CY101EDU
Keysight Cyber Training Simulator

KEYSIGHT

USER'S GUIDE

Notices

Copyright Notice

© Keysight Technologies 2023
No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies as governed by United States and international copyright laws.

Manual Part Number

CY101-90004

Edition

Edition 1, October 2023

Printed in

Printed in Malaysia

Published by

Keysight Technologies
Bayan Lepas Free Industrial Zone
11900 Penang, Malaysia

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Declaration of Conformity

Declarations of Conformity for this product and for other Keysight products may be downloaded from the Web. Go to http://www.keysight.com/go/conformity. You can then search by product number to find the latest Declaration of Conformity.

U.S. Government Rights

The Software is “commercial computer software,” as defined by Federal Acquisition Regulation (“FAR”) 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement (“DFARS”) 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at https://www.keysight.com/my/en/assets/ndx/9018-08126/exhibits/9018-08126.pdf. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing else- where in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

Warranty

THE MATERIAL CONTAINED IN THIS DOCUMENT IS PROVIDED “AS IS,” AND IS SUBJECT TO BEING CHANGED, WITHOUT NOTICE, IN FUTURE EDITIONS. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KEYSIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, WITH REGARD TO THIS MANUAL AND ANY INFORMATION CONTAINED HEREIN, INCLUD ING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. KEYSIGHT SHALL NOT BE LIABLE FOR ERRORS OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, USE, OR PERFORMANCE OF THIS DOCUMENT OR OF ANY INFORMATION CON- TAINED HEREIN. SHOULD KEYSIGHT AND THE USER HAVE A SEPARATE WRITTEN AGREEMENT WITH WARRANTY TERMS COVERING THE MATERIAL IN THIS DOCUMENT THAT CONFLICT WITH THESE TERMS, THE WARRANTY TERMS IN THE SEPARATE AGREEMENT SHALL CONTROL.

Safety Information

CAUTION

A CAUTION notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Sales and Technical Support

To contact Keysight for sales and technical support, refer to the support links on the following Keysight websites:

- Product-specific information and support, software, and documentation updates
  www.keysight.com/find/CY101EDU (Keysight Cyber Training Simulator)
- Worldwide contact information for repair and service
  www.keysight.com/find/assist

Table of Contents

Notices 1

Introduction 5

PathWave Lab Operations for Remote Learning 5

Keysight Cyber Training Simulator 5

Characteristics and Specifications 5

Intended Use of the User's Guide 6

First-Time Setup 6

User Interface Overview 7

Home View 7

Bench Management View 8

Instructor Settings View 9

Schedule Remote Lab Session View 10

Reporting and History View 11

User Menu 12

Registration and Login 13

Schedule a Remote Lab Session 16

Connect to a Scheduled Session 17

Extend a Scheduled Session 19

Manage Virtual Lab Sessions 20

Map Virtual Labs to LMS Course 20

Schedule a Virtual Lab Session 21

Connect to a Virtual Lab Session 23

Management Menu 28

Keycloak Administration Console 28

Configure Roles 30

Add User 32

Manage User 34

Email Settings 35
Set Up Single Sign-On (SSO) 35
Set Up Email Settings 36
Mail Settings 36
Client Details 36
Guest Approval View 38
Install the Remote Agent 39
Add a New Bench 41
Session Management View 43
Manage Scheduled Sessions 43
Manage Remote Benches 44
License Management 45
License and Support View 45
License Installation and Activation 45

(Optional) Learning Tools Interoperability (LTI) Features 47
Integrate Moodle and PathWave Lab Operations for Remote Learning into LTI 1.3 47
Registering LTI 1.3 Tool 47
Integrate PathWave Lab Operations for Remote Learning into LTI 1.3 Blackboard 50
Add External Tools in Blackboard Platform 53
Obtain the Deployment ID 57
Add Details to the Application 58
Launch the Application in Blackboard 59

General Troubleshooting 60
Seeing a Blank Screen 60
Application Ceases to Respond or Bench Freeze 60
VRF Settings 60
Frequently Asked Questions 61

Recommended Password Practices 62

Criteria for Warranty Claims 63

Introduction

PathWave Lab Operations for Remote Learning

Online learning has been a part of many educational institutions since the spread of the Internet. Now, new norms such as physical distancing and limits on face-to-face interaction is dramatically accelerating the shift from traditional in-building learning to virtual classes offered remotely on digital platforms. The availability of online courses opens opportunities to international and distance learning students, and remote learning offers students the flexibility of learning anytime, anywhere. With these benefits, online learning is expanding exponentially, and educational institutes must rapidly transform to keep pace with this megatrend.

Keysight's industry-ready remote access lab solution offers you a convenient way to make the switch to online learning. This end-to-end solution is designed for complete remote setup of your basic instrument lab and covers your needs from web-based lab management and scheduling administration to instrument control and remote access for measurement and analysis. And since your students continue working with industry-grade test and measurement instruments and software, they will gain the similar practical skills and application knowledge as industry engineers conducting their work in the lab today.

Keysight Cyber Training Simulator

Demand for industry-ready cyber warriors is intense. There's no shortage of bad actors in cyberspace. But there is a serious shortage of trained professionals to counter them. Businesses, government agencies, education institutions, and other critical organizations have openings they're anxious to fill—immediately. An academic program that produces professionals who can step quickly into their roles would attract top students and forge strong relationships with the foremost hiring institutions.

Keysight Cyber Training Simulator is a complete, turnkey cyber range designed to prepare students for employers' real challenges daily. The cyber range has a critical difference: our educational solution is based on Keysight BreakingPoint, the gold standard application and security traffic generator used by our global enterprise and government agency customers.

With a full range of hands-on red and blue team exercises based on the Cyber Kill Chain model, students hone their defense strategies on customizable, realistic scenarios that are continuously updated by Keysight's Global Application and Threat Intelligence Team (ATI)—the same team that keeps our professional customers one step ahead of the bad guys.

Characteristics and Specifications

For the characteristics and specifications of the Keysight Cyber Training Simulator, refer to the Data Sheet at https://www.keysight.com/sg/en/assets/3122-1436/data-sheets/Keysight-Cyber-Training-Simulator-CY101KCTS.pdf.

Intended Use of the User's Guide

This User's Guide is intended for use by students, lecturers, and University Teaching Lab Managers as a guide for set up the Keysight Cyber Training Simulator application and its subsequent applications.

First-Time Setup

Before you use the Keysight Cyber Training Simulator application for the first time, take note of the following items:

- Ensure that your PC meets the software prerequisites listed below and that the instruments are set up on your bench.
- For security purposes, it is recommended to change the password of the Account Console. Go to Keycloak Administration Console for the instructions.
- By default, the **User registration** setting is set as **OFF**. This is the recommended setting to prevent other users from registering an account using the link. For more information, go to Add User.

Software Required

1. Google Chrome or Firefox web browser
2. Remote Agent (provided by Keysight personnel)
3. (Optional) VPN access to range of IPs

NOTE

Before you can use Keysight Cyber Training Simulator, you must set up the PathWave Lab Operations for Remote Learning application as described above and learn the features that you can access according to the roles assigned to your account.

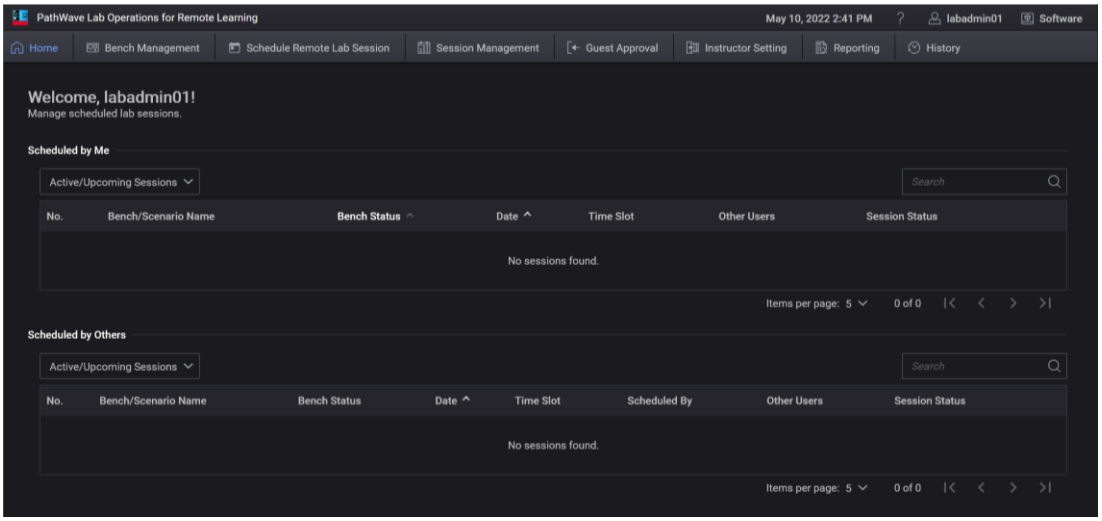
- To install the license(s) to use the platforms and application in Keysight Cyber Training Simulator, follow the instructions as described in License Installation and Activation.
- Administrators must link the PathWave Lab Operations for Remote Learning application to the university's LMS platform manually. Go to (Optional) Learning Tools Interoperability (LTI) Features for information to link Moodle or Blackboard platform. Lecturers must then log in from an existing course in LMS which you have mapped to PathWave Lab Operations for Remote Learning application.

  Once you have completed the setup, you may log in to PathWave Lab Operations for Remote Learning application via the LMS or from the link provided.

User Interface Overview

Home View

This view displays a summary of the lab benches scheduled and the lab sessions that you are invited to join.

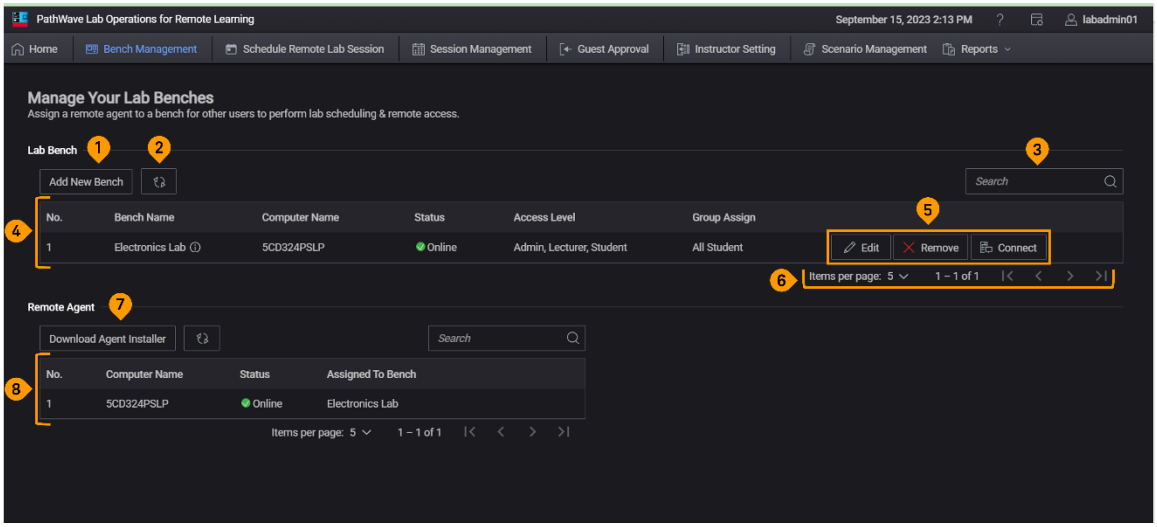


Subject to the roles assigned to your account, you may see the following tabs on your home page:

- Bench Management (accessible by Administrator and Lecturer access levels)
- Schedule Remote Lab Session (accessible by Administrator, Lecturer, and Student access levels)
- Session Management (accessible by Administrator access level only)
- Instructor Settings View (accessible by Lecturer access level only)
- Reporting and History View (information shown will differ subject to Student or Lecturer access levels)

Bench Management View

For this page, administrators can manage the bench or set up a new remote agent while those with Lecturer and Student access levels can only view and connect to the bench.



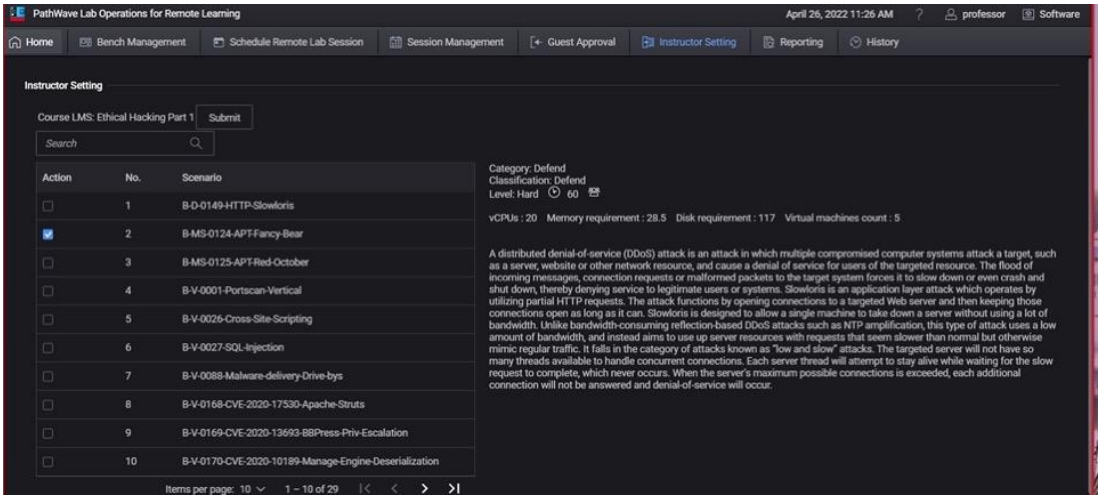
No.	Function	Description
1	Add New Bench	– Bench Name: Name the bench. – Bench Description: Describe the usage of this bench. – Bench Location: State the physical location of this bench. – Bench Instruments: Lists the instruments available to this bench. – Agent: Assign a Remote agent to this bench. – Access Level: Select the type of accounts allowed to use this bench.
2	Refresh button	Refresh the list of benches available or assigned.
3	Search bar	Enter the keywords here to filter the list of benches available.
4	List of Lab Bench	Click any of the header in the table to sort the list.
5	Lab Bench Controls	Manage the settings for the respective lab bench: – Edit: Modify the details of selected lab bench or change the assigned remote agent. The list will only show the unassigned agents that you can use (even it is offline). – Remove: Remove the bench from the list. This will also remove the remote agent assigned to the bench (when applicable). – Connect: Connect to the bench remotely and begin the remote lab session. A countdown timer will appear when it is 15 minutes before the scheduled session. You will not be able to connect to the bench when the status is 'Offline'.
6	View	Set the number of items to view in the table in each page.
7	Download Agent Installer	Download the Remote Agent installation package to add a new PC to the Keysight Cyber Training Simulator application server.
8	List of Remote Agents	Lists the remote agents available in the server for management purposes and display the status of each remote agent and assigned bench. To remove a remote agent from the list, you must first ensure that it is not assigned to any bench.

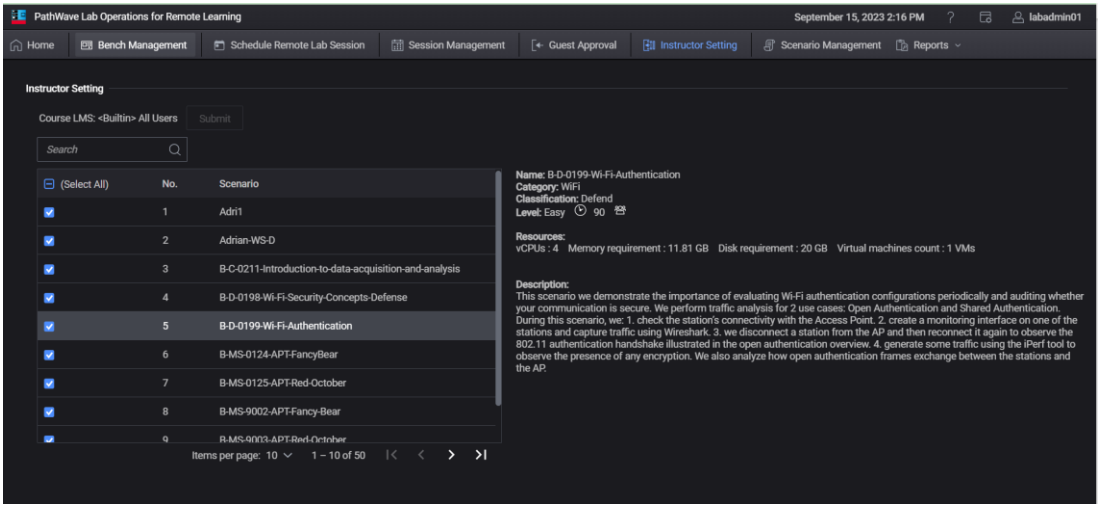
Instructor Settings View

NOTE The information in this page is retrieved from the course you have set up in Learning Management System (LMS) and linked to Keysight Cyber Training Simulator application. Go to (Optional) Learning Tools Interoperability (LTI) Features for more details.

In this view, lecturers will select the desired scenarios (as populated from the LMS) to map it to the course that the students will go through the lab and exercises during the scheduled session.

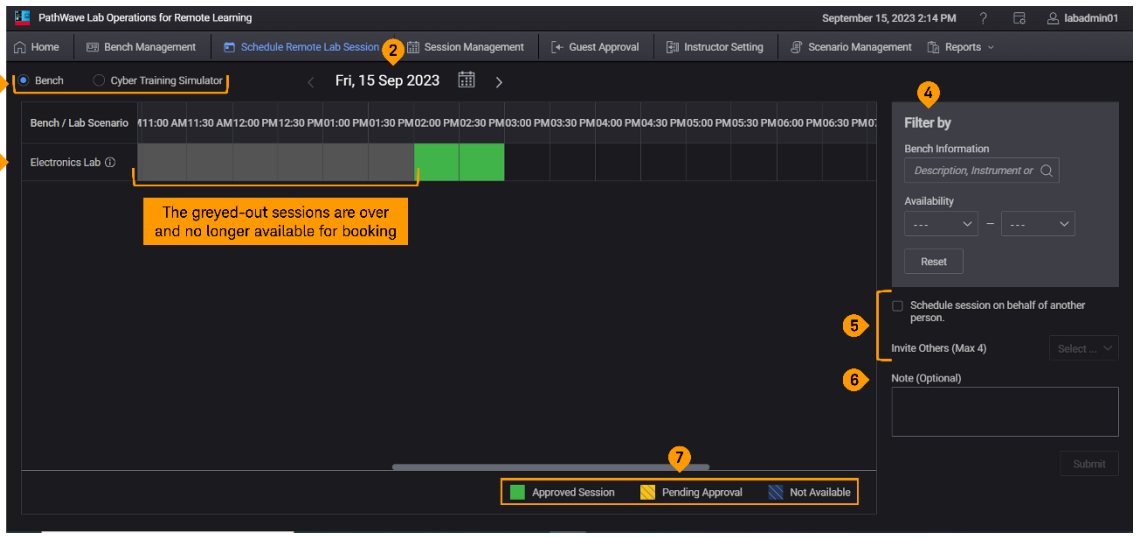
For more instructions, go to Map Scenario to LMS Course.





Schedule Remote Lab Session View

This page is accessible across all access levels.

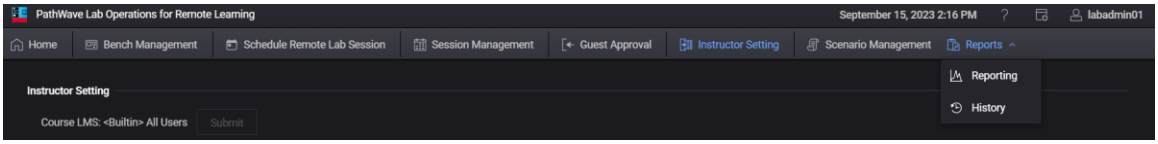


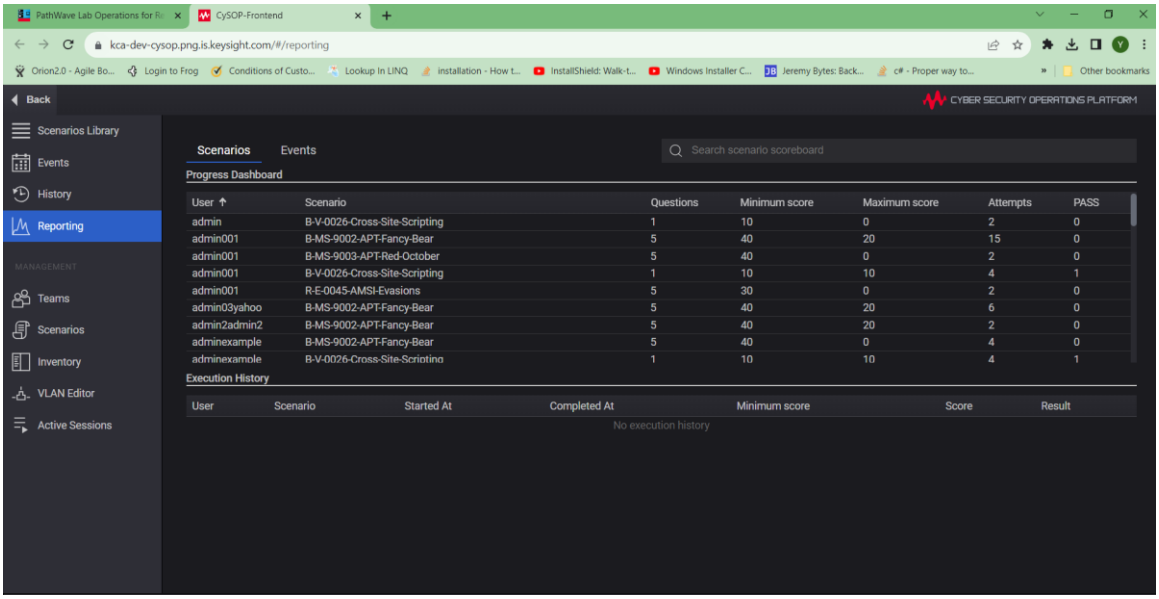
No.	Item	Description
1	Application	– Select Bench to use Keysight Cyber Training Simulator and schedule a lab session – Select Cyber Training Simulator to schedule a lab scenario.
2	Date	Set the desired date of your lab session. For the monthly view, click the Calendar icon.
3	Bench or Scenario	Subject to the application selected, the table will show a list of benches or scenarios available for the remote lab session.
4	Filter by (for PathWave Lab Operations for Remote Learning only)	Filter the benches according to the keywords or available time slots. Click Reset to clear the information.
5	Schedule or Invite (for PathWave Lab Operations for Remote Learning only)	There are two options to schedule a remote lab session: - Select 'Schedule on behalf of another person' check box to submit a request for booking. For this case, you will be able to invite up to five participants to access this test bench at the selected booking timeframe. - Use 'Invite Others' field to invite four other participants (maximum) in the same session. Note: You may only invite the participants with the same access level as you are. Those with the administrator roles can invite participants of all access roles.
6	Note (Optional)	You may enter the information of the session here.
7	Legend	The visual representation of the indicator on the chart when identifying the time slots available.

Reporting and History View

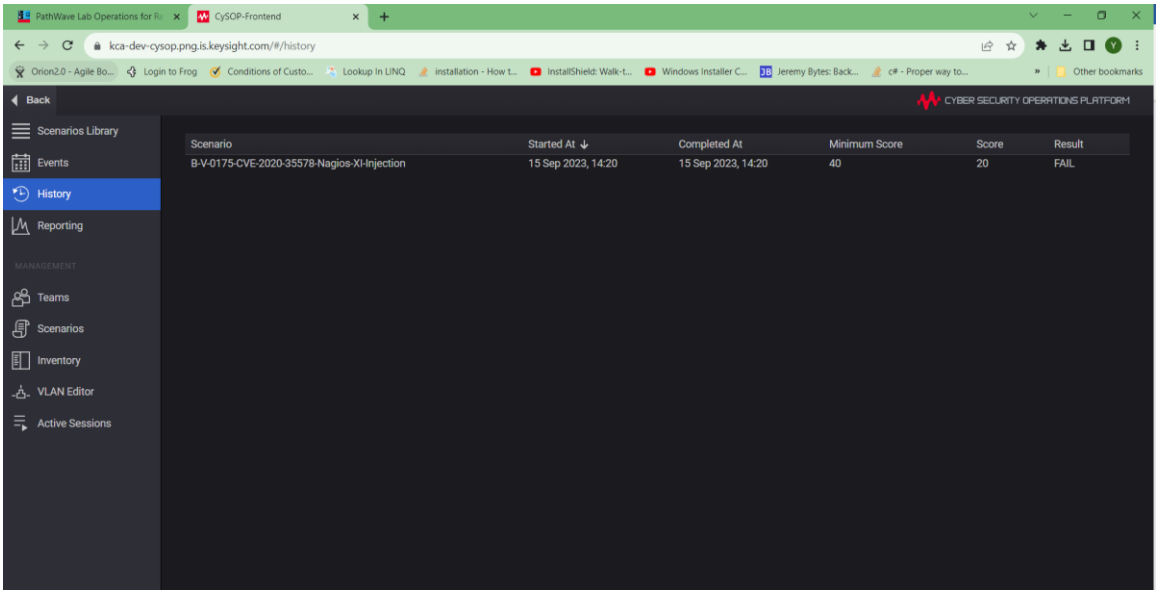
Subject to your access level, the information shown in these pages may differ.

- Lecturer: A list of virtual labs completed and quiz scores for each student.
- Student: A list of virtual labs completed.





The History tab lists the scenarios launched and the timestamps of each session.



User Menu

This section covers the commonly used functions that you will need to navigate around the PathWave Lab Operations for Remote Learning application.

The features that you can access in this software may vary depending on the roles assigned to your account. New accounts will be assigned with the Guest roles upon registration. To change the roles assigned, consult your lecturer or lab managers.

Here are the three access levels or roles that you can assign to the accounts:

Student

- Schedule Remote Lab Session (only invite other users with the Student role)
- View and Connect to Scheduled Sessions
- Connect to Test Bench (via scheduled session)

Lecturer

- Schedule Remote Lab Session (only invite other users with the Lecturer and Student role)
- View and Connect to Scheduled Sessions
- Connect to Test Bench (via scheduled session)

Administrator

Go to Management Menu for more information.

This section covers the commonly used functions that you will need to navigate around the Keysight Remote Laboratory application. First time users will need to go through the following sections.

NOTE

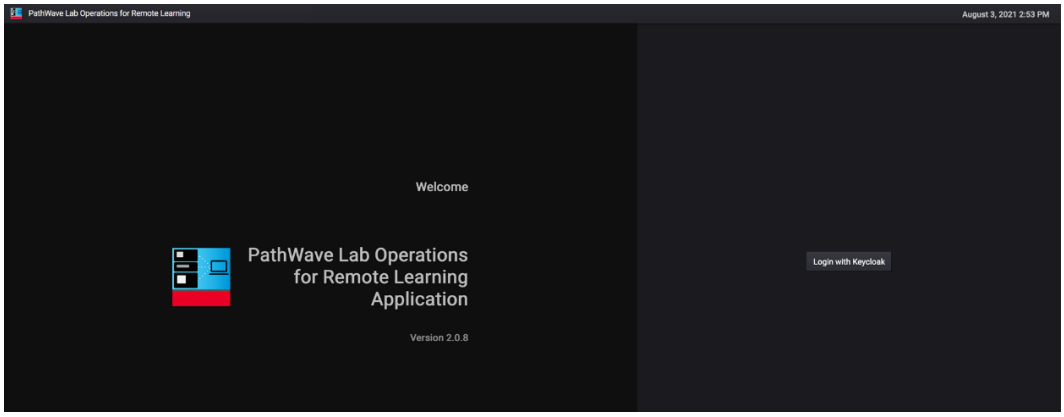
Before you begin, ensure that PC is connected to the internet.

By default, the **User registration** setting is set as **OFF**. This setting will only allow accounts with administrator roles to register new users and set the appropriate roles and access. To change this setting to ON, go to Add User.

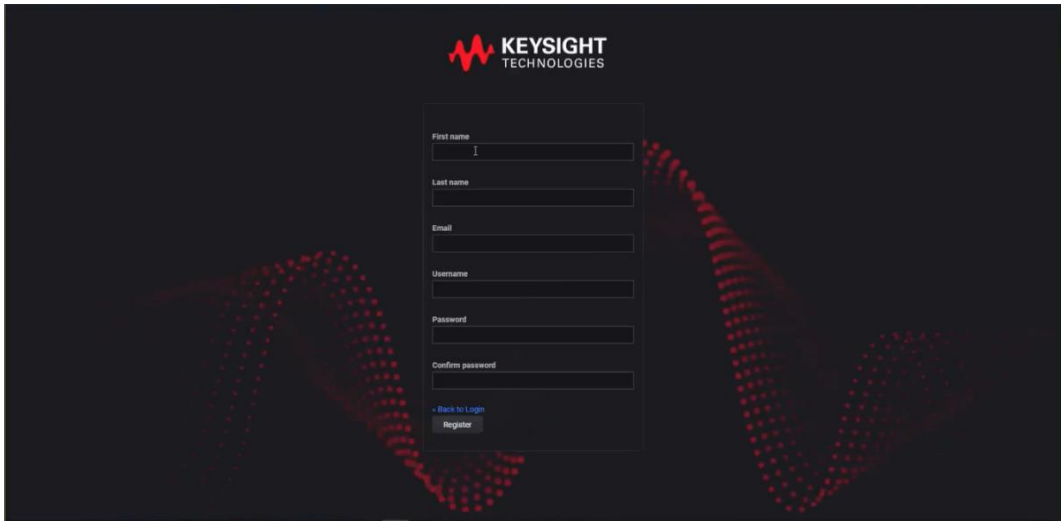
Registration and Login

New users will need to register and create a new account. Go to **Step 4** to log in with your existing account.

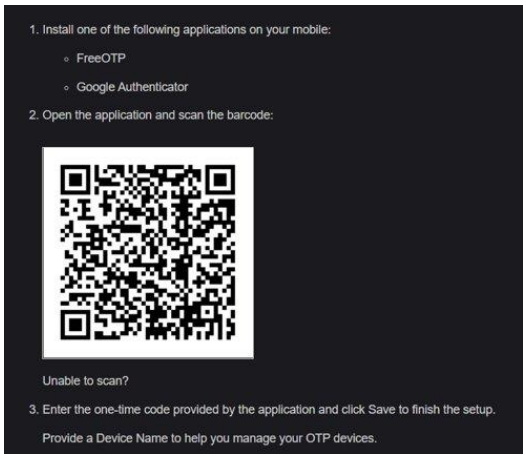
1 Launch your web browser and enter the link provided (subject to the hostname) in the address bar to launch the Keysight Remote Lab Application. First time users will need to click **Register** and create a new account.



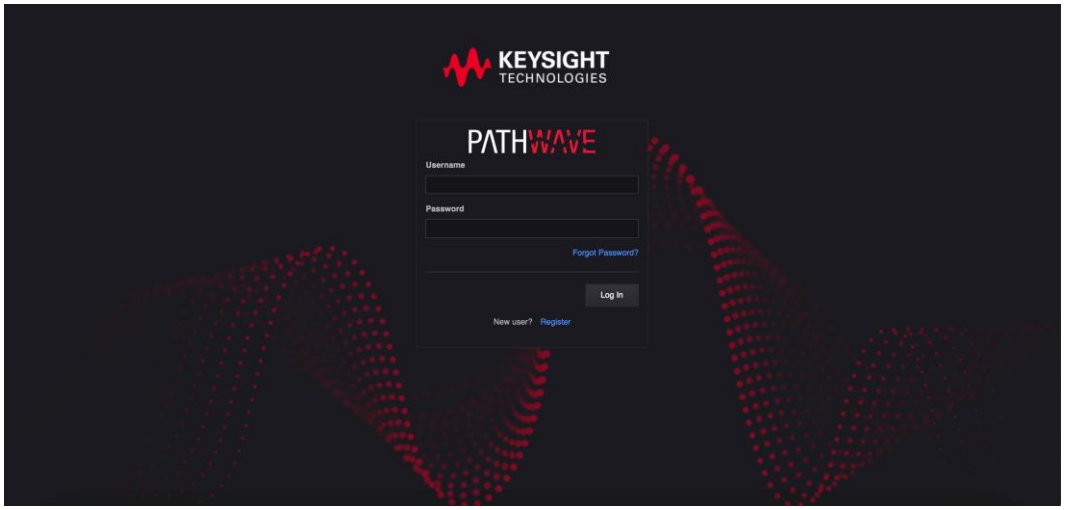
2 Enter the details to set up your account. By default, new accounts are assigned with the Guest role. Accounts with Guest role will not be able to log in until the administrator approves your registration.



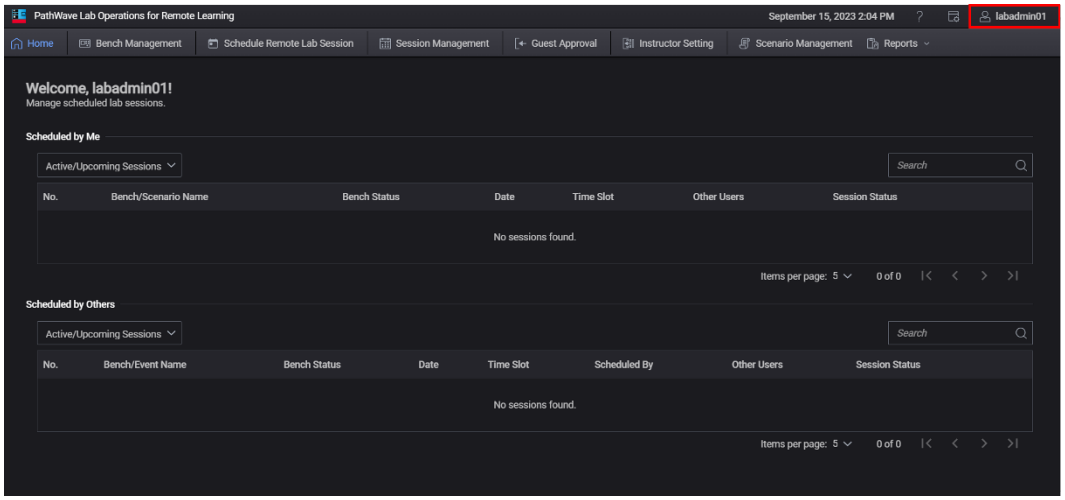
3 When prompted, set up a Mobile Authenticator to activate your account. It is recommended to set up either FreeOTP or Google Authenticator to secure your account with a one-time password.



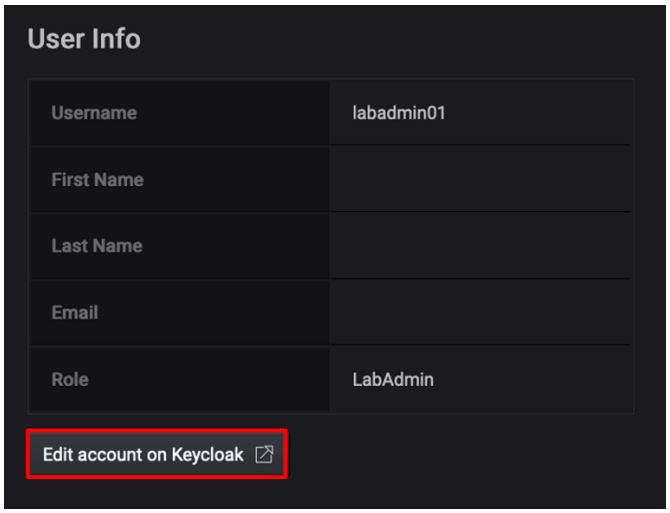
4 Log in with your details when see this page.



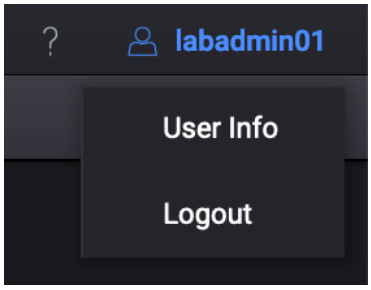
5 Once you are logged in, you should see the Home View. Click your username at the top-right corner to access information about your profile and account.



6 In User Info, click **Edit account on Keycloak** to modify your account details and password in a separate window.

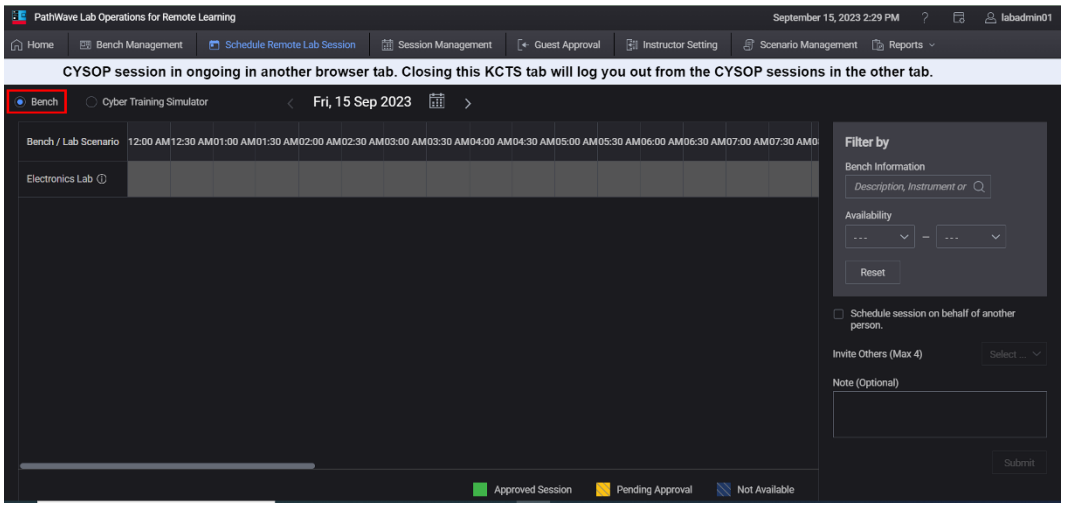


7 At the end of your session, click your account name (top-right corner) and click **Logout**.



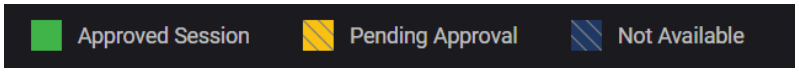
Schedule a Remote Lab Session

1 Click **Schedule Remote Lab Session** tab and select the **Bench** option. It will show the available test benches at 30-minute intervals according to the time of your PC.



2 Use the forward (›) and back (‹) button to switch between the dates or click the calendar icon to see the monthly view. You can schedule bookings up to 30 days.

3 Select one or more time slots for your session. Refer to the legend to identify the time slots available.



4 You can also enter keywords in the Filter by bar or enter the desired time slots to only show the available benches. For more information about the session, move your mouse over the info icon.

5 Select the **Schedule on behalf of another person** check box to submit a request for booking. If you are hosting the remote session, you can invite four other participants to join the lab session.

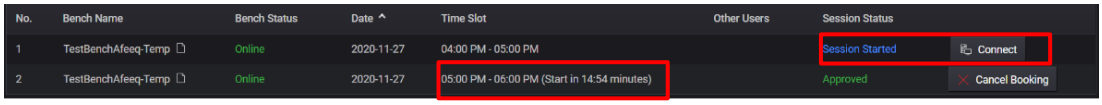
NOTE You can only schedule a session on behalf of another person if you have the Lecturer or Administrator roles assigned to your account.

---

6 Before you click **Submit**, you may add notes about this session which will be visible to the attendees and those with administrator access. The bookings submitted will then be approved by those with administrator roles.

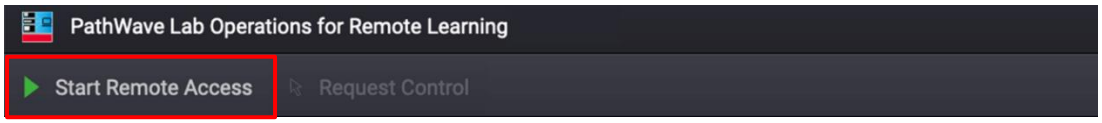
Connect to a Scheduled Session

1 When it is 15 minutes before the session, you will see a timer counting down to the scheduled session. The **Connect** button will only appear when it is time to start the scheduled session or when the host or participant has started the session.



NOTE When you click **Connect** on a Lab Bench that is currently online, you will not see a timer. You will return to the Bench Management page upon exit.

2 Follow the on-screen instructions. As the host, click the **Start Remote Access** button in the Remote Access page.



3 A successful connection to the remote agent will show the screen of PC. Click the **Request Control** button to take control the PC.

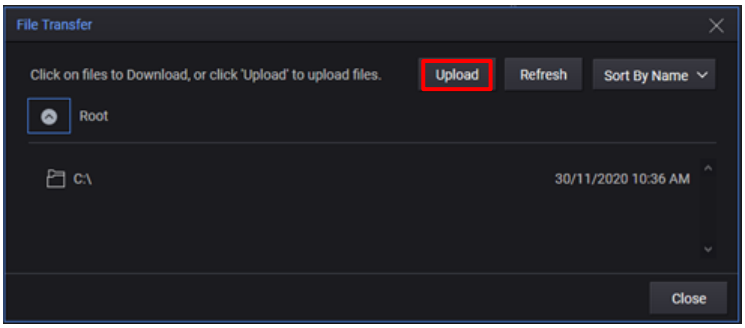
WARNING Performing the actions below during a scheduled session may cause the application to freeze and cease to respond:

- It is not recommended to stream videos on the remote bench PC.
- The application does not support the action of switching Windows user account.
- Participants must avoid uploading or downloading large files simultaneously during a session. The application can only support a maximum of two users performing these actions simultaneously.

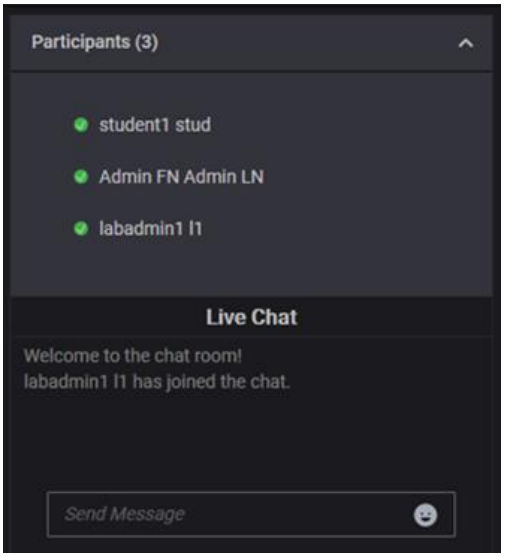
4 When you are currently controlling the remote desktop, this icon ( ) will appear next to your username. Other participants in the session can click the **Request Control** button and it will send a notification to the current presenter to Allow or Deny the request.

5 Here are a few other controls that you can access during the Remote Lab Session.

- Open File ( ): Click this button to upload or download any files. Click **Upload** and browse to the directory of the file. The speed to upload the files is subject to your network bandwidth.

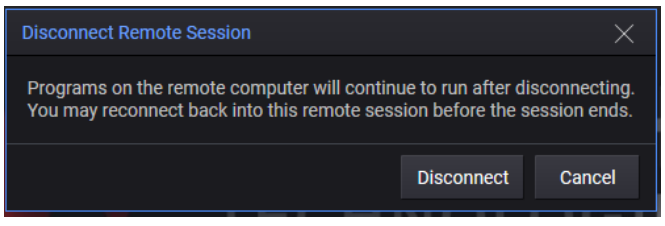


- Chat ( ): Click this button to expand the Chat panel and view the list of Participants. Use this panel to send messages to other participants in the session.



- Full Screen Mode ( ): Click this button to view in full screen. Press the **Esc** button to return to this window.

6 To disconnect from the Remote Lab Session, click **Stop Remote Access**.

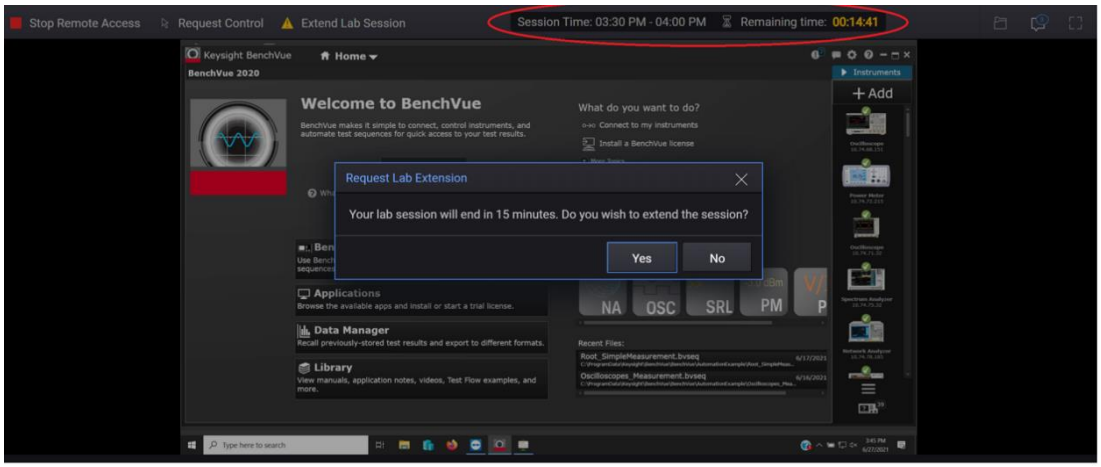


Click the **Close** (Close) button to exit the session and return to the **Bench Management** page.

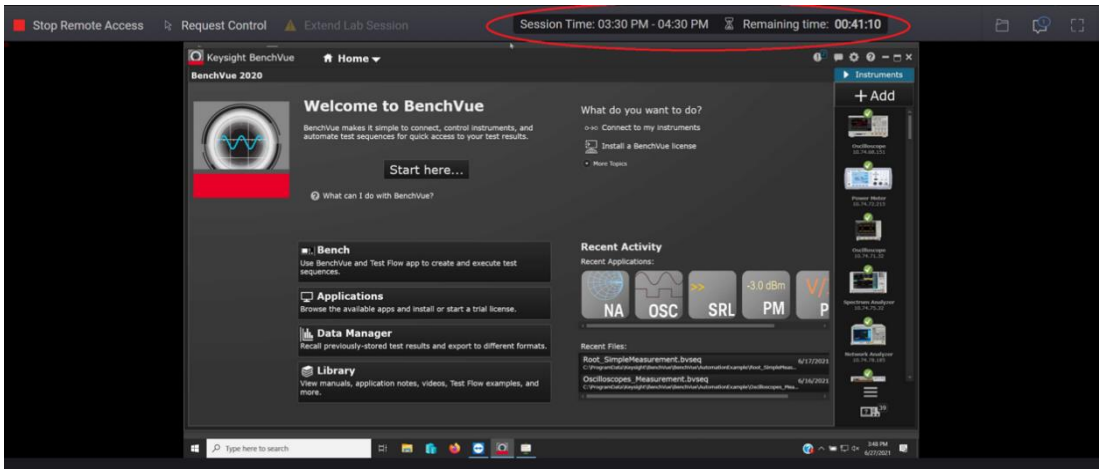
Extend a Scheduled Session

NOTE You can only extend the ongoing session for the next 30 minutes provided the next slot is available. Only the users who scheduled the session can see this prompt and extend the session accordingly.

1 When it is 15 minutes before the session ends, you will see a countdown timer and a prompt asking if you want to extend the ongoing session as shown below.



2 Click **Yes** will update the information and the timer as shown in the example below.



Manage Virtual Lab Sessions

NOTE

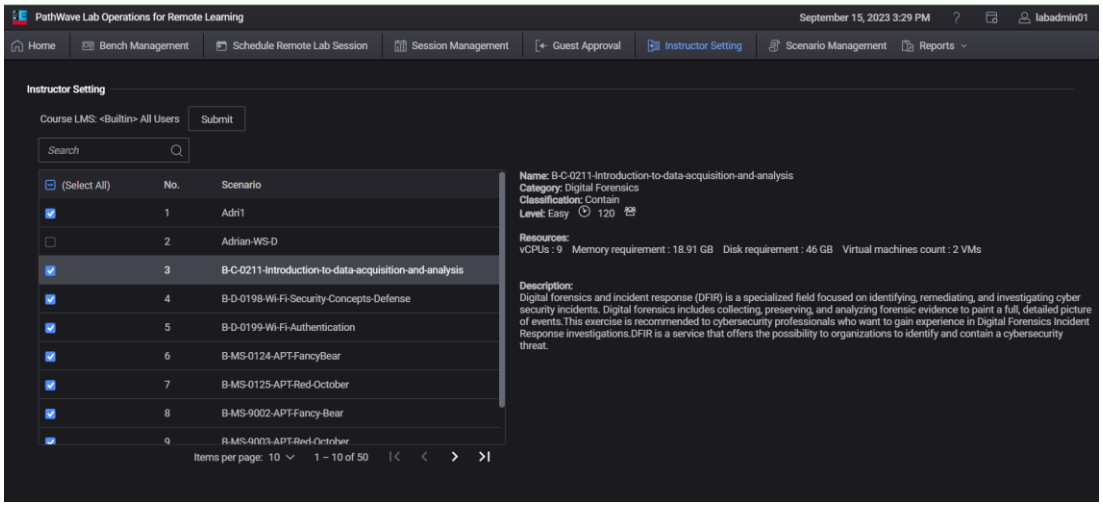
Administrator must manually link the PathWave Lab Operations for Remote Learning application to the university's LMS platform.

Go to (Optional) Learning Tools Interoperability (LTI) Features for information to link Moodle or Blackboard platform.

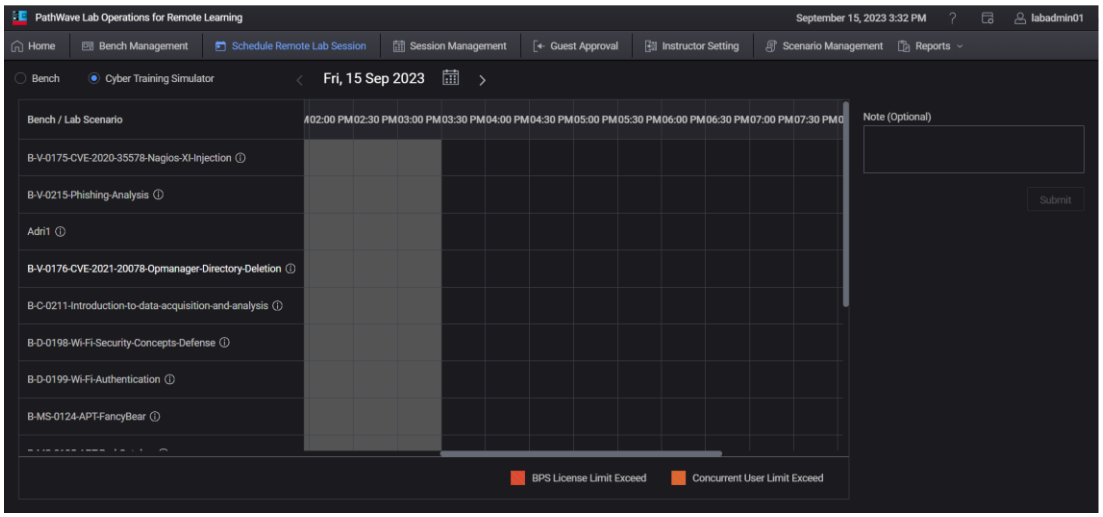
Once you have completed the setup, you have the option to log in to PathWave Lab Operations for Remote Learning application via the LMS or from the link provided.

Map Virtual Labs to LMS Course

1. From the Home view of the PathWave Lab Operations for Remote Learning application, click **Instructor Setting** tab.
2. Select the desired virtual lab(s) to map it to your course and click **Submit**.



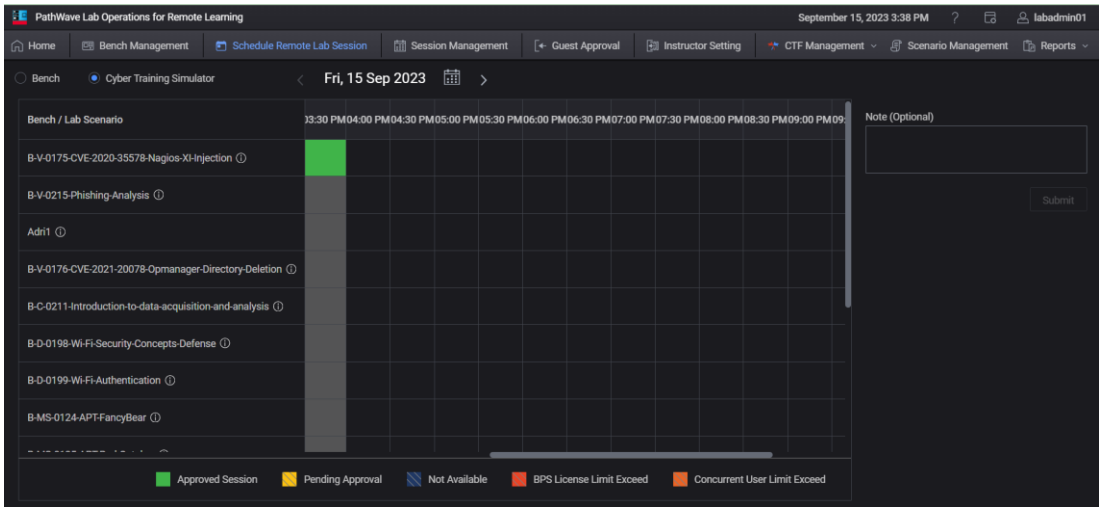
3. Successfully mapped virtual lab(s) will appear in the **Schedule Remote Lab Session** tab where students can use to schedule a remote session.



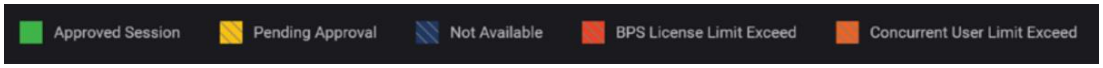
Schedule a Virtual Lab Session

1 From the Home view, click **Schedule Remote Lab Session** tab and select the **Cyber Training Simulator** option.

NOTE The Bench option is only applicable for those who are using the benches in the PathWave Lab Operations for Remote Learning application.



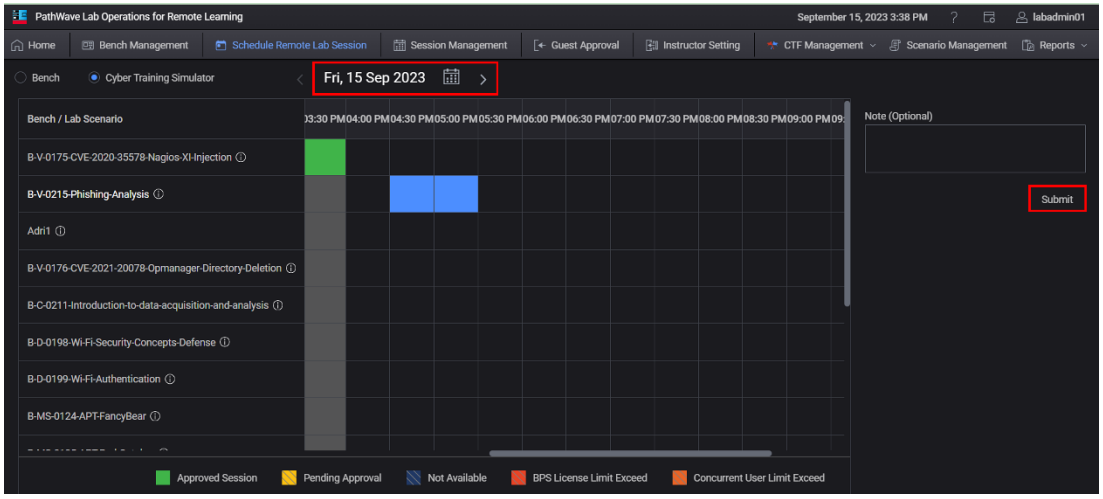
There are two additional indicators added to the legend:



a **BPS License Limit Exceed** is only applicable for virtual labs with the BreakingPoint (BPS) license tag.

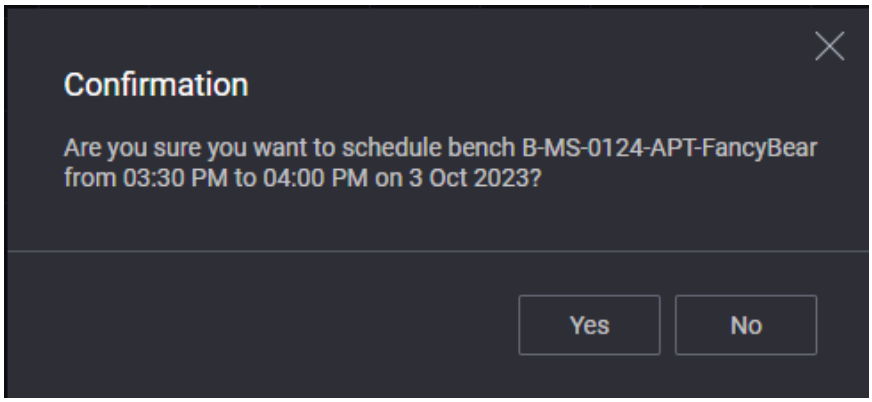
b **Concurrent User Limit Exceed** indicates that the time slot has achieved the maximum concurrent virtual lab scheduled (45 per design).

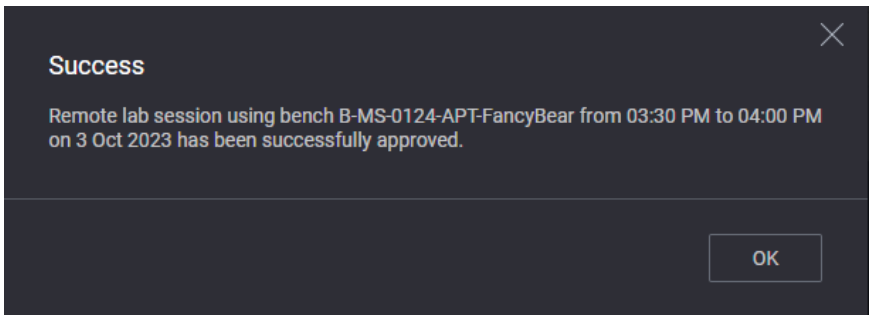
2 Modify the date and select the desired time slot to schedule a session. Click **Submit**.



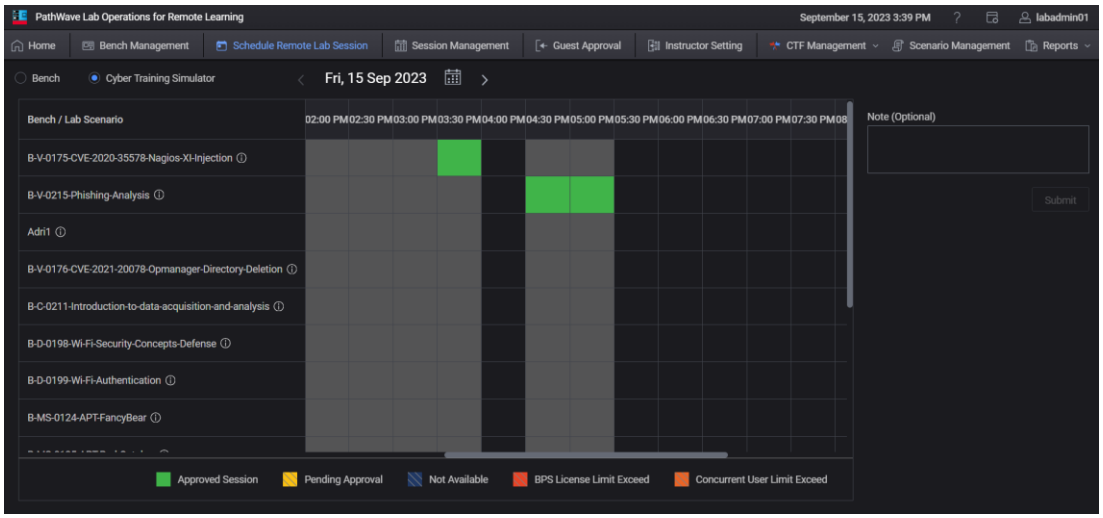
NOTE You can only schedule one virtual lab at any one time slot.

3 Click **Yes** to confirm the scheduled session and you will see the confirmation message as below. The system automatically approves any scheduled sessions.

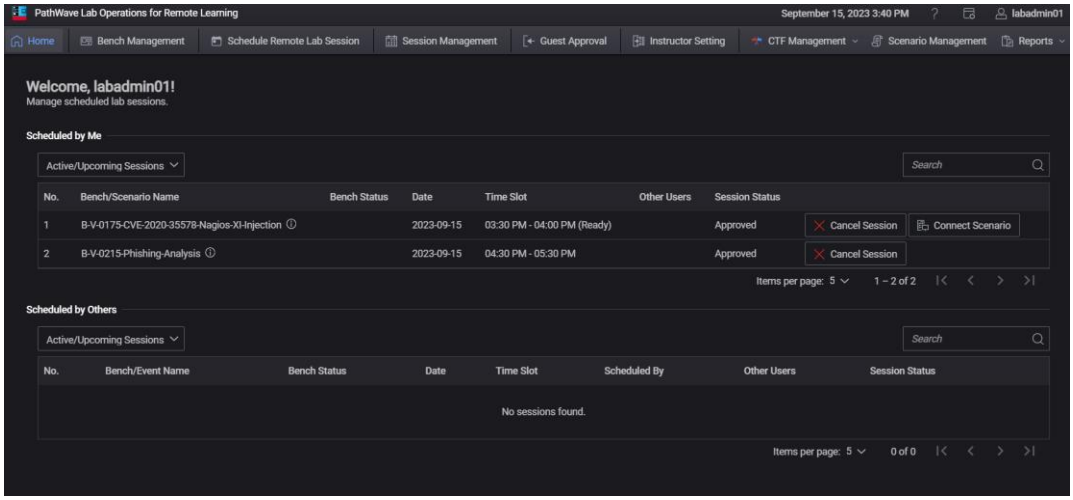




When you return to the Schedule Remote Lab Session view, you will notice that the selected slot is now marked as 'Approved Session'.

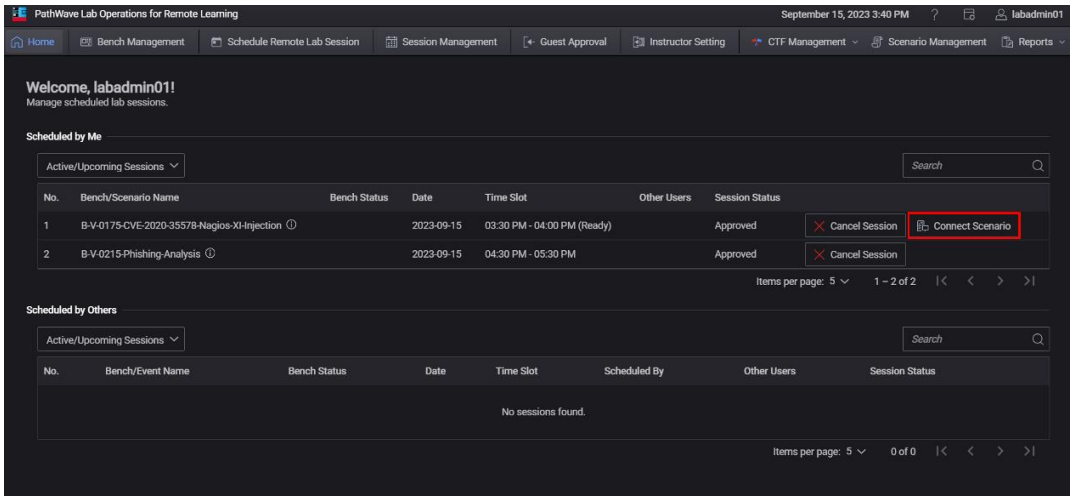


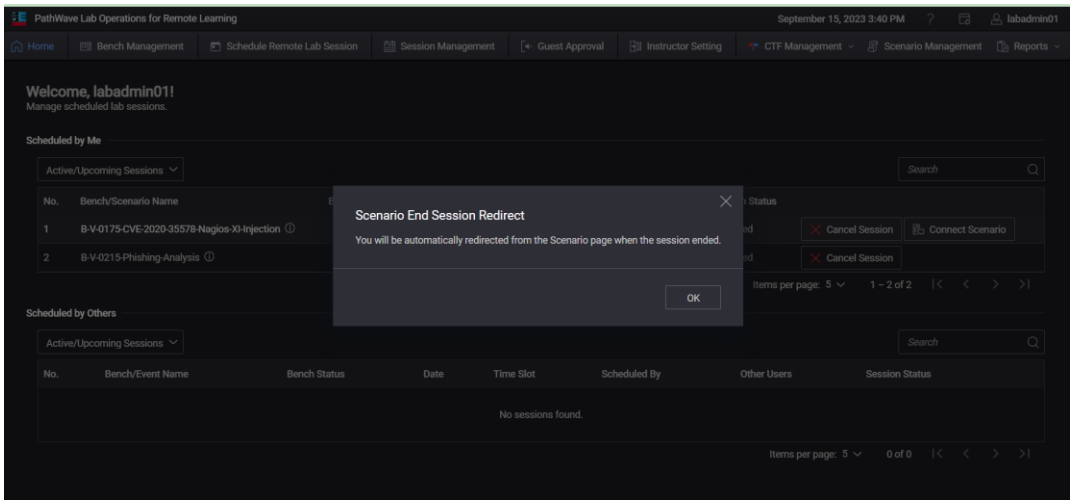
4 Back in home page, you will also see the information about the scheduled session.

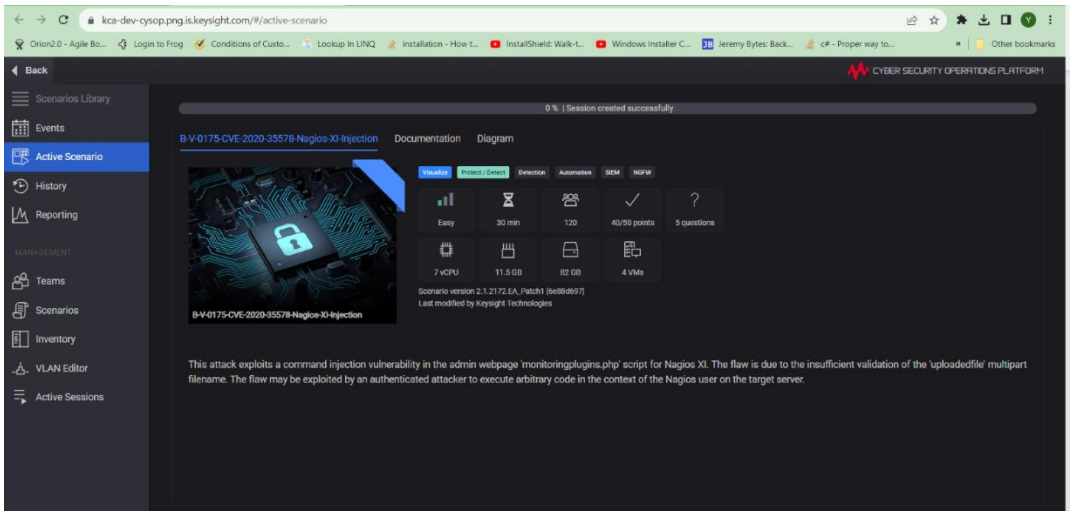


Connect to a Virtual Lab Session

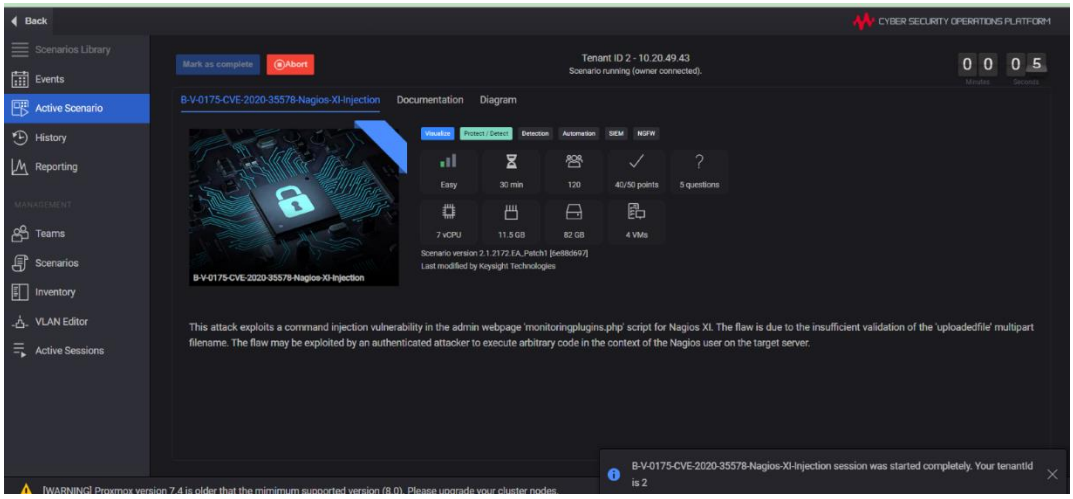
1 When it is time to start your virtual lab session, click **Connect Scenario** to begin. It will take some time for the application to create the virtual lab.



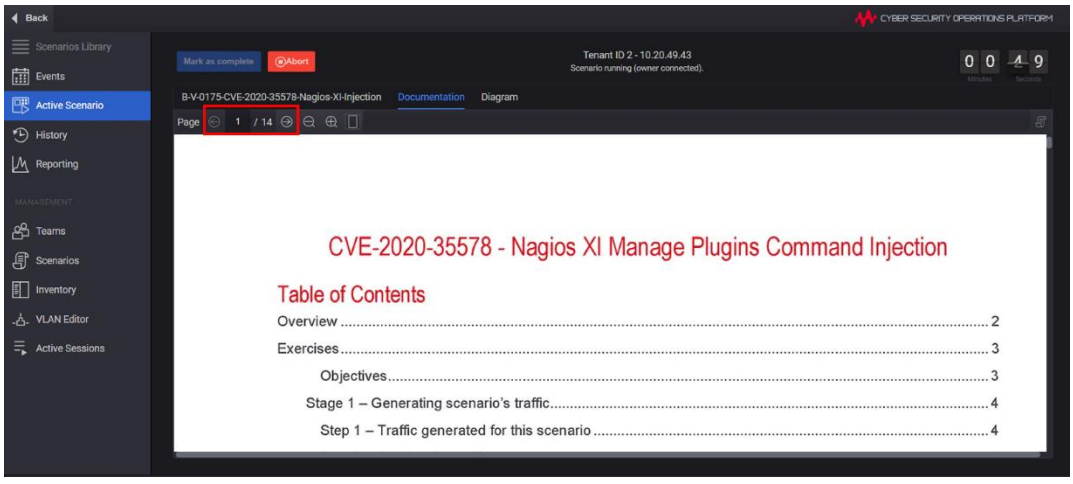




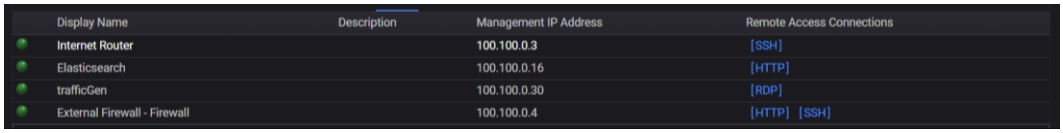
2 Once a session starts, you must complete it within the allocated time (as indicated in the timer).



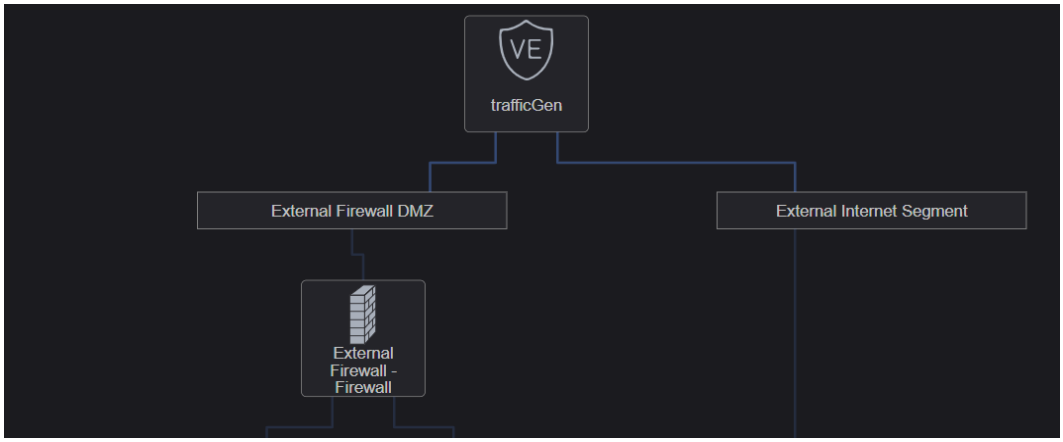
In the Documentation view, click **Next** or **Previous** buttons to navigate through the content.

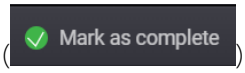


The Connection Table view will show a list of virtual machine(s) (with its network and login information) running in the virtual lab. Refer to the lab content to identify which device(s) require access in each virtual lab.

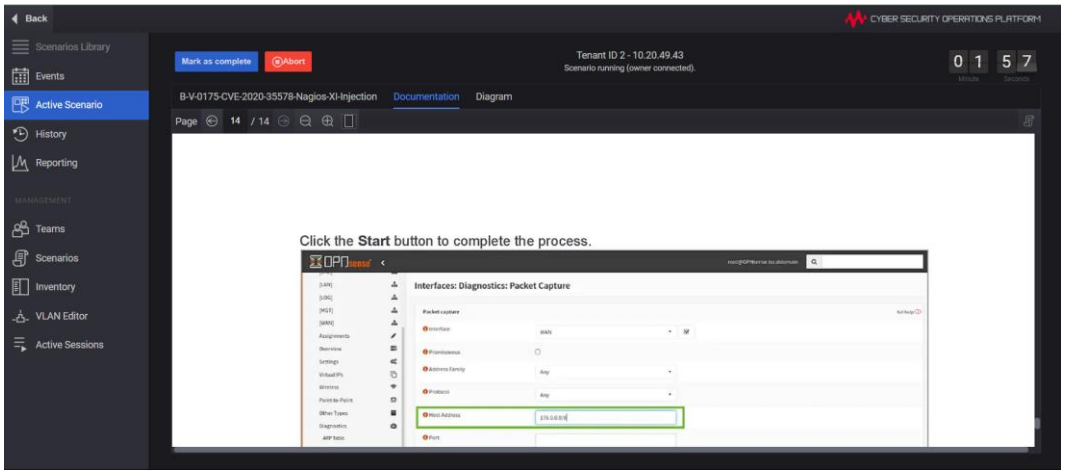


The Diagram view will display the network topology for the current virtual lab.

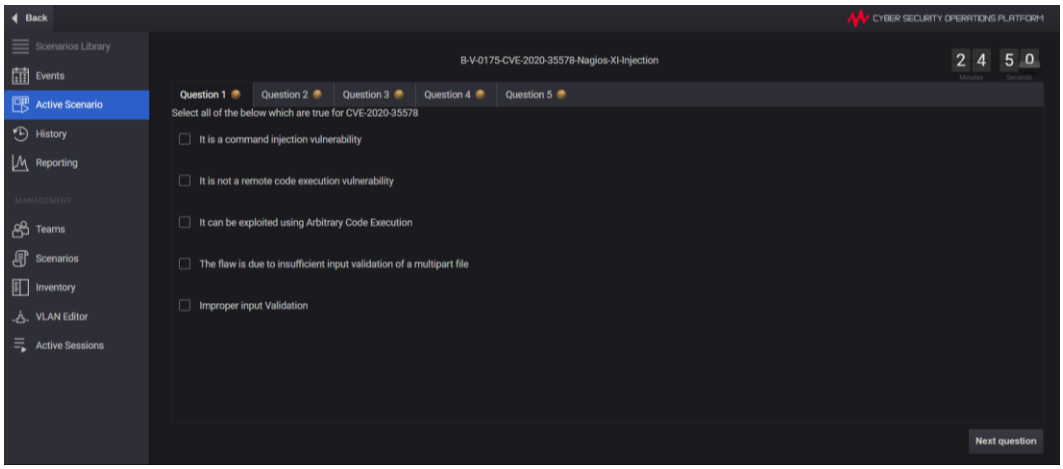


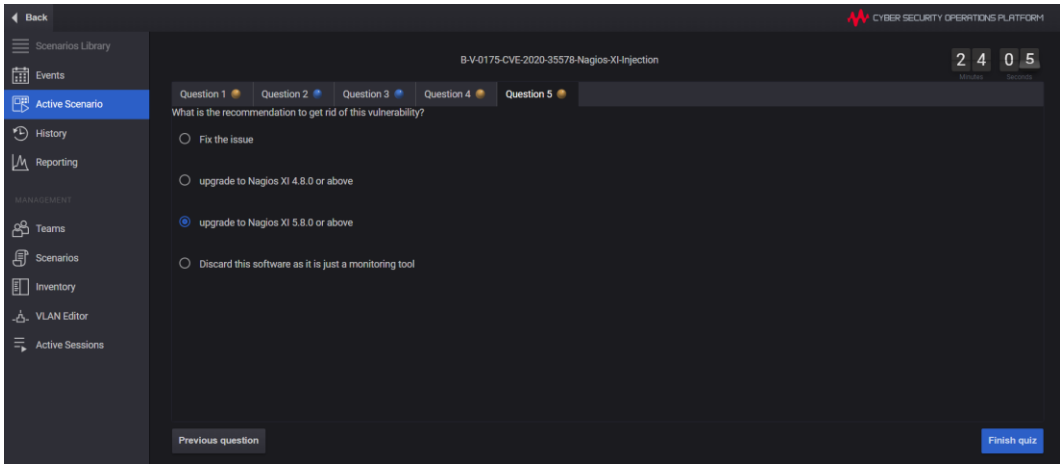
3 At the end of the document, click **Mark as complete to complete the lab** (

). Certain virtual labs come with a quiz which students must complete to test their knowledge.

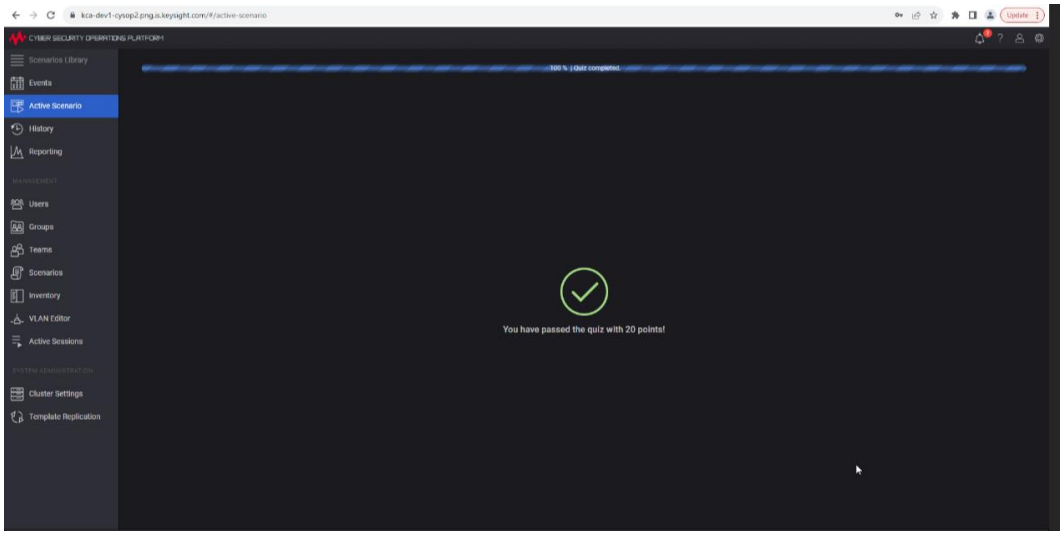


4 An example of the quiz is shown below. Students must answer the question accordingly and click **Submit Answer** to proceed to the next question.

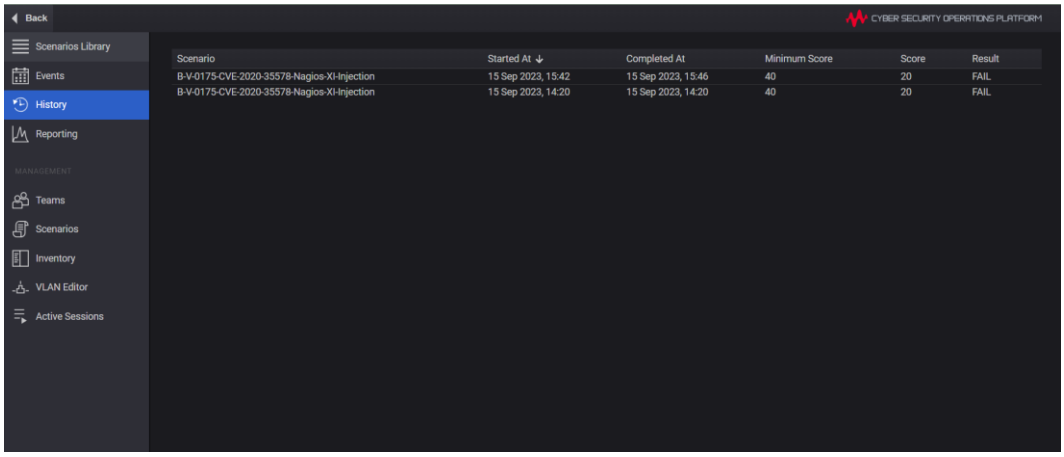




5 Once you have completed the quiz, the score will appear at the top of the page.



6 You can view the data for the scenarios in the History tab.



7 Close the tab to return to the main page of Keysight Cyber Training Simulator system.

Management Menu

This section covers the additional functions available for those with administrator roles to manage users, benches, and sessions scheduled in the Keysight PathWave Lab Operations for Remote Learning application.

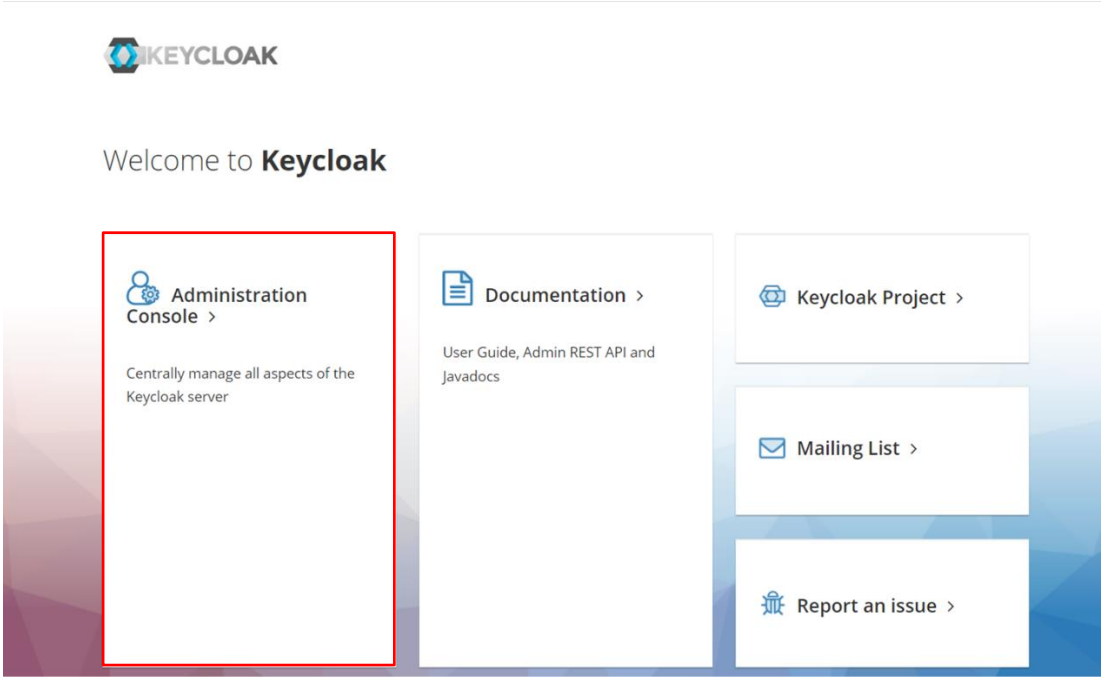
Keycloak Administration Console

To access the Keycloak Administration Console, you will need to use the default credentials as below:

- Username: admin
- Password: K3yCloak@**Order Number** (you may contact Keysight support to retrieve your Order Number)

It is recommended to change the password before you begin to use the application.

1 On a web browser, copy the link provided by Keysight Technologies (in the URL Notification Sheet) and add port **":8443"** at the end of the link. For example, the link will be https://dev.realremotelab.keysight.com:8443/. When you see the page below, click **Administration Console** and log in with details above.



2 Go to the **development** realm as shown below.

3 Go to **Users** on the left panel and click **View All Users**. For the account “admin”, click **Edit**.

4 Go to the **Credentials** tab and under **Manage Password**, enter a new secure password and disable **Temporary** option. Click **Reset Password**.

Once you have access to the development realm, you can perform the following tasks:

- **Configure Roles**

  This section describes the steps to create or configure the types of roles that you could later assign to the accounts.

- **Add User**

  This is an optional step provided you have the User registration setting as Off (default). Follow the step-by-step instructions in this section to manually add users.

- **Manage User**

  Perform the steps in this section to assign the types of roles to the registered accounts.

- **Email Settings**

  Perform the steps in this section to turn on the ‘Forgot Password’ feature.

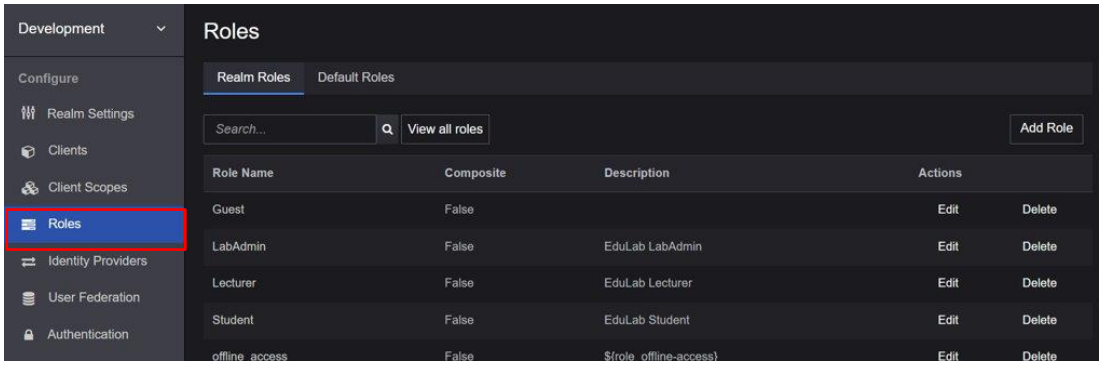
- **Set Up Single Sign-On (SSO)**

  This is an optional step to set up the social sign in for your application.

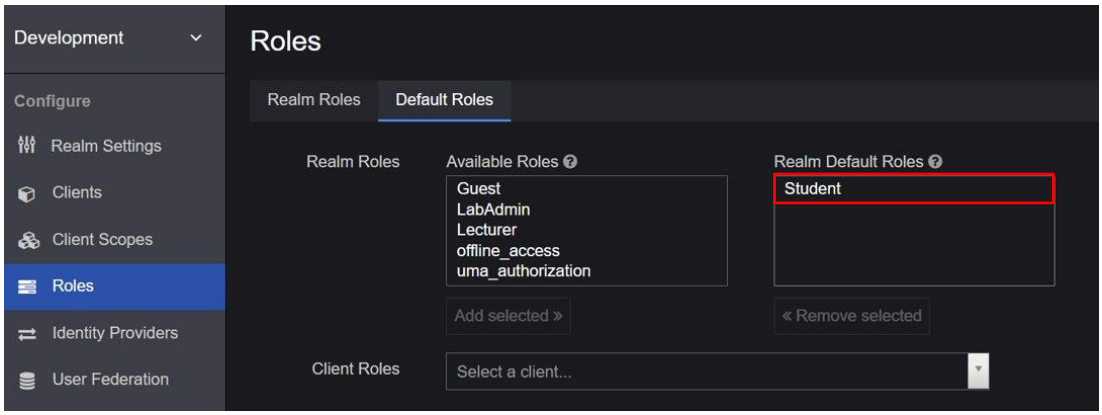
Configure Roles

This section describes the steps to set and assign the roles to an account. The types of roles assigned will determine the access level to the application. With the administrator role, you can set the default role to assign to new accounts and assign specific roles to each account.

1 Go to the **Roles > Realm Roles** to view the type of roles available. These are the roles that you can assign to an account.

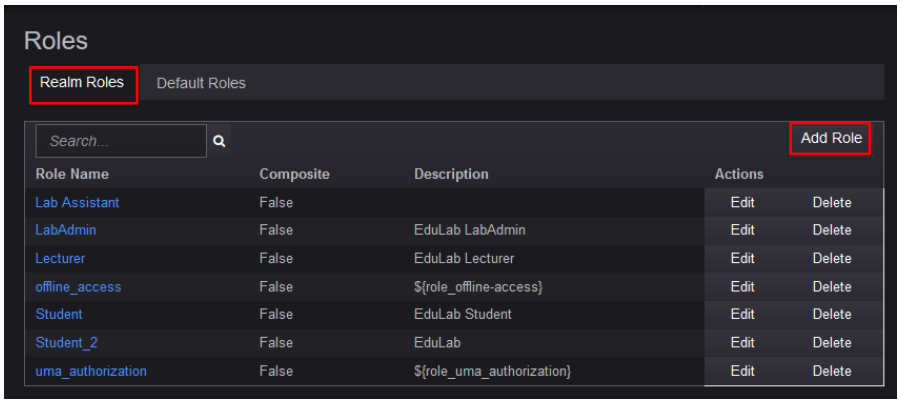


2 Go to the **Default Roles** tab to view or modify the default roles assigned to new accounts. By default, new accounts are assigned with Guest role during registration.

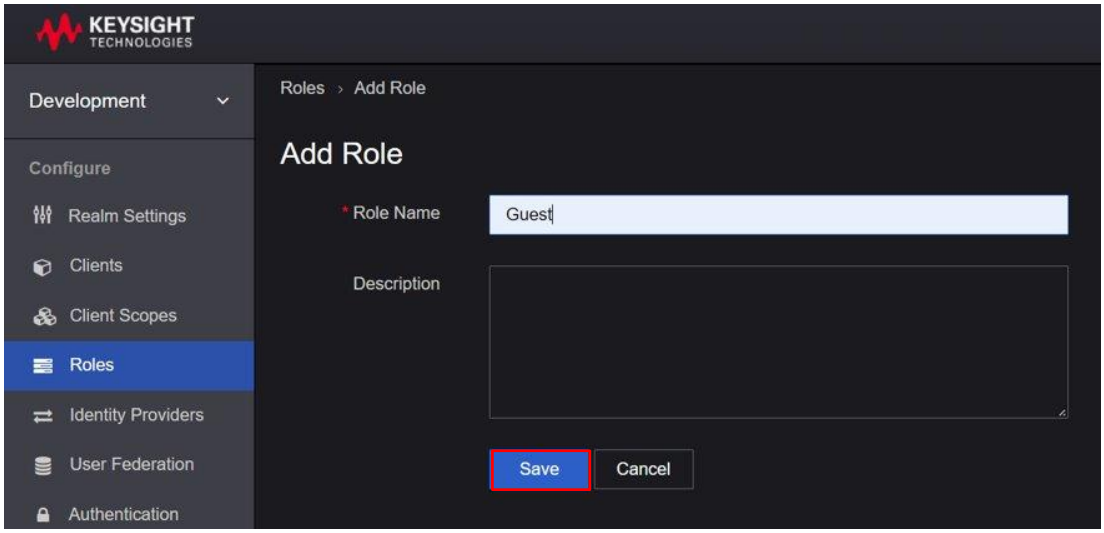


NOTE You can only add or remove one role at a time. To change the default role, you must first select the Guest role and click **Remove Selected** button. Then, select the desired role and click **Add Selected** to set it as the Realm Default Role.

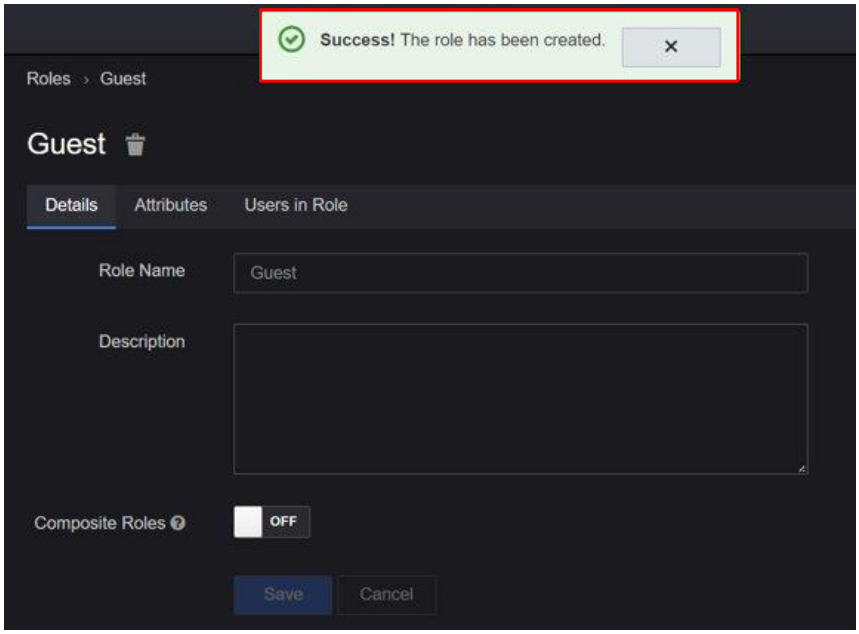
3 To add a new role, return to **Realm Roles** tab and click the **Add Role** button.



4 Enter the name and click the **Save** button. The example below will create a Guest role.



5 Successful creation of the role will prompt the following message. You should now see the new role listed in the Realm Roles tab.

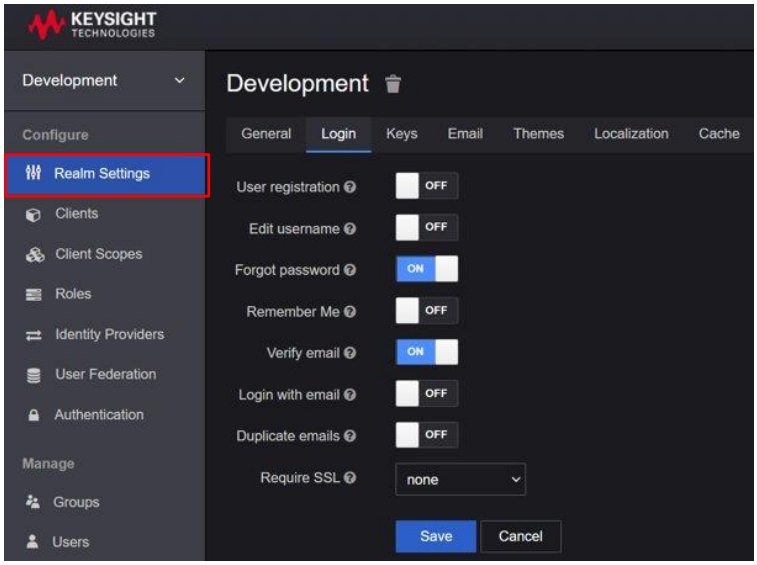


Add User

NOTE

By default, the **User registration** setting is set as **OFF**. This is the recommended setting to prevent other users from registering an account using the link to the application.

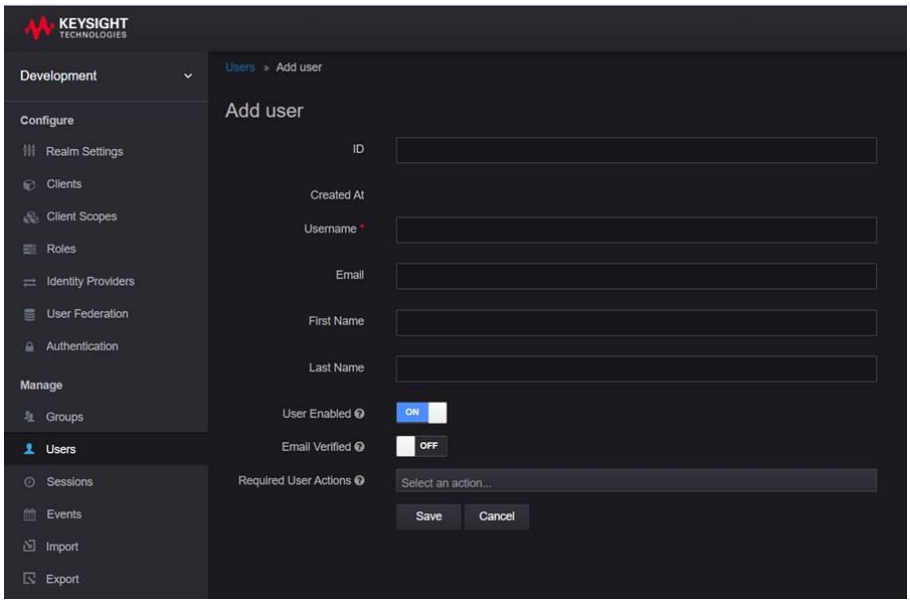
Go to **Realm settings > Login** to view this setting.



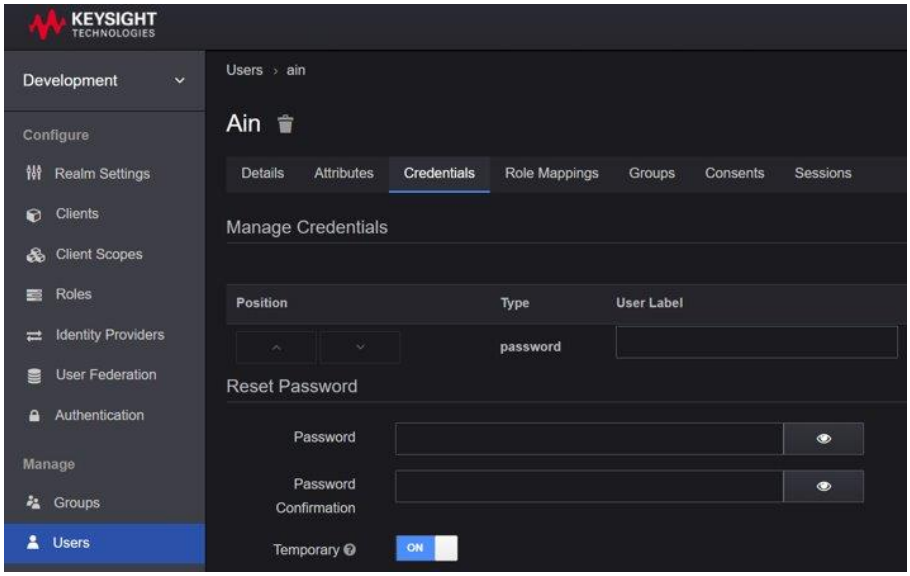
- When the User registration setting is set as **OFF**, only accounts with administrator roles assigned will be able to register new users and set the appropriate roles and access.
- When the User Registration is set to **ON**, any users with the link to the application will be able to register on their own with the default Guest role.

---

1 From the side panel, click **Users** to view the **Add user** page as shown below. At minimum, you will need to enter the desired Username. Click **Save** when you have completed the form.



2 You will be redirected to the **Credentials** tab where you will need to perform the following steps:



a In the Manage Password section, enter the desired password as shown above.

b Enable the **Temporary** option to create a temporary password.

NOTE When the **Temporary** option is enabled, users are required to change the password when they first log in to the application. You may turn off the **Temporary** option if you prefer to create a permanent password for the user.

c In the Credential Reset section, select the appropriate Reset Actions from the drop-down list. The recommended options are:

i Verify Email: This option will send an email to the user to verify their email address.

ii Update Password: You will be prompted to enter a new password when you first log in to the application.

iii Expires in: This is the duration set before the link expires. You will need to request for another link to verify your account.

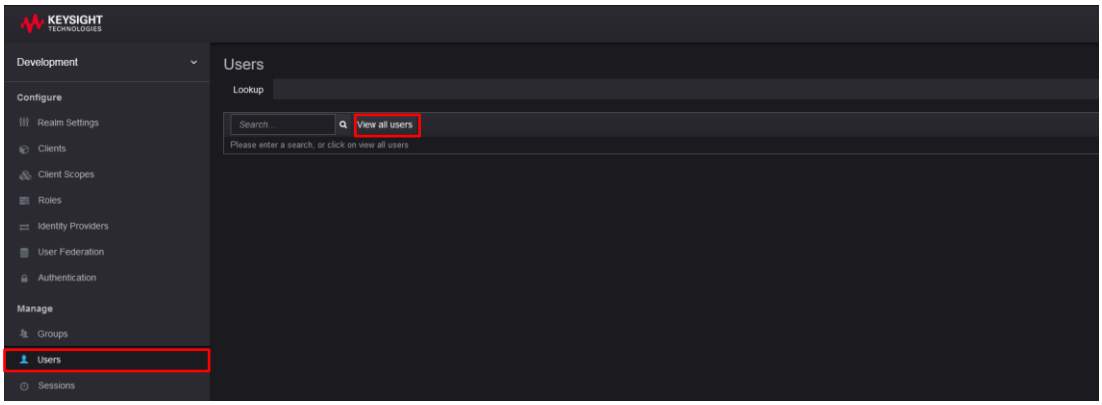
3 Click **Change Password** to update the password to the newly created account. Click **Reset Password** to activate the new password.

4 Click **Send email** to send out the email as per the settings above. When the user has verified the account, the Verified switch will change to 'ON'.

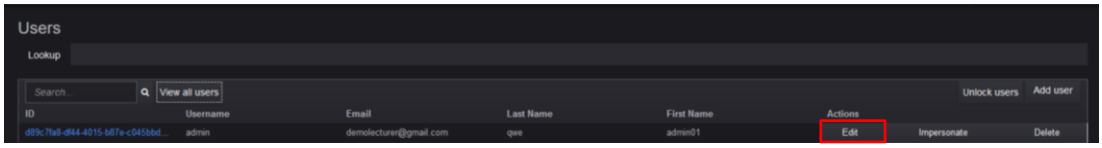
Manage User

Perform the following steps to assign the types of roles to the registered accounts.

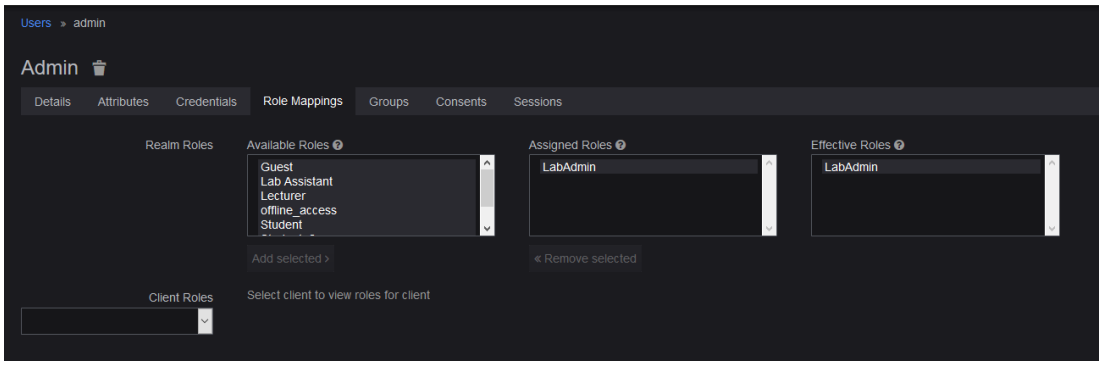
1 To modify the assigned roles for an account, go to **Manage > Users** and click **View all users**.



2 You should now see a list of users and their registered accounts. Click **Edit** in the Action column.



3 Go to the **Role Mappings** tab to view the role assigned. Note that you must first remove the assigned role (if any) before you can assign a new role to an account. The changes will take effective immediately.



Email Settings

NOTE In order to turn on the 'Forgot Password' feature, you will need to complete the Email Settings. Go to https://wjw465150.gitbooks.io/keycloak-documentation/content/server_admin/topics/realms/email.html for instructions on how to enable Email Settings in Keycloak.

Keycloak sends emails to users to verify their email address, when they forget their passwords, or when an administrator needs to receive notifications about a server event. To enable Keycloak to send emails, you need to provide Keycloak with your SMTP server settings. This is configured per realm. Go to the Realm Settings left menu item and click the Email tab.

Set Up Single Sign-On (SSO)

An identity provider is usually based on a specific protocol that is used to authenticate and communicate authentication and authorization information to their users. It can be a social provider or cloud-based identity service that you want to integrate with PathWave Lab Operations for Remote Learning Solution.

Once you have set up an identity provider, you may sign in to the PathWave Lab Operations for Remote Learning Solution application using any of the social provider such as Facebook, Google or Twitter.

Refer to the https://www.keycloak.org/docs/latest/server_admin/#_identity_broker for specific instructions to set up the Identity Brokering.

Here are a few examples:

- OpenID Connect v1.0 Identity Providers.

  OpenID Connect (OIDC) is an authentication protocol that is an extension of OAuth 2.0. While OAuth 2.0 is only a framework for building authorization protocols and is mainly incomplete, OIDC is a full-fledged authentication and authorization protocol.

  Go to https://www.keycloak.org/docs/latest/server_admin/#_identity_broker_oidc

- SAML v2.0 Identity Providers

  Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers.

  Go to https://www.keycloak.org/docs/latest/server_admin/#saml-v2-0-identity-providers

NOTE The authentication and authorization process uses Keycloak solution which is designed following standard security protocols to provide dynamic single sign-on solution. University IT can configure PathWave Lab Operations for Remote Learning Solution to access the university's active directory. This addresses security concerns, helps eliminate tedious registration process and streamlines the authentication and authorization process.

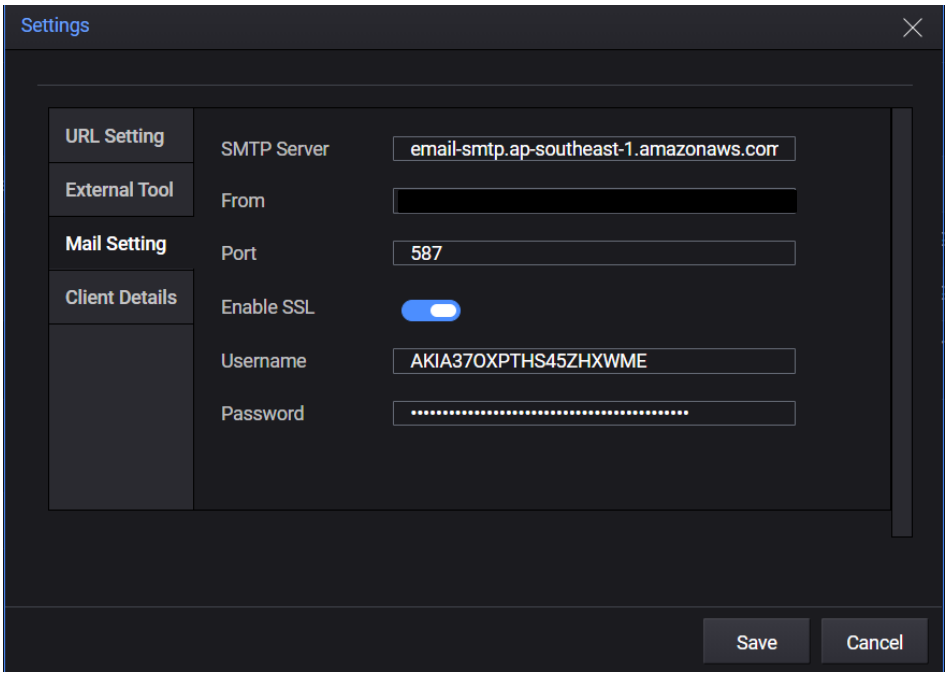
Keycloak's documentation: https://www.keycloak.org/docs/latest/server_admin/

Set Up Email Settings

This feature will send a confirmation email to the users to inform them of the status of the sessions in PathWave Lab Operations for Remote Learning Solution. The setup will depend on the SMTP server setup in the university.

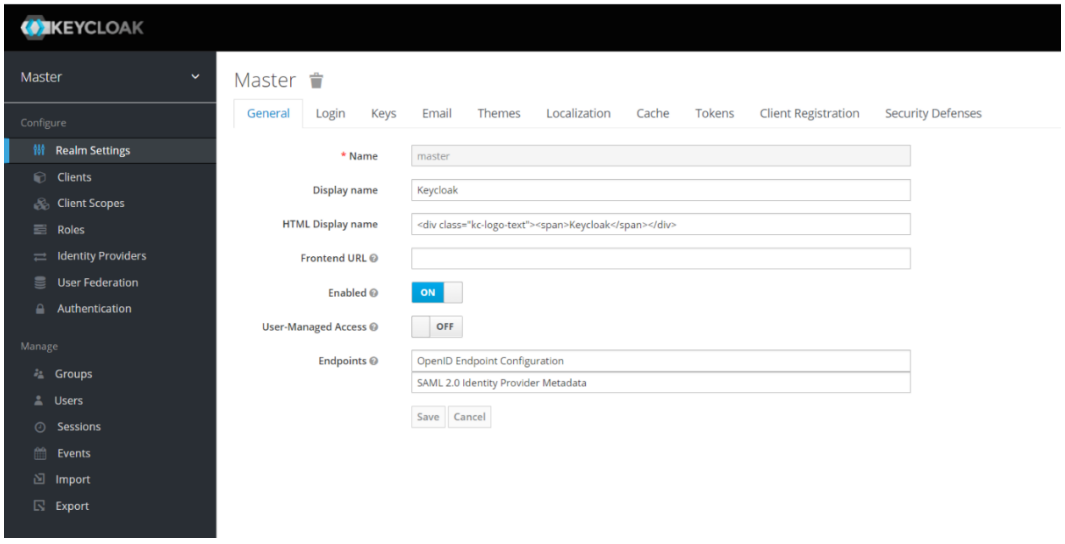
Mail Settings

Enter the information regarding your server.

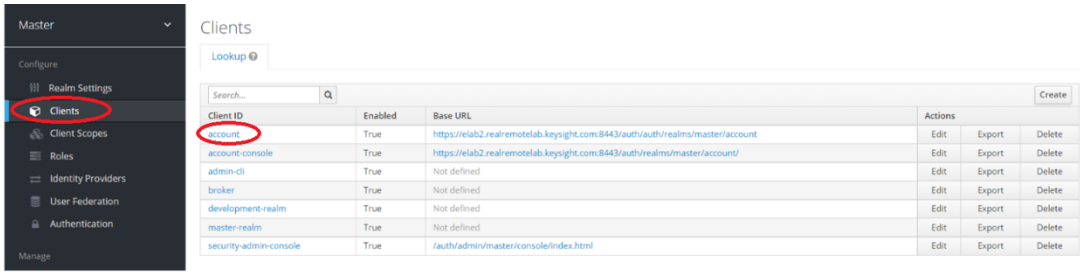


Client Details

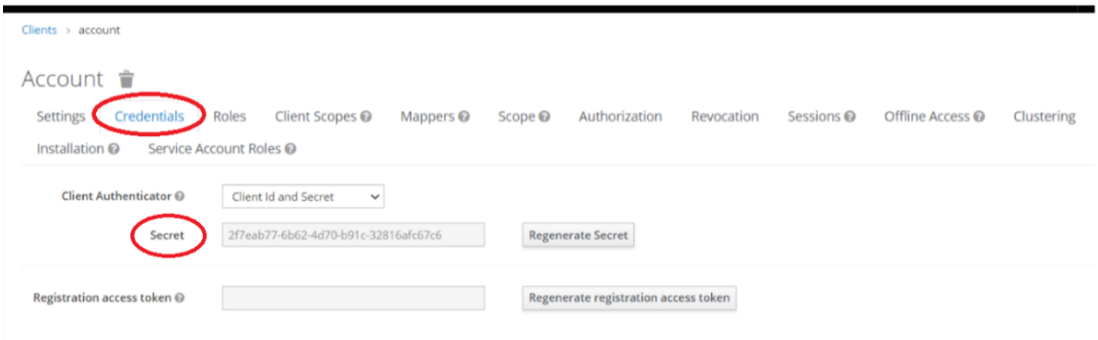
1 Go to **Realm > Master Realm**.



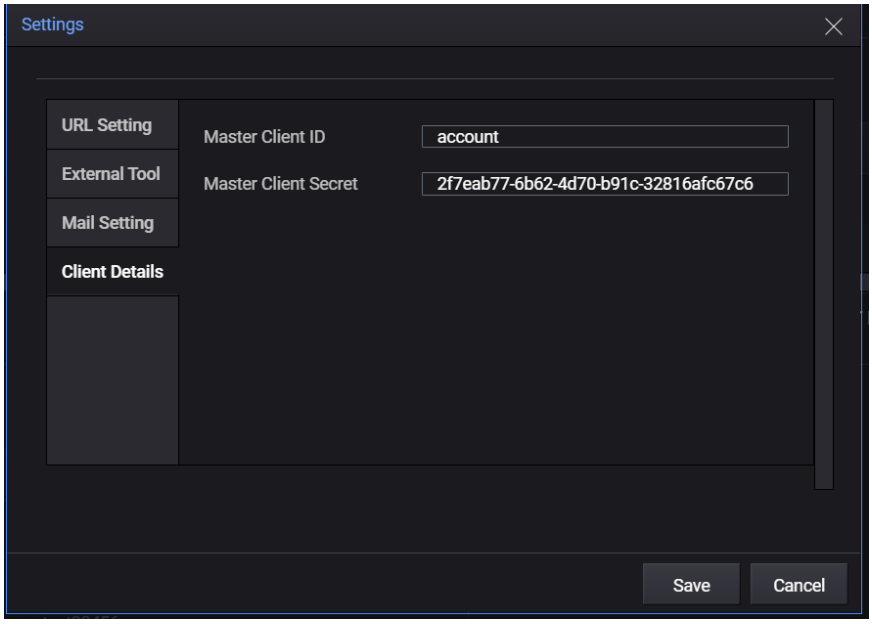
2 In the Clients tab, select **account**.



3 Click the **Credentials** tab and copy the information in the Secret field.

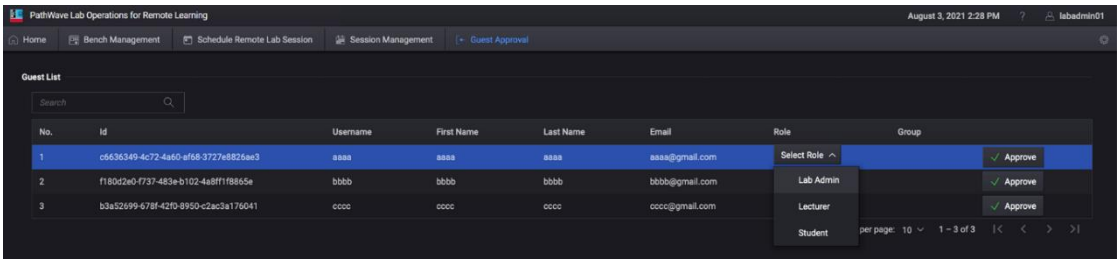


4 Return to the PathWave Lab Operations for Remote Learning Solution and paste the information under the **Client Details > Master Client Secret** field.

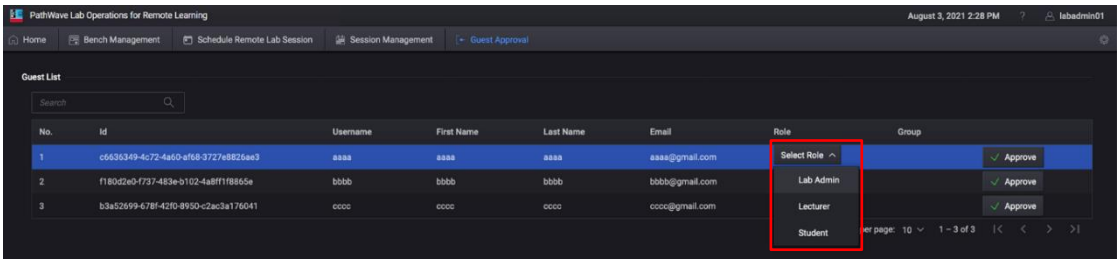


Guest Approval View

Accounts with administrator access level can approve and assign the appropriate access levels to new users. By default, new accounts registered will be assigned with the Guest role.



To assign and approve roles for new accounts, go to the Role column and click **Select Role** to display the available options in a drop-down list. Assign the desired role and click **Approve** for the changes to take effect.

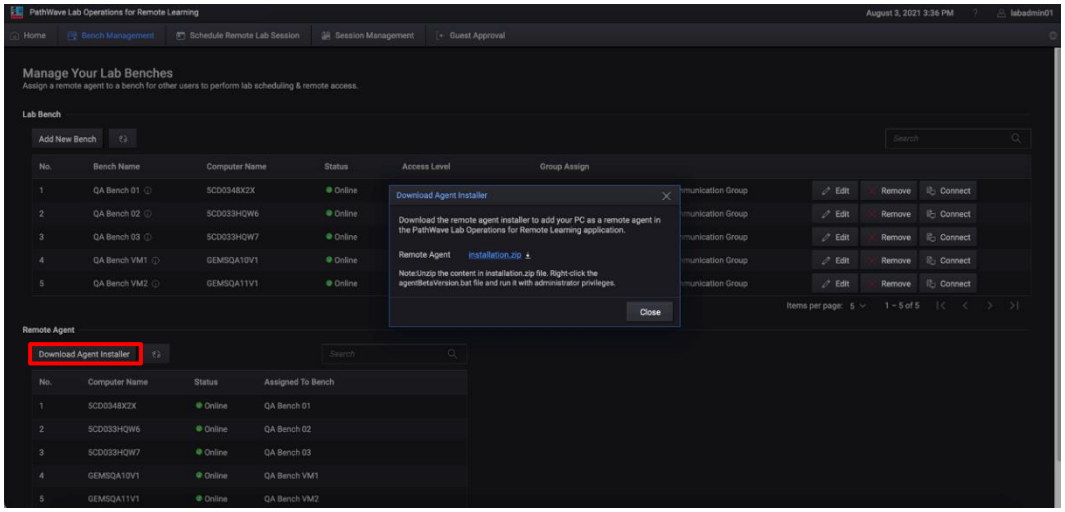


Install the Remote Agent

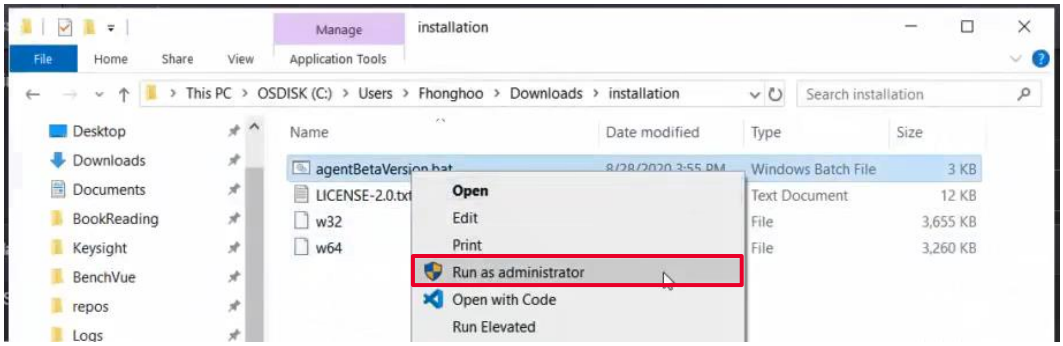
A remote agent is a .exe installation file that you will need run and install in the PC at the benches.

Before you can use the PC as a remote agent, you must perform the following steps to download and run the Remote Agent installation package to add it as an agent in the server.

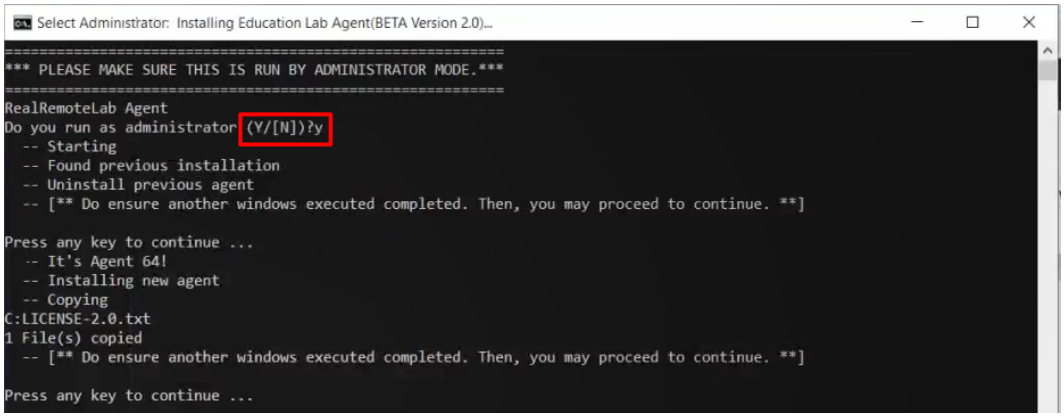
1 Click **Download Agent Installer** to see the pop-up window below. Click the installation.zip link.



2 Unzip the content in installation.zip file to the PC that acts as the remote agent. Right-click the **agentBetaVersion.bat** file and run it with administrator privileges.

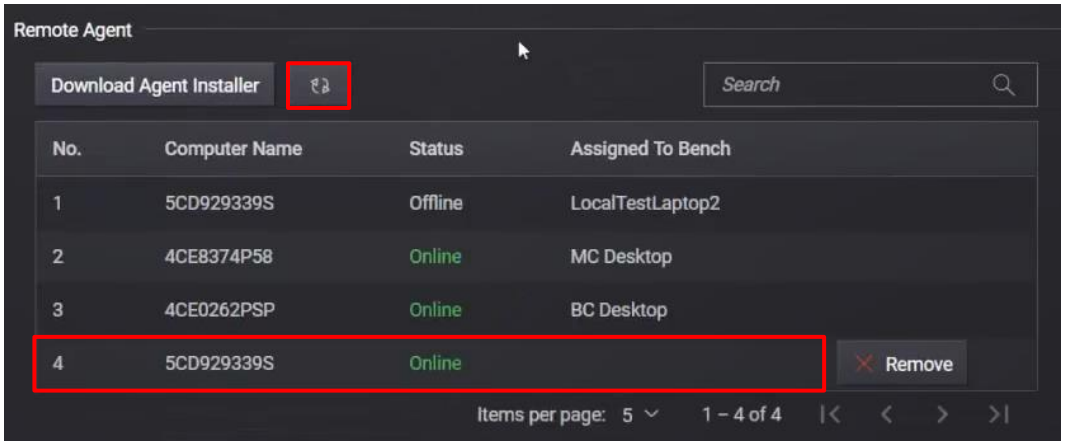


3 You should see a Command Prompt window where you will need to enter **Y** to initiate the installation process. Close this window when the installation has completed.



NOTE If you have previously installed an older version of the Agent in the same PC, running the batch file will uninstall the existing version before installing the latest version.

4 Return to the Home view and click **Refresh** to update the list of Remote Agent. You should now see the newly added Agent in the list.



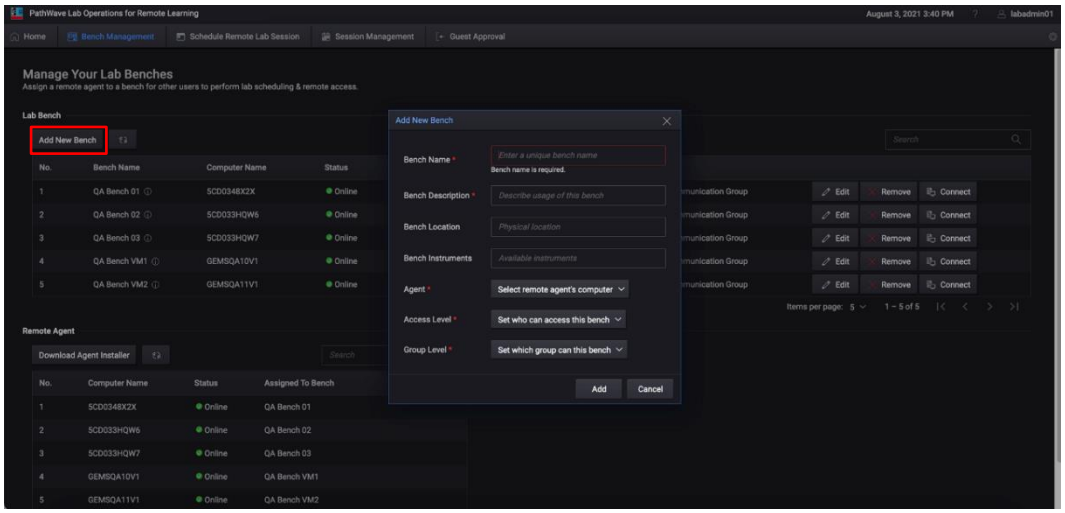
5 Repeat **Step 1** to **4** to set up a new Remote Agent in another PC.

Proceed to the next section to assign a bench to the newly added agent.

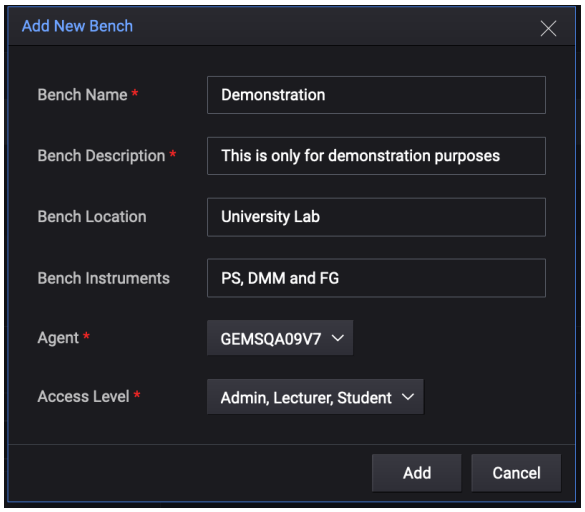
Add a New Bench

A bench is a location where you have set up the hardware connections and which the PC assigned as the remote agent will interact with.

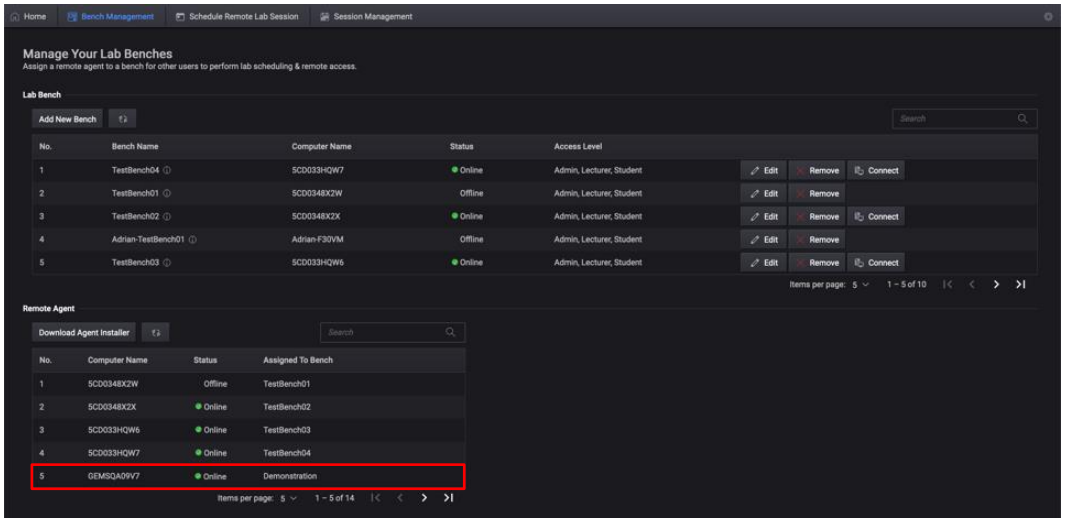
1 Click **Add New Bench** and enter the required details in the pop-up window below.



2 The example below assigns the Agent GEMSQA09V7 and the Administrator, Lecturer, and Student Access Levels. Accounts with Admin, Lecturer, and Student roles will be able to see this bench. Click **Add** when you have completed the form.



3 Upon successful setup, you should see the newly assigned remote agent to the respective bench.

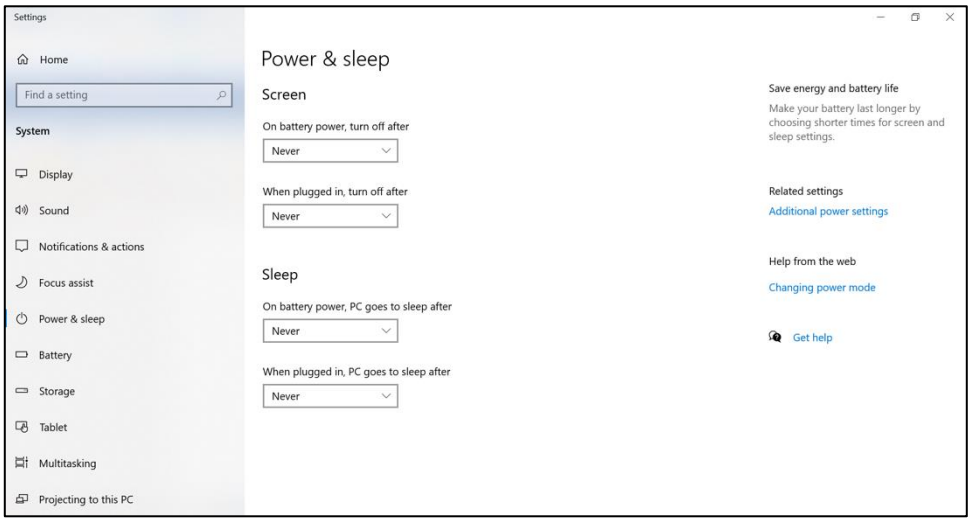


4 Unzip the content in installation.zip file to the PC that acts as the remote agent.

NOTE

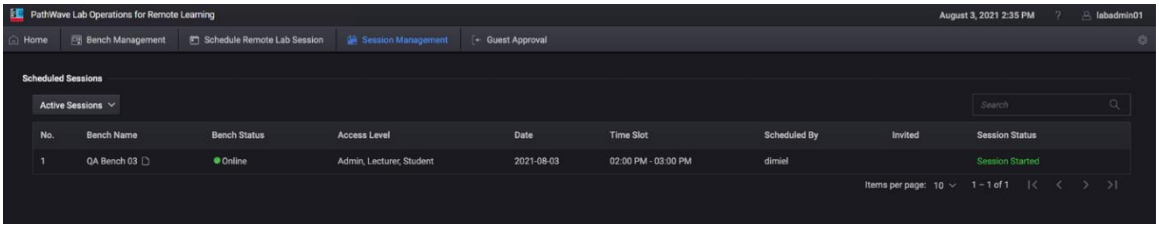
It is recommended that you disable the power saving and sleep mode of the Remote PC. This is so that the PC can continue to run as necessary without any disruption.

On the Start menu, search for 'Power & sleep settings' and turn all the settings to **Never** as shown below.



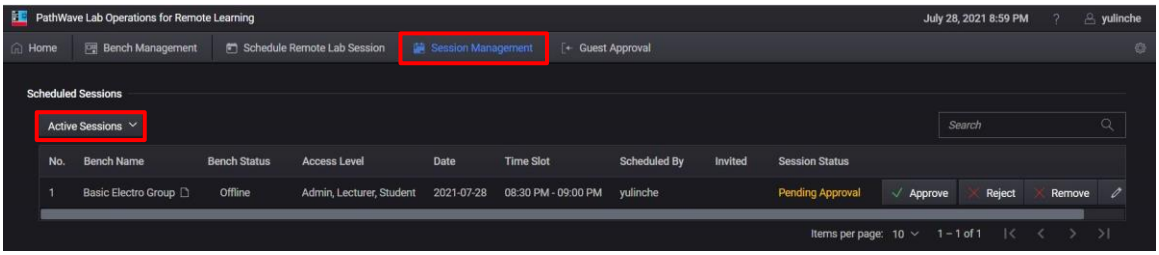
Session Management View

In this view, you will find the Active Sessions or Past Sessions as shown in the table below. Only the administrators can access this page and view the information of each session such as date, time, and status of the scheduled session.



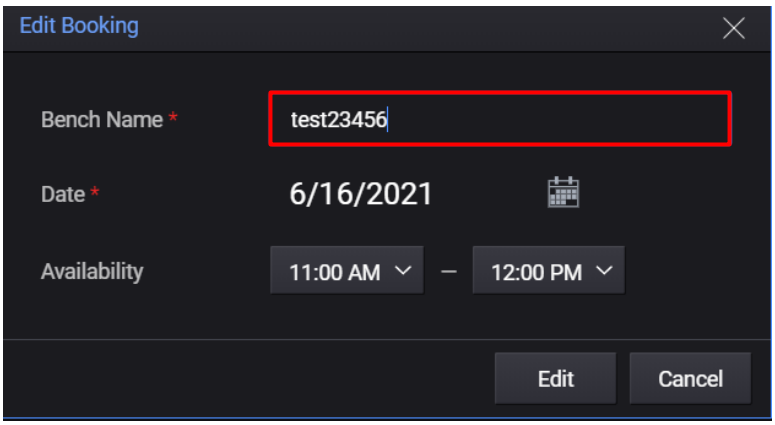
Manage Scheduled Sessions

Click **Session Management** to manage and view the status of the scheduled sessions. Use the drop-down list to only view either Active Sessions or Past Sessions in the table. Similarly, you can enter the keywords in the Search bar to filter and show only the sessions with the keywords.



The sessions submitted will approved by those with the administrator roles. Once approved, the system will send a confirmation email to the organizer (as per the username in the Scheduled By column).

The requests that are rejected will remain in the “Reject” status until the administrator removes or deletes it from the database. Administrators can reschedule sessions that falls under the Reject/Not approved category as shown below.



NOTE Students and lecturers are encouraged to check the information regarding your session in Home View as the administrator may reschedule your session.

Manage Remote Benches

Click **Bench Management** the view a list of test benches that you can sort according to their names, status, or access levels.

For each of the test bench, you have the option to Edit or Remove it from the table. The Connect button will only appear when the specific test bench is online.

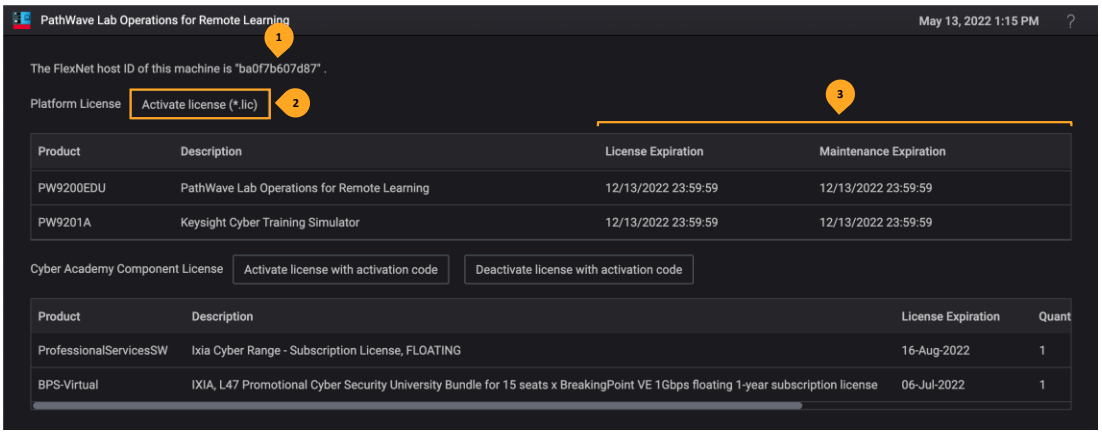
License Management

This section covers matters pertaining to the application and software license.

License and Support View

Go to **Software > Licenses and Support** to view license-related information:

- Platform License: The license to use PathWave Lab Operations for Remote Learning and Keysight Cyber Training Simulator appear here.
- Cyber Training Simulator Component License: The license(s) to use BreakingPoint and Ixia Cyber Range appear here.



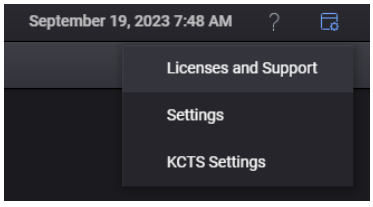
No.	Item	Description
1	FlexNet Host ID	This is the Host ID assigned to your machine/PC. The platform license(s) will use this ID.
2	License Activation	Click the respective buttons (next to each section) to activate or deactivate the license(s). Once activated, it will populate the information in the summary table.
3	License and Maintenance Expiration	This is when your license to use the application expires along with KeysightCare support and maintenance. After this date, you will not be able to access this application and will need to renew your license to continue using the application.

License Installation and Activation

For first time setups, Keysight will install and activate these license(s) on your behalf.

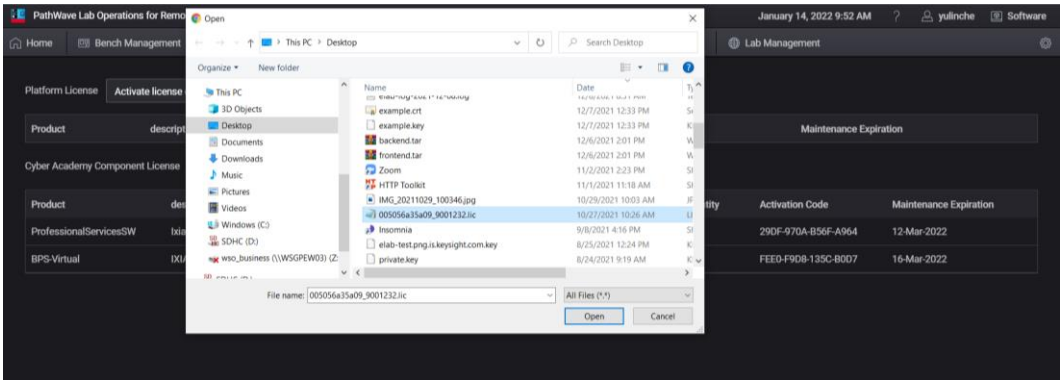
If you renewed your license(s), follow the steps below to install and activate it accordingly. Refer to your entitlement certificate and redemption email for more details.

1 Click on **Software > Licenses and Support** next to your Username to view the license(s) and related support services.

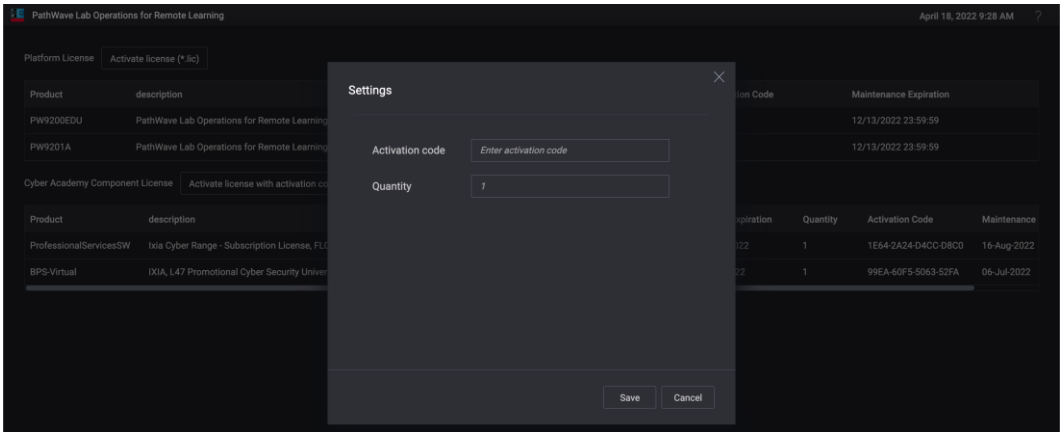


2 Use any of the options below to proceed with the license renewal/installation:

a Click **Activate license (*.lic)** and browse to the location of your license file. Select it and click **Open** to upload it to the server.



b If not already activated, retrieve the activation code from your email and click **Activate license with activation code**. Correspondingly, click **Deactivate license with activation code** to deactivate the desired license.



3 Once you have activated the license to use the platforms and application, the software is now ready to use. Subject to the role assigned to your account, proceed to the User Interface Overview or User Menu to learn more about the Keysight Cyber Training Simulator application.

NOTE To restart the license server if the license does not display after being uploaded, SSH into the virtual machine and issue the following command:

```
systemctl restart keysight-license
```

(Optional) Learning Tools Interoperability (LTI) Features

NOTE This section describes the steps to integrate PathWave Lab Operations for Remote Learning application into Learning Management System (LMS) system such as Moodle and Blackboard.

This is an optional task provided the university has an existing LMS system.

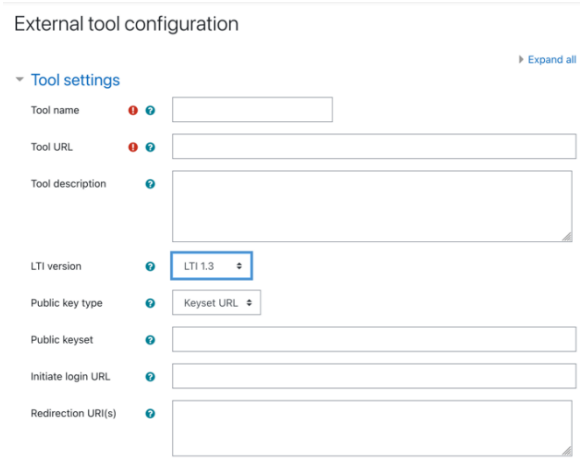
Integrate Moodle and PathWave Lab Operations for Remote Learning into LTI 1.3

You must use LTI version 1.3 in order to integrate Moodle as part of the LMS system.

Registering LTI 1.3 Tool

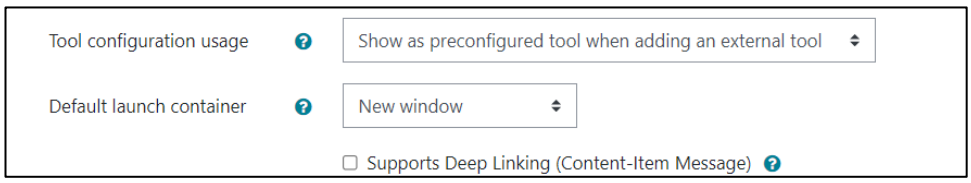
1. Navigate to **Site Administration > Plugins > Activity Modules > External Tool > Manage Tools**.
2. Under Manage Tools, select **Configure a tool manually** option.
3. Fill in the following information where you will replace the URL as Keysight provided.
   - **a** Tool name: Enter the desired name for PathWave Lab Operations for Remote Learning application. This is the name that you will see when you launch the course later. This example will use 'Remote Learning Application'.
   - **b** Tool URL: http://<Enter the URL given by Keysight>:30080
   - **c** LTI version: **LTI 1.3**
   - **d** Public Key Type: Keyset URL
   - **e** Public keyset: https://<Enter the URL given by Keysight>:30080/lti/settingJwkUrl
   - **f** Initiate login URL: http://<Enter the URL given by Keysight>:30080/lti/launch
   - **g** Redirection URL(s): http://<Enter the URL given by Keysight>: 30080/lti/tool
   - **h** Icon URL: https://<Enter the URL given by Keysight>/assets/favicon.png
   - **i** Secure icon URL: https://<Enter the URL given by Keysight>/assets/favicon.png

The completed form should appear as follows:

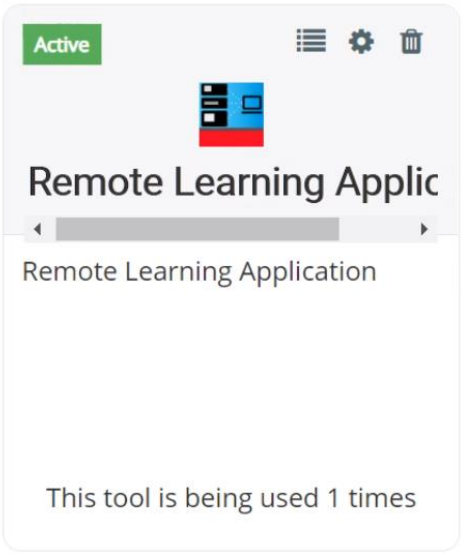


4 Tool configuration usage: Show as preconfigured tool when adding an external tool

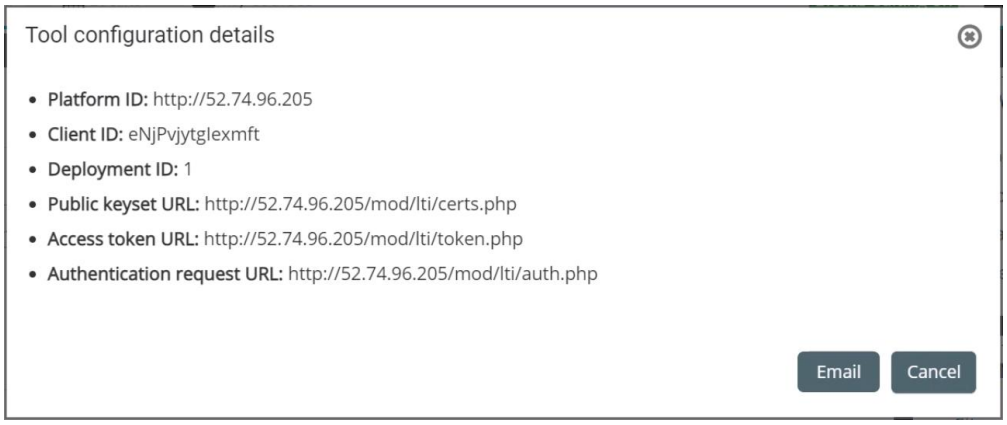
5 Set the default launch container to New Window.



6 Save the changes and you may begin to use the external tool according to the given tool name. This example will use the 'Remote Learning Application'.



Next, use the following information to set up the PathWave Lab Operations for Remote Learning application.



7 Log in to your PathWave Lab Operations for Remote Learning application as an administrator and click **Setting External Tool**.

8 Enter the details from Moodle and set up as an External Tool:

a Tool name: Enter the desired name for PathWave Lab Operations for Remote Learning application. This is the name that you will see when you launch the course later. This example will use the name 'Remote Learning Application'.

b Issuer: Issuer

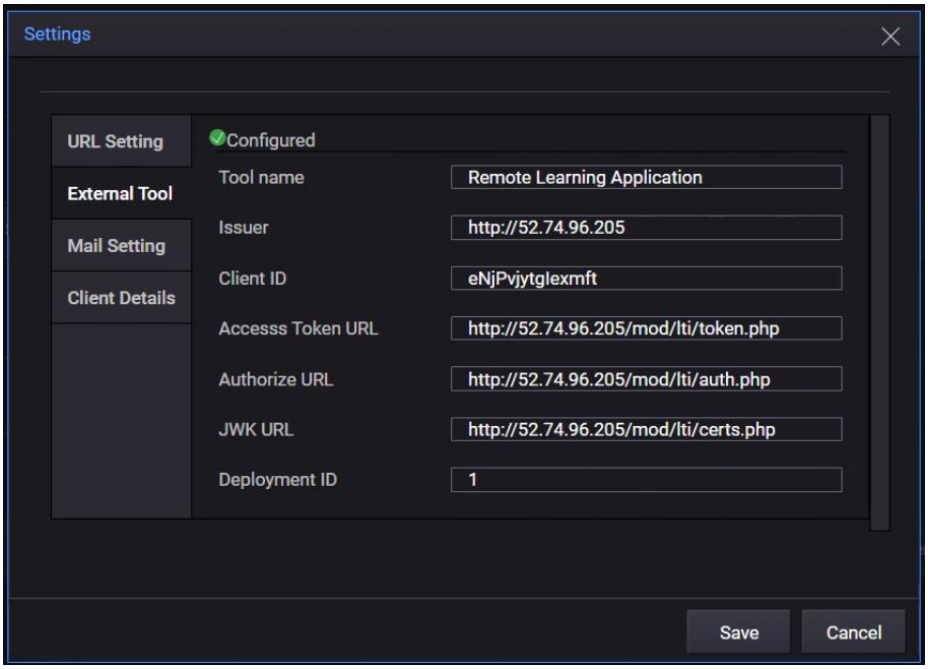
c Client ID: This will use the Application ID for the Moodle application

d Access Token URL: Access Token URL

e Authorize URL: Authentication Request URL

f JWK URL: Public Keyset URL

The completed settings should appear similar to the example below.

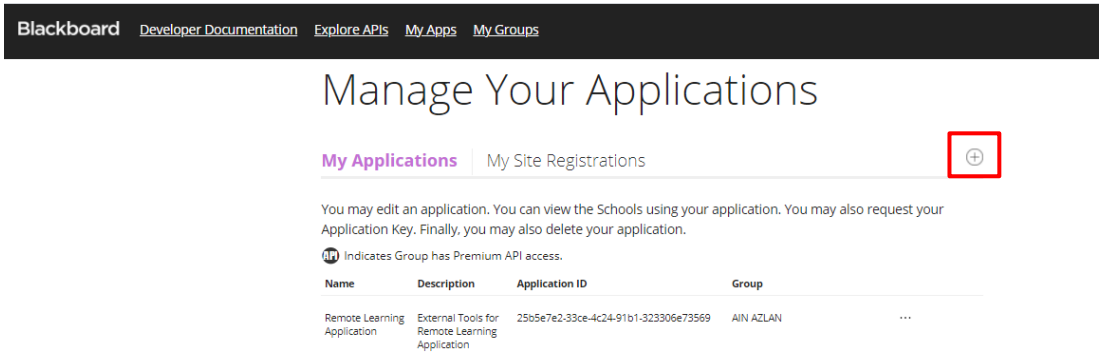


Integrate PathWave Lab Operations for Remote Learning into LTI 1.3 Blackboard

You must use LTI version 1.3 to integrate Blackboard as part of the LMS system.

1 Go to https://developer.blackboard.com/ and sign up as a new user. Log in with your credentials and password.

2 Once you are logged in, click **+** as shown below.



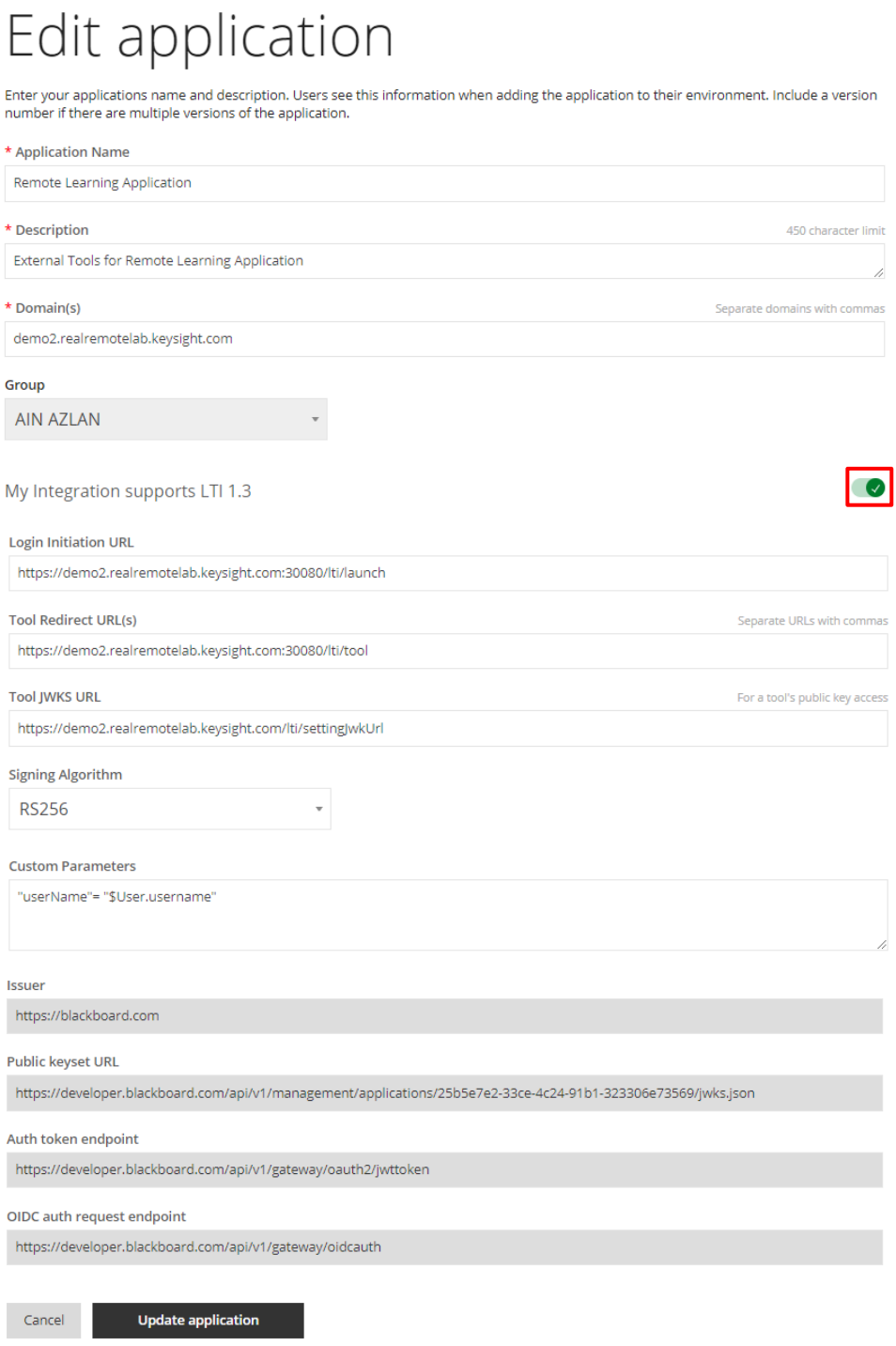
3 Enter the details below.

- **a** Domain: Enter the URL given by Keysight.
- **b** Login Initiation URL: https://<Enter the URL given by Keysight>:30080/lti/launch
- **c** Tool Redirect URI(s): https://<Enter the URL given by Keysight>:30080/lti/tool
- **d** Tool JWKS URL: https:// <Enter the URL given by Keysight>:30080/lti/settingJwkUrl
- **e** Signing Algorithm: RS256
- **f** Custom Parameter: "userName"= "$User.username".
- **g** Blackboard will provide the information for the Issuer, Public Keyset URL, Auth Token Endpoint, and OIDC Auth Token endpoint.

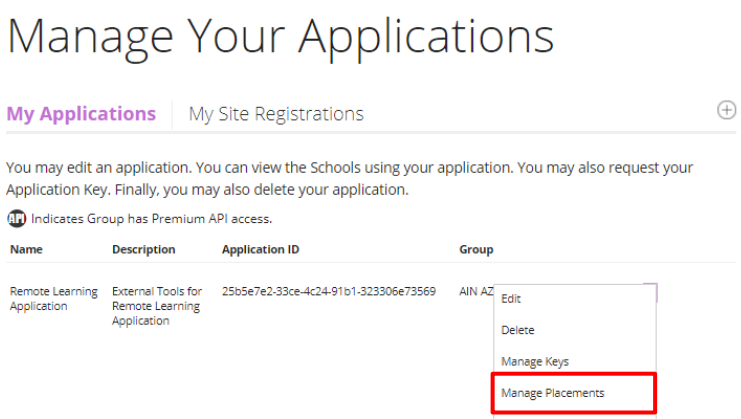
4 Click **Register Application** and **Generate API Key**.

NOTE The Application ID is the Client ID that you will use as you set up the PathWave Lab Operations for Remote Learning. This information is auto-generated after creating the application.

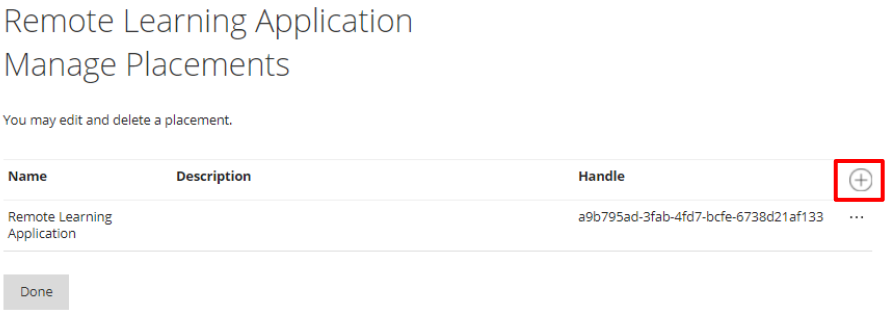
5 An example of a completed form is shown below. Click **Update application** when you are done.



6 Go to the page below and click **Manage Placement**.



7 Click **+** to add a new placement.



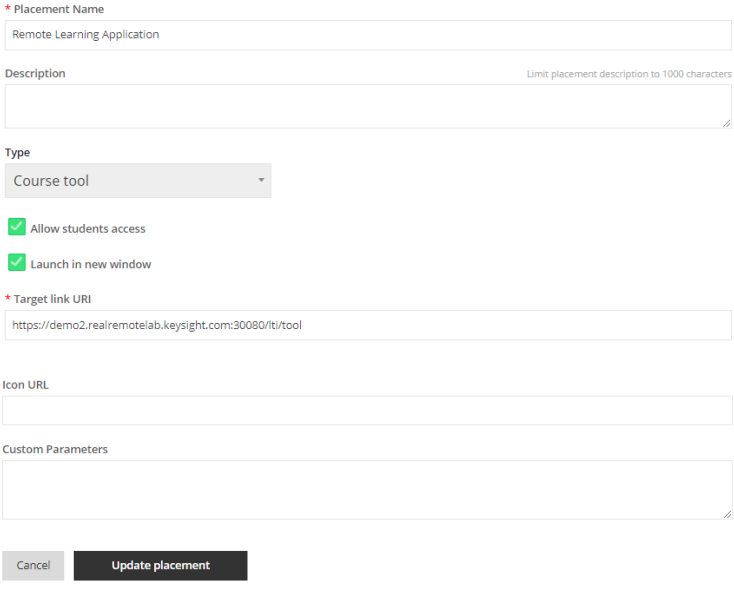
8 Fill in the information accordingly as shown in the image below.

a Type: Course Tool

b Target Link URL: https://<Enter the URL given by Keysight>:30080/lti/tool

c Select the 'Launch in new window' check box

d Click **Register placement**.

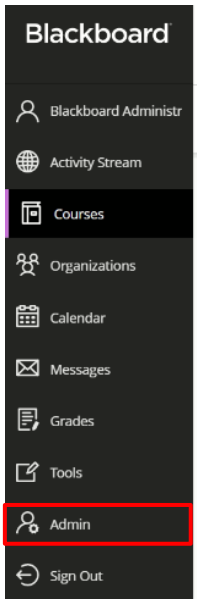


Add External Tools in Blackboard Platform

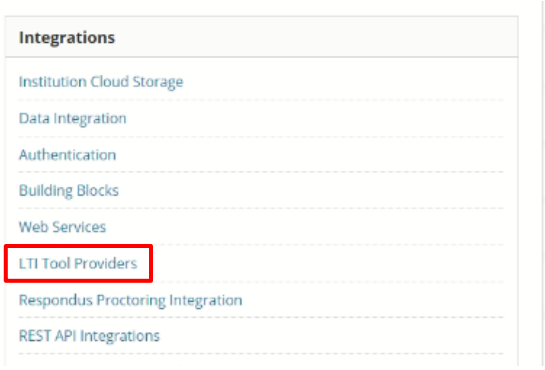
Proceed with the steps below to add an external tool in Blackboard.

1 Go to your Blackboard LMS system and log in with your username and password.

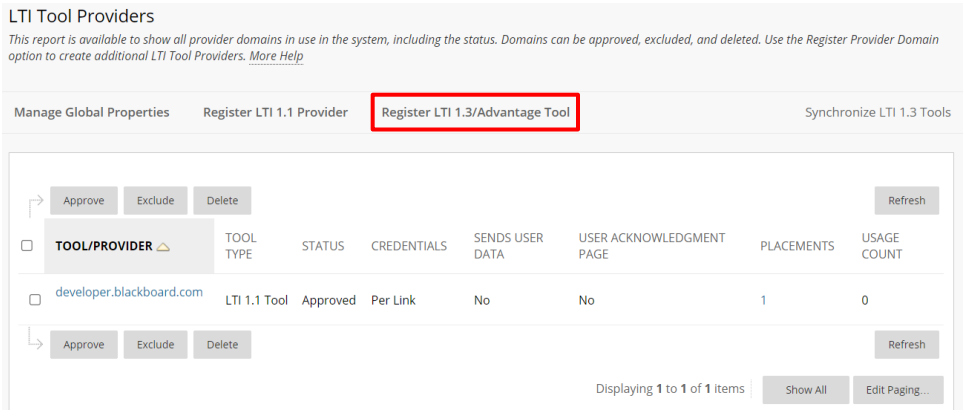
2 Click the **Admin** tab.



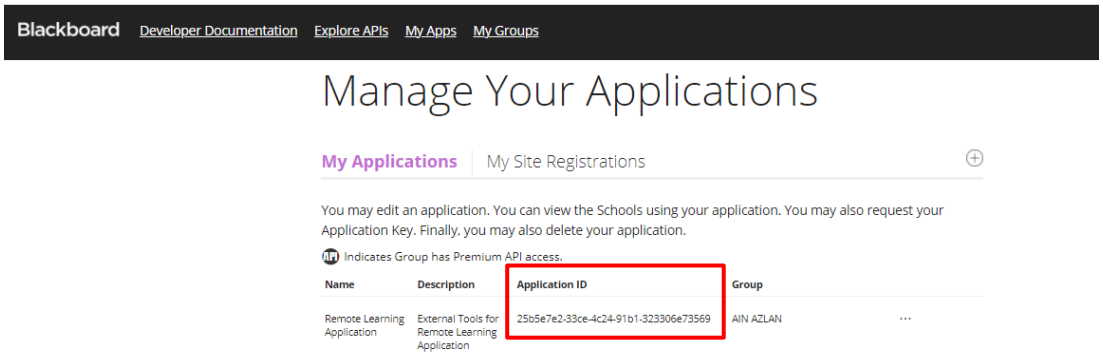
3 Select **LTI Tool providers**.



4 Click **Register LTI 1.3/Advantage Tool**.



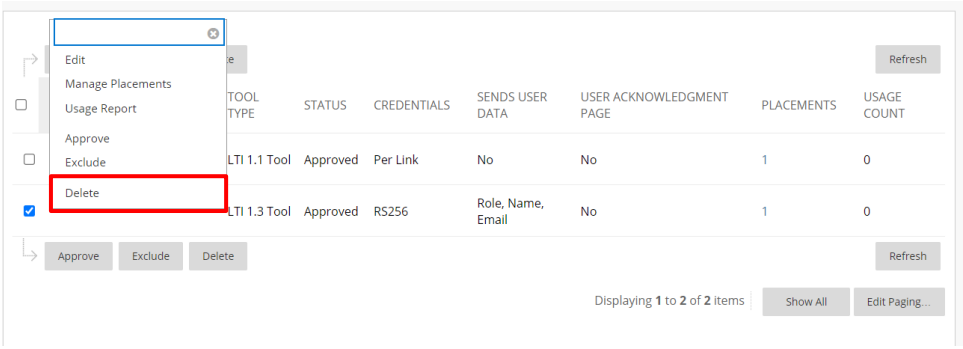
5 When prompted for a Client ID, retrieve and enter the Application ID as shown below (refer to step 6 of Integrate PathWave Lab Operations for Remote Learning into LTI 1.3 Blackboard) and click **Submit**.



NOTE

In the case if you have an existing tool that uses the same domain as your Remote Learning Application, you must delete the tool before you continue. You can only use one domain in Blackboard.

To delete a tool, select it from the list and click **Delete**.



6 Review the details. Select the **Approved** option as the tool status.

The following fields are read-only, but you can toggle the status of this tool

Client ID

25b5e7e2-33ce-4c24-91b1-323306e73569

Name

Remote Learning Application

Description

External Tools for Remote Learning Application

Deployment ID

6a39d24e-9e86-41c1-b882-16aeda48ea11

Initiate Login URL

https://demo2.realremotelab.keysight.com:30

Tool Redirect URLs

https://demo2.realremotelab.keysight.com:30

JWKS URL

https://demo2.realremotelab.keysight.com/lti

Domains

demo2.realremotelab.keysight.com

Tool Status

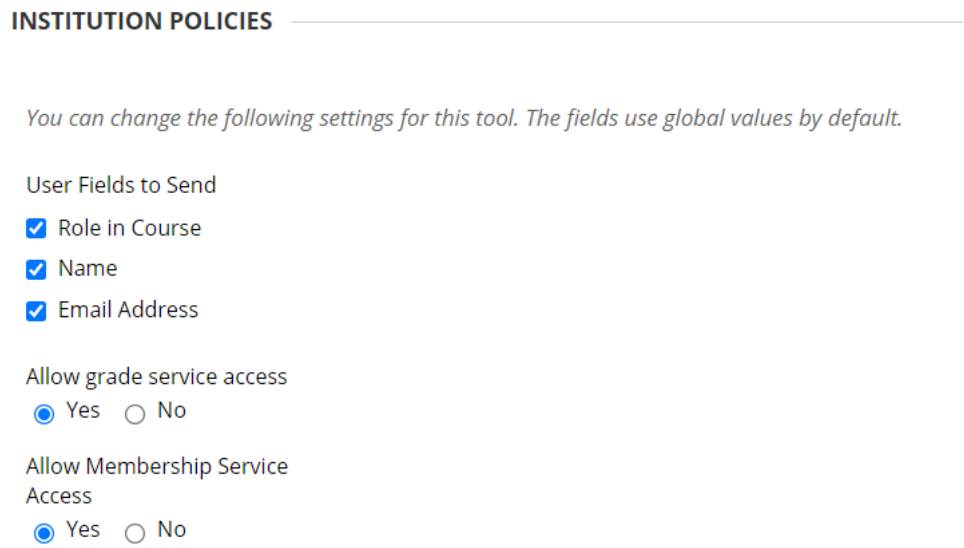
- (●) Approved
- ( ) Excluded

Tool Provider Custom Parameters

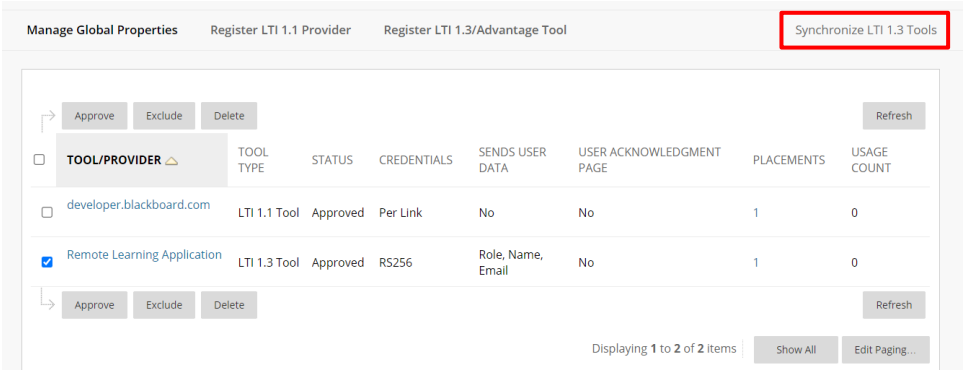
"userName"= "$User.username"

Enter any custom parameters required by the tool provider. Parameters must each be on their own line and be entered in "name=value" format.

7 Set the details as shown below and click **Submit**.



8 Click **Manage Placement** to view the tool added from Blackboard Developer. If there is no placement, click **Synchronize LTI 1.3 Tools**.



NOTE

Next, you may proceed to add a user, add a course, and enroll a user to the desired course.

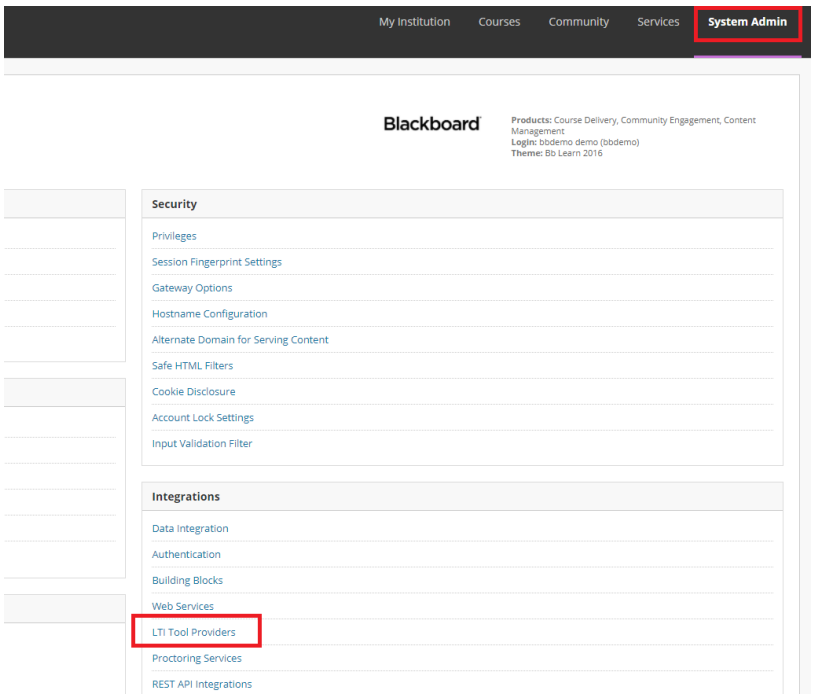
Go to Blackboard Help (https://help.blackboard.com/Learn) for instructions on how to perform these actions.

Obtain the Deployment ID

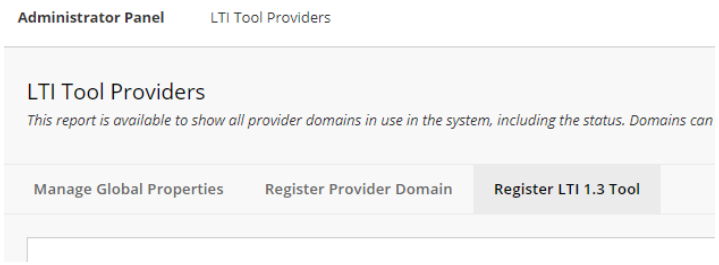
Next, you will log in with your account and launch the PathWave Lab Operations for Remote Learning application.

1 Log in to your administrator account on Blackboard.

2 Navigate to the **System Admin tab** and click **LTI Tool Providers** as shown below.



3 Click the **Register LTI 1.3 Tool** tab.



4 Enter the Client ID, which is the Application ID created in Integrate PathWave Lab Operations for Remote Learning into LTI 1.3 Blackboard. Click **Submit**.

5 In the next screen, copy the Deployment ID and paste it in the Deployment ID field.

6 Click **Activate**.

7 Make the following changes in Blackboard.

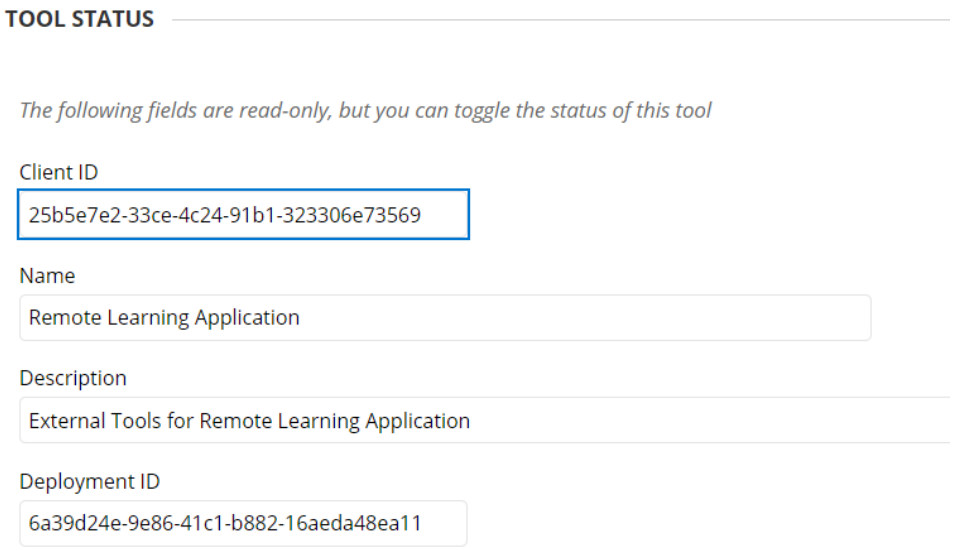
- **a** Tool Status: Set as **Approved**
- **b** User Fields to Send: Select all three check boxes
- **c** Allow grade service access: Set to **Yes**
- **d** Allow Membership Service Access: Set to **Yes**

Add Details to the Application

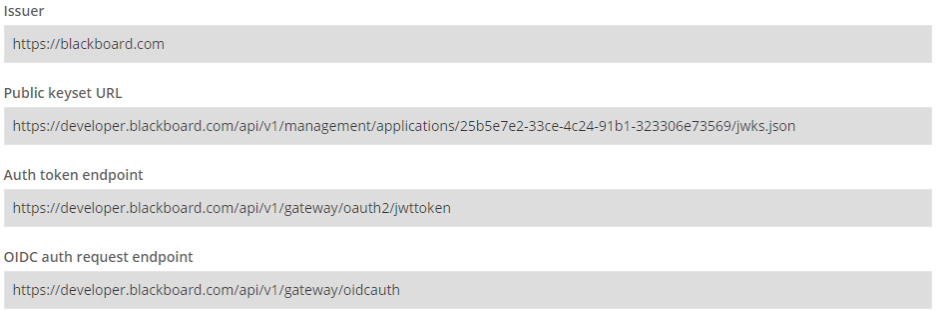
1 Go to your PathWave Lab Operations for Remote Learning application and log in as an administrator. Click **Setting External Tool**.

2 Enter the same information as you did for the LTI 1.3 Tool Provider.

- **a** Issuer: Issuer
- **b** Client ID: Application ID
- **c** Access Token URL: Auth token Endpoint
- **d** Authorize URL: OIDC Auth request endpoint
- **e** JWK URL: Public Keyset URL
- **f** Deployment ID: Refer to Obtain the Deployment ID.



3 The completed form will appear as below.



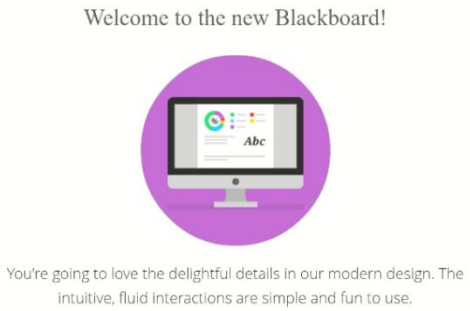
Launch the Application in Blackboard

Before you launch the PathWave Lab Operations for Remote Learning application in Blackboard, you must first log in with your account.

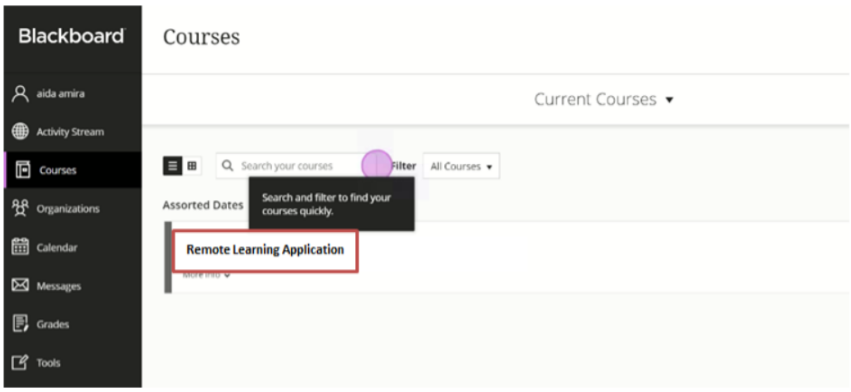
NOTE For latest information on how to launch application, go to Blackboard Help (https://help.blackboard.com/Learn).

---

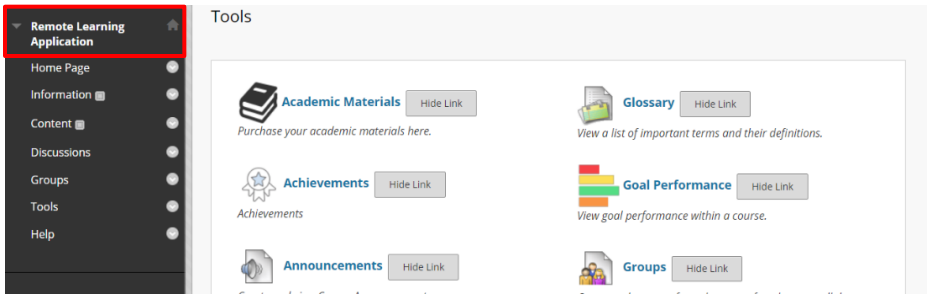
1 Log in to launch the course. You should see this page.



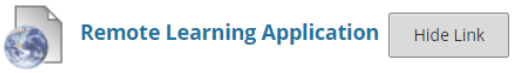
2 Select the course.



3 Click **Remote Learning Application** and scroll downwards until you see the course tool.



4 Click the course tool shown below to launch **Remote Learning Application**.



General Troubleshooting

Seeing a Blank Screen

A stable internet connection is required when using this application.

1 Check your internet connection

2 Restart your remote PC at the bench

Application Ceases to Respond or Bench Freeze

This could happen when the participants are downloading large files simultaneously in a session. The application supports a maximum of two users to perform downloads at the same time.

NOTE To optimize the use of this application, it is not recommended to stream videos on the remote bench PC.

---

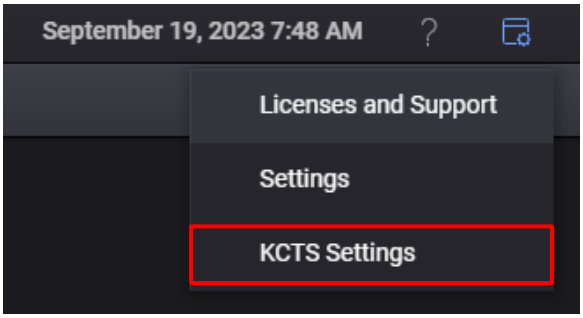
1 All participants in the session are recommended to exit and rejoin the session.

2 Restart the web browser that you are using to access the application.

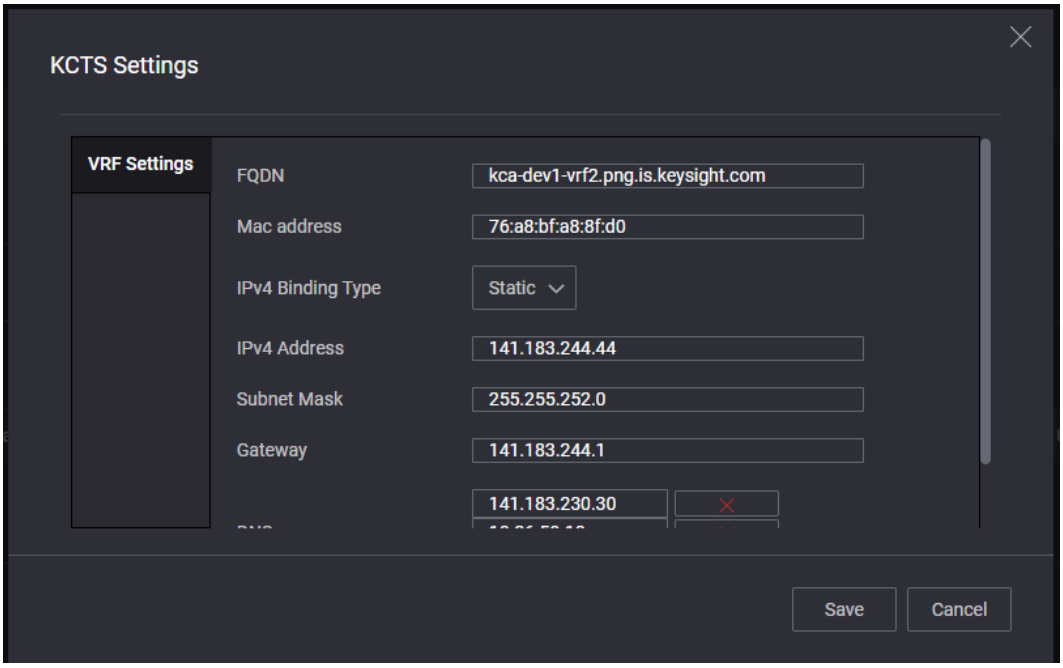
VRF Settings

The Keysight Cyber Training Simulator utilizes a virtual router to perform Virtual routing and Forwarding (VRF) for users to access the virtual machines in the virtual labs. In the case where the virtual router's IP needs to change (for example, relocating the system to another subnet), follow the steps below to perform network configuration changes to the virtual router.

To access these settings, click **Software > KCTS Settings**.



Follow the steps below to perform network configuration changes to the virtual router.



1 Change the IP, subnet mask, gateway, DNS, and FQDN (if required) then click **Save** to apply the changes.

2 On the machine that is accessing the VM on the virtual labs, ensure that static route is configured so that the traffic for subnet 100.100.0.0/16 and 100.64.0.0/24 will be routed to the virtual router defined in VRF Setting.

3 For example, on a Windows machine that is on the same subnet as the virtual router, you must execute two lines of static route to access the virtual lab environment like example below:

```
route -p add 100.100.0.0 mask 255.255.0.0 VRF_IP
route -p add 100.64.0.0 mask 255.255.255.0 VRF_IP
```

NOTE Before running the command, ensure that VRF_IP is replaced with the new virtual router IP.

Frequently Asked Questions

1 Question: How do I reset the Cyber Security Operations Platform (CySOP) admin password?

Answer: Contact Keysight support (www.keysight.com/find/assist) to reset the password.

2 Question: As Keysight has set up the Cyber Training Simulator system, I do not know the admin login and password to access KCTS. Where can I find the KCTS admin login and password?

Answer: Retrieve the details of the admin account from your entitlement certificate.

3 Question: How do I create my own virtual lab?

Answer: Adding new virtual lab to the system is not supported in the current release and is scheduled for the next upcoming release.

Recommended Password Practices

Passwords are used to protect access to confidential information. This includes Keysight software as well as any personal accounts you may have. A compromised password could result in a leak of your confidential information, an attack on Keysight's systems integrity and availability.

A compromised password means that someone could use your account to access your personal information to which you have been granted permission. At the very least, this could lead to misuse, but it could also result in financial loss. You may be held responsible for the misuse since the account belongs to you.

Here are some tips to keep your password safe and keep it from being compromised.

- Choose strong passwords

  A strong password consists of a few dimensions. The main dimensions are the length of the password and the character sets used to create the password.

  Keysight's password recommendation is a minimum of 12 characters for standard accounts and a minimum of 15 characters for accounts with administrative privileges. The passwords must include a mix of at least 3 of the 4-character sets - upper and lower-case letters, numbers, and special characters.

- Do not reuse past passwords

  It is possible that older passwords were cracked, so do not repeat previously used passwords.

- Do not use dictionary words as your password

  Hackers use special computer hardware and software to crack passwords. Dictionary word passwords will not stand up to a password cracking attack.

- Do not use terms that can be related to you

  These are things such as your name, username, company, company products/terms, the names of your children or relatives, dates, locations, sports teams, pet names, or any combination of these.

- Do not use patterns in your password

  Keyboard patterns, such as 'qwertyuiop[]', '1qazxcvbnm,.', 'aaaaaabbbbbb', or '1234567890-=' are well known and easily cracked.

- Do not write passwords down, anywhere

  Memorize them or use a password management application (see below).

- Use a different password for every different account

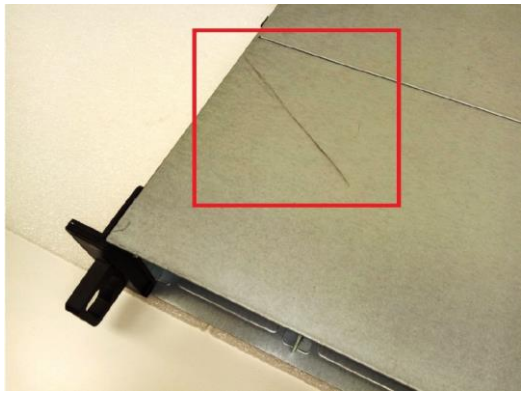
  It is the best practice to use a different password for every different account. This way if one account is compromised, then the attacker will not have access to any of your other accounts. Using a password manager helps keep track of different login credentials.

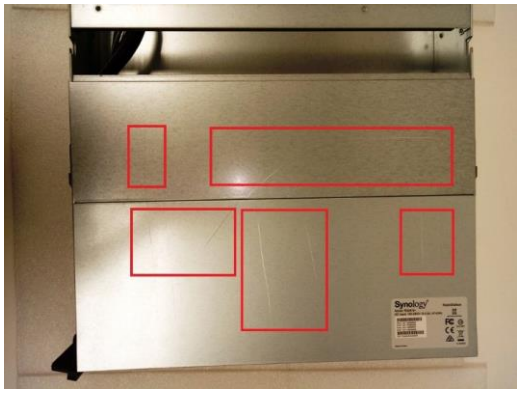
Criteria for Warranty Claims

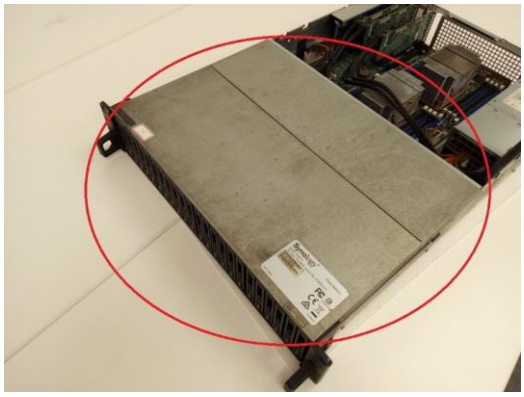
It is important to ensure that the hardware appearance is in good condition before any warranty claim. The warranty will be voided if Keysight concludes that the hardware appearance is unacceptable.

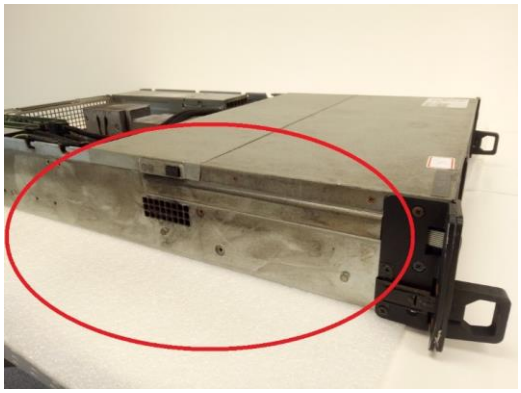
Here are some examples of hardware appearances which Keysight considers invalid for warranty claim.

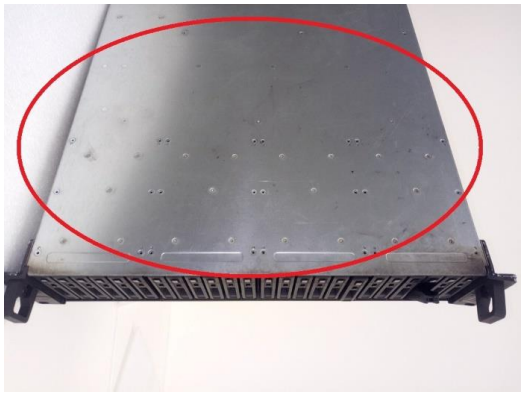
– Scratched, rusted, dirty, or dusty surfaces.



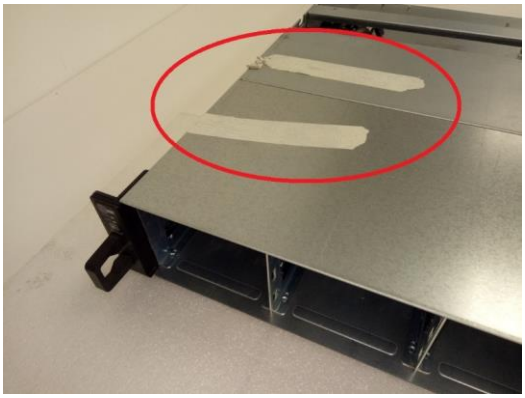




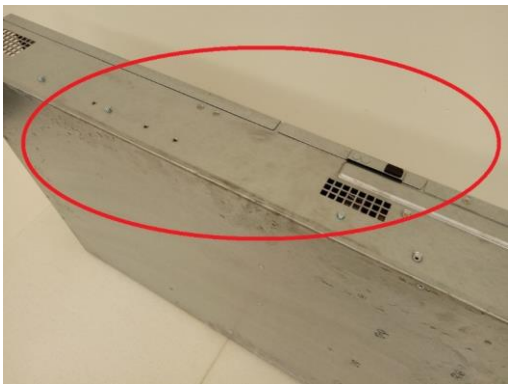


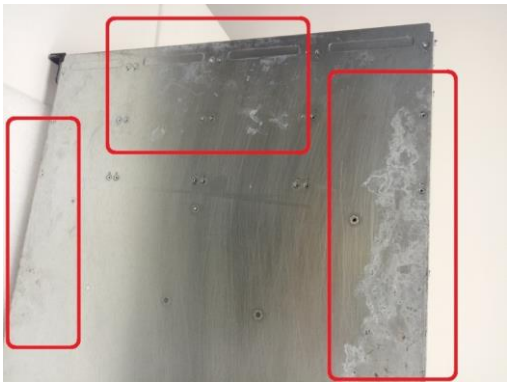


– Pasted with sticky tapes, anti-collision materials, or glue residuals.

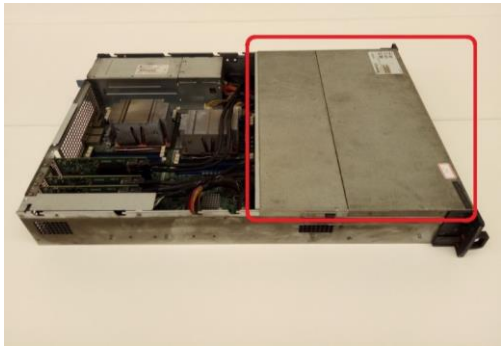
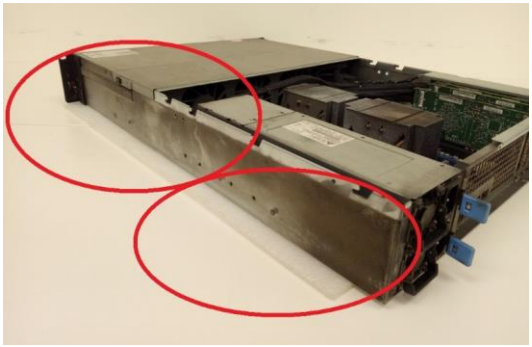


– Dirt marks such as spilled liquid or food.

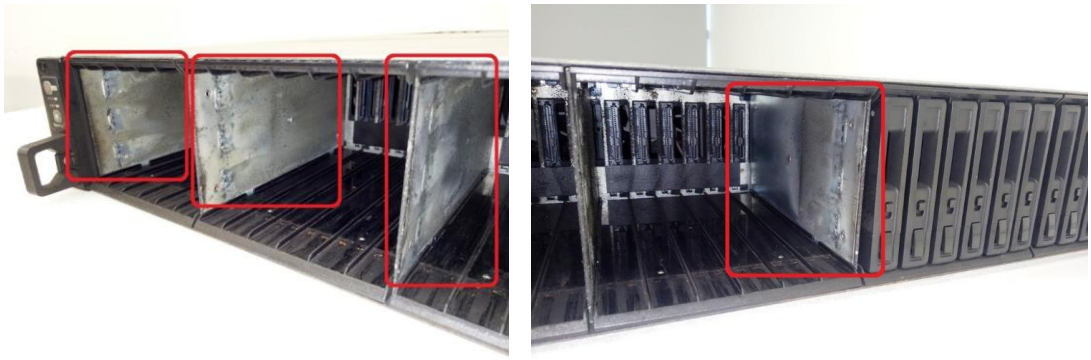




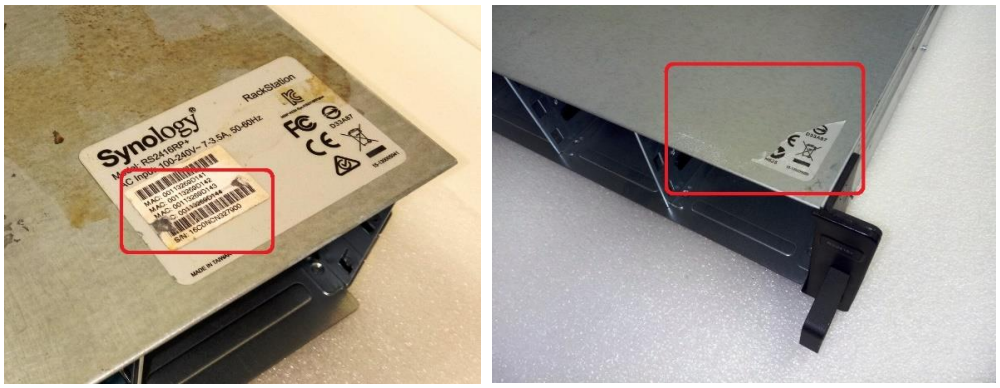
– Burning marks or smoke stains.

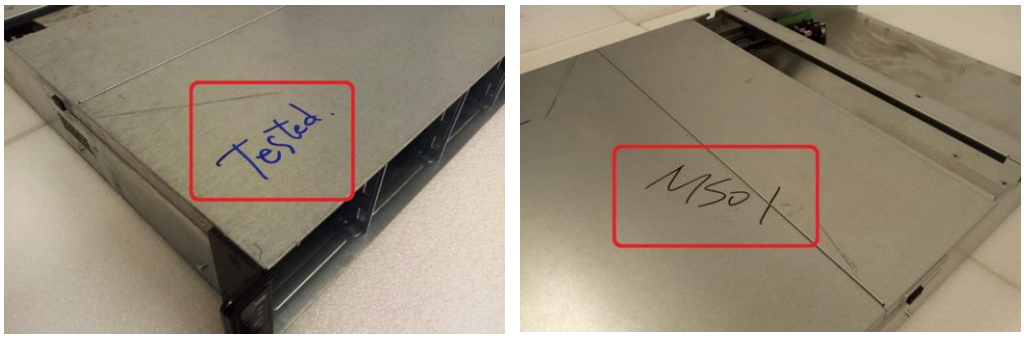
– Rusts on hard drive tray slot.



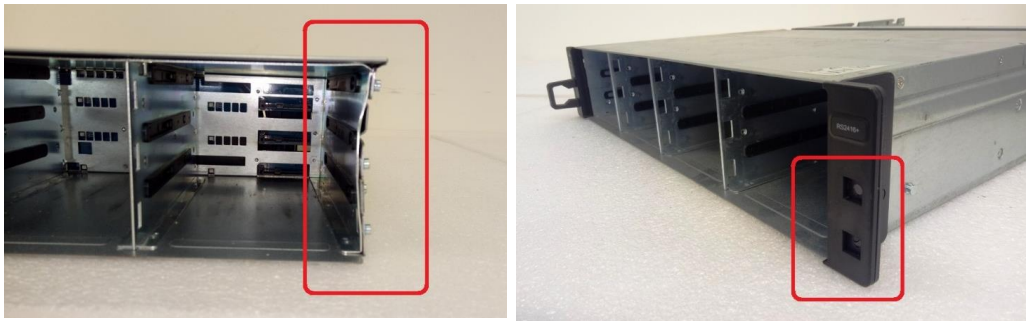
– Missing or damaged product stickers (serial number), resulting in unreadable information.



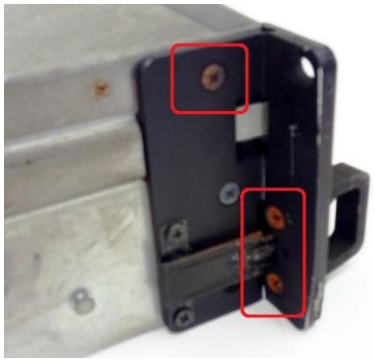
– Scribbled texts or marks

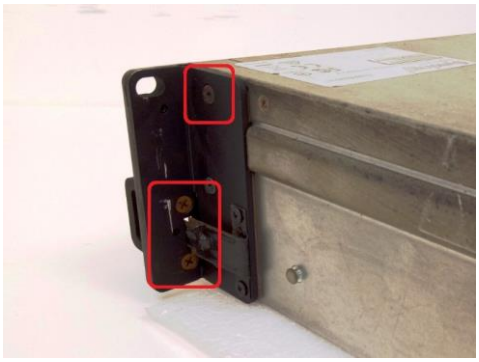


– Missing original parts (such as metal handles).

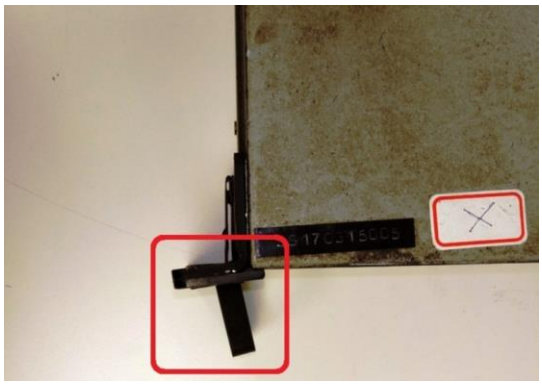


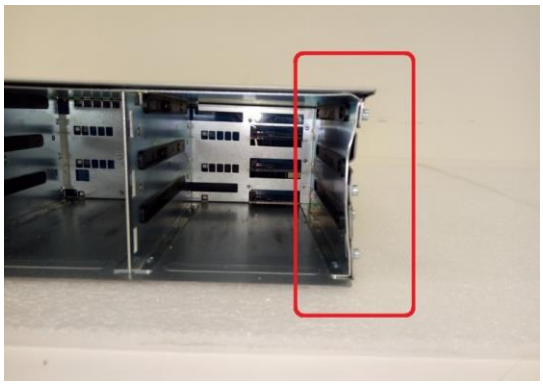
– Rusty fixing screws on handles.



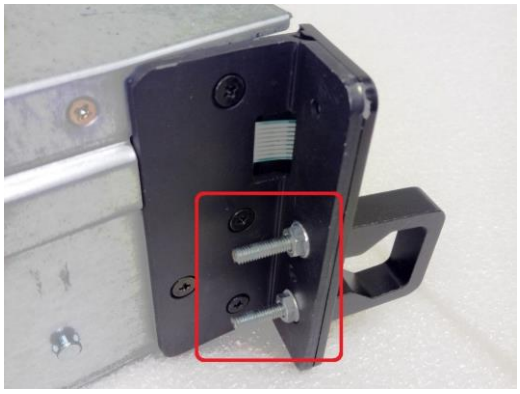


– Deformed body structure or metal handle.



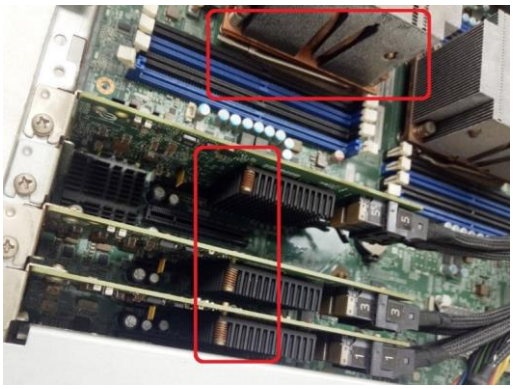


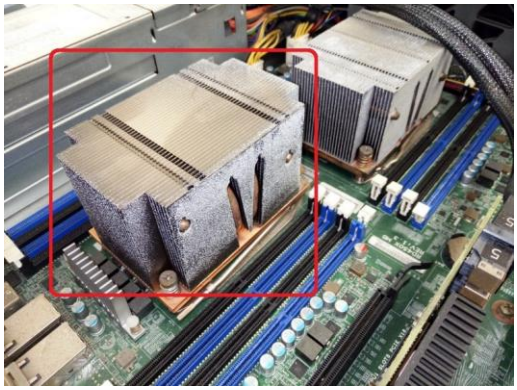
– Change of fixing screws on handles to non-original ones.

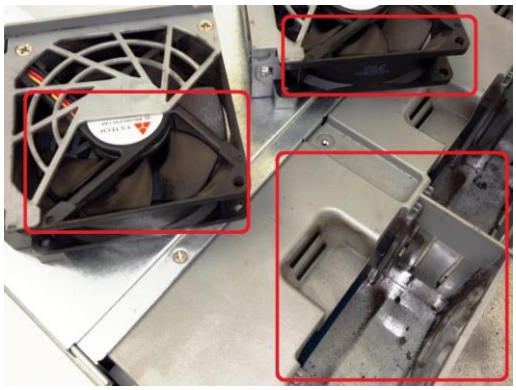


– Mismatched serial number between the motherboard and enclosure.

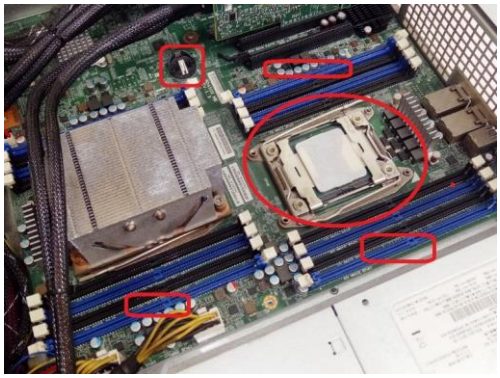
– Rusted, dirty, or dusty components.

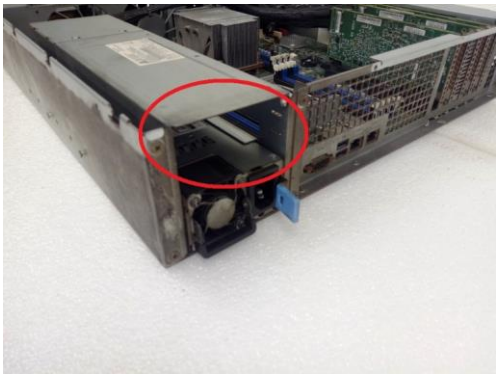




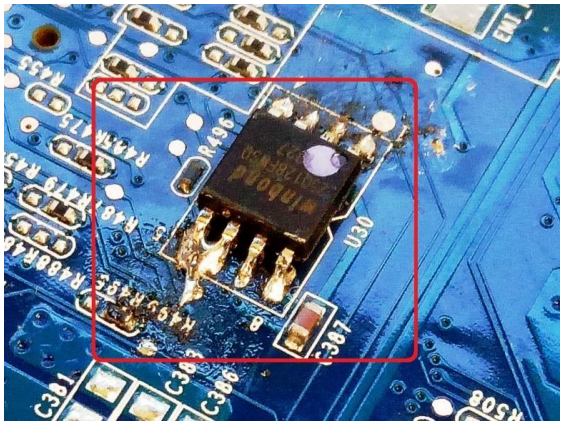


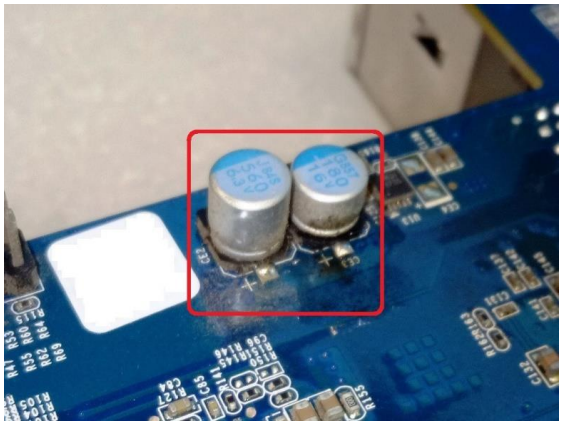
– Missing original components (LED boards/cables, battery, heat sink, memories, fans, PSU, and so forth).





– Disassembled or re-welded motherboard components.





This information is subject to change without notice.
© Keysight Technologies 2023
Edition 1, October 2023
Printed in Malaysia

CY101-90004
www.keysight.com