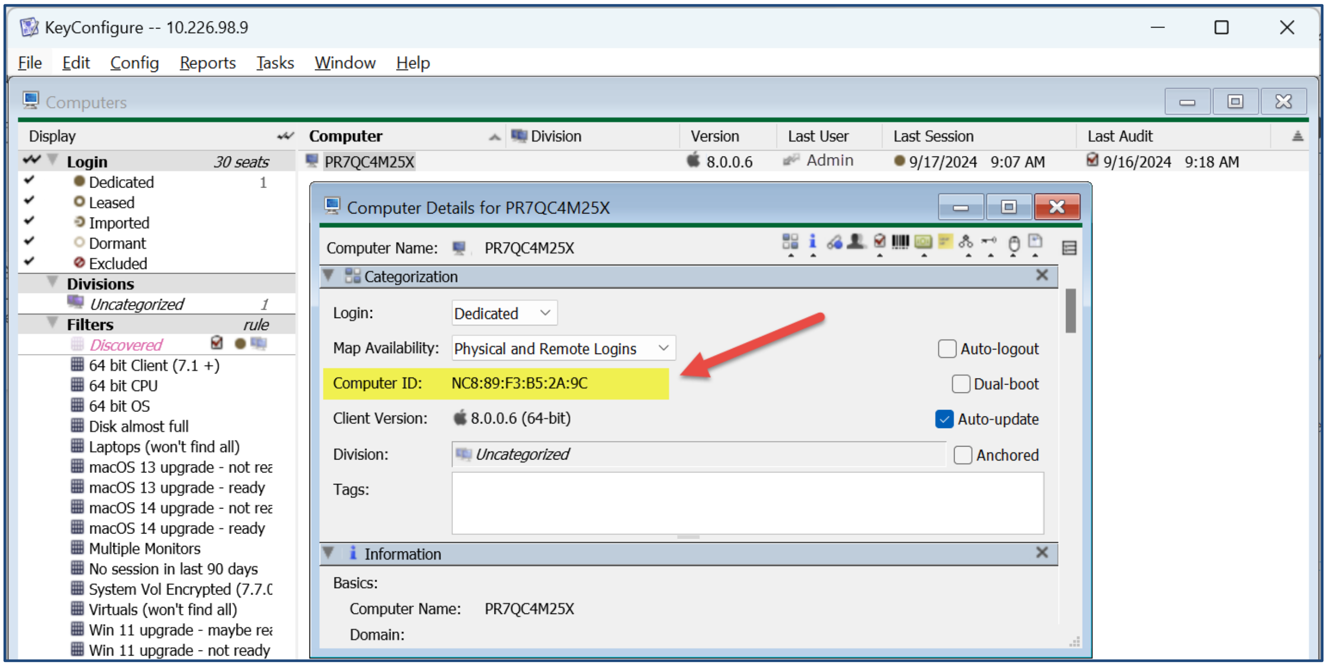
Once the *KeyAccess* client is installed, allow 10-20 minutes for *KeyAccess* to connect to KeyServer, and upload a complete list of installed software programs. Within seconds of installing, you can proceed to the next step of *Locate Computer ID* in the *KeyConfigure* interface.

Locate Computer ID
Within the *KeyConfigure* interface, open the *Computers* window by going to the *Window* option in the top navigation menu and selecting *Computers*:



Version	Last User	Last Session	Last Audit
8.0.0.6	Admin	9/17/2024 9:07 AM	9/16/2024 9:18 AM

Next, locate the workstation that hosts the software you wish to control in the *Computers* list. Double-click on its name to open the details window as shown below. Note its Computer ID. You can right-click on this ID to Copy it to the clipboard.



Computer	Division	Version	Last User	Last Session	Last Audit
PR7QC4M25X		8.0.0.6	Admin	9/17/2024 9:07 AM	9/16/2024 9:18 AM

Display
Login 30 seats
✓ Dedicated 1
✓ Leased
✓ Imported
✓ Dormant
✓ Excluded
Divisions
Uncategorized 1
Filters *rule*
Discovered
64 bit Client (7.1 +)
64 bit CPU
64 bit OS
Disk almost full
Laptops (won't find all)
macOS 13 upgrade - not rea
macOS 13 upgrade - ready
macOS 14 upgrade - not rea
macOS 14 upgrade - ready
Multiple Monitors
No session in last 90 days
System Vol Encrypted (7.7.(
Virtuals (won't find all)
Win 11 upgrade - maybe rea
Win 11 upgrade - not ready

Computer Name: PR7QC4M25X

Categorization

Login: Dedicated
Map Availability: Physical and Remote Logins
Computer ID: NC8:89:F3:B5:2A:9C
Client Version: 8.0.0.6 (64-bit)
Division: *Uncategorized*
Tags:

☐ Auto-logout
☐ Dual-boot
☑ Auto-update
☐ Anchored

Information

Basics:
Computer Name: PR7QC4M25X
Domain:

Within iLab

Basic Requirements for Using the iLab Bridge and Software Interlock

To take full advantage of the Software Interlock, some coordination will be required with the institution's IT and networking teams. The IT professionals should be able to follow the instructions below and utilize the linked resources in this document to set up the bridge.

Network Requirements

Interlock Subnet

An onsite IT team will need to create a secure local network in which the iLab Bridge will reside. The Bridge and Sassafras server do not have to be on the same subnet:

- The Bridge needs only to be connected to the internet.
- When the Bridge is installed, the Sassafras server should be able to connect to the Bridge on port 80 (HTTP).
- The Bridge should be able to connect to the Sassafras server on port 443 (HTTPS).

Hardware Requirements

iLab Bridge

Once an agreement is in place, the iLab engineering team will configure and send you an iLab Bridge. The Bridge initiates a secure connection to our iLab servers from within your organization. The only needs to be connected to the internet. You will work with your iLab implementation team to determine timing and availability of the iLab Bridge.

Note: One Bridge is needed per network; if your institution has multiple networks, you will need multiple Bridges if you can't route everything to one network.

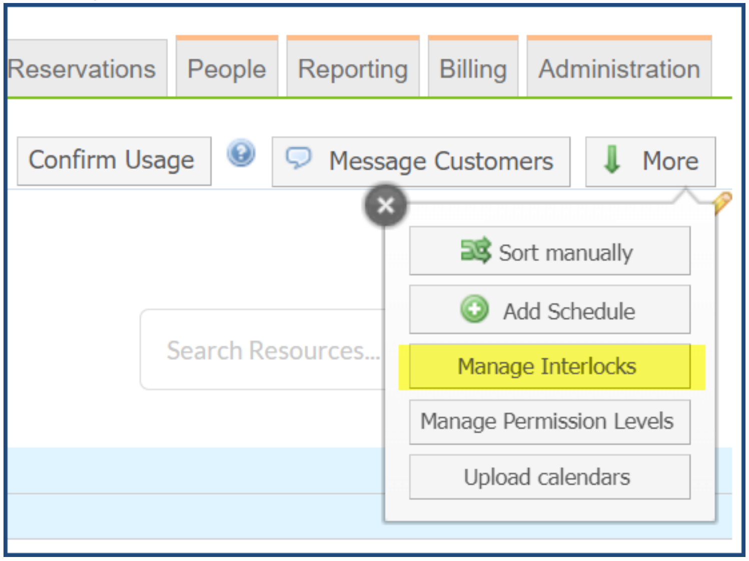
Configure Calendars

Create a calendar for each piece of controlled software and configure settings.

Manage Interlocks Interface

Configure the Software Interlock set up

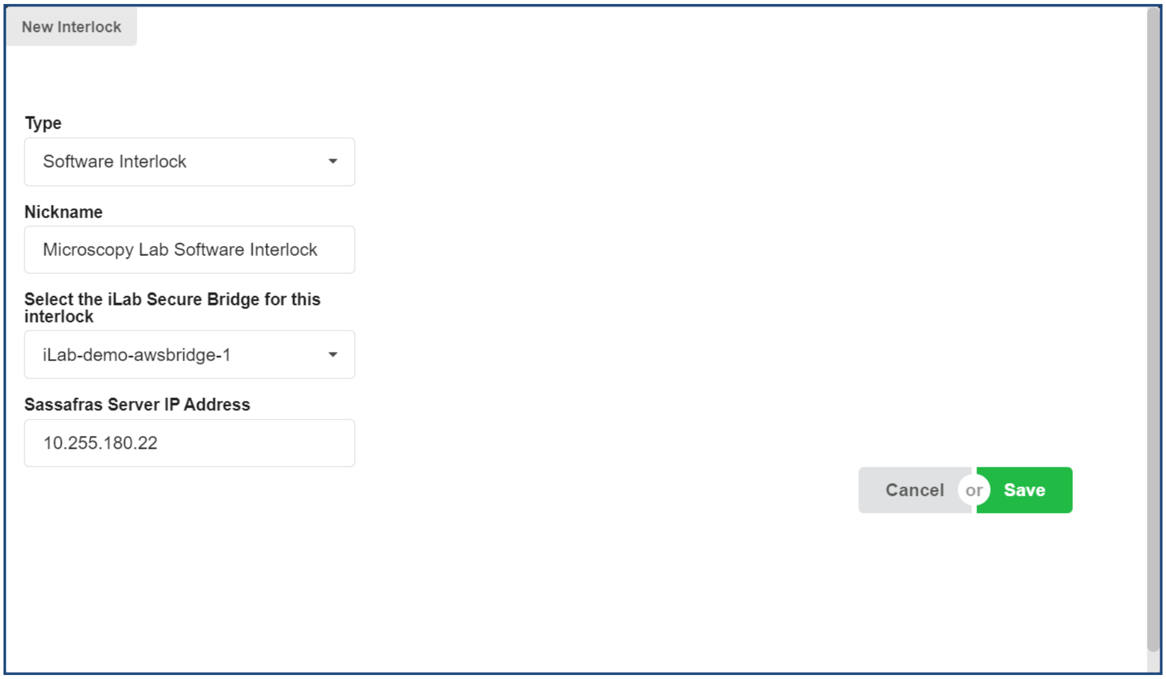
1. On the *Schedule Equipment* tab, click the *More* button and select *Manage Interlocks*



   a. Create new software interlock:

      Steps:

      1. Choose the Type of interlock
      2. Give it a Nickname
      3. Enter the IP address of the Sassafras Server as provided by network admin at institution or Sassafras administrator
      4. Choose the appropriate iLab Bridge to associate to the software interlock and click save.



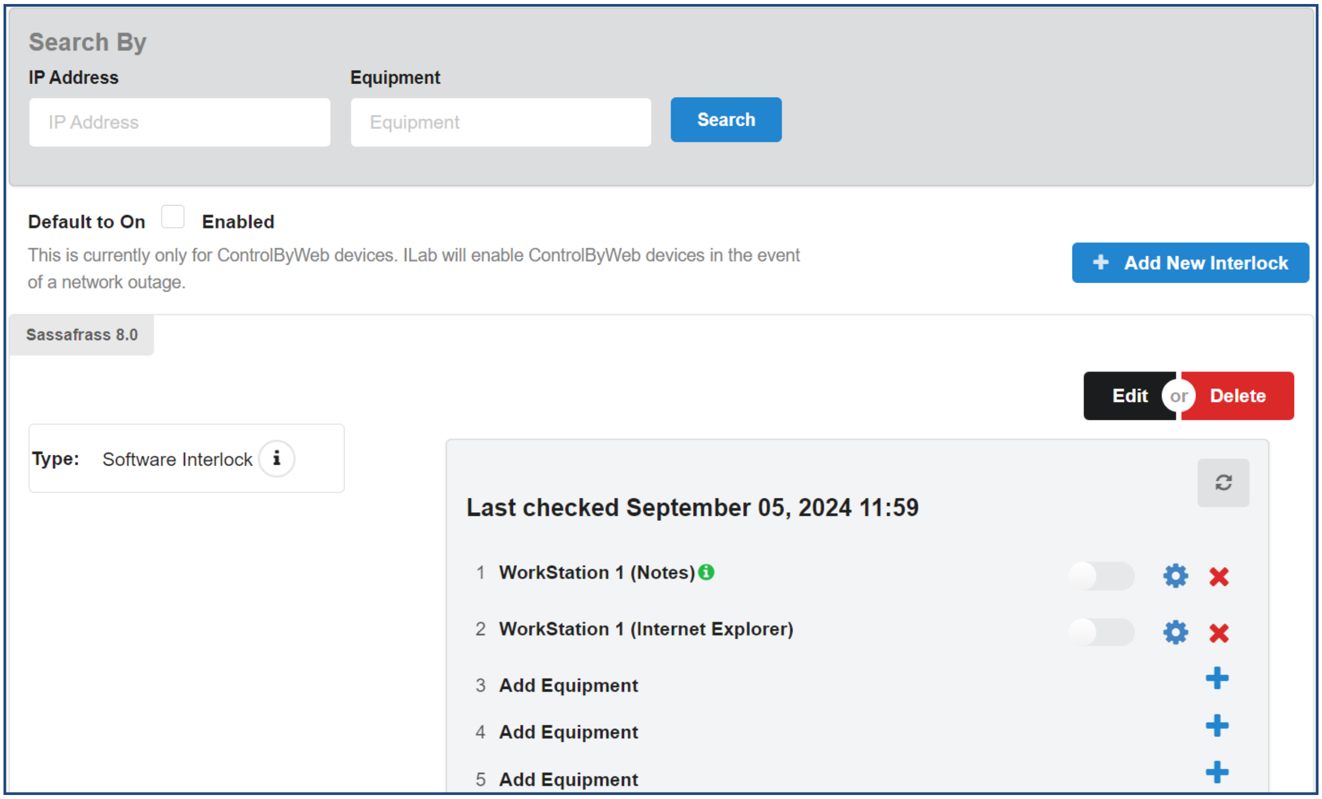
Type: Software Interlock

Nickname: Microscopy Lab Software Interlock

Select the iLab Secure Bridge for this interlock: iLab-demo-awsbridge-1

Sassafras Server IP Address: 10.255.180.22

b. OR access an existing software interlock:



Default to On □ Enabled

This is currently only for ControlByWeb devices. ILab will enable ControlByWeb devices in the event of a network outage.

Type: Software Interlock ℹ

Last checked September 05, 2024 11:59

1 WorkStation 1 (Notes) ℹ

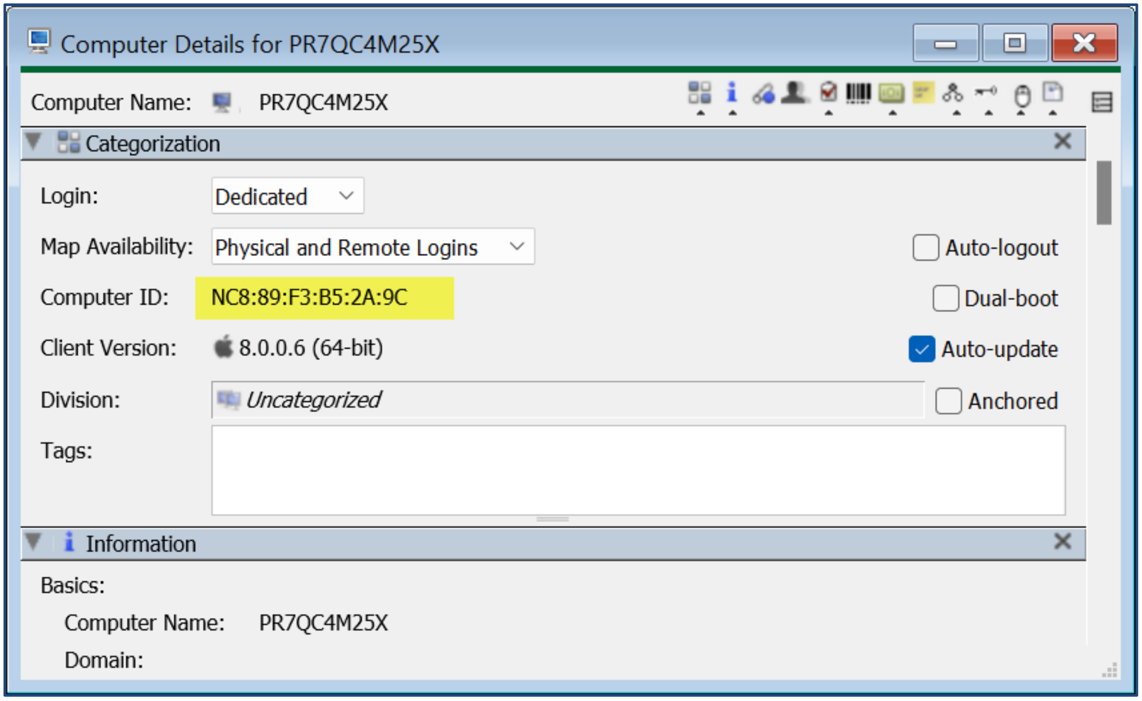
2 WorkStation 1 (Internet Explorer)

3 Add Equipment

4 Add Equipment

5 Add Equipment

a. Add the controlled software calendar to the software interlock list.
b. Select the next available blue + icon and choose the software calendar from the drop-down menu.
c. Next, access that calendar's software interlock settings by clicking on the blue gear icon. Here, you will enter in the Computer ID you noted earlier from Sassafras (use Paste if you Copied it earlier). You'll also now copy the iLab Group ID.



Computer Details for PR7QC4M25X

Computer Name: PR7QC4M25X

Categorization

Login: Dedicated

Map Availability: Physical and Remote Logins

□ Auto-logout

Computer ID: NC8:89:F3:B5:2A:9C

□ Dual-boot

Client Version: 8.0.0.6 (64-bit)

☑ Auto-update

Division: *Uncategorized*

□ Anchored

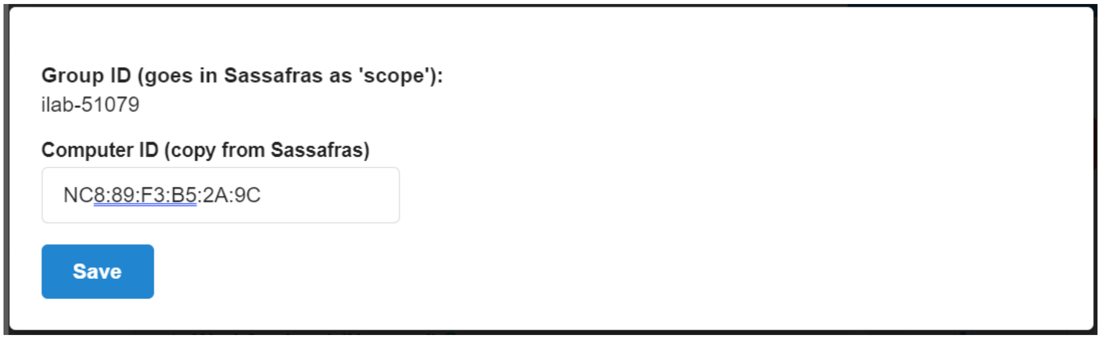
Tags:

Information

Basics:

Computer Name: PR7QC4M25X

Domain:



Group ID (goes in Sassafras as 'scope'):
ilab-51079

Computer ID (copy from Sassafras)

NC8:89:F3:B5:2A:9C

Configuring Applications and Policies in Sassafras

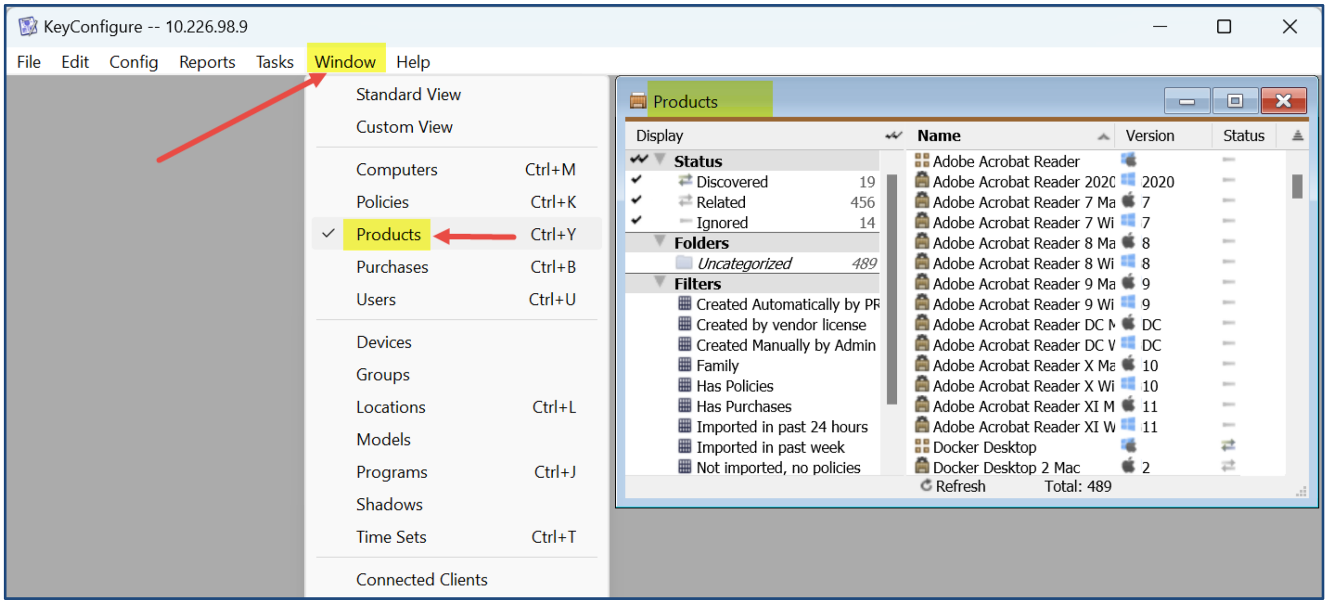
Create a Product

For this step you should wait until the client has completed the initial audit of all installed software (you can check this by looking at the “Last Audit” column in the Computers window). You will then create a new product in Sassafras. A product will be created in Sassafras for each software calendar in iLab.

Note: These directions represent the basic setup of a product in Sassafras for use in iLab’s Software Interlock feature. For additional details, you can refer to the following blog post:

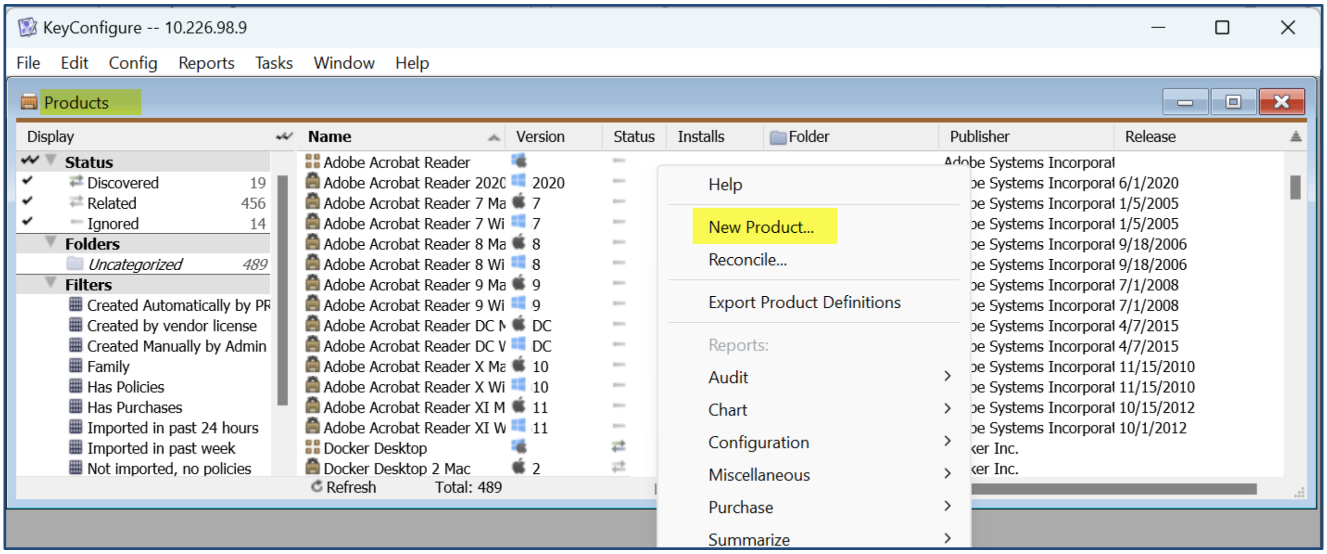
http://www.sassafras.com/manually-creating-accurate-product-definitions/

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



Name	Version	Status
Adobe Acrobat Reader		—
Adobe Acrobat Reader 2020	2020	—
Adobe Acrobat Reader 7 Ma	7	—
Adobe Acrobat Reader 7 Wi	7	—
Adobe Acrobat Reader 8 Ma	8	—
Adobe Acrobat Reader 8 Wi	8	—
Adobe Acrobat Reader 9 Ma	9	—
Adobe Acrobat Reader 9 Wi	9	—
Adobe Acrobat Reader DC M	DC	—
Adobe Acrobat Reader DC V	DC	—
Adobe Acrobat Reader X Ma	10	—
Adobe Acrobat Reader X Wi	10	—
Adobe Acrobat Reader XI M	11	—
Adobe Acrobat Reader XI W	11	—
Docker Desktop		⇄
Docker Desktop 2 Mac	2	⇄

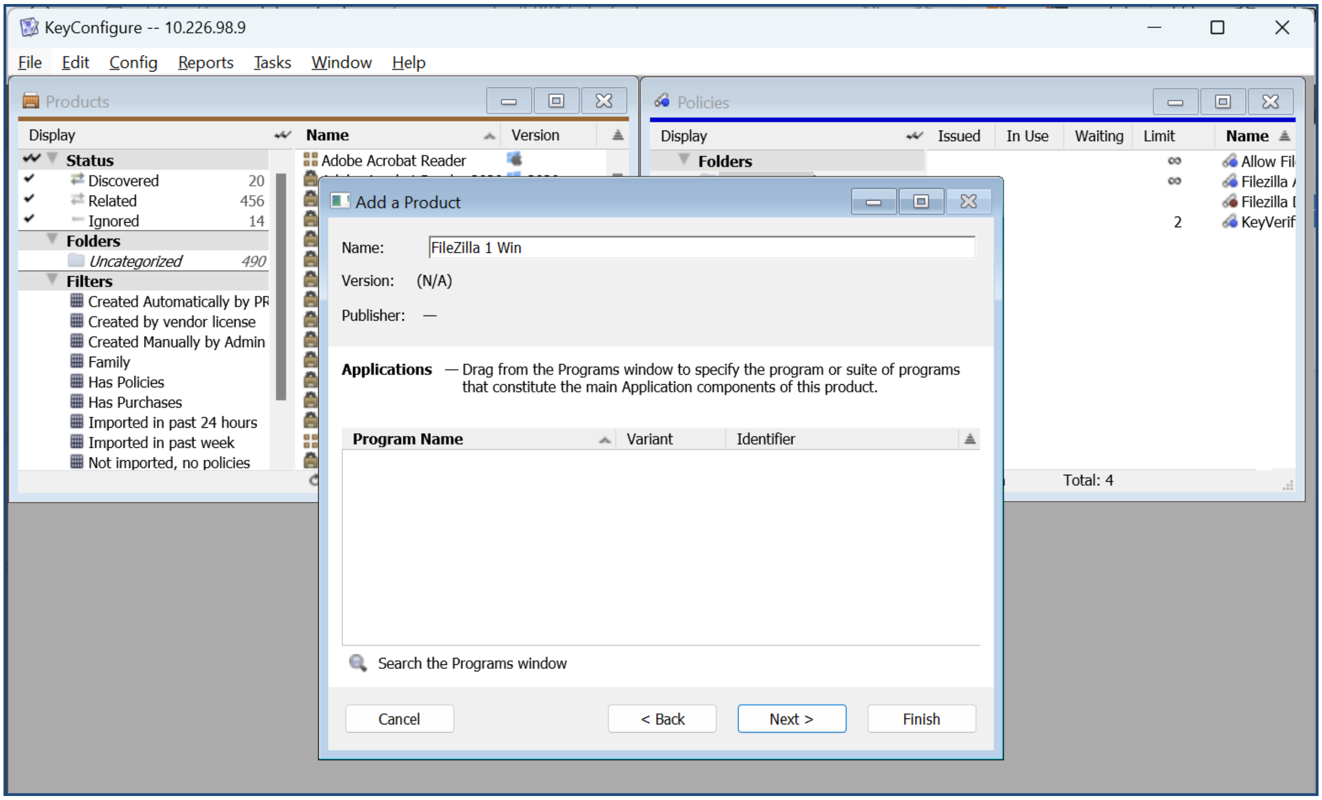
Now, right-click anywhere in the Product window and choose *New Product…*



Name	Version	Status	Installs	Folder	Publisher	Release
Adobe Acrobat Reader		–			Adobe Systems Incorporat	
Adobe Acrobat Reader 202C	2020	–			be Systems Incorporat	6/1/2020
Adobe Acrobat Reader 7 Ma	7	–			be Systems Incorporat	1/5/2005
Adobe Acrobat Reader 7 Wi	7	–			be Systems Incorporat	1/5/2005
Adobe Acrobat Reader 8 Ma	8	–			be Systems Incorporat	9/18/2006
Adobe Acrobat Reader 8 Wi	8	–			be Systems Incorporat	9/18/2006
Adobe Acrobat Reader 9 Ma	9	–			be Systems Incorporat	7/1/2008
Adobe Acrobat Reader 9 Wi	9	–			be Systems Incorporat	7/1/2008
Adobe Acrobat Reader DC M	DC	–			be Systems Incorporat	4/7/2015
Adobe Acrobat Reader DC V	DC	–			be Systems Incorporat	4/7/2015
Adobe Acrobat Reader X Ma	10	–			be Systems Incorporat	11/15/2010
Adobe Acrobat Reader X Wi	10	–			be Systems Incorporat	11/15/2010
Adobe Acrobat Reader XI M	11	–			be Systems Incorporat	10/15/2012
Adobe Acrobat Reader XI W	11	–			be Systems Incorporat	10/1/2012
Docker Desktop		⇄			ker Inc.	
Docker Desktop 2 Mac	2	⇄			ker Inc.	

Follow the steps in the basic product creation wizard:

1. Give your Product a name and then click *Next* until you reach the *Program* section.



Issued	In Use	Waiting	Limit	Name
			∞	Allow Fil
			∞	Filezilla /
				Filezilla I
			2	KeyVerif

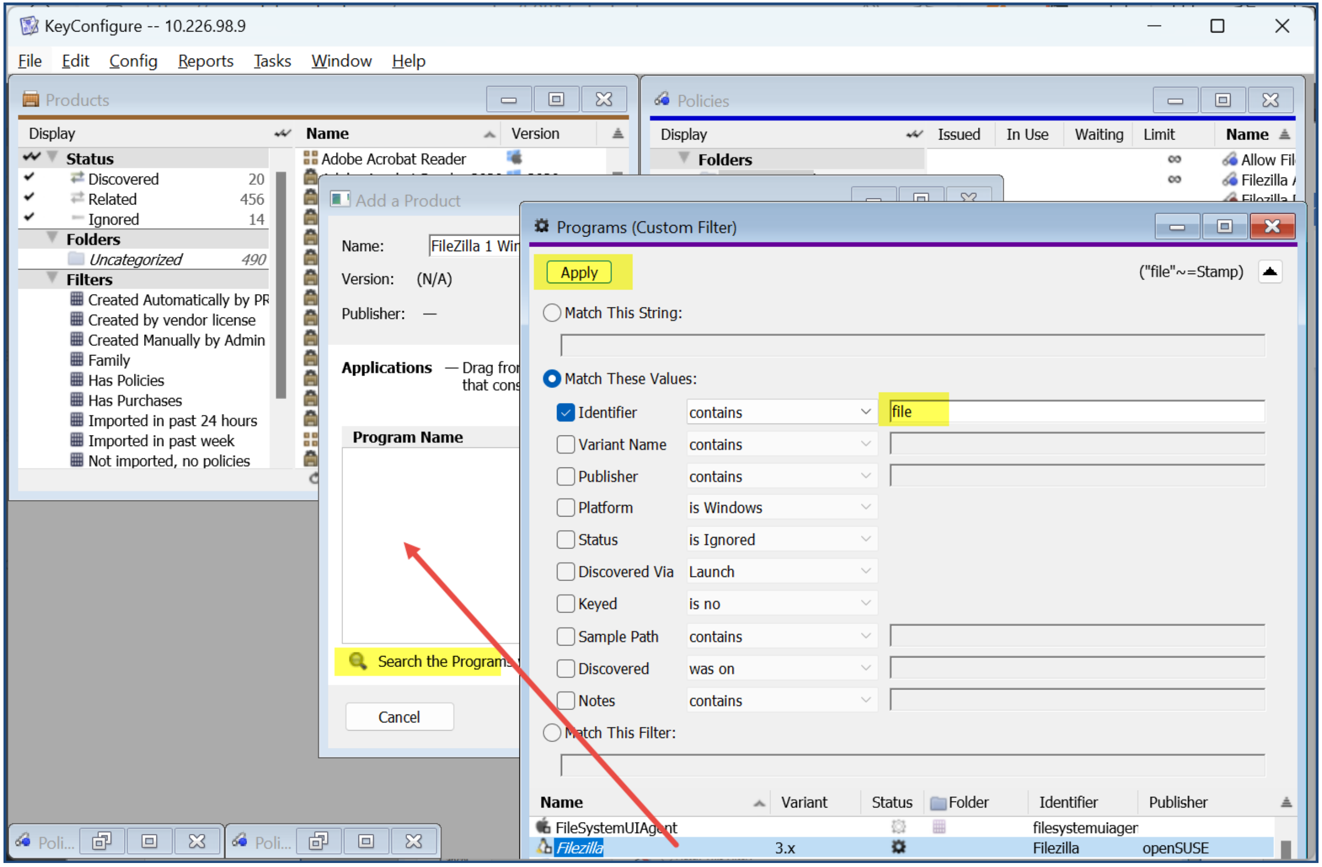
Total: 4

Name: FileZilla 1 Win
Version: (N/A)
Publisher: —

Applications — Drag from the Programs window to specify the program or suite of programs that constitute the main Application components of this product.

Program Name	Variant	Identifier

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



Name: FileZilla 1 Wir
Version: (N/A)
Publisher: —

("file"~=Stamp)

○ Match This String:

● Match These Values:

☑ Identifier	contains	file
□ Variant Name	contains	
□ Publisher	contains	
□ Platform	is Windows	
□ Status	is Ignored	
□ Discovered Via	Launch	
□ Keyed	is no	
□ Sample Path	contains	
□ Discovered	was on	
□ Notes	contains	

○ Match This Filter:

Name	Variant	Status	Folder	Identifier	Publisher
FileSystemUIAgent				filesystemuiager	
Filezilla	3.x			Filezilla	openSUSE

3. Click *Next*. You can generally skip the previous product [H(6] step for this setup process. Click *Next* again.

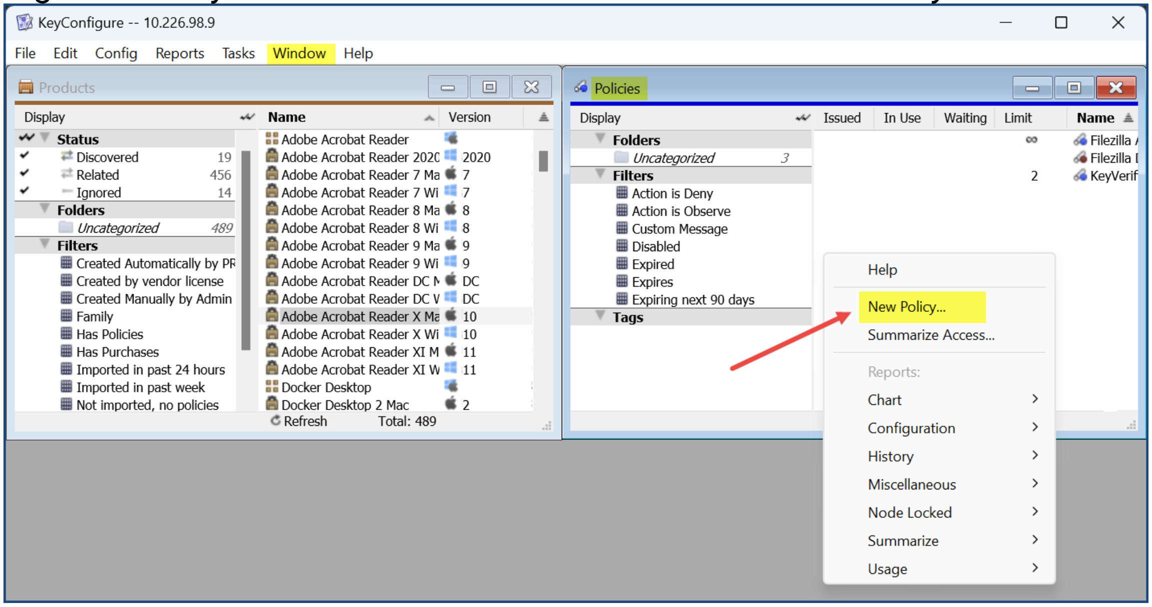
4. Click *Finish*.

Create Policies

You will now create policies for this product. For every product, there will be two policies - a deny policy and a second control policy.

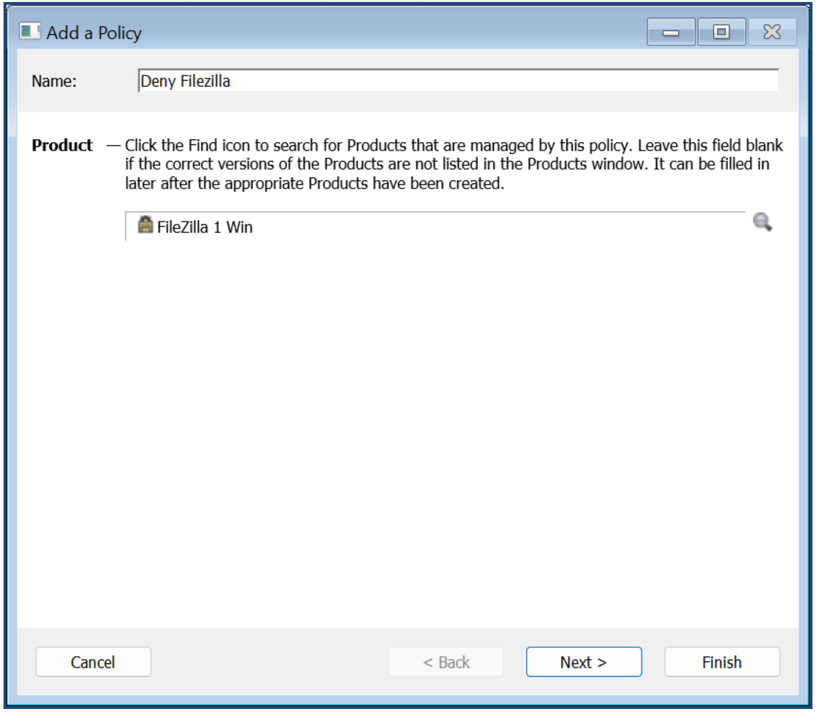
Create the Deny Policy

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



The first step is to associate a deny policy to your product. This policy functions to deny access
to this software by anyone who is not accessing it via the iLab kiosk.

1. Give your deny policy a name. Click *Next*.

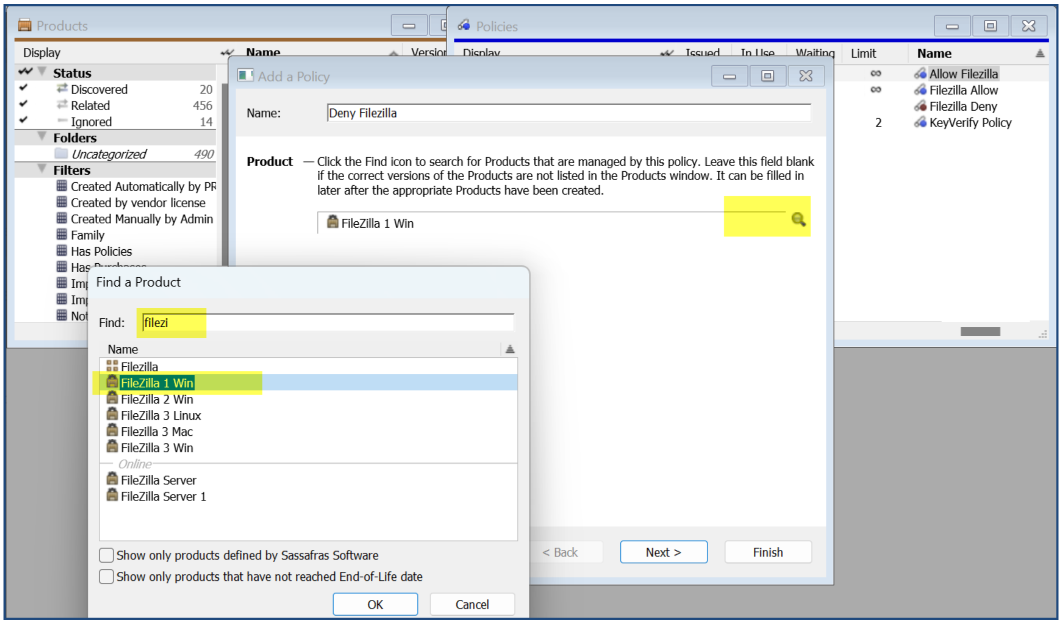


Name: Deny Filezilla

Product — Click the Find icon to search for Products that are managed by this policy. Leave this field blank if the correct versions of the Products are not listed in the Products window. It can be filled in later after the appropriate Products have been created.

FileZilla 1 Win

2. Now, associate the product you created previously by adding it to this policy, using the *Search by Products* magnifying glass:



Status
Discovered 20
Related 456
Ignored 14

Folders
Uncategorized *490*

Filters
Created Automatically by PR
Created by vendor license
Created Manually by Admin
Family
Has Policies
Has Purchases
Imp
Imp
Not

Limit	Name
∞	Allow Filezilla
∞	Filezilla Allow
	Filezilla Deny
2	KeyVerify Policy

Name: Deny Filezilla

Product — Click the Find icon to search for Products that are managed by this policy. Leave this field blank if the correct versions of the Products are not listed in the Products window. It can be filled in later after the appropriate Products have been created.

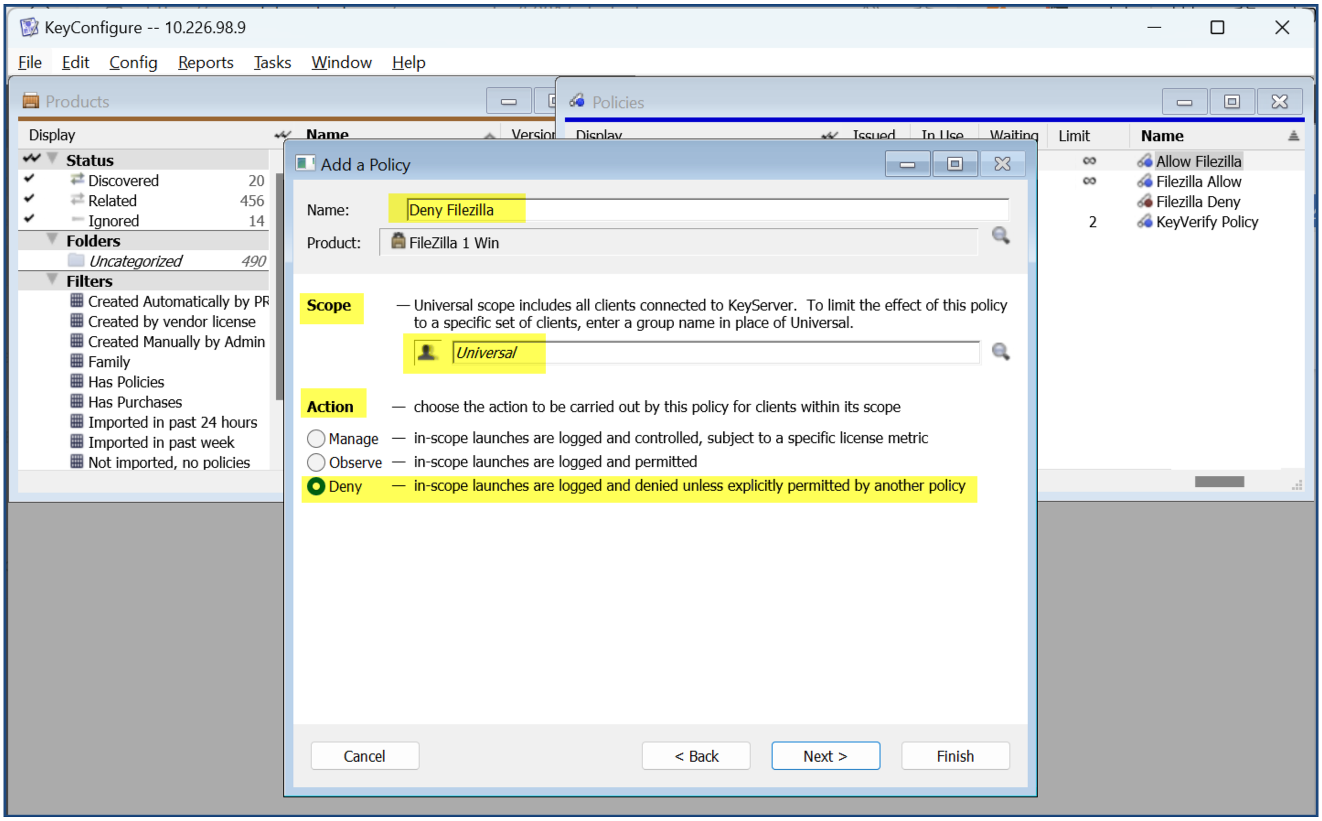
FileZilla 1 Win

Find: filezi

Name
Filezilla
FileZilla 1 Win
FileZilla 2 Win
FileZilla 3 Linux
Filezilla 3 Mac
FileZilla 3 Win
Online
FileZilla Server
FileZilla Server 1

☐ Show only products defined by Sassafras Software
☐ Show only products that have not reached End-of-Life date

3. Set the Action option to *Deny*. Leave the *Scope* field set to *Universal*. Click *Next*.



Name: Deny Filezilla

Product: FileZilla 1 Win

Scope — Universal scope includes all clients connected to KeyServer. To limit the effect of this policy to a specific set of clients, enter a group name in place of Universal.

Universal

Action — choose the action to be carried out by this policy for clients within its scope

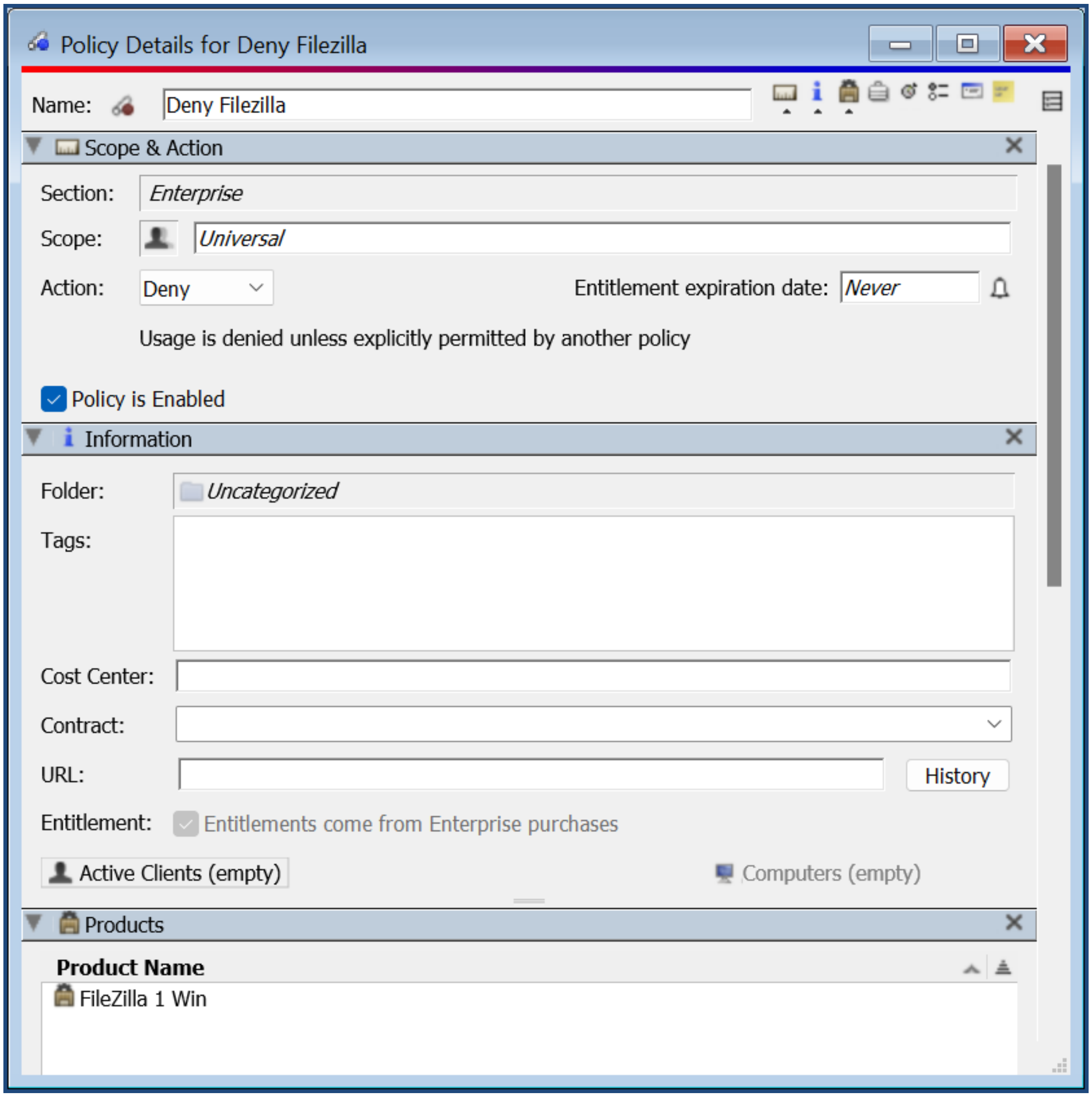
○ Manage — in-scope launches are logged and controlled, subject to a specific license metric

○ Observe — in-scope launches are logged and permitted

● Deny — in-scope launches are logged and denied unless explicitly permitted by another policy

4. Click *Finish*.

You can confirm your final deny policy configuration by opening the policies window, locating your deny [software] policy and double-clicking on it. This will bring up the policy details and should look something like this:



Name: Deny Filezilla

Section: *Enterprise*

Scope: *Universal*

Action: Deny

Entitlement expiration date: *Never*

Usage is denied unless explicitly permitted by another policy

☑ Policy is Enabled

Folder: *Uncategorized*

Tags:

Cost Center:

Contract:

URL:

Entitlement: ☑ Entitlements come from Enterprise purchases

Active Clients (empty)

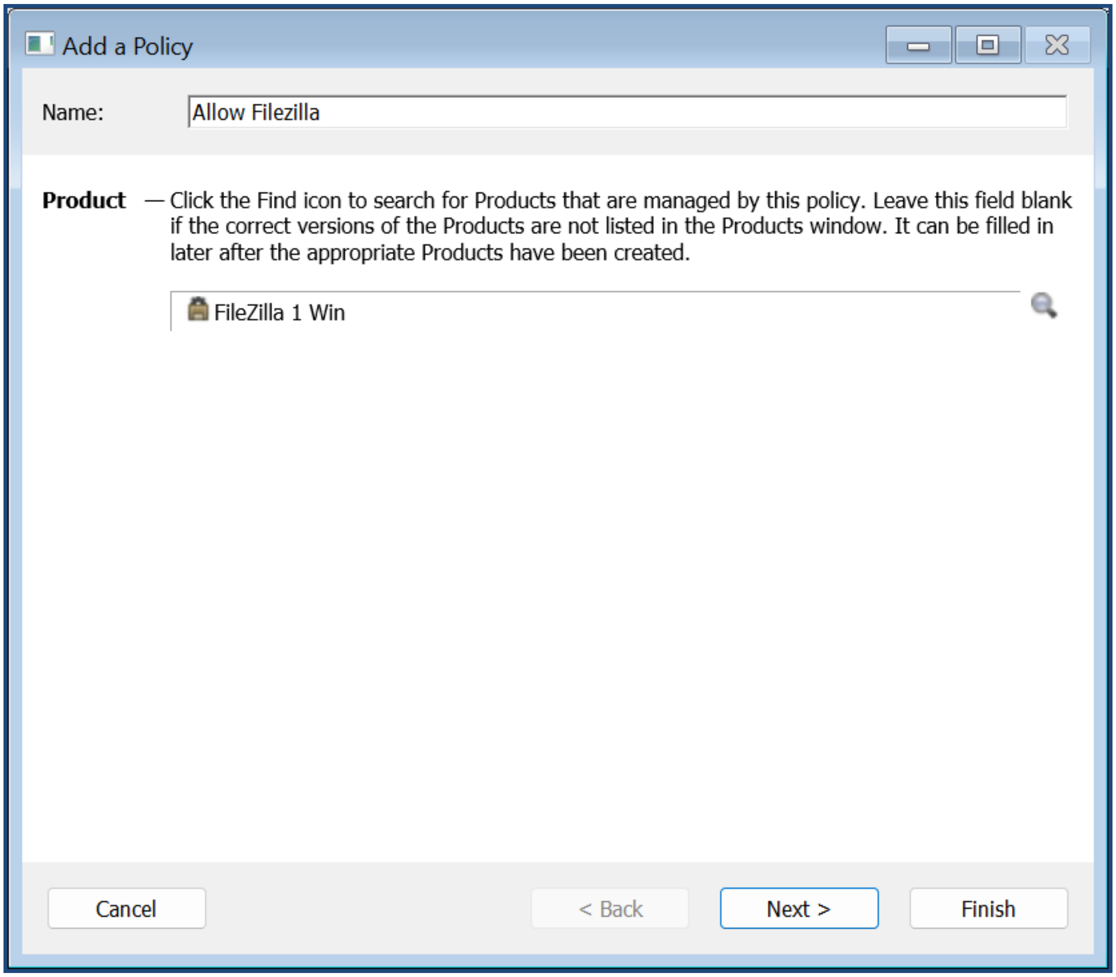
Computers (empty)

Product Name
FileZilla 1 Win

Create the Control Policy

The next step is to associate a second control policy to your product. This policy will allow only iLab users with appropriate reservations access to this product.

1. Create another new policy and give it a name. Start by right-clicking the first Deny policy and selecting “Duplicate”. You will again see the Add a Policy wizard, but it will have initial values just like the first policy - now you will change some properties. First change the name.



Add a Policy

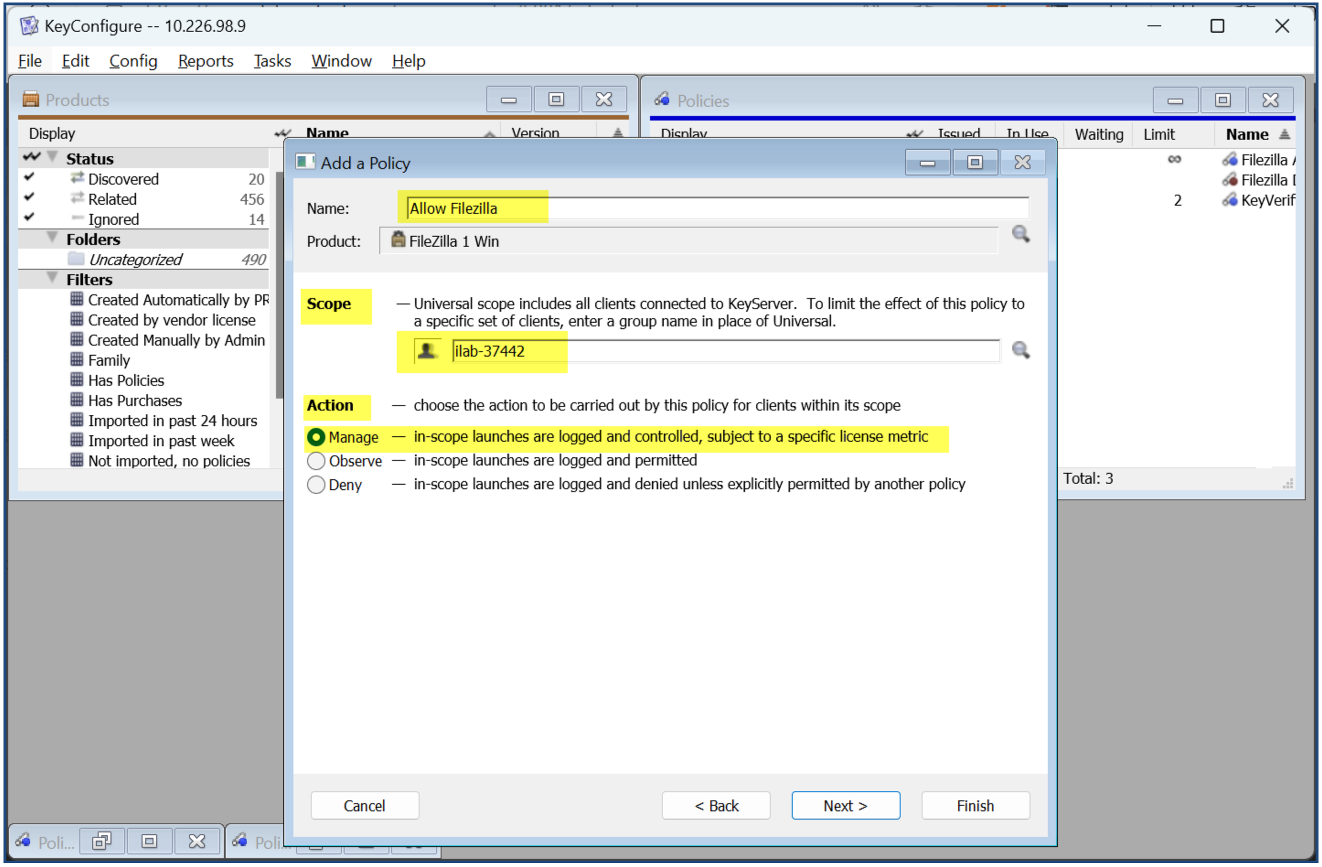
Name: Allow Filezilla

Product — Click the Find icon to search for Products that are managed by this policy. Leave this field blank if the correct versions of the Products are not listed in the Products window. It can be filled in later after the appropriate Products have been created.

FileZilla 1 Win

2. Click *Next* until you get to the Scope/Action screen.

3. Within this second policy, you will now enter the *Group ID* name (previously captured from the Software Interlock calendar setting) into the *Scope* field. Set the *Action* option to *Manage*.



Name: Allow Filezilla

Product: FileZilla 1 Win

Scope — Universal scope includes all clients connected to KeyServer. To limit the effect of this policy to a specific set of clients, enter a group name in place of Universal.

ilab-37442

Action — choose the action to be carried out by this policy for clients within its scope

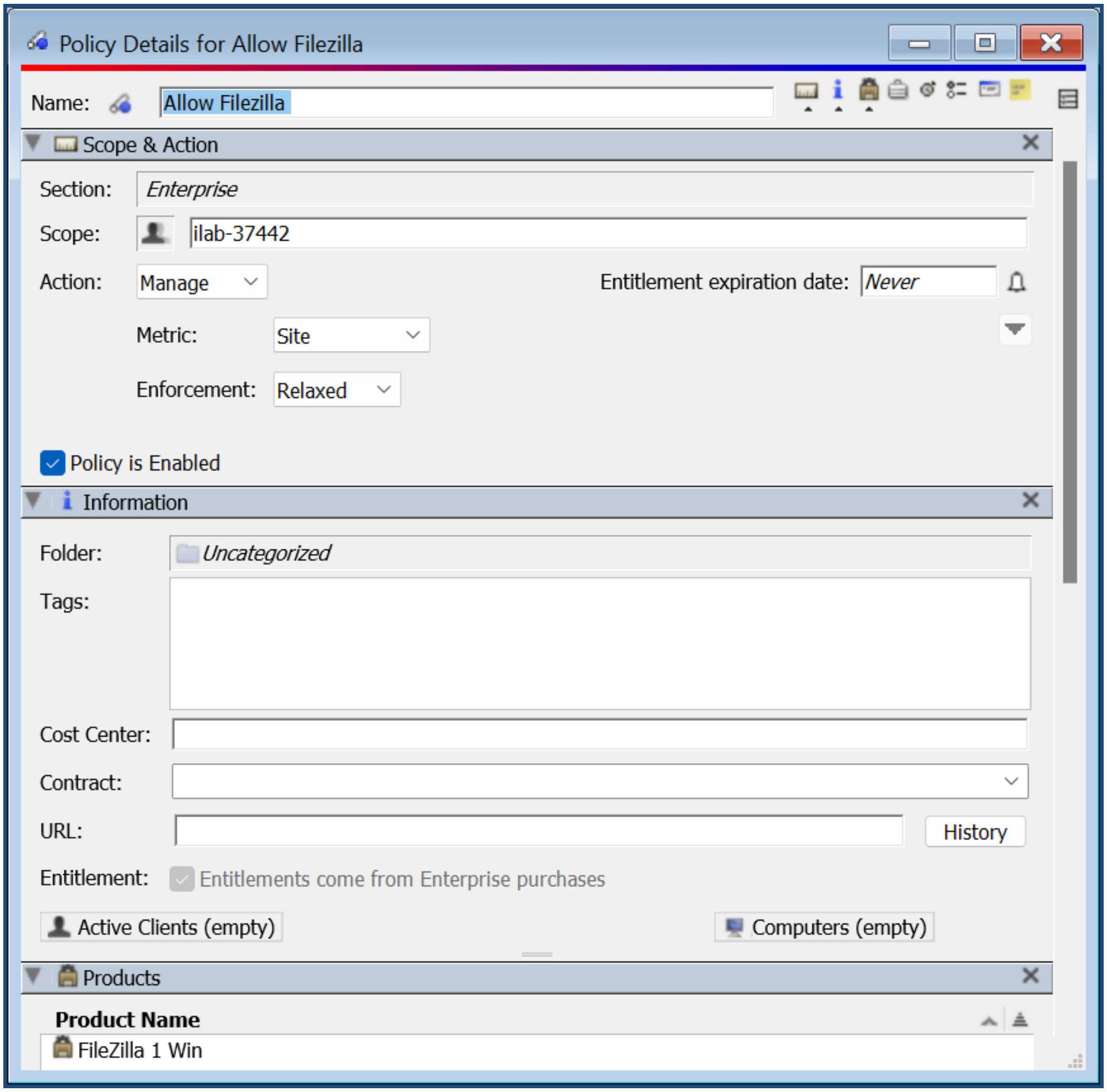
● Manage — in-scope launches are logged and controlled, subject to a specific license metric

○ Observe — in-scope launches are logged and permitted

○ Deny — in-scope launches are logged and denied unless explicitly permitted by another policy

4. Click *Finish*.

You can confirm your final allow policy configuration by opening the policies window, locating your allow [software] policy and double-clicking on it. This will bring up the policy details and should look something like this:



Policy Details for Allow Filezilla

Name: Allow Filezilla

Scope & Action

Section: *Enterprise*

Scope: ilab-37442

Action: Manage

Entitlement expiration date: *Never*

Metric: Site

Enforcement: Relaxed

☑ Policy is Enabled

Information

Folder: *Uncategorized*

Tags:

Cost Center:

Contract:

URL:

Entitlement: ☑ Entitlements come from Enterprise purchases

Active Clients (empty)

Computers (empty)

Products

Product Name
FileZilla 1 Win

Note that if you have more than one computer using the same product, you will need to make an additional Control Policy for each additional computer.

This completes the basic configuration of Software Interlock.

Additional Resources

Sassafras

http://www.sassafras.com/

Sassafras Sales

sales@sassafras.com

Sassafras Support

support@sassafras.com
Phone: (603) 643-3351

Sassafras K2 product

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